



SAPIENZA
UNIVERSITÀ DI ROMA

Design Methodologies for Cryptographic Hardware with Countermeasures Against Side Channel Attacks

by
Davide Bellizia

A thesis submitted in partial fulfillment of the requirements for the degree
of Doctor of Philosophy in Information and Communication Technology
at

Sapienza University of Rome
Department of Information Engineering,
Electronics and Telecommunications (DIET)
Cycle XXX

Candidate

Davide Bellizia

ID Number: 1234474

Thesis Advisor

Prof. Giuseppe Scotti
DIET, Sapienza Univ. of Rome

Thesis Co-Advisor

Prof. Domenico Caputo,
DIET, Sapienza Univ. of Rome

February 2018

Thesis defended on 22 February 2018.

This thesis was evaluated by the two following external referees:

Prof. Tommaso Addabbo, University of Siena, Siena, Italy

Prof. Davide De Caro, University of Naples "Federico II", Naples, Italy

The time and effort of the external referees in evaluating this thesis, as well as their valuable and constructive suggestions, are very much appreciated and greatly acknowledged.

Design Methodologies for Cryptographic Hardware with Countermeasures Against Side Channel Attacks

Ph.D. thesis. Sapienza – University of Rome

ISBN: 000000000-0

© 2017 Davide Bellizia. All rights reserved

This thesis has been typeset by L^AT_EX and the Sapthesis class.

Version: March 28, 2018

Author's email: bellizia@diet.uniroma1.it davidebellizia@gmail.com

*Dedicated to
my grandfather Costantino,
who passed away too early
to see the end of this adventure.*

Ennyn Durin Aran Moria. Pedo
Mellon a Minno. Im Narvi hain
echant. Celebrimbor o Eregion
teithant i thiw hin.
- Inscription on the Doors of Durin
(*Lord of the Rings - The Fellowship
of the Ring, J.R.R. Tolkien*)

Abstract

Scientific Context

In the context of sensible data protection, technological aspects of circuits that implement cryptographic primitives have played a key role. Since the first appearance of physical-based attacks in 1996, companies and academia made effort in proposing design methodologies to provide protection from such kind of attacks. In a physical attack, the adversary does not attack directly the weakness of the cryptographic algorithm, as in classical cryptanalysis. Instead of mathematically attacking the algorithm, the adversary targets the physical implementation of the algorithm itself. In general, cryptographic primitives are implemented using electronic integrated circuits (ICs), making use of Very Large Scale Integration (VLSI) design techniques. The critical issues concerning these kind of attacks is that the adversary can recover sensible data from a cryptographic device taking advantage of its physical emissions, even without destroying the chip. Such kind of attacks, called *Side-Channel Attacks* (SCAs), are usually non-invasive, since the adversary may be able to capture and measure physical emissions without mechanically opening the chip. Non-invasive attacks are made possible by the fact that a device may offer several physical channels which leak sensible information during the elaboration of data and allow the recovery of secret keys. Such channels may be the power consumption, the electromagnetic emission, the timing of operations or analysis of faults that an attacker can eventually induce from the outside (in the latter case we speak of semi-invasive attack). To counteract such attacks, there are several techniques, which operate at different levels of abstraction of the design flow, from the lower comprising individual logic gates passing through the register-transfer level (RTL) up to the algorithmic level.

Objective of The Thesis

The pervasive diffusion of cryptography in daylife activities (e.g. smart-cards, data logger, medical and healthcare devices, Internet of Things nodes, etc.) has changed the way we think about cryptography, and how the security is intended to be. From the designer point of view, the security of a cryptographic implementation has to be provided not only in terms of classical cryptanalysis. Real and physical implementations have to deal with *physically observable leakage*. As reported in [59], "*A security system is as strong as its weakest part*". It is clear that if a concrete implementation of a cryptographic algorithm is proved to be resistant to cryptanalysis but its physical emissions can still leak information, the device is still *not protected*. The latter aspect is strongly related to the VLSI implementation of the secure system. The role of designers in this context is to build secure systems that can be proved to be resistant also under the point of view of *physical observable cryptography* [104]. The analysis and evaluation of such physical emission plays a key role in the design of a secure system, since physical behaviors of a device may dramatically reduce the level of security provided by the algorithm itself. It has to be noted that in literature there isn't yet a general theory about *physical security*. Nevertheless, this recent

field of research contains several sub-fields, cutting transversely multiple aspects of a digital design and analysis&evaluation of data-dependency of physical emissions.

It is clear that building a system which is SCA-tolerant requires heterogeneous skills, ranging from VLSI design, through measuring real-world physical emissions, to statistical analysis. In the design of a cryptographic implementation, the designer has to be able to investigate possible sources of information leakage through side-channels, and thus, constraining the whole project to reduce as much as possible the data-dependency of physical emissions. It is worth noting that the technology aspect is critical, since the behavior of physical emissions could change in different technologies. Moreover, advances in technologies allow also more powerful attack procedures. Hence, the evaluation of the security of devices needs to be continuously updated, in order to provide new design methodologies to reduce the possibility of next generations of secure devices to be broken.

Although is almost impossible to cover all possible sub-fields in SCAs context, in this thesis work we focus on specific arguments regarding the security issues due to information leaked through power consumption of cryptographic devices. More specifically, the aim of this work is to give new design methodologies to thwart *Power Analysis Attacks* (PAAs) [84] under the perspective of recent issues arose with new technologies. In the last twenty years, the Complementary Metal-Oxide-Semiconductor (CMOS) technology is changed, reducing the minimum feature size from 250nm down to 10nm. At the same time, issues in security originated by reduced geometric sizes are evolved too. Therefore, improvements in how security devices are designed are discussed in this thesis work, giving also new ways to evaluate the vulnerability of new designs with new attack procedures and techniques. New PAA-countermeasures are proposed in this work, to provide solutions that are able to cope with the main problems related to typical non-idealities of modern integrated circuits.

In this context, this work proposes new methodologies and techniques to design hardware countermeasures against PAAs, regarding recent issues highlighted by latest technologies. The presence of second-order effects, often neglected in classical VLSI designs, impacts dramatically on the level of security of cryptographic devices. Most critical non-idealities in CMOS implementations are related to electrical mismatches. Commonly adopted gate-level PAA-countermeasures make use of Dual-rail Pre-charge Logic (DPL) paradigm. It is known that they suffer significantly from capacitive and timing mismatch from a physical security point of view, even vanishing the presence of such kind of countermeasures. These implementative-level aspects have to be mitigated in order to obtain the minimization of data-dependent power consumption. It has to be noted that electrical mismatches are expected to grow with the technology scaling [125].

The onset of deep sub-micron technologies have led to a strong increase in static power consumption's importance on the power budget of a device. It has been demonstrated that static power consumption is also relevant in terms of physical security. Most of works in PAAs context concerns about dynamic power consumption exploitation and countermeasures, and only few of them discuss about security issues due to static power. The adoption of static currents to recover sensible information from cryptographic implementation arises new issues and poses new requirements in designing secure systems. An in-depth analysis of security issues due static power

in nanometer technology is given in this thesis work. Static and dynamic power consumption exploitation require different measurement setups due to the different nature of their physical reason. New findings in static power exploitation have been addressed in this work.

Outline of the Thesis

This thesis is composed by seven chapters, dealing with novel PAA countermeasures and attack procedures. The work is structured as follows.

In Chapter 1, the context of SCAs is presented. Since the protection of sensible data is considered a major concern in modern devices, the importance of technological aspects have to be addressed properly. Although cryptographic algorithms are considered trustworthy in terms of cryptanalytic resilience, devices that implement such algorithms may not be physically secure. It has been proved that physical emissions in electronics devices can be related to devices' activity. Hence, hardware implementations of cryptographic algorithms have to deal with unavoidable physical emissions.

In Chapter 2, common PAA attacks and leakage assessment procedures are briefly recalled. The verification of robustness of an architecture with a given SCA has to deal with the evaluation of data-dependency of the target physical emission. This basic knowledge on PAAs allows us to introduce the terminology used in this thesis for physical security evaluations and attacks.

In Chapter 3, an in-depth analysis of static power exploitation is given. *Attacks Exploiting Static Power* (AESP) are a sub-class of PAAs that benefit of the data-dependency of the static currents. We demonstrate how AESP can be very powerful in recovering secret key even from dynamic PAA-protected implementations in nanometer technologies. Moreover, the temperature dependency of this side-channel is evaluated, since each static current relate phenomenon is strongly dependent from the working temperature of the device under attack. Making use of this additional dependency, it is possible to simplify the extraction of information through static power consumption. A multivariate analysis of static power consumption using the working-temperature as additional domain is also given, and a brand new profiled attack, *Template Attack Exploiting Static Power* (TAESP) is presented. In addition, a new measurement setup for mounting AESP and TAESP is presented. The proposed measurement setup makes use of only low-cost off-the-shelf components and featuring a control-loop for the working temperature of the device under attack. In this work, a DC pico-ammeter is used in place of the classical Digital Storage Oscilloscope (DSO) to measure static power consumption at steady state.

In Chapter 4, we propose a novel logic style named *Delay-based Dynamic Differential Logic* (DDDL or D³L) as a new logic-level countermeasure against PAAs. The new logic style has been conceived to be implemented using only standard-cells, usually provided with each digital design kit. The D³L makes use of the *Time Enclosed Logic* (TEL) signaling, which has been recently demonstrated to outperform the conventional Return-to-Zero (RTZ) protocol in terms of security if mismatch effects are properly taken into account. The new library is presented with a template for 2-input Boolean operands and also a sequential gate is described. Simulations

on the novel logic style are provided using a 40nm CMOS design kit, provided by STMicroelectronics. Moreover, also implementation details for two FPGAs (Xilinx Spartan-6 and Altera Cyclone-IV) are reported, since it is possible to easily design the D³L library using VHDL. Dynamic and static power attacks and evaluations are given on the FPGA implementation using a 4-bit PRESENT-based crypto-core as case study, making also a comparison with other popular FPGA-compatible dual-rail pre-charge logic styles used to counteract PAAs.

In Chapter 5, an analog-approach in counteracting PAAs is investigated, acting directly on the analog signal targeted by PAAs. The analog-approach is not well explored in literature, but it offers several possibility in counteracting the steal of information through power consumption. We propose two countermeasure schemes based on a feedback-loop architecture and with a pure current-mode approach, named *On-chip Current Equalizer* (OCE) and *improved On-chip Current Equalizer* (iOCE). The purpose of OCE and iOCE is to maintain the current consumption constant neglecting the data-dependent activities that take place in the cryptographic circuit. OCE and iOCE aim to equalize the instantaneous current consumption as well as the energy per cycle.

In Chapter 6, the test and security evaluation of the 65nm SERPAES prototype chip is presented and discussed. The SERPAES, designed at our laboratory, contains five implementations of AES-128 block cipher and two full-custom designed prototype implementations of 4-bit data-path of the SERPENT block cipher. AES implementations are designed with RTL-level countermeasures, aiming to randomize the power consumption of the data-path. Experimental analysis of PAA-resilience on AES-4 core is presented, giving actual and information theoretic security metrics. The protection scheme implemented on AES-4 is based on the adoption of the Secure Double Rate Register (SDRR), aiming to randomize the power consumption of combinational network and registers. CPA and DPA attack results are also presented. Moreover, security analysis and attacks on the full-custom section of the SERPAES chip, containing two implementations of 4-bit data-path based on round-0 of the SERPENT block cipher, is presented. SERPENT-based cores are implemented using the following full-custom logics: Sense Amplifier-Based Logic (SABL) and improved Delay-based Dual-rail Pre-charge Logic (iDDPL). PAA evaluations on both cores are presented, giving a fair comparison of state-of-the-art full-custom PAA-countermeasures. The comparison has been carried out for different cases of capacitive unbalance, in order to measure the performance of both logic styles in tolerating capacitive mismatches.

In Chapter 7, we draw the conclusions to this work and give possible future developments.

Contents

1	Introduction	1
1.1	<i>On the shoulders of giants...</i>	1
1.2	Cryptography in the Digital-Era	3
1.3	Side-Channel Analysis, Physical Emissions and Information Leakage	5
1.4	Power Consumption in CMOS Technologies	7
1.4.1	Dynamic Power Consumption	8
1.4.2	Static Power Consumption	10
1.5	Technological Issues in Real World Hardware Cryptography	11
1.5.1	Ringling	12
1.5.2	Crosstalk	12
1.5.3	Ground Bounce	13
1.5.4	Voltage Drop	13
1.5.5	Electrical Mismatch	13
1.5.6	Process Variations	14
1.6	Countermeasuring PAAs	15
2	Power Analysis Evaluation Methodologies	17
2.1	Introduction	17
2.2	Actual Security Metrics	18
2.2.1	Signal-to-Noise Ratio, SNR	18
2.2.2	Energy-based Security Metrics	19
2.2.3	Measurements To Disclosure, MTD	19
2.3	Attack Methodologies	19
2.3.1	Differential Power Analysis	21
2.3.2	Correlation Power Analysis	21
2.3.3	Extensions of CPA Algorithm	22
2.4	Template Attacks	23
2.4.1	Improving Efficiency of Template Attacks	25
2.5	Enhancement of Effectiveness of PAAs through Pre-Processing	27
2.5.1	Principal Component Analysis, PCA	28
2.5.2	Wavelet-based Denoising	29
2.6	Information Theoretic Security Metrics	31
2.6.1	Mutual Information	32
2.6.2	Perceived Information	32

3	Attack Exploiting Static Power in Deep Sub-Micron Technologies	33
3.1	Introduction	33
3.2	Leakage Current Sources	36
3.2.1	Sub-Threshold Leakage	36
3.2.2	Reverse-biased pn Junction Leakages	38
3.2.3	Gate Leakage	39
3.3	Data-Dependency of Static Current	39
3.4	AESP in Cryptography	43
3.5	Vulnerability of DPA-countermeasured Logic Styles to AESP	46
3.5.1	DPL logic styles	48
3.5.2	Evaluation of vulnerability to AESP on the SERPENT block cipher	50
3.5.3	Evaluation of vulnerability to AESP on the PRESENT block cipher	56
3.6	Temperature Exploitation of Static Current's Information Leakage	59
3.6.1	Temperature dependency on the 4-bit PRESENT crypto-core	61
3.6.2	Temperature dependency on the full implementation of the PRESENT-80 block cipher	63
3.6.3	Multivariate Analysis of Static Currents	64
3.7	Template Attack Exploiting Static Power: TAESP Methodology	68
3.7.1	TAESP Algorithm	69
3.7.2	TAESP Against The 4-bit PRESENT Crypto-core	71
3.7.3	TAESP in a Simulated Experiment	73
3.8	Measurements Setup for AESP Security Evaluations	74
3.8.1	State-of-the-art of Measuring Static Power for SCA	74
3.8.2	Issues in Measuring Static vs. Dynamic Leakage	76
3.8.3	Novel Measurements Setup for AESP Analysis	76
3.8.4	Experimental Measurement: Xilinx Spartan-6 ROM	79
3.8.5	AESP on the 4-bit PRESENT crypto-core on the Xilinx Spartan-6 FPGA	79
3.9	Conclusions	82
4	D³L - A TEL-based Standard-Cell PAA Resilient Logic Style	85
4.1	Introduction	85
4.2	Issues in Implementations of DPL Logic Styles	86
4.2.1	Capacitive Unbalance	87
4.2.2	Capacitive Imbalance Minimization on ASICs	88
4.2.3	Capacitive Imbalance Minimization on FPGAs	90
4.3	Time Enclosed Logic Principle and Guidelines	92
4.3.1	Assumption on the Adversary Model in TEL signaling	92
4.3.2	The TEL Protocol	93
4.3.3	TEL-based Cell Templates	95
4.3.4	Power Analysis Considerations on TEL-compatible Logic	97
4.3.5	Timing Constraints of TEL-based Circuits	98
4.4	Full-custom DDPL/iDDPL Logic Style	100
4.4.1	Limitations of the DDPL Style	102
4.4.2	Improved DDPL (iDDPL)	103

4.5	D ³ L - Standard Design Flow for Secure Applications	106
4.5.1	Standard Design Flow vs Full/Semi Custom Design Flow . . .	107
4.5.2	D ³ L Logic Cell Template	108
4.5.3	Early Evaluation Free D ³ L Combinational Gates	112
4.5.4	Conversion from CMOS Domain to Secure TEL Domain . . .	117
4.5.5	Analysis of $\Delta\delta$ in D ³ L Style	120
4.6	Sequential Element in D ³ L Style	123
4.6.1	Sequential Elements in DPLs Styles	123
4.6.2	Design of the Sequential Element in D ³ L Style	125
4.7	Design and Characterization of the D ³ L Style	130
4.7.1	Energy Balancing in D ³ L Combinational Gates	130
4.7.2	Security Evaluation in the Frequency Domain	133
4.7.3	Fluctuations of t_{eval} in Combinational Gates	135
4.7.4	Analysis of $\Delta\delta$ with Process Variations	137
4.7.5	Sequential Element Characterization	139
4.7.6	Timing Constraints	143
4.8	D ³ L Implementation of the 4-bit PRESENT Crypto-Core	147
4.8.1	Proof of PAA Resistance using Correlation Power Analysis . .	148
4.8.2	High grade DSO, Case 1	149
4.8.3	Mid Grade DSO, Case 2	150
4.8.4	Low Grade DSO, Case 3	151
4.8.5	D ³ L with $t_{eval}=500ps$	153
4.8.6	Final Remarks on PAA-Resilience of D ³ L	154
4.9	FPGA Implementations using the D ³ L	156
4.9.1	Combinational Logic	158
4.9.2	Sequential Element	162
4.9.3	Generation of the Delayed Clock	167
4.9.4	4-bit PRESENT Crypto-Core	168
4.9.5	Dynamic Power Analysis on FPGA Implementation of D ³ L PRESENT Crypto-Core	176
4.9.6	AESP Attack on FPGA Implementation of D ³ L PRESENT Crypto-Core	184
4.10	Final Remarks on the Novel D ³ L Style	189
5	Countermeasures based on Analog Current Equalizers	193
5.1	Introduction	193
5.2	State-of-the-Art of Analog Approach Countermeasures	194
5.3	OCE: On-chip current equalizer	196
5.3.1	Performance on Single Logic Gates	199
5.3.2	Case Study: Application of OCE on the 4-bit PRESENT Crypto-core	201
5.4	Improved OCE: an area and power efficient solution	205
5.4.1	Case Study:4-bit PRESENT Crypto-Core	207
5.4.2	Full Implementation of the iOCE-Protected PRESENT-80 . .	209

6	Test and Security Evaluation of the SERPAES Chip	217
6.1	Introduction	217
6.1.1	Securing RTL Implementation of Cryptographic Devices, State-of-the-Art	220
6.2	RTL-Level Countermeasures for AES-128	220
6.2.1	Unprotected Reference Implementation (AES-0)	221
6.2.2	Random Pre-charged Interleaved Pipeline Countermeasure (AES-1)	222
6.2.3	XOR-Series Countermeasure (AES-2)	222
6.2.4	XOR-Parallel Countermeasure (AES-3)	223
6.2.5	Secure Double Rate Register (AES-4)	224
6.3	Security Level Evaluation of AES-4, a Case Study	227
6.3.1	FPGA Prototyping of AES-0 and AES-4	227
6.3.2	Leakage Assessment on the SERPAES chip of AES-0 and AES-4	228
6.4	Full-Custom 4-bit SERPENT Crypto-cores	234
6.4.1	Data-path of 4-bit SERPENT Crypto-Cores	236
6.4.2	Capacitive Mismatch Analysis	237
6.5	Power Analysis Attacks on SERPENT-based Crypto-cores	238
6.5.1	Evaluation of Security Metrics	239
6.5.2	CPA Attacks on SERPENT-based Crypto-Cores	242
6.5.3	DPA Attacks on SERPENT-based Crypto-Cores	245
6.6	Conclusions	246
7	Conclusions and Future Developments	249
7.1	Summary of the Research Contributions	249
7.1.1	Additional Research Activities	254
7.2	Future Works	255
A	Introduction to Modern Lightweight Cryptography	257
A.1	Advanced Encryption Standard: AES-128 Block Cipher	258
A.2	PRESENT	261
A.2.1	Design of the PRESENT S-BOX	262
A.3	SERPENT	262

List of Figures

1.1	Generic SCA scenario.	7
1.2	Short circuit current in a CMOS inverter.	9
2.1	Signal-strength function evaluation using DoM, SoST, VAR and CPA on a FPGA implementation of a AES-128 block cipher.	27
2.2	FFT of a power traces of a FPGA implementation of AES-128 pre (top) and post (bottom) the wavelet decomposition, stopped at level 2 using 'dB4' as mother wavelet.	30
3.1	Static versus dynamic power consumption of the same design on four different Xilinx Virtex FPGAs [75].	35
3.2	Power consumption trend within three decades. The inflection of 90nm technology has remarked a critical point for designers, highlighting the importance of static consumption in the power budget [69]. . . .	35
3.3	Power consumption in integrated circuits [81].	36
3.4	NMOS structure with the three main static current sources.	37
3.5	Temperature dependency of the sub-threshold current in 4x4bit PRESENT crypto-core.	38
3.6	Power analysis of a CMOS inverter.	40
3.7	Attack Exploiting Static Power procedure.	46
3.8	Example of dual-rail gate using single-rail gates.	47
3.9	Dual-rail pre-charge encoding (RTZ protocol) of the logic value '1' and '0', assuming '0' as pre-charge value. The clock signal $CK/\overline{PRE}$ is used as pre-charge signal. The pre-charge phase occurs when the signal $CK/\overline{PRE} = 0$, while the evaluation phase for $CK/\overline{PRE} = 1$	48
3.10	WDDL building blocks. In (a), the AND/NAND gate in WDDL logic is shown. In (b), the CMOS-to-WDDL converter is shown, using a pre-charge value of '0'. In (c) the WDDL 1-bit flip-flop is shown. The low-level of the clock signal is used to generate the pre-charge wave, avoiding the use of an explicit signal.	49
3.11	MDPL building blocks. In (a), the AND/NAND gate in MDPL logic is shown. In (b) the MDPL 1-bit flip-flop is shown.	50
3.12	Implementation of the buffer/inverter with SABL logic style.	51
3.13	4-bit data-path of the SERPENT block cipher used as cased study to analyze and compare the vulnerability of different DPL logic styles against AESP.	52

3.14	Time diagram of the clock signal to collect only static current samples.	52
3.15	AESP using correlation coefficient against the 4-bit SERPENT crypto-core with LVT (blue), SVT(red) and HVT(green) devices. The key $(7)_2$ has been set on this scenario.	54
3.16	AESP using correlation coefficient against 40nm CMOS and DPLs implementation of the 4-bit SERPENT crypto-core.	54
3.17	Mutual information plots versus the standard deviation of the noise with various DPL logic styles. The CMOS implementation has been used as reference.	55
3.18	4-bit data-path of the PRESENT block cipher.	56
3.19	Data-path of the full implementation of the PRESENT-80 block cipher with iterative-loop structure.	57
3.20	Mutual information versus noise standard deviation of WDDL (bold line) and CMOS (dotted line) implementation of the 4-bit PRESENT crypto-core, using $(10)_2$ as secret key.	58
3.21	Mutual information versus the standard deviation of the noise for WDDL (bold line) and CMOS (dotted line) implementation of the PRESENT-80 cryptographic processor, using 100°C as working temperature.	60
3.22	Correlation coefficient as function of the number of measurements CMOS 3.22(a) and WDDL 3.22(b) implementation of PRESENT-80 in a simulated experiment, using a SNR of -60dB. The correlation coefficient of the correct key is plotted in black, while correlation coefficients of wrong keys are plotted in grey.	61
3.23	Average value of the static current samples collected on the 4-bit PRESENT crypto-core among all Monte Carlo simulations' circuits. Results are shown regarding the input vector and the working temperature.	62
3.24	Mutual information curves as function of working temperature and the noise standard deviation for the 4-bit PRESENT based crypto-core.	63
3.25	Average value of the static current samples collected on full implementation of the PRESENT-80. Results are shown regarding the input vector and the working temperature.	63
3.26	Mutual information curves as function of the working temperature and noise standard deviation on full implementation of PRESENT-80.	64
3.27	Correlation coefficient versus the number of measurements in the AESP procedure on the full implementation of the PRESENT-80. Plots (a) to (e) are referred to working temperature from 0°C to 100°C . Black bold lines represent the correlation coefficient of the correct key; grey lines represent the correlation coefficient of wrong keys.	65

3.28	Figure (a) shows the distribution of the maximum value of the perceived information using $[60^{\circ}\text{C}; 100^{\circ}\text{C}]$ as temperature points over all 100 Monte Carlo's chips. In (b), box-plot of the median value of the maximum of perceived information regarding the best temperature points combinations, from 1-point to 6-points. Black dots represents the median value for each case over the 100 chips. The bottom and the top of each box represent the first and the third quartiles, respectively.	67
3.29	Perceived information versus the noise standard deviation for chip 46. Mutual information curve is used as reference.	68
3.30	Template Attacks Exploiting Static Power algorithm and procedure flow graph.	71
3.31	Percentage of chips with $\text{SVI} \geq 0.8$ (see Equation 3.30) among all successfully attacked chips.	74
3.32	Probability in Equation 3.27 versus the number of measurements for chip 46, using chip 0 for the profiling phase. Black lines refer to the probability value of the correct key. Grey lines represent the probability of wrong keys. Plot (a), (b), (c), and (d) are referred to TAESP with increasing number of temperature points, from 1-point to 4-points, respectively. The combinations used are reported in Table 3.16, since we have found them as the-best case also for chip 46.	75
3.33	Schematic of the feedback loop controller of the Peltier cell.	78
3.34	Cross-view of the stack in the mechanical locking system used to match the heater and the device under attack.	78
3.35	Block scheme of the novel measurement setup (a) and timing digram of signals (not in scale) during a measurement operation (b).	80
3.36	Static current absorption of a Xilinx Spartan 6 with a 4kbit ROM, filled with '0' (blue) and '1' (red), measured at $T = 65^{\circ}\text{C}$	81
3.37	Correlation coefficient as function of the number of measurements used to perform the AESP attack on the 4-bit PRESENT crypto-core, implemented on the Xilinx Spartan-6 FPGA. The black line represents the correct key's correlation coefficient, while gray lines are referred to correlation coefficients of wrong keys.	81
4.1	Model of the output capacitance of a CMOS gate.	88
4.2	DPL styles capacitive parasitics due to C_i , C_o and C_w	89
4.3	In (a) each DPL cell is routed as single-ended cell using fat wire connections. In (b) the fat wire connections are splitted and separated in <i>true</i> connection (red) and <i>false</i> connection (blue).	90
4.4	The "back-end duplication" method explained in [66].	91
4.5	TEL protocol signaling for the logical '1' (a), logical '0' (b) and NULL logic value (c) (not in scale).	94
4.6	Template of a TEL-compatible gate using two independent circuit for the complementary function F_1 and F_2	96
4.7	RTZ (a) and TEL-compatible (b) inverter.	98
4.8	DDPL p-type AND/NAND gate (a) and DDPL p-type XOR/XNOR gate (b).	102
4.9	TDPL inverter gate (a) and timing diagram (b).	105

4.10	In (a), iDDPL inverter/buffer schematic. In (b), iDDPL inverter/buffer timing diagram. It has to be noticed that $t_{\text{eval,IN}}$ and $t_{\text{eval,OUT}}$ are generally different.	107
4.11	iDDPL AND/NAND gate with enhanced pull-down network for EE-free design.	108
4.12	D ³ L 2-input combinational gate template.	109
4.13	D ³ L AND/NAND gate.	110
4.14	D ³ L OR/NOR gate.	111
4.15	D ³ L XOR/XNOR gate.	112
4.16	CMOS NAND2 (a) and NAND3 (b) gates.	113
4.17	D ³ L AND/NAND (a) and OR/NOR gate with enhanced output layer to avoid unbalancing in fan-out values between the compounds. . . .	114
4.18	Equivalent model of the first evaluation layer of the D ³ L AND/NAND gate for the four possible combinations of the CMOS input data: $(A,B) = (0,0)$ (a), $(A,B) = (0,1)$ (b), $(A,B) = (1,0)$ (c), $(A,B) = (1,1)$ (d). The ON-resistance is depicted in black and the OFF-resistance is depicted in gray.	115
4.19	Equivalent model of the second evaluation layer of the D ³ L AND/NAND gate for the four possible combinations of the CMOS input data: $(A,B) = (0,0)$ (a), $(A,B) = (0,1)$ (b), $(A,B) = (1,0)$ (c), $(A,B) = (1,1)$ (d). The ON-resistance is depicted in black and the OFF-resistance is depicted in gray.	116
4.20	Circuit for the conversion from the single-ended CMOS domain to the dual-rail TEL domain in D ³ L style.	118
4.21	Timing diagram of signals in CMOS-to-TEL converter of Figure 4.20. . . .	118
4.22	Delay element implemented using the starved inverter in [27] for iDDPL implementations. The V_{CTRL} voltage can be used to vary the delay provided by the starved inverter.	119
4.23	Time diagram of the AND/NAND gate in D ³ L with $t_2 < 2t_{\text{NAND}}$	121
4.24	Time diagram of the AND/NAND gate in D ³ L with $t_2 > 2t_{\text{NAND}}$	122
4.25	In (a), cell schematic of a WDDL register without the pre-charge wave generator. The CK signal has frequency equal to double of the data-rate. In (b), a block scheme of the SABL fully dynamic flip-flop [93].	124
4.26	Block scheme of the iDDPL flip-flop proposed in [27].	125
4.27	In (a), a self-timed pulse clock latch used as TEL-to-RTZ converter in iDDPL flip-flop architecture. In (b), the n-type RTZ-to-TEL latch/converter.	126
4.28	Block scheme of the sequential element building block in D ³ L style. . . .	127
4.29	Timing diagram of signals in D ³ L sequential element.	127
4.30	NAND SR latch used as TEL-to-RTZ converter in D ³ L sequential element.	128
4.31	Timing diagram of the D ³ L TEL-to-RTZ collected on a Cadence Virtuoso transient simulation on 40nm STMicroelectronics CMOS standard-cells implementation: D (green), $\overline{D}$ (pink), D_{RTZ} (blue) and $\overline{D_{\text{RTZ}}}$ (violet).	128
4.32	OR-gated NOR SR latch used for both master and slave device. . . .	129

4.33	Timing diagram of the signals in the OR-gated NOR SR latch. . . .	129
4.34	Half circuit of the OR-gating scheme.	129
4.35	Scheme of the RTZ-to-TEL converter used as output interface in the D ³ L sequential element to restore the TEL encoding.	130
4.36	Timing diagram of the signals in the RTZ-to-TEL converter at the output of the D ³ L sequential element. It has to be noted that the output evaluation phase duration of the sequential element is the nominal t_{eval} , according to TEL-compatible flip-flop's requirements. .	131
4.37	ΔFFT vectors for D ³ L XOR/XNOR gate used as inverter, with $t_{eval} = 1ns$	135
4.38	ΔFFT vectors for WDDL XOR/XNOR gate used as inverter. . . .	136
4.39	Testbench used to evaluate ΔFFT and FED plots.	136
4.40	FED plots of the implementation of the PRESENT-80 S-BOX in D ³ L (blue), D ³ L with $C^{opt} = 32pF$ (green) and WDDL (red) style for $MF = 3$	136
4.41	Testbenches used for the evaluation of the 4-bit register. Figure (a) shows the testbench used for WDDL, MDPL and D ³ L registers, and figure (b) shows the testbench used for the CMOS register, which is falling-edge triggered.	137
4.42	Distributions of the output delay $t_{eval,CL}$ of D ³ L combinational gates for 500 iterations of Monte Carlo simulations: AND/NAND (a), OR/NOR (b) and XOR/XNOR (c).	138
4.43	Current traces of 4-bit registers implemented in CMOS (a), D ³ L (b), WDDL (c), MDPL with change in the masking bit (d) and without change in the masking bit (e), using $MF=3$ (strong mismatch). . . .	141
4.44	Standard deviation of the current absorption in a clock cycle as function of the time for the 4-bit registers implemented in CMOS (a), D ³ L (b), WDDL (c), MDPL with and without change in masking bit ((d) and (e) respectively).	142
4.45	Plot of the t_{CQ} as function of data-to-clock t_{CD}	145
4.46	Plot of the derivative of the $\delta t_{CQ}/\delta t_{DC}$ as function of data-to-clock t_{CD}	146
4.47	RTL schematic of the implementation of the 4-bit PRESENT crypto-core with D ³ L style.	147
4.48	Output load for each gate (both combinational and sequential) in the analysis of the 4-bit PRESENT crypto-core, to simulate the presence of mismatch.	147
4.49	Noise-free power traces collected on D ³ L implementation of 4-bit PRESENT crypto-core with $t_{eval} = 1ns$ and $MF = 3$. The sampling rate of the simulator is 50GS/s.	149
4.50	Noise-free power traces collected on WDDL implementation of 4-bit PRESENT crypto-core with $MF = 3$. The sampling rate of the simulator is 50GS/s.	149

4.51	Plots of simulated CPA attack on the D ³ L implementation with $t_{eval} = 1ns$, using a high grade DSO (10GS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	150
4.52	Plots of simulated CPA attack on the WDDL implementation, using a high grade DSO (10GS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	151
4.53	Plots of simulated CPA attack on the D ³ L implementation with $t_{eval} = 1ns$, using a mid grade DSO (1GS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	152
4.54	Plots of simulated CPA attack on the WDDL implementation, using a mid grade DSO (1GS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	152
4.55	Plots of simulated CPA attack on the D ³ L implementation with $t_{eval} = 1ns$, using a low grade DSO (500MS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	153
4.56	Plots of simulated CPA attack on the WDDL implementation, using a low grade DSO (500MS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	153
4.57	Plots of simulated CPA attack on the D ³ L implementation, with $t_{eval} = 500ps$, using a low grade DSO (500MS/s) (a), mid grade DSO (1GS/s) (b) and high grade DSO (10GS/s) (c). Top figures show the correlation coefficient ρ vs. current traces time samples. Bottom figures show the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	155
4.58	FPGA boards. In (a), the ComBlock COM 1500-A board [44] with the Xilinx Spartan-6 LX45 FPGA chip. In (b), the EP4C10 development board with the Altera Cyclone-IV EP4CE10E22C8.	157

4.59	Post-synthesis and post-optimization technology view of the D ³ L AND/NAND gate with Altera Quartus II 13.0 (a) and Xilinx ISE 14.1 (b).	161
4.60	Post-synthesis and post-optimization technology view of the D ³ L XOR/XNOR gate with Altera Quartus II 13.0 (a) and Xilinx ISE 14.1 (b).	163
4.61	Logic element (in Normal Mode) architecture in Altera Cyclone-IV devices [8].	164
4.62	SLICEX in Xilinx Spartan-6 FPGAs [153].	165
4.63	OR-gated NOR SR-latch post-synthesis and post-optimization in Altera Quartus II.	167
4.64	RTL view of the implementation of the S-BOX after the synthesis and the map steps; (a) for the Altera Cyclone-IV and (b) for the Xilinx Spartan-6.	169
4.65	ASM diagram of the finite state machine that acts as controller for the 4-bit PRESENT crypto-core.	170
4.66	Block scheme of the testbed used for the implementation of the 4-bit PRESENT crypto-core on FPGA.	171
4.67	FTDI FT-232RL daughter board for USB-to-UART connection mounted on the Altera Cyclone-IV's evaluation board.	172
4.68	Block scheme of the dynamic power measurement setup.	174
4.69	Dynamic power measurement setup.	174
4.70	<i>Chip Planner</i> view of PRESENT crypto-cores' implementations on the Altera Cyclone-IV FPGA: CMOS (a), MDPL (b), WDDL (c) and D ³ L (d). Red boxes represent the <i>logic elements</i> used by the cryptographic circuit, while blue ones are referred to non-cryptographic circuitry.	175
4.71	NED and NSD values of dynamic power consumption of the 4-bit PRESENT crypto-core implementations.	177
4.72	Power traces collected during the encryption of the 4-bit PRESENT crypto-core in the Altera Cyclone-IV FPGA: CMOS (a), WDDL(b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D ³ L (e). Plot (f) shows the clock signal <i>CK</i>	178
4.73	Plots of correlation coefficients for CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D ³ L (e) using the output word of the S-BOX and the HW as power model. Attacks have been performed using 2 ¹⁷ power traces. Black lines correspond to the correct key's correlation coefficients. Grey lines are referred to wrong keys' correlation coefficients.	180
4.74	Plots of correlation coefficients for CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D ³ L (e) using the output word of the 4-bit XOR and the HW as power model. Attacks have been performed using 2 ¹⁷ power traces. Black lines correspond to the correct key's correlation coefficients. Grey lines are referred to wrong keys' correlation coefficients.	181
4.75	MTD diagrams on CMOS implementation: (a) using S-BOX and (b) using XOR.	182

4.76	MTD diagrams on WDDL implementation: (a) using S-BOX and (b) using XOR.	182
4.77	MTD diagrams on MDPL implementation with PRNG enabled: (a) using S-BOX and (b) using XOR.	183
4.78	MTD diagrams on MDPL implementation with PRNG disabled: (a) using S-BOX and (b) using XOR.	183
4.79	MTD diagrams on D ³ L implementation: (a) S-BOX and (b) using XOR.	184
4.80	SNR curves as function of time: CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D ³ L (e). . .	185
4.81	Mutual information curves as function of time: CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D ³ L (e).	186
4.82	Correlation coefficient ρ_{MAX} as function of the number of measurements used to perform AESP attacks on 4-bit PRESENT crypto-cores, using the 3 rd clock cycle with $CK = 0$: CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D ³ L (e). Black lines represent the correct key's correlation coefficient, while gray lines are referred to correlation coefficients of wrong keys. . . .	190
4.83	Correlation coefficient ρ_{MAX} as function of the number of measurements used to perform AESP attacks on 4-bit PRESENT crypto-cores, using the 3 rd clock cycle with $CK = 1$: CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D ³ L (e). Black lines represent the correct key's correlation coefficient, while gray lines are referred to correlation coefficients of wrong keys. . . .	191
5.1	Realistic PAAs scenarios: (a) the SCA sensor is placed before the off-chip filter, (b) the SCA sensor is placed after off-chip filter. . . .	195
5.2	Block scheme of the OCE.	197
5.3	Simplified and linearized model of the current equalizer.	198
5.4	Circuit implementation of the proposed current equalizer.	198
5.5	Circuit implementation of the V_{sync} signal. The delay element is implemented with a starved inverter.	199
5.6	Timing diagram of the V_{sync} signal.	200
5.7	Protected implementation of the 4-bit PRESENT crypto-core. Each sub-block is protected locally by an on-chip current equalizer. . . .	201
5.8	Power traces of unprotected (a) and protected (b) implementation of the 4-bit PRESENT crypto-core using the on-chip current equalizer with different plaintexts.	202
5.9	Plots of the CPA attack on the unprotected 4-bit PRESENT crypto-core. In (a), the correlation coefficient ρ vs. current traces time samples. In (b), the MTD diagram is shown. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	203

5.10	Plots of the CPA attack on the protected 4-bit PRESENT crypto-core, using the on-chip current equalizers as analog approach countermeasure. In (a) the correlation coefficient ρ vs. current traces time samples. In (b), the MTD diagram is shown. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	204
5.11	Simplified and linearized block scheme of the on-chip current-mode suppressor. I_{LOGIC} is considered as a disturbance to be rejected, in order to counteract a CPA attack.	205
5.12	CMOS implementation of the improved on-chip current-mode suppressor. The protected crypto-core is fed through the suppressor circuit.	206
5.13	Implementation of the pulse generator, which generates the signal V_{PULSE}	207
5.14	CMOS implementation of the improved on-chip current mode suppressor with each sub-system in Figure 5.11 highlighted.	208
5.15	Power traces on the protected implementation of the 4-bit PRESENT crypto-core. The improved on-chip current-mode feedback equalizer is able to strongly reduce the power variability due to data-dependency of the CMOS crypto-core.	209
5.16	CPA attacks on unprotected PRESENT crypto-core. Top figure shows the correlation coefficient ρ vs. current traces time samples, using 1000 power traces. Bottoms figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	209
5.17	CPA attacks on the protected 4-bit PRESENT crypto-core implementation. The correlation coefficient ρ vs. current traces time samples, using 100k power traces, is shown in (a). The MTD diagram is shown in (b). The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	210
5.18	Plots of the CPA attack on the unprotected PRESENT-80. Figure in (a) shows the correlation coefficient ρ vs. current traces time samples. Figure in (b) shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	212
5.19	Plots of the CPA attack on the protected PRESENT-80 (nominal case), using the on-chip current-mode suppressor of Figure 5.12 as analog approach countermeasure. Figure (a) shows the correlation coefficient ρ vs. current traces time samples. Figure (b) shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	213

5.20	Plots of the CPA attack on the protected PRESENT-80 (SS corner), using the on-chip current-mode suppressor of Figure 5.12 as analog approach countermeasure. Figure (a) shows the correlation coefficient ρ vs. current traces time samples. Figure (b) shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	214
5.21	Plots of the CPA attack on the protected PRESENT-80 (FF corner), using the on-chip current-mode suppressor of Figure 5.12 as analog approach countermeasure. Figure (a) shows the correlation coefficient ρ vs. current traces time samples. Figure (b) shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	215
6.1	Macro-blocks in SERPAES chip.	218
6.2	Microphotograph of the SERPAES chip.	219
6.3	Printed circuit board with the SERPAES chip, power supply network and level shifters.	219
6.4	Simplified schematic of the SERPAES' standard-cell section with AES-128 implementations.	221
6.5	Data-path of the basic implementation of the AES-128 block cipher (AES-0).	221
6.6	Random Pre-charged Interleaved pipeline countermeasure in AES-1.	223
6.7	Commutator implementation.	223
6.8	The XOR-series countermeasure in AES-2.	224
6.9	The XOR-parallel countermeasure in AES-3.	224
6.10	Block scheme of the <i>Secure Double Rate Register</i> in AES-4.	226
6.11	Block scheme of the architecture of AES-4 with SDRR units instead regular registers.	226
6.12	Plots of the CPA attack on AES-0 (FPGA implementation). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	228
6.13	Plots of the CPA attack on AES-4 (FPGA implementation). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	228
6.14	Block scheme of the measurement setup for SERPAES chip.	229
6.15	Plots of the CPA attack on AES-0 (SERPAES). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	230

6.16	Plots of the CPA attack on AES-4 (SERPAES). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	230
6.17	Plots of the DPA attack on AES-4 (SERPAES). Top figure shows the difference of mean (DoM) coefficient vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.	232
6.18	SNR curves for AES-0 (top) and AES-4 (bottom) at the first-round.	232
6.19	Mutual information curves for AES-0 (top) and AES-4 (bottom) at the first round.	233
6.20	Welch's T-test with power samples from AES-0 (top) and AES-1 (bottom) at the first round.	234
6.21	Architecture of the full-custom section of the SERPAES chip, containing two implementations of a 4-bit SERPENT-based crypto-core.	236
6.22	Layout of the SERPENT macro. The section on the left is the iDDPL implementation, while the one on the right is the SABL implementation.	236
6.23	Block scheme of the 4-bit SERPENT-based crypto-cores in the SERPAES chip. The signal <i>CKD</i> is used only on the iDDPL core.	237
6.24	Programmable output load in SERPAES chip.	238
6.25	Current traces of the SABL (a) and iDDPL (b) 4-bit SERPENT-based crypto-cores collected on the respective main voltage supply pin, running at 1MHz, with 1.2V of core voltage. Yellow traces represent the trigger signal, while pink traces are current traces, measured with the Tektronix-CT1 inductive probe.	240
6.26	Time diagram of the encryption in SABL/iDDPL cores: clock signal (top), SABL current absorption (middle), iDDPL current absorption (bottom).	241
6.27	Peak values of SNR (a) and mutual information (b) regarding <i>VBAL</i> configurations.	242
6.28	Plots of correlation coefficients for SABL (left column) and iDDPL (right column) implementations with $C_{add} = 0fF$ (a)-(b), $C_{add} = 3.2fF$ (c)-(d), $C_{add} = 6.4fF$ (e)-(f), $C_{add} = 9.6fF$ (g)-(h). Black lines correspond to the correct key's correlation coefficients. Grey lines are referred to wrong keys' correlation coefficients.	243
6.29	MTD diagrams for SABL (left column) and iDDPL (right column) implementations with $C_{add} = 0fF$ (a)-(b), $C_{add} = 3.2fF$ (c)-(d), $C_{add} = 6.4fF$ (e)-(f), $C_{add} = 9.6fF$ (g)-(h). Black lines correspond to the correct key's correlation coefficients. Grey lines are referred to wrong keys' correlation coefficients.	244
6.30	Plots of difference of means for SABL (left column) and iDDPL (right column) implementations with $C_{add} = 0fF$ (a)-(b), $C_{add} = 3.2fF$ (c)-(d), $C_{add} = 6.4fF$ (e)-(f), $C_{add} = 9.6fF$ (g)-(h). Black lines correspond to the correct key's DoM coefficient. Grey lines are referred to wrong keys' DoM coefficient.	247

A.1	Different elaboration steps of the encoding procedure of AES-128. . .	260
A.2	Basic operations on state matrix in AES-128: <i>SubBytes</i> (a), <i>ShiftRows</i> (b), <i>MixColumns</i> (c) and <i>AddRoundKey</i> (d).	260
A.3	Data-path of the PRESENT-80 in [25].	262
A.4	PRESENT S-BOX.	263

List of Tables

1.1	A survey of most important techniques for protecting cryptographic circuit against PAAs.	15
2.1	Number of templates needed to attack a 8-bit sub-key of a hardware implementation of AES-128 with various partitioning schemes. . . .	25
3.1	Power analysis of a CMOS inverter for each input/output transition.	40
3.2	Variability of the current of a 40nm inverter gate.	41
3.3	Variability of the current of a 40nm NAND gate.	41
3.4	Variability of the current of a 40nm NOR gate.	41
3.5	Variability of the current of a 40nm XOR gate.	42
3.6	Variability of the current of a 40nm D flip-flop.	42
3.7	Comparison of the CV of a NAND gate using 90nm, 65nm, 40nm and 28nm (with SVTLP option).	42
3.8	Comparing of noise performance regarding 3bit of mutual information values for SABL, MDPL, WDDL and CMOS. The CMOS implementation is used as reference.	55
3.9	Area and static power consumption details of CMOS and WDDL implementation of the PRESENT-80 cryptographic processor. . . .	57
3.10	Correlation coefficient on CMOS and WDDL implementation of the 4-bit PRESENT crypto-core at 100°C.	58
3.11	AESP attack against CMOS and WDDL implementation of the PRESENT-80 engine on noise-free static current samples. The working temperature has been set to 100°C.	60
3.12	Average values of the static currents and standard deviation for the Monte Carlo simulations' circuits of the 4-bit PRESENT crypto-core.	62
3.13	Results of the MTD analysis using the AESP procedure on the full implementation of the PRESENT-80 in the range 0 – 100°C. . . .	64
3.14	Median values over the maximum of perceived information over 100 sample circuits in the presence of intra-die variations. 1-points case is used as reference.	67
3.15	Maximum values of perceived information for chip 46.	67
3.16	Results of the TAESP attack on the 100 samples generated by Monte Carlo simulations, with the best-case temperature points combinations.	72

3.17	Results of the TAESP procedure on the 100 circuit samples generated by Monte Carlo simulations with all possible temperature points combination, regarding the number of successfully attacked chips with correct key ranked as first.	73
4.1	RTZ voltage values for each phase of the clock signal.	92
4.2	TEL voltage values for each phase of the clock signal.	94
4.3	Dynamic power consumption for a TEL-compatible and for a DPL (using RTZ encoding) inverter, assuming unbalanced load.	98
4.4	Road map for timing performances of TEL-compatible circuits for different technologies.	100
4.5	D ³ L AND/NAND complete truth table.	110
4.6	D ³ L OR/NOR truth table.	111
4.7	D ³ L XOR/XNOR truth table.	112
4.8	Time constant for charging/discharging event on the first evaluation layer of the D ³ L AND/NAND gate.	113
4.9	Sum of the time constants of the D ³ L AND/NAND gate for RTZ signaling.	116
4.10	Sum of the time constants of the D ³ L AND/NAND gate for TEL signaling.	117
4.11	Delay time of basic gates in standard-cells logic style. Basic delays t_{NAND} , t_{NOT} , t_{NOR} and t_{XOR} , are referred to respective single-ended CMOS gates' delay.	117
4.12	NED value of combinational gates in D ³ L.	132
4.13	NSD value of combinational gates in D ³ L.	133
4.14	NED value of combinational gates in WDDL.	133
4.15	NSD value of combinational gates in WDDL.	133
4.16	Area and power consumption comparison for the PRESENT-80 S-BOX implementation.	137
4.17	$t_{eval,CL}$ of combinational gate in D ³ L style.	137
4.18	Average and standard deviation of the $\Delta\delta$ for D ³ L combinational gates under process variations (500 iterations of Monte Carlo simulations).	139
4.19	Maximum values of standard deviation of the noise-free current samples for the 4-bit registers in different logic styles with MF=3. CMOS implementation is used as reference.	140
4.20	Comparison of the NED on the 4-bit registers.	143
4.21	Comparison of the NSD on the 4-bit registers.	143
4.22	Comparison of the average power P_{av} of the 4-bit registers.	143
4.23	Summary of the CPA attacks results on the 40nm implementation of 4-bit PRESENT crypto-core with D ³ L and WDDL styles.	154
4.24	Resource usage for the Altera Cyclone-IV FPGA using Altera Quartus II 13.1.	173
4.25	NED and NSD values of dynamic power consumption of the 4-bit PRESENT crypto-core implementations.	176
4.26	Average power consumption of PRESENT-based cryptographic processors (f_{CLK} =2MHz and $V_{DD,core}$ =1.2V) on the Altera Cyclone-IV.	177

4.27	Results of CPA attacks against various implementation of the 4-bit PRESENT crypto-core on Altera Cyclone-IV FPGA using dynamic power consumption.	177
4.28	SNR and mutual information values on the PRESENT-based cryptographic processor within the processing time window (from sample no.2000 to sample no.8000).	184
4.29	SNR, mutual information and σ_{data} of static power measurements collected during the 3 rd clock cycle	187
4.30	Results of AESP attacks on PRESENT-based crypto-cores ($T = 65$, 3 rd cycle).	188
5.1	Comparison of unprotected CMOS and protected CMOS using the OCE, in terms of NED and NSD for basic logic gates.	200
5.2	Comparison between unprotected and protected implementation of the 4-bit PRESENT crypto-core.	204
5.3	Comparison of the unprotected and protected implementation of the 4-bit PRESENT crypto-core, using the improved on-chip current equalizer.	211
5.4	Comparison of the unprotected versus protected implementation of the PRESENT-80 using the improved on-chip suppressor as protection circuit.	211
5.5	Comparison of the iOCE feedback suppressor with other analog approach and gate-level CPA/DPA countermeasure in terms of area and average power overhead. Unprotected CMOS implementation is used as reference.	211
6.1	FPGA implementation of AES-0 and AES-4 cores on a Xilinx Spartan-6 LX45.	227
6.2	Actual and information theoretic security metrics of AES-0 and AES-4 cores on the SERPAES chip.	234
6.3	Comparison of performances of SABL and iDDPL 4-bit SERPENT-based crypto-cores.	235
6.4	CPA attacks results on iDDPL and SABL implementations of 4-bit SERPENT-based data-path.	245
A.1	S-BOX of PRESENT regarding the input value.	261
A.2	Permutation rule in <i>PermLayer</i> of PRESENT.	262
A.3	Boolean equations describing the PRESENT 4×4 S-BOX using only 2-input Boolean operands.	263

List of Acronyms and Abbreviations

ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
AESP	Attacks Exploiting Static Power
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
ATM	Automatic Teller Machine
BG	Blurring Gate
BSIM4	Berkeley Short-channel IGFET Model 4
BTBT	Band-to-Band Tunneling
CMG	Current Mask Generator
CMOS	Complementary Metal-Oxide-Semiconductor
CPA	Correlation Power Analysis
CPFA	Correlation Power Frequency Analysis
CPSA	Correlation Power Spectrum Analysis
CV	Coefficient of Variation
D3L	Delay-based Dynamic Differential Logic
DC	Direct Current
DDPL	Delay-based Dual-rail Pre-charge Logic
DES	Data Encryption Standard
DIBL	Drain Induced Barrier Lowering
DLL	Delay Locked Loop
DoM	Difference of Means
DPA	Differential Power Analysis
DPL	Dual-rail Pre-charge Logic
DSO	Digital Storage Oscilloscope
DSP	Digital Signal Processing
EDA	Electronic Design Automation
EE	Early Evaluation
EMA	Electro-Magnetic Analysis
FF	Fast-Fast
FFT	Fast Fourier Transform
FPGA	Field Programmable Gate Array
FVFCS	Flipped Voltage Follower Current Sensor
HD	Hamming Distance

HVT	High Voltage Threshold
HW	Hamming Weight
IC	Integrated Circuit
iDDPL	Improved Delay-based Dual-rail Pre-charge Logic
iOCE	Improved On-chip Current Equalizer
IoT	Internet of Things
KSA	Kolmogorov-Smirnov Analysis
LFSR	Linear Feedback Shift Register
LPA	Leakage Power Analysis
LUT	Look-Up Table
LVT	Low Voltage Threshold
MDPL	Masked Dual-rail Pre-charge Logic
MF	Mismatch Factor
MI	Mutual Information
MIA	Mutual Information Analysis
MOS	Metal-Oxide-Semiconductor
MSB	Most Significant Bit
NED	Normalized Energy Deviation
NFC	Near-Field Communication
NSD	Normalized Standard Deviation
OCE	On-chip Current Equalizer
PAA	Power Analysis Attack
PCA	Principal Component Analysis
PI	Perceived Information
PLC	Power-Line Cycle
PLL	Phase Locked Loop
PRNG	Pseudo Random Number Generator
RFID	Radio-Frequency Identification
RNG	Random Number Generator
RPI	Random Pipeline Interleave
RPL	Random Pre-charge Logic
RSA	Rivest-Shamir-Adleman
RTL	Register-Transfer Level
RTZ	Return-to-Zero
SABL	Sense Amplifier-Based Logic
SCA	Side-Channel Analysis
SDRR	Secure Double Rate Register
SI	Signal Integrity
SIM	Subscriber Identity Module
SNR	Signal-to-Noise Ratio
SoC	System-on-Chip
SoSD	Sum of Squared Difference
SoST	Sum of Squared T-test
SS	Slow-Slow
STFT	Short-Time Fourier Transform
SVI	Success Value Indicator
SVT	Standard Voltage Threshold

SVTLP	Standard Voltage Threshold Low Power
TA	Template Attack
TAESP	Template Attack Exploiting Static Power
TDPL	Three-phase Dual-rail Pre-charge Logic
TEL	Time Enclosed Logic
TOA	Time of Arrival
TT	Typical-Typical
UART	Universal Asynchronous Receiver-Transmitter
VAR	Variance
VHDL	VLSI Hardware Description Language
VLSI	Very Large Scale Integration
WDDL	Wave Dynamic Differential Logic

Chapter 1

Introduction

1.1 *On the shoulders of giants...*

The need of security in exchanging messages has been one of the most important aspects in communications. Evidences of a rudimentary system to protect the contents of a message have been discovered in engraved inscription around 1900 B.C., in the main chamber of the the tomb of Khnumothep II, who lived in Egypt during the 12th dynasty. Strange and unusual hieroglyphs have been discovered on such inscription. Archeologists suppose that scribes aimed to hide the real content of the inscription by inconsistencies and mistakes in the grammatical syntax. It cannot be considered as first example of secret communication, but, nevertheless, it can be considered as a first attempt at obfuscate the real meaning of a text. This is not a rare case. Jumping ahead in time, another attempt at encrypting text has been discovered in a craftsman's recipe for pottery glaze in Mesopotamia, dated near 1500 B.C.. Also in India (400-200 B.C.), documented evidences of the ancient indian art of secret writing and secret communications (*Mlecchita Vikalpa*) are reported in Chapter 3-Part I of *Kamasutra*.

One of the best documented method of primitive secret communications (or also for authentication), mainly used for military circumstances, is the *scytale transposition cipher* (400 B.C.), used by Spartan military. The method is based on the use of the *lacedemonic scytale*, that is a stick with a leather tape wrapped on to form a non-overlapped spiral. The secret text was written on the tape for columns, letter by letter. Removing the leather tape from the stick, the secret text was transposed enough to become not understandable. The secret text could become readable and understandable only if a second stick, identical in diameter of the first one, was used for wrapping the leather tape.

Also during the Roman Empire, a wonderful example of encryption has been the *Caesar cipher*, which is based on on a simple shift operation of the alphabet. The receiver has to know the shifting rule to recover the original message. The *Caesar*

cipher is a simple example of *substitution cipher*. More complex encryption techniques are based on this approach, using multiple alphabet at a time (*polyalphabet cipher*), to improve differences between plaintext and ciphertext.

The first well-documented *polyalphabet cipher* was formulated by Leon Battista Alberti in 1467, using a mechanical disk to switch between different cipher alphabets. Alberti's system was improved, firstly by Johannes Trithemius (1507), and then by Giovan Battista Bellaso (1553). Bellaso's cipher makes use of non-fixed changes in the cipher alphabet. This non-fixed patterning was handled by a special character denoted as key. This approach appears more similar to modern cryptographic algorithms, making that encryption security relies only on the key. In 1586, the French scientist Blaise Vigenère proposed an improved version of the Bellaso's system, increasing the robustness of the algorithm by adopting a key-autokey approach, which is nowadays used in *stream ciphers*. The so-called Vigenère's code has been considered the best encryption system for almost three centuries.

Since protection of information has a strong relationship with warfare, cryptography and the art of the encryption experienced a huge leap forward during the last two centuries of the past millennium. The English mathematician Charles Babbage proposed an innovative approach to *cryptanalysis*, which is the study of analyzing mathematics weakness of cryptographic algorithms, in order to breach their security even if the key is unknown. During the Crimean War, he broke the Vigenère's code, but his finding remained a military secret and not published until the end of the war. Babbage found that the Vigenère's code was vulnerable to *modular arithmetic* analysis, and, also the Prussian officer Friederich Kasiski ended with similar conclusions. In 1883, Auguste Kerckhoffs published *Le Cryptographie Militaire (Military Cryptography)*, as state-of-the-art in military cryptography, that contains advices for practical cryptography, still used in modern systems.

With the First World War, cryptography and cryptanalysis played an important role, since it was the first big conflict where radio-telecommunications have assisted armies on field. For example, British Admiralty broke German naval codes, allowing the British fleet to intercept German ships in the North Sea. Just after the finish of the conflict, a new way to protect information has been proposed, making use of electromechanical devices as cipher machines. These devices had a strong diffusion mainly during the Second World War, and their utilization has been critical. German army made an intensive use of the *Enigma* machine, which was based on an electromechanical rotor machine. *Enigma* has been one of the most complex semi-automated cipher machine of its era. In 1932, Poland's Cipher Bureau deduced the internal architecture of *Enigma*, making use of limited documentation provided by French intelligence service and cryptanalysis. After the beginning of the WWII, Poland's Cipher Bureau started to collaborate with British cryptologists at Bletchley Park, to speed up researches they were conducting on Enigma. The Bletchley Park's team could rely on the brilliant scientists as Gordon Welchman, Max Newman and Alan Turing, who is considered as the father of modern computing. They succeeded in decrypting messages encrypted with newer versions of *Enigma*, changing the outcome of the war. The possibility to use a decrypting machine, called *Colossus*,

made the tracking of German convoys and troops easier.

After the end of the conflict, this research field has experienced a giant leap forward, mainly thanks to the availability of enormous computational capability of modern computers. During the second half of the past century, the concept of cryptography has changed under several aspects. Claude Shannon, who is considered the father of modern and mathematical cryptography, published "A mathematical theory of cryptography" [134] in 1945 posing two main concepts of cryptography: secrecy and authenticity. Shannon investigated deeply the secrecy aspect, redefining in a more mathematical fashion the concept of "unbreakability" of a secure system. Shannon wrote [134]:

If a secrecy system with a finite key is used, and N letters of cryptogram intercepted, there will be, for the enemy, a certain set of messages with certain probabilities, that this cryptogram could represent. As N increases the field usually narrows down until eventually there is a unique "solution" to the cryptogram—one message with probability essentially unity while all others are practically zero. A quantity $Q(N)$ is defined, called the equivocation, which measures in a statistical way how near the average cryptogram of N letters is to a unique solution; that is, how uncertain the enemy is of the original message after intercepting a cryptogram of N letters. Various properties of the equivocation are deduced—for example the equivocation of the key never increases with increasing N . This quantity Q is a theoretical secrecy index—theoretical in that it allows the enemy unlimited time to analyse the cryptogram.

These sentences state two aspects for a perfectly secure system:

- the length of the key must be at least equal to the length of the message;
- the key must be used only one time.

In 1979, the algorithm initially named *Lucifer*, developed by Horst Feistel at IBM, was elected as the first standard encryption algorithm in United States. The algorithm, renamed *Data Encryption Algorithm* (DES) has encouraged also business community to adopt cryptography to protect transactions. In parallel, a research carried on by W.Diffie, M.Hellman and R. Merkle theoretically solved the problem of key distribution by means of asymmetric encryption scheme, giving the birth to public-key cryptography. A practical solution to asymmetric encryption was proposed firstly by Ronald Rivest, Adi Shamir and Leonard Adleman, introducing the famous *RSA* algorithm.

1.2 Cryptography in the Digital-Era

Modern cryptography is based on the adoption of electronic circuits to provide encryption and decryption of data. The onset of the digital-era and the consequent

decreasing in the cost of integrated circuits have pushed forward the presence of cryptography in our daylife. During the last three decades, the pervasive presence of smart devices, such as smartphones, laptop, tablets, have changed needs and habits. In turns, also the way we think about cryptography has changed. From being a research field devoted to military intelligence services and secure communications for the business sector only, cryptography is now pervasive as well as smart devices. In fact, in nowadays designs, it's critical to maintain sealed personal and/or sensible data.

The adoption of cryptography to protect sensible data is one of the main concern in most recent applications. Several secured devices (e.g smartphones, smart-cards, etc.) are frequently used to exchange private informations, such as ID and bank account credentials. Alongside regular circuitry for data processing, communications traffic, data logging, daylife devices are designed including specific cryptographic functions, to avoid the stealing of information. Cryptographic functionalities are implemented at various level, from software application level to on-chip hardware accelerator. Given the benefit of the newest technology, in addition to the "More Than Moore" approach to the design of electronic devices, the *Internet of Things* (IoT) paradigm had an incredible growth, since its first appearance during the 1998. IoT allows to interconnect several "smart devices" or "nodes", in order to collect real-world data by means of network connectivity. Typically, these intelligent networks are based on the identification and authentication of smart devices, and exchanged data are actually private and sensible (e.g. medical and healthcare applications). It is clear that data stream has to be protected, in order to avoid the possibility to be hijacked or sniffed [55][68].

Since early 80's, one of the most representative object of real-world cryptography is the *smart-card*. Smart-cards are composed by a thin plastic support, that contains a small micro-chip which can be interconnected with the external world with metal contacts or through RF antennas. The micro-chip can handle several functions, usually supporting cryptographic functions (e.g. authentication ID, memory, etc.). Smart-cards were initially diffused as support to private authorization/authentication for bank transactions (e.g. withdrawing of money from ATMs). Their fields of application expanded over the years, and they are now used for a huge number of human activities. SIM (Subscriber Identity Modules) cards in smartphones/tablets are basically smart-cards with smaller aspect ratio, and they contains phone numbers, text messages, etc., of the owner. To guarantee protection, they use on-chip cryptographic co-processors, that can be implemented in software for microcontroller, or as a standalone hardware macro. Identification and access badges represent another substantial section of the smart-cards' market, since they are very cheap (usually, they provide only authentication of their owner). Several services, such as public transit operators, use smart-cards to administer users authorization. Badges based on smart-cards are usually featured of magnetic stripes or integrated antennas (providing the so-called RFID, or Radio-Frequency Identification, tag functionality) that make their utilization easier. The onset of RFID and Near-Field Communication (NFC) protocols has raised new issues in security of these devices, since contactless interfaces may give additional opportunities to reveal secret informations.

1.3 Side-Channel Analysis, Physical Emissions and Information Leakage

The strong diffusion of secured devices implied also a wide diffusion of attack procedures, aiming to break their security. During the 90's, a huge number of researchers were involved in testing the security of smart-cards, due to their wide diffusion, and companies and academic community made a meaningful effort in developing tamper-resistant cryptographic circuits. In 1996, Paul Kocher demonstrated that is possible to recover sensible information from a cryptographic device analyzing the *time execution* of modular exponential and multiplication operations in Diffie-Hellman, RSA and other encryption algorithms on a 120MHz Pentium running MS-DOS [85]. The non-fixed time execution of such kind of operations has been found to reveal information about the private key used by the algorithm, and thus, breaking the security of the system bypassing the classic mathematical approach to cryptanalysis. These results relied on the behavior of the electronic system rather than the mathematical weakness of the algorithm. Kocher's work on *timing attacks* has been the first in investigating potential weakness of secure systems relying on physical behavior of devices implementing cryptographic functions.

After the Kocher's publication of *timing attacks*, research on security of trustworthy platforms has been extended to new frontiers regarding the way cryptographic algorithms are implemented. *Timing attack* procedures do not use directly cryptanalysis techniques, but they are based on physical measurements of the device under attack, while performing the cryptographic operation, stating a new way in breaking secure systems. In fact, beyond the time execution analysis, it has been demonstrated that there are other possible *side-channels* in recovering information from cryptographic implementations without forcing the mathematical properties of the algorithm or, literally, the device itself. So, at the end of 90's, the new frontier of physical security of cryptographic devices and systems are *Side-Channel Attacks* (SCAs). We can define SCAs as a subset of cryptanalysis attacks that do not use mathematical weakness of the algorithm under attack or the classical *brute force* approach, but make use of physical emissions of the device implementing the algorithm. The SCA's approach in recovering information from a physical device, such as an integrated circuits, can use multiple sources of emissions:

- time execution [85];
- power consumption [84], [32];
- electromagnetic radiation [119];
- sound [60];
- optical [38].

When an emission can be related to data (or operations) manipulated inside the secure device, and under the assumption that it can be reasonably measured,

the emission becomes a *side-channel*. Under this assumption, Standaert defines *side-channel* as "*an unintended communication channel that leaks some information from a device through a physical media*" [137]. It may provide useful and exploitable information under several point of views:

- it may reveal the operation that it is performed by the device;
- it may reveal the data manipulated by the device;
- it may reveal which algorithm has been implemented;
- it may reveal electronic parameters and implementation details that are not accessible without reverse engineering the device;
- etc..

We must state also that SCAs take advantage of specific characteristics of the secure device's implementation, making them less general than regular cryptanalysis attacks, but, at the same time, more powerful, since they address a specific implementation. In fact, SCAs are classified as a subset of *implementation attacks*, that can be assumed as a generalization of device-based attacks. In literature, we can find a two-fold characterization of physical attacks [136]:

- *Invasive vs. Non Invasive Attacks*. In the case of *Invasive Attacks*, the secure device is mechanically opened, or unpackaged, in order to gain access to internal components, while *Non Invasive Attacks* do not require any mechanical forcing, and exploit information leakage by physical emissions in normal activity conditions.
- *Active vs. Passive Attacks*. In *Active Attacks*, the attacker/adversary interacts directly with the device, altering its nominal activity conditions (e.g. altering voltage supply and/or working temperature). In *Passive Attacks*, the device is monitored during cryptographic activities, and no alterations on its working condition is performed.

SCAs fall in the category of passive and non-invasive attacks, since they do not require (in general) to alter the working conditions of the cryptographic implementations, as the attacker/adversary monitors the target physical emission without unpacking the device. Moreover, SCAs have assumed a role of primary importance in the cryptographic community in last twenty years, since they can be mounted with relatively low-cost equipment and not massive computational capability are required, if compared to cryptanalytic attacks. In Figure 1.1, a generic SCA scenario is shown. In a SCA, there are two actors: the cryptographic implementation, which performs the cryptographic operation with a secret key and leaks information about them, and the adversary, who wants to attempt at recovering the secret key through the side-channel. The aim of a physically secure design is to reduce as much as possible the physically observable leakage of the implementation (ideally, to zero), neglecting

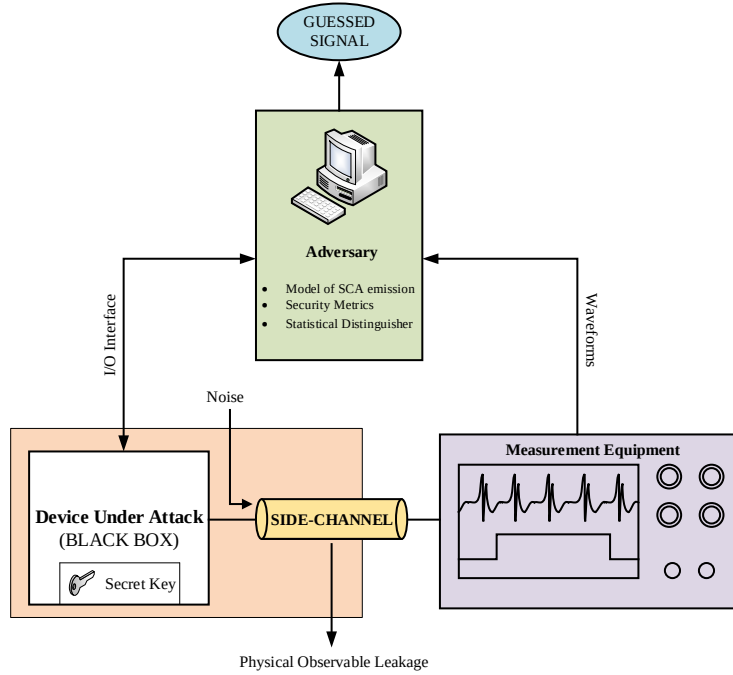


Figure 1.1. Generic SCA scenario.

the attack capability of the adversary. The capability in attack a cryptographic implementation relies on the velocity at recovering the secret information from the device, that, in other words, depends on the quality of his/her observations.

In this work, we will discuss more in deep security issues concerning the possibility to recover information from hardware implementations of cryptographic algorithms using the power consumption as side-channel. As we will discuss in next sections, the power consumption is considered the most representative and discussed side-channel.

1.4 Power Consumption in CMOS Technologies

CMOS, acronym for Complementary Metal-Oxide-Semiconductor, technology, appeared on the market during the second half of the 80's, and it has been the leading logic style of the last thirty years. Almost 99% of modern integrated circuits are fabricated with CMOS technology, or, at least, CMOS-baseline compatible. In this section, we will discuss about the power consumption in CMOS circuits, since it has a strong impact on the security level in CMOS manufactured cryptographic devices. The strong relation between current absorbed $i(t)$ and data processed within a chip, makes the power consumption $p(t)$ a suitable side-channel to mount a recovering procedure extracting sensible information:

$$p(t) = v(t) \cdot i(t) = V_{DD} \cdot i(t) \quad (1.1)$$

We define the *average power consumption* as the integral of the instantaneous power consumption $p(t)$ on a period of elaboration divided by the period:

$$P_{AV} = \frac{1}{T} \int_0^T p(t) dt = \frac{V_{DD}}{T} \int_0^T i(t) dt = V_{DD} \cdot I_{AV} \quad (1.2)$$

It has to be noted that the overall power consumption of a CMOS circuit is given by the sum of two components:

$$P_{TOT} = P_{dyn} + P_{stat} \quad (1.3)$$

where P_{dyn} represents the *dynamic power consumption*, and P_{stat} corresponds to the *static power consumption*. Of course, they both depend directly on the size of the CMOS circuit and on its topology. In the following, a description of contributions in Equation 1.3 is given.

1.4.1 Dynamic Power Consumption

The dynamic power consumption of a CMOS circuit is defined as the fraction of the total power that is due to charge/discharge events (switching) in a logic circuit. As suggested by its name, the dynamic power consumption is related to the dynamic behavior of a CMOS circuit, since it is originated by transitions in signals alongside the circuit. Dynamic component of the overall power consumption is given by the sum of two main components, as described in Equation 1.4 [93]:

$$P_{dyn} = P_{SC} + P_{switch} \quad (1.4)$$

where P_{SC} is the *short-circuit power*, and P_{switch} is the *switching power*. The *short-circuit power* is a component of the dynamic power of a CMOS circuit due to non-ideal effects in CMOS gates. By construction, each CMOS gate is composed by a pMOS pull-up network, that provides a charging path for the output capacitance to V_{DD} , and a nMOS pull-down networks, that allows the output capacitance to discharge towards to ground. Depending on the combination of input values, only one network at a time is fully connected to the respective power rail, and in general, no direct path between V_{DD} and ground exists. Nevertheless, since real signals has finite rise and fall times, during the transition from a logic state to the opposite, both pull-up and pull-down network provide a resistive path between the two power rails for a short time. When it occurs, an impulse of current is drawn from V_{DD} directly to ground, de facto, generating the *short-circuit current* i_{SC} and its relative

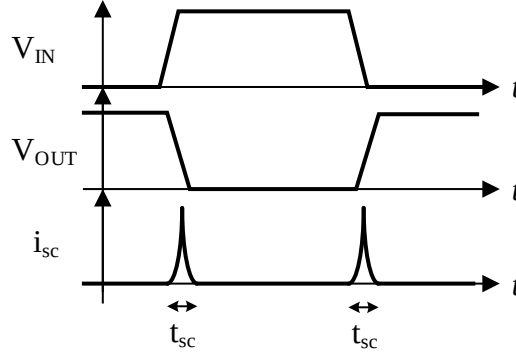


Figure 1.2. Short circuit current in a CMOS inverter.

power consumption. It occurs for both output transitions, $0 \rightarrow 1$ and $1 \rightarrow 0$. The short-circuit power consumed in a period of elaboration of length T is expressed as follows:

$$P_{SC} = \frac{1}{T} \int_0^T V_{DD} i_{SC}(t) dt \quad (1.5)$$

Regarding Figure 1.2, showing the short-circuit current absorption in a CMOS inverter, we can assume that i_{SC} pulses are triangular shaped, with base t_{SC} and height $I_{SC,peak}$. So, Equation 1.5 can be rewritten as follows:

$$P_{SC} = V_{DD} \cdot I_{SC,peak} \cdot f_{CLK} \cdot t_{SC} \cdot \alpha_t \quad (1.6)$$

where $f_{CLK} = 1/T$ is the frequency of the clock signal, and α_t is the *switching activity* of the gate, that represents the probability that a transition of a net occurs in a clock period. The short-circuit power depends strongly on the activity of the gate, both in terms of operating frequency ($P_{SC} \propto f_{CLK}$) and of the probability to change the output state ($P_{SC} \propto \alpha_t$), as well as the the power supply voltage.

The *switching power* is the most important component in dynamic consumption, since it is directly related to charge and discharge of the output capacitance of each gate. Switching events of the output state to its complementary involve the charging or discharging of the output capacitance through the pull-up or pull-down network respectively. In the output transition $0 \rightarrow 1$, the output capacitance is charged to V_{DD} through the pull-up network. The pull-up network provides a resistive path between the output of the cell and the V_{DD} , and a charging current is absorbed from the power rail. During the opposite output transition $1 \rightarrow 0$, the pull-down network offers a resistive path from the output node to ground, while the pull-up network is

in high impedance. The output capacitance discharges towards to ground, and no extra current is absorbed from V_{DD} in this case. The average switching power can be expressed similarly to the short-circuit power, adopting one period of elaboration as time window. For each possible j configuration of inputs, with $j = 1, \dots, N$, we can express average switching power as:

$$P_{switch}^j = \frac{1}{T} \int_0^T V_{DD} \cdot i_{switch}^j dt = V_{DD}^2 \cdot f_{CLK} \cdot C_L \cdot Pr_{0 \rightarrow 1}^j \quad (1.7)$$

where $Pr_{0 \rightarrow 1}^j$ is the probability that a $0 \rightarrow 1$ output transition occurs for the given j -th input combination in T , and C_L is the output capacitance of the gate. We can define the switching activity, introduced in Equation 1.6, with the following formula:

$$\alpha_t = \frac{\sum_{j=1}^N Pr_{0 \rightarrow 1}^j}{N} \quad (1.8)$$

Extending Equation 1.7-1.8 for each possible input, we define the expression of the switching power consumption as follows:

$$P_{switch} = \frac{1}{N} \sum_{j=1}^N P_{switch}^j = \frac{1}{N} \sum_{j=1}^N V_{DD}^2 C_L f_{CLK} Pr_{0 \rightarrow 1}^j = V_{DD}^2 C_L f_{CLK} \alpha_t \quad (1.9)$$

It is clear that the switching power consumption plays a key role in the power budget of a chip, and the technology process impacts meaningfully on its magnitude. In nowadays CMOS technologies, nominal V_{DD} values are reduced compared to past, in order to maintain electric field magnitude constant with shrunk geometry of MOS devices. This allows a strong reduction of the switching power consumption, due to quadratic relation between P_{switch} and V_{DD} . Moreover, the reduction of the transistor size, allows to have smaller C_L , obtaining an additional reduction of P_{switch} . The switching power consumption is also proportional to the operating frequency f_{CLK} and switching activity factor α_t .

1.4.2 Static Power Consumption

In this section, we give only a brief recall of the static current. Further explanation of the phenomenon and its implications in security issues are addressed in Chapter 3. CMOS technologies had an intensive diffusion since early 80's for the very high density of device per mm^2 and for providing theoretically zero static consumption. The static power consumption of a CMOS circuit is defined as the fraction of power linked to the currents flowing in the devices independently from the signals commutations. It is given by the sum of several contributions [127]. In common deep submicron technologies, the sub-threshold current and the reverse biased pn -junction

current are the most important components of the overall static current, and the other contributions are usually neglected in normal operation. Thus, a simplified model for static current is given by the following equation [40]:

$$I_{sub} = K \cdot \frac{W}{L} \cdot e^{\frac{V_{GS} - (V_{TH} - \eta V_{DS} + \gamma V_{SB})}{nV_T}} \cdot \left(1 - e^{\frac{-V_{DS}}{V_T}}\right) \quad (1.10)$$

Thus, we can express the static power consumption as:

$$P_{stat} = V_{DD} \cdot I_{sub} \quad (1.11)$$

More details on the causes and the meaning of static power consumption in this context are reported in Chapter 3.

1.5 Technological Issues in Real World Hardware Cryptography

The first key issue to be faced in the design of cryptographic circuits concerns miniaturization and security assessment of the security modules. As we will discuss further in this work, the concept of security of a cryptographic circuit is strongly related to the paradigm of miniaturization of the integrated circuits. More in general the trend of reducing dimension and power consumption of integrated circuits could be a very challenging task for designers. The reason is that miniaturized devices are optimized under the perspective of improving the performances in terms of area and power, but these improvements do not take security into account. The use of nanometer CMOS technology encountered several problems when the active devices have been used to create complex digital systems such as ASIC (Application Specific Integrated Circuit) and SoC (System-on-Chip) using processes below 90nm. Currently, for the most advanced devices the scaling of transistors has arrived beyond the threshold of 20nm. The reduction of the size of active devices, combined with the increase in the number of levels of metal to be used for the interconnections, led to a higher density in the active area of integrated circuits and to a decrease of the switching delays of the logic elements. For this reason, now it is possible to integrate multiple functions in the same chip and achieve higher frequencies.

However, VLSI (Very Large Scale Integration) design in so-called "deep submicron" technologies revealed some major disadvantages that need to be properly identified and discussed. The main disadvantage of scaling is that also the power supplied to the digital system must unavoidably decreased for physical reasons, and this has a negative outcome on the switching delays, as it takes longer to charge and discharge load capacitances. At the same time, the load capacitance is dominated by capacitance of the interconnect wires, which in turn depend on the physical parameters of the dielectric and the metal (e.g. area of the capacitive plates and

distance between them). This increase of delay, however, is partially mitigated by the decrease of the threshold voltages, due to the reduction of the thickness of the gate oxides. Another problem related to the high scaling of integration is the increase of process variability, which can impact the functionality of the test-chip and must be properly addressed. In order to mitigate these effects, which introduce noise and distortions on the electrical signals to the point that malfunctions can occur during the normal working, techniques for the analysis of the Signal Integrity (SI) at each design step have become increasingly popular. Basically SI has the purpose to monitor the quality of electrical signals in the circuit during all phases of the project in order to provide the designer with a set of methods to guide the design and mitigate these effects. There are several issues that may affect the integrity of the signal, such as ringing, crosstalk, ground and power supply bounce, voltage drop, distortion, signal attenuation, power supply noise, electromagnetic emissions, etc. In the following sections some of the most important issues are mentioned and briefly described.

1.5.1 Ringing

Ringing is an unwanted oscillation of a voltage or a current in a circuit. It happens when an electrical pulse causes the parasitic capacitances and inductances in the circuit (i.e. those that are not part of the design, but just by-products of the materials used to construct the circuit) to resonate at their characteristic frequency [74]. Ringing is undesirable because it causes extra current to flow, thereby wasting energy and causing extra heating of the components; it can cause unwanted electromagnetic radiation to be emitted, generate delays (increase settling time) and also unwanted triggering of bistable elements in digital circuits (e.g. flip-flops) [74]. Usually, ringing can be due to signal reflection, and in this case it may be minimized by a good impedance matching.

1.5.2 Crosstalk

Crosstalk is the interference on the signal propagating on a wire due to the coupling with an adjacent wire [120]. It is a critical issue in the design of deep submicron circuits, because with the technology scaling the metal wires are designed with increasingly reduced distances, and therefore this issue must be adequately described and assessed. Crosstalk has a strong impact on the local interconnection wires of the standard cells, where the most important problem is provided by the capacitive coupling between the wires. Local interconnect wires are typically short and numerous per area unit, leading to a great density; therefore, the amount of cross-coupled capacitance on each wire can be noticeable. The physical reason of crosstalk is the presence of dielectric (e.g. SiO_2 or HfO_2) which separates different metal and causes the appearance of parasitic capacitances; when a signal propagates along a wire, the cross coupled capacitance between that wire and a wire in proximity is charged, and it may create a charge flow in the near wire. Crosstalk may introduce unexpected

delays on the so called “aggressor” wire, and disturbs on the so called “victim” wires. There are several techniques to reduce crosstalk, both a logic and layout level.

1.5.3 Ground Bounce

Ground bounce is an electric phenomenon by which in the internal logic on the die of a chip the ground voltage may have undesired variations with respect to the physical ground voltage of the chip during the switching phases of the internal logic ports, bouncing between values more negative and more positive than what wanted [120]. The ground bounce is associated to the high density of the digital chip and occurs when a high number of logic gates switch at the same time instants; in such case, the current which serves to charge/discharge the load capacitances of the interconnections has a transient when flows to the electrical ground. The ground bounce creates a potential drop on the terminals of the transistor, resulting in unexpected variations of noise margins of the circuit, increases in the propagation times and in several cases also malfunctions. It also represents a major cause of metastability in the circuits. One possible method to mitigate this effect is to ensure the presence of very small resistance path to ground. A similar phenomenon is the power supply bounce which happens on the terminals connected to the power supply.

1.5.4 Voltage Drop

Voltage drop is the percent variation of the nominal value of the supply voltage due to high currents drawn by the devices: higher is the number of devices, higher is the drop [120]. The reduction of the supply voltage of digital circuits is a direct consequence of the technology scaling. In order to have a perspective of how much voltage supplies decreased in last 10 years, we can consider that a $0.6\mu\text{m}$ was supplied with a voltage of 5V, passing through 1.2V for the $0.13\mu\text{m}$ technology, down to less than 1V of modern 18nm technologies. Furthermore power consumption increased considerably due to the fact that the supply voltage decreases less than the increase of the adsorbed current, given that the number of transistors in a chip continues noticeably to grow with the reduction of dimensions. The adoption of higher working frequencies is another important factor. For all these reasons, the voltage drop has become an important issue in submicron circuits. Increasing the width of the power supply wires, the number of metal layers for the power supply wires, and the thickness of the power supply nets are possible solutions for the problem of voltage drop.

1.5.5 Electrical Mismatch

Electrical mismatches [120][40] are a very challenging aspect to deal with during the design steps of digital circuits in modern submicron technologies. They can be originated at different levels of abstraction and are due to two main reasons:

the different propagation times of the signals and the capacitive unbalances of the interconnect wires. Both of them are critical because can reduce the level of security of a specific circuit if not correctly assessed. If two signals have different propagation times, physical leakage generated by the charge flowing (power, EM, etc.) is in general more simple to detect with respect to the ideal situation in which the signals flow simultaneously; indeed, in this second case the physical emission generated by the signals interfere reciprocally. It is very simple to understand this phenomenon in application like PAAs, where timing mismatches are a well-known leakage source [86][139]. Similarly, capacitive mismatches are another potential vulnerability in modern nanometer circuits [148]. With the technology scaling, it is well known that the total amount of load capacitance for a digital circuit is given by the sum of three contributions: the intrinsic output capacitance of the diffusion region of the transistors, the interconnect capacitance, and the intrinsic input capacitance of the gate [120]. The technology scaling leads to a reduction of the dimension of the transistors together with the reduction of the gate capacitance; at the same time, also the parasitic contribution is wanted to be reduced. Thus, the main contribution to the overall capacitance is dominated by the interconnect capacitance, which takes in consideration the contribution of the parasitics and the cross-coupled capacitances on the interconnection. Higher interconnection capacitances increase the delay of the signals and create a mismatched observable leakage.

1.5.6 Process Variations

Variability is a central issue in deep submicron technologies, in which it becomes increasingly difficult to produce two chips with the same behavior. While the impact of variability is well understood from the microelectronic point of view, very few works investigated its significance for cryptographic implementations. The scaling of the CMOS technology, that is the basis of most present microelectronic devices, is a permanent trend since the apparition of integrated circuits in the late 1950s. Shrinking transistors is generally motivated by the need of increased performances and reduced energy per operation. But when reaching the nanometre scale, two major detrimental side effects also arise. First, the relative importance of the static currents increases (i.e. energy is consumed, even if no computation is performed) [110]. Second, device variability becomes important (i.e. it becomes increasingly difficult to engineer identical chips) [31] [112]. As a consequence, during the design of a cryptographic device these issues must be adequately investigated, with a specific focus on power variability, from the point of view of physical attacks. The most important effort in such activity is to properly estimate the level of security of a crypto-device, considering that previously published approaches and methods could be not accurate anymore for 65nm and smaller technologies. Hence, their use may lead to overestimate the security of a (protected or unprotected) implementation. Recent works in the area of leakage resilient cryptography frequently assume that independent computations lead to independent leakage, but this assumption is not fulfilled anymore for 65nm and smaller technologies [125]. Summarizing, while an important literature covers the impact of nanoscale technologies from a microelectronic point of view, e.g. [61],

Table 1.1. A survey of most important techniques for protecting cryptographic circuit against PAAs.

	System	Architecture	Logic	Transistor
Time	Random change of clock frequency	Insertion of random jitter	Asynchronous logic gates	
	Skipping clock pulses	Shuffling of operations	Desynchronization at cell level	
	Multiple clock domains	Insertion of dummy cycles		
Amplitude	Decoupling capacitances	Circuit duplication	Standard-cells DPLs	Full custom DPLs
	Shielding	Architecture masking	Logic masking	Current Mode Logics (CMLs)
	Insertion of noise	Dummy logics		Adiabatic circuits
	Hardware randomizations			
	Current flattening circuitry			
	Supply current suppression			

only a few works consider its consequences in terms of security.

1.6 Countermeasuring PAAs

A brief review of the most known methodologies to counteract PAAs at hardware level is reported [93], [46]. Earlier countermeasures were conceived to overcome PAAs through the insertion of additional dummy instructions at software level in the code running on the microcontroller. Hardware implementations are also based on the addition of redundant circuitry, similarly to the similar approach. The purpose of the countermeasures against PAAs is to balance the switching activity of digital logic circuits in order to prevent any correlation between data and dynamic power consumption. In general, hardware countermeasures can be classified on the basis of two orthogonal axes: the abstraction level and the domain at which they act. According to the abstraction level, hardware countermeasures can be distinguished in system, architecture, logic, and transistor level. For what concerns the domain, hardware countermeasures act in the amplitude or in the time domain. A survey of the most known and adopted hardware countermeasure is reported in Table 1.1, [93], [46].

On a mathematical point of view, hardware countermeasures attempt to reduce the information leakage in two ways: reducing the intensity of the physical observable or increasing the environment noise. This is in accordance to the definition of signal to noise ratio, which will be described in more detail in the next chapter. Basically this can be done in two ways at physical level: some countermeasures have the purpose of breaking directly the link between processed data and power consumption, and fall in the category of hiding countermeasures, because they hide the observable leakage in the amplitude or in the time domain. Other countermeasures try to randomize the power consumption, so that the observed leakage is only poorly correlated to the data; this methodology is called masking. System level techniques have the purpose of preventing the physical observation of the instantaneous power consumption by acting directly on the body of the chip. Decoupling, shielding, randomization, noise insertion, current suppression and flattening circuitry are the most known categories of system level countermeasures and attempt to reduce the amplitude of the physical observable. Among them, decoupling is certainly one of the most efficient techniques, which have been adopted since PAA were discovered for the first time [133]. A

decoupling capacitor acts as an intermediate storage element which filters out the high frequency noise components superimposed on the supply voltage. Therefore, the presence of some capacitance on the power supply line of integrated circuits is mandatory to guarantee the correct functionality, and each EDA tool provides to insert some decoupling capacitors during the back-end design flow. Since PAAs are based on the monitoring of the switching transitions at the power supply line, the presence of decoupling capacitors is an intrinsic countermeasure against PAAs. With the adoption of even more scaled technologies, new countermeasures which adopt on-chip decoupling capacitors were presented in [111], [121], [122], [150], [65]. On the contrary, time domain system level countermeasures act directly on the clock signal of the circuit, in order to insert random jitter or period variation with the aim of introducing misalignment in the measures. Architecture level techniques are probably the most used and effective countermeasure for semi-custom designs. In general, architecture countermeasures are based on the insertion of additional circuitry, which aims at hiding or masking the observable leakage. Note that masking can be done also at logic level by the adoption of novel logic cells, which refer to the Masked Dual-rail Pre-charge Logic (MDPL) family [117]. More in general, lower is the level of abstraction, higher is the effectiveness of the countermeasure but also the design efforts. For instance, Dual-rail Precharge Logic (DPL) styles are the best strategy to protect a circuit directly at physical level [46]. DPLs are based on a specific compound with a differential architecture, and a two phase data-encoding; they can be implemented both at logic level, using pre-designed CMOS standard-cells, and at circuit level, using novel circuit topologies. Design of DPL styles is widely treated in this work, as we will present a novel hardware countermeasure based on a transistor level optimization. In general, the adoption of novel logic styles is used to develop full custom macro-blocks with increased security performances. Several countermeasures links countermeasures at different level (architectural, logical, physical) in order to obtain higher level of security [26].

Chapter 2

Power Analysis Evaluation Methodologies

2.1 Introduction

The concept of physical security, introduced in the previous chapter, have raised new issues in the design of cryptographic devices. Moreover, possible weaknesses due to technology implementations need to be addressed during the design of such secure systems. The evaluation of the information that an adversary could extract from physical emissions requires two basic elements [50]:

1. a leakage model of the device;
2. a distinguisher.

In literature, several works discussed on both aspects, since determining what is the possibility to recover information is not often an easy task, whereas it can be obfuscated and hidden by the presence of countermeasures [50], [137], [91], [49]. The certification of the information leaked from a chip is still an open problem. In fact, we must take into account that the exploitability of a physical emission and its certification have to deal with a concrete exploitation of the information leaked through the target side-channel. In this work, we focus on the *power consumption* as side-channel. Therefore, in this chapter we will address attack procedures based on the adoption of power consumption as side-channel. Also evaluation methodologies need to be introduced to give a measure of performances of electronic circuits for secure applications. For designers, the need of being also on the side of the *expected* adversary helps in determining possible weakness of cryptographic devices in terms of physical security. The definition of *expected* adversary, or the *adversary model* is discussed throughout this work, since it is considered as an important aspect in determining the relevance of potential weakness in a design. Both attack procedures

and evaluation tests have to deal with the concept of statistical security, since the leakage certification is based on the probability density function estimation [49].

2.2 Actual Security Metrics

The evaluation of the capability of an implementation to resist to PAA can be estimated through an evaluation of power measurements and attack outcomes. In literature, various physical security metrics have been proposed to quantify aspects as power variability and effort needed to break the security of a cryptographic device through observation of physical emissions. In the context of analyzing the power consumption, we should consider the structure itself of a power trace. Since the measure of power consumption is performed through an analog-to-digital converter, we consider the power traces/sample as discrete variables. So far, each time sample of a power trace can be consider as the sum of a data-dependent component P_{data} , electronic noise P_{el} and switching noise P_{sw} [93]:

$$P_{total}[j] = P_{data}[j] + P_{el}[j] + P_{sw}[j] = P_{data}[j] + P_{noise}[j] \quad (2.1)$$

In general, the adversary wants to exploit the data-dependent component P_{data} of the overall power consumption, in order to recover the secret information. Under the assumption of additive Gaussian noise, which takes in consideration both electronic and on-chip (or switching) noise [93], different measurements of a selected time sample, performed with the same input, lead to Gaussian distributed sample values. Hence, the density function describing the normal distribution of noise can be described with mean μ_{noise} and standard deviation σ_{noise} . In general, we can consider:

$$P_{noise} \sim N(\mu_{noise} = 0, \sigma_{noise}) \quad (2.2)$$

2.2.1 Signal-to-Noise Ratio, SNR

One of the first security metrics based on the presence of a noisy component in the overall power consumption is the *Signal-to-Noise Ratio* (SNR). The SNR relies on matching between the concept of variance and power, and it is defined as follows:

$$SNR[j] = \frac{\sigma_{data}^2[j]}{\sigma_{noise}^2[j]} \quad (2.3)$$

where σ_{data}^2 represents the variance of the data-dependent part of the power consumption, and quantifies how much the power consumption varies due to data-dependency,

which is the component that the adversary wants to exploit. In other words, the SNR quantifies how much information is leaked in a time sample in terms of power.

2.2.2 Energy-based Security Metrics

In literature, another common approach to evaluate the data-dependency of the power consumption of a digital circuit is to use the energy variability. We define the energy per cycle E_{cycle} as:

$$E_{cycle} = \int_0^{T_{ck}} V_{DD} \cdot i_{DD}(t) dt \quad (2.4)$$

where T_{ck} is the clock signal's period, V_{DD} the power supply voltage, and i_{DD} is the current absorbed. Using the definition in [144], we introduce the *Normalized Energy Deviation* (NED):

$$NED = \frac{\max(E_{cycle}) - \min(E_{cycle})}{\max(E_{cycle})} \quad (2.5)$$

where $\min(E)$ and $\max(E)$ are the minimum and maximum value of the energy regarding the input vectors, and the *Normalized Standard Deviation* (NSD):

$$NSD = \frac{\sigma_E}{\overline{E_{cycle}}} \quad (2.6)$$

where σ_E and $\overline{E_{cycle}}$ represent the standard deviation and the average value of the energy per cycle respectively.

2.2.3 Measurements To Disclosure, MTD

In order to give an estimation of the robustness of an implementation to a side-channel attack, it is useful to find the minimum number of measurements that are necessary to recover the secret key used by the hardware implementation [92] [145]. This security metric is called *Measurements To Disclosure* (MTD), and allows to quantify the effort that the adversary has to make regarding a certain attack scenario.

2.3 Attack Methodologies

The analysis of the possibility to break the physical security of a cryptographic accelerator through a target side-channel is strictly related to the probability that

the *expected* adversary has to recover the secret information from the device itself. It is clear that we must consider that the adversary sees the cryptographic device as a *black box*. Since Power Analysis Attacks are non-invasive SCAs, monitoring side-channel emission for retrieving information about a not easily-accessible system can be considered as a classical engineering problem [52].

In general, PAAs are based on the strong relation between processed data and the respective power consumption in a electronic circuit. If the malicious adversary has the possibility to monitor the power consumption of a cryptographic device while it is performing encryption/decryption operations, he/she can extract useful information to break its security. As we have previously mentioned, in a PAA, and in general, in a SCA, it is critical to have a sounding *leakage model*, that in this case is a *power model*. During a PAA, the adversary collects a certain number of so-called power traces of the device under attack, with known input vectors. Under proper assumptions of the operation that the device under attack could perform (e.g. the secret key), he/she can build a set of hypothetical power consumptions related to the input vectors set and a target intermediate function of the cryptographic algorithm, adopting a certain power model. At this point, he/she compares the hypothetical power consumptions with actual power consumptions with statistical tools. Relying on the output of the adopted statistical tools, the adversary guesses one (or a sub-set) of the operation (e.g. the key) that took place on the device under attack. This simple paradigm hides a plethora of different procedures. Their effectiveness depends on several aspects of both sides of the attack:

- the attack capability of the adversary;
- the design of the device under attack.

These two aspects play key roles in the the typology of the attack and its effectiveness against a specific hardware device. In terms of *power model*, attack procedures can be divided in two categories: *non-profiled* and *profiled* attacks. In a *non-profiled* attack, the adversary makes use of an *a priori* model of the actual data-dependent consumption of the device, relying on a linear (or quasi-linear) relation between processed data and current absorption. Usually *a priori* power models are in the form of a number, and allowing to exploit linear (or quasi-linear) dependencies of actual power consumption with processed data. In a *profiled* attack, the adversary needs of a clone device of the same class of the device under attack to build a sounding power model. The clone device has to be implemented using the same design but it should also offer the possibility to be programmed in terms of key and plaintext. In this case, a sounding power model is built upon the clone device's power consumption, creating so-called profiles. They are used to exploit similarities with the power consumption measured on the device under attack. A huge difference between *profiled* and *non-profiled* attacks relies on the fact that in *profiled* attacks the power model is built using real power samples rather than a merely relation between processed data and consumption.

2.3.1 Differential Power Analysis

The first example of a PAA has been proposed by Kocher *et al.* in [84], with *Differential Power Analysis* (DPA). In DPA attacks, the attacker chooses a single bit of a target intermediate function output word processed within the device. The target output function needs to be related on the secret the adversary wants to recover. Then the attacker divides the collected set into two sub-sets according to the value of the chosen bit. In this case, the power model is the simple bit value. The guess on the correct key is obtained by using the *difference of means* (DoM) test as statistical distinguisher. Higher is the difference of means for a certain key hypothesis at sample j , higher is the correlation between the power model and the actual measurements. If we consider the binary matrix H , with n rows and K columns (with K number of possible key hypothesis), as the power model matrix related to the target bit for each key hypothesis, and T the power measurements set for n plaintexts, each composed by N samples, we compute the difference of means for key hypothesis k_i as:

$$DoM_i[j] = \frac{\sum_{l=1}^n h_{l,i} \cdot t_l[j]}{\sum_{l=1}^n h_{l,i}} - \frac{\sum_{l=1}^n (1 - h_{l,i}) \cdot t_l[j]}{\sum_{l=1}^n (1 - h_{l,i})} \quad (2.7)$$

with $j = 1, 2, \dots, N$ and $i = 1, 2, \dots, K$. Equation 2.7 can be rewritten as:

$$DoM_i[j] = M_{1,i}[j] - M_{0,i}[j] \quad (2.8)$$

The key hypothesis k^* which maximizes the difference of means is chosen as guessed key:

$$k^* = \operatorname{argmax}_i \{|DoM_i|\} \quad (2.9)$$

2.3.2 Correlation Power Analysis

In 2004, Brier *et al.* proposed the *Correlation Power Analysis* (CPA) [32] as attack procedure, which makes use of multi-bit related power consumption to retrieve sensible information. In a CPA attack, the adversary chooses an intermediate result of the cryptographic algorithm as target function, similarly to DPA. For each possible key k_i , with $i = 1, \dots, K$, the hypothetical result of the target function is computed for each input vector used. A matrix J of size $n \times K$ is built with hypothetical results, where n is the number of queries used in the attack. In CPA, a multi-bit power model is used to compute the matrix H of hypothetical power consumption from the matrix J . A common choice is to use the *Hamming Weight* (HW) or the *Hamming Distance* (HD) as sounding power model for CMOS circuits. The underlying assumption of HW/HD models can be resumed as follows: each bit in a m -bit slice architecture

contributes equally to the total power consumption. The matrix H is then compared with the collected power traces set $T = t_i[j] | i = 1, 2, \dots, n, j = 1, 2, \dots, N$, by means of the Pearson's correlation coefficient as statistical distinguisher, obtaining the matrix R of size $K \times N$. Each element of $R = \rho_i[j]$ is expressed as follows:

$$\rho_i[j] = \frac{\sum_{l=1}^n (h_{l,i} - \bar{h}_i) \cdot (t_l[j] - \bar{t}[j])}{\sqrt{\sum_{i=1}^N (h_{l,i} - \bar{h}_i)^2 \cdot \sum_{i=1}^N (t_l[j] - \bar{t}[j])^2}} \quad (2.10)$$

The key hypothesis k^* which maximizes the correlation coefficient in Equation 2.10 is chosen as guessed key:

$$k^* = \operatorname{argmax}_i \{|\rho_i|\} \quad (2.11)$$

In the context of CPA/DPA attacks, the *Success Value Indicator* (SVI) [111] is widely diffused to assess how well the correct key can be distinguished from the wrong keys. For CPA attacks, it is defined as follows:

$$SVI = \max \{|\rho_{corr}|\} - \max \{|\rho_{wrong}|\} \quad (2.12)$$

where $\max \{|\rho_{corr}|\}$ is the maximum value of the correct key's correlation coefficient, and $\max \{|\rho_{wrong}|\}$ is the highest value of the correlation coefficients corresponding to the best ranked wrong key. If the SVI is strictly positive, the correct key is successfully recovered among wrong keys.

2.3.3 Extensions of CPA Algorithm

CPA attacks have been extended and analyzed in-depth in several works during the last two decades. Noteworthy extension of the methodology behind CPA has been proposed by Schimmel *et al.* in [130], with *Correlation Power Frequency Analysis* (CPFA). In CPFA, the data-set is pre-processed with Fast Fourier Transform (FFT) to extract Power Density Spectrums (PSDs) of power traces, and then the CPA is performed in the frequency domain. The attack performed in the frequency-domain allows to relax some attack requirements, such as time alignment of power traces. In a regular CPA attack, such as also in DPA attacks, the acquisition of power traces has to be synchronized with a precise time sample, in order to guarantee alignment of the data set. CPA/DPA attacks are intrinsically univariate attacks, and they require that the information leakage has to appear approximately in the same time samples to be effective. CPFA relax this constraint, as the transformation to the frequency domain removes the time shifting (desynchronization) if the PSD windows is large enough. In CPFA, the information in time-domain is totally removed, since it works only in the frequency-domain. In some countermeasure schemes, the clock frequency is changed randomly to provide desynchronization and immunity to CPFA. In [80],

an enhancement of CPA technique based on spectrogram analysis is proposed, called Correlation Power Spectrogram Analysis (CPSA), to overcome limitations of CPFA. In this case, the *Short-Time Fourier Transform* (STFT) is adopted to convert the data-set in a mixed time/frequency domain before performing the CPA.

On the side of adopted power model, in [143] a slight different multi-bit power model is adopted. In modern MOS transistors, the drain current in the saturation region does not follow the classical square law $I_D \propto V_{ov}^2$. In fact, in many applications the drain current expression is evaluated through the *alpha-power law* in saturation region [7]:

$$I_D = K(V_{GS} - V_{TH})^\alpha \quad (2.13)$$

with $1 \leq \alpha < 2$. In order to better fit *a priori* power models to actual power consumptions, each element of the hypothetical power matrix H is pre-processed using exponentiation with a factor $\beta \in (0, 1)$, in order to improve values of correlation coefficients:

$$\tilde{H} = (H)^\beta \quad (2.14)$$

The CPA comparison is then performed using $\tilde{H}$ instead H .

2.4 Template Attacks

In several cases, dependencies of processed data in power consumption do not rely on linear relations. In such cases, it is not always possible to use *a priori* models to soundly fit actual consumption. To overcome issues in efficiency of *a priori* power models, Chari *et al.* introduced *Template Attacks* (TAs) in 2003 as the strongest sub-class of PAAs [41]. In TAs, that are classical examples of *profiled* attacks, the adversary has to have an identical experimental device, called *clone device*, which can be programmed. This requirement can be limiting, but it holds in many practical cases [56], [103]. The adversary makes use of the clone device to create a set of profiles of power consumption in order to detect features on the cryptographic activity on the device under attack. These profiles, also called *templates*, contain a characterization of the device in terms of statistical estimation of moments, and can be conducted as univariate or multivariate. In practical cases, the adversary can build a profile for each possible couple of input and sub-key to attack, in order to get a classification of the leakage over the entire space of keys. Each template contains a characterization of the data-dependent component of the overall power consumption, and can contain also a characterization of the noise. In literature, it is common to adopt Gaussian models for the noise [41]. A TA is structured in two stages. The first one is called profiling and it is performed on the clone device. During this stage, the adversary estimates first order and second order moments of the power consumption on the clone device, obtaining a characterization for each

key and input couple (e.g. operations). We can summarize the steps in the profiling stage as follows:

1. The adversary collects L power traces of N points on the clone device for each key and input couple. For easiness, we call each key and input couple a operation. Let us assume that we have K operations $O_1, O_2, \dots, O_K$. Hence, we have K matrix T_i of size $L \times N$, with $i = 1, \dots, K$.
2. K average vectors $M_1, M_2, \dots, M_K$ are computed for each O_i operation:

$$M_i[j] = \sum_{l=1}^L \frac{T_i^{(l)}[j]}{L} \quad (2.15)$$

with $j = 1, 2, \dots, N$. These average vectors represent the data-dependent component of the measured power consumption, since the noise is supposed to have zero-mean.

3. Average vectors M_i are used to extract $I < N$ *interest points* or *features* (in the case of multivariate analysis) $P_1, P_2, \dots, P_{N_P}$. The relevance of these *interest points* relies on the fact that meaningful samples in a power traces are those ones that are strongly dependent in magnitude from the processed data. Time samples that carry no information are non relevant for PAA, and thus, they can be discarded. After the extraction, the average vectors are compressed to the sub-set of index related to $P_1, P_2, \dots, P_{N_P}$. A small loss in accuracy is traded for reduced processing overhead if the features are extracted properly.
4. For each operation O_i , the N_P -dimensional noise vectors are computed between the L power traces and their respective average vectors. After that, L *noise covariance matrices* Σ_i are computed between all pairs of components of the noise vectors for operation O_i .

At this point, the adversary has characterized data-dependent and noisy components of each key and input couple on the clone device. For each key-input couple, he/she has defined a template (M_i, Σ_i) , that is used to retrieve secret information from the actual power consumption of the device under attack. The second stage of the template is called *attacking*. The adversary measure the power consumption t of the device under attack, and uses the templates to perform a matching detection by computing the following probability with each collected power traces l over the interest points of index $P_1, P_2, \dots, P_{N_P}$:

$$Pr(t; O_i) = \frac{1}{\sqrt{(2\pi)^{N_P} |\Sigma_i|}} \exp \left(-\frac{1}{2} (t - M_i)^T \cdot \Sigma_i^{-1} (t - M_i) \right) \quad (2.16)$$

where $|\Sigma_i|$ is the determinant of Σ_i , and Σ_i^{-1} is its inverse. If the noise is Gaussian, the approach of selecting the O_i which maximizes $Pr(t; O_i)$ is optimal. This is approach

Table 2.1. Number of templates needed to attack a 8-bit sub-key of a hardware implementation of AES-128 with various partitioning schemes.

Partitioning Scheme	No. Of Templates
(key,input) pairs	$256 \times 256 = 65536$
S-BOX out. value	256
HW(S-BOX out. value)	9

is also known as *maximum likelihood* decision rule. In a practical attacks, multiple measurements are taken into account, in order to minimize noise. So, the adversary collects a data set $T = t_s$ with $s = 1, \dots, S$. Since we are interested in computing the probability $Pr(O_i|T)$ from the prior probability $Pr(O_i)$ and probabilities $Pr(t_s|O_i)$ for each $s = 1, \dots, S$ and $i = 1, \dots, K$, the adversary can compute [93]:

$$Pr(O_i|T) = \frac{\left(\prod_{s=1}^S Pr(t_s|O_i)\right) \cdot Pr(O_i)}{\sum_{g=1}^K \left(\left(\prod_{s=1}^S Pr(t_s|O_g)\right) \cdot Pr(O_g)\right)} \quad (2.17)$$

where probabilities $Pr(t_s|O_g)$ are computed according to Equation 2.16. At this point, the *maximum likelihood* decision rule is used to choose the template O_i , and thus the key, which exhibits the highest probability:

$$k^* = \operatorname{argmax}_i \{Pr(O_i|T)\} \quad (2.18)$$

2.4.1 Improving Efficiency of Template Attacks

Also Template Attacks have been extended since the first paper was published in 2003, and many researchers have worked to improve the effectiveness of this powerful sub-class of attacks. In [93], authors propose alternative ways to create partitions in profiling, in order to work with a reduced number of profiles, thus, reducing the processing overhead. In fact, we must take into consideration that during the attacking phase, it is required to compute the inverse of a covariance matrix, which is indeed a source of numerical and computational problems. This computation requires an inversion of a square matrix for each template, so, reducing the number of templates, the adversary can reduce also the average computational cost of the attack algorithm. A possible strategy is to make partitions of templates. For example, it is possible to use the value of a certain key-dependent intermediate function of the cryptographic algorithm we want to exploit to create partitions of templates. Moreover, it is also possible to make use of power consumption properties to further reduce the number of templates. For example, using the HW of an intermediate value, it is possible to make the number of templates to less than a tenth in AES-128 implementation (see Table 2.1).

A huge effort has been also devoted to compression techniques. The reduction of the dimensionality of a detection problem is widely diffused in Data Analysis (e.g. image recognition, neural networks, pattern recognition, etc.). When the adversary collects power traces, each measured vector can contain thousands of time samples. It can be demonstrated that most of them are not relevant for PAA, and thus, they can be discarded [93]. The problem behind the compression of power traces during profiling stage is two-fold:

- how many points of interest?
- how do they can be selected?

These two questions have been discussed in-depth in [57], [43], [123] and [11]. Regarding on the number of points of interest to maintain as outcome of the compression, there is no a general rule to follow. If the number of points is high, two problems can come up. Firstly, the problem of detection can be *overdetermined* and the effectiveness of the attack in recovering the secret is reduced. Moreover, numerical problems can occur due to the inversion of large covariance matrices. If the number of points is too low, the problem of detection can be *underdetermined* and the accuracy of profiles may be very poor, as well as the capability of the attack in recovering the secret. Regarding the extraction of interesting points during the profiling stages, there are several techniques that can be used. Many of them are quiet similar to non-profiled attacks procedures. A commonly used approach is to define a *signal-strength* f function with a given rule [57]. Computing the signal-strength function, the adversary should search for N_P points, exhibiting N_P highest values of f . Popular techniques to extract interesting points are summarized in the following:

- Difference of means (DoM) [41];
- Sums of Squared Differences (SoSD) [63];
- Sums of Squared T-test (SoST) [63];
- Correlation Power Analysis (CPA) [93];
- Signal-to-Noise Ratio (SNR) [93];
- Variance based Method (VAR) [95];
- Mutual Information Analysis (MIA) [62];
- Kolmogorov-Smirnov Analysis (KSA) [152];
- Principal Component Analysis (PCA) [11].

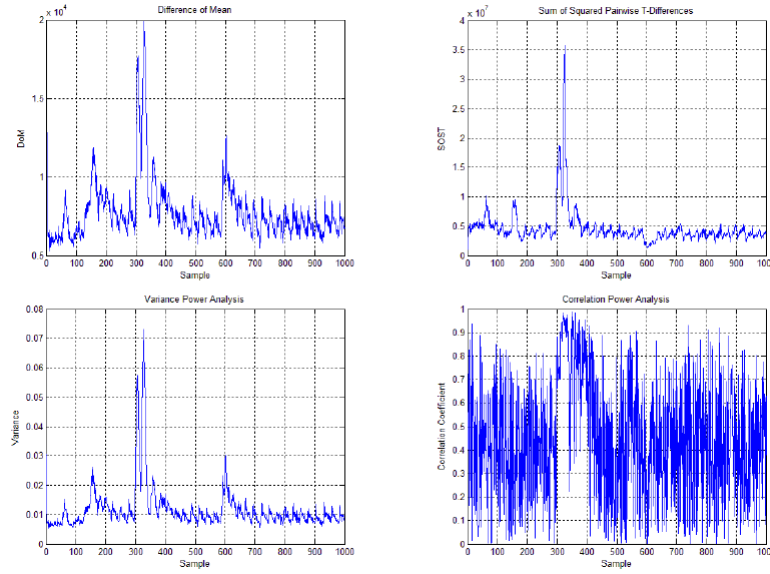


Figure 2.1. Signal-strength function evaluation using DoM, SoST, VAR and CPA on a FPGA implementation of a AES-128 block cipher.

2.5 Enhancement of Effectiveness of PAAs through Pre-Processing

In this chapter, we have discussed about the composition of a power trace as a sum of a data-dependent and cryptography-related component and a noisy component. It is natural to think that higher is the magnitude of the data-dependent component, higher will be the probability to successfully exploiting the power consumption. On the other hand, we can assume also that smaller is the noisy component, higher will be the probability of success. In all research contexts where a noise process is intrinsically part of the observed system (this position always holds in practical cases), a lot of the effort is made in the reduction of the power of noise. Techniques used to reduce the noise power, thus, increasing the output SNR, are called *de-noising* techniques. Since, in PAA it is useful to de-noise the data set before performing the PAA itself, the act of reducing the noise power is also called *pre-processing*. In the context of PAAs, several pre-processing techniques have been proposed with the purpose of increasing the probability of success in recovering the secret key from a cryptographic device. Adopting such techniques allows to:

- speed up the velocity to reach the secret key;
- reduce the computational cost of the actual PAA (optional).

The first aspect is very relevant, because impacts indirectly also on the latter. A real adversary has a limited storage capability in collecting power traces/samples, and he/she is limited by the storage capability of the computer used to save the data-set. Speeding up the velocity of the attack experiment means also that the MTD can be

smaller if compared with straight PAA, which corresponds to relax the demanding constraints in time needed to recover the secret key and the minimum storage capability to store the data-set. In this section we briefly present two pre-processing techniques that have been proposed in literature in the context of PAAs.

2.5.1 Principal Component Analysis, PCA

Principal Component Analysis (PCA) is a compression/filtering technique widely diffused in several research contexts for reduction of the noise and data-set dimensionality using a variance-oriented conservative approach [14] [71]. The aim of PCA is to search for linear combinations in the given data-set, that lead to high values of variance, summarizing them in principal components, representing most of the information carried within the data-set, discarding secondary, or non-principal, components, corresponding to noise. This operation is performed by projecting the data-set to a new space, using a basis composed by eigenvectors of the covariance matrix of the data-set itself. In order to perform PCA denoising, means M_t and standard deviations σ_t for each time sample of collected power traces data-set L have to be computed:

$$M_t = \frac{\sum_{i=1}^N L_{i,t}}{N} \quad (2.19)$$

$$\sigma_t = \sqrt{\frac{\sum_{i=1}^N (L_{i,t} - M_t)^2}{N}} \quad (2.20)$$

At this point, the data-set L is standardized into L_s using means and standard deviations in Equation 2.19-2.20:

$$L \rightarrow L_s \quad (2.21)$$

The covariance matrix Σ_s is then computed on L_s . Eigenvectors and eigenvalues of Σ_s are computed, decomposing the covariance matrix as follows:

$$\Sigma_s = U \cdot \Lambda \cdot U^{-1} \quad (2.22)$$

where Λ represents the diagonal matrix containing eigenvalues and U eigenvectors matrix. Eigenvectors corresponding to highest values of eigenvalues are considered *principal components*, since their magnitude are strongly related to the variance (and thus PAA information) of their respective eigenvectors. These principal eigenvectors represent directions with the maximal variance. Selecting a limited number c of those directions, it is possible to create a new matrix representing the data-set, using these eigenvectors as basis. There are several rules that can be used to define the

number c of principal components to consider. A simple but effective method use a threshold rule to define c . The threshold can be obtained as a particular ratio of the sum of total variance, expressed as the sum of all eigenvalues. If the eigenvalues as ranked in descending order, one can perform a cumulative sum of the eigenvalues, until the threshold value is reached. At this point, all eigenvectors related to unused eigenvalues are discarded. A new matrix U_r is built using remaining eigenvectors, and padding with zeros all unused columns, and a denoising matrix U_d is the computed as:

$$U_d = U_r U_r^T \quad (2.23)$$

In order to restore the original space without the noisy components, one should perform:

$$L_d = L_s U_d \quad (2.24)$$

Another possible approach allows to reduce also the dimensionality of the denoised data-set. In this case, the rotation matrix U_{rc} is built only using the principal components, and the rotation into the original space provides also a reduction of the dimensionality to a c -sized problem:

$$L_d = L_s U_{rc} \quad (2.25)$$

In both approaches, the denoised data-set L_d should be de-standardized.

2.5.2 Wavelet-based Denoising

The adoption of the *Wavelet Transform* in SCAs is widely diffused [135], [115], [47], [90]. In [128], a combination of PCA and wavelet transform denoising technique is presented. As we have previously discussed about CPFA, Fourier transform totally removes the dependency of the time, moving the analysis to the frequency-domain. The adoption of the STFT, partially relax, maintaining a mixed domain analysis. The problem behind the STFT is that the efficiency of the analysis is strongly dependent by the adopted length of the window function $g(t)$, since both time and frequency accuracy rely on the window length. Wavelet transform allows to overcome this issue since the analysis is performed by means of scaling and time translation of a function Ψ , named *mother wavelet*. The continuous time wavelet transform is expressed as follows:

$$W_{f(a,b)} = |a|^{-\frac{1}{2}} \int f(t) \Psi \left(\frac{t-b}{a} \right) dt \quad (2.26)$$

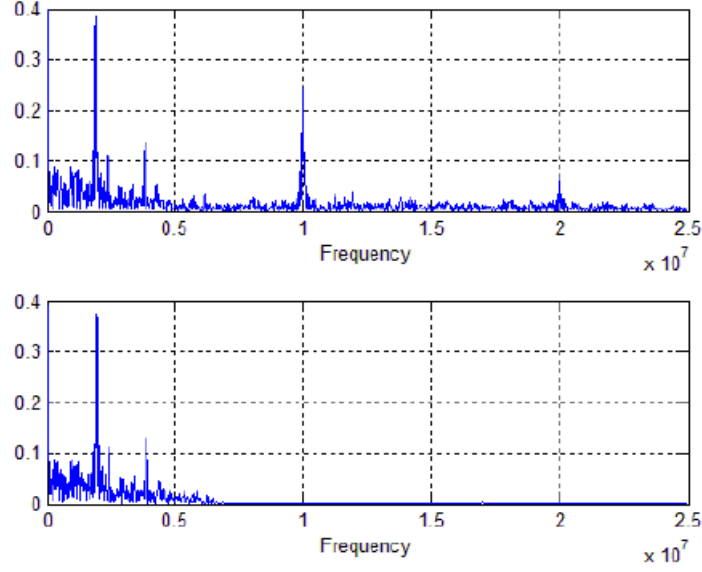


Figure 2.2. FFT of a power traces of a FPGA implementation of AES-128 pre (top) and post (bottom) the wavelet decomposition, stopped at level 2 using 'dB4' as mother wavelet.

whereas the mother wavelet $\Psi(t)$ is defined as:

$$\Psi_{a,b}(t) = |a|^{-\frac{1}{2}} \Psi\left(\frac{t-b}{a}\right) \quad (2.27)$$

Coefficient a and b define the scaling and time shifting of the mother wavelet respectively. $W_{f(a,b)}$ coefficient express the similarity between $f(t)$ and $\Psi_{a,b}(t)$. Since in our context, collected signals are discrete in time and magnitude, we make use of the *discrete wavelet transform*. Coefficients a and b can be rewritten as:

$$a_m = 2^m \quad (2.28)$$

$$b_{mn} = a_m nT = 2^m nT \quad (2.29)$$

where T is the sampling period of the input signal $f[k]$. The discrete wavelet transform can be expressed as follows:

$$W_{(m,n)} = 2^{-\frac{m}{2}} \sum_k f[k] \Psi[2^{-m}k - n] \quad (2.30)$$

The input signal $f[k]$ is decomposed by a diadic decomposition, and for each new level of decomposition, it is splitted in two components, called *approximation*

and *detail*, corresponding to low-frequency contents and high-frequency contents respectively. Each new approximation is sub-sampled by a factor of 2, and it is used to generate a new diadic decomposition with new coefficients. The application of wavelet transform as denoising technique is based on the assumption that the information leakage is contained from DC to a certain frequency. It is reasonable to consider relevant only approximation coefficients of the diadic decomposition of the input signal (e.g. power trace) $f[k]$. It is critical to understand the following aspects:

- which is the optimal level of decomposition;
- which mother wavelet provides better results.

The optimal level of decomposition has been formalized in [115], while the latter one is still an open problem in the context of PAA.

Once defined the level of decomposition and the mother wavelet, the denoising process takes place before running the PAA algorithm, and it has to be applied to each power measurement within the collected set. An example of the effect in the frequency domain of denoising with wavelet transform is depicted in Figure 2.2.

2.6 Information Theoretic Security Metrics

In the SCA attack community, the role played by the practical evaluation and quantification of information leaked through physical emission has gained growing relevance. It is clear that the presence of a leakage model can mislead to different interpretations of the physical security, since different devices leak differently [138] [104] [134]. In 2009, Standaert *et al.* proposed an information theoretic approach with the aim of fairly evaluating the robustness of different implementations without adopting a specific power model [137]. A fairly and sounding evaluation tool needs also to be *adversary independent* in addition to *implementation/technology independent*, avoiding limitations due to ad hoc approaches in the analysis of physical emissions. The framework proposed in [137] takes advantage of the information theoretic concept of entropy, introduced in [134] by Shannon. This intuitive approach aims to give a fair measure of the information leaked through the physical emission, without demanding limitations of a specific power model. In the context of quantifying the information leakage, two practical security metrics have been introduced:

- mutual information;
- perceived information.

In the following, the two information theoretic security metrics are briefly introduced.

2.6.1 Mutual Information

Introduced in [91], the *mutual information* (MI) quantifies the amount of information leaked by a hardware implementation of a cryptographic algorithm. The MI is able to quantify the information leaked by the processor using the conditional entropy, by means of probability density functions (PDFs), assuming a Gaussian distribution for the power samples. It can be expressed as follows:

$$MI(X; L) = H[X] - \sum_{x \in X} Pr(x) \sum_{l \in L} Pr_{chip}(l|x) \log_2 Pr_{chip}(x|l) \quad (2.31)$$

where X is a random variable, $H[x]$ its entropy, $Pr(x)$ the probability of $x \in X$ and L is the observed leakage. The probability $Pr_{chip}(x|l)$ is derived from $Pr_{chip}(l|x)$ by means of Bayes' theorem. The underlying assumption is based on the fact that the adversary has a perfect knowledge about the distribution $Pr_{chip}(l|x)$. So, mutual information represents the upper bound of the amount of information that can be extracted from a hardware implementation.

2.6.2 Perceived Information

The *perceived information*, presented in [137] and defined in [125], captures the information about the secret variable X obtained when observing leakage L , generated according to the probability distribution $Pr_{chip}(L|x)$, and interpreted with the model $Pr_{model}(L|X)$:

$$\hat{P}I(X; L) = H[X] - \sum_{x \in X} Pr(x) \sum_{l \in L} Pr_{chip}(l|x) \log_2 Pr_{model}(x|l) \quad (2.32)$$

The perceived information in Equation 2.32 estimates how well the model described by $Pr_{model}(L|x)$ is suitable for the implementation under analysis, and how much information an adversary could extract with this model, considering it *non perfect*. The use of this metric allows to define the "average case" for the adversary, because assumptions used in this case describe well a realistic attack scenario. In a real scenario, we have [125]:

$$\hat{P}I(X; L) \leq MI(X; L) \quad (2.33)$$

Moreover, the perceived information is not lower bounded [125], and thus, can assume negative values.

Chapter 3

Attack Exploiting Static Power in Deep Sub-Micron Technologies

3.1 Introduction

In the history of Power Analysis Attack, the first physical source that has been used to recover secret information from cryptographic device is dynamic power. Since the total power consumption has been dominated by dynamic power consumption from the early days of CMOS technology, both for regular and secure design, the primary aspect to look for in the power domain has been the instantaneous current absorption. In the last decade, this aspect of the digital design has been progressively altered by the side-effects in sub-micron technologies. New technologies in CMOS fabrication allowed to reduce transistors' geometric and physical feature size. The aim of this reduction is double-fold. The reduction of the transistors size has brought to a reduction in the capacitive parasitics, which has a direct impact on power consumption. In fact, since the instantaneous power consumption of a CMOS gate is linearly dependent on the capacitive load C_L , as shown in Equation 3.1, reducing the minimum size of a transistor leads to a reduction of the power consumption. Reducing the oxide thickness T_{OX} , also the maximum supply voltage V_{DD} has to be scaled accordingly, in order to accommodate the shorter channel length and keeping constant the electric field to avoid reliability issues. The dynamic power consumption of a CMOS gate is shown in Equation 3.1:

$$P_{dyn} = V_{DD}^2 \cdot f_{clk} \cdot \alpha \cdot C_L \quad (3.1)$$

where f_{clk} is the clock frequency and α is the switching activity of the gate. As we can see, reducing the V_{DD} leads to a quadratic reduction of the overall dynamic power consumption, while P_{dyn} decreases linearly with C_L . For example, in Figure 3.1,

the same logic design on four different Xilinx Virtex FPGAs, implemented with four different sub-100nm technologies, has different $P_{\text{dyn}}/P_{\text{stat}}$ ratio. The dynamic power consumption decreases as the scaling factor increases, while the static one increases [75] [69].

In modern integrated circuits the overall power budget is not dominated by the dynamic power consumption anymore. For CMOS technologies with channel lengths below 40nm, the static component is a not negligible part of the overall power consumption. The static power consumption is defined as the power that a circuit consumes when no transitions occur, and the state of the circuit remains stable:

$$P_{\text{stat}} = V_{DD} \cdot I_{\text{stat}} \quad (3.2)$$

In Equation 3.2, the static power consumption is described as the product of the static current absorption I_{stat} due to parasitic phenomena in a MOS circuit with the power supply voltage. This current is expected to increase in the future, as we will see in the next sections.

In a MOS transistor, there are several phenomena that lead to a static power dissipation. As the technology of CMOS fabrication went below the 100nm process, these phenomena have led to a rapid increase of static current magnitude in an integrated circuit. The reduction of the geometry of a MOS transistor implies that the thickness of the oxide T_{OX} has to be reduced, and the minimum distance between the drain and the source region has been reduced as well. As we will discuss later, the scaling of the geometry of the MOS transistor has a direct relation with the static current, which has also a strong relation with the level of security of a hardware implementation of a cryptographic algorithm.

The strong increase in the static currents magnitude implies critical problems in design of modern integrated circuits. The presence of not negligible static consumption impacts on several aspects. In mobile devices, and in nowadays Internet of Things (IoT) smart nodes, long idle time intervals are dominant in the lifetime of the device. In order to save power, it is a common practice to use clock gating, which actually stops the activity of unused sections of the chip. In this situation, static power is dominant compared to dynamic, and with newer technologies is not negligible. Higher static consumption reduces the battery life, and thus, the usability of the device. Another straightforward issue related to modern technologies and to the rising of the static power consumption magnitude is the increment of the device's working temperature, due to self-heating. This aspect impacts meaningfully also on the cost of the fabrication, since higher temperatures require special packaging techniques and expansive cooling systems. In addition, higher working temperatures can affect the reliability of the chip, due to problems with electromigration which can easily reduce the device's lifetime.

Beyond technologies issues, there is a less explored aspect related to the static

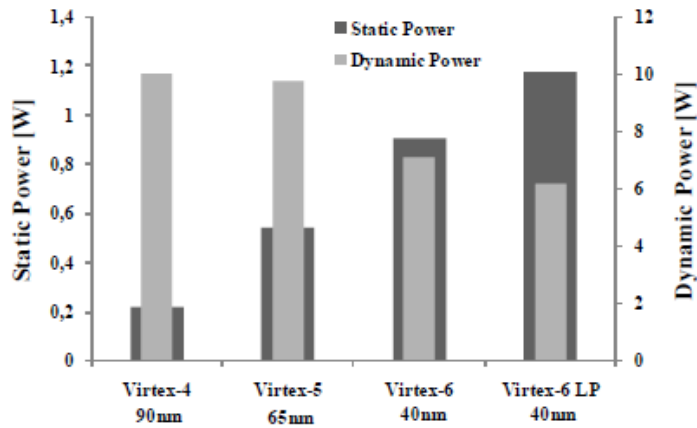


Figure 3.1. Static versus dynamic power consumption of the same design on four different Xilinx Virtex FPGAs [75].

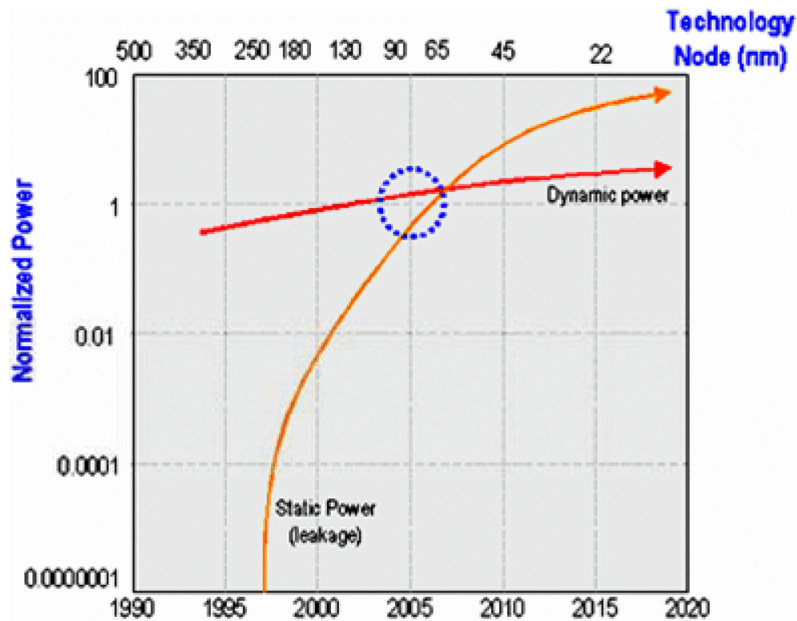


Figure 3.2. Power consumption trend within three decades. The inflection of 90nm technology has remarked a critical point for designers, highlighting the importance of static consumption in the power budget [69].

power consumption of modern technology. As we will discuss later on this chapter, the static power consumption has been found to be data-dependent, and it implies that it will not be only a secondary issue anymore for secure applications.

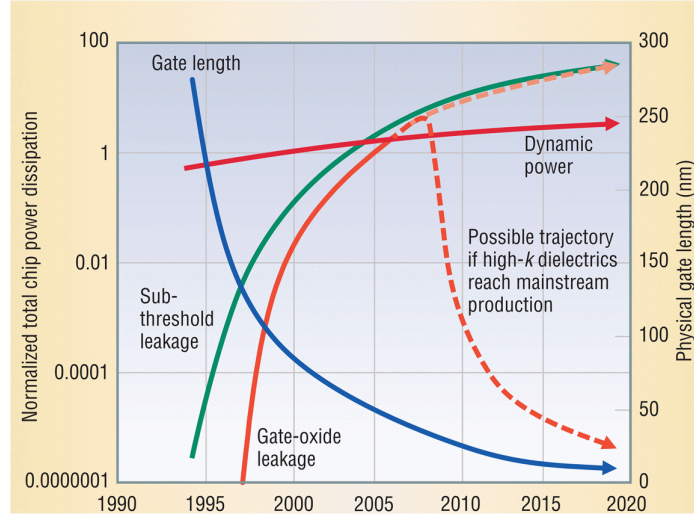


Figure 3.3. Power consumption in integrated circuits [81].

3.2 Leakage Current Sources

We can resume three main leakage current sources in a MOS transistor as follows [53]:

- sub-threshold leakage I_{sub} ;
- reverse-biased pn junction leakages I_{pn} ;
- gate leakage I_{gate} .

A simplified view of the MOS structure for a N-channel device with the three main components of the overall static current absorption is depicted in Figure 3.4.

The overall static current of a MOS transistor can be seen as the sum of three main components:

$$I_{\text{stat}} = I_{\text{sub}} + I_{\text{pn}} + I_{\text{gate}} \quad (3.3)$$

3.2.1 Sub-Threshold Leakage

If the gate-source voltage of the MOS transistor is below the threshold voltage V_{TH} , a small current still flows through the source and the drain regions, because the transistor is not completely switched off. Several factors can impact on the threshold voltage as the threshold voltage itself depends on several working conditions and it is not a fixed parameter, as shown in Equation 3.4:

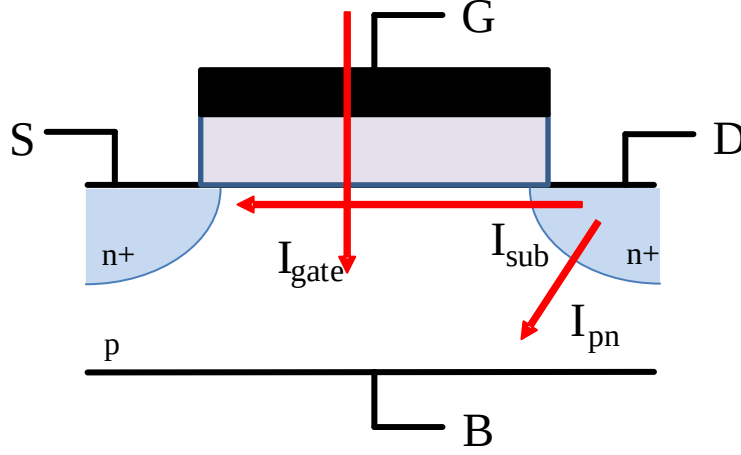


Figure 3.4. NMOS structure with the three main static current sources.

$$V_{TH} = V_{TH0} + \gamma(\sqrt{|2\phi_F| + V_{SB}} + \sqrt{|2\phi_F|}) - \eta V_{DS} \quad (3.4)$$

where V_{TH0} is the zero-bias threshold voltage, γ is the body effect coefficient, V_{SB} is the source-body voltage, and η represents the Drain Induced Barrier Lowering (DIBL) coefficient. In general γ is $0.4V^{0.5}$, $|-2\phi_F|$ is typically $0.6V$, and η is in the range $0.02 - 0.1$. It must be noted that the zero-bias threshold voltage, which can be seen as the typical threshold voltage of the device, depends strongly on the manufacturing process. Modern CMOS design kits provide different devices for different threshold voltage, in order to meet different needs in IC designs, such as performance versus power consumption. The sub-threshold current I_{sub} is influenced by several parameters that alter the device's threshold voltage:

- V_{TH} -Rolloff: when the device is in the short-channel working condition, the threshold voltage is not independent from the channel length anymore, affecting the switching behavior of the transistor.
- DIBL effect: in sub-100nm process, drain and source region are close enough to partially deplete a not negligible section of the active area under the gate also without a biasing voltage. The partially depleted channel region needs a smaller voltage than the nominal V_{TH0} voltage to be inverted. The resulting effect is a lowering of the threshold voltage with shorter channel length.
- Body Bias: the V_{SB} voltage in equation 3.4 directly impacts on the threshold voltage of the MOS transistor. As this voltage increase, the V_{TH} increases as well, reducing the sub-threshold current.
- Temperature: also the working temperature of the device alters the sub-threshold current, by altering the threshold voltage. In the context of deep

sub-micron technologies, the temperature sensitivity of the threshold voltage is in the range of $0.3 - 3.0\text{mV}/^\circ\text{C}$, while the sub-threshold current has exponential behavior with the working temperature, as shown in Figure 3.5.

In up-to-date technologies, the sub-threshold current is the most important leakage source [40]. A comprehensive model of the sub-threshold current is given by:

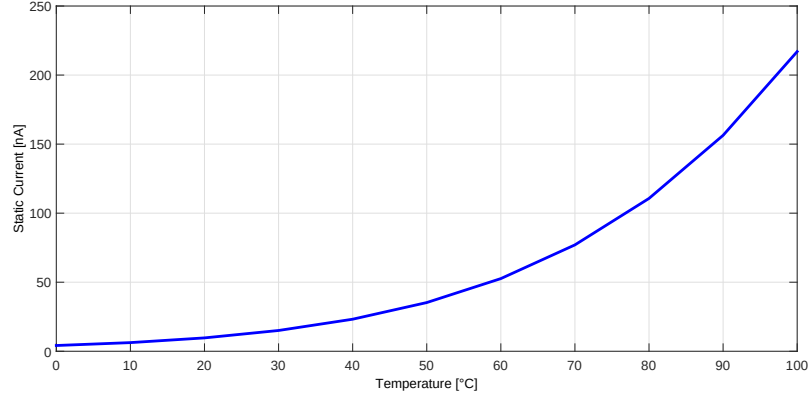


Figure 3.5. Temperature dependency of the sub-threshold current in 4x4bit PRESENT crypto-core.

$$I_{sub} = K \cdot \frac{W}{L} \cdot e^{\frac{V_{GS} - (V_{TH} - \eta V_{DS} + \gamma V_{SB})}{nV_T}} \cdot \left(1 - e^{-\frac{V_{DS}}{V_T}}\right) \quad (3.5)$$

where V_T is the thermal voltage, which is equivalent to 25mV at room temperature (27°C), W and L are respectively the width and the length of the gate. V_T is defined as follows:

$$V_T = \frac{kT}{q} \quad (3.6)$$

where k is the Boltzmann's constant, T is the absolute temperature and q is the electrical charge of the electron.

3.2.2 Reverse-biased pn Junction Leakages

In the MOS structure, the source and the drain wells are strongly doped and they will form pn junctions with the substrate. This two pn junctions are reverse-biased and a small current flows. This mechanism is supported by the high doping profile of the source/drain well, which in turns, supports the tunnel effect of electrons through the pn junctions. The magnitude of the reverse-bias static current depends also on the area of drain/source diffusion. The presence of halo doping to control short channel effects in deep sub-micron devices provides a reverse doped region nearby

the source/drain wells. The combination of a both types of highly doped region supports the Band-To-Band Tunneling (BTBT) [110][37][127], and a high electric field allows charges to flow from the valence band of the p-region to the conduction of the n-region.

3.2.3 Gate Leakage

In nowadays MOS devices, the oxide layer between the gate electrode and the substrate has been intensively engineered. For almost 30 years, the gate oxide has been fabricated using the native oxide of the silicon (SiO_2), which has been used for its high reliability and very good electrical performance. Along with the reduction of the transistors' feature size, the thickness of the oxide has been scaled as well, in order to accommodate the reduced voltage and geometry. The minimum thickness for direct tunneling for the silicon oxide is 2nm. Approaching 2nm of thickness, a not negligible tunneling current flows through the gate also with zero-bias, and the electrical insulation of the gate electrode becomes very poor. Since the mass production of chips with 45nm process, the silicon oxide has been replaced with high-k oxide, which can provide an equivalent thickness below 2nm compared to the silicon one, but with strongly reduced tunneling effect. In this case the probability of direct tunneling is limited, but other phenomena can provide tunneling currents, such as trap-assisted-tunnel. The magnitude of the gate leakage current will increase as the physical thickness of the newer high-k oxides will be reduced. Also the aging of the chip will impact on the gate leakage, due to the generations of new defects in the oxide, which provides a percolation path in the MOS stack.

3.3 Data-Dependency of Static Current

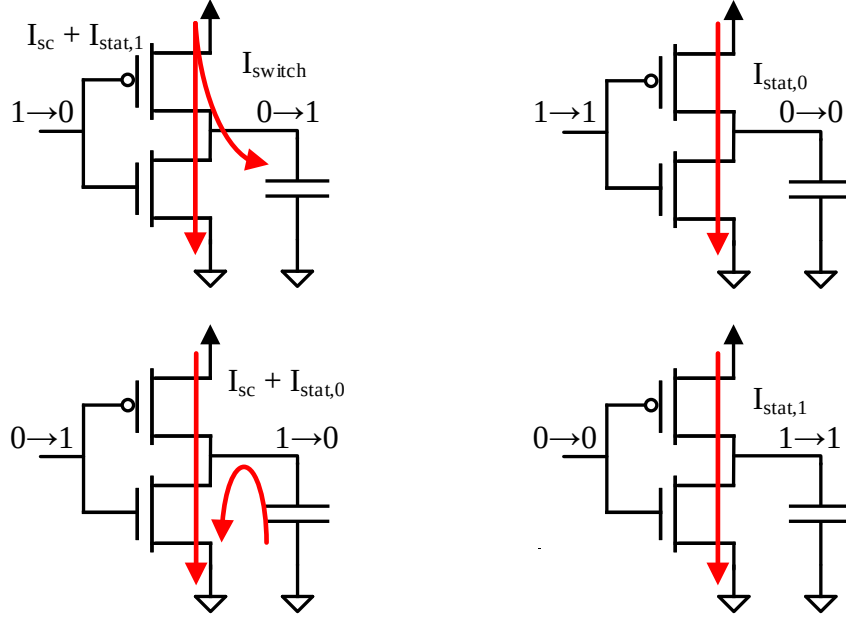
First studies on the data-dependency of the static current of CMOS technologies have been enforced by the needs to reduce the impact of the static power consumption on the performance and on the cost of the device in sub-micron technologies. Since the physical phenomena behind the static current absorption are directly related to the input state of each transistor in a circuit, input vectors of a CMOS circuit are critical in the SCA context.

The simple static power analysis of a CMOS gate is useful to understand how the static current can reveal the input state of the inverter, similarly to the dynamic power consumption exploitation. A simple power evaluation on a CMOS inverter is shown in Figure 3.6, and the power consumption that can be measured at the power supply node is listed in Table 3.1 for each input/output transition.

We must consider that for input transitions $0 \rightarrow 0$ and $1 \rightarrow 1$, no capacitance is charged/discharged because no real transition occurs. The power dissipation in this case is only due to static mechanism. The power consumption $P_{stat,1}$ and $P_{stat,0}$ of the output state 1 and 0 respectively are generically different, due to differences

Table 3.1. Power analysis of a CMOS inverter for each input/output transition.

Input Transition	Output Transition	Power Consumption
$0 \rightarrow 0$	$1 \rightarrow 1$	$P_{stat,1}$
$0 \rightarrow 1$	$1 \rightarrow 0$	$P_{stat,0} + P_{sc}$
$1 \rightarrow 0$	$0 \rightarrow 1$	$P_{stat,1} + P_{sc} + P_{switch}$
$1 \rightarrow 1$	$0 \rightarrow 0$	$P_{stat,0}$

**Figure 3.6.** Power analysis of a CMOS inverter.

in carrier mobility in the PMOS compared to NMOS. In fact, it is meaningfully to understand which transistors are off, in order to better understand how much the static current is.

$$P_{stat,0} \neq P_{stat,1} \quad (3.7)$$

Since these two consumptions are different, we can recover the state of the CMOS inverter by measuring also the static current. This property is general for CMOS gates, as we have said before for the dynamic power consumption. Also experimental results have confirmed this kind of results.

The input state has a direct impact on the static power consumption. This data-dependency of static current has been analyzed on main standard cells implemented in a 40nm CMOS STMicroelectronic process. *Spice* level simulations have been

Table 3.2. Variability of the current of a 40nm inverter gate.

IN	Current [nA]				
	$T = 0^\circ C$	$T = 25^\circ C$	$T = 50^\circ C$	$T = 75^\circ C$	$T = 100^\circ C$
0	0.186	0.384	0.704	1.200	1.913
1	0.101	0.267	0.611	1.250	2.330
CV [%]	41.88	25.42	10.00	3.12	13.90

Table 3.3. Variability of the current of a 40nm NAND gate.

IN		Current [nA]				
		$T = 0^\circ C$	$T = 25^\circ C$	$T = 50^\circ C$	$T = 75^\circ C$	$T = 100^\circ C$
0	0	0.011	0.033	0.083	0.165	0.290
0	1	0.174	0.336	0.602	1.013	1.618
1	0	0.052	0.191	0.481	0.917	1.548
1	1	0.203	0.534	1.223	2.502	4.669
CV[%]		84.49	77.97	79.10	85.12	91.64

Table 3.4. Variability of the current of a 40nm NOR gate.

IN		Current [nA]				
		$T = 0^\circ C$	$T = 25^\circ C$	$T = 50^\circ C$	$T = 75^\circ C$	$T = 100^\circ C$
0	0	0.374	0.768	1.410	2.394	3.826
0	1	0.062	0.239	0.620	1.314	2.485
1	0	0.090	0.230	0.525	1.083	2.043
1	1	0.004	0.020	0.056	0.132	0.277
CV[%]		84.49	98.45	76.03	86.07	75.48

carried out using accurate BSIM4 models of MOS transistors in Cadence Virtuoso, using Standard Voltage Threshold Low Power (SVTLP) devices. To assess the variation of the static current due to data-dependency, the Coefficient of Variation (CV) [3] [2] is used and it is defined as follows:

$$CV = \frac{\sigma_{static}}{\mu_{static}} = \frac{\sqrt{\frac{1}{n} \sum_{j=1}^n (I_j - \mu_{static})^2}}{\frac{1}{n} \sum_{j=1}^n I_j} \quad (3.8)$$

where σ_{static} is the standard deviation and μ_{static} is the mean value of the static current sample I_j , with $j=1,2,\dots,n$. Larger is the CV, larger will be the dependency of the static current from the input vectors. The CV is widely used in hardware security literature, and, in this context, is useful to give a measure of the potential vulnerability of a circuit to a side-channel attack.

Table 3.2-3.6 show the static current with all possible input vectors, and variability

Table 3.5. Variability of the current of a 40nm XOR gate.

		Current [nA]				
IN		$T = 0^{\circ}C$	$T = 25^{\circ}C$	$T = 50^{\circ}C$	$T = 75^{\circ}C$	$T = 100^{\circ}C$
0	0	0.632	1.777	3.960	7.705	13.762
0	1	0.501	1.587	3.702	7.170	12.588
1	0	0.649	1.883	3.960	7.280	12.350
1	1	0.542	1.690	3.906	7.847	14.349
CV[%]		12.23	7.26	3.16	4.35	7.18

Table 3.6. Variability of the current of a 40nm D flip-flop.

D	CK	D_{int}	Current[nA]@25
0	1	1	1.080
0	1	0	1.010
0	0	0	1.163
0	0	1	1.080
1	0	0	0.969
1	0	1	1.265
CV[%]			9.76

Table 3.7. Comparison of the CV of a NAND gate using 90nm, 65nm, 40nm and 28nm (with SVTLP option).

Process	CV@ $T = 0$	CV@ $T = 25$	CV@ $T = 50$
90nm	70%	63%	62%
65nm	58%	40%	40%
40nm	84%	78%	79%
28nm	158%	151%	145%

due to data-dependency for minimum driving gates and D flip-flop from the standard-cell library with SVTLP option. As further analysis, a comparison of the CV of the NAND gate with different technologies with different working temperature is shown in Table 3.7.

It has to be noted that the CV of the static current increases with the scaling factor [15]. In the 28nm process, the CV is very high, and even greater than 100%. As we will see in the next section, high values of CV with basic gates is a critical sign of potential vulnerabilities in the side-channel attacks context. Since the design of electronic devices is moving toward new technologies, the data-dependency of the static consumption is not anymore a secondary problem in security applications.

3.4 AESP in Cryptography

The strong relation between static current magnitude and input vectors for CMOS gates is the physical basis of the Attacks Exploiting Static Power (AESP) [15]. This property can be used to exploit secret information from hardware implementation of cryptographic algorithms. Real devices are frequently designed using m -bit-sliced circuits, in which the complete architecture is composed by a certain number of replicas of the same atomic structure. In bit-slice based circuits, the overall static current is equal to the sum of the static currents of the m -bit slices, each of which can be reasonably equal to the high (or low) level of static current I_H (or I_L) when the corresponding input bit is '1' (or '0') [6] [64]. Considering that the number of '1' of the input vector of a slice is the Hamming Weight (HW) w of the input vector, the overall static current consumption of a m -bit slice can be expressed as:

$$I_{leak} = w \cdot I_H + (m - w) \cdot I_L = w \cdot (I_H - I_L) + m \cdot I_L \quad (3.9)$$

This model expresses the linear dependency of the static current of a slice from the Hamming Weight of its input vector. There is a strong assumption behind this model, which holds in most cases. In fact, it is assumed that each bit in a m -bit slice implementation contributes equally to the overall power consumption.

In [64],[1] and [5], authors pointed out that a strong relation exists between processed data and static consumption. Abdollahi *et al.* benefits from the direct relation between input vectors and leakage current to minimize the static power consumption, through the adoption of a *Leakage Computing Network* to build a power model of the static consumption. After that, a minimum leakage input vector is identified through a SAT solver finding the input pattern that minimize the static power consumption. In [5], the static consumption of an off-the-shelf 8-bit CMOS register (ON Semiconductor MC74ACT273) has been measured varying the stored data. It has been demonstrated that the static consumption is directly linear with the Hamming Weight of the stored data, and this behavior has been observed on five different chips, obtaining the same results.

The critical role played by the static power consumption in PAA has now becoming a primary concern. Since the magnitude of static power consumption has growth of more than one order of magnitude in ten years, the possibility to recover secret information using leakage currents as side-channel is the new frontier of power analysis attacks. In [5], a first attempt to use the static power consumption to recover the secret key of a hardware implementation of a cryptographic algorithm is presented. In this work, a 65nm CMOS implementation of a 4-bit slice of the SERPENT block cipher's data-path has been attacked using static current as side-channel. Alioto *et al.* demonstrated the possibility to successfully attack the implementation adopting a novel and well-defined procedure called *Leakage Power Analysis* (LPA). This formulation has been extended in [15] and named *Attack Exploiting Static Power* (AESP). Since the experimental activity on the 8-bit CMOS register reported in [5] highlighted the linear relationship between the Hamming Weight of the stored data

and the static current consumption, authors have demonstrated as the Hamming Weight is a suitable and sounding power model for the static power consumption. The new and well-defined procedure introduced in [5] and extended in [15] is based on the classic Correlation Power Analysis, introduced in [32], and they share the same statistical distinguisher: the Pearson's correlation coefficient.

A common approach to perform a power analysis attack is to use multiple samples collected by a set of power traces and compare them with a predicted power model, which has to be sounding accordingly to the information leakage mechanism of the cryptographic device. This class of attack are called multivariate attacks. Accordingly to [93], each one of the T samples of a power measurement of the attacked device is given by the sum of a data-dependent component and uncorrelated noise component:

$$P_{leak}[j] = P_{data}[j] + P_{noise}[j] \quad (3.10)$$

with $j = 1, 2, \dots, T$. The data-dependent component is what the attacker wants to exploit in order to recover the secret information processed in the device. Under the assumption that the noise component is additive white Gaussian noise [93] [125], which takes into account both electronic and on-chip noise, several measurements need to be collected in order to extract only the data-dependent component.

$$P_{noise}[j] \sim N(k, 0, \sigma_{noise}^2) \quad (3.11)$$

In equation 3.11, the sample mean of the noisy component is zero, while the variance is σ_{noise}^2 . In the case of static current, the attack is intrinsically univariate, because one sample for each measurement is used to perform the attack. So, in the case of static current exploitation, we have only one sample which is relevant for the attack, and we consider:

$$T = 1 \quad (3.12)$$

$$P_{leak}[j^*] = P_{data}[j^*] + P_{noise}[j^*] \quad (3.13)$$

The procedure proposed in [5] [6] to exploit information leakage from static power consumption, can be described as follows. In the first step of the LPA attack, the adversary chooses an internal m -bit data word X , processed inside the device under attack, during the execution of the cryptographic algorithm. In general, the intermediate signal X depends on the input vector I and the secret key K , by the function f , which is given by the cryptographic algorithm:

$$X = f(I, K_{corr}) \quad (3.14)$$

After that, the adversary stimulates the device under attack using l input vectors I_i , with $i = 1, 2, \dots, l$, measuring the corresponding static current drawn by the device $I_{leak,i}$, capturing the consumption at the point in time in which target word X is evaluated. This operation assumes that the adversary has the knowledge of which is the point in time, or, in other words, the clock cycle, in which the intermediate signal X is evaluated in the device. At the end of the measurement campaign, the adversary has a set of l measurements $I_{leak,i}$. At this point, the adversary has to estimate the physical value of X for each input vector I_i . Since the secret key K used within the chip is unknown to the adversary, the estimation of the physical value of X has to be extended to each possible key K_k , with $k = 1, 2, \dots, 2^m$ according to equation 3.15:

$$X_{i,k} = f(I_i, K_k) \quad (3.15)$$

The result of this operation is the 2-D matrix $X_{i,k}$. In order to exploit the information leaked by the device from the static currents, the adversary needs to compute the hypothetical values of the power consumption using the physical estimation of X . Since the static current provides information about the Hamming Weight of the m -bit X , the adversary builds another 2-D matrix $H_{i,k}$ with estimated static current of each element of $X_{i,k}$. The Hamming Weight of each element of $X_{i,k}$ is computed, according to equation 3.16:

$$H_{i,k} = HW(X_{i,j}) = HW(f(I_i, K_k)) \quad (3.16)$$

After the estimation of the hypothetical power consumption, the matrix of hypothetical static power consumption $H_{i,k}$ is compared with the measurement set $I_{leak,i}$, accordingly to the index of the input vector i . When the key guess K_k is correct ($K_k = K_{corr}$), the estimated and the actual static power consumption are maximally correlated, while for wrong key guess, the correlation is very poor. The linear correlation is estimated by Pearson's correlation coefficient as in a CPA attack:

$$\rho_k = \frac{\sum_{i=1}^l (H_{i,k} - \overline{H_i}) \cdot (I_{leak,i} - \overline{I_{leak}})}{\sqrt{\sum_{i=1}^l (H_{i,k} - \overline{H_i})^2 \cdot (I_{leak,i} - \overline{I_{leak}})^2}} \quad (3.17)$$

As result, the adversary will compute m values of Pearson's correlation coefficient, one for each possible key guess. Hence, he/she will choose the key K_{k^*} guess which maximizes the correlation coefficient among all possible keys:

$$\rho_{k^*} = \max_k \rho_k \longrightarrow \widehat{K_{corr}} = K_{k^*} \quad (3.18)$$

A graphical resume of the Attack Exploiting Static Power presented in this section is shown in Figure 3.7.

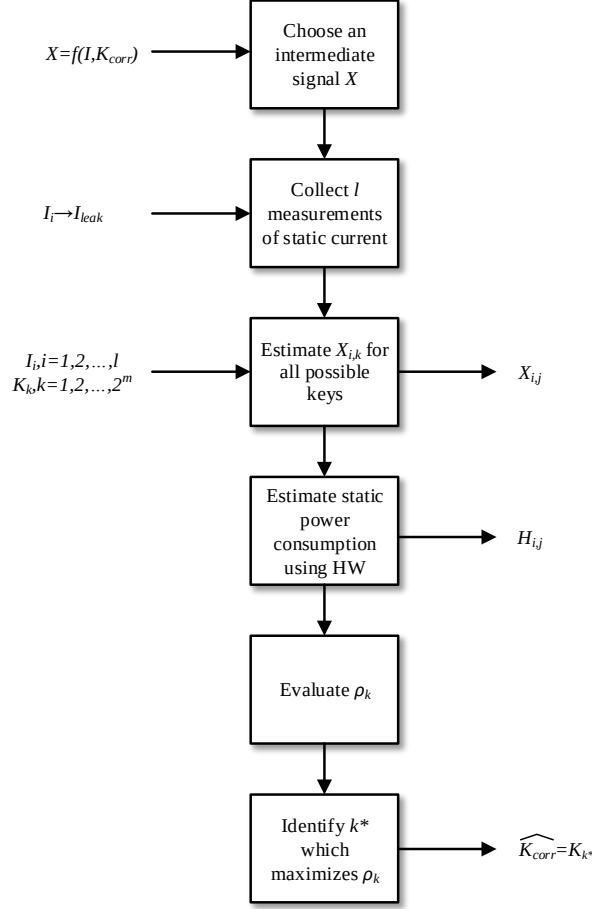


Figure 3.7. Attack Exploiting Static Power procedure.

3.5 Vulnerability of DPA-countermeasured Logic Styles to AESP

In literature, several countermeasures have been proposed to thwart power analysis attacks exploiting dynamic power consumption. Most common ones use the gate-level and logic-level as abstraction level to make the consumption poorly related with the processed data. In gate-level and logic-level approach, the main technique to counteract CPA and DPA attacks is the hiding technique. Counteracting at logic-level using hiding techniques means to minimize the data-dependent component of the dynamic power consumption. In CMOS circuits, the dynamic power consumption of a gate can be expressed with Equation 3.1. In order to minimize the possibility to recover the state of the input/output of a gate by monitoring its dynamic power consumption, the designer has to make the consumption independent from the input vector. Since the gate's dynamic consumption depends on its switching activity factor α , which represents the probability of its output to make a transition within

a clock cycle, the designer wants to ensure that each gate of the secure path has to perform a transition of its output signal for each clock cycle. In this way, the switching activity factor α will typically increase towards to unity.

$$\alpha \rightarrow 1 \quad (3.19)$$

In order to make this condition to be fulfilled, the common approach is to use a *Dual-Rail Pre-charge* signaling and logic styles. In Dual-Rail Pre-charge Logics (DPLs), each gate is duplicated in order to have complementary input and complementary output signals. To achieve this kind of porting, a DPL gate has to provide two complementary functions F and $\bar{F}$, as shown in Figure 3.8 and Equation 3.20.

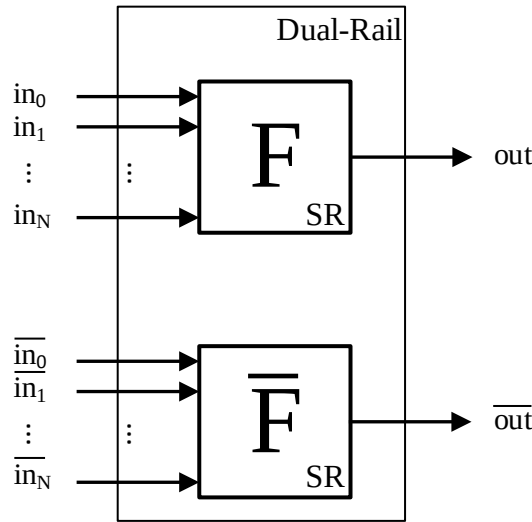


Figure 3.8. Example of dual-rail gate using single-rail gates.

$$\begin{aligned} out &= F(in_0, in_1, \dots, in_N) \\ \bar{out} &= \bar{F}(\bar{in}_0, \bar{in}_1, \dots, \bar{in}_N) \end{aligned} \quad (3.20)$$

To ensure a constant consumption for each clock cycle, also pre-charged circuitry is used along dual-rail approach. In a pre-charged circuit, the clock cycle is divided in two phases. During the *pre-charge phase*, each signal of the net has to be tied to the pre-charge value, which can be '0' or '1'. At the end of the pre-charge phase, the value of each signal is evaluated and the output result is generated. This step is called *evaluation phase*. In many logic styles, the sequence pre-charge $\rightarrow$ evaluation phase is handled directly by the clock signal, or, in other cases, one or more explicit signals are used to maintain the synchronization. In security applications, the combination of both dual-rail and pre-charged logics is used to achieve the condition shown in

equation 3.19. Since each complementary signals couple assumes the value (0,1) or (1,0) only during the evaluation phase, and during the pre-charge (post-evaluation) phase they will assume both the pre-charge (post-evaluation) value (0,0) (or (1,1)), the power consumption is theoretically data-independent. The signaling described above and shown in figure 3.9 is also called Return-to-Zero (RTZ) protocol in the context of cryptography [93]. As we will see in the next chapter, this condition will not hold in many cases due to novel issues with modern CMOS technologies.

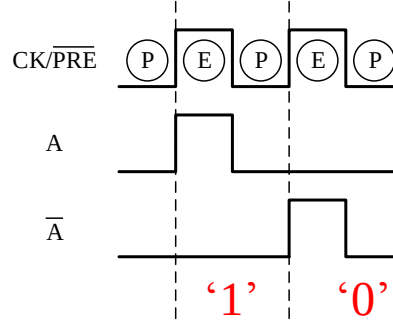


Figure 3.9. Dual-rail pre-charge encoding (RTZ protocol) of the logic value '1' and '0', assuming '0' as pre-charge value. The clock signal $CK/\overline{PRE}$ is used as pre-charge signal. The pre-charge phase occurs when the signal $CK/\overline{PRE} = 0$, while the evaluation phase for $CK/\overline{PRE} = 1$.

From a security point of view, the presence of a countermeasure to thwart attacks exploiting dynamic power does not make the implementation secured from AESP. The investigation on the vulnerability of commonly adopted countermeasures, such as DPLs, is critical since the relevance of the information that can be recovered from hardware implementation of cryptographic algorithm through static power.

3.5.1 DPL logic styles

In the context of counteracting power analysis attacks several DPL logic styles have been proposed, both standard-cell based and full custom. In this chapter we will introduce three mainly used logic styles to counteract CPA/DPA attacks.

The *Wave Dynamic Differential Logic* (WDDL) [147] is a dynamic and differential logic style based on the interconnection of standard CMOS gates. The idea behind WDDL logic styles is to balance the power consumption per clock cycle for any input combination. Each combinational gate is replaced with its dual rail version. A CMOS-to-WDDL converter is needed to convert the single rail CMOS signal to the WDDL domain, which is RTZ. The converter, depicted in 3.10(b), has to generate also the pre-charge value ('0' in this case) for both complementary signals. The pre-charge value is propagated through the net, in order to pre-charge each node of WDDL gate. The AND/NAND gate is shown in figure 3.10(a). As we can see, both the function and its complementary counterpart are implemented with standard

CMOS gates to balance the power consumption, ensuring one output transition $0 \rightarrow 1$ per clock cycle for each gate. The sequential element is made with standard CMOS D flip-flop, and it is depicted in Figure 3.10(c). At the rising edge of the clock signal, the differential input data is sampled during its evaluation phase. Two AND gates are used to restore the pre-charge wave during the '0' phase of the clock signal. It has to be noted that the WDDL logic can be implemented in FPGA, because it is based on standard CMOS logic gates, and thus, no full custom design is required.

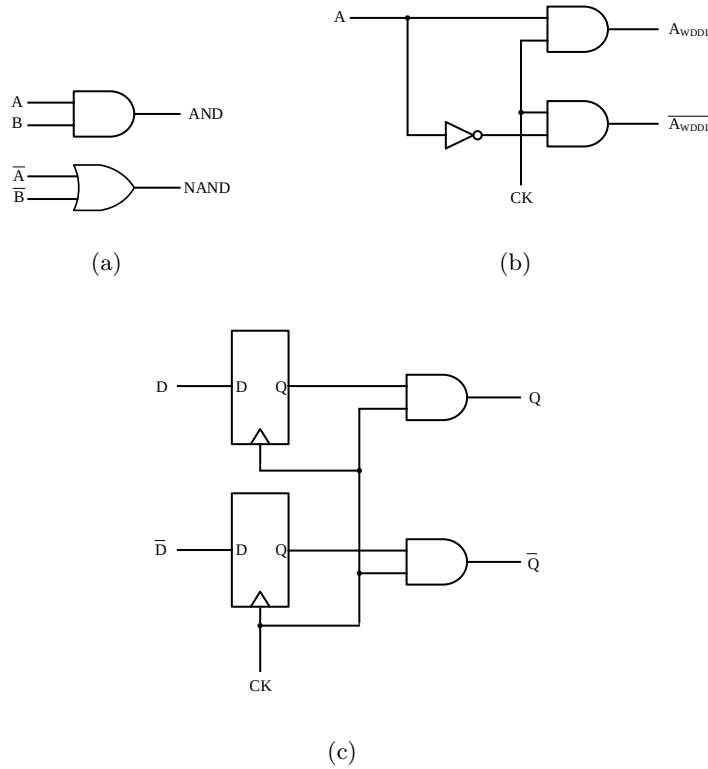


Figure 3.10. WDDL building blocks. In (a), the AND/NAND gate in WDDL logic is shown. In (b), the CMOS-to-WDDL converter is shown, using a pre-charge value of '0'. In (c) the WDDL 1-bit flip-flop is shown. The low-level of the clock signal is used to generate the pre-charge wave, avoiding the use of an explicit signal.

The Masked Dual-rail Pre-charge Logic (MDPL) [117] is another standard-cell based on the DPL principle, such as the WDDL. The main difference is that also a masking scheme is used at logic-level to increase the security level. The DPL approach allows to balance the switching activity, fulfilling equation 3.19, but in addition, the MDPL aims to randomize the power consumption using an additional differential input M , which is fed with a random mask value. Assuming that D is the real data, each MDPL gate acts as XORing gate, where the real data is masked with M :

$$D_m = D \oplus M \quad (3.21)$$

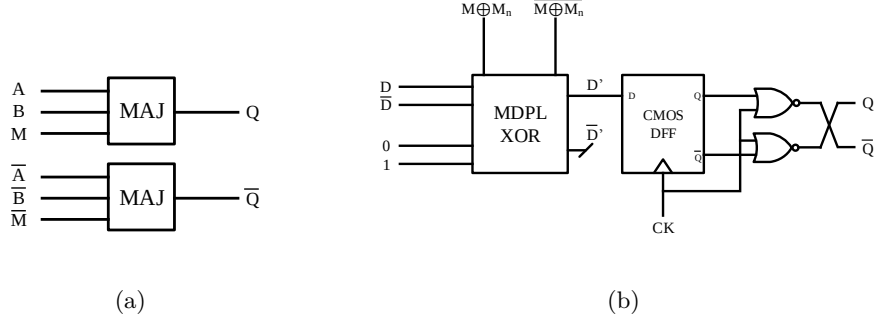


Figure 3.11. MDPL building blocks. In (a), the AND/NAND gate in MDPL logic is shown. In (b) the MDPL 1-bit flip-flop is shown.

The MDPL AND/NAND gate and sequential element are shown in Figure 3.11. The MDPL relaxes some of the implementation constraints of the WDDL, but requires the implementation of a PRNG or TRNG to generate the mask.

The Sense Amplifier-Based Logic (SABL), introduced by Tiri *et al.* in [144], is a full custom dual-rail pre-charge logic family specifically designed to achieve the condition in Equation 3.19. In order to avoid information leakage due to Time-Of-Arrival (TOA), gates are designed to evaluate the output value only after each of the inputs have been set to the respective complementary value. Since each gate is connected to the clock signal, every gate pre-charges simultaneously. The SABL logic styles require a very high number of MOS per gate, and it is considered as the state-of-the-art of logic-level countermeasure. Compared to WDDL and MDPL, SABL logic style cannot be implemented on a FPGA, and thus requires a specific design and custom libraries, as can be seen from Figure 3.12. It is considered one of the best gate-level countermeasure against CPA/DPA, due to its capability to thwart attacks exploiting dynamic power.

The aforementioned logic styles have been designed to counteract attacks exploiting dynamic power, but, since the emerging issues in security applications due to the strong impact of static power consumption, a vulnerability analysis has to be carried out. Moreover, logic styles, such as WDDL and MDPL, very common also in FPGA and microcontroller applications, are based on the interconnection of CMOS gates, and they have to be carefully analyzed, in order to reveal if there is information leakage through the static current absorption.

3.5.2 Evaluation of vulnerability to AESP on the SERPENT block cipher

The analysis of vulnerability to AESP of the aforementioned logic styles has been performed on simulated power traces, carried out using Cadence Virtuoso with 40nm

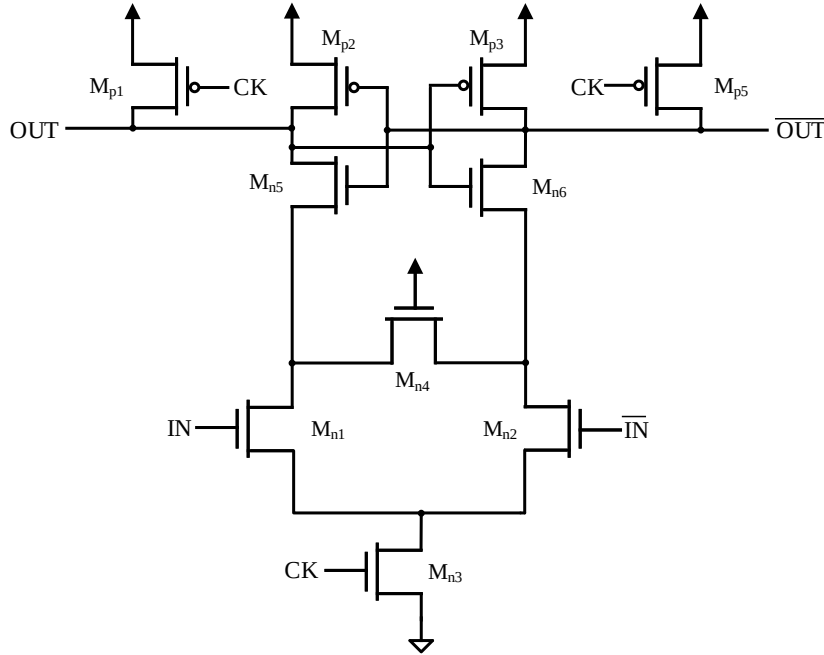


Figure 3.12. Implementation of the buffer/inverter with SABL logic style.

CMOS process from STMicroelectronics. The standard CMOS has been used as the reference logic style for comparisons. A 4-bit data-path of the first round of the SERPENT block cipher implementation has been used as case to study (shown in Figure 3.13), analyze and compare vulnerabilities of the aforementioned DPL logic styles to AESP. The crypto-core is composed by an input layer of flip-flops, to store the input plaintext and the 4-bit key, a XOR layer, implementing a slice of the *AddRoundKey* operation, and a 4x4 bit SERPENT *S0* S-BOX. It is worth noting that the S-BOX used in these implementations has been designed with the smallest number of 2-inputs combinational logic gates known from literature [124]. The output register samples the output word of the S-BOX, and provides the output ciphertext. Testbenches for DPL logic styles require CMOS-to-DPL and DPL-to-CMOS converters, which are not needed in the case of standard CMOS implementation.

The power supply is kept constant at 1V, while the clock frequency has been set to 10MHz, in accordance to typical working frequency of most cryptographic devices [51][118][26][20]. The current samples are collected on the main V_{DD} of the design, assuming the worst-case model for the adversary. In fact, in order to collect only static currents for our purpose, it has to be ensured that only static phenomena are captured. In a real attack scenario, a malicious attacker may need to force the device at the steady state condition to measure the static current, after the target word is processed by the device implementation. To perform the attack and making the device to be in a steady state before the processing, the clock has been switched

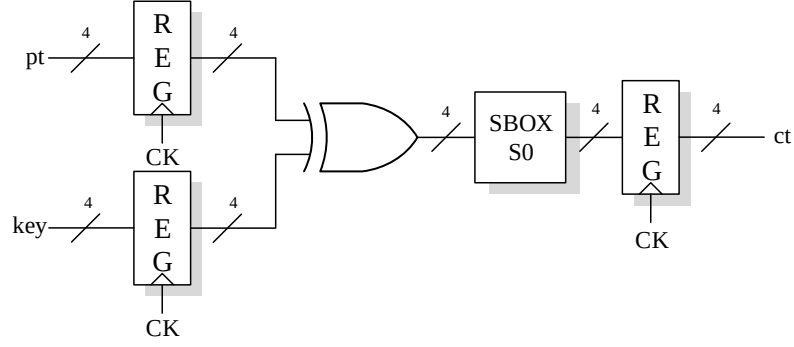


Figure 3.13. 4-bit data-path of the SERPENT block cipher used as cased study to analyze and compare the vulnerability of different DPL logic styles against AESP.

off after the second sampling edge following the start of the encryption operation, as depicted in Figure 3.14. As target intermediate value, the output word ct of the S-BOX has been chosen, which depends on the input plaintext pt and the secret key key , accordingly to Equation 3.22:

$$ct = SBOX(pt \oplus key) \quad (3.22)$$

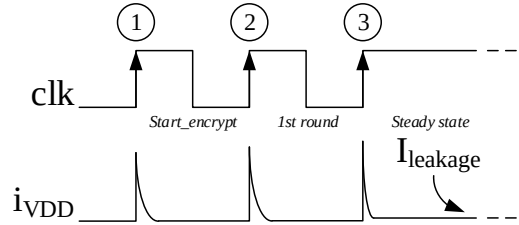


Figure 3.14. Time diagram of the clock signal to collect only static current samples.

The first analysis and comparison involves the possibility to use different devices with different threshold voltage options in the design kit:

- Low Voltage Threshold (LVT);
- Standard Voltage Threshold (SVT);
- High Voltage Threshold (HVT).

In non-cryptographic design, the multi- V_{TH} approach is widely used to trade-off between performance and power consumption, using LVT devices for high performance paths and HVT on non critical ones [40]. In the context of cryptographic

design, the exploitation of different threshold voltage options and sub-threshold working condition have been used to develop a countermeasure against dynamic power attacks [67], neglecting the vulnerabilities due to static current information leakage. The CMOS implementation has been designed with the three different options available and they have been compared to better understand the impact of the V_{TH} options on the vulnerability against AESP. The working temperature has been set to 50°C for each implementation. Simulating noise-free AESP attacks allow to reveal the secret key in all cases, as shown in Figure 3.15. The correct key, taht has been set to $(7)_2$, has been correctly recovered, demonstrating that the reduction of the correlation coefficient adopting the HVT option is negligible, and no real improvement in thwarting AESP can be gained if higher threshold devices are chosen. In this scenario, the static current exploitation allows to recover the secret information neglecting the devices' threshold voltage. It has to be noted that the SVT option offers the best correlation coefficient among the others.

The CMOS implementation has been compared with WDDL, MDPL and SABL implementation of the SERPENT crypto-core, using actual security metrics. Also an information theoretic approach has been used, which have been demonstrated to be a "fair" method to assess the security level of cryptographic processor without referencing to a specific power model. In this experiment, the key used by the crypto-cores has been set to $(5)_2$, and again, the analysis has been carried out firstly noise-free, to assess the worst-case condition for the implementation (no limits in storage capability and for the duration of the experiment). In all cases, the secret key has been correctly recovered. It has to be noticed from Figure 3.16, that the correlation coefficient of the correct key of the MDPL and WDDL is higher than CMOS. The SABL implementation shows a lower correlation coefficient compared to the CMOS reference. This results is double-fold. Firstly, the univariate Gaussian model using static power consumption presented in this chapter is effective in recovering secret information also if the target implementation is conceived to thwart attacks exploiting dynamic power consumption. Secondly, since MDPL and WDDL show higher correlation coefficient compared to CMOS, we could conclude that the interconnection of CMOS gates to make the dynamic consumption independent from the processed data can leak through static power even more information than a standard CMOS implementation. In fact, the only DPL logic style which does not show this behavior among the case study is the SABL implementation, which is intended to be for ASIC applications, since it does not use interconnection of CMOS standard-cells.

Furthermore, the analysis has been conducted also with the information theoretic approach presented in 2, which can quantify precisely the amount of information leaked by the static current without using a specific power model. In this case the Mutual Information has been used to make a comparison of CMOS with DPL styles. As it is widely accepted in the side-channel attacks literature [137], a univariate Gaussian model has been adopted to quantify the information leaked through the static power consumption. A plot of the mutual information versus the noise standard deviation is shown in Figure 3.17. Comparing curves for different logic styles, the SABL has a sharper reduction, and the information leaked through CMOS, WDDL

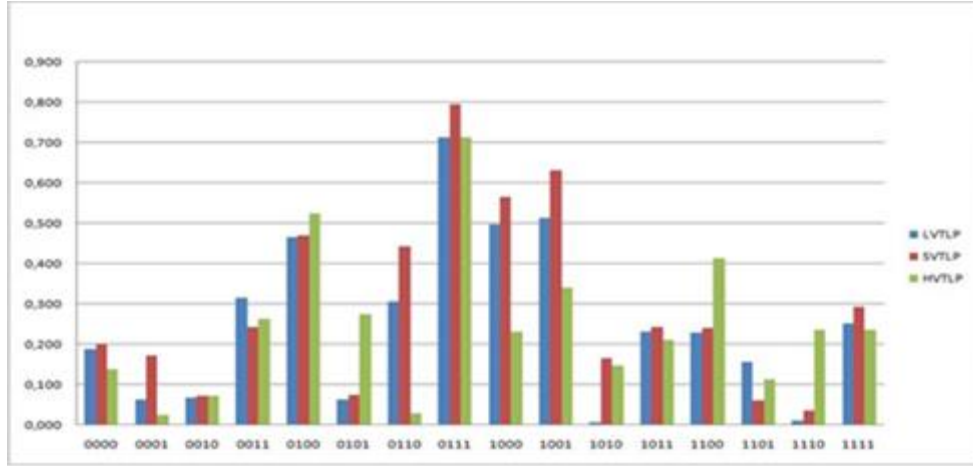


Figure 3.15. AESP using correlation coefficient against the 4-bit SERPENT crypto-core with LVT (blue), SVT(red) and HVT(green) devices. The key $(7)_2$ has been set on this scenario.

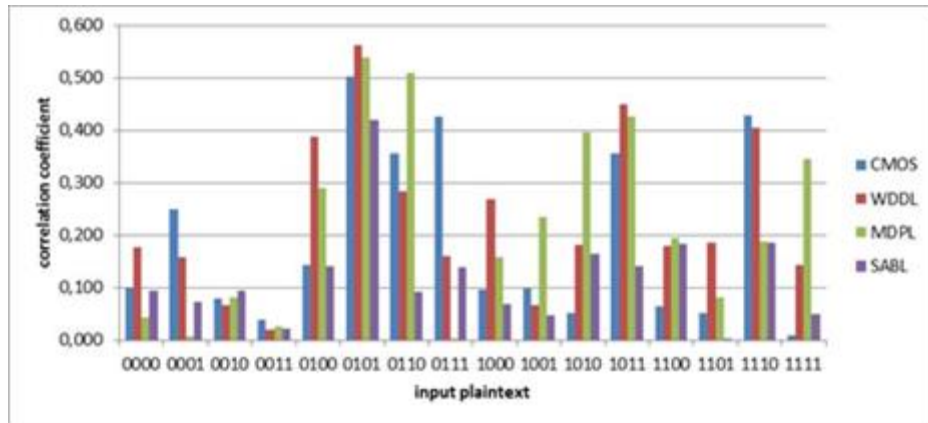


Figure 3.16. AESP using correlation coefficient against 40nm CMOS and DPLs implementation of the 4-bit SERPENT crypto-core.

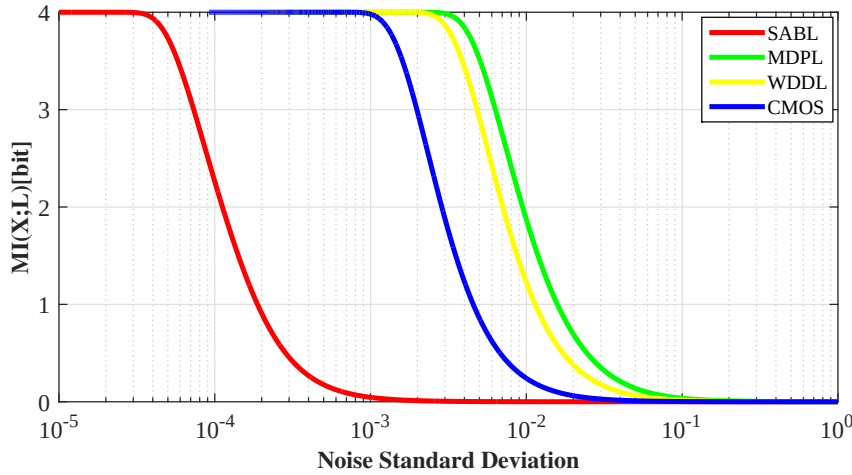


Figure 3.17. Mutual information plots versus the standard deviation of the noise with various DPL logic styles. The CMOS implementation has been used as reference.

and MDPL implementations can be exploiting also in the presence of higher level of noise. It is worth noting that the CMOS-based DPL logic styles (MDPL and WDDL) can leak more information than standard CMOS, confirming the results obtained with the previous AESP analysis.

The vulnerability of DPLs to AESP has been tested and verified for standard-cell based and full custom logic. Since actual and information theoretic security metrics have confirmed that using RTZ protocol with logic styles designed by interconnection of CMOS standard-cells is able to counteract dynamic power exploitation but they do not give increasing level of security if static power consumption is used as side-channel. Moreover, MDPL and WDDL provide a better exploitation than CMOS reference, which is a critical standpoint in hardware security, since these two logic style are very common in cryptographic hardware (also for reconfigurable devices, such as FPGAs).

Table 3.8. Comparing of noise performance regarding 3bit of mutual information values for SABL, MDPL, WDDL and CMOS. The CMOS implementation is used as reference.

Implementation	$\sigma_{noise}@3bit$	Ratio
SABL	$7.4 \cdot 10^{-5}$	$x0,037$
MDPL	$7 \cdot 10^{-3}$	$x3,5$
WDDL	$5.8 \cdot 10^{-3}$	$x2,9$
CMOS	$2 \cdot 10^{-3}$	$x1$

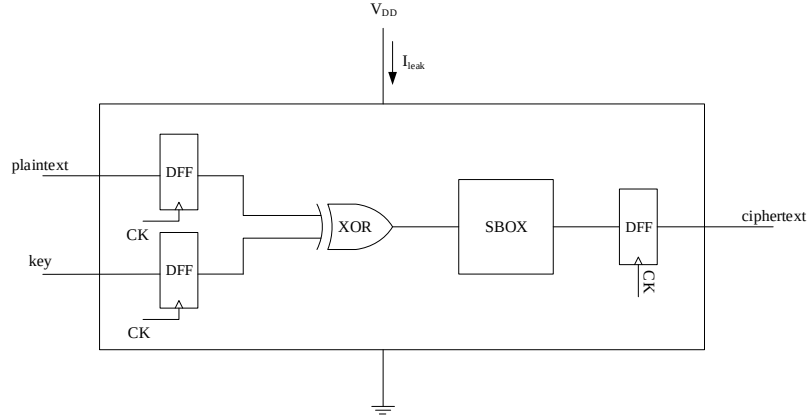


Figure 3.18. 4-bit data-path of the PRESENT block cipher.

3.5.3 Evaluation of vulnerability to AESP on the PRESENT block cipher

To better extend this vulnerability analysis, also the PRESENT-80 block cipher has been used as case study, making a comparison between CMOS and WDDL. This comparison is very significant because WDDL is very common in many secure applications, because it provides a good level of security, without the huge area footprint and power overhead that a MDPL implementation can require. The investigation of the vulnerability of the WDDL to AESP[19][15] has been carried out on a 4-bit data-path of the PRESENT-80, similarly to the 4-bit SERPENT-based crypto-core, and on the iterative-loop full implementation of the algorithm. The usage of a complete implementation allows to take into account the electronic noise due to other non-targeted blocks in the cipher. In general, the adversary measures the overall static power consumption of the core, which has a direct impact on the SNR. The motivation behind this further analysis is to investigate the vulnerability in a more realistic scenario.

Both the 4-bit and full-implementation of the PRESENT-80 have been implemented using the aforementioned 40nm CMOS process provided by STMicroelectronics, using Cadence Virtuoso as simulation environment. The voltage and the power supply have been set similarly to the SERPENT case study. A block diagram of the 4-bit PRESENT crypto-core is depicted in Figure 3.18. The iterative-loop implementation of the PRESENT-80 block cipher is depicted in Figure 3.19. It is composed by three main layers:

- *AddRoundKey*: the 64 most significant bits of the round key are XORed with the 64-bit round ciphertext.
- *SubsLayer*: 16 parallel 4x4 bit PRESENT S-BOXes perform non-linear function, providing *diffusion*.

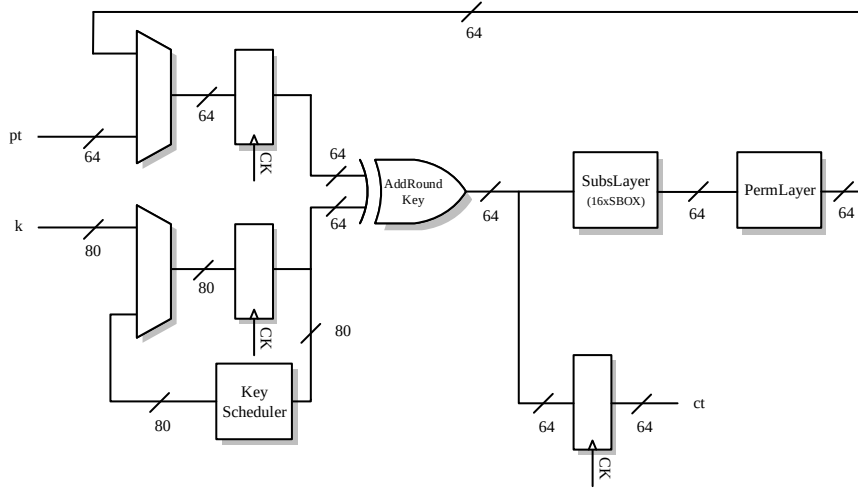


Figure 3.19. Data-path of the full implementation of the PRESENT-80 block cipher with iterative-loop structure.

Table 3.9. Area and static power consumption details of CMOS and WDDL implementation of the PRESENT-80 cryptographic processor.

Implementation	Number of devices	Average Static Current	Standard Deviation
CMOS	12094	$4.89\mu A$	$3.20nA$
WDDL	36548	$12.89\mu A$	$11.22nA$

- *PermLayer*: a linear permutation is performed after the non-linear operation, and the round ciphertext is stored in the status register. This layer has no combinational logic, and thus it has no actual consumption because it has been implemented using a proper wiring of the output of the *SubsLayer* to the input of the input multiplexer.

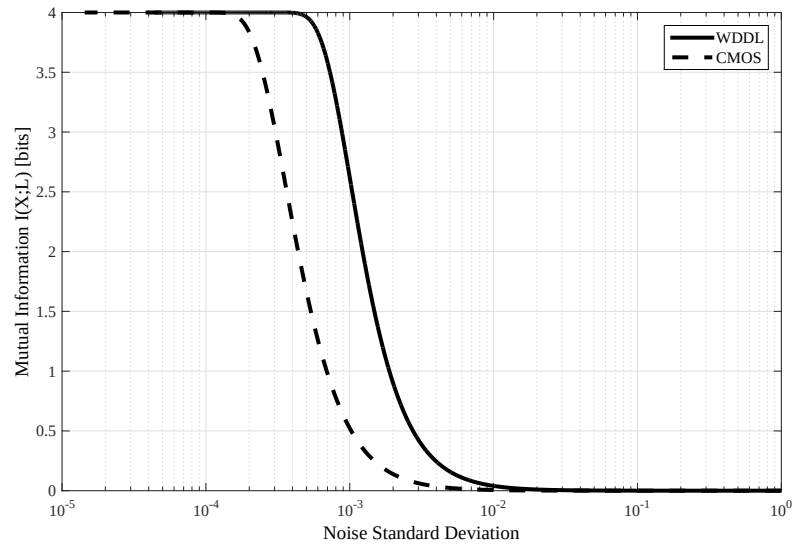
The results of the AESP against the 4-bit PRESENT crypto-core (noise-free) running the processor with all possible keys are reported in Table 3.10. It has to be noticed that both CMOS and WDDL are vulnerable to AESP also with a different algorithm. The difference in correlation coefficient of the correct key and the maximum correlation coefficient of the best ranked wrong key is ≈ 0.10 in all cases for the WDDL, which is an order of magnitude higher than the CMOS counterpart. This result is in line with the outcome of the previous analysis, remarking the higher vulnerability of the WDDL to AESP compared to CMOS.

A plot of the mutual information versus the noise standard deviation is reported in Figure 3.20 for both implementation of the PRESENT crypto-core, using $(10)_2$. Also in this case, the WDDL implementation exhibits more information than CMOS one, regarding the same level of noise, since the WDDL's curve is shifted to the left.

Regarding the complete implementation of the PRESENT-80, the AESP has

Table 3.10. Correlation coefficient on CMOS and WDDL implementation of the 4-bit PRESENT crypto-core at 100°C.

Key	CMOS			WDDL		
	Max ρ	Max ρ	SVI	Max ρ	Max ρ	SVI
	correct key	wrong key		correct key	wrong key	
0000	0.6048	0.5821	0.0227	0.6415	0.5496	0.0919
0001	0.5851	0.5621	0.0230	0.6642	0.5519	0.1123
0010	0.5501	0.5415	0.0086	0.6450	0.5537	0.0913
0011	0.5337	0.5250	0.0087	0.6476	0.5560	0.0916
0100	0.5858	0.5657	0.0201	0.6529	0.5551	0.0978
0101	0.5707	0.5314	0.0393	0.6550	0.5578	0.0972
0110	0.5415	0.5340	0.0075	0.6561	0.5591	0.0970
0111	0.5291	0.5105	0.0186	0.6600	0.5629	0.0971
1000	0.5774	0.5557	0.0217	0.6434	0.5510	0.0924
1001	0.5602	0.5392	0.0210	0.6461	0.5536	0.0925
1010	0.5277	0.5194	0.0083	0.6470	0.5552	0.0918
1011	0.5652	0.5040	0.0612	0.6496	0.5576	0.0920
1100	0.5519	0.5460	0.0059	0.6549	0.5569	0.0980
1101	0.5334	0.5242	0.0092	0.6581	0.5595	0.0986
1110	0.5242	0.5168	0.0074	0.6583	0.5608	0.0975
1111	0.5129	0.5058	0.0071	0.6614	0.5635	0.0979

**Figure 3.20.** Mutual information versus noise standard deviation of WDDL (bold line) and CMOS (dotted line) implementation of the 4-bit PRESENT crypto-core, using $(10)_2$ as secret key.

been performed using the most significant nibble of the output of the *AddRoundKey* layer at the first round as intermediate value. In detail, the target word can be

expressed as follows:

$$X = k_{79}k_{78}k_{77}k_{76} \oplus pt_{63}pt_{62}pt_{61}pt_{60} \quad (3.23)$$

where $k_{79}k_{78}k_{77}k_{76}$ is the most significant nibble of the 80-bit key and $pt_{63}pt_{62}pt_{61}pt_{60}$ is the most significant nibble of the 64-bit plaintext. The chosen key is the same on both implementations:

$$K = '07D607C504B507BFB4B0' \quad (3.24)$$

Results of AESP using the output word of the *AddRoundKey* are reported in Table 3.11. We obtain again higher correlation coefficient for the WDDL. This results are again matching with the mutual information analysis, shown in Figure 3.21. The WDDL implementation leaks more information than CMOS also in this case. The mutual information analysis remarks the previous result on the 4-bit crypto-core also for the complete implementation.

Since all the current samples collected in Cadence Virtuoso are given noise-free, Gaussian white noise has been added to PRESENT-80's static current measurements, simulating a realistic attack scenario [125]. The SNR has been set to -60dB, in order to take into account the electronic noise and the static current consumption of other on-chip non-cryptographic circuitry (e.g. glue logic). This value has been chosen in order to make a fair comparison of both implementations, because, at the given power of the noise, they exhibit almost zero mutual information, as shown in Figure 3.21. 100k static current samples have been generated for both implementations. As shown in Figure 3.22 the MTD value for the WDDL implementation is ~ 4000 samples, while for the CMOS version of the core ~ 30100 measurements are needed to recover the secret key. Again, the CMOS implementation has been found more resilient to AESP attack compared to WDDL. The presence of a DPL logic-style to counteract DPA/CPA attacks using interconnection of CMOS gates is ineffective in counteracting attacks exploiting static power.

3.6 Temperature Exploitation of Static Current's Information Leakage

In the common AESP approach, the attack is performed as univariate, as one sample of static current per measurement is collected, and also the statistic of the static power consumption is built upon a univariate model [15][19][5]. As it is clear from Equation 3.5 and from Figure 3.5, the main contribution to static current has a strong dependency on the working temperature of the integrated circuit. The possibility to enforce the information recovering through static power from a hardware implementation of cryptographic algorithm using the working temperature as new domain relies on the physical relation between the static current phenomena

Table 3.11. AESP attack against CMOS and WDDL implementation of the PRESENT-80 engine on noise-free static current samples. The working temperature has been set to 100°C.

Key ($k_{79}k_{78}k_{77}k_{76}$)	CMOS ρ	WDDL ρ
0000	0.6755	0.8431
0001	0.6675	0.6612
0010	0.0033	0.4319
0011	0.0113	0.2501
0100	0.1091	0.0211
0101	0.1011	0.1608
0110	0.5697	0.3901
0111	0.5777	0.5719
1000	0.5777	0.5719
1001	0.5697	0.3901
1010	0.1011	0.1608
1011	0.1091	0.0211
1100	0.0113	0.2501
1101	0.0033	0.4319
1110	0.6675	0.6612
1111	0.6755	0.8431

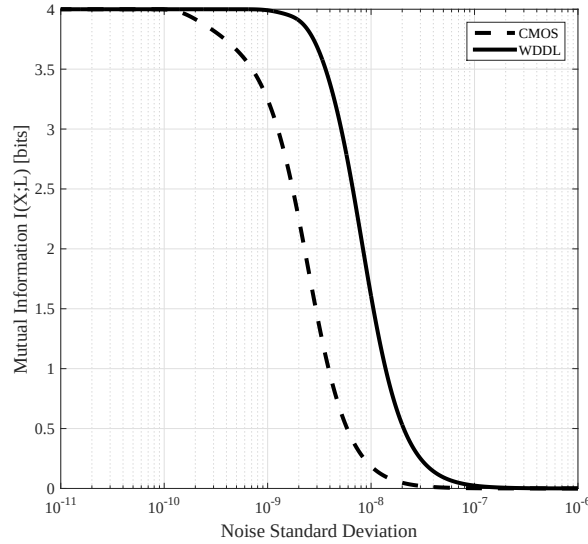


Figure 3.21. Mutual information versus the standard deviation of the noise for WDDL (bold line) and CMOS (dotted line) implementation of the PRESENT-80 cryptographic processor, using 100°C as working temperature.

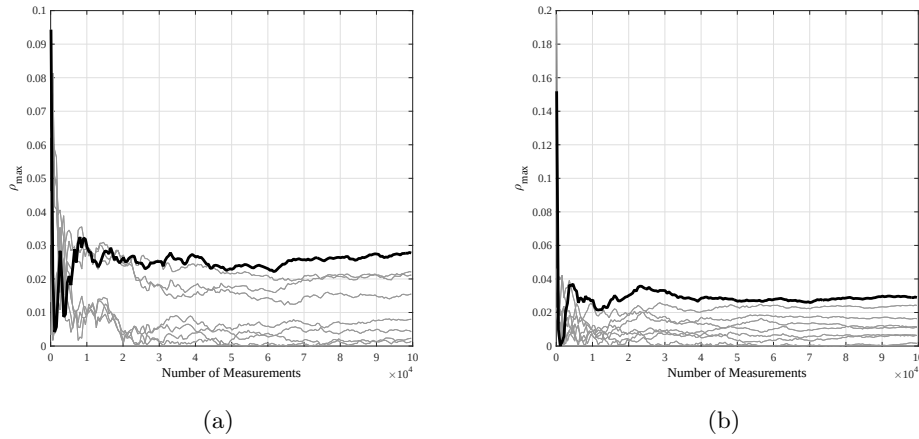


Figure 3.22. Correlation coefficient as function of the number of measurements CMOS 3.22(a) and WDDL 3.22(b) implementation of PRESENT-80 in a simulated experiment, using a SNR of -60dB. The correlation coefficient of the correct key is plotted in black, while correlation coefficients of wrong keys are plotted in grey.

and their dependency from the temperature itself. When the integrated circuit works at higher temperature, the magnitude of the static current increases, since each contribution to the overall static consumption has exponential terms with the thermal voltage V_T , which is linear with the absolute temperature accordingly to Equation 3.6. The temperature-dependence of the static current can help the adversary to easily recover information from the cryptographic device, and a security assessment of this dependency has to be correctly verified.

The temperature dependency of the static current and its impact on the security level of a cryptographic device has been investigated on the same 4-bit PRESENT crypto-core and on the full implementation of the PRESENT-80, presented in the previous section and shown in Figure 3.18 and 3.19 respectively, using the same testbenches. In addition, also the presence of intra-die variations have been taken into account for the 4-bit PRESENT-based crypto-core, by means of Monte Carlo generated circuit samples. The analysis of temperature dependency of the security level using static power consumption has been carried out using both actual and information theoretic security metrics. To completely cover the classic working temperature range, the analysis has been carried out in the range $0 - 100^\circ\text{C}$, with steps of 20°C .

3.6.1 Temperature dependency on the 4-bit PRESENT crypto-core

In Figure 3.23, the behavior of the average static current values among the Monte Carlo simulations' circuits is in accordance with [40] and with Equation 3.5. In Table 3.12, average values of the static currents and standard deviation in the presence

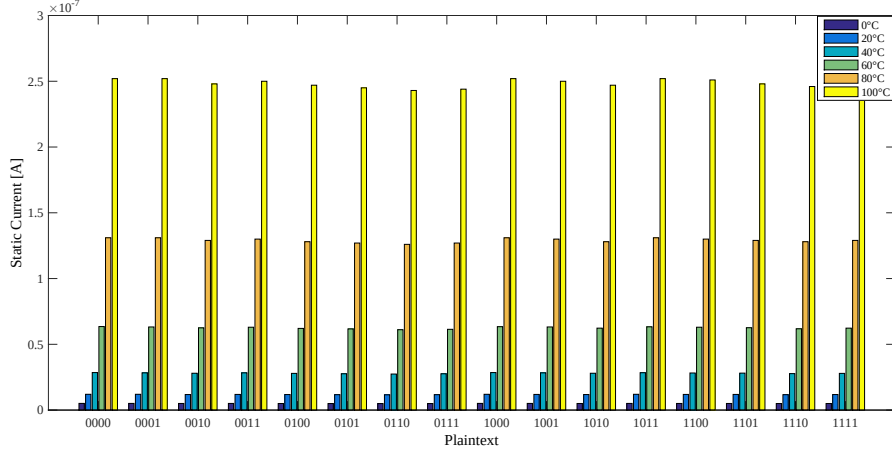


Figure 3.23. Average value of the static current samples collected on the 4-bit PRESENT crypto-core among all Monte Carlo simulations' circuits. Results are shown regarding the input vector and the working temperature.

Table 3.12. Average values of the static currents and standard deviation for the Monte Carlo simulations' circuits of the 4-bit PRESENT crypto-core.

Temperature	0°C	20°C	40°C	60°C	80°C	100°C
μ	5.02nA	11.85nA	28.06nA	62.52nA	129.01	248.27nA
σ	0.19nA	0.52nA	1.25nA	2.64nA	5.12nA	9.50nA
CV [%]	3.78	4.38	4.45	4.22	3.97	3.82

of intra-die variations are reported. In order to precisely quantify the information leaked by the static power consumption regarding the working temperature, the mutual information has been used on the nominal case of the 4-bit PRESENT crypto-core. The mutual information curves as function of the standard deviation of the noise are reported in Figure 3.24.

It has to be noticed that the mutual information curves shift to right as the working temperature increases. In other words, the implementation leaks more if the working temperature is higher. As we have mentioned before, the mutual information quantifies the amount of information that an adversary can extract from a given side-channel. Assuming that he/she has a perfect knowledge of the chip's behavior in terms of statistical model of the physical emission. It can be seen as the best-case from the adversary point of view, and it represents the upper bound limit of the extraction of information from a device [137] [91]. Considering a 3.5bit of information for 0°C and the same mutual information value for 100°C, the noise standard deviation is two orders of magnitude higher in the latter case, which means that even in the presence of lower SNR, the adversary can extract the same amount of information. It remarks the importance of this result, because there is a strong increase in the information leaked through the static power consumption if the device works at higher temperature. This temperature dependency impacts directly also on the possibility to achieve a successful attack.

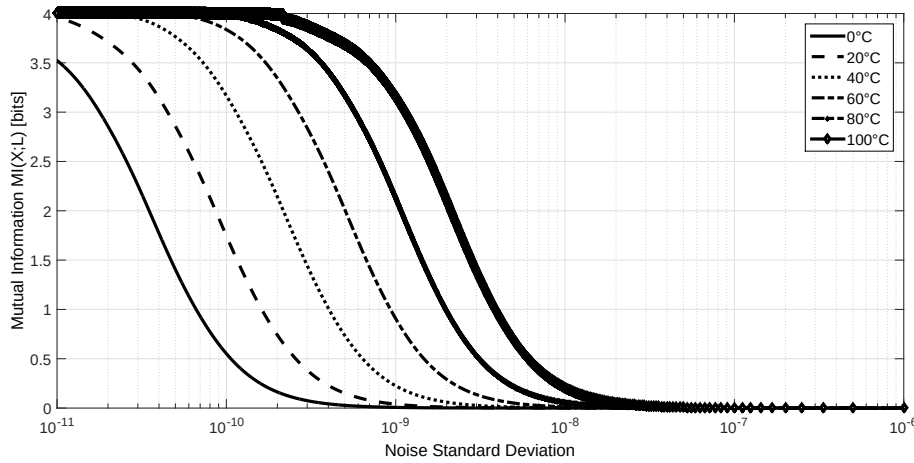


Figure 3.24. Mutual information curves as function of working temperature and the noise standard deviation for the 4-bit PRESENT based crypto-core.

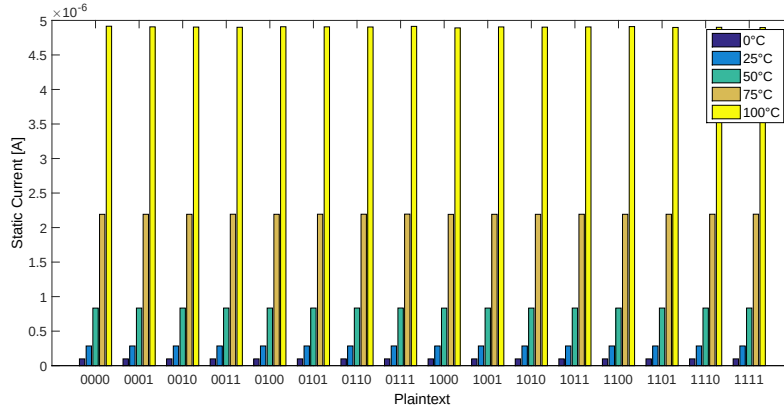


Figure 3.25. Average value of the static current samples collected on full implementation of the PRESENT-80. Results are shown regarding the input vector and the working temperature.

3.6.2 Temperature dependency on the full implementation of the PRESENT-80 block cipher

The temperature-dependency of the static current is also strong in the complete implementation of the PRESENT-80 block cipher, as can be seen in Figure 3.25. Mutual information curves versus standard deviation of the noisy component are shown in Figure 3.26. In the range 25 – 100°C, the mutual information exhibits a slower reduction between 4 and 3.5bit, compared to 0°C plot. At 0°C, the slope of the mutual information curve is very similar to the slopes of mutual information curves of the 4-bit PRESENT crypto-core, as shown in Figure 3.24.

In order to better assess the exploitability of the static current and its relation with the temperature, the full implementation of the PRESENT-80 has been attacked

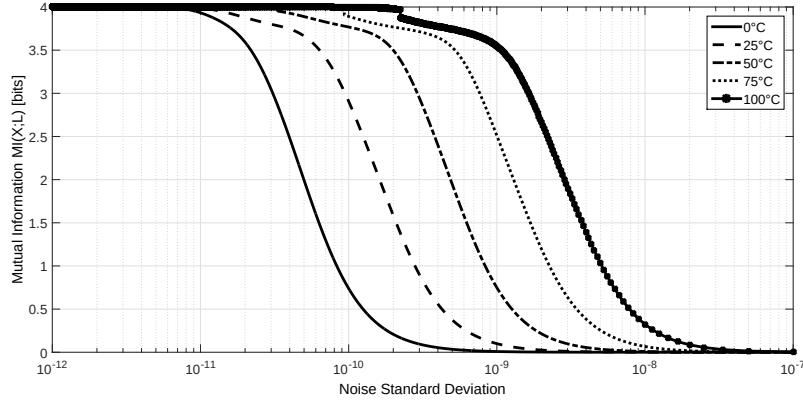


Figure 3.26. Mutual information curves as function of the working temperature and noise standard deviation on full implementation of PRESENT-80.

Table 3.13. Results of the MTD analysis using the AESP procedure on the full implementation of the PRESENT-80 in the range 0 – 100°C.

Temperature [°C]	0	25	50	75	100
MTD	>100k	>100k	84k	72k	19.1k

using the AESP procedure in the range 0 – 100°C, using the same key reported in the previous section for the vulnerability analysis. To simulate a real experiment, Gaussian white noise has been added in Matlab. A SNR of -60dB has been used to recreate a real world experiment. The most significant nibble at the output of the *AddRoundKey* at the first round has been chosen as intermediate result to mount the AESP, as shown in Equation 3.25. The maximum storage capability has been set to 100k for each temperature.

$$x_{63}x_{62}x_{61}x_{60} = I_{63}I_{62}I_{61}I_{60} \oplus k_{79}k_{78}k_{77}k_{76} \quad (3.25)$$

In order to get the MTD, experiments have been repeated increasing the number of plaintext. Results of AESP as function of the number of plaintext used are shown in Figure 3.27(a)-3.27(e). It has to be noticed that the MTD is progressively reduced from >100k to 19.1k, if the temperature is increased from 0°C to 100°C. At temperature below 50°C, it was not possible to recover the key within the given SNR and the maximum storage capability. A resume of the results of AESP attacks against the full implementation of PRESENT-80 is reported in Table 3.13.

3.6.3 Multivariate Analysis of Static Currents

The multivariate approach in dynamic power exploitation is mainly devoted to the use of two domains:

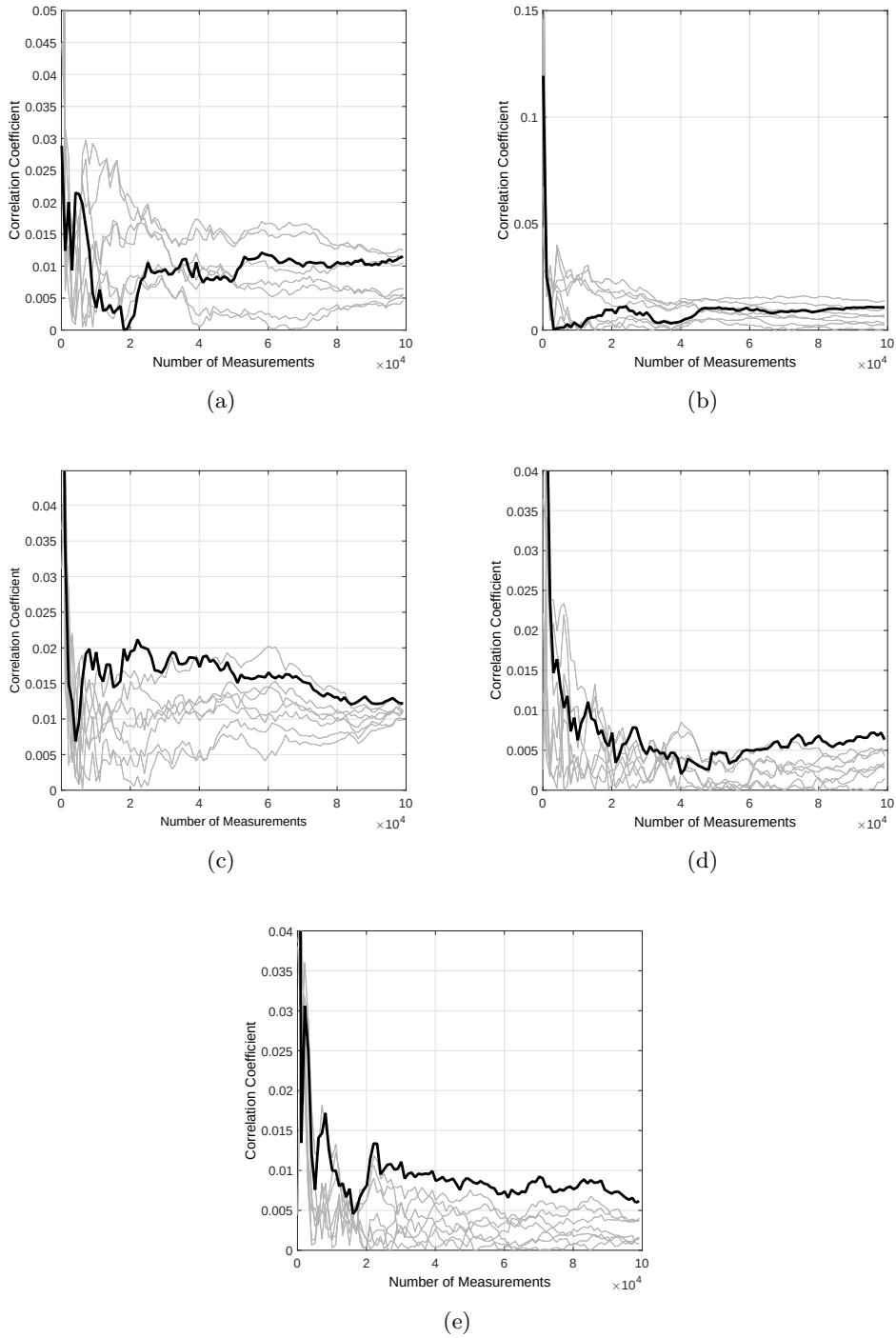


Figure 3.27. Correlation coefficient versus the number of measurements in the AESP procedure on the full implementation of the PRESENT-80. Plots (a) to (e) are referred to working temperature from 0°C to 100°C. Black bold lines represent the correlation coefficient of the correct key; grey lines represent the correlation coefficient of wrong keys.

- dynamic current samples magnitude;
- time domain.

It has been proven that in hardware implementations, there is a high correlation (in time) between neighboring points in a power trace [93]. As we have said before, a single static current sample can be considered as an extraction of a Gaussian distributed random variable for each given operation. This non-deterministic behavior is due to the presence of noise, and, if we now consider to use more than one sample, each characterized by its own Gaussian distribution, we have to move to a *multivariate analysis* [48]. In order to get a *multivariate* approach to attack exploiting static power as side-channel, an adversary can make use of the temperature dependence expressed in Equation 3.5. Instead of using time as other domain, a multivariate approach to AESP can make use of the temperature domain. The idea to use the temperature domain for a multivariate approach is justified since the analysis in Figure 3.24 and 3.26 confirm the possibility to extract "more" information forcing the device under analysis to work at higher temperature.

Process variability of deep sub-micron CMOS technologies raises new issues in security for cryptographic applications. Experiments performed on 20 prototype chips in [125], implemented in 65nm CMOS process showed that common attack procedures like DPA are no more effective like in the past to evaluate the level of security of a device. As a consequence of the strong dispersion of process parameters due to intra-die and inter-die variations in deep sub-micron technologies, static current phenomena are even more variable and their behavior changes a lot from chip to chip. So, in general, it is not easy to assess "how much the implementation leaks". The multivariate analysis exploiting static power is based on the possibility to perform experiments on the device under analysis at different temperatures and combining results to extract as much information as possible. To study the impact of intra-die variations on the amount of the information that a generic adversary can extract, 100 sample circuits have been generated by mean of Monte Carlo simulations of the 4-bit PRESENT based crypto-core shown in Figure 3.18. As reference, the univariate analysis has been performed on chips, at 100°C as working temperature, since it has been proved to be the best temperature to extract information from the hardware implementation of the 4-bit PRESENT crypto-core, as reported above.

In order to take into account the presence of intra-die variations, the use of perceived information is necessary. In fact, the mutual information assumes a best-case model for the adversary. In the context of mutual information, the adversary has a perfect knowledge of the device and of the statistical behavior of the power consumption. In other words, he/she profiles the device and use the profiles to extract information from the same chip. In a real world, this model cannot fit the "average case" for the adversary, which generically use one chip for profiling and makes use of these profiles to extract information from a similar one. In addition to that, he/she does not have a perfect knowledge, thus the profiles that he/she can build are not perfect. The perceived information is able to capture and evaluate how profiles built on a chip *A* fit actual power consumption of a chip *B*. In Figure 3.28(a),

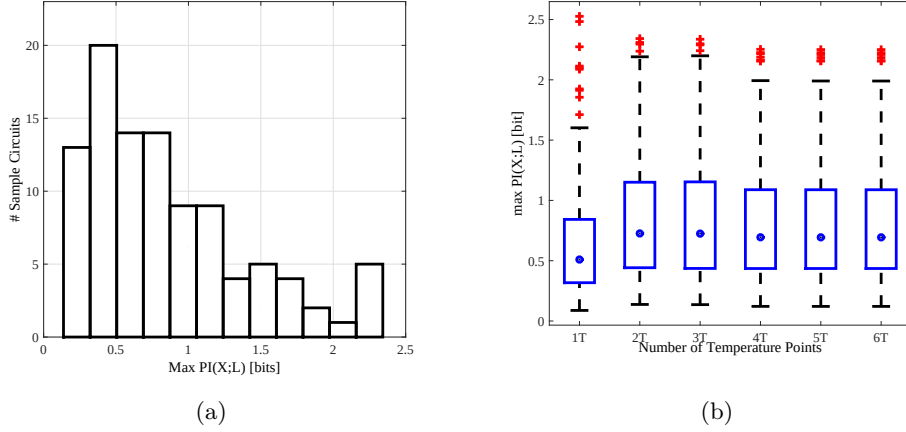


Figure 3.28. Figure (a) shows the distribution of the maximum value of the perceived information using $[60^{\circ}\text{C}; 100^{\circ}\text{C}]$ as temperature points over all 100 Monte Carlo's chips. In (b), box-plot of the median value of the maximum of perceived information regarding the best temperature points combinations, from 1-point to 6-points. Black dots represents the median value for each case over the 100 chips. The bottom and the top of each box represent the first and the third quartiles, respectively.

Table 3.14. Median values over the maximum of perceived information over 100 sample circuits in the presence of intra-die variations. 1-points case is used as reference.

No. Of Temp. Points	1	2	3	4	5	6
$\text{median}(\max(\text{PI}(\text{X};\text{L})))$ [bits]	0.51	0.73	0.72	0.69	0.69	0.69
Gain Factor	1	1.44	1.42	1.36	1.36	1.36

the distribution of the maximum value of the perceived information using two temperature-points $[60^{\circ}\text{C}; 100^{\circ}\text{C}]$ over all sample circuits. To evaluate perceived information, the nominal chip has been used to build profiles. It has to be noted that the distribution is not symmetric, and thus not normal. This behavior can be demonstrated using all possible combination of temperature points, in any number. To better estimate the *typical outcome* of the positively skewed distribution shown in Figure 3.28(a), the *median* values are used instead mean values [83]. The maximum value of perceived information has been analyzed regarding best combinations among possible combination of temperature points in the range $0 - 100^{\circ}\text{C}$ (with steps of 20°C), and medians have been evaluated and reported for best combinations of temperature points in Figure 3.28(b), from 1-point to 6-points.

Table 3.15. Maximum values of perceived information for chip 46.

No. Of Temp. Points	1	2	6
$\max(\text{PI}(\text{X};\text{L}))$ [bits]	0.64	1.22	1.17
Gain Factor	1	1.91	1.83

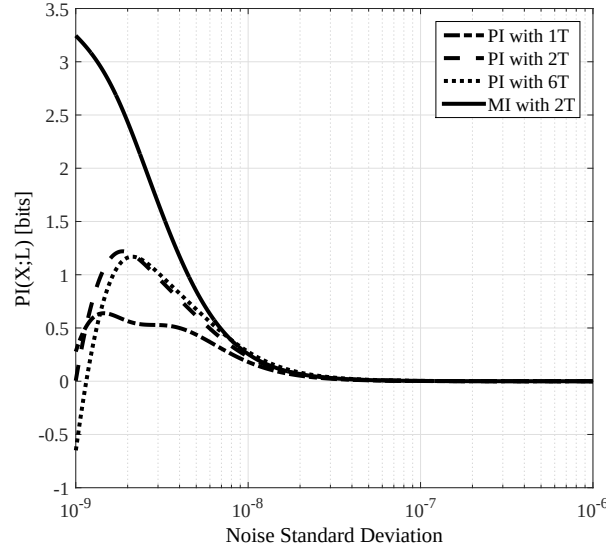


Figure 3.29. Perceived information versus the noise standard deviation for chip 46. Mutual information curve is used as reference.

In Table 3.14, median values of the maximum perceived information evaluated over the Monte Carlo generated sample circuits are reported, regarding the number of temperature points used. Using more than one temperature, the amount of information that can be extracted using non perfect profiles can be increased of a 44% compared to the univariate case. This result confirm the strengths of the multivariate approach in extracting secret information from static power consumption. Moreover, focusing on a single chip, randomly picked from the Monte Carlo generated sample circuits, the improvement in the maximum value of the perceived information is 91% if 2-points are used. Looking at Figure 3.29, the multivariate approach can yield up to twice the information with the same noise standard deviation if compared to univariate analysis. It remarks a strong increase in probability to get a successful attack within the same scenario. A resume of the results about the perceived information's maximum values on chip 46 is reported in Table 3.15.

3.7 Template Attack Exploiting Static Power: TAESP Methodology

In recent years, profiled attack procedures, in particular *Template Attacks* (TAs), have been considered to be the most effective attacks, among SCAs, to recover secret information from hardware implementations of cryptographic algorithms. First formulation of TAs have been introduced in [41], regarding the possibility to take advantage of all possible information that can be extracted from a physical emission. During a TA, a clone device of the device under attack is characterized (profiled) to study the probability distribution of the leaked information by means of

its power consumption. Conclusions about probability distributions are further used to extract relevant information from the device under attack, by means of maximum likelihood criteria, which is able to capture linear and non-linear dependencies. The main reason that makes TAs more efficient than CPA and DPA, is due to the fact that a characterization of a clone device is performed to derive a precise power model of the entire class device [41]. Conventional TAs exploit the dynamic power consumption and rely on the possibility to use a profiling phase to build a sounding power model of the device, which is based on actual power measurements, instead using *a priori* power model, such as the Hamming Weight or Hamming Distance [41]. A key requirement for a TA is that the adversary has an identical experimental device, which can be reprogrammed. While such an assumption is limiting, it holds in many cases. In the context of profiled attacks, it has to be pointed out that their effectiveness is limited by inter-die and intra-die process variations, which introduce differences in the behavior of the profiled device compared to the device under attack [125].

The *Template Attacks Exploiting Static Power* (TAESP) is a novel procedure to exploit information from static current, that has been proposed during the Ph.D. work in [17]. A profiling phase is used to build a precise model (template) of the static power consumption of a clone device performing cryptographic operations. In the subsequent attack phase the template is used to attack different devices. This approach allows to extend the conventional TA in two ways:

- Templates are built using the static power consumption. It has to be pointed out that, differently from dynamic power consumption, static power measurements are made up of a single sample resulting from a relatively long integration time (instead of several instantaneous time samples), and therefore, TAESP procedure has to be intrinsically considered as univariate in which noise is averaged in time domain.
- The *multivariate* TAESP procedure, in which static power measurements collected at different controlled working temperature are used both in the profiling and attacking phase. The temperature domain is used in place of the time domain to get multivariate statistics.

3.7.1 TAESP Algorithm

The TAESP procedure can be summarized as follows: during the profiling phase, the clone device's static power consumption is profiled (e.g. measured) while executing the target operation (e.g. the key is processed). In the attacking step, experiment on the device under attack (which is a different chip sample) are performed in order to collect static power measurements. These samples are then compared against the templates, built in the previous step. Finally, the posteriori probability is computed for each target operation, comparing collected samples from the attacking phase with the profiles by means of maximum likelihood criteria.

The detailed implementation of the TAESP procedure is reported as follows:

1. *Profiling Phase*

- (a) Choose a number N of temperature points $\{T_1, \dots, T_N\}$, in the working range of the device class.
- (b) Collect a set of static current measurements $L_{profile}$ of the clone device for each O_i target operation $\{O_1, \dots, O_K\}$, at each of the N temperature point.
- (c) Compute the sample mean for each target operation measurement set, related to respective temperature points, obtaining K vectors of N -length sample means $\{M_1, \dots, M_K\}$.
- (d) Compute the pairwise difference between sample means and measurement set, in order to estimate the covariance matrix of the noise process for each operation at each temperature point, obtaining K covariance matrix $\{\Sigma_1, \dots, \Sigma_K\}$. The output of step 3 and 4 are the K profiles (M_i, Σ_i) for $i=1, \dots, K$, which map each target function O_i to a profile.

2. *Attacking Phase*

- (a) Collect a set of static power measurements L_{attack} on the device under attack, while it is processing D known input vectors, recording the current at each of N chosen temperature point. The new measurement set is then compared with the profiles, computing the *conditional probability* for each measurement $l_j \in L_{attack}$ for each profile:

$$Pr(l_j|O_i) = \frac{1}{\sqrt{(2\pi)^N |\Sigma_i|}} e^{\{-\frac{1}{2}(l_j - M_i)^T \cdot \Sigma_i^{-1} \cdot (l_j - M_i)\}}, \forall i = 1, \dots, K, \forall j = 1, \dots, D \quad (3.26)$$

where l_j are N -length vectors measured on the device under attack with the same input at each chosen temperature point [93].

- (b) Compute the *likelihood function* for each O_i (with $i=1, \dots, K$) target function, estimating the posteriori probability to get the correct profiled used while observing the measurement set L_{attack} , by means of the Bayes' theorem [93]:

$$Pr(O_i|L_{attack}) = \frac{(\prod_{j=1}^D Pr(l_j|O_i)) \cdot Pr(O_i)}{\sum_{k=1}^K (\prod_{j=1}^D Pr(l_j|O_k)) \cdot Pr(O_k)} \quad (3.27)$$

where $Pr(O_i)$ is the prior probability related to O_i target function. Then, the key guess is extracted as follows:

$$O_{guess} = \operatorname{argmax}_i (Pr(O_i|L_{attack})) \quad (3.28)$$

where Equation 3.28 corresponds to the maximum likelihood criteria, which aims to minimize the probability of error when determining the target operation (e.g. the key used by the device under attack).

A graphical resume of the TAESP algorithm is reported in Figure 3.30.

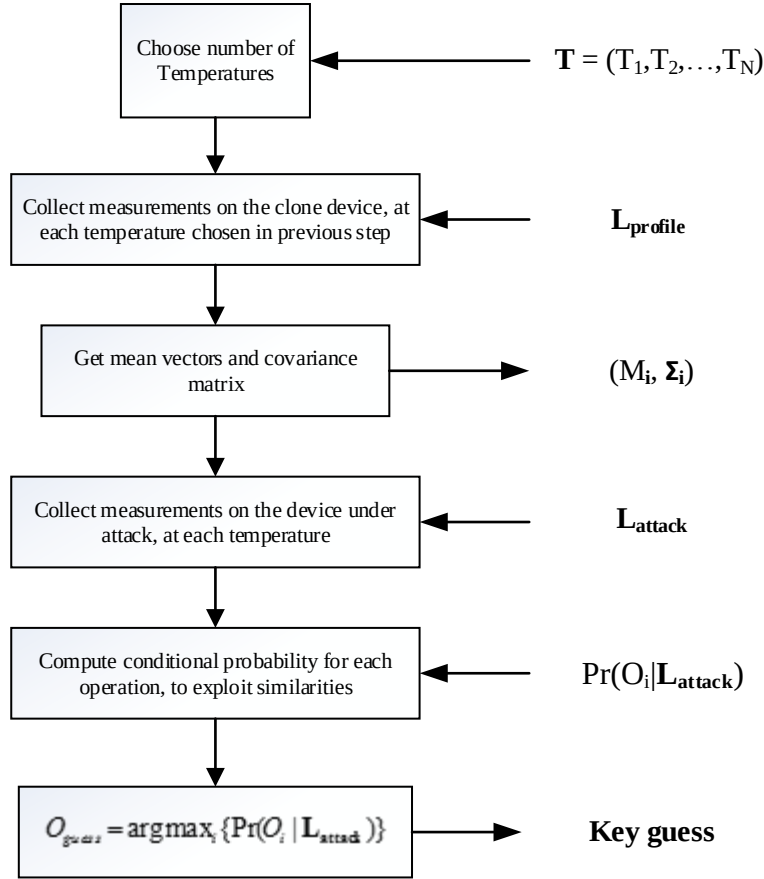


Figure 3.30. Template Attacks Exploiting Static Power algorithm and procedure flow graph.

3.7.2 TAESP Against The 4-bit PRESENT Crypto-core

In order to demonstrate the effectiveness of TAESP, simulated experiments have been performed on the 4-bit PRESENT crypto-core presented in 3.5.3. Also the same measurement procedure has been used to collect static current samples. For each possible key k_j , with $j=1, \dots, 16$, static current samples have been measured with all possible plaintext pt_i , with $i=1, \dots, 16$, resulting with all possible value $X_{i,j}=f(pt_i, k_j)$. All simulations have been repeated in the range $0 - 100^\circ\text{C}$ with steps of 20°C .

Referring to the 4-bit PRESENT crypto-core case study, profiles have been built on the nominal simulations (namely, the chip 0), and 100 Monte Carlo generated sample circuits have been used as different devices under attack. The secret key for all

Table 3.16. Results of the TAESP attack on the 100 samples generated by Monte Carlo simulations, with the best-case temperature points combinations.

No. Of Temp. Points	Temperature Comb. [$^{\circ}\text{C}$]	No. Of 1 st Ranked Chips	No. Of 1 st and 2 nd Ranked Chips
1	100	30	47
2	20, 60	46	63
3	20, 60, 80	37	53
4	20, 40, 60, 80	32	46
5	0, 20, 40, 60, 80	26	33
6	0, 20, 40, 60, 80, 100	18	21

experiments has been set at $k=(6)_2$. Results of univariate and multivariate TAESP are reported in Table 3.16, where the combinations of temperature points which give the best attack results, the number of successfully attacked chips considering only the correct key (e.g. first ranked), the number of chips for which the correct key corresponds to the second highest probability (e.g. second ranked) are reported. As it can be noted, results from Table 3.16 confirm that multivariate TAESP using the combination of two temperatures allows to increase the number of successfully attacked chips of more than 50%, compared to univariate TAESP (1-point attack). Table 3.17 shows a summary of the results for all possible temperature combinations. The first column reports the number N of temperature points used for the attack; the second column shows the minimum number of successfully attacked chips (the corresponding temperatures set is reported in the third column); the fourth column reports the maximum number of the successfully attacked chips (the corresponding temperatures set is reported in the fifth column), whereas the sixth column reports the average value (across all possible combinations with the given number of temperature points) of successfully attacked chips. As we can see from Table 3.17 the multivariate TAESP allows to increase the minimum number of successfully attacked chips, from 9 to 18.

The dependency of the TAESP effectiveness on the chosen temperature combination is similar to the dependency of the conventional TAs exploiting dynamic power on the points of interest in the time domain [41].

To better highlight the results of these experiments, we re-defined the *Success Value Indicator* (SVI), a security metric introduced in [111] for DPA/CPA attacks, as follows:

$$SVI = Pr(k_{correct}|L_{attack}) - \max_i(Pr(k_{i,wrong}|L_{attack})) \quad (3.29)$$

According to this formulation, the SVI assesses how well the correct key can be distinguished from wrong keys, by comparing results of the statistical distinguisher used. If the SVI is strictly positive, the correct key is successfully recovered among wrong keys. This definition of the SVI allows to fairly compare the effectiveness of

Table 3.17. Results of the TAESP procedure on the 100 circuit samples generated by Monte Carlo simulations with all possible temperature points combination, regarding the number of successfully attacked chips with correct key ranked as first.

No. Of Temp. Points	Min	Temp. at Min [°C]	Max	Temp. at Max [°C]	Average
1	9	0	30	100	19
2	8	0, 20	46	20, 60	27
3	14	60, 80, 100	37	20, 60, 80	26
4	13	0, 60, 80, 100	32	20, 40, 60, 80	23
5	13	0, 20, 60, 80, 100	26	0, 20, 40, 60, 80	19
6	18	0, 20, 40, 60, 80, 100	18	0, 20, 40, 60, 80, 100	18

the multivariate TAESP (more than one temperature) with the univariate case (one temperature). In fact, the use of SVI gives an estimation of the confidence of the result of an attack. The higher is the SVI, the higher will be the confidence that the adversary can rely on the key guess given by the attack procedure. Considering the percentage of chips for which $SVI \geq 0.8$ among all successfully attacked chips, accordingly to Equation 3.30, the TAESP is able to increase also this figure of merit if the number of temperature points increase (in both profiling and attacking stage), as shown in Figure 3.31.

$$FoM = \frac{n_{SVI \geq 0.8}}{n_{SVI > 0}} \cdot 100 \quad (3.30)$$

3.7.3 TAESP in a Simulated Experiment

In order to complete the analysis of the effectiveness of the TAESP and to compare multivariate with univariate procedure in realistic experiment, chip 46 has been attacked again, adding Gaussian white noise to the simulated measurements [125] [19] [2]. The SNR has been set to -60dB, as in the previous analysis. Results of the TAESP attack procedure are shown in Figure 3.32. For this attack, 15000 static power samples have been generated for all the different temperatures and performed the TAESP procedure considering from 1 to 4 temperature points.

As shown in Figure 3.32(a), the univariate case (one temperature point), it is not possible to recover the correct key with 15000 measurements. In this case, the MTD is greater than 15000. Using more than one temperature, the correct key can be correctly recovered with less than 4000, 2300 and 1900 measurements in 2-points, 3-points and 4-points cases, respectively.

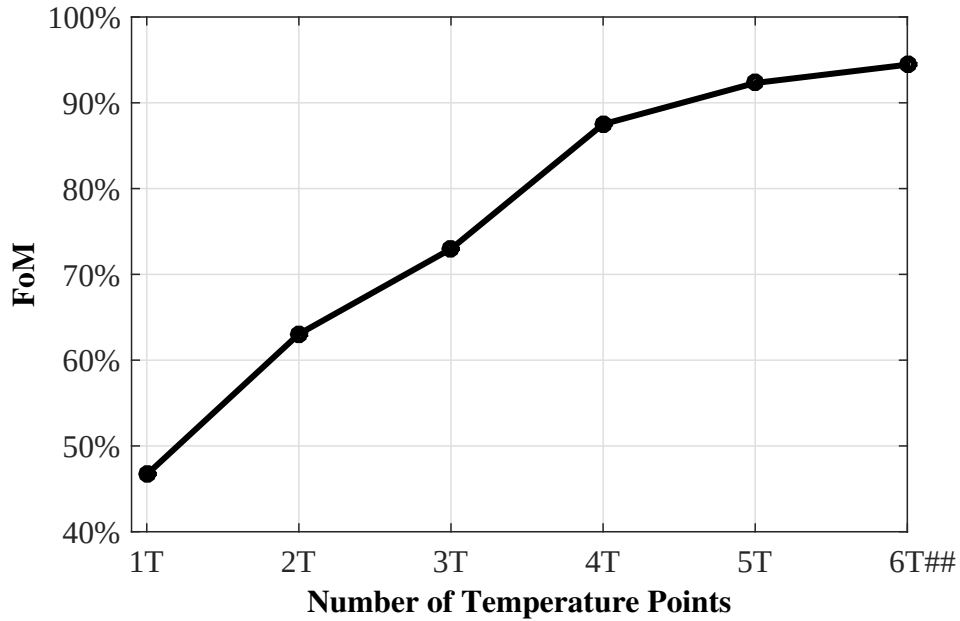


Figure 3.31. Percentage of chips with $SVI \geq 0.8$ (see Equation 3.30) among all successfully attacked chips.

3.8 Measurements Setup for AESP Security Evaluations

Static and dynamic power analysis require different measurement procedures, due to physical reasons. Dynamic phenomena are intrinsically related to time domain, because every event has a location in time. This location in time matches (or, at least, is related to) the time at the event occurs. Static phenomena are not related to time domain, and they are concerned with the steady state of a system. This difference impacts critically on the procedure that is needed to measure the phenomena and to get a precise procedure to attack and evaluate the robustness of cryptographic devices to AESP.

3.8.1 State-of-the-art of Measuring Static Power for SCA

In [107], Moradi compared Xilinx FPGA devices from three different families (65nm, 45nm and 28nm process) in terms of static current absorption. In these experiments, a huge number of registers (14k flip-flops) with pre-stored '1' and '0' have been placed in FPGA devices. By means of measurements of the static power consumption, author demonstrate the feasibility of retrieving information through the aforementioned side-channel from those devices. Measurements have been collected by evaluating the static voltage drop across a 1Ω resistor in series with the power supply line, using a Digital Storage Oscilloscope (DSO) and differential probes. Moradi shows that the power consumption of two different states leads to different values of static currents drawn by the device, in each of the three cases.

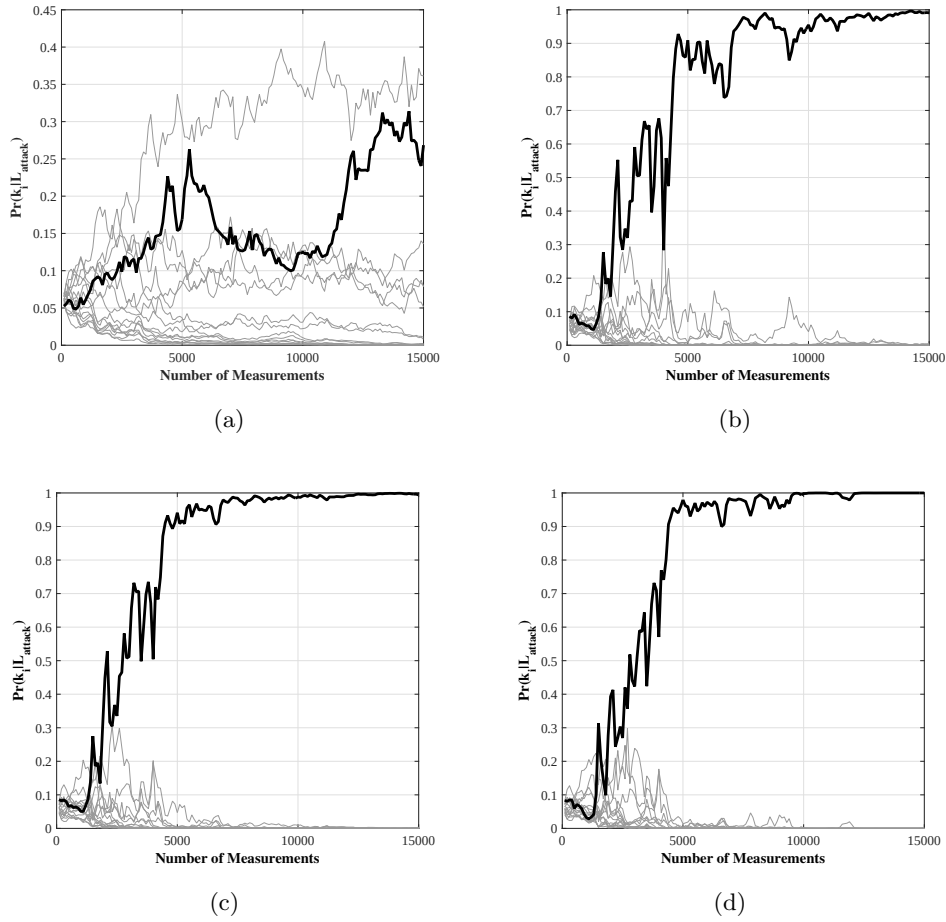


Figure 3.32. Probability in Equation 3.27 versus the number of measurements for chip 46, using chip 0 for the profiling phase. Black lines refer to the probability value of the correct key. Grey lines represent the probability of wrong keys. Plot (a), (b), (c), and (d) are referred to TAESP with increasing number of temperature points, from 1-point to 4-points, respectively. The combinations used are reported in Table 3.16, since we have found them as the-best case also for chip 46.

In [118], authors presented a study on a 65nm ASIC chip, which implements the AES Rijandel's S-BOX function. In order to reduce influences of dynamic phenomena, the clock signal has been set to 2MHz, to easy capture dynamic and static leakage separately. These results are then used to compare and evaluate the SNR of dynamic and static leakage, from the adversary point of view. It has been demonstrated that the use of static currents is very effective in the presence of masking scheme, reducing the complexity of the attack.

In [106], it has been stated that changes in environmental temperature inside the laboratory can affect significantly the time required to correctly recover the key from the device under attack. The solution they propose is to use a climate chamber. In this procedure, the measured signal is amplified by a differential DC amplifier.

3.8.2 Issues in Measuring Static vs. Dynamic Leakage

There are several major problems in order to get "good" static current samples for AESP and static power vulnerability analysis. As we have said before, the measurement procedure can be quite different. Since the static current is a static phenomena, the presence of dynamic phenomena during the measurement operation can influence the result of the attack. If the device is working with a reasonably high frequency (e.g. the maximum operating frequency), the static component of the overall consumption is meaningfully smaller than the dynamic one. Hence, the SNR of the information leakage contained in static currents is strongly limited by the presence of dynamic phenomena [118], and, consequently, limiting the possibility to get a successful attack. The small amplitude of the static component is one of the most critical factor in real world measurement and attacks. The presence of the noise is more critical when the signal to be measured becomes smaller, which is exactly the situation of measuring static currents in CMOS devices.

The SNR is highly influenced by the measurement setup. In Equation 3.5, the dependency of the static current on the working temperature is very strong. In fact, each phenomena involved in static dissipation, contains Arrhenius-like dependencies with the working temperature. So far, in AESP, variations in the operating temperature can be considered as a strong disturbance, because it influences not only the mean values of measured static currents, but also the data-dependent variance, corrupting the correlation with processed data.

3.8.3 Novel Measurements Setup for AESP Analysis

Both designing and attacking secure devices needs post-silicon security evaluation of the robustness against SCAs. A novel measurements setup for AESP attacks has been proposed in [16]. This novel measurement setup is intended to be optimized to evaluate the security of hardware implementations of cryptographic algorithms to AESP attacks. In literature, PAAs have been commonly performed using DSOs to

collect power traces, by using the voltage drop across a resistor in series with the power supply line of the device under attack. Also for static current measurement, authors in [118][107][106], present their framework based on the same approach. The value of the sampled signal is strongly influenced by the value of the resistor, which acts as a simple transimpedance converter. Using high value resistor has the advantage to increase the magnitude of the sample differential voltage, but, on the other hand, it provides a lower supply voltage fed to the device and higher noise power. In order to measure the static current while minimizing the noise power and avoiding the voltage burden on the power supply line due to the presence of the series resistor, we have chosen to use a pico-ammeter rather than a DSO. More in detail, the new measurement setup makes use of a precision pico-ammeter to measure static current: the Keithley 6585. The Keithley 6485 [78] is usually used as benchtop ammeter for measuring low DC currents with high accuracy and very low voltage burden. The worst-case accuracy (current range set at maximum: 20mA) is $\pm 100\text{nA}$. The low voltage loss is achieved thanks to the use of internal feedback, which makes the Keithley 6485 more similar to an ideal ammeter. The highest voltage burden (current range 20mA) is 1mV. The instrument is designed to offer the lowest noise performance if the integration time of the internal Analog-to-Digital converter is set from one to ten Power Line Cycles (PLC). For AESP analysis, 1 PLC is a good compromise between noise performance and readings rate.

In order to mitigate the effect of the temperature on static currents measurements, device under attack's working temperature has to be controlled properly. The solution proposed by Moos *et al.* in [106], makes use of a climate chamber. The chamber will enclose both the device under attack and a very fundamental sub-system of their measurement chain: the differential DC amplifier. By this way, the DC amplifier has set to work at the same temperature of the device under attack, which, regarding [19] and [48], can be even higher than the room temperature, in order to exploit more information leakage from static power. As it is clear from classic electronics textbooks, the DC amplifier would give the best if it would be placed outside the climate chamber, to minimize the noise injected between the device under attack and the sampling instrument. In the proposed measurement setup, it has been used a Marlow Ind. RC3-8L-01LS 18W Peltier cell [94] as heater element, which is a 2x2cm solid-state heater/cooler that makes use of Seebeck effect to move heat from a cold side of the element to the hot one. In order to force the device's working temperature to the desired one, the Peltier cell has to be placed above the target chip, using the hot side as contact surface. To enforce the thermal coupling, thermal paste can be applied.

To control the temperature of the device, a control system is needed. The circuit shown in Figure 3.33 implements a feedback loop control system, and it has been designed using low-cost and off-the-shelf components, to reduce the cost. The operational amplifier used in this design is the rail-to-rail dual op-amp LM-358N [142]. The Texas Instrument LM-35 [141] has been used as temperature sensor, which can provide a low-cost solution for 0.5°C of accuracy. Since the sensor has a 3mm thickness, it has been placed closely to the Peltier cell's perimeter, and low-thermal resistivity aluminum foil has been used to provide a good thermal coupling with the

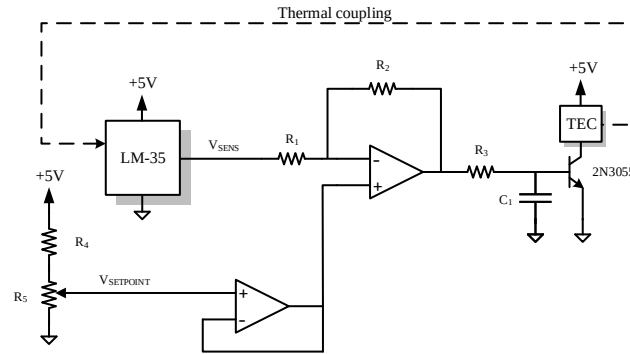


Figure 3.33. Schematic of the feedback loop controller of the Peltier cell.

hot side of the heater. In order to ensure the best heat transfer, the device under attack and the heater are mechanically locked, as shown in Figure 3.34.

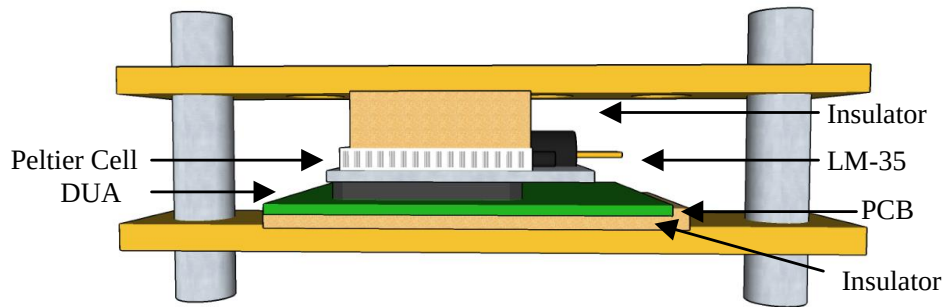


Figure 3.34. Cross-view of the stack in the mechanical locking system used to match the heater and the device under attack.

The system is able to set the working temperature of the device under attack from 25°C up to 90°C. In addition, the device under attack is placed inside an isolated environment to keep the air still and minimizing interactions with the laboratory. To optimize the signal strength, we assume that the adversary has a complete control on the clock signal, and he/she has the ability to stop it, in order to isolate the static component of the overall power consumption.

In the followings, the measurement chain is explained. A PC, running a Matlab script, controls the whole measurement setup, handling each operation by means of UART connections between the device under attack and the instrument. The clock signal which feeds the device under attack is generated by a control device implemented in a Altera Cyclone II FPGA. When the Matlab script demands a static current measurement, the PC sends a plaintext to device under attack, and it will generate a trigger signal during the execution of the target intermediate function. The control FPGA is able to receive a trigger signal from the device under attack, to synchronize the measurement operation and stop the clock signal properly. It

generates also the trigger signal for the pico-ammeter. The instrument requires a low-active signal *trg_in* to start the measurement. This *trg_in* signal has to assume '0' for a minimum of $2\mu\text{s}$ and it is needed to synchronize the integration of the internal A/D converter of the instrument. After the instrument has completed the measurement operation, it will generate a low-active *trg_out* signal, that communicates the end of the activity to the control FPGA. At this point, the clock signal is restored and the device under attack completes the cryptographic operation. At the end of this paradigm, the Matlab script requires the measurement to the pico-ammeter, and stores the sample in its memory. A detailed time diagram of the signaling is shown in Figure 3.35(b) and a block scheme of the measurement setup is shown in Figure 3.35(a).

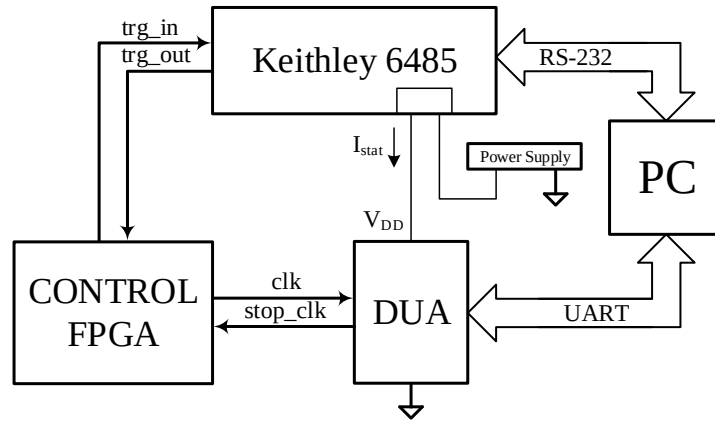
3.8.4 Experimental Measurement: Xilinx Spartan-6 ROM

The novel measurement setup has been used to mount AESP analysis. As first experiment, the static power consumption of a Xilinx Spartan-6 (45nm technology) FPGA has been used. The FPGA has been programmed to act as a 4kbit ROM. In one case, the FPGA has been set with all bits preset to '1's, and in the other one with all bits preset '0's. The aim of this experiment was to understand if we were able to distinguish the two cases. In Figure 3.36, The static power consumption of the Xilinx Spartan 6 (45nm technology) acting as a 4kbit ROM filled with 1 (in blue) and 0 (in red) is shown. The working temperature has been set to 65°C . As we can see, the two power consumption can be clearly distinguished and the state of the memory can be revealed.

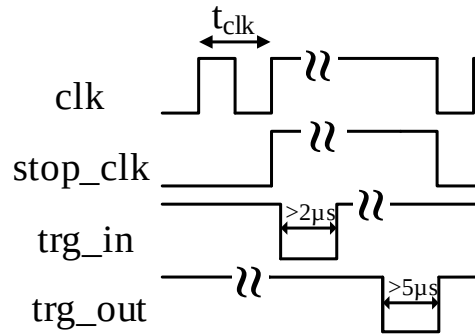
The average value for the case '0' is $\sim 22.5\text{mA}$, while for the case '1' the average static current is $\sim 22,4\text{mA}$. So, a difference of $100\mu\text{A}$ between the two cases allows us to define an average of $100/4096\text{bit} \approx 24\text{nA/bit}$ differences for each bit.

3.8.5 AESP on the 4-bit PRESENT crypto-core on the Xilinx Spartan-6 FPGA

To evaluate a more realistic scenario, the measurement setup has been used to perform AESP on the 4-bit PRESENT crypto-core (see Figure 3.18), implemented on the aforementioned Xilinx Spartan-6 FPGA. The core supply voltage has been set to 1.2V. The control FPGA provides a 1MHz clock signal, which is gated by the *stop_clk* signal, according to time diagram shown in Figure 3.35(b). As intermediate result, we have chosen the output word of the 4-bit S-BOX. The clock has been switched off after the second rising edge from the start of the encryption. The current has been measured from the main V_{DD} pad of the device under attack. The integration time of the internal analog-to-digital converter (ADC) of the Keithley 6485 has been set to 20ms, in order to take advantage of the noise performance of the instrument on this settings. The working temperature of the device has been set to 65°C . The number of measurement collected for this experiment was 4k, using $(7)_2$



(a)



(b)

Figure 3.35. Block scheme of the novel measurement setup (a) and timing diagram of signals (not in scale) during a measurement operation (b).

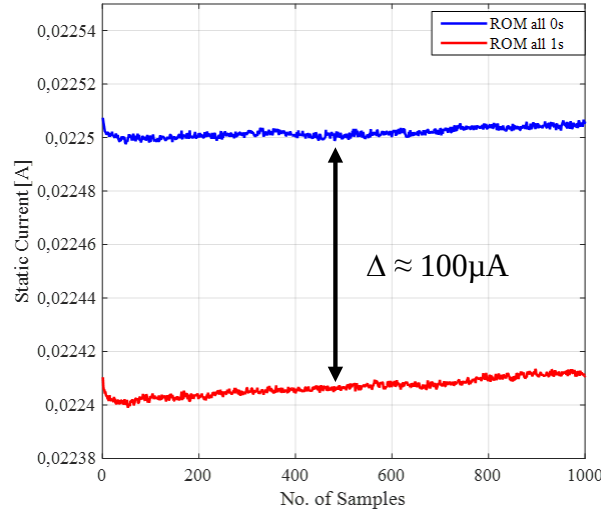


Figure 3.36. Static current absorption of a Xilinx Spartan 6 with a 4kbit ROM, filled with '0' (blue) and '1' (red), measured at $T = 65^{\circ}\text{C}$.

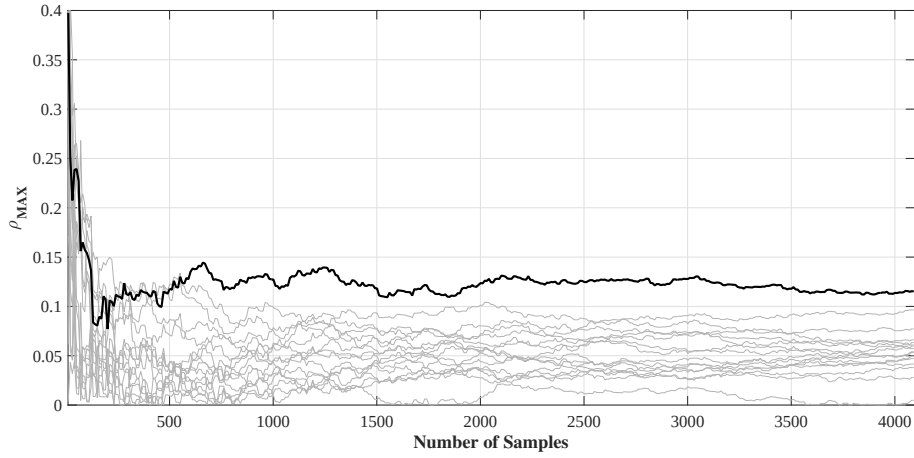


Figure 3.37. Correlation coefficient as function of the number of measurements used to perform the AESP attack on the 4-bit PRESENT crypto-core, implemented on the Xilinx Spartan-6 FPGA. The black line represents the correct key's correlation coefficient, while gray lines are referred to correlation coefficients of wrong keys.

as secret key. A plot of the correlation coefficient curves for each key guess versus the number of measurement are depicted in Figure 3.37. We obtained a MTD value of 547 samples, and the correct key's correlation curve can be clearly distinguish among all the others, remarking the ability of this setup and procedure to reveal the secret information.

3.9 Conclusions

In this chapter, an in-depth analysis of Attacks Exploiting Static Power in deep sub-micron CMOS technologies is presented. The arise of nanometer technologies has highlighted new issues in terms of physical security. The strong increase of static power is not anymore a secondary concern. The data-dependency in parasitic static currents can be used to recover secret information from secure devices, even in the presence of countermeasures against dynamic power exploitation. The AESP approach has shown that countermeasures conceived to protect cryptographic hardware from attacks based on dynamic power consumption (e.g. WDDL, MDPL, SABL) exhibit a leakage through the static power side channel and that this leakage can be even higher than the leakage of standard CMOS logic. Increasing the number of MOSFET devices in order to flatten the instantaneous current of the circuit and reduce variability may be not sufficient to protect a crypto-device. Furthermore, common techniques adopted to reduce static power in nanometer circuits can be ineffective in decorrelating its data-dependance.

A multivariate approach to exploit information leakage using static power dissipation has been also presented in this chapter. The temperature-dependency of parasitic static currents has been used to expand the dimensionality of AESP, which is intrinsically univariate. The use of the mutual information has shown that using higher temperature, the possibility to get a successful experiment is increased significantly. In fact, simulated AESP attacks have showed that the MTD value can be significantly reduced using higher temperature. With the aim of studying the effect of intra-die variations with an information theoretic approach, the multivariate analysis has been applied intensively on sample chips generated through Monte Carlo simulations. With a population of 100 chips, the median of the distribution of the maximum value of the $PI(X; L)$ is increased by 44% compared to the univariate case. Focusing on a randomly picked chip, the increasing in the maximum value of perceived information is of 91% using two temperatures, comparing the best result obtained with 1-point analysis, which means that the multivariate approach can lead to a strong reduction in the security level.

A new class of template attacks aiming at recovering the secret key of a cryptographic core from measurements of its static power consumption has been presented in this chapter. In Template Attacks Exploiting Static Power (TAESP), we take advantage of the temperature dependence of static currents in order to build a new multivariate approach able to extract relevant information from cryptographic devices. Referring to Monte Carlo simulation results on the 4 bit data path of the PRESENT crypto core, we have shown that, using just two temperature points the multivariate TAESP allows to attack almost 50% more chips, if we consider the number of chips that show the correct key as first ranked.

In this chapter, we have also presented a novel and effective measurement setup to perform AESP and vulnerability analysis using static power as side-channel. The use of not expansive and dedicated instrument to measure DC current instead of

DSOs, helps to maximizes the SNR. In order to minimize the effect of temperature on static current, we designed a controlled heater system using only off-the-shelf components and a commercial Peltier Cell as heater. To verify the effectiveness of the measurement setup, a 4x4 bit crypto-core based on PRESENT-80 has been implemented on a Xilinx Spartan-6 FPGA. AESP has been performed to evaluate the MTD of the implementation at 65°C. It has been found that 547 static current samples are sufficient to recover the correct key.

Chapter 4

D³L - A TEL-based Standard-Cell PAA Resilient Logic Style

4.1 Introduction

As we have mentioned in the previous chapter, new needs in commercial applications require that modern designs are often implemented with latest technologies. In Chapter 3, we have analyzed the security vulnerability due to the data-dependency of the static current consumption in recent technologies. The strong increase in static power consumption and its dependence on the processed data are not the only issue in modern CMOS processes. In the last two decades, many PAA countermeasures have been proposed, transversely at all abstraction levels of a digital design. In nowadays integrated circuits, it is critical the presence of intrinsic electrical mismatch due to extremely scaled geometry of MOS transistors. Because of complex requirements in manufacturing deep scaled CMOS integrated circuits, the presence of electrical mismatches is expected to increase in the future as the repeatability of the process becomes poorer. Since several PAAs countermeasures are based on the DPL principle, introduced in the previous chapter, the intra-die and inter-die variations due to electrical mismatches can impact significantly on the level of security of cryptographic processors.

To overcome issues in security applications due to electrical mismatches, authors in [33] have proposed an alternative to the classical RTZ encoding to avoid information leakage due to capacitive unbalance: the *Time Enclosed Logic* (TEL) principle. In this chapter, we propose a novel gate-level hardware countermeasure that is based on the TEL principle, allowing to relax some requirements and constraints of previous state-of-the-art logic styles used in counteracting PAAs: the *Delay-based Dynamic Differential Logic* (D³L). The novel gate-level countermeasure is intended to be standard-cell based, in order to make the design of secure devices easier and also

mismatches tolerant. Most logic styles for counteracting PAAs require the adoption of non-standard design flow, which usually requires additional effort to get a secured sign-off. The aim of the new countermeasure is to relax also this design aspect. Since most powerful logic styles are intended to be for ASIC application, the novel logic style can be implemented on both ASIC and FPGA, as it does not require custom designed cells.

The effectiveness of the novel logic style in counteracting PAAs is introduced by simulations and real experiments on FPGAs. Both dynamic and static power analysis have been taken into account, since these two side-channels are strongly related to new technologies' issues.

4.2 Issues in Implementations of DPL Logic Styles

The major problem concerning the security level in gate and logic level countermeasure using the DPL approach is related to the effective balance of the total capacitive load at each output of a dual-rail gate. If the capacitive load of each output of a DPL gate differs, there is still a possibility to mount a successful attack using the dynamic power consumption as side-channel. To better highlight this aspect, we must discuss how the capacitive mismatch impacts on the security level of a protected implementation.

The physical justification of PAAs is based on the difference in power (and in energy) consumption of CMOS gates due to data-dependency. The energy per cycle E_{ck} of a CMOS gate, defined already in Chapter 2, can be expressed as follows [93]:

$$E_{ck} = \int_0^{T_{ck}} V_{DD} \cdot i_{DD}(t) dt \rightarrow const \quad (4.1)$$

where T_{ck} is the clock period, V_{DD} the supply voltage and $i_{DD}(t)$ the instantaneous current absorption. In classic PAA, the information leakage is exploited using the dynamic power consumption. In a CMOS gate, the dynamic power consumption occurs if the output signal switches, and a current is drawn from the power supply. For example, in a CMOS inverter, we have four possible transitions, as stated in Table 3.1 and depicted in Figure 3.6. The dynamic power consumption of a CMOS inverter, as well as a generic CMOS gate, is related to charge/discharge of the load capacitor (usually the input capacitance of the next gate), as we will discuss in the following. In $1 \rightarrow 0$ output transition, the load capacitor is discharged from V_{DD} to 0V through the n-channel device. In this case, a current is drawn by the power supply line, because, around the logical threshold of the gate, both the p-channel and the n-channel device are conducting, and they provide a resistive path from the power supply line to ground. A simple model of the short-circuit power assumes that the current absorption during the switching has a triangle shape, with base t_{sc} and height I_{peak} :

$$P_{sc} = \frac{1}{T_{ck}} \int_0^{T_{ck}} V_{DD} \cdot i_{sc}(t) \cdot dt = \alpha \cdot f_{ck} \cdot V_{DD} \cdot I_{peak} \cdot t_{sc} \quad (4.2)$$

where T_{ck} and f_{ck} are the clock period and frequency respectively, α is the switching activity factor and C_L is the load capacitance of the gate.

In $0 \rightarrow 1$ output transition, the capacitive load is charged from 0V to V_{DD} through the p-channel device. In this case, the current to charge the load to V_{DD} is provided directly from the power supply line. In addition, also short-circuit current occurs during the switching, similarly to the other case. The average charging power consumed in a clock cycle is expressed as follows:

$$P_{ch} = \frac{1}{T_{ck}} \int_0^{T_{ck}} V_{DD} \cdot i_{ch}(t) \cdot dt = \alpha \cdot f_{ck} \cdot C_L \cdot V_{DD}^2 \quad (4.3)$$

Since these two transitions have different power consumptions, an adversary can recover which transition occurs without effectively evaluate the output of the CMOS inverter by monitoring its current absorption, which is the base of PAA.

As we have seen in Chapter 3, DPLs aim to achieve a constant power consumption over the clock cycle. The main requirements for each DPL cell are:

- maximize the switching activity factor α , in order to ensure that each cell provides a transition.

$$\alpha \rightarrow 1 \quad (4.4)$$

- balancing the total capacitive load $C_{tot,L}$ at each single-rail output of the cell:

$$C_{tot,L-T} = C_{tot,L-F} \quad (4.5)$$

where $C_{tot,L-T}$ and $C_{tot,L-F}$ is the total capacitance at the *true* and *false* output of the DPL cell.

These two conditions are mandatory but not sufficient to achieve a concrete resilience against power analysis.

4.2.1 Capacitive Unbalance

In a CMOS gate, the term $C_{tot,L}$ can be seen as the sum of three components:

- the internal output capacitance of the gate, C_o ;
- the parasitic capacitance of the wiring that connects the output of the gate to the next one, C_W ;

- the input capacitance of the next gate, C_i .

$$C_{tot,L} = C_o + C_W + C_i \quad (4.6)$$

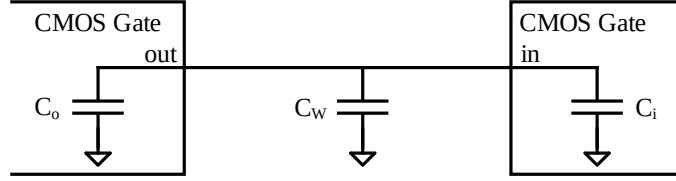


Figure 4.1. Model of the output capacitance of a CMOS gate.

In modern technologies, the deep scaled geometry of transistors, and, consequently, of a logic cell, allows to reach very small C_o . The two dominant factors in Equation 4.6 are the input capacitance of the driven gate C_i and the parasitic capacitance C_W of the wire interconnection between the two cells.

In DPL logic styles, it is required to achieve a balancing in load capacitance of *true* and *false* outputs, as indicated in Equation 4.5. In fact, capacitive mismatches impact significantly on the security level. If the condition in Equation 4.5 are not fulfilled, for example $C_{tot,L-T} > C_{tot,L-F}$, the *true* output provides an higher power consumption compared to *false* one. This condition allows the adversary to distinguish the activity of the *true* output of the cell among the *false*, since the capacitive loads are different. In recent technology, the C_i and C_o can be easily balanced during the design. However, balancing C_W is difficult to get. In fact, the very high density of devices per area in modern integrated circuits has a strong impact on the length of interconnections. The higher variability of the process makes the matching of complementary wires difficult to achieve.

4.2.2 Capacitive Imbalance Minimization on ASICs

As we have said before, capacitive mismatch has an critical relevance on the security level of a hardware implementations of cryptographic algorithms. In [148], a routing methodology for DPL styles has been introduced as the "fat wire" method to minimize mismatches on differential interconnections. In this method, which can be applied by using available EDA tools, the routing is a two-steps operation:

- The fat wire covers the differential outputs of the DPL gate, placing the centerline of the wire in the centerline between them. The width of the fat wire is set by the sum of the pitch between the normal single-ended wires and 2 times half the width of the normal wire. The pitch between the single-ended output pins of the DPL can be made larger than the minimum to reduce

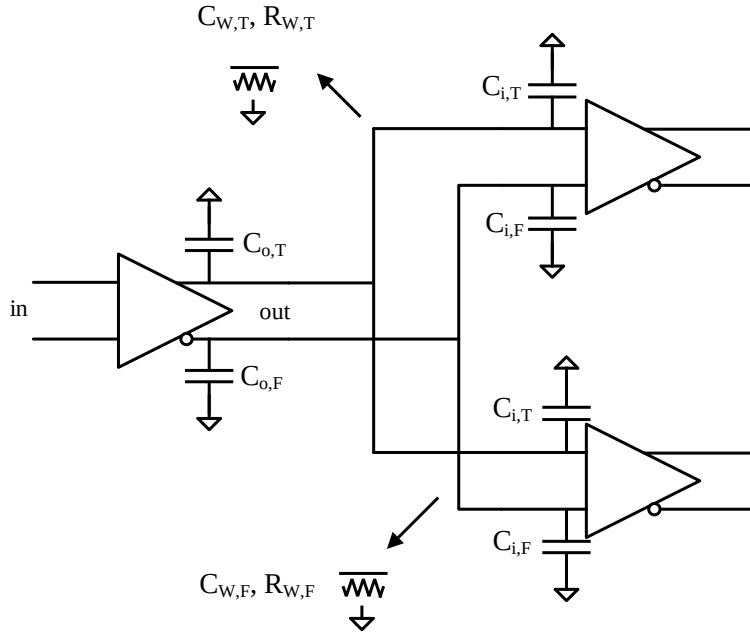


Figure 4.2. DPL styles capacitive parasitics due to C_i , C_o and C_W .

cross-talk. During the first routing, each DPL cell is routed as a single ended cell using the fat wire (see Figure 4.3(a)).

- After the place and route of the DPL cells with the fat wire, existing fat connections are splitted and separated in order to create two single-ended interconnections per each fat wire, as shown in Figure 4.3(b).

The fat wire method allows to minimize the mismatch between two complementary wires, since each connection of a DPL cell has the same distributed resistive and capacitive parasitics.

In [66], authors propose the "back-end duplication" method to overcome capacitive mismatches issues in dual-rail implementations. The main idea is to use a regular design flow on a single-ended netlist, taking care to leave enough free space on the core section of the floorplan to make possible to place and route the duplicated part of the netlist. The duplication is basically done by row. For each row used for placing, the next row is kept free for duplication. This strategy requires that each connection has to be done straight vertically, in order to get a simple duplication by right shifting of the vertical routing. Horizontal routing are left free to make turns, if and only if they remain in the routing row, to avoid shorts. As additional requirement, the duplicated netlist has to be shifted to right by one routing pitch, in order to accommodate both differential placing and routing constraints.

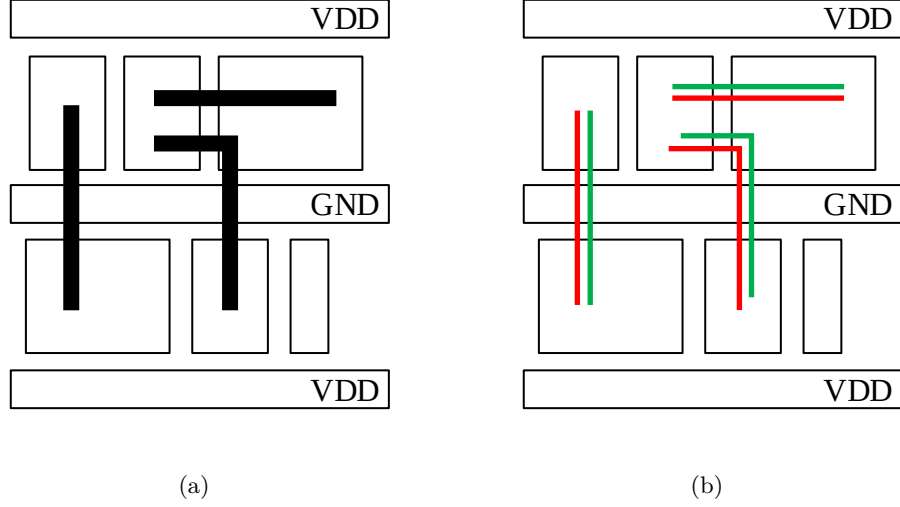


Figure 4.3. In (a) each DPL cell is routed as single-ended cell using fat wire connections. In (b) the fat wire connections are splitted and separated in *true* connection (red) and *false* connection (blue).

4.2.3 Capacitive Imbalance Minimization on FPGAs

Both "fat wire" [148] and "back-end duplication" [66] methods are intended to be for ASIC implementations, since they require a fine manipulation of the place and route steps of the design flow. If the target platform for the cryptographic application is a FPGA, other techniques can be used to minimize the mismatches due to differences in interconnections delay. In ASIC, the designer has more degrees of freedom to place and route the circuit, and also about the choice off full-custom *versus* standard-cell logic styles. In FPGA platforms, the designer has additional and implicit constraints due to the physical implementation of the FPGA. Since the FPGA is basically made of atomic cells, that contain programmable Look-up Tables and flip-flops with a pre-existing infrastructure for interconnections via switch-boxes, it can be difficult to implement PAAs resistant DPL styles, taking care of electrical mismatches. In literature, also several papers discuss about the possibility to make the place and route compliant with the needs of a perfectly balanced DPL. In [13], a FPGA version of the "back-end duplication" method is presented. In this case, the duplication is performed by routing the *true* netlist in a half of the desired region of the FPGA, and then, both placing and routing are mirrored vertically, in order to provide also the *false* implementation. This strategy allows to get a good balancing but it will not reduce other information leakage. In fact, an Electro-Magnetic Analysis (EMA) can successfully recover the secret key, because the *true* and *false* netlist are geographically far from each other, and if the EM-probe is sufficiently directional, the information leakage through electromagnetic emissions can be exploited separately. In addition, this duplication strategy requires additional area and power overhead because of the *wire swapping* cannot be used to perform the logical inversion on

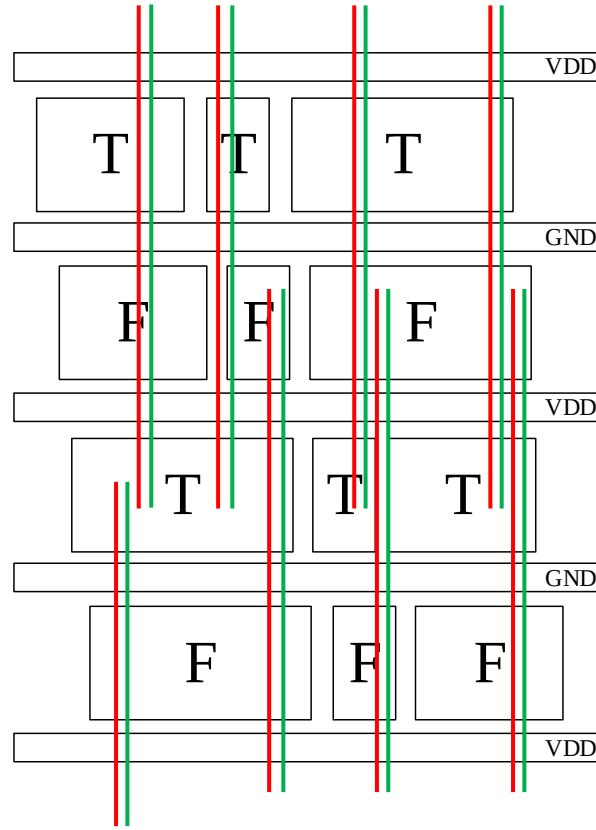


Figure 4.4. The "back-end duplication" method explained in [66].

complementary wires. In [70], authors presented a methodology to get an identical routing on Xilinx FPGA based on the set of APIs named RapidSmith. After a standard place and route of the design with the standard flow, RapidSmith allows to repair the imbalanced routing, minimizing net delay differences in complementary wires, reducing the effective information leakage due to capacitive mismatch. The set of APIs implemented in RapidSmith can be used only in Xilinx ISE, as the output .XDL file can be interpreted by Xilinx products only. Amouri *et al.* [9], propose a methodology for mesh-style FPGA similar to the "fat wire" method proposed in [148] for ASIC applications. The complementary signals are routed using the "double-wire" graph, grouping interconnections with the following properties:

- they belong to the same routing channel
- they have the same logical length
- they are routed following the same routing direction
- they are connected to more than one input of adjacent atomic cell of the FPGA

Table 4.1. RTZ voltage values for each phase of the clock signal.

Pre-Charge		Evaluation		RTZ Encoding	Logical Value
A	$\overline{A}$	A	$\overline{A}$	$(A, \overline{A})$	IN
0	0	0	V_{DD}	(0,1)	0
0	0	V_{DD}	0	(1,0)	1
0	0	V_{DD}	V_{DD}	$NULL$	<i>Invalid</i>

- they are connected to more than one output of adjacent atomic cell of the FPGA

To obtain the "double wire graph", each pair of complementary wires is converted to a single double wire, and routed properly. As in the "fat wire" method, the single "double wire" is then split in two single wires.

4.3 Time Enclosed Logic Principle and Guidelines

The *Time Enclosed Logic* (TEL) principle has been introduced in [33] aiming to reduce the sensibility of the security level of cryptographic devices to electrical mismatches. As we have said before, capacitive mismatches in security applications when DPL styles are adopted impact critically on the security level of the implementation, as they assess the information that can still be exploited through dynamic power consumption. In *Time Enclosed Logic*, the datum is encoded in the delay domain instead of the differential level domain. As we will discuss in this chapter, TEL encoding allows the designer to relax routing constraints for DPL implementations.

4.3.1 Assumption on the Adversary Model in TEL signaling

Before explaining in detail how the TEL protocol works, we have to state what is the main assumption on the model of the adversary used in this context. In the design of a secure implementation, it is needed to make assumptions on the adversary that the designer could expect. This model has to take into account the real attack capability that the adversary could have in extracting secret information from the device. The use of the SPICE level simulations is very meaningful in preliminary assessment of the information leaked by the device during the design step [72]. SPICE level simulations are able to provide a useful tool to evaluate the information leakage, allowing the designer to estimate the effectiveness of the countermeasure in counteracting PAAs. Nevertheless, such high-accuracy simulations allow the designer to evaluate the capability of the *Perfect Adversary* to extract information from the hardware implementation. The *Perfect Adversary* model has specific properties, that can be resumed as follows:

- infinite bandwidth in collecting physical emissions (e.g. power consumption);
- infinite storage capability.

The *Perfect Adversary* model is able to provide a conservative approach in designing and evaluating secure applications. However, this model does not hold in practice [93]. In fact, it is impossible to get infinite bandwidth in measuring the physical emission. The entire measurement equipment, and the device itself, provides a limited bandwidth, which can be able to filter off information leaked through power consumption. The DSO used to collect and digitize power samples has an analog front-end, which is limited in bandwidth, and also the Analog-to-Digital converter inside the instrument has limited time resolution and number of bits to represents the sampled data. More demanding are these limits, higher will be the cost of the instrument. In addition, the storage capability is always limited, which reduces the possibility to filter-off noisy component on the collected data. In the TEL signaling, the assumption on the adversary model are more realistic. The main assumption behind the practical application of TEL signaling is that **the adversary has limited resources in time resolution and bandwidth** [93]. As we will discuss further, this factor impacts critically on the possibility to recover information on implementations that use TEL signaling and TEL-compatible logic styles to protect information, since it is a delay-based time encoding.

4.3.2 The TEL Protocol

As we have discussed before, the *Time Enclosed Logic* is a different signaling methodology and protocol which differs from the classic RTZ, used in DPL styles. The main differences of the TEL with RTZ is that the datum is encoded in the time-domain instead of magnitude-domain. In TEL signaling, the differential signal is routed by to complementary wires, as in RTZ. The signaling is divided in three phase during the clock cycle:

- pre-charge phase t_{pre} ;
- evaluation phase t_{eval} ;
- post-evaluation phase t_{post} .

As it is clear, we have that the sum of the three phases is equal to the clock cycle period:

$$t_{ck} = t_{pre} + t_{eval} + t_{post} \quad (4.7)$$

During the pre-charge phase of duration t_{pre} , both wires of a complementary pair assume the same value, for example '0'. In this phase, all transistors are pre-charged

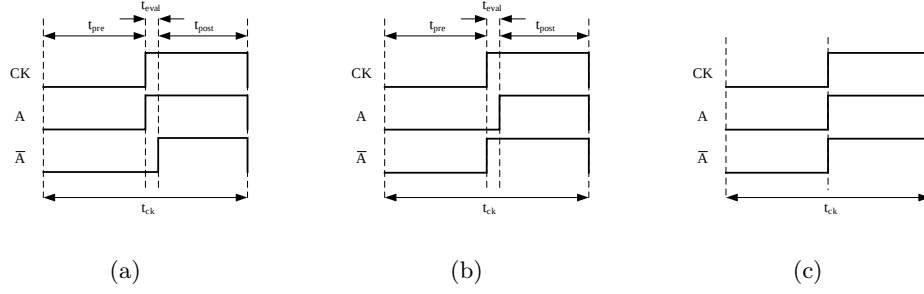


Figure 4.5. TEL protocol signaling for the logical '1' (a), logical '0' (b) and NULL logic value (c) (not in scale).

Table 4.2. TEL voltage values for each phase of the clock signal.

Pre-Charge		Evaluation		Post-Evaluation		TEL Encoding	Logical Value
A	$\bar{A}$	A	$\bar{A}$	A	$\bar{A}$	$(A, \bar{A})$	IN
0	0	0	V_{DD}	V_{DD}	V_{DD}	(0,1)	0
0	0	V_{DD}	0	V_{DD}	V_{DD}	(1,0)	1
0	0	V_{DD}	V_{DD}	V_{DD}	V_{DD}	NULL	Invalid

to '0', and the complementary output of each TEL-compatible cell is '0'. Thus, the entire combinational path is pre-charged and all internal capacitance of each gate is at the same value. During the evaluation phase, the complementary pair assumes its differential value, and the logic net evaluates the results. After the evaluation phase, all the signals of the net are forced to logic value '1' during the post-evaluation phase t_{post} . The need of a third phase allows to avoid information leakage due to memory effect, which is typical of some standard-cell based logic style using the RTZ encoding [34]. It has to be noted that the duration of evaluation phase t_{eval} is much shorter than both pre-charge and post-evaluation:

$$\begin{cases} t_{eval} \ll t_{pre} \\ t_{eval} \ll t_{post} \end{cases} \quad (4.8)$$

The signaling used in TEL protocol is depicted in Figure 4.5(a) and 4.5(b), respectively for the logical '1' and '0'. For the invalid logic value, shown in Figure 4.5(c), both complementary wires have the same value throughout the entire clock cycle. A resume of the value of both wires in each phase for each logical value, is reported in Table 4.2.

Looking at Figure 4.5 and Table 4.2, a differential signal $(A, \bar{A})$ in the TEL domain can assume three possible states, and the logical value is encoded as follows. If the single-ended rail $\bar{A}$ reaches the post-evaluation voltage before the single-ended rail A, the corresponding logical value is '0'. On the contrary, if the single-ended rail A reaches the post-evaluation voltage before the single-ended rail $\bar{A}$, the corresponding

logical value is '1'. If both wires are charged to the post-evaluation voltage at the same time, the logical value is NULL. It has to be noticed that the TEL encoding evaluates only in t_{eval} , which is a small fraction of the semi-period of the clock signal $t_{ck}/2$, according to Equation 4.8. In addition, TEL data encoding has the property of *functional completeness*. The completeness is the property of logic circuit to be represented by symbolically complete logic expression, and a set of Boolean function is *functionally complete*, if and only if all other Boolean functions can be constructed from this set [58]. In TEL encoding, the differential datum is coded into a mutually exclusive value assertion domain, and only one single-ended wire in a TEL signal is asserted during the evaluation phase. In order to make the Boolean logic symbolically complete, the NULL value is added to the value domain, as shown in Table 4.2, ensuring the completeness of the input set. The completeness of the input set allows to automatically synchronize the signals at the output of a combinational path, because a gate asserts data only when a complete set of input data values is presented at its input [58]. In fact, each gate acts as a synchronization node, and this property has been intensively used to design asynchronous logic [58] and *delay insensitive* circuits [87] [30]. The most important property of the TEL encoding and protocol is that the relevant information is enclosed in the duration of the evaluation phase t_{eval} , and all the information that is leaked by the hardware implementation can be captured only during the time window t_{eval} . As we have mentioned before, the TEL encoding assumes that the adversary has limited resources in terms of time resolution and bandwidth for monitoring the power consumption of the cryptographic device. If the sampling period of the DSO is greater than t_{eval} , no relevant power samples can be captured and the adversary will not be able to recover information from the device's consumption anymore. In order to clarify this property of TEL-based circuits, let us introduce an example. Let us suppose that the adversary has a DSO with sampling rate 2GS/s, which is able to capture signal in the bandwidth from DC to 1GHz (due to Nyquist's theorem), the minimum evaluation phase duration t_{eval} to prevent PAA is 500ps, that can reasonably be achieved using nowadays technologies. This simple consideration can be enforced by the presence of other on-chip or on-board low-pass effects, which can filter off relevant information.

4.3.3 TEL-based Cell Templates

The property of completeness of the TEL encoding requires that complementary signals have to propagate with reciprocal time delays equal to the evaluation phase duration t_{eval} . Any mismatch on propagation times can be balanced by exploiting the property of completeness. In RTZ encoding, each complementary pair has one complete commutation in a clock cycle, to maximize the switching activity factor at gate-level. In TEL encoding, this property is applied on each single-ended signal of a complementary pair, ensuring that each signal has one and only one complete commutation cycle in a clock cycle. In the previous chapter, we have discussed about the WDDL [147], as a widely used DPL logic style which can be implemented using standard-cells. The WDDL uses the RTZ encoding. The aim of WDDL is to satisfy the condition expressed in Equation 3.20. Re-arranging Equation 3.20, we have:

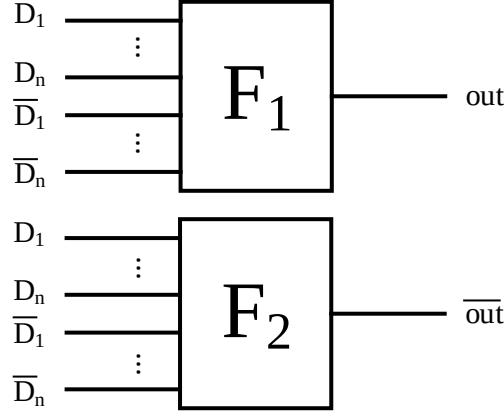


Figure 4.6. Template of a TEL-compatible gate using two independent circuit for the complementary function F_1 and F_2 .

$$\begin{aligned} out &= F_1(D_1, D_2, \dots, D_n) \\ \overline{out} &= F_2(\overline{D_1}, \overline{D_2}, \dots, \overline{D_n}) \end{aligned} \quad (4.9)$$

Asserted signals are all connected to F_1 , while complementary input signals are all connected to F_2 . The functions F_1 and F_2 are compatible with RTZ encoding if and only if they are *positive monotonic* Boolean functions [93]. It has to be noted that functions F_1 and F_2 in WDDL are implemented using different logic compounds. This approach in designing secure devices leads to a mismatch-sensitive implementation. In fact, WDDL may suffer from capacitive and timing mismatches strongly, since the two logic functions could offer different C_o values and different propagation times. In TEL-compatible gates, the property of completeness requires redundancy on the input vector, and equations shown in Equation 4.9 and Equation 3.20 have to be modified to take into account this requirement. The new set of equation to satisfy the requirement on the completeness is shown in the followings:

$$\begin{aligned} out &= F_1(D_1, D_2, \dots, D_n, \overline{D_1}, \overline{D_2}, \dots, \overline{D_n}) \\ \overline{out} &= F_2(D_1, D_2, \dots, D_n, \overline{D_1}, \overline{D_2}, \dots, \overline{D_n}) \end{aligned} \quad (4.10)$$

Each TEL-compatible gate has to satisfy Equation 4.10. In this case, the *positive monotonic* property holds and it provides the correctness of the pre-charge and post-evaluation values. In fact, during the pre-charge, when the input values $(D_i, \overline{D_i})$ (with $i = 1, \dots, n$) are set to '0', the output values of F_1 and F_2 are '0'. In the post-evaluation, all input values are set to V_{DD} , and the output values are set, in turns, to V_{DD} . In TEL encoding, all signals exhibit a $0 \rightarrow 1$ and $1 \rightarrow 0$ transition within a clock cycle, making the switching behavior of TEL-compatible gates *strictly positive monotonic*. This property has as an important consequence on how a TEL-compatible gate has to be designed. In fact, each compound of a TEL-compatible

gate can be designed using the NAND function, and since the NAND function is the minimum complete function, it can be adopted to design a self-synchronized TEL-based gate.

Once the property and functional requirements of the TEL principle and cell template have been defined, it is possible to design a logic style based on the adoption of this encoding scheme, as we will discuss further in this chapter.

4.3.4 Power Analysis Considerations on TEL-compatible Logic

The TEL principle discussed previously has been proposed to overcome security issues due to electrical mismatch. In this paragraph, dynamic power consumptions of a TEL-compatible gate and of a DPL-RTZ gate regarding output transitions are evaluated and compared. In Table 4.3, a summary of the dynamic power consumption of both encoding schemes is reported. Regarding the timing paradigm reported in Table 4.2, a TEL-compatible gate shows three peaks in dynamic consumption, as the signaling in TEL encoding takes into account three phases. The first peak occurs at the pre-charge phase; each single-ended signal is set to 0V, and all parasitic capacitors are discharged. The other two peaks occur at the evaluation and post-evaluation phase, which, nominally, are separated by t_{eval} . In the TEL encoding, each capacitance is charged and discharged once in the clock cycle [26]. Since the consumption of the gate depends directly on the sum of the consumption of the two complementary halves, and given $C_{L1} \neq C_{L2}$ due to automatic routing, the total power consumption in a TEL-compatible gate is balanced within the clock cycle. It has to be noted that in RTZ encoding, the switching activity factor is balanced at gate level, ensuring that in each gate, seen as *macro-blocks*, occurs a transition per clock cycle. At this level of abstraction, it is not possible to deal with the unbalancing of the load capacitors, as can be seen in Table 4.3. In the TEL encoding, the switching activity is not balanced only at differential level, but **it is also balanced at single-ended level**, providing that each signal in a gate behaves like the clock signal. Hence, the TEL protocol allows to tolerate capacitive mismatches, as reported in Table 4.3, providing the balancing throughout the clock cycle and making the total dynamic power consumption to be independent from differences of load capacitors. Since in a TEL-compatible gate the total power consumption depends on the sum of the load capacitors, the TEL principle is able to make the consumption independent from both input vectors and electrical mismatches.

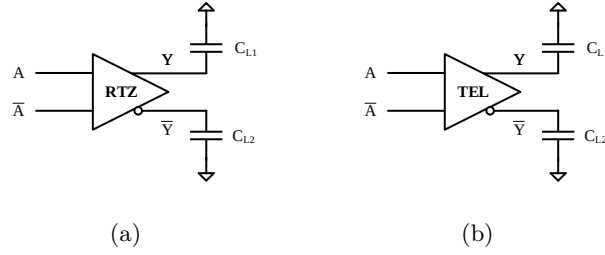
Since the capacitive unbalance depends strongly on the routing process, we define the *Mismatch Factor* (MF), introduced in [66], to indicate the degree of unbalance of the differential interconnections as the ratio of the maximum and the minimum differential load capacitance:

$$MF = \frac{C_{L,max}}{C_{L,min}} \quad (4.11)$$

The capacitive unbalance, and consequently the MF, relies on the complexity

Table 4.3. Dynamic power consumption for a TEL-compatible and for a DPL (using RTZ encoding) inverter, assuming unbalanced load.

	$(Y, \bar{Y})$	1 st Semiperiod		2 nd Semiperiod		$P_{\text{dyn}}^{1^{\text{st}}}$	$P_{\text{dyn}}^{2^{\text{nd}}}$	$P_{\text{dyn, TOT}}$
		Y	$\bar{Y}$	Y	$\bar{Y}$			
RTZ	(0,1)	$0 \rightarrow 0$	$0 \rightarrow 1$	$0 \rightarrow 0$	$1 \rightarrow 0$	0	$V_{\text{DD}}^2 C_{\text{L2}} f_{\text{ck}}$	$V_{\text{DD}}^2 C_{\text{L2}} f_{\text{ck}}$
	(1,0)	$0 \rightarrow 1$	$0 \rightarrow 0$	$1 \rightarrow 0$	$0 \rightarrow 0$	$V_{\text{DD}}^2 C_{\text{L1}} f_{\text{ck}}$	0	$V_{\text{DD}}^2 C_{\text{L1}} f_{\text{ck}}$
TEL	(0,1)	$0 \rightarrow 1$	$0 \rightarrow 1$	$1 \rightarrow 0$	$1 \rightarrow 0$	$V_{\text{DD}}^2 C_{\text{L1}} f_{\text{ck}}$	$V_{\text{DD}}^2 C_{\text{L2}} f_{\text{ck}}$	$V_{\text{DD}}^2 (C_{\text{L1}} + C_{\text{L2}}) f_{\text{ck}}$
	(1,0)	$0 \rightarrow 1$	$0 \rightarrow 1$	$1 \rightarrow 0$	$1 \rightarrow 0$	$V_{\text{DD}}^2 C_{\text{L1}} f_{\text{ck}}$	$V_{\text{DD}}^2 C_{\text{L2}} f_{\text{ck}}$	$V_{\text{DD}}^2 (C_{\text{L1}} + C_{\text{L2}}) f_{\text{ck}}$

**Figure 4.7.** RTZ (a) and TEL-compatible (b) inverter.

of the layout, and how the routing generation is carried out by the specific tool. Generally, if no additional routing constraints are given, automatic EDA provides high values of the MF, since the layout is not optimized for secure applications.

4.3.5 Timing Constraints of TEL-based Circuits

In the following paragraphs, we introduce the timing constraints for TEL-based circuits. It must be noted that according to the timing diagram reported in Figure 4.5 and Table 4.2, the synchronization scheme is *semi-synchronous*. The pre-charge phase is perfectly synchronous with the clock signal's falling edge. On the contrary, the post-evaluation phase is not strictly synchronous with the clock signal, since the duration of the evaluation phase is nominally t_{eval} , but it can vary along the combinational path, as we will discuss in the followings. At the output of converter circuitry, from the single-rail CMOS domain to TEL domain, the evaluation phase has its nominal duration, which is equal to t_{eval} . TEL-compliant differential signals propagate throughout the pipeline combinational path, and they are evaluated at different time instants. The delay of each gate cannot be equal to the nominal t_{eval} , due to non-ideal behavior of logic cells in TEL-based circuit. The variation of the t_{eval} along the combinational path is called *fluctuation effect*, which limits the number of logic stages between two sequential cells in a pipeline stage. In order to preserve the security level of the implementation and to avoid timing violations, a TEL-compatible circuit has to meet the following requirements:

1. t_{eval} can decrease at the output of a combinational cell (or path), but cannot

increase:

$$t_{eval,CL} < t_{eval} \quad (4.12)$$

2. $t_{eval,CL}$ at the output of a combinational cell must be greater than the setup-time of the flip-flop, in order to avoid timing violations:

$$t_{eval,CL} > t_{setup} \quad (4.13)$$

3. The nominal t_{eval} has to be regenerated at the output of each flip-flop in the TEL domain (neglecting the propagation time of the flip-flop):

$$t_{FF} = t_{eval} \quad (4.14)$$

Equation 4.12-4.14 represent the timing constraints of a TEL-based circuit.

The *propagation delay* $\Delta\delta$ in a TEL-based circuit is defined as the difference of the $t_{eval,IN}$ of the input and the $t_{eval,OUT}$ of the output:

$$\Delta\delta = t_{eval,IN} - t_{eval,OUT} > 0 \quad (4.15)$$

We define the propagation time of the critical path $t_{eval,CP}$ as the maximum variation of t_{eval} along a combinational path. It is calculated as the difference between the $t_{eval,1}$ at the input of the first gate (which is the nominal t_{eval}) and the minimum delay $t_{eval,CL}$ at the output of the combinational path:

$$\Delta t_{eval,CP} = \max [t_{eval} - t_{eval,CL}^{out}] = t_{eval} - \min t_{eval,CL} \quad (4.16)$$

The propagation time of the critical path is strongly related to the number of stages between two flip-flops, and it can be calculated as follows:

$$\Delta t_{eval,CP} = \sum_{i=1}^N \Delta\delta_i = N \cdot \overline{\Delta\delta} \quad (4.17)$$

where N is the number of stages in a path, and $\overline{\Delta\delta}$ is the average propagation time of TEL combinational gates in a given technology. The *setup time* of the TEL flip-flop is defined as the minimum propagation delay at the output of the critical path (which is the input of the flip-flop) that get the sequential element to correctly sample the TEL signal. Combining Condition 2 with Equations 4.16 and 4.17, we can define the timing constraint for the critical path:

$$t_{eval,CP} = t_{eval} - \Delta t_{eval,CP} = t_{eval} - N \cdot \overline{\Delta\delta} \geq t_{setup} \quad (4.18)$$

It has to be noticed that the adopted technology set the average propagation delay, which in turns limits the number of stages between two flip-flops, according to Equation 4.18:

Table 4.4. Road map for timing performances of TEL-compatible circuits for different technologies.

Technology [nm]	$t_{eval,CL}$ [ps] TEL AND/NAND	t_{setup} [ps]	$t_{eval,MIN}$ [ps]
90	100	180	380
65	50	90	190
45	25	45	95
28	12	20	48

$$N_{MAX} = \frac{t_{eval} - t_{setup}}{\Delta\delta} \quad (4.19)$$

As previously mentioned, the nominal evaluation phase duration t_{eval} is chosen by the designer, accordingly to the level of security he/she wants to reach. This choice has to met the specific technology limit, imposing the minimum t_{eval} and the maximum N . In addition, we must consider that we must meet Condition 2, and considering the propagation delay of a minimum two combinational gates (e.g. two AND/NAND gates), we can calculate $t_{eval,MIN}$ as follows:

$$t_{eval,MIN} = 2 \cdot t_{eval,CP} + t_{setup} \quad (4.20)$$

Since the technology process used to implement the cryptographic device indirectly set the lower bound for $t_{eval,MIN}$, it is possible to consider Table 4.4 as a road map for timing performances of TEL-compatible circuits considering the technology process node. At each new technology process, the propagation delay is expected to be halved, as well the setup time t_{setup} , and, consequently $t_{eval,MIN}$. This analysis is useful in order to make the assumption on the upper bound of the security level that the adversary can reach setting the nominal t_{eval} as small as possible with the given number of stage of the design.

4.4 Full-custom DDPL/iDDPL Logic Style

In the previous section, we have defined the background of the *Time Enclosed Logic* principle for counteracting PAAs. In the TEL encoding, the diversities in power consumption due to electrical mismatches are confined in a very short time window, which corresponds to the duration of the evaluation phase t_{eval} . Shorter is the evaluation phase, higher must be the sampling rate and the bandwidth of the measurement equipment to capture the information leakage contained in the power consumption even in the presence of capacitive imbalances. This property defines two demanding constraints for both the designer and the attacker, under the assumption of *Non Perfect Adversary* model.

Looking at the property of TEL encoding discussed in the previous section, TEL-compatible logic styles can be designed following different approaches and targets. There are two leading requirements on the technology side of the secure implementation:

- the target platform;
 - FPGA-compatible;
 - ASIC only.
- the synchronization scheme.

Regarding the target platform, there are two main approaches in designing a new logic styles. If the template of logic style can be implemented using only pre-designed gates, connected to provide the desired functional and electrical behavior, or by designing new gates from scratch. If the new logic style can be implemented using standard-cells and no custom logic is needed, the target platform can be (in general) both FPGAs and ASICs. The ASIC-only solution with custom designed cells is adopted when standard-cell approach is not suitable for the implementation of the template.

Regarding the synchronization scheme, the design of a new logic style can require or not a special routing for synchronization signals throughout the combinational path, in order to maintain its timing closure. In the latter case, the design has to be able to maintain the timing closure on its own, in accordance with the TEL principle for the signaling in a clock cycle due to pre-charge $\rightarrow$ evaluation $\rightarrow$ post-evaluation sequence.

In literature, full custom designs for implementing TEL principle at gate-level has been proposed. In [33], authors introduce the TEL principle and propose a first logic family TEL-compatible. This new logic family, named *Delay-Based Dual-rail Pre-charge Logic* (DDPL), has been demonstrated to be less sensitive to capacitive mismatches compared to DPL logic styles, such as SABL [144] and WDDL [147]. Authors in [33] presented a full custom template to implement DDPL gates. In Figure 4.8(a)-4.8(b), the AND/NAND and XOR/XNOR gate in DDPL style are shown. In this preliminary version of the DDPL logic style, the pre-charge voltage is V_{DD} , while the post-evaluation voltage is 0V. The evaluation phase takes place at the falling edge of the clock signal, instead of the rising edge. The DDPL is intended to be implemented in ASIC, and in this case, the synchronization scheme requires that each combinational gate is connected to the clock signal CK . When CK is high, the output of each gate pre-charge to V_{DD} , and every pull-up network is open. During the evaluation phase, the differential output is evaluated. When CK is low, the pull-down network goes open and the differential output $(Y, \bar{Y})$ goes to (0,0). Since all the signals are set to 0V, all output signals in each gate are set to 0V, satisfying all TEL requirements.

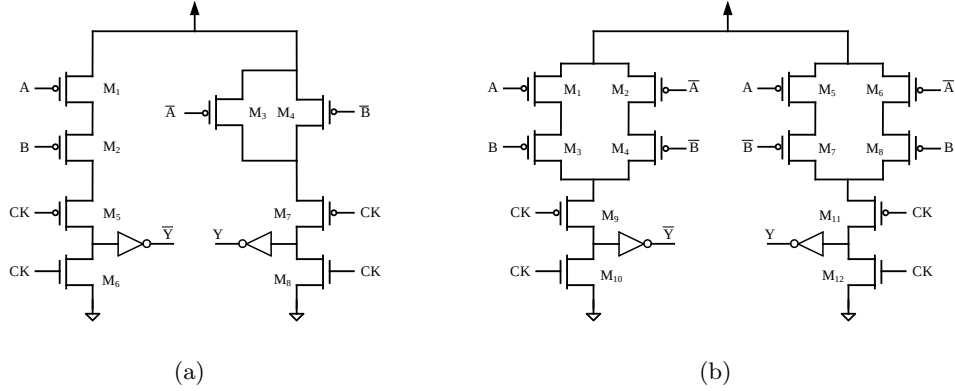


Figure 4.8. DDPL p-type AND/NAND gate (a) and DDPL p-type XOR/XNOR gate (b).

4.4.1 Limitations of the DDPL Style

The DDPL logic style presented in [33] has been the first attempt to design a new template that can be compliant with the TEL principle, aiming to balance the energy per cycle and enclosing the information leakage due to electrical mismatches in a narrow time window. Although it can be considered the first example of TEL-compatible logic style, it suffers from a critical problem which is common in PAAs' literature, as we will discuss in this section.

The DDPL gates in Figure 4.8(a)-4.8(b) are often referred to DDPL p-type gates, since evaluation networks are implemented with p-channel devices. As briefly mentioned above, this implementation has a larger area overhead compared to the DDPL n-type, as we will discuss further, due to the fact that p-channel devices have to be designed larger than n-channel, to overcome the reduced carrier mobility. Let us analyze the AND/NAND gate, as depicted in Figure 4.8(a). The evaluation network is composed of four transistors, in order to implement the AND/NAND function. We must notice that the gate can propagate its logical output value without waiting that all input signals are valid. In fact, the *evaluation depth*, which in a p-type gate corresponds to the number of transistor in series between the supply line and the output internal capacitance, is not the same for the two branches. The evaluation depth for the NAND side of the gate is 3 transistors (M_{1,2,5}), while for the AND side, we have two transistor (M_{3/4,7}). This will cause internal unbalance of propagation times of the gate. In fact, the AND side will behave as a OR gate, making the gate internally unbalanced. Early propagated transitions provide data-dependent power consumption, which the adversary can exploit to recover secret information from the device [29]. The DDPL gates in Figure 4.8(a)-4.8(b) are often referred to DDPL p-type, since evaluation networks are implemented with p-channel devices. In general, this implementation has a larger area overhead compared to the DDPL n-type, as we will discuss further, due to the fact that p-channel devices have to be designed larger than n-channel, to overcome the reduced carrier mobility. Let us analyze the AND/NAND gate, as depicted in Figure 4.8(a). The evaluation network

is composed of four transistors, in order to implement the AND/NAND functions. We must notice that the gate can propagate its logical output value early, without waiting that all the input signals are valid. In fact, the *evaluation depth*, which in a p-type gate corresponds to the number of transistor in series between the supply line and the output internal capacitance, is not the same for the two branches. The evaluation depth for the NAND side of the gate is 3 transistors ($M_{1,2,5}$), while for the AND side, we have two transistor ($M_{3,4,7}$). This will cause internal unbalance of the timing propagation of the gate. In fact, the AND side will behave as a OR gate, making the unbalanced internally. The early propagated transition implies a data-dependent power consumption, which can be exploited by the adversary [29].

This effect is called *early evaluation* (EE). The EE is very critical in DPL implementations [139], because it produces a dependency of the current absorption on the arrival times of the input signals. From the adversary point of view, the EE helps to maintain high the correlation between power consumption and processed data, vanishing the presence of PAAs countermeasure. In literature, the effect of EE has been evaluated for DPA-resistant logic. In [86], authors present a study of the effect of the EE on SABL logic on the current absorption behavior. They demonstrated that the data-dependency of the evaluation time of a combinational net regarding the input vectors has a strong impact on the power consumption, which can be exploited to recover sensible information, also in the presence of DPL countermeasure. In [23], Bhasin *et al.* remark the vulnerability of dual-rail pre-charge logic due to EE effect. It has been demonstrated that most of the information leaked by a WDDL implementation is given by the data-dependency of the early evaluation effect. In fact, even if the WDDL is built upon a monotonic positive Boolean function set, it is possible to observe EE, and thus, recovering the information processed within the device. Moreover, they propose also a technique to reduce, at least halving, the information leaked through dynamic power consumption due to EE effect. Modifying the truth table of each function, and making the combinational function to evaluate only when the input signals are in a "VALID" state, the EE can be reduced as well as the information leaked due to non-perfect timing matching between signals. In [149] and [86] also the SABL style has been enhanced with a EE-free pull-down template, that allows to easily balance timing mismatches in generating output values. In the first formulation of the SABL template [144], the pull-down network provides unbalanced paths for output load capacitance. The *Enhanced Fully Connected DPDN* SABL allows the designer to make the evaluation depth of the pull-down network equal for every discharge event. A formalization of the fully connection method adopted in [149] and [146], adopting the *Boolean Decision Diagram*, is presented in [79].

4.4.2 Improved DDPL (iDDPL)

As we have discussed in the previous section, the DDPL is able to balance the energy per cycle, by means of the TEL encoding. Although, the DDPL exhibits information leakage due to intrinsic unbalancing in timing mismatches internally at

monotonic positive gates, such as the AND/NAND or the OR/NOR. The imbalances in evaluation depth of the *true* and *false* evaluation network, makes the instantaneous current absorption dependent from the arrival times of data. This aspect can be determinant and critical from a security point of view, since it helps to maintain high the correlation with the processed data. In addition to that, the first proposal for the DDPL style makes use of p-type cells. The p-type approach implies a larger area overhead, due to larger transistor compensating the reduced carrier mobility in p-channel devices.

In order to overcome these issues, an improved version of the DDPL proposed by Bongiovanni *et al.* in [29]: the *Improved DDPL* (iDDPL). The iDDPL, similarly to its predecessor DDPL, is a full custom logic styles, which is compatible with TEL requirements and that can be optimized at transistor-level to counteract power analysis. Both DDPL and iDDPL can be considered as successors of the *Three-phase DPL* (TDPL) [34]. The TDPL has been proposed basically as improvement of the SABL style, in order to enhance the robustness against PAAs also in the presence of electrical mismatches. Authors in [34] extended the classic RTZ paradigm with a *post-charge* phase, which is functionally equivalent to the post-evaluation phase in the TEL encoding. The purpose of this additional phase is to balance the energy per cycle even in the presence of capacitive unbalances. The TDPL adds to SABL template a third transistor in order to implement the three-phase signaling, as shown in Figure 4.9(a) for a TDPL inverter gate. During the *charge* phase, both complementary wire are set to 0V, and both *charge* and *discharge* signals are low. The output load capacitors are charged to V_{DD} by transistors $M_{p1,p4,p5}$. When the *charge* signal goes high, also the *eval* signal goes high, the input signals are evaluated through the pull-down network, which is now connected to ground by the foot-transistor M_{n3} . At the end of the *evaluation phase*, the signal *discharge* is set active and *eval* signal is set to low. At this point, the main pull-up transistor M_{p5} behaves like an open circuit, and the output load capacitors are forced to discharge through transistors $M_{n7,n8}$. A timing diagram of the TDPL inverter is shown in Figure 4.9(b). The main drawback of a TDPL implementation is that at least two synchronization signals has to be routed, which implies a larger area overhead to reduce the cross-talk effects. In addition to that, the presence of a complex synchronization scheme implies more stringent timing requirements.

The iDDPL has been proposed to overcome issues in robustness of the DDPL style, since the level of security may be reduced by the presence of the early evaluation effect. The aims of the iDDPL are:

- balancing the energy per cycle;
- instantaneous power consumption independent from the input vectors;
- enclosing data-dependent leakage in t_{eval} .

The circuit in Figure 4.10(a) shows a iDDPL inverter/buffer. As we can see, it is quiet similar to the TDPL buffer/inverter, but it does not needs multiple synchronization signals, and less devices are used to design a gate. The synchronization

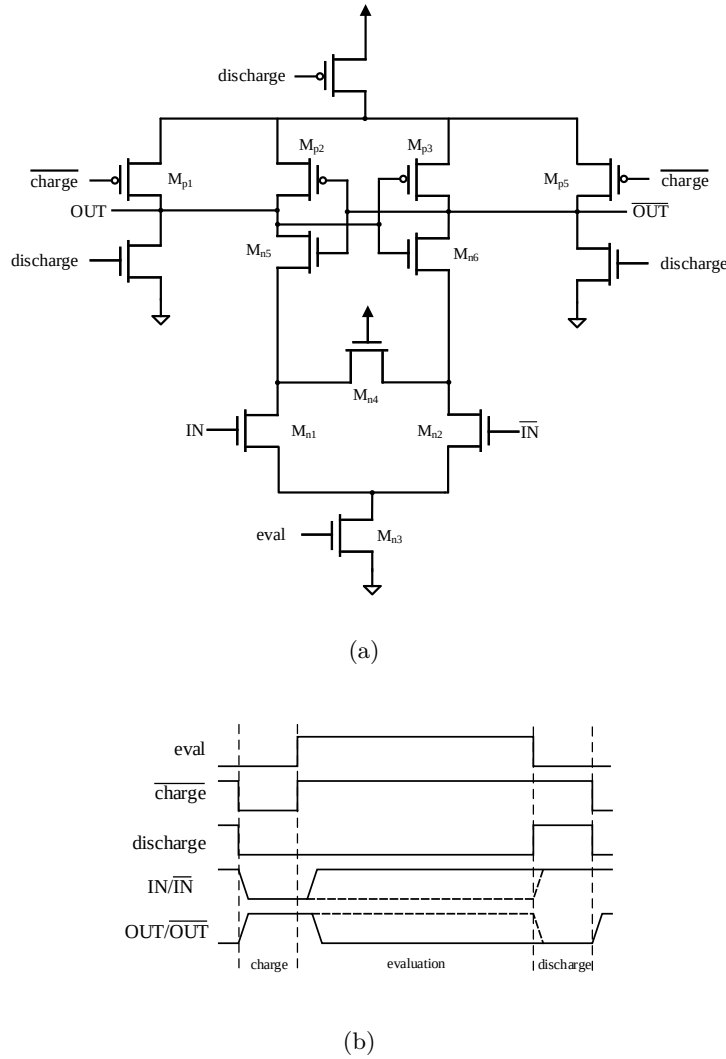


Figure 4.9. TDPL inverter gate (a) and timing diagram (b).

scheme in iDDPL requires only the routing of the clock signal CK , in order to maintain the timing correctness along combinational paths. The absence of multiple signal for synchronization impacts strongly on the silicon area and on the power overhead, since the number of devices per gate has been reduced as well.

Let us analyze the iDDPL inverter/buffer shown in Figure 4.10(a). The pull-down network has a direct connection with the ground line, saving the space due to foot-transistor in TDPL. When CK is low, the combinational logic is in pre-charge phase, and input and output signals of each gate are set to 0V, because of transistors $M_{p1,2}$ force the inputs of the inverters to V_{DD} . During the evaluation phase, the complementary signals at the input assume their TEL value after the rising edge of CK . Assuming $(A, \overline{A}) = (1, 0)$, as shown in the timing diagram in Figure 4.10(b), the output signal Y is charged after $\overline{Y}$, providing the correct TEL value $(Y, \overline{Y}) = (0, 1)$

at the output of the gate. After the evaluation, both input signals are charged to V_{DD} , and consequently, both output lines are set to V_{DD} . The two transistor $M_{p3,4}$ are necessary to remove memory effect due to internal capacitance of the pull-down network, during the pre-charge phase. At the beginning of each pre-charge phase, the upper nodes of the pull-down network are both charged to V_{DD} ; this approach limits the information leakage due to non perfect balancing of the two differential side of a iDDPL gate due to internal mismatch. The presence of these two additional transistor respect to the DDPL combinational template, allows to achieve a better balancing in the energy per cycle, making the consumption of each gate throughout the clock cycle independent from the input pattern.

As discussed in Section 4.3.2, the TEL encoding requires *strictly positive monotonic* behavior of a gate, in order to achieve the completeness. The property of completeness requires that each compound of a TEL-compatible gate can be designed using a NAND *approach*. In [29], the iDDPL AND/NAND gate has been designed using the NAND *approach*, as shown in Figure 4.11. The presence of additional transistors in the evaluation network provides an additional benefit. They allow to equalize the resistive path during the evaluation phase, avoiding, de facto, the occurrence of the early evaluation effect. This approach, similarly to the fully connected SABL in [149], allows to balance the propagation times for each possible input pattern [29].

4.5 D³L - Standard Design Flow for Secure Applications

In the previous section, we have discussed about the application of the TEL principle with the DDPL [34] and iDDPL [29] logic styles. Both logic styles have been conceived to be implemented in a custom ASIC, using full-custom or semi-custom design flow. In security applications, designers have to make huge effort to adopt a *secure design flow*, since several aspects of the design and implementation impact critically on the final level of security of the cryptographic device. In this section, we introduce a novel logic style which is TEL-compatible and does not require full/semi-custom design flow and it relaxes some constraints respect to other state-of-the-art gate-level countermeasures. The novel logic style, which is based on a pure standard-cells approach, is intended to be compliant with both FPGA and ASIC applications, making it more flexible than previous TEL-based logic styles. The validity and the robustness of this new family is supported with simulated and practical evaluation on FPGAs, using only standard design flow, to remark the strong reduction in design effort compared to other gate-level countermeasures that imply standard-cells to counteract PAAs.

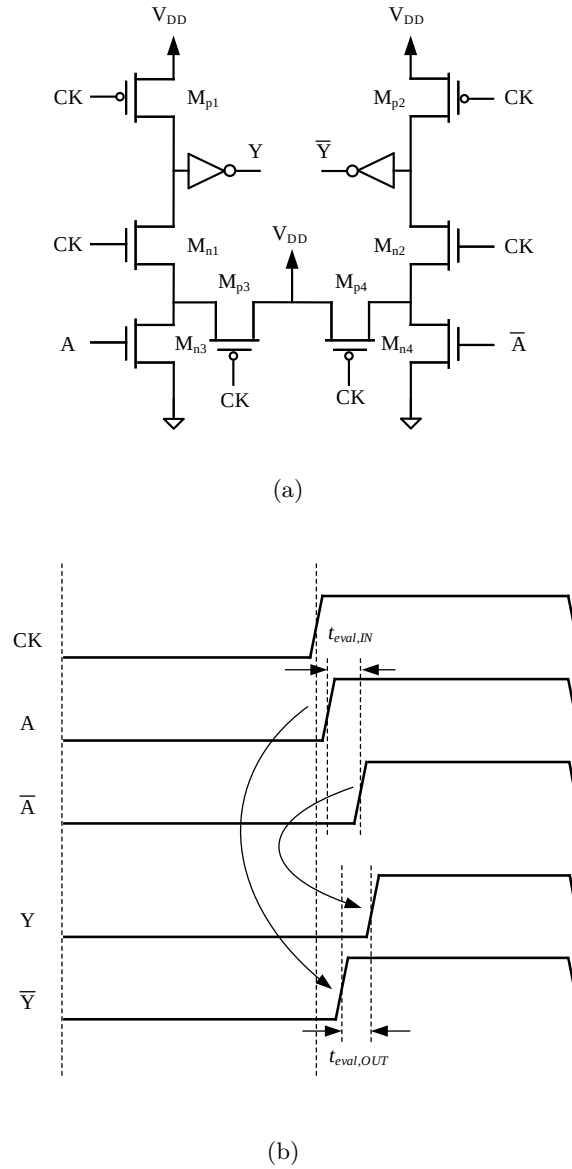


Figure 4.10. In (a), iDDPL inverter/buffer schematic. In (b), iDDPL inverter/buffer timing diagram. It has to be noticed that $t_{eval,IN}$ and $t_{eval,OUT}$ are generally different.

4.5.1 Standard Design Flow vs Full/Semi Custom Design Flow

The design steps of a trustworthy platform has several critical points that have to be addressed properly to not underestimate the information leakage of an architecture. Compared to standard and classical design of digital devices, secure IPs for cryptographic applications often require additional steps, according to the required security level. Adding steps to the design flow has a strong impact to the total cost of final product's engineering process. Several modifications of the standard digital design flow are typical of security applications and it is common to refer to them as

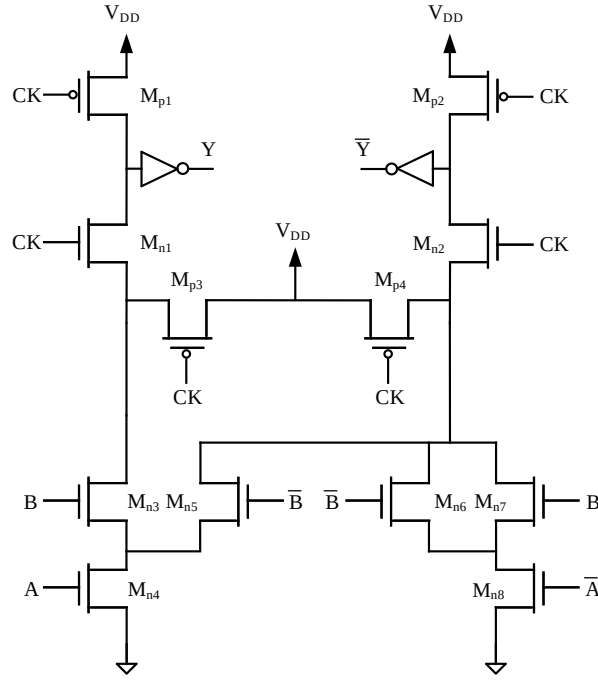


Figure 4.11. iDDPL AND/NAND gate with enhanced pull-down network for EE-free design.

secure digital design flow.

4.5.2 D³L Logic Cell Template

The application of the TEL principle on a digital circuit requires some special attentions in how the basic gates are designed. These requirements can be used as a direct guideline to design the basic gates. The intention of this new logic style is to implement digitally the TEL encoding scheme using a standard-cell approach, in order to simplify the *secure digital design flow* and relaxing demanding requirements of other gate-level countermeasures. The standard-cell approach provides also FPGA-compatible implementations, relaxing the capacitive mismatch requirements typical of most DPL styles on this kind of target platform. The *Delay-Based Differential Dynamic Logic* (DDDL or D³L), presented in this chapter, is a novel dynamic and differential logic style based on the TEL principle, and represents the first attempt to outline a TEL-compatible logic style using a standard-cell approach and standard design flow for secure applications. The D³L style has the following properties:

- supports both TEL and RTZ encoding;
- no complex pre/post place&route modifications are required;

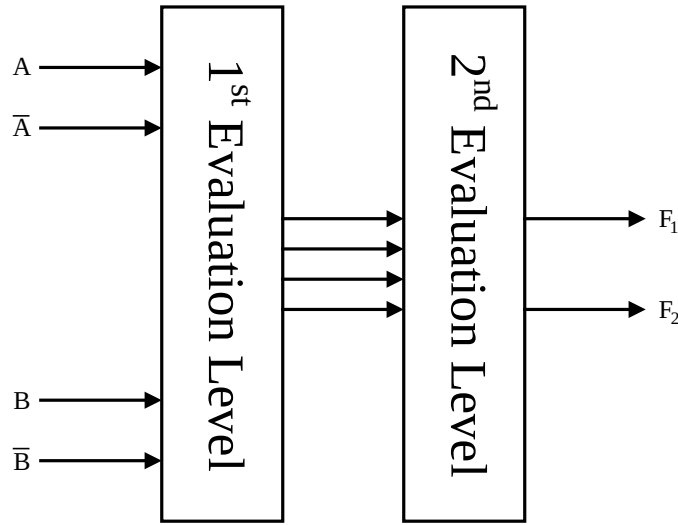


Figure 4.12. D³L 2-input combinational gate template.

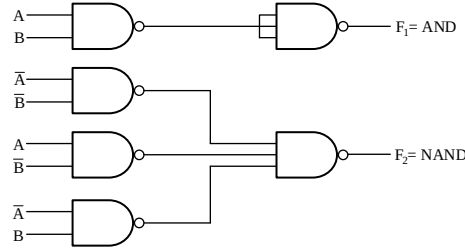
- implementable using only standard cells, available in most commercial digital design kits;
- FPGA-compatible.

As mentioned in previous sections, the TEL encoding scheme requires that the logic circuitry has to meet the property of completeness. Consequently, the property of completeness requires that each gate has to satisfy Equation 4.10 and each signal has both $0 \rightarrow 1$ and $1 \rightarrow 0$ transitions in a clock cycle. The requirement of *strictly positive monotonic* gates can be satisfied if the NAND function is used as basic function to derive every Boolean function needed in a cryptographic device. In order to fulfill all those mathematical and functional requirements, we decided to re-arrange the basic Boolean functions using only the NAND function as basic building block. Since the D³L is a dual-rail logic style, both complementary output functions have to be defined, according to TEL encoding requirements. A 2-input combinational gate template in D³L style is shown in Figure 4.12. As we will discuss in this section, the evaluation of the output values is performed by using two layers, both based on the use of the NAND functions. In the following, the three main Boolean function implementations for the D³L style using only CMOS NAND gates are presented.

In Table 4.5, the AND/NAND truth table is reported. All the possible four combinations of signals A , $\bar{A}$, B and $\bar{B}$ are used to re-write the functions. It must to be noted that the function AND/NAND is evaluated in two levels. Using DeMorgan's laws and the properties of Boolean algebra, it is possible to rearrange both functions as *product of products*. As we will discuss later, each D³L gate is composed by two

Table 4.5. D³L AND/NAND complete truth table.

A	B	$\overline{A \cdot B}$	$\overline{\overline{A} \cdot \overline{B}}$	$\overline{A \cdot \overline{B}}$	$\overline{\overline{A} \cdot B}$	AND	NAND
						F_1	F_2
0	0	1	0	1	1	0	1
0	1	1	1	1	0	0	1
1	0	1	1	0	1	0	1
1	1	0	1	1	1	1	0

**Figure 4.13.** D³L AND/NAND gate.

NAND layers for each compound. The complementary output signals are computed as depicted in Figure 4.13 and their expressions are shown in Equation 4.21 and 4.22. The AND/NAND function can be evaluated using 6 NAND gates, and requires approximately the same number of gates required for a MDPL masked AND/NAND gate.

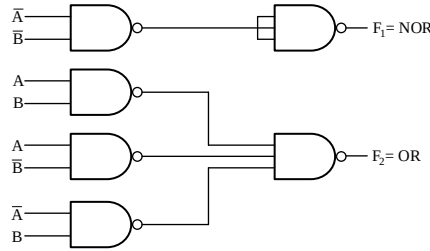
$$F_1 = \overline{\overline{A \cdot B}} = A \cdot B \quad (4.21)$$

$$\begin{aligned}
 F_2 &= \overline{(\overline{A \cdot B}) \cdot (\overline{A \cdot \overline{B}}) \cdot (\overline{\overline{A} \cdot B})} = \\
 &= \overline{((A + B) \cdot (A + \overline{B}) \cdot (\overline{A} + B))} = \\
 &= \overline{(A \cdot A + A \cdot \overline{B} + A \cdot B + B \cdot \overline{B}) \cdot (\overline{A} + B)} = \\
 &= \overline{[A + A \cdot (B + \overline{B})] \cdot (\overline{A} + B)} = \\
 &= \overline{A \cdot (\overline{A} + B)} = \overline{A \cdot \overline{A} + A \cdot B} = \overline{A \cdot B}
 \end{aligned} \quad (4.22)$$

The OR/NOR in the D³L can be rewritten similarly to the AND/NAND gate. The same number of NAND are required, and it is fairly symmetric to the AND/NAND gate. It has to be noted that the $\overline{AB}$ and $\overline{\overline{A} \cdot \overline{B}}$ products are swapped, to accommodate the OR and NOR functions. The truth table and expressions of the output signals are reported in Table 4.6 and Equations 4.24-4.23. The OR/NOR gate in D³L's template is depicted in Figure 4.14.

Table 4.6. D³L OR/NOR truth table.

A	B	$\overline{\overline{A \cdot B}}$	$\overline{A \cdot B}$	$\overline{A \cdot \overline{B}}$	$\overline{\overline{A \cdot B}}$	NOR	OR
						F ₁	F ₂
0	0	0	1	1	1	1	0
0	1	1	1	1	0	0	1
1	0	1	1	0	1	0	1
1	1	1	0	1	1	0	1

**Figure 4.14.** D³L OR/NOR gate.

$$F_1 = \overline{\overline{A \cdot B}} = \overline{A + B} \quad (4.23)$$

$$\begin{aligned}
 F_2 &= \overline{(\overline{A \cdot B}) \cdot (A \cdot \overline{B}) \cdot (A \cdot B)} = \\
 &= \overline{(\overline{A + B}) \cdot (\overline{A} + B) \cdot (A + \overline{B})} = \\
 &= \overline{(\overline{A \cdot A} + \overline{A \cdot B} + \overline{A \cdot \overline{B}} + \overline{B \cdot B}) \cdot (A + \overline{B})} = \\
 &= \overline{\overline{A} \cdot (A + \overline{B})} = \\
 &= \overline{\overline{A} \cdot A + \overline{A} \cdot \overline{B}} = \overline{\overline{A} \cdot \overline{B}} = A + B
 \end{aligned} \quad (4.24)$$

The XOR/XNOR gate, which is one of the main building block in the implementation of block ciphers, can be designed using the same approach, using only the NAND functions, as shown in Figure 4.15. The truth table and the expressions with Boolean operands are reported in Table 4.7 and Equations 4.25-4.26.

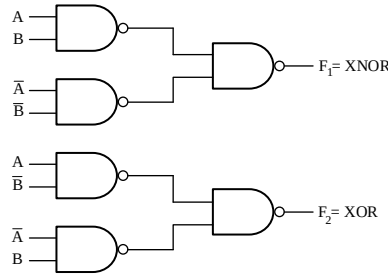
$$F_1 = \overline{(\overline{A \cdot B}) \cdot (\overline{\overline{A \cdot B}})} = A \cdot B + \overline{A} \cdot \overline{B} = XNOR \quad (4.25)$$

$$F_2 = \overline{(\overline{\overline{A \cdot B}}) \cdot (\overline{A \cdot B})} = \overline{A} \cdot B + A \cdot \overline{B} = XOR \quad (4.26)$$

As it can be seen from Figure 4.13-4.15, the gates are perfectly symmetric in terms of functionality, since both compounds of each gate has been derived using only NAND functions. The NAND approach ensures the property of completeness which

Table 4.7. D³L XOR/XNOR truth table.

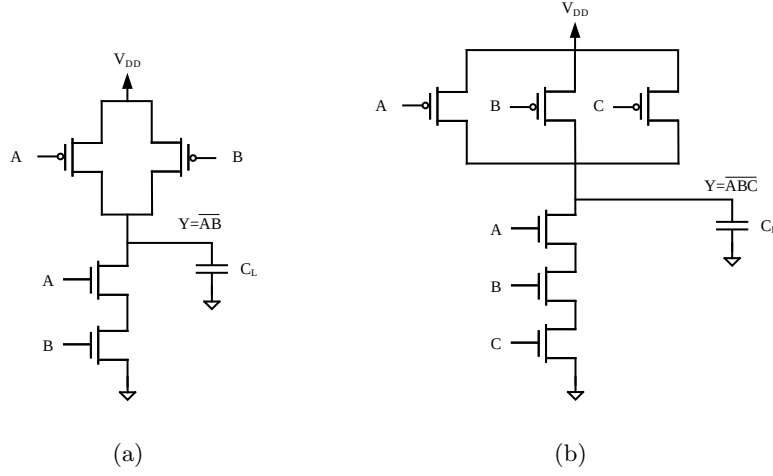
A	B	$\overline{A \cdot B}$	$\overline{\overline{A} \cdot \overline{B}}$	$\overline{A \cdot B}$	$\overline{A \cdot \overline{B}}$	XNOR	XOR
						F ₁	F ₂
0	0	1	0	1	1	1	0
0	1	1	1	0	1	0	1
1	0	1	1	1	0	0	1
1	1	0	1	1	1	1	0

Figure 4.15. D³L XOR/XNOR gate.

is required from the TEL encoding. In addition, the design method used in this case, allows to get homogenous gate, by reason of the presence of gate of the same type. Nevertheless, this particular way to design a standard-cell TEL-compatible logic family has a major drawback. The presence of non perfectly balanced timing path and fan-out between the two branches of a gate may be a potential weakness in the design, as previously mentioned for the early evaluation effect. As we will discuss later on this chapter, the D³L style can be designed to perfectly match the balancing requirement to avoid unwanted information leakage in the dynamic power consumption.

4.5.3 Early Evaluation Free D³L Combinational Gates

The leading philosophy in designing D³L cells templates is to derive fully symmetric basic gates for combinational functions. The cell templates for the basic logical functions depicted in Figure 4.13-4.15 satisfy this main requirement, but it is compliant with a fully symmetric design only in terms of functional behavior. Since in TEL encoding the evaluation phase takes place with then rising edge of CK signal, the critical transition where the information leakage may be at its maximum is the $1 \rightarrow 0$ transition for the 1st evaluation level, and $0 \rightarrow 1$ for the 2nd, time constants of charge/discharge events at each internal interface of the system have to be investigated. A simple resistive model of each NAND gate is used to analyze the time constant at the output of each gate. We will use the AND/NAND gate in Figure 4.13 as reference example for this analysis, which can be easily applied to

**Figure 4.16.** CMOS NAND2 (a) and NAND3 (b) gates.**Table 4.8.** Time constant for charging/discharging event on the first evaluation layer of the D³L AND/NAND gate.

A	B	$\overline{A \cdot B}$	$\overline{\overline{A} \cdot \overline{B}}$	$\overline{A \cdot \overline{B}}$	$\overline{\overline{A} \cdot B}$
0	0	$R_p/2 \ C$	$2R_n C$	$R_p C$	$R_p C$
0	1	$R_p \ C$	$R_p C$	$R_p/2 \ C$	$2R_n C$
1	0	$R_p \ C$	$R_p C$	$2R_n C$	$R_p/2 \ C$
1	1	$2R_n \ C$	$R_p/2 \ C$	$2R_n C$	$R_p/2 \ C$

OR/NOR gate as well.

If we use standard-cell CMOS NAND2 and NAND3 gates (Figure 4.16(a)-4.16(b)), we can model the charge and discharge event of the load capacitor using a simple resistive model. Assuming that the ON-resistance of a p-channel device is R_p and the ON-resistance of a n-channel device is R_n and the OFF-resistance of both kind of device is infinite (open-circuit model of the MOS device), we can calculate the RC-type time constant of each input pattern that we have in D³L AND/NAND gate. In the D³L AND/NAND gate presented previously and shown in Figure 4.13 (and similarly the OR/NOR gate, shown in Figure 4.14), the NAND2 gate on F_1 branch has a fan-out of 3, which is greater than the other three NAND2 gates, which have a fan-out of 1. Assuming that the four NAND gates at the first evaluation layer of the D³L AND/NAND gate have the same drive-strength, the first one is over-loaded, and the rise and fall time of the gate will not match with the other three. Moreover, since the first NAND gate sees three times the value of the load capacitance, its power consumption is also higher compared to the rest of the first layer's gates. Thus, the information leakage due to this internal unbalance can be easily detected and the power analysis may still recover the input/output state of the D³L gate. In addition to that, the rise and fall time of the output NAND3

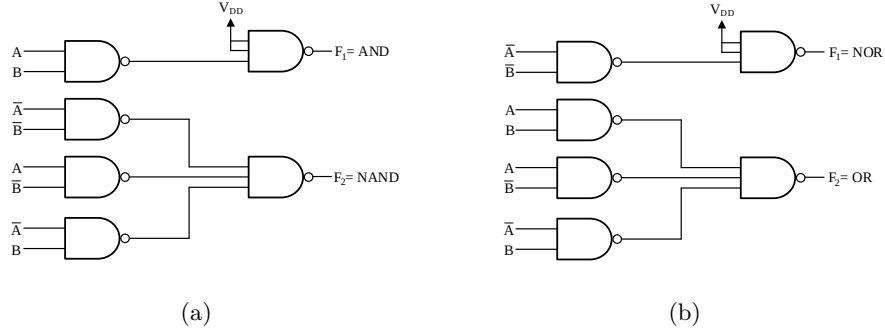


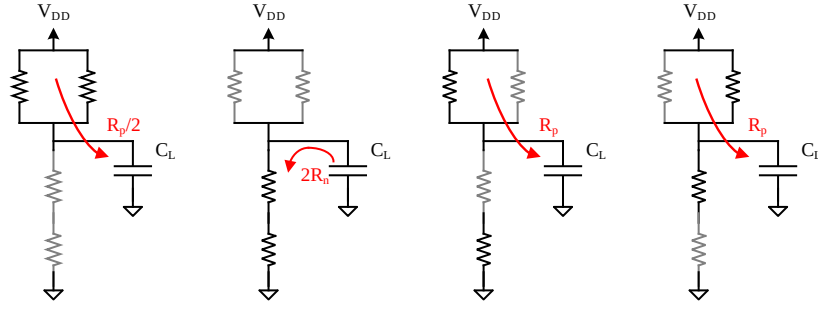
Figure 4.17. D³L AND/NAND (a) and OR/NOR gate with enhanced output layer to avoid unbalancing in fan-out values between the compounds.

gate that provide F_1 cannot match the other NAND3 on the output layer, since the evaluation depth resistance is not matched assuming the same load capacitance. The D³L OR/NOR gate in Figure 4.14 has a similar behavior, since they are built on the same functional template. The D³L XOR/XNOR gate in Figure 4.15 is fully symmetric, since there is no unbalance in the internal fan-out, and the evaluation depth resistance is the same for the two compounds. Thus no information leakage due to internal mismatch can be exploited in the XOR/XNOR gate in D³L style, as we will analyze further.

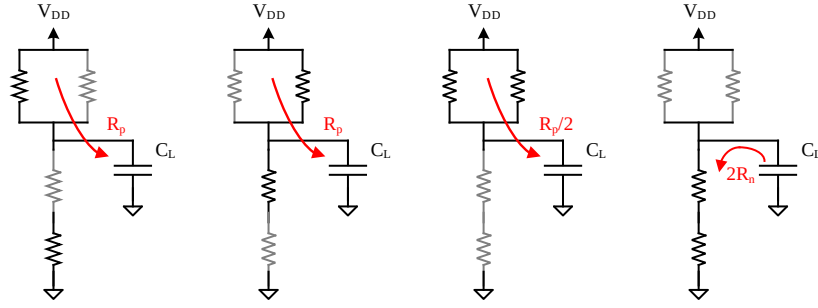
In order to overcome the issue related to internal unbalance of the first evaluation layer in AND/NAND (OR/NOR) gate, a simple solution is to set fixed two inputs of the NAND3 gate which provides the F_1 at the output layer, without changing the functional behavior of the AND/NAND (OR/NOR) gate. Since the NAND function can be seen as a logical 1-bit inverter if all unused input are tied to '1', we can re-arrange the AND/NAND, and similarly the OR/NOR gate, as shown in Figure 4.17(a)-4.17(b).

Considering only the first layer of NAND gates, we can have the four possible situations depicted in Figure 4.18. A summary of the time constant for each combination is reported in Table 4.8.

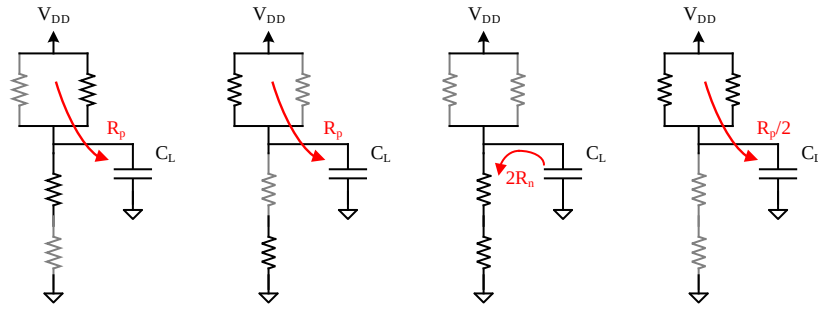
As we can see, the first evaluation layer can be characterized with four possible time constants. This will ensure that the sum in time of the four transitions is always constant. In fact, since the drive strength of each NAND2 gate is the same by design, and since their capacitive loads are the same, the consumption for each cycle is the same, neglecting the input pattern. Moreover, in TEL signaling, 1st evaluation layer provides only $1 \rightarrow 0$ transitions during the evaluation phase. Thus, the time constant for each discharge events between at the output of the 1st evaluation level is always $2R_nC$. As we have said before, NAND gates behave as synchronization nodes, since they will evaluate (in this case, drive outputs to '0') only when all inputs are high. At the end of the post-evaluation phase, all NAND2 gates are pre-charged to V_{DD} with the same time constant $0.5R_pC$. A similar analysis can be applied to the 2nd evaluation level, using the NAND3 equivalent model, as shown in Figure 4.19.



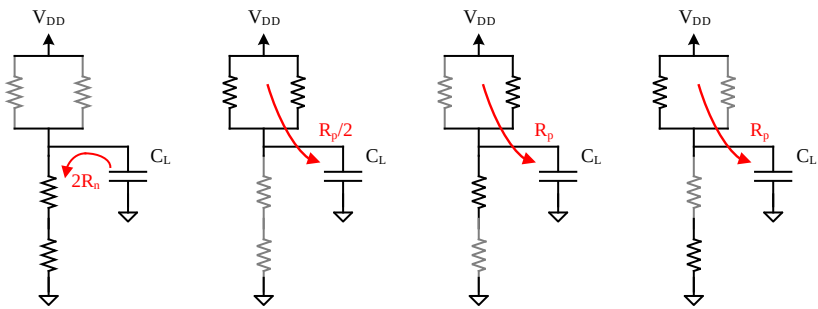
(a)



(b)



(c)



(d)

Figure 4.18. Equivalent model of the first evaluation layer of the D³L AND/NAND gate for the four possible combinations of the CMOS input data: $(A,B) = (0,0)$ (a), $(A,B) = (0,1)$ (b), $(A,B) = (1,0)$ (c), $(A,B) = (1,1)$ (d). The ON-resistance is depicted in black and the OFF-resistance is depicted in gray.

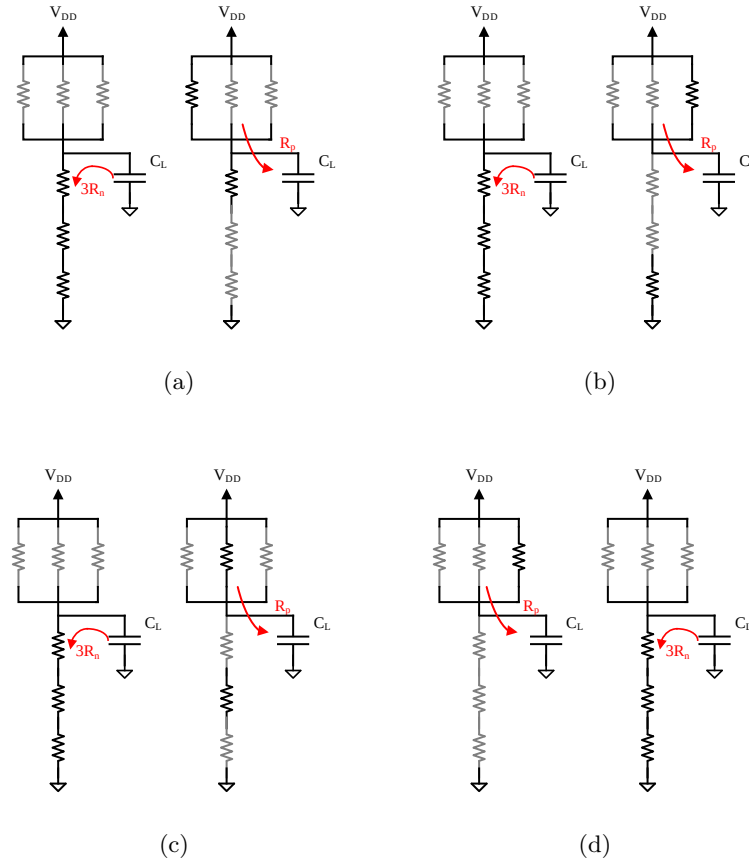


Figure 4.19. Equivalent model of the second evaluation layer of the D³L AND/NAND gate for the four possible combinations of the CMOS input data: $(A,B) = (0,0)$ (a), $(A,B) = (0,1)$ (b), $(A,B) = (1,0)$ (c), $(A,B) = (1,1)$ (d). The ON-resistance is depicted in black and the OFF-resistance is depicted in gray.

Table 4.9. Sum of the time constants of the D³L AND/NAND gate for RTZ signaling.

A	B	1 st Eval. Level	2 nd Eval. Layer
0	0	$(2R_p + 0.5R_p + 2R_n)C$	$(R_p + 2R_n)C$
0	1	$(2R_p + 0.5R_p + 2R_n)C$	$(R_p + 2R_n)C$
1	0	$(2R_p + 0.5R_p + 2R_n)C$	$(R_p + 2R_n)C$
1	1	$(2R_p + 0.5R_p + 2R_n)C$	$(R_p + 2R_n)C$

To summarize this analysis, a resume of the sum of the time constant for each combination of the equivalent CMOS input data is reported in Table 4.9-4.10.

It is clear that this symmetry makes the implementation of the AND/NAND gate in D³L, as well as OR/NOR gate, symmetric also for the evaluation time, making the basic gates free from information leakage due to early evaluation effect for both RTZ and TEL signaling. It has to be noted that also the implementation of basic

Table 4.10. Sum of the time constants of the D³L AND/NAND gate for TEL signaling.

	Pre-charge → Evaluation	Post-evaluation → Pre-charge
1 st Eval. Lev.	$4 \cdot (R_p/2C)$	$2R_nC$
2 nd Eval. Lev.	$3R_nC_o$	R_pC

Table 4.11. Delay time of basic gates in standard-cells logic style. Basic delays t_{NAND} , t_{NOT} , t_{NOR} and t_{XOR} , are referred to respective single-ended CMOS gates' delay.

Implementation	NAND	NOR	XOR
CMOS	t_{NAND}	t_{NOR}	t_{XOR}
WDDL	$t_{NAND} + t_{NOT}$	$t_{NOR} + t_{NOR}$	$t_{NAND} + t_{NOR} + 2t_{NOT}$
MDPL	$t_{AND} + t_{OR}$	$t_{AND} + t_{OR}$	$2(t_{AND} + t_{OR})$
D ³ L	$2t_{NAND}$	$2t_{NAND}$	$2t_{NAND}$

gates using all CMOS NAND gates allows the designer to obtain a static glitch-free implementation. In fact, it can be demonstrated that, since during the pre-charge all the input signals of each gate are forced to 0V, all intermediate signals in each gate are forced to V_{DD} . The presence of NAND gates at output interface allows only $1 \rightarrow 0$ transitions, and no unwanted pulses can be generated. This approach helps in eliminating additional information leakages due to unwanted second-order effects.

4.5.4 Conversion from CMOS Domain to Secure TEL Domain

In order to convert the input data from single-ended CMOS domain to the secure TEL domain, a conversion circuit is needed. The converter circuit is shown in Figure 4.20. The input of the circuit is composed by the single-ended CMOS signal A to be converted, and the clock signal CK . The signal CKD is a delayed replica of the clock signal CK . The time delay between CK and CKD is equal to the nominal duration of the evaluation phase t_{eval} . There are several approaches to generate CKD from CK , as we will discuss later. This delayed version of the clock can be shared throughout the D³L architecture, in order to save silicon area and maintain small the power overhead. Two 2:1 multiplexers are used to feed CK and CKD signals to the next stage. Control signals of the two multiplexers are connected both to the single-ended CMOS input data A . When $A = '1'$, outputs of the multiplexers will be CK for the upper one and CKD for the lower one. When $A = '0'$, the two clock signals are exchanged at the output of the two multiplexers. At the output of the two multiplexers we do not have a TEL compatible dual-rail signal. In fact, as shown in Figure 4.5, the dual-rail signal has to be aligned properly with CK , in order to respect the TEL signaling paradigm *pre-charge* → *evaluation* → *post-charge*. Two AND gates perform the logical AND function to gate signals at the output of multiplexers with CK , providing the correct TEL encoding and generating the TEL-compatible pair $(A_TEL, \overline{A_TEL})$. The timing diagram of the CMOS-to-TEL converter circuit is depicted in Figure 4.21. It is clear that the converter is able to

generate a TEL-compatible signal from its CMOS value, using the nominal duration t_{eval} of the evaluation phase.

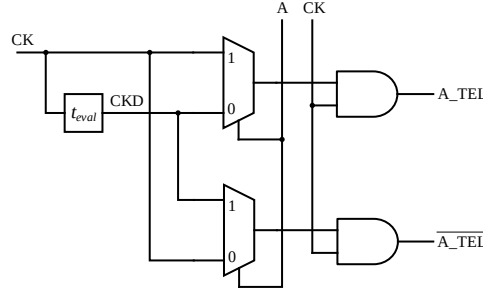


Figure 4.20. Circuit for the conversion from the single-ended CMOS domain to the dual-rail TEL domain in D³L style.

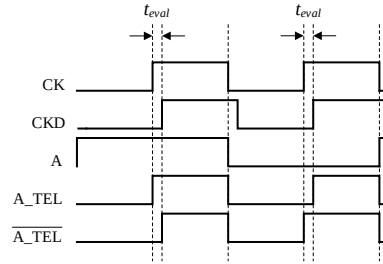


Figure 4.21. Timing diagram of signals in CMOS-to-TEL converter of Figure 4.20.

The generation of the nominal t_{eval} is a critical task in TEL-compatible logic styles, because it has to meet the following requirements:

- constant with voltage power supply and temperature variations;
- compact in terms of silicon area and power consumption.

The simplest solution to implement a delay line is to use a chain of inverter stages, which can be applied to both FPGA and ASIC implementations. Using the propagation delay of the inverter, it is possible to shift in time a digital waveform. Typically, the propagation delay of inverters in nowadays CMOS technology process is very small. In the STMicroelectronics 40nm process, the typical propagation delay of the minimum inverter is approximately 10ps at 1V of power supply voltage. To achieve a delay line of 1ns, the chain has to get a minimum of 100 inverters. Moreover, this solution suffers from a high dependency of the propagation time of the single inverter cell from the power supply voltage and from the working temperature of the device. A malevolent adversary can alter one (or both) of these two attack variables to alter the duration of the evaluation phase. From a security point of view, it is not recommended to use an inverter chain as a delay element. Regarding

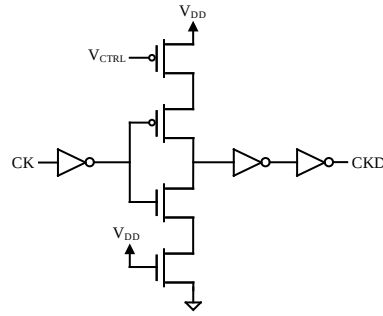


Figure 4.22. Delay element implemented using the starved inverter in [27] for iDDPL implementations. The V_{CTRL} voltage can be used to vary the delay provided by the starved inverter.

ASIC implementations, another possible solution to generate longer delay is to use the linear current starved delay element proposed in [76]. The delay element is implemented using a starved inverter circuit with linearized biasing scheme. The solution proposed by Jovanovic and Stojcev can provide a delay up to tenths of nanosecond, which is very long compared to the needs of TEL-compatible circuits to reach a reasonably level of security. In [27], the circuit shown in Figure 4.22 has been used to generate the nominal t_{eval} for an iDDPL implementation. The circuit is a slight modified version of the starved inverter in [76]: the main difference is that the control voltage is applied only to the upper p-channel transistor, resulting in a shorter delay.

Among open-loop solutions to generate specified delay, we choose the most general possible solution. Since we want to provide a general template for the D³L style, we need to address solutions that are reliable and feasible in both FPGA and ASIC applications. The starved inverter solution used in [27] offers a very compact and power efficient solution, if the delay element is not controlled in with a feedback control loop. In fact, variations in the working temperature of the device may cause variations and/or not negligible fluctuations of the nominal t_{eval} value. Deviations in the t_{eval} value may reduce the level of security, making the implementation still vulnerable to PAAs. To overcome this issue, we propose to use a generic macro to generate precise delay values that is based on a feedback loop approach. This solution requires the presence of one of this two following subsystems: *Phase-Locked Loop* (PLL) and *Delay-Locked Loop* (DLL). Both of them can be easily found in complex System-on-Chip and also in FPGAs. In fact, the needs of multiple clock domains requires the use of a PLL to generate all required frequencies and phases. Nowadays integrated circuits require the re-phasing of digital modulated signals, and this task is often handled using a DLL. In most commercial FPGA, a not negligible portion of the total die area is reserved to pre-implemented PLLs. They are able to generate multiple clocks from multiple input signals, with different output frequencies and phases. DLLs can be also implemented in FPGA using DSP blocks, but since PLLs are generically pre-implemented in most FPGAs, we choose the latter in order to provide the most generic template for D³L cryptographic implementation.

Nowadays PLL macros, available for both FPGAs and ASICs, offer an almost ready-to-use solution to generate delayed version of the main clock through multiple phase outputs. Thanks to the presence of the negative feedback, such kind of hardware macro can be generically considered more tolerant to power supply voltage and working temperature variations compared to other solutions, making them more attractive to generate the delayed clock signal *CKD* for D³L implementations.

4.5.5 Analysis of $\Delta\delta$ in D³L Style

The property of time-enclosing of TEL signaling is based on the use of short delay between the two rail used to propagate the information. The duration of the short delay is ideally constant, but, in practice, the evaluation phase has no constant duration through the combinational path of a pipeline stage. In Section 4.3.5, we have defined the timing constraints of a TEL-compatible logic. Each combinational gate in a TEL-compatible path has to satisfy and Equation 4.12 Equation 4.15. Hence, we must ensure $t_{eval,CL}$ to be smaller than the nominal t_{eval} for any input combination, in order to maintain the time enclosure of the information leakage. In this section, we want to show that D³L combinational gates can satisfy Equation 4.15, making the proposed logic style compliant with the time-enclosing requirements.

In order to provide an analysis of the behavior of basic D³L gates in terms of fluctuations of $t_{eval,CL}$, the synchronization of the input TEL-compatible signals of a gate has to be defined properly. Considering a basic gate, we assume the input signal $(A, \overline{A})$ has an evaluation phase duration $t_{eval,A} = t_{eval}$, without loss of generality, and the input signal $(B, \overline{B})$ is delayed with the input $(A, \overline{A})$ so that the rising edge of the respective asserted signals is t_1 , while the rising edge of the non-asserted signals is t_2 , with $t_2 < t_1$. Let us assume that the signals $(A, \overline{A})$ and $(B, \overline{B})$ are provided by gates which do not suffer from the fluctuation of t_{eval} . We can define $t_{eval,B}$ as follows:

$$t_{eval,B} = t_{eval,A} + t_2 - t_1 \leq t_{eval,A} = t_{eval} \quad (4.27)$$

With a first-order approximation, the delay provided by a single rail from a basic gate in D³L style can be assumed as $2t_{NAND}$, as reported in Table 4.11. Since $t_2 < t_1$, we have to verify if Equation 4.12 is satisfied for the two cases $t_2 < 2t_{NAND}$ and $t_2 > 2t_{NAND}$. As case study, we will refer to the AND/NAND gate in D³L style depicted in Figure 4.17(a), using all minimum NAND2 and NAND3 gates. Let us to assume, that the dominant capacitance in the AND/NAND of Figure 4.17(a) is due to load capacitors at the output interface, neglecting internal unbalance or asymmetry, since the 1st level of the evaluation network is composed of all similar NAND2 gates, each one with fan-out equal to 1 towards a NAND3, all the internal signals are forced to load almost the same capacitance with the same drive strength. The case $t_2 < 2t_{NAND}$ is reported in Equation 4.28-4.31.

$$t_{eval,CL}^{1,1} = t_{eval} - t_1 \quad (4.28)$$

$$t_{eval,CL}^{1,0} = t_{eval} + t_2 - t_1 \quad (4.29)$$

$$t_{eval,CL}^{0,1} = t_{eval} - t_1 \quad (4.30)$$

$$t_{eval,CL}^{0,0} = t_{eval} + t_2 - t_1 \quad (4.31)$$

Since $t_2 < t_1$ and $t_1 < t_{eval}$, for each input combination, the output delay will be always smaller than the nominal t_{eval} and $\Delta\delta > 0$. Time diagrams of the case $t_2 < 2t_{NAND}$ are shown in Figure 4.23.

The case $t_2 > 2t_{NAND}$ is described by Equation 4.32-4.35, and depicted in Figure 4.24.

$$t_{eval,CL}^{1,1} = t_{eval} - t_1 \quad (4.32)$$

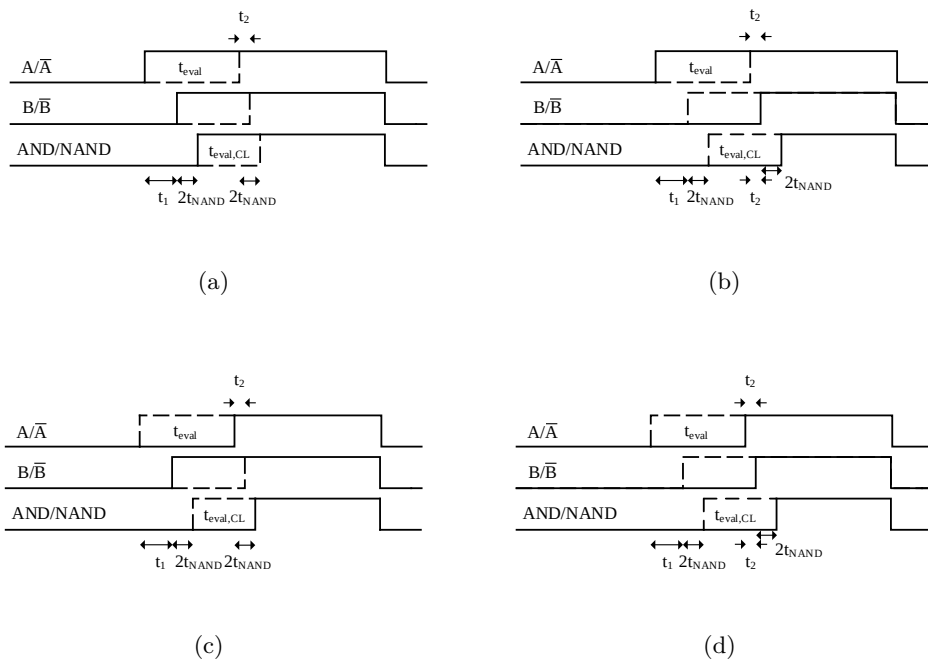


Figure 4.23. Time diagram of the AND/NAND gate in D³L with $t_2 < 2t_{NAND}$.

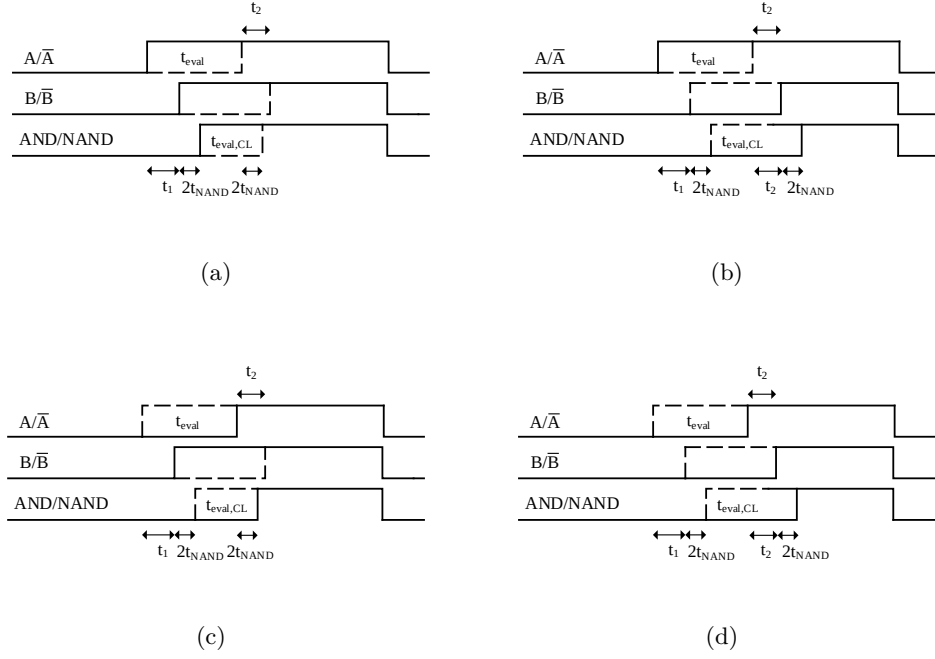


Figure 4.24. Time diagram of the AND/NAND gate in D³L with $t_2 > 2t_{NAND}$.

$$t_{eval,CL}^{1,0} = t_{eval} + t_2 - t_1 \quad (4.33)$$

$$t_{eval,CL}^{0,1} = t_{eval} - t_1 \quad (4.34)$$

$$t_{eval,CL}^{0,0} = t_{eval} + t_2 - t_1 \quad (4.35)$$

Similarly to the previous case, the propagation delay in Equation 4.15 is always negative, and the $t_{eval,CL}$ will be always shorter than nominal t_{eval} . This analysis allows us to define the time enclosing for the AND/NAND gate in D³L. The OR/NOR gate has the same behavior of the AND/NAND, since they share the same template and structure of the AND/NAND. Due to the fully symmetric structure of the XOR/XNOR gate in D³L style, the output evaluation phase duration is always equal to $t_{eval} - t_1$ for both scenario $t_2 < 2t_{NAND}$ and $t_2 > 2t_{NAND}$. This analysis ensure that the D³L is able to guarantee the time enclosing throughout the combinational path in a pipeline stage. Moreover, we can conclude this section making a further consideration on the upper bound of the propagation delay of a D³L logic gate. In fact, the maximum value of the propagation delay provided by a D³L depends on the delay between the rising edge of the two asserted signal at the input of the D³L gate:

$$\Delta\delta_{MAX} = t_1 \quad (4.36)$$

As it is clear, the value of t_I is given by the sum of delay times between the driver of $(B, \overline{B})$ and the gate.

4.6 Sequential Element in D³L Style

The design of the sequential element is a critical task in each logic family. In security applications, and particularly in DPL implementations, the design of the sequential element is often the most complex building block, since additional parameters and requirements have to be taken into account if compared to classical storage primitives [108]. Secure sequential elements are required to be able to balance the instantaneous power consumption, but, at the same time, to provide a memory element which is optimized in terms of area, power consumption and speed. In many design scenario, these different needs cannot be satisfied at the same time, since to protect the implementation from a PAA, the design of sequential element has to use larger silicon area, which implies also larger power consumption. It is worth noting that registers are one of the most critical part in cryptographic implementations in terms of security, as the instantaneous current drawn by registers strongly depends on the sampled data, making it extremely vulnerable to power analysis.

In a DPL implementation, registers and memory elements have to meet several specifications and provide special features that are non-standard. We can resume features of a DPL sequential element as follows:

- balance the instantaneous current absorption, making the power consumption independent from the sampled and stored data;
- allow differential signaling;
- according to the input signaling, the output stage of the memory element must be able to restore the correct encoding before providing the data at the next active clock edge;
- balance internal timing and capacitive mismatch, to avoid additional and unwanted information leakage through dynamic power consumption.

4.6.1 Sequential Elements in DPLs Styles

In security applications, the role played by the sequential element is critical, since it can be considered one of the most vulnerable building block. In previous sections, we have discussed about the vulnerability that DPL styles have due to capacitive mismatch [148] and early evaluation effect [139]. These two aspects have to be

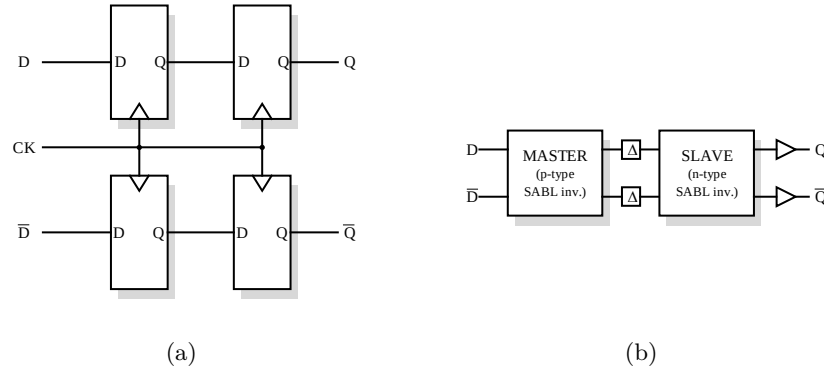


Figure 4.25. In (a), cell schematic of a WDDL register without the pre-charge wave generator. The CK signal has frequency equal to double of the data-rate. In (b), a block scheme of the SABL fully dynamic flip-flop [93].

taken into account also in the design of the sequential element, and not only for combinational gates. In fact, we must consider that in the sequential element, the input data is processed for an entire clock cycle, making it more vulnerable to power analysis, if special attentions are not taken into account during its design. In WDDL [147], the sequential element can be designed in different ways. An optimized way to design a WDDL sequential element is to use two CMOS D-FF in parallel, running with the same clock, which capture the RTZ signal at the input. Once the data is stored in the registers, it cannot be considered RTZ anymore, since it loses the *pre-charge* $\rightarrow$ *evaluation* signaling. Two AND gate, the *wave generator* can be used to restore the RTZ signaling, in order to generate the wave of pre-charge. Another design for a WDDL sequential element, which may not be optimized in terms of area and power overhead, makes use of four CMOS D-FF, two for each input signal. The clock frequency is doubled compared to the other architecture, in order to preserve the same throughput. In this architecture, when a register stores the pre-charge value, the previous one stores the evaluation value. The wave generator is no longer needed, since the use of two registers in series per branch clocked at double the data-rate, allows to maintain correct the RTZ encoding.

In MDPL [117] and improved MDPL (iMDPL), the sequential element has to take into account the RTZ encoding and the masking scheme. The input data is masked and at the next clock cycle, the output data of the register has to be masked with the new masking value. Hence, the sequential element in MDPL/iMDPL is composed by three main components, as shown in Figure 3.11(b). The first one is a XOR/XNOR gate in MDPL style, which is used to remove the old mask and apply the new one. After that a single-ended CMOS D-FF is used to store the masked data. At the output of the register, a wave generation circuit restore the RTZ encoding. In [129], it has been demonstrated that the presence of the masking scheme combined to DPL approach may not increase the security level of the cryptographic applications. The presence of physical leakage due to capacitive unbalance and glitches can still occur, making the implementation still intrinsically not secure.

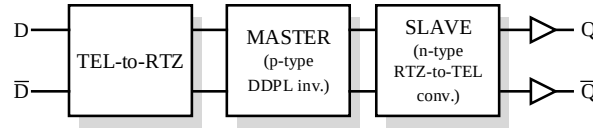


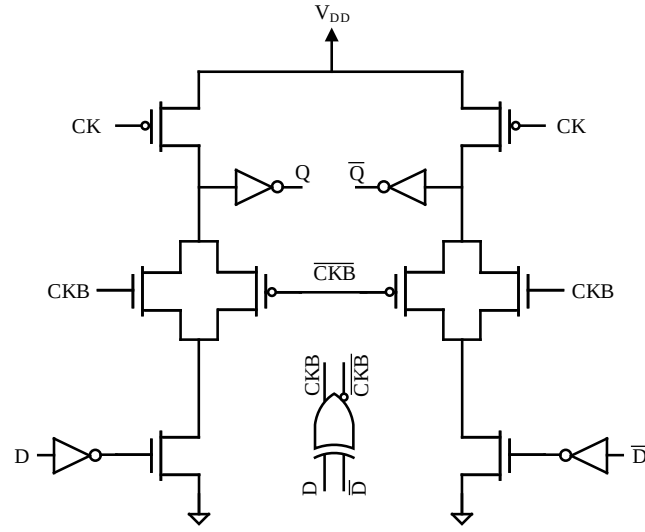
Figure 4.26. Block scheme of the iDDPL flip-flop proposed in [27].

Regarding the SABL sequential element, the first implementation given in [96] adopts a master-slave configuration. Matsui *et al.* took advantage of the intrinsically latch behavior of the SABL inverter to implement the master device, and a CMOS NAND SR latch to implement the slave device. This implementation of the flip-flop in SABL logic has a major drawback that if there is no change in the captured value for two or more clock cycles, there is no dynamic switching. This condition does not allow to balance the consumption for each input pattern and makes the flip-flop vulnerable to power analysis. An improved version of the SABL flip-flop has been presented in [113], where a fully dynamic flip-flop has been used to solve the problem in [96]. In [93], a cascade of p-type and n-type SABL inverter have been used to implement a fully dynamic flip-flop, using only building blocks from a SABL template, as shown in Figure 4.25(b). As we have analyzed in this chapter, SABL implementations, and moreover the sequential element, are extremely vulnerable to power analysis in the presence of capacitive mismatches [26]. This aspect represents a limiting factor in implementing cryptographic applications using the SABL style, as a huge effort in routing (at least a designer can adopt manual routing to achieve balancing) has to be taken into account.

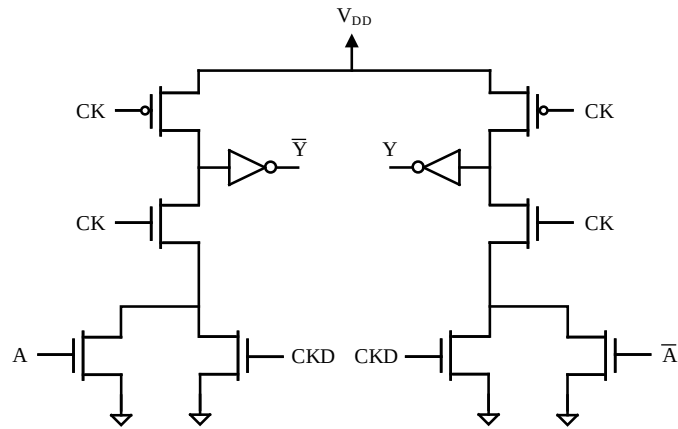
In [27], a balanced flip-flop that is compatible for TEL data encoding has been proposed. The DDPL flip-flop uses the master-slave architecture of the SABL flip-flop in [93]. In order to reuse the paradigm of p-type+n-type inverter shown in Figure 4.25(b), the flip-flop in DDPL needs of additional sub-systems which actually convert the signal from/to the TEL domain to/from the RTZ domain. A self-timed pulse clock latch is used to convert the TEL signal to an RTZ signal. A transistor schematic of the self-timed pulse clock latch in [27] is depicted in Figure 4.27(a). A p-type DDPL inverter is used as master latch, while the slave device has been implemented using the n-type RTZ-to-TEL converter shown in Figure 4.27(b), which acts as a latch and allows to restore the TEL encoding. The architecture proposed in [27] is able to tolerate higher capacitive mismatch compared to other DPL flip-flops, remarking the ability of the TEL encoding to increase the level of security also in the presence of strong mismatch.

4.6.2 Design of the Sequential Element in D³L Style

Thanks to the TEL encoding, the D³L can be implemented using two parallel compounds, as they evaluate the output results based on the arrival time of the input signals. In D³L style, the sequential element can be designed adopting a



(a)



(b)

Figure 4.27. In (a), a self-timed pulse clock latch used as TEL-to-RTZ converter in iDDPL flip-flop architecture. In (b), the n-type RTZ-to-TEL latch/converter.

master-slave approach, as used also for SABL [113] [93] and iDDPL [27] flip-flops. The block scheme of the D³L sequential element is shown in Figure 4.28.

Similarly to the iDDPL sequential element, the D³L flip-flop requires the presence of a TEL-to-RTZ converter. According to Figure 4.5, the TEL paradigm makes use of the difference in the time of arrival of the two complementary signals, allowing to convert from TEL domain to RTZ domain using this information. The TEL-to-RTZ converter used in D³L has been implemented using a NAND SR latch, as shown

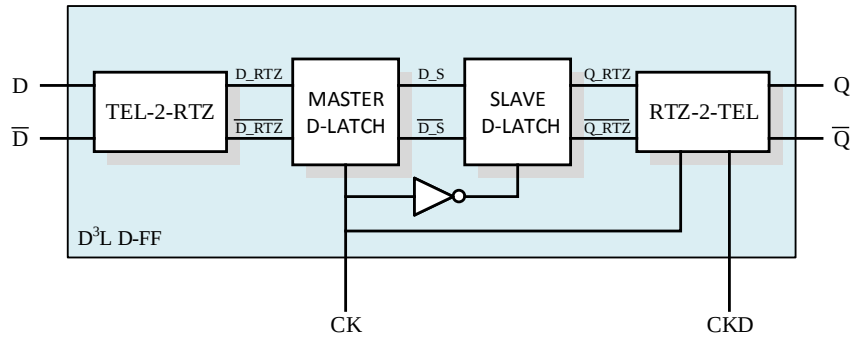


Figure 4.28. Block scheme of the sequential element building block in D³L style.

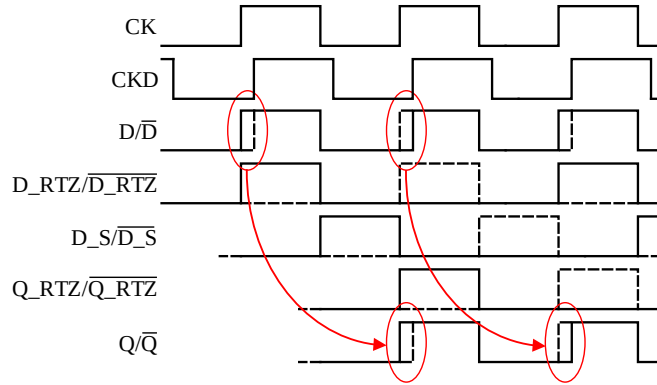


Figure 4.29. Timing diagram of signals in D³L sequential element.

in Figure 4.30. During the pre-charge phase, both TEL rails at the input are set to 0V. This input configuration corresponds to the *Invalid State* of the NAND SR latch. In this case, both output signals of the latch are forced to assume both the logical '1' value, which is inverted by the output inverters. During the evaluation phase, the complementary signals assume their respective value, according to TEL signaling. If we consider D and $\bar{D}$ as *Set* and *Reset* respectively, the NAND SR latch is able to capture which of them reach the post-evaluation value as first, and generates output values according to the TEL value. During the post-evaluation phase, both input signals are set to V_{DD} , which corresponds to *Hold State* of the SR latch. At this point, the RTZ value is set according to the stored value. A transient simulation on the circuit shown in Figure 4.30 performed in Cadence Virtuoso using the STMicroelectronics 40nm CMOS Design Kit is reported in Figure 4.31.

The most critical building block used to implement the D³L flip-flop is the OR-gated NOR SR latch, and it has been used for both master and the slave device. Its architecture is shown in Figure 4.32. When CK is high, both *Set* and *Reset* are high, and $(0,0)$ is forced at the output of the latch. During the falling edge of the clock signal, one of the input line of the NOR SR latch is high, due to inertial delay of

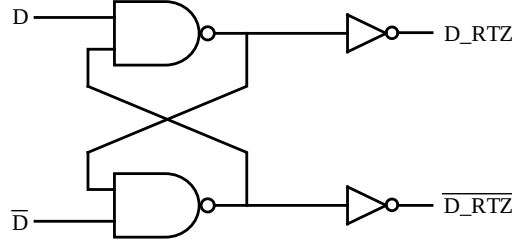


Figure 4.30. NAND SR latch used as TEL-to-RTZ converter in D³L sequential element.

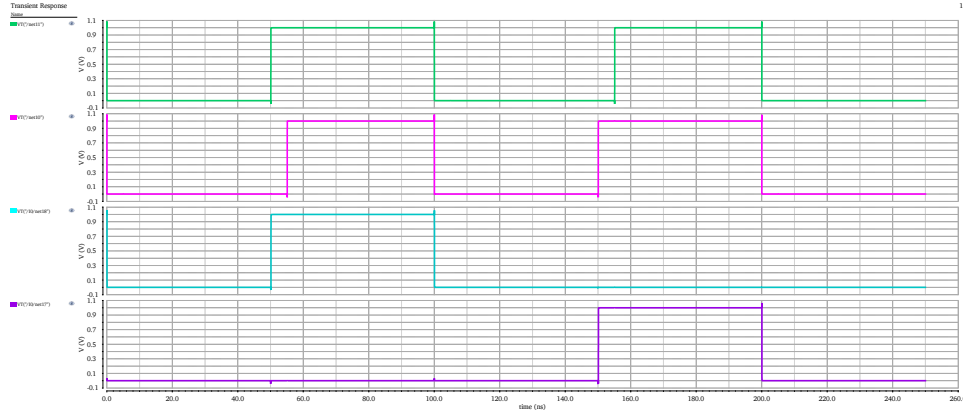


Figure 4.31. Timing diagram of the D³L TEL-to-RTZ collected on a Cadence Virtuoso transient simulation on 40nm STMicroelectronics CMOS standard-cells implementation: D (green), $\overline{D}$ (pink), D_{RTZ} (blue) and $\overline{D_{RTZ}}$ (violet).

the previous block to react to the clock signal's transition, while the other one is low. The respective output of the OR-based gate is then forced to 0V after the other, and the NOR SR latch can sample the state of the input signals. For example, let us assume that the input data of the OR-based NOR SR latch is $(D, \overline{D}) = (0, 1)$, when a falling edge of CK occurs, the OR-based gate has the following input transitions:

$$\begin{aligned} (CK, D) &: (1, 0) \rightarrow (0, 0) \\ (CK, \overline{D}) &: (1, 1) \xrightarrow{\delta_{prev}} (1, 0) \rightarrow (0, 0) \end{aligned} \quad (4.37)$$

The two output signals of the OR-based gating circuitry assume their respective value for a time interval equal to δ_{prev} that corresponds to the propagation delay of the previous stage. After all input signals are set to zero, *Set* and *Reset* are both forced to logical '0', and the latch is in the *Hold state*, storing the sampled data. The timing diagram of signals involved in the OR-gated NOR SR latch is shown in Figure 4.33. It has to be mentioned that, according to Figure 4.28, the slave latch is identical to the master device, but it is clocked by $\overline{CK}$.

At this point, the RTZ signal has been sampled and stored for one clock cycle.

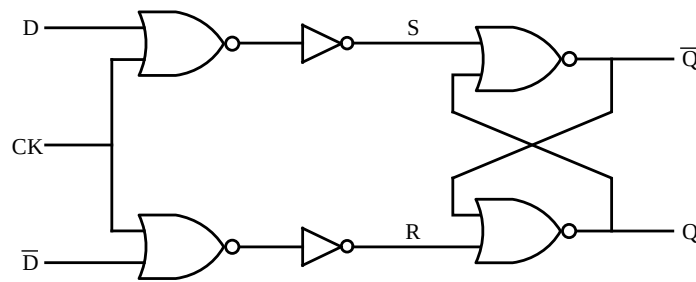


Figure 4.32. OR-gated NOR SR latch used for both master and slave device.

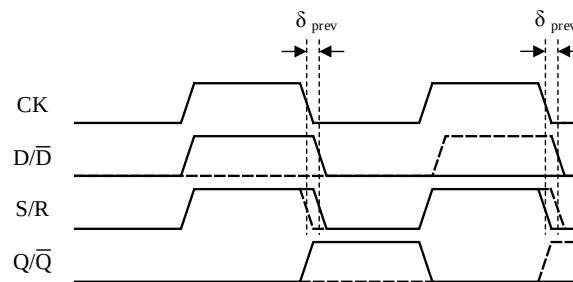


Figure 4.33. Timing diagram of the signals in the OR-gated NOR SR latch.

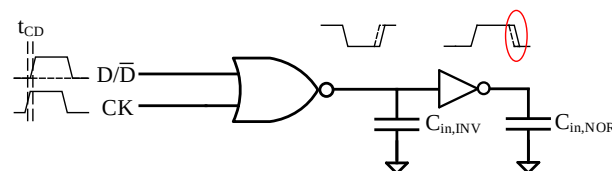


Figure 4.34. Half circuit of the OR-gating scheme.

In order to restore the TEL signaling, a RTZ-to-TEL converter is used at the D³L flip-flop's output. A circuit schematic of the RTZ-to-TEL converter is depicted in Figure 4.35. It is composed by a first OR gates layer and a second AND gates layer. The first layer will logical add the delayed clock CKD to the RTZ input signal. Since the RTZ encoding adopted in the sequential element requires that both signals pre-charge at 0V when CK is low, the ORing with CKD allows to reintroduce the evaluation phase of the TEL encoding using the nominal t_{eval} . The RTZ signal ORed with CKD is not yet a TEL-compatible signal, since the complementary wires at this interface are not synchronized with CK . To solve this problem, the second layer will gate the RTZ signal ORed with CKD by forcing both lines to 0V when CK goes low. The gating operation is performed using AND gates. This conversion allows to restore the TEL signaling and the nominal t_{eval} , providing a TEL-compatible signal

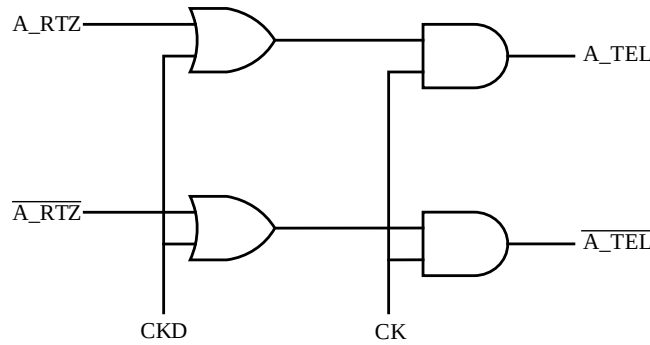


Figure 4.35. Scheme of the RTZ-to-TEL converter used as output interface in the D³L sequential element to restore the TEL encoding.

at the output of the sequential element.

4.7 Design and Characterization of the D³L Style

The design of the novel logic style has been carried out on the 40nm STMicroelectronics CMOS design kit, mentioned in previous chapters. Simulations and *Computer Aided Design* tools help the designer to evaluate and test the logic circuit, providing very accurate modeling of the real implementation. Moreover, using simulations is also useful in finding potential weakness of a secure design in a pre-silicon design phase. In fact, there are several aspects that cannot be analyzed and evaluated in a real environment, since, in general there is no possibility to catch in-depth the behavior of the circuit under test. Moreover, the presence of a real environment could influence in a no negligible way the result of the analysis. So far, in this section we present the simulation aided design of the D³L, using standard-cells from the aforementioned design kit. We have chosen to adopt both energy and frequency-domain security metrics to evaluate the strength of the D³L to PAAs. Furthermore, the analysis on combinational gates and sequential element, has been carried out taking into account the presence of capacitive mismatch, to provide a complete characterization of the novel logic style.

4.7.1 Energy Balancing in D³L Combinational Gates

The adoption of the DPL approach in counteracting PAAs is due to the possibility to achieve a switching activity of 1 for each DPL gate in a combinational path. This requirement is usually achieved using the *dual-rail* design and adopting the RTZ encoding. Also in the development of the D³L, the energy balance has been a practical aspect to be taken into account. As we have already discussed in Section 4.4.2, the TEL encoding uses three phases signaling with dual-rail approach

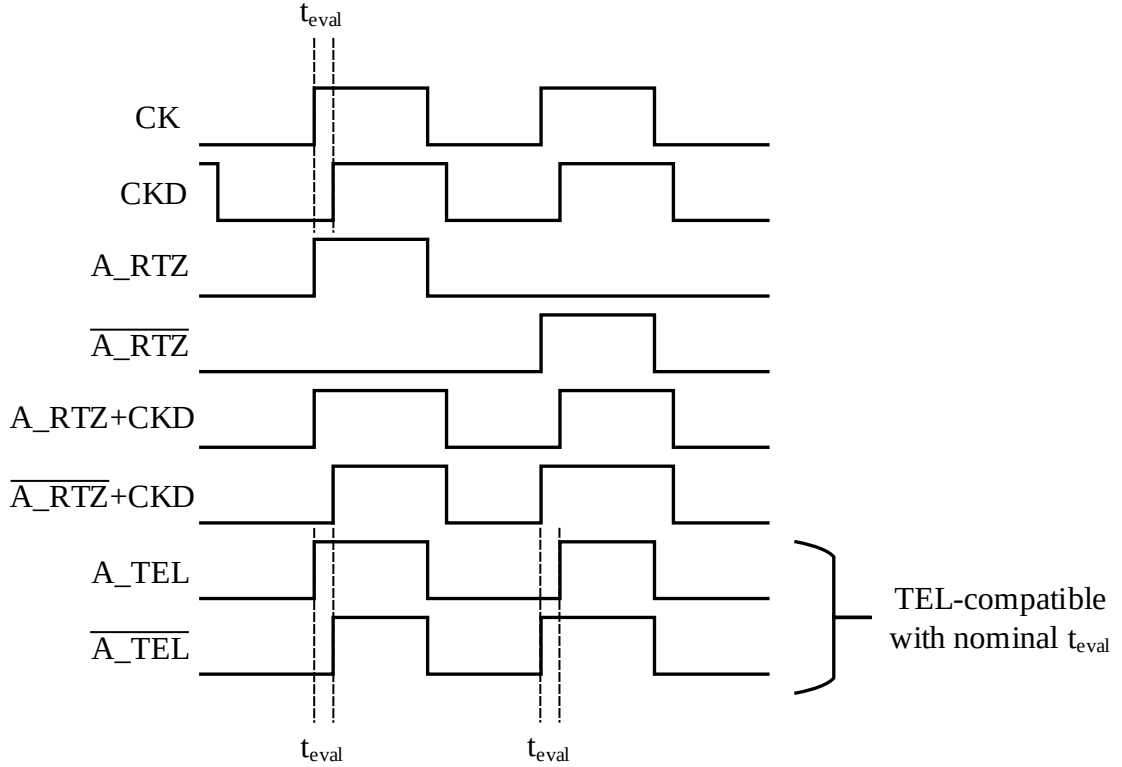


Figure 4.36. Timing diagram of the signals in the RTZ-to-TEL converter at the output of the D³L sequential element. It has to be noted that the output evaluation phase duration of the sequential element is the nominal t_{eval} , according to TEL-compatible flip-flop's requirements.

to guarantee the energy balancing also in the presence of capacitive mismatch. As reported in [148], [66], [13], [54], [26] and [70], the capacitive balance represents one of the most critical issue in the implementation of the secure DPL cryptographic circuits. Thus, during the evaluation of the D³L, it has been necessary to study the impact of the capacitive mismatch on the capability to balance the energy per cycle.

It is worth noting that in D³L, the combinational cell template in Figure 4.12 ensure a critical difference with classic DPL styles based on RTZ encoding. Due to internal symmetry and homogeneity of the architecture of each D³L gate, the requirement about the needs to provide a switching activity equals to unity to get energy balancing and independence from the processed data of the power consumption, is conducted not only at DPL level, but also at internal level. In fact, since the TEL encoding requires the compatibility with the three phase signaling presented in Section 4.3.2, both evaluation levels in Figure 4.12 are able to replicate the TEL signaling also at NAND gates level. By means of TEL encoding, each D³L

gate provides switching activity equals to unity at each hierarchy level.

In this analysis, we have used the WDDL style as reference, to compare the performance of the novel D³L with a classic DPL and RTZ gate-level countermeasure based on a standard-cells design. The evaluation of the security level of the proposed D³L has been carried out by simulations in Cadence Virtuoso, using the 40nm STMicroelectronics design kit, which support BSIM4 models for the best accuracy. Schematics in Figure 4.17 have been implemented using only standard-cells from the digital library with minimum driving capability. The power supply has been set to 1V and the t_{eval} has been set to 1ns. The clock frequency has been set to 10MHz, according to previous works [26], [15], [19], [126]. The time resolution of the simulation has been set to 10ps, providing a bandwidth of 50GHz. In order to simulate capacitive mismatch, the output capacitors have been sized accordingly to the previously mentioned Mismatch Factor (MF), here defined as follows:

$$MF = \frac{C_{L2}}{C_{L1}} \quad (4.38)$$

where C_{L1} and C_{L2} are the load capacitor of the *true* and *false* output of each gate respectively, with MF varying from 1 to 4 and C_{L1} set to 1fF. We consider the following levels of mismatch:

- no mismatch: MF=1;
- light mismatch: MF=2;
- strong mismatch: MF=3;
- extreme mismatch: MF=4.

Results for NED and NSD values for both logic families are reported in Table 4.12-4.15. It has to be noted that also without output mismatch (MF=1), both NED and NSD for D³L are strongly reduced compared to WDDL. The presence of mismatch impacts critically on WDDL implementation, since both NED and NSD increase significantly as MF is greater than 1. In fact, these results highlights the weakness of this logic style, because of the presence of capacitive mismatch yields to a strong reduction in the security level. In the D³L, the NED and NSD do not increase, remarking its capability to limit the possibility to mount a successful PAAs. The maximum values of the NED and NSD for D³L are 2.87% and 1.30% respectively.

Table 4.12. NED value of combinational gates in D³L.

	MF=1	MF=2	MF=3	MF=4
AND/NAND	2.58%	2.20%	1.92%	1.71%
OR/NOR	2.87%	2.48%	2.18%	1.94%
XOR/XNOR	2.27%	1.93%	1.69%	1.51%

Table 4.13. NSD value of combinational gates in D³L.

	MF=1	MF=2	MF=3	MF=4
AND/NAND	1.11%	0.95%	0.83%	0.73%
OR/NOR	1.20%	1.03%	0.91%	0.81%
XOR/XNOR	1.30%	1.10%	0.97%	0.86%

Table 4.14. NED value of combinational gates in WDDL.

	MF=1	MF=2	MF=3	MF=4
AND/NAND	11.13%	35.03%	50.24%	59.67%
OR/NOR	11.24%	35.18%	50.94%	60.52%
XOR/XNOR	5.33%	19.63%	71.00%	39.79%

Table 4.15. NSD value of combinational gates in WDDL.

	MF=1	MF=2	MF=3	MF=4
AND/NAND	4.86%	18.09%	27.94%	34.50%
OR/NOR	4.95%	20.83%	37.61%	51.60%
XOR/XNOR	2.32%	10.84%	47.26%	27.00%

4.7.2 Security Evaluation in the Frequency Domain

Since the D³L is a TEL-based logic style, it is necessary to evaluate the frequency contents of the information leakage. In [26], Bongiovanni *et al.* have introduced new criteria for assessment of the information leakage in the frequency domain. In TEL compatible circuits, the duration of the evaluation phase t_{eval} is directly related to the frequency content of the dynamic power consumption. Shorter the evaluation phase, higher will be the frequency at which the information leakage can be detected. A preliminary evaluation of the leakage distribution in the frequency domain can be performed using the squared absolute value of the difference of the *Fast Fourier Transform* (FFT) of the current absorption of an inverter for the two data transitions:

$$|\Delta FFT| = |FFT_0^2 - FFT_1^2| \quad (4.39)$$

In order to get a generalized evaluation for N input vectors, we adopt the *Frequency Energy Deviation* (FED), which is defined as follows:

$$FED = [\sigma_1 \sigma_2 \dots \sigma_F] \quad (4.40)$$

where the elements σ_f are defined as:

$$\sigma_f = \left[\frac{1}{N} \sum_{i=1}^N \sqrt{\overline{FFT}^2[f] + FFT_i^2[f]} \right] \quad (4.41)$$

with $f = 1, 2, \dots, F$ are the frequency points of the FFT calculation, and $\overline{FFT}[f]$ represents the average of the FFT at bin f . $\overline{FFT}[f]$ is calculated as follows:

$$\overline{FFT}[f] = \frac{1}{N} \sum_{j=1}^N FFT_j[f] \quad (4.42)$$

The FED security metric represents the variance in the frequency domain of the information leakage in the dynamic power consumption of the digital circuits. In a secure implementation, the FED has to maintain a value which has to be as lowest as possible into the attacking bandwidth, assuming the TEL model of the adversary. Generically, the attacking bandwidth is upper bounded by the frequency cutoff that it is possible to get at the power supply pin (or pins) of the cryptographic chip. Of course, this is an optimistic upper bound, because the final attacking bandwidth will be stated by the entire measurement chain.

In [26], authors present a study of the ΔFFT on a SABL and iDDPL inverter. Since in D³L and WDDL there are no explicit inverter gates, we have used the XOR/XNOR gate to compare the ΔFFT , setting one of the input to logical ‘1’ in each respective encoding scheme. We have used 2M points to get an approximated resolution of 50kHz for each bin current traces’ FFT from the simulations. ΔFFT plots are shown in Figure 4.37 and Figure 4.38 for different mismatch conditions. At low frequency, FFT is around -115dB for D³L neglecting the mismatch factor. The slope for MF=1 remains approximately flat, while for MF>1 the slope becomes positive for a certain cutoff frequency $f_c \approx 30MHz$. Beyond this cutoff frequency, differences due data-dependency start to increase in magnitude. Higher is the mismatch factor, higher will be the slope. It is worth noting to mention that some lobes are visible at multiple of 1GHz, due to higher order effects, which are not relevant for our analysis, since they can be considered out of the attacking bandwidth.

The WDDL shows approximately the same ΔFFT value of the D³L at low frequency in no mismatch condition. If $MF > 1$, FFT plots shows higher values even at low frequency (+10dB). At extreme condition ($MF = 4$), the low frequency ΔFFT is approximately -99dB, which is significantly higher than the respective D³L. These results are in accordance with Table 4.12-4.15 since it is sufficient a slight mismatch ($MF \geq 2$) to strongly increase information leakage that the adversary can exploit from dynamic consumption. Moreover, the low-frequency side of ΔFFT is extremely relevant from the adversary point of view [26]. In general, the presence of on-chip and off-chip filters limits the useful bandwidth to mount the attack. In order to remove the information leakage due to capacitive mismatch in D³L, we can implement a simple low-pass filter using, aiming to flatten the ΔFFT plots with $MF > 1$. Assuming the testbench in Figure 4.39, with $R_s = 100\Omega$, the minimum

value of the on-chip capacitance to flatten ΔFFT plots is expressed according to [26]:

$$C = C^{opt} \approx \frac{1}{2\pi f_c R_s} \cong 53pF \quad (4.43)$$

As additional analysis, we have used the implementation S-BOX in PRESENT-80 algorithm function to evaluate the FED security metrics on a complex network, using $MF = 3$. The S-BOX has been designed adopting K-map synthesis and using only 2-input Boolean operands. We have chosen $MF = 3$ since it can be suitable to model two worst-case scenarios:

- ASIC applications without routing constraints;
- FPGA applications without optimized *placeroute*.

The testbench used in this evaluation is the same of Figure 4.39. Results of the FED analysis are shown in Figure 4.40. It has to be noted that the behavior of the D³L implementation of the S-BOX is similar to $\Delta 0FFT$ plots in Figure 4.37. In this case, the cutoff frequency is approximately 50MHz, and the C^{opt} is approximately equal to 31.83pF. The low-frequency FED for the WDDL implementation has been found higher than the respective D³L (+5dB), remarking that the novel logic style is able to provide a PAA resistant design library using only standard-cells, which is also capacitive mismatch tolerant. A resume of area and power overhead of the D³L versus the WDDL implementation of the S-BOX is reported on Table 4.16.

4.7.3 Fluctuations of t_{eval} in Combinational Gates

In Section 4.5.5, we have discussed about the property of D³L combinational gates to satisfy the condition $t_{eval,CL} \leq t_{eval}$. In this section, we want to verify the

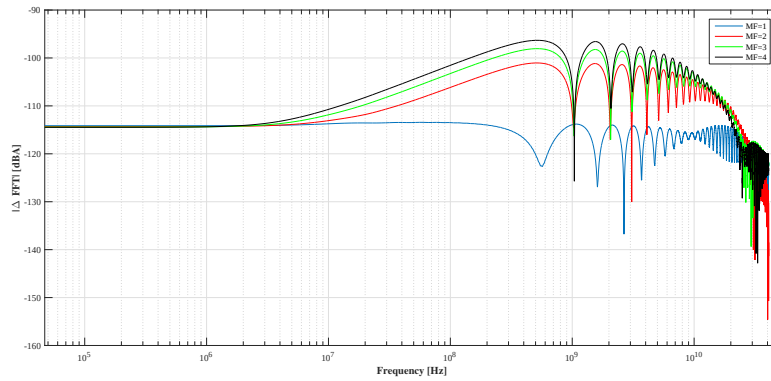


Figure 4.37. ΔFFT vectors for D³L XOR/XNOR gate used as inverter, with $t_{eval} = 1ns$.

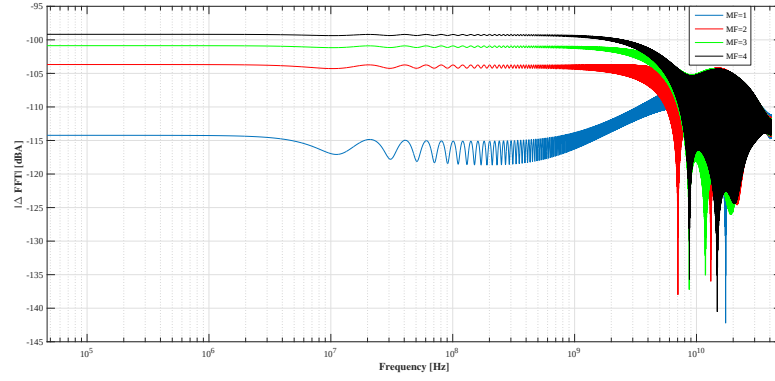


Figure 4.38. ΔFFT vectors for WDDL XOR/XNOR gate used as inverter.

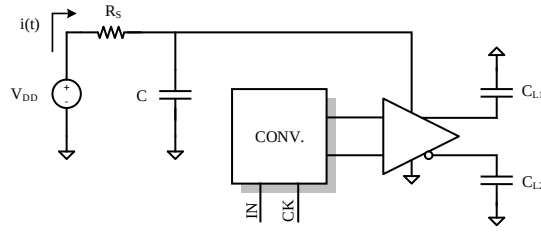


Figure 4.39. Testbench used to evaluate ΔFFT and FED plots.

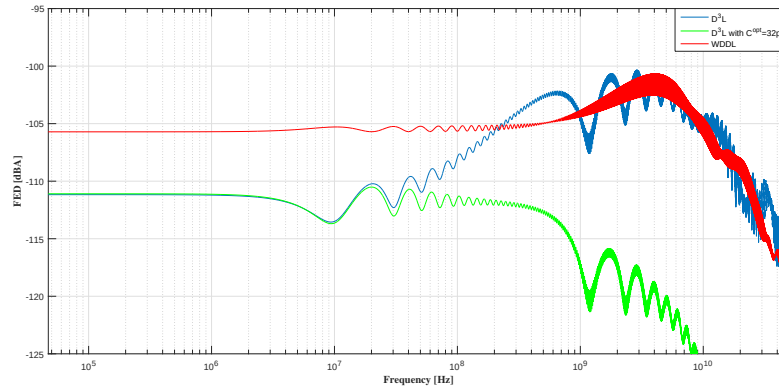
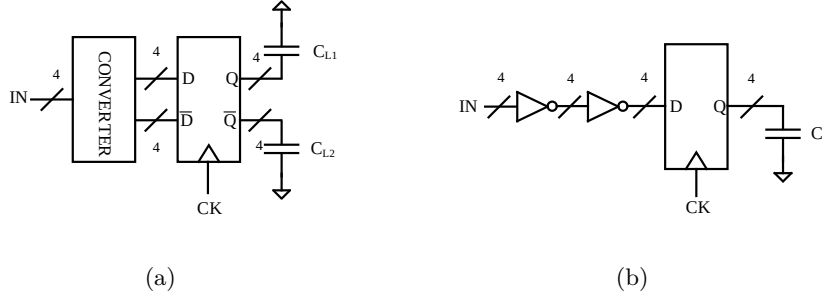


Figure 4.40. FED plots of the implementation of the PRESENT-80 S-BOX in D³L (blue), D³L with $C^{opt} = 32pF$ (green) and WDDL (red) style for $MF = 3$.

correctness of this timing model proposed for D³L combinational gates. Simulations in Cadence Virtuoso have been performed to demonstrate the validity of this timing model, assuming a clock frequency of 10MHz and a nominal t_{eval} of 1ns. The output capacitance has been set to 200aF, that is equal to the input capacitance of a CMOS D flip-flop in the 40nm design library. Signals A and B have been set with the nominal t_{eval} , and the time shift t_1 and t_2 has been set to 140ps. It has been

Table 4.16. Area and power consumption comparison for the PRESENT-80 S-BOX implementation.

Implementation	# of Devices	Area Overhead	Average Power	Power Overhead	NED	NSD
CMOS	132	x1	$0.60\mu W$	x1	52.04%	17.36%
WDDL	360	x2.72	$1.02\mu W$	x1.7	3.27%	1.14%
D ³ L	948	x7.18	$2.52\mu W$	x4.2	0.57%	0.13%

**Figure 4.41.** Testbenches used for the evaluation of the 4-bit register. Figure (a) shows the testbench used for WDDL, MDPL and D³L registers, and figure (b) shows the testbench used for the CMOS register, which is falling-edge triggered.

found that the validity of the timing model in Section 4.5.5 is correct for all the combinational gates defined in this chapter, as shown in Table 4.17.

4.7.4 Analysis of $\Delta\delta$ with Process Variations

A critical aspects of security designs is the presence of process variations. In this chapter, we have considered the capacitive mismatch as the main source of additional information leakage [125]. In order to get a complete characterization of the D³L style, the fluctuation effect of the evaluation phase duration at each combinational gate's output has been studied in the presence of process variations, by means of Monte Carlo simulations. 500 iterations with a nominal t_{eval} of 1ns have been considered. Results of the statistics are shown in Figure 4.42.

The results shown in Figure 4.42 remark that distributions are approximately

Table 4.17. $t_{eval,CL}$ of combinational gate in D³L style.

A	B	AND/NAND		OR/NOR		XOR/XNOR	
		Bal.	Unbal.	Bal.	Unbal.	Bal.	Unbal.
0	0	999ps	994ps	866ps	861ps	866ps	860ps
0	1	865ps	859ps	999ps	1000ps	867ps	873ps
1	0	1000ps	995ps	860ps	866ps	860ps	866ps
1	1	864ps	870ps	999ps	1000ps	861ps	856ps

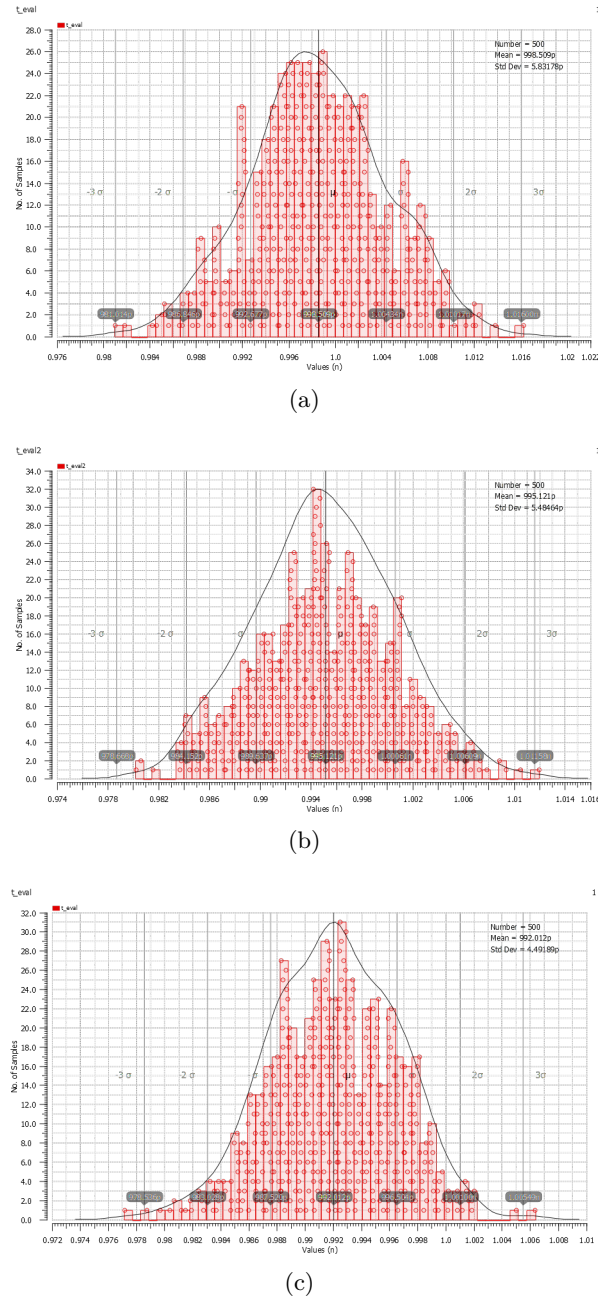


Figure 4.42. Distributions of the output delay $t_{eval,CL}$ of D³L combinational gates for 500 iterations of Monte Carlo simulations: AND/NAND (a), OR/NOR (b) and XOR/XNOR (c).

Gaussians. The average value is approximately 1ns in all cases, that corresponds to the nominal t_{eval} , as it was expected. In addition, the spread around the average values is always less than 6ps, which corresponds to a CV of 0.6%, which is a very small value. The Therefore, it has been found that combinational gates in D³L styles are compliant with the requirement of $\Delta\delta < 0$, also in the presence of process

variations. A resume of average and standard deviation values are reported in Table 4.18.

Table 4.18. Average and standard deviation of the $\Delta\delta$ for D³L combinational gates under process variations (500 iterations of Monte Carlo simulations).

	AND/NAND	OR/NOR	XOR/XNOR
μ	998.51ps	995.12ps	992.02ps
σ	5.83ps	5.48ps	4.49ps
CV	0.58%	0.55%	0.45%

4.7.5 Sequential Element Characterization

The design of D³L sequential element makes use of the same approach used to design the SABL flip-flop [93] and the iDDPL flip-flop [27]. The capability of the novel flip-flop to counteract PAAs has to be verified and compared to other implementations. In this section, a comparison of the proposed D³L sequential element with other sequential elements from standard-cell based DPL styles is presented. 4-bit registers have been designed in CMOS, WDDL [147], MDPL [117], in addition to D³L, to be used as case study. It has to be noted that in the MDPL case, both *change* and *no change* of the masking bit have been taken into account. Simulations, that have been carried out using Cadence Virtuoso and using the 40nm CMOS design kit from STMicroelectronics, have been performed using the same working condition. The power supply voltage has been set to 1V, and the clock frequency has been set to 10MHz. The evaluation phase duration for the D³L has been set to 1ns for these simulations. The output load capacitance C_{L1} on the *true* output of each sequential element has been set to 1fF, while the output load capacitance on the *false* output has been set from 1fF to 4fF (with steps of 1fF), to simulate mismatch conditions, from no mismatch (MF=1) to extreme mismatch (MF=4), as used in the previous section. Each 4-bit register has been driven by its respective converters (see Figure 4.41(a)), and in the case of CMOS, buffers are used instead of converters (see Figure 4.41(b)). The working temperature has been set to *room temperature* for each experiment. The simulation step is fixed to 20ps (which corresponds to 50GS/s of sampling rate), providing 5000 points per clock cycle.

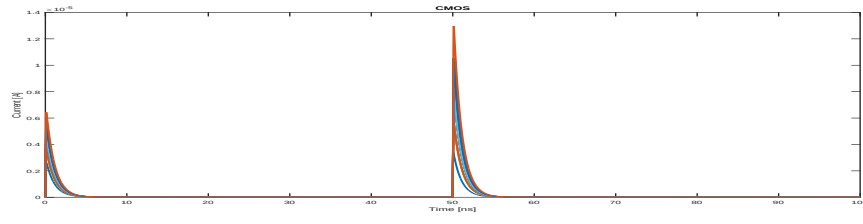
The results of the simulations are reported in Figure 4.43, using strong mismatch (MF=3) as representative case. The CMOS case is used as reference. It has to be mentioned that the first peak is referred to the rising edge of the clock signal, while the second one is related to the falling edge. In the first half of each plot in Figure 4.43, we have the evaluation phase (evaluation and post-evaluation for D³L). During the second half, the pre-charge phase takes place and both RTZ and TEL signals are forced to 0V. At a first glance, it is clear that for WDDL and MDPL, the current absorption has a really strong dependency on the stored data in the case of strong mismatch. The design of flip-flops in WDDL and MDPL styles suffer from strong leakage using the Hamming Weight, as it can be easily understand from

a visual inspection of power traces. The reason behind this strong dependency of the dynamic power consumption from the value of stored vectors, is due to the fact that they are based on CMOS D-type flip-flop, as storage element. In fact, Figure 4.43(c)-4.43(e) are very similar to Figure 4.43(a) in terms of variability of the current absorption regarding the input vectors.

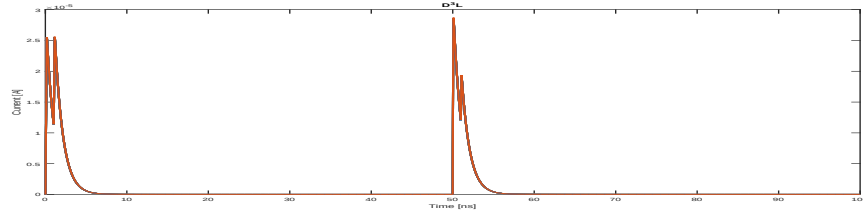
The presence of the DPL using RTZ encoding does not help to equalize the power consumption of the register regarding the stored data if capacitive mismatch exists. The information leakage that can be extracted for unbalanced WDDL and MDPL implementations can still reveal the internal state of the register, neglecting the intrinsic presence of redundancy for PAAs resilience. In Figure 4.44, the standard deviation of the 4-bit registers' noise-free current absorption traces are shown. The standard deviation is helpful in understanding where the power consumption has its maximum variability, since it is related to the magnitude of the data-dependent power consumption. In this simulation, current traces are noise-free, which allows us to highlight the information leakage magnitude of the dynamic consumption of registers' different implementations. As it can be noted from Figure 4.44, the maximum of the standard deviation due to data-dependency occurs during the falling edge of the clock signal (50ns to 100ns), which corresponds to the beginning of the pre-charge phase in all dual-rail implementations considered in this analysis. The WDDL register shows a similar behavior if compared to the CMOS counterpart, while the MDPL shows a higher standard deviation in both scenario. In the presence of strong mismatch, MDPL shows the worst performance among the considered ones, with a maximum of the standard deviation that is x4.63 and x6.20 higher than the CMOS. The proposed D³L allows to remarkably decrease the standard deviation of the absorbed current, also in the presence of strong mismatch. It has been found also in this case that the maximum of the standard deviation occurs at the falling edge of the clock signal, but its magnitude is significantly lower than CMOS. The maximum of σ_i is x0.05 compared to CMOS. The ability of the D³L in tolerating the presence of capacitive mismatch at the output has been tested and verified also in this context, since, in many cases, the most of the information leakage that can be extracted from a hardware implementation is due to the large dependence of the sequential elements' power consumption on the stored data. In Table 4.19, the maximum values of the standard deviation are reported for MF=3, using CMOS as reference.

Table 4.19. Maximum values of standard deviation of the noise-free current samples for the 4-bit registers in different logic styles with MF=3. CMOS implementation is used as reference.

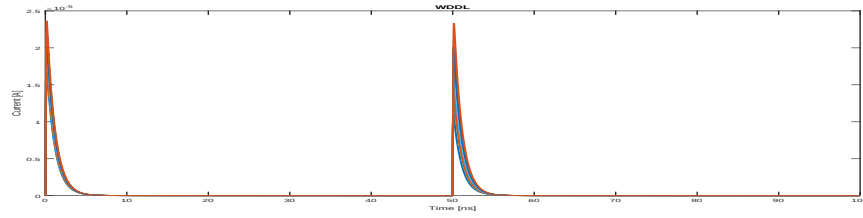
	CMOS	WDDL	MDPL (change)	MDPL (no change)	D ³ L
$\max(\sigma_i(t))$	$2.50\mu A$	$3.25\mu A$	$4.63\mu A$	$6.20\mu A$	$0.12\mu A$
Ratio	x1	x1.20	x1.85	x2.48	x0.05



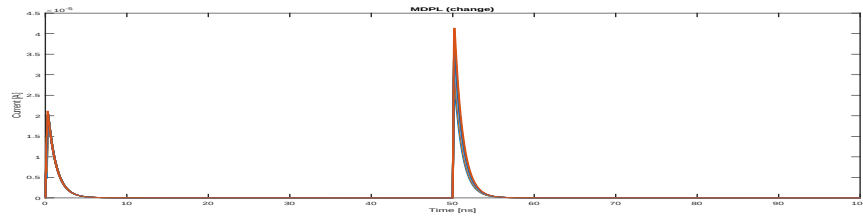
(a)



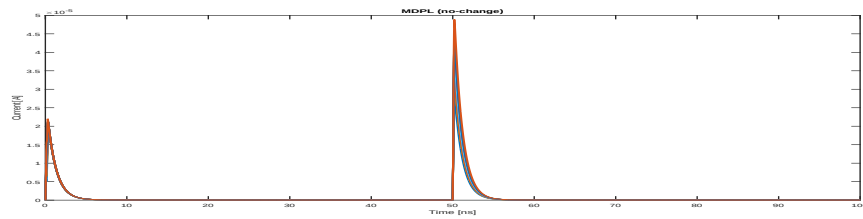
(b)



(c)

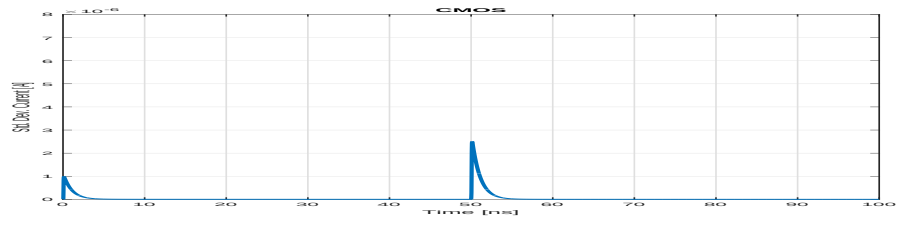


(d)

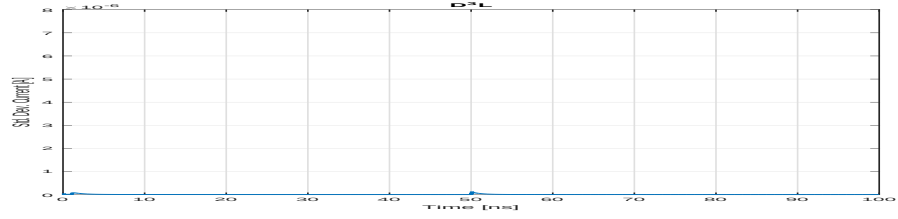


(e)

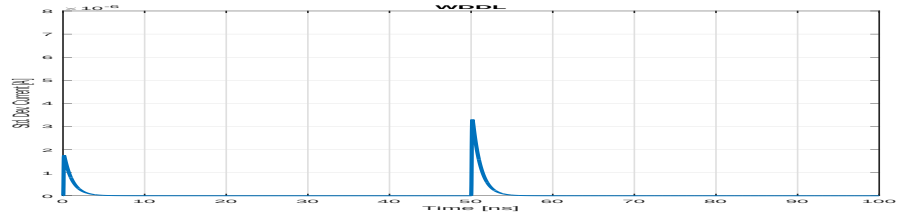
Figure 4.43. Current traces of 4-bit registers implemented in CMOS (a), D³L (b), WDDL (c), MDPL with change in the masking bit (d) and without change in the masking bit (e), using MF=3 (strong mismatch).



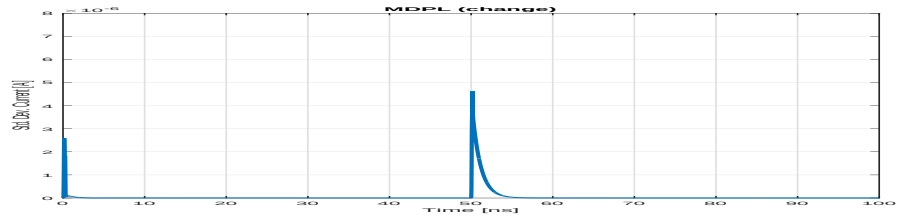
(a)



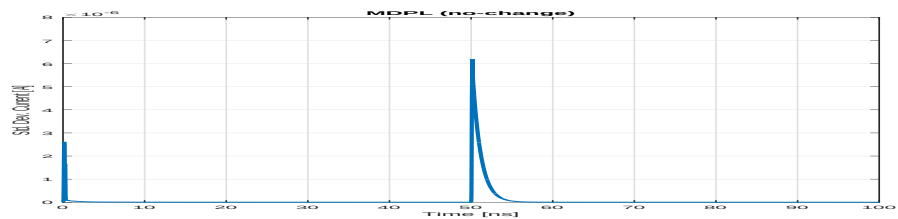
(b)



(c)



(d)



(e)

Figure 4.44. Standard deviation of the current absorption in a clock cycle as function of the time for the 4-bit registers implemented in CMOS (a), D³L (b), WDDL (c), MDPL with and without change in masking bit ((d) and (e) respectively).

Table 4.20. Comparison of the NED on the 4-bit registers.

Implementation	MF=1	MF=2	MF=3	MF=4
	[%]	[%]	[%]	[%]
CMOS	68.58	-	-	-
WDDL	45.57	43.86	40.69	37.95
MDPL-0	24.29	27.49	31.24	34.25
MDPL-1	23.32	23.33	23.34	23.36
D³L	1.54	1.47	1.40	1.34

Table 4.21. Comparison of the NSD on the 4-bit registers.

Implementation	MF=1	MF=2	MF=3	MF=4
	[%]	[%]	[%]	[%]
CMOS	26.95	-	-	-
WDDL	16.11	14.51	13.19	12.09
MDPL-0	7.12	8.36	9.54	10.65
MDPL-1	6.80	6.80	6.80	6.81
D³L	0.40	0.38	0.36	0.35

4.7.6 Timing Constraints

The combinational path in a pipeline stage reduces the actual evaluation phase duration. The minimum value of the evaluation phase at the output of the combinational path is bounded by the capability of the flip-flop to correctly sample the datum. In CMOS logic, as well as other DPL styles, the maximal length of the combinational path, namely the *critical path* length, is constrained by the maximum clock frequency and the *setup time* of the flip-flop. The *setup time* is defined as the time window in which the input data has to remain stable before the sampling edge of the clock signal to ensure the correct transfer of the data from the input to the output [4]. In addition, it is defined also the *hold time*, as the time window in which the input data of a flip-flop has to remain stable after the sampling edge of the clock signal to ensure a correct sampling operation. In most Master-Slave (MS) flip-flop types, it is mandatory that the clock-to-data delay t_{DC} has to satisfy the following condition [4]:

$$t_{DC} > t_{setup} \quad (4.44)$$

Table 4.22. Comparison of the average power P_{av} of the 4-bit registers.

	CMOS	WDDL	MDPL-0	MDPL-1	D ³ L
$P_{av} [\mu W]$	14.46	35.92	69.57	67.86	79.65

where t_{DC} represents the delay between data transition and the sampling edge of the clock signal. Then condition in Equation 4.44 is mandatory, and it has to be satisfied to maintain the correctness of the stored data. More in detail, a MS flip-flop has to match the condition in Equation 4.44 locally at master device, because it is designed to work alternatively with the slave device on opposite level of the clock signal.

In the TEL domain, the encoding of the signal is different from CMOS, and moreover, it has different requirements. The presence of a three-phases signaling, as discussed in Section 4.3.2, implies that every signal in the secured TEL domain has similar behavior, through each phase of the TEL paradigm. In this section, we want to present a set of timing constraints that the designer has to take into account to design a secure implementation with the D³L style.

Analyzing the D³L flip-flop in Figure 4.28, we can decompose its architecture in a TEL side and in a RTZ side. In the TEL side we have the TEL-to-RTZ and the RTZ-to-TEL converters, acting as input and output interfaces for the storage element. A primary constraints is due to the capability of the TEL-to-RTZ converter in Figure 4.30. It allows to convert the TEL data into a RTZ data, by means of a NAND SR latch. The limit of the NAND SR latch in distinguishing the two single-rail signals is established by the intrinsic inertial time of the latch itself. It has to be noted that TEL signals can only perform $0 \rightarrow 1$ transitions, that corresponds to the evaluation phase duration at the input of the flip-flop. This limitation impacts directly on the minimum $t_{eval,CL}$ that it is possible to guarantee the correct conversion of the TEL signal to the RTZ domain:

$$t_{eval,CL} \geq t_{lim} \quad (4.45)$$

For the 40nm CMOS design kit, it has been found that the minimum acceptable $t_{eval,CL}$ at the output of a combinational net is approximately 7ps:

$$t_{eval,CL}^{min} \approx 7ps \quad (4.46)$$

This value is directly related on the maximum number of logical depth of the longest path in between two flip-flops.

On the other side, the architecture of the D³L flip-flop is based on a MS flip-flop architecture using the RTZ encoding, with dynamic behavior. In fact, the two clocked latches in the D³L flip-flop, are based on the OR-gated NOR SR latch in Figure 4.32. As we have already discussed, this building block samples the input data at the falling edge of the clock signal. The sampled data, which is stored on the output capacitance of the OR-gate, is regenerated by the NOR SR latch, which is in *Hold state* when CK is low. In order to get the data correctly sampled, the OR-gated NOR SR latch, the clock-to-data delay t_{CD} has to be positive (see Equation 4.47). The definition of the t_{CD} is given in the following:

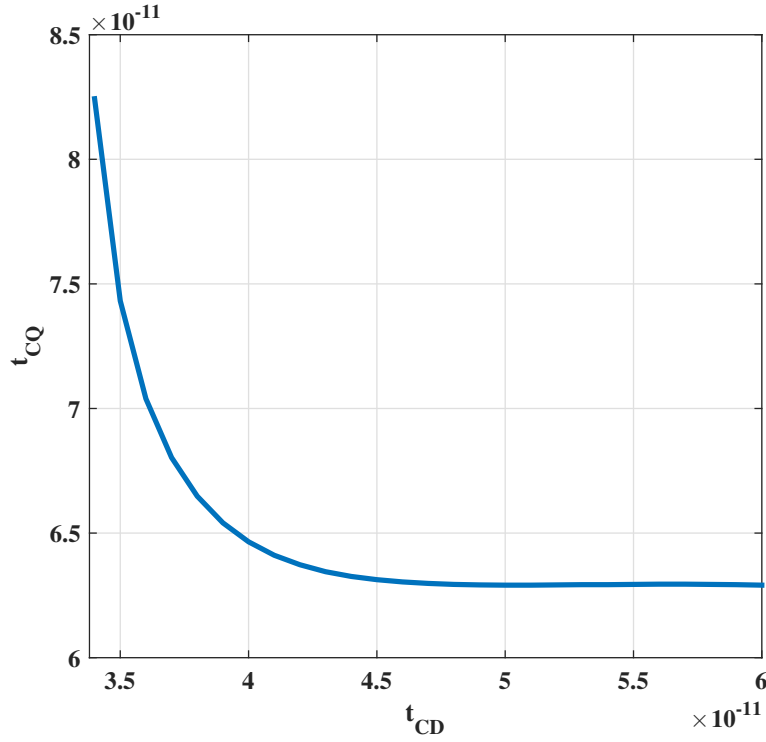


Figure 4.45. Plot of the t_{CQ} as function of data-to-clock t_{CD} .

$$t_{CD} = t_{rise,D/\overline{D}} - t_{rise,CK} > 0 \quad (4.47)$$

To ensure the correctness of the sampled data, the t_{CD} has to be constrained. In fact, if t_{CD} is too short, the NOR SR latch is not able to correctly sample the data at the falling edge of the clock. Similarly to a pulsed CMOS flip-flop, the D³L flip-flop has to provide a minimum t_{hold} , needed to provide a timing constraint. According to [4], the t_{hold} can be derived by analyzing the clock-to-Q delay t_{CQ} of the master latch as function of t_{CD} . Figure 4.46 shows the t_{CQ} as function of t_{CD} . The t_{hold} can be found as the value of t_{CD} that provides -1 as the value of the derivative of t_{CQ} in t_{DC} [4].

$$t_{hold} \rightarrow \frac{\delta t_{CQ}}{\delta CD}_{t_{CD}=t_{hold}} = -1 \quad (4.48)$$

It has been found that for the D³L flip-flop, the value of t_{hold} is $39.198ps$, with a minimum value of $t_{CQ,min}$ equals to $62.928ps$. The timing constraint to avoid t_{hold} violation is:

$$t_{CD} \geq 39.194ps \quad (4.49)$$

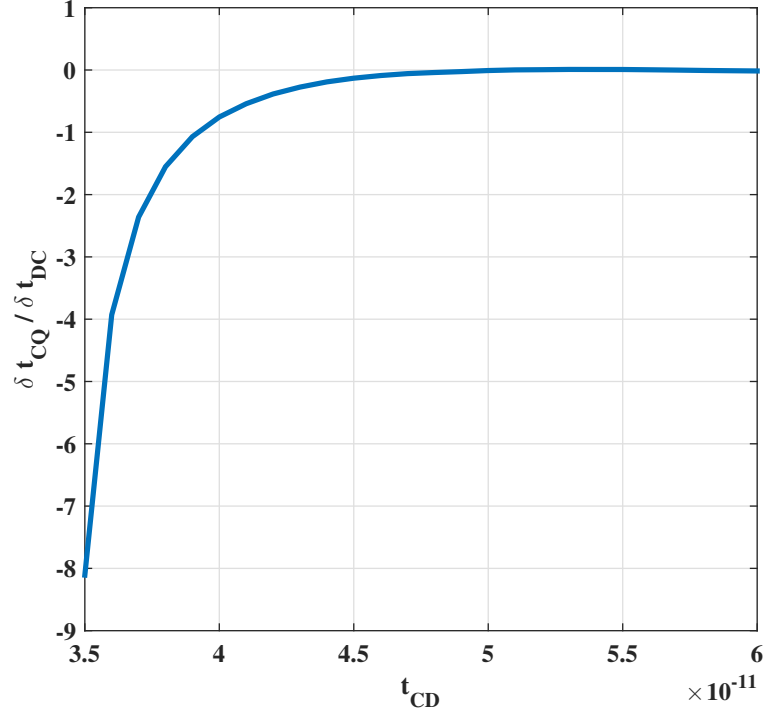


Figure 4.46. Plot of the derivative of the $\delta t_{CQ} / \delta t_{DC}$ as function of data-to-clock t_{CD} .

To resume the timing constraints of the D³L with the 40nm design kit:

1. $t_{eval,CL} \geq t_{eval,CL}^{min} = 7ps$
2. $t_{CD} \geq t_{hold} = 39.194ps$

These values are collected on pre-layout simulations, so, they are given as best-case estimations. As it is clear, we expect higher values taking into account the presence of parasitic capacitance and resistance of local routing wires. In TEL compatible logic, we have to deal with two different timing constraints, since we have on one hand the evaluation phase duration at the output of combinational path $t_{eval,CL}$, and on the other one, the delay of the TEL signal compared to clock t_{CD} . In fact, we must consider that D³L is a domino logic, similarly to WDDL. It is worth noting that WDDL and D³L share also the *pre-charge wave*, but in this case, we have both *pre-charge wave* and *evaluation wave*.

4.8 D³L Implementation of the 4-bit PRESENT Crypto-Core

Analysis performed on combinational gates and sequential element, and presented in previous section, have been conducted only on basic elements of D³L style. The adoption of the DPL approach with TEL signaling has led to the design of a new template for a standard-cell based logic style, which is able to thwart PAAs and to deal with electrical mismatch due to capacitive unbalance. In this section, we analyze the ability of the core to counteract PAAs, adopting the same approach used previously, in order to simulate various level of capacitive mismatch. The 4-bit PRESENT crypto-core, used in the Chapter 3, has been adopted as case study to evaluate the vulnerability of the D³L to power analysis in a more realistic environment. The crypto-core has been designed in Cadence Virtuoso using the aforementioned 40nm STMicroelectronics design kit. The RTL implementation of the crypto-core is shown in Figure 4.47. To take into account the presence of mismatch, a specially designed block has been connected to the output each D³L gate (both combinational and sequential). This block contains two capacitors, as shown in Figure 4.48. Single lines in Figure 4.47 represents single-rail signals (CMOS domain), while double line ones are referred to TEL-domain signals. In order to compare the effectiveness of the D³L in thwarting PAAs with other standard cell based gate-level countermeasures, WDDL implementation has been designed.

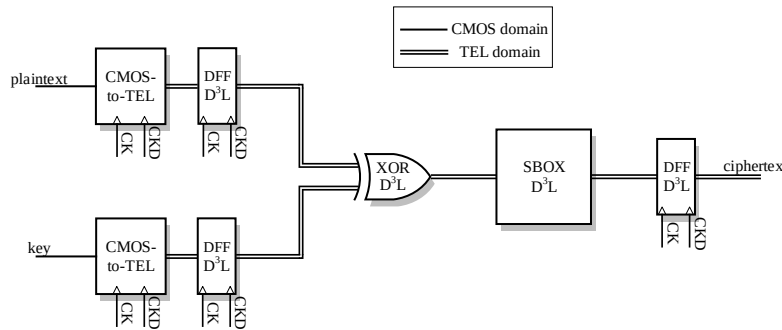


Figure 4.47. RTL schematic of the implementation of the 4-bit PRESENT crypto-core with D³L style.

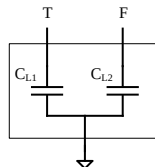


Figure 4.48. Output load for each gate (both combinational and sequential) in the analysis of the 4-bit PRESENT crypto-core, to simulate the presence of mismatch.

4.8.1 Proof of PAA Resistance using Correlation Power Analysis

Simulated CPA attacks on a 4-bit PRESENT crypto-core using D³L style are presented in this section, adopting a WDDL implementation for a straight comparison with a common RTZ-based standard-cell logic style. The clock frequency has been set to 10MHz, and the core voltage is kept constant at 1V. In order to get a more realistic behavior of the simulation, the noise-free samples collected in Cadence Virtuoso have been processed in Matlab. Additive Gaussian noise has been added to the data set, according to previous works [125] [20], in order to take into account the presence of both electronic and switching noise. The standard deviation of the additive noise σ_{noise} has been set to $1^{-5}A$. Moreover, simulations time resolution is too optimistic, since samples have been collected with a time step of 20ps, which roughly corresponds to a very expensive 50GS/s DSO. In Section 4.3.1 we have introduced the concept of *Perfect Adversary model*, assuming that the adversary has infinite bandwidth and infinite storage capability. The adversary model introduced with TEL principle deals with a more realistic scenario. In the TEL adversary model, he/she has limited bandwidth and storage capability, hence, which, in fact, reduces the feasibility of a successful attack. As we have discussed in Section 4.7.2, the duration of the *evaluation phase* D³L states a lower bound on the minimum bandwidth that the adversary should have to mount a successful PAA. To verify that this property holds, we have decimated simulated power traces in Matlab, using a custom function. This function filters power traces to avoid aliasing effect due to decimation, and then reduces the sampling rate to the desired one. In addition, we have considered to filter power traces set using the output Nyquist's frequency as cut-off. Thus, we have assumed that the analog front-end of the emulated DSO provides an analog bandwidth equal to the corresponding Nyquist's bandwidth. Generically, analog front-end circuitry has a cut-off frequency which is less than the Nyquist limit. Oversampling analog-to-digital converters are commonly adopted in most of modern DSOs, featuring the possibility to reduce noise by using post-sampling processing:

$$f_{analogFE} < f_{Nyquist} \quad (4.50)$$

We present the following cases:

1. High grade DSO with 10GS/s;
2. Mid grade DSO with 1GS/s;
3. Low grade DSO with 500MS/s.

The D³L and WDDL implementations of the 4-bit PRESENT crypto-core has been simulated with a strong mismatch (MF=3), which can be assumed as the regular case in a FPGA implementation. For this evaluation, 100k power traces (for each core and for each case) have been generated to perform CPA attacks.

In all cases, the 4-bit output word of the S-BOX function has been adopted as target intermediate result. The key has been fixed to $(5)_2$. The D³L evaluation phase has been set to 1ns. The testbench used for this experiment is the same of Figure 4.39. In Figure 4.49-4.50, noise-free power traces collected on D³L and WDDL implementations are shown. The current absorption in D³L exhibits a very small variations with the input plaintext, and the only evidence in the difference of plaintext due to mismatch is visible only during the *evaluation phase*, that is confined in a 1ns time window. The only possibility to capture the data-dependency in the current absorption is confined in this short time window, making straightforward to mount an attack. For the WDDL implementation, the data-dependency is stronger with the same MF. In fact, it will be simpler to attack the unbalanced WDDL implementation, and the requirement on the sampling rate will be way less stringent. It has to be pointed out that the strongest variation of the current absorption appears at the beginning of the pre-charge, that corresponds to the falling edge of the clock signal. As we will see, it will provide two correlation peaks using CPA attack.

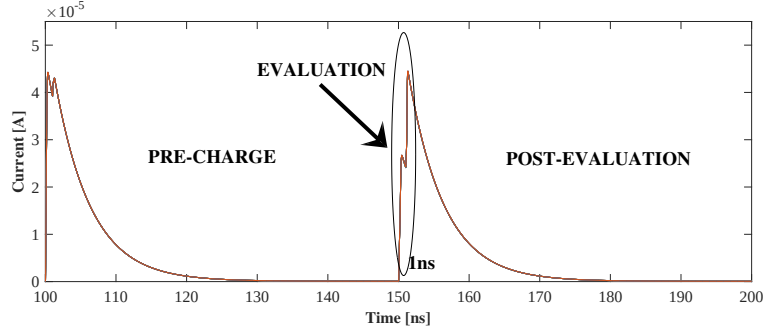


Figure 4.49. Noise-free power traces collected on D³L implementation of 4-bit PRESENT crypto-core with $t_{eval} = 1ns$ and $MF = 3$. The sampling rate of the simulator is 50GS/s.

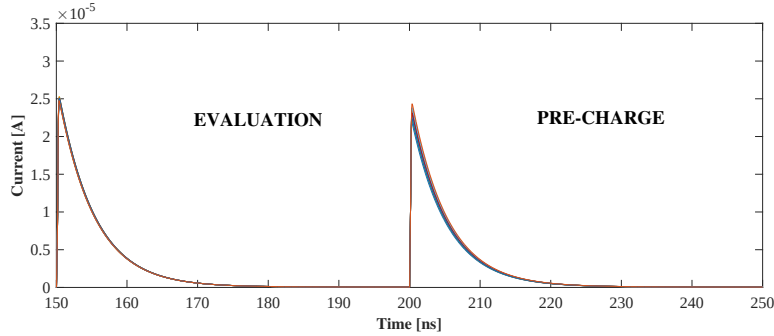


Figure 4.50. Noise-free power traces collected on WDDL implementation of 4-bit PRESENT crypto-core with $MF = 3$. The sampling rate of the simulator is 50GS/s.

4.8.2 High grade DSO, Case 1

In case 1, the high grade DSO is assumed to simulate the attack. The sampling rate is reduced to 10GS/s before executing the attack script. The time resolution in

case 1 becomes 100ps/pts. In D³L implementation, the *evaluation phase* contains 10 current samples. The CPA attack using 100k measurements yields to a MTD of $\approx 37k$ power traces for the D³L implementation and to ≈ 1000 for WDDL. The correlation coefficient value is reduced from 71.7×10^{-3} for WDDL to 20.5×10^{-3} for D³L. It has to be noted that the correlation coefficient for the D³L implementation appears only during the *evaluation phase*, as it was expected. The peak is composed by 9 time samples, which corresponds to the 90% of the *evaluation phase* length. In the WDDL implementation, we have two correlation peaks, as it was expected comparing Figure 4.50. In fact, the visual inspection of the noise-free samples has highlighted that there is a strong dependency of the current absorption at both clock edges. Hence, we have found correlations between processed data and current absorption in two time points, corresponding to the beginning of the *pre-charge* and the beginning of the *evaluation phase*.

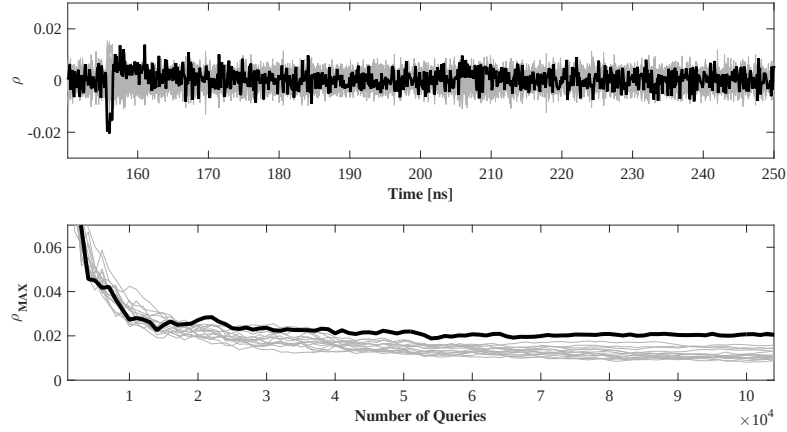


Figure 4.51. Plots of simulated CPA attack on the D³L implementation with $t_{eval} = 1ns$, using a high grade DSO (10GS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

4.8.3 Mid Grade DSO, Case 2

In case 2, the mid grade DSO post-processing has been used, and the sampling rate is reduced to 1GS/s, corresponding to a time resolution of 1ns/pts. This is a very common choice for a not expansive DSO (generically, it costs under 10k€), and it represent the average case. The *evaluation phase* of the D³L is sampled with only 1 point in time. In fact, in this case, the result of the CPA attack on the D³L is less accurate, and correct key's correlation coefficient is slightly higher than the best ranked wrong key ($SVI_{\%} = +6.18\%$). However, it is possible to identify an MTD of $\approx 77k$ measurements. The correlation peak contains only 1 sample, that can be considered as the only relevant for the PAA for the D³L. In this case, it is critical the jitter value on the DSO. We have hypothesized zero jitter, and a perfect phase

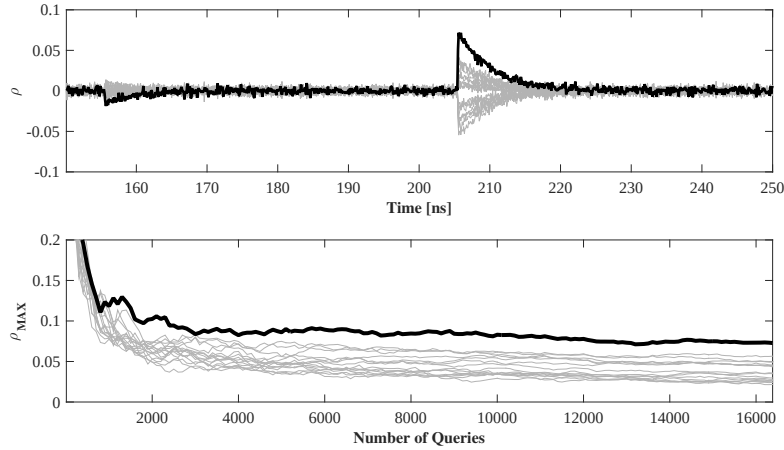


Figure 4.52. Plots of simulated CPA attack on the WDDL implementation, using a high grade DSO (10GS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

alignment between the sampling and the *CK* signal. These assumptions allow us to define a worst-case situation for the designer, in order to present *pros* and *cons* of the D³L. In general, the jitter of the DSO's sampling clock is non zero, and also the phase alignment with the core's clock signal is almost impossible; consequently, the correlation coefficient could significantly be smaller, and the attack could provide poorer results. With the mid grade DSO situation, the WDDL implementation exhibits a MTD of 1100, that is slightly higher than case 1. The correct key's correlation coefficient with 100k power measurements and the time positions of correlation peaks are similar.

4.8.4 Low Grade DSO, Case 3

Attacks performed assuming low grade DSO (case 3) are very significant. Lower grade DSOs have lower sampling rates and reduced analog bandwidth compared to more expensive equipment. They are widely diffused, due to lower cost, but also less effective in performing power analysis attacks. In this case, the sampling rate of the DSO has the most critical impact on the effectiveness of the attack for the D³L implementation. In case 3, the sampling rate is reduced to 500MS/s, resulting in 0.5 sample/pts for the evaluation phase. The D³L implementation has a MTD higher than the maximum number of generated measurements ($MTD > 100k$). The SVI is always negative in this case, and the attack is unsuccessful. According to TEL assumptions discussed in Section 4.3.1, the sampling rate of case 3 is not sufficient to mount a successful attack, since the information leakage is completely out of the available bandwidth. The correct key's correlation coefficient is strongly reduced compared to best ranked wrong key ($SVI_{\%} = -28.72\%$). Regarding the WDDL

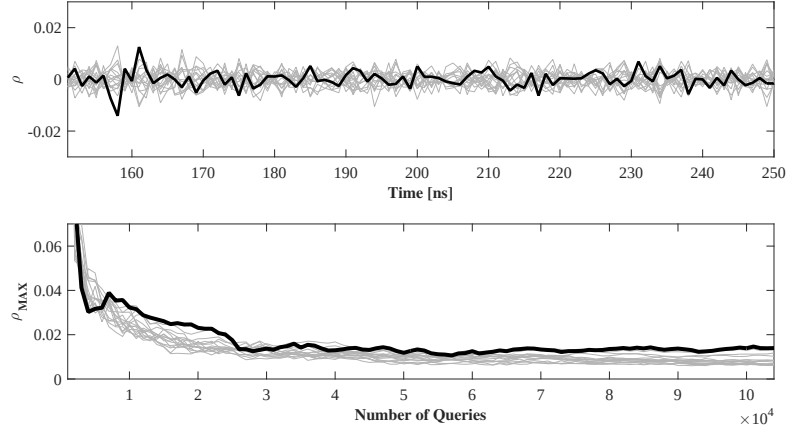


Figure 4.53. Plots of simulated CPA attack on the D³L implementation with $t_{eval} = 1ns$, using a mid grade DSO (1GS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

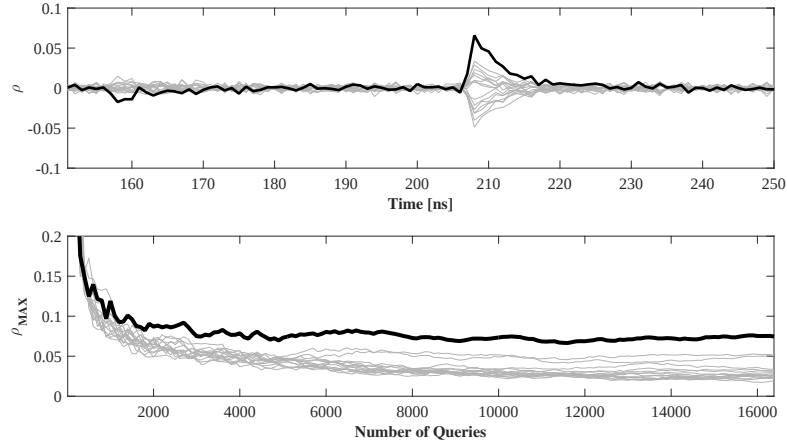


Figure 4.54. Plots of simulated CPA attack on the WDDL implementation, using a mid grade DSO (1GS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

implementation, CPA attacks is successful with a MTD of $\approx 6.6k$ measurements. It is worth noting that the correct key's correlation coefficient peak has a huge spread with wrong keys' correlation coefficients ($SVI_{\%} = +30.13\%$). In fact, as we have discussed in Section 4.7.2, WDDL style (and more in general, RTZ-compatible DPLs) exhibits higher values of FED at low frequency compared to TEL-compatible circuits, and reducing the bandwidth, we filter also the noise as well. Comparing the correct key's correlation coefficient value for both implementations, the D³L is able to reduce it by a factor of $0.0604/0.0094 \approx 6.43$.

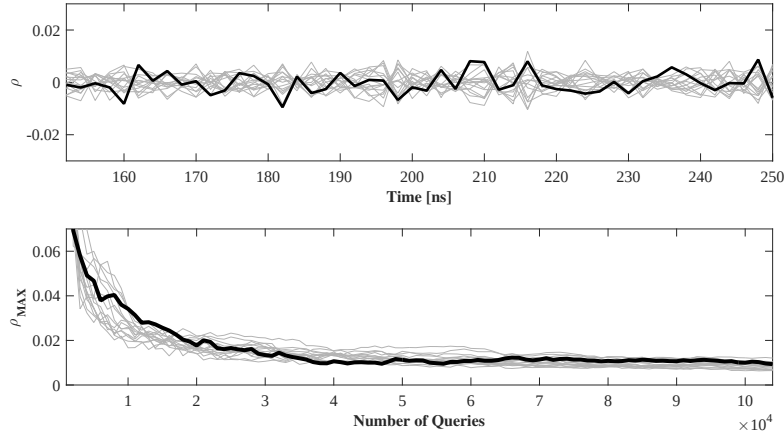


Figure 4.55. Plots of simulated CPA attack on the D³L implementation with $t_{eval} = 1ns$, using a low grade DSO (500MS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

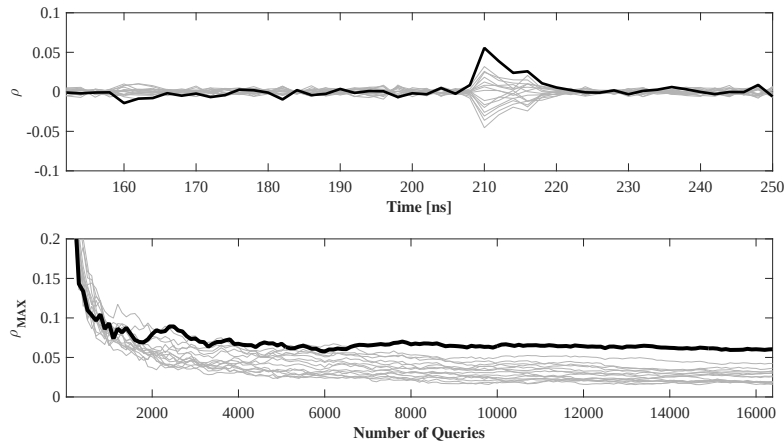


Figure 4.56. Plots of simulated CPA attack on the WDDL implementation, using a low grade DSO (500MS/s). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

4.8.5 D³L with $t_{eval}=500ps$

As additional case study, we have also simulated the D³ implementation with $t_{eval} = 500ps$, in order to better evaluate the relation between the value of t_{eval} with the attack capability of the adversary. Results of the attack are shown in Figure 4.57. The chosen value of t_{eval} requires a minimum sampling rate of 4GS/s, that can be considered halfway between mid and high grade DSO in our analysis. Also this

Table 4.23. Summary of the CPA attacks results on the 40nm implementation of 4-bit PRESENT crypto-core with D³L and WDDL styles.

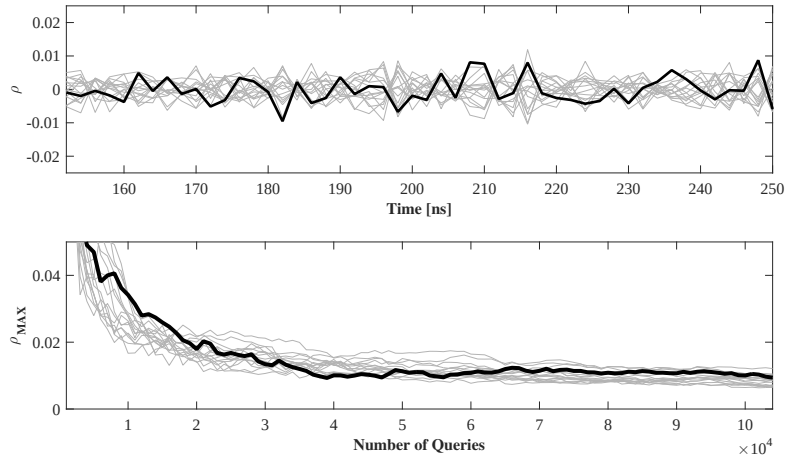
		ρ_{corr}	SVI	SVI%	MTD
D ³ L with $t_{eval} = 1ns$	Low Grade DSO	0.0094	-0.0027	-28.72%	> 100k
	Mid Grade DSO	0.0140	+0.0009	+6.14%	~ 77k
	High Grade DSO	0.0205	+0.0047	+22.78%	~ 37k
D ³ L with $t_{eval} = 500ps$	Low Grade DSO	0.0094	-0.0027	-28.62%	> 100k
	Mid Grade DSO	0.0106	-0.011	-10.96%	> 100k
	High Grade DSO	0.0205	+0.0047	+22.78%	~ 38k
WDDL	Low Grade DSO	0.0604	+0.0182	+30.13%	~ 6.6k
	Mid Grade DSO	0.0668	+0.0175	+26.14%	1100
	High Grade DSO	0.0717	+0.0173	+24.13%	1000

scenario has been evaluated using three DSO grades presented previously.

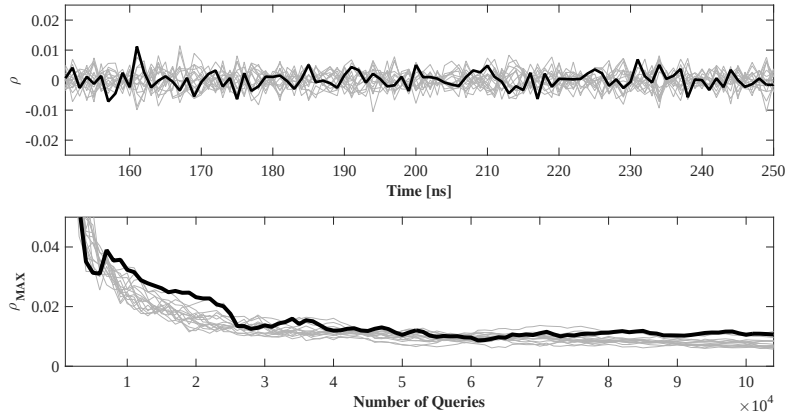
The attack has been successful only in case 1, where the sampling rate is reasonably high to correctly capture the information leakage during the *evaluation phase*. The MTD in this case is $\approx 38k$ current measurements, which is also similar to case 1 of previous section also in terms of correlation coefficient's value. Low and mid grade DSOs do not meet requirements for mounting a successful attacks, thus the MTD is always higher than 100k. Also the SVI is sufficiently higher to avoid a successful recovering of the secret key.

4.8.6 Final Remarks on PAA-Resilience of D³L

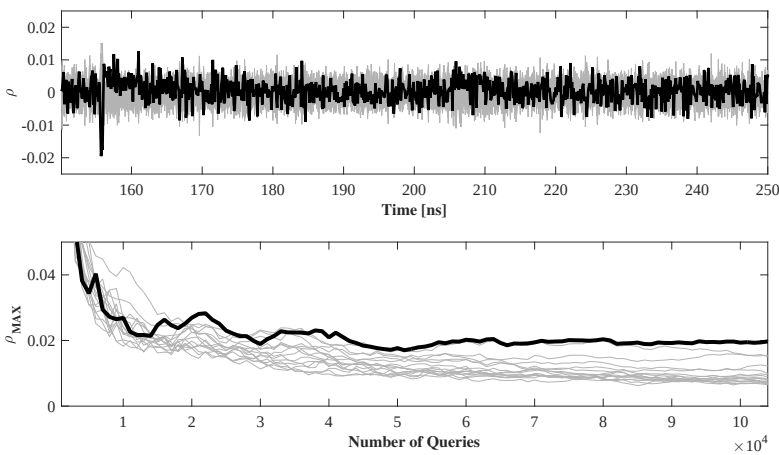
In this section, we have demonstrated how the D³L style is able to protect a cryptographic circuit from PAA, also in the presence of mismatch. The validation has confirmed also main assumptions of TEL signaling regarding the adversary model. It has been found that the the duration of the *evaluation phase* t_{eval} affects the minimum requirement of available bandwidth and sampling rate for the adversary. Compared to WDDL, the D³L has been found dramatically more resistant if the t_{eval} is very short. The analysis presented in this section has been carried out without the proper filtering capacitance (only 50pF has been used, that is a very small capacitor for a 4-bit PRESENT crypto-core), allowing us a case study in worst-case scenario. The presence of a proper sized filtering capacitance on the supply net will improve the ability of the D³L to minimize the residual information leakage at high frequency, that is possible to capture only with very high sampling rate (>1GS/s). Results presented in this section are summarized in Table 4.23.



(a)



(b)



(c)

Figure 4.57. Plots of simulated CPA attack on the D³L implementation, with $t_{eval} = 500ps$, using a low grade DSO (500MS/s) (a), mid grade DSO (1GS/s) (b) and high grade DSO (10GS/s) (c). Top figures show the correlation coefficient ρ vs. current traces time samples. Bottom figures show the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

4.9 FPGA Implementations using the D³L

The developing process of new countermeasures should take every abstraction level of the design, from the concept to the real and physical implementation. At each level, the new countermeasure has to be tested, to evaluate the strength and potential weakness. Starting from a model, which relies on a mathematical background, the designer can take advantage of the ease of use, making the new countermeasure as more *bullet-proof* as possible. In previous sections of this chapter, we have discussed about the physical modeling and the mathematical background of the use D³L as gate-level countermeasure against PAAs. The characterization using Cadence Virtuoso and the 40nm STMicroelectronics digital design kit makes use of very accurate BSIM4 models, provided by the foundry. Since the presence of the capacitive unbalance (as well as other electrical mismatch and non-idealities) and its impact on the secure device's developing cost forces the designer to adopt more complex design flow, we want to provide an easier way to design trustworthy platforms and devices using the D³L style, without the presence of additional steps to deal with those implementation problems. In this section, we present the design of a D³L library that allows designers to implement cryptographic accelerator for FPGA applications without the effort of a secure design flow. The library, written in VHDL language, has been tested functionally on two different FPGAs:

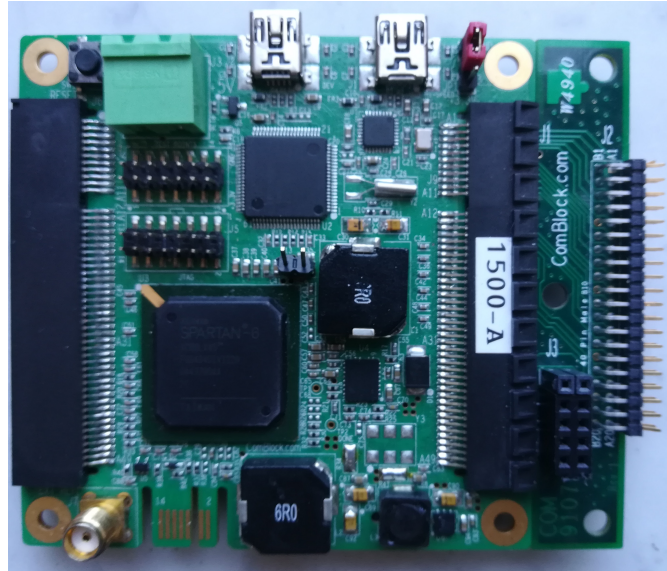
- Xilinx Spartan-6 LX45 (45nm process);
- Altera Cyclone-IV EP4CE10E22C8 (65nm process).

The hardware description has been elaborated using the two development environment of their respective vendors:

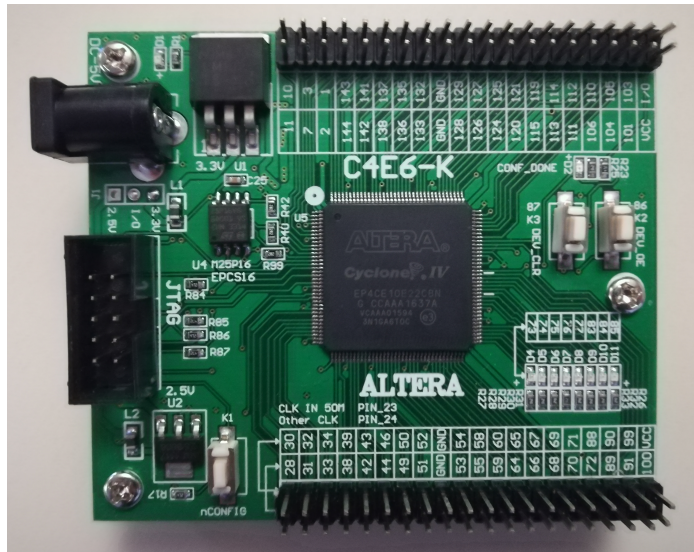
- Xilinx ISE 14.1;
- Altera Quartus II 13.0.

Basically, the VHDL code for the library is almost the same. In fact, since the two development and synthesis applications (and their respective design tool-chains) have slight differences, *attributes* and *synthesis directives* are different as well. In fact, the approach behind the D³L VHDL library is "**keep it simple**", in order to simplify the adoption of this novel logic style. As we will see in the next section, the same VHDL code has been used for ASIC implementations.

It has to be mentioned that this is the first implementation of the D³L on a real platform, in order to understand if the novel logic style along with TEL signaling could be supported using FPGA as final hardware platform. The degrees of freedom in designing digital circuits for FPGAs are relatively low if compared to ASIC designs, and thus, implies that the presence of additive leakage due to imperfect balancing in load capacitance is more evident and less controllable. Therefore, the



(a)



(b)

Figure 4.58. FPGA boards. In (a), the ComBlock COM 1500-A board [44] with the Xilinx Spartan-6 LX45 FPGA chip. In (b), the EP4C10 development board with the Altera Cyclone-IV EP4CE10E22C8.

possibility to design secure implementations without the additional effort due to balancing capacitive loads (see [70], [9]) can significantly reduce the developing time and cost. In literature, there are no implementations that make use of TEL signaling for FPGA applications. So far, this is the first attempt to provide a TEL compatible logic style suitable for FPGA applications.

4.9.1 Combinational Logic

In a regular design flow with default settings, the redundancy is often optimized away, to improve the three main factors in a digital design:

- area occupation;
- maximum frequency;
- power consumption.

Generically, the synthesizer is set to drive the synthesis engine to improve one (or at least two) of these aspects. With this aim, the designer should write a constraint file (e.g. *.sdc* files) to drive the synthesizer to his/her needs. In D³L, the combinational logic contains a huge amount of redundancy, as shown in Figure 4.17 and Figure 4.15, to satisfy requirements of TEL signaling. Four NAND2 are required to implement the first evaluation level, and two NAND3 for the second one (two NAND2 for the XOR/XNOR gate). In most VHDL synthesizer, the following code, which describes the behavior of a D³L AND/NAND gate, will be optimized if not correctly addressed:

```

AND
data_O(1) <= '1' NAND ('1' NAND (data_A(1) NAND data_B(1)));
NAND
data_O(0) <= (data_A(0) NAND data_B(0)) NAND (data_A(1) NAND
data_B(0)) NAND (data_A(0) NAND data_B(1));

```

where signals with *(1)* are intended to be the *true* signals, while signals with *(0)* are intended to be the *false* signals. Without any kind of specifications, the synthesizer will build the AND function as a pure AND, while the NAND function will be implemented using the correct NAND architecture depicted in Figure 4.17(a). This synthesis carries internal unbalance, which will cause additional leakage due differences in power consumption and time propagation within the two compounds. To force the synthesizer to design the AND/NAND gate, we decided to design the NAND3 as separate entity, using the followings attributes:

```

Altera CycloneIV attributes
attribute dont_touch : boolean;
attribute dont_touch of NAND_3IN : entity is true;
attribute syn_keep : boolean;

```

```

attribute of A, B, C, F : signal is true;
attribute altera_attribute : string;
attribute altera_attribute of NAND_3IN : entity is "name_
    REMOVE_DUPLICATE_LOGIC_OFF";
attribute altera_attribute of A, B, C : signal is " name_
    IGNORE_LCELL_BUFFERS_ON";

```

Xilinx Spartan6 attributes

```

attribute KEEP_HIERARCHY : string;
attribute KEEP_HIERARCHY of NAND_3IN_architecture : architecture is
    "YES";

```

where A , B and C are the input signals of the NAND3 and F is the NAND3's output signal. The behavior description of the NAND3 gate can be rewritten as:

```

F <= '0' when (A='1' AND B='1' AND C='1') else '1';

```

The NAND3 can be now used as a standalone component, since its architecture and attributes are correctly defined and the synthesizer cannot modify it, during the optimization process. The first evaluation level has been designed with basic NAND2, defined in the IEEE VHDL library. The VHDL code for the complete 1st evaluation level and the connection with the 2nd level is shown in the following:

...

Altera CycloneIV attributes

```

signal data_VDD1, data_VDD2 : std_logic := '1';
attribute syn_keep : boolean;
attribute syn_keep of data_C, data_D, data_E, data_F : signal is true;
attribute syn_keep of data_VDD1, data_VDD2 : signal is true;

```

Xilinx Spartan6 attributes

```

attribute KEEP_HIERARCHY: string;
attribute KEEP_HIERARCHY of D3L_AND_NAND_architecture:
    architecture is "YES";

```

begin

1st evaluation layer

```

data_C <= data_A(1) NAND data_B(1);
data_D <= data_A(0) NAND data_B(0);
data_E <= data_A(1) NAND data_B(0);
data_F <= data_A(0) NAND data_B(1);

```

2nd evaluation layer

N1 : NAND_3IN

port map (

A => data_C,

B => data_VDD1,

```

    C => data_VDD2,
    F => data_O(1)
  );

N2 : NAND_3IN
port map (
  A => data_D,
  B => data_E,
  C => data_F,
  F => data_O(0)
);

for Xilinx Spartan6 only
P1 : PULLUP
port map(
  O => data_VDD1
);

P2 : PULLUP
port map(
  O => data_VDD2
);

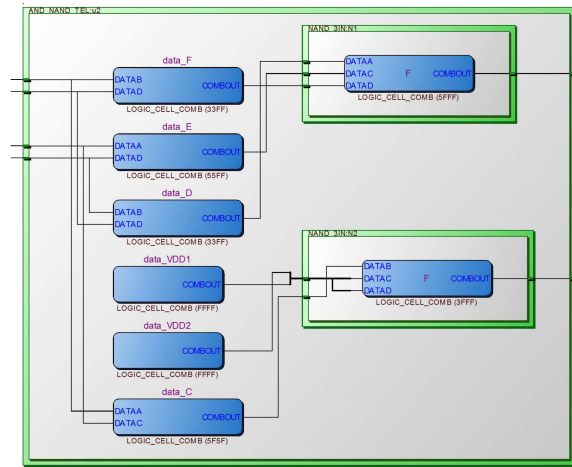
end architecture;

```

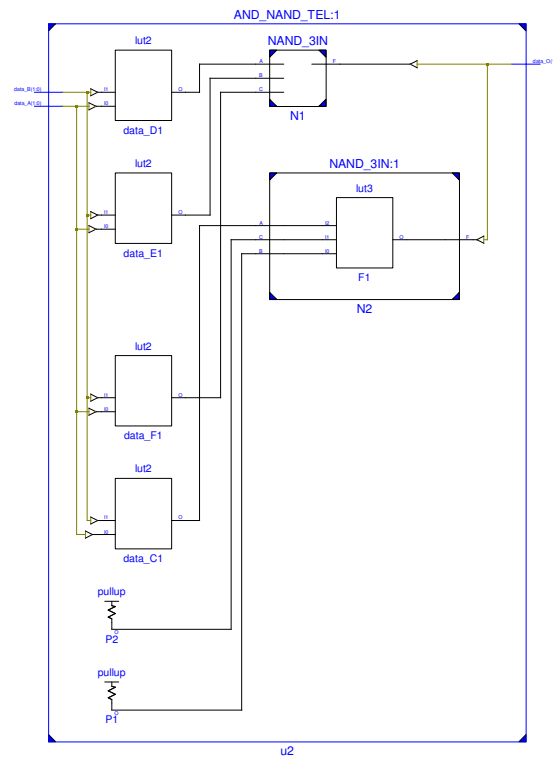
The signals *data_VDD1* and *data_VDD2* are used to tie up two unused input ports of the NAND3 gate on the *true* branch of the D³L AND/NAND gate. Definitions of these two signals are different with the target FPGA. For the Altera Cyclone-IV, we have defined them as *std_logic* tied up to logical '1', inserting the *syn_keep* attribute to avoid optimization during the synthesis. Attributes on *data_VDD1* and *data_VDD2* signals force the synthesizer to instantiate two LUT providing both the logical output '1'. Since Xilinx ISE does not support directly the same approach to tie up cell, we have adopted the *PULLUP* Xilinx primitive, which is recalled from the *UNISIM.VComponents* library, available with the development environment. This primitive allows to tie up the signal to logical '1'. Results of the post-synthesis are shown in Figure 4.59.

The same approach has been used to design the OR/NOR gate, which also requires two NAND3 gates on the 2nd evaluation level. The design of the D³L XOR/XNOR is slightly different, since the 2nd evaluation level requires only NAND2 gate. In this case, the definition of the XOR and XNOR compound requires only *syn_keep* attributes for the Altera Cyclone-IV implementation. In Xilinx ISE, it is needed to specify the *save_net_flag* to avoid the optimization of the flattened design. So far, the XOR/XNOR design in Xilinx ISE has required the additional attribute *S* as shown in the following code:

...



(a)



(b)

Figure 4.59. Post-synthesis and post-optimization technology view of the D³L AND/NAND gate with Altera Quartus II 13.0 (a) and Xilinx ISE 14.1 (b).

Altera Cyclone IV attributes

```
attribute syn_keep : boolean;
attribute syn_keep of data_C, data_D, data_E, data_F : signal is true;
```

Xilinx Spartan6 attributes

```
attribute KEEP_HIERARCHY : string;
attribute KEEP_HIERARCHY of D3L_XOR_XNOR_architecture:
    architecture is "YES";
attribute S : boolean;
attribute S of data_C : signal is true;
attribute S of data_D : signal is true;
attribute S of data_E : signal is true;
attribute S of data_F : signal is true;
```

```
begin
```

XNOR

```
data_C <= data_A(1) nand data_B(1);
data_D <= data_A(0) nand data_B(0);
data_O(0) <= data_C nand data_D;
```

XOR

```
data_E <= data_A(0) nand data_B(1);
data_F <= data_A(1) nand data_B(0);
data_O(1) <= data_E nand data_F;
```

```
end architecture;
```

The post-synthesis and post-optimization results with both development environment are shown in Figure 4.60.

It has to be noted that the results of the synthesis is correctly mapped into LUT2 implementing NAND2 operation.

4.9.2 Sequential Element

The implementation of the sequential element is commonly used standard-cell based DPL styles, such as WDDL and MDPL, relies on the CMOS D-type flip-flop. In FPGAs, 1-bit flip-flops are usually available at each basic module, providing both storage and basic 2-input computation (such as AND2 function). In Altera Cyclone-IV, the basic element, named *Logic Element* and shown in Figure 4.61, is composed by a 4-inputs LUT, a 1-bit configurable register, and internal routing circuitry [8].

In the Xilinx Spartan-6 family, there are three main version of the basic element, named *SLICEX*, *SLICEL* and *SLICEM*. The SLICEX version [153] is the smallest

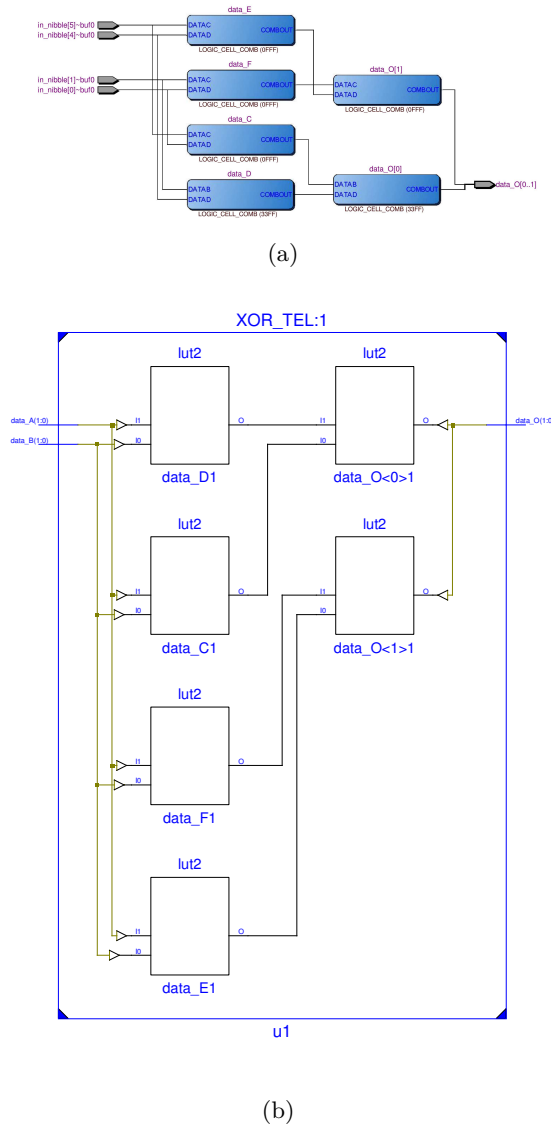
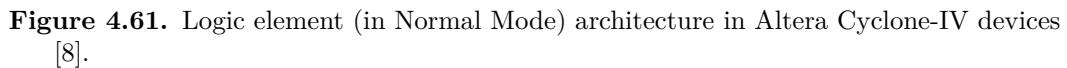


Figure 4.60. Post-synthesis and post-optimization technology view of the D³L XOR/XNOR gate with Altera Quartus II 13.0 (a) and Xilinx ISE 14.1 (b).

among the others and contains four 6-inputs LUTs, 8 flip-flops and internal routing circuitry, as shown in Figure 4.62. SLICEX basic elements represent almost 50% of the total basic elements pre-implemented in a Xilinx Spartan-6 LX45 FPGA.

A huge fraction of the information leakage that can be exploited from power consumption is usually provided by storage elements. In Section 4.6, we have introduced the sequential element in D³L style. As it can be noted from Figure 4.30 and Figure 4.32, the D³L sequential element can be implemented using combinational gates, avoiding the adoption of optimized scheme often used to implement flip-flops in ASIC and FPGA integrated circuits. In fact, from the analysis in Section 4.7.5, it has been found that flip-flops based on the CMOS D-type flip-flop from the



The first building block of the D³L D-type flip-flop is the TEL-to-RTZ converter in Figure 4.30, which is basically a NAND SR-latch. The VHDL code of the NAND SR-latch in its combinational gates implementation, usually provides warning messages. In fact, in VHDL, a SR-latch is recognized as a *combinational loop*, which provides a latching behavior. Designs which contain latches can have issues in terms of timing violations and unwanted behavior. In this case, we want to instantiate a latch to provide the conversion from a domain to the other. To make sure that the synthesizer does not optimize the latch, attempting to remove the combinational loop and preserving the time enclosure of the hierarchy, we have used synthesis attributes in both FPGA designs, as shown in the followings:

Altera Cyclone IV attributes

Xilinx Spartan6 attributes

```

attribute KEEP_HIERARCHY : string;
attribute KEEP_HIERARCHY of TEL_2_RTZ_architecture : architecture
    is "YES";
attribute S : boolean;

```

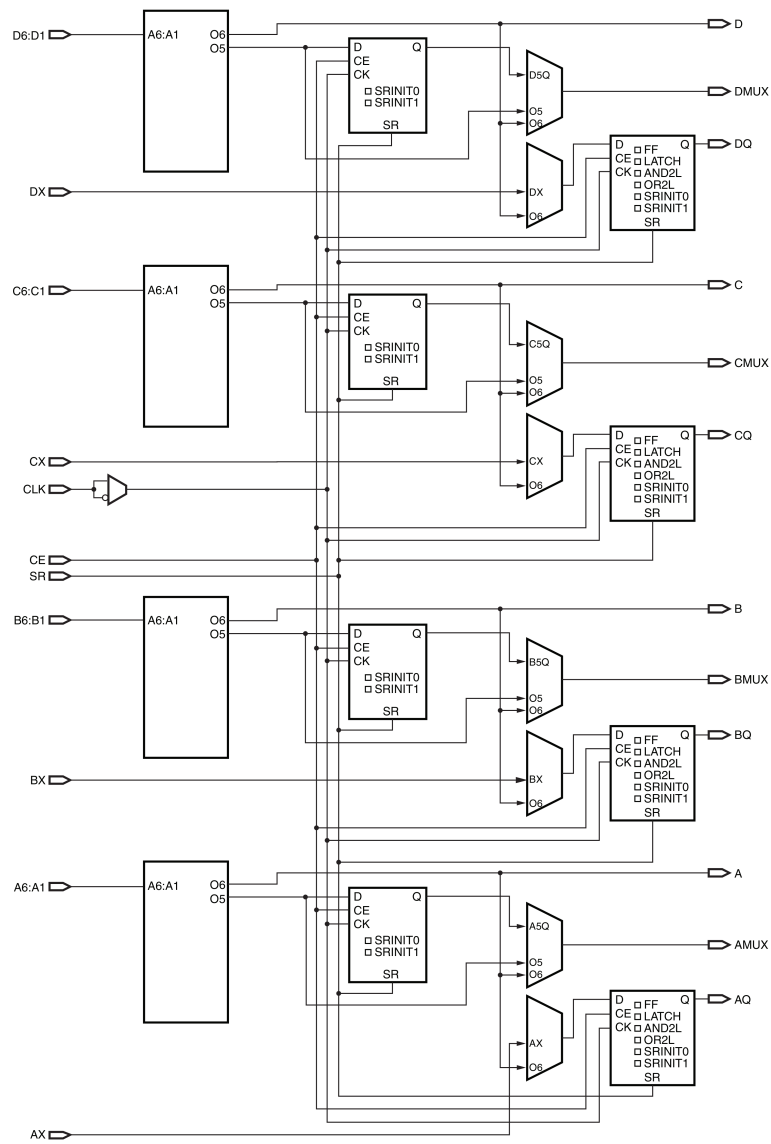


Figure 4.62. SLICEX in Xilinx Spartan-6 FPGAs [153].

```

attribute S of Q : signal is true;
attribute S of Q_not : signal is true;
attribute S of A_RTZ : signal is true;

```

```

begin

```

```

Q_not <= A_TEL(1) NAND Q;
Q <= A_TEL(0) NAND Q_not;

```

```

A_RTZ(0) <= NOT Q;
A_RTZ(1) <= NOT Q_int;

```

```

end architecture;

```

In this case, we have used the attribute *dont_touch* on the entity *TEL_2_RTZ* which has the same behavior of the *KEEP_HIERARCHY* in Xilinx ISE. In a similar fashion, we have designed the OR-gated NOR SR-latch used for both master and slave latches. In this case, we need of additional circuitry to implement the gating scheme, as discussed in Section 4.6.2, which is basically composed by a pair of clocked NOR followed by a pair of inverters:

...

Altera Cyclone IV attributes

```

attribute keep of D_gated : signal is true;
attribute keep of D_gated_not : signal is true;
attribute keep of Q_int : signal is true;

```

Xilinx Spartan6 attributes

```

attribute KEEP_HIERARCHY : string;
attribute KEEP_HIERARCHY of Behavioral : architecture is "YES";
attribute S: boolean;
attribute S of D_gated_not : signal is true;
attribute S of D_gated : signal is true;

```

```

begin

```

```

D_gated (1) <= D(1) NOR CK;
D_gated (0) <= D(0) NOR CK;

```

```

D_gated_not <= not D_gated;

```

```

Q_int(0) <= D_gated_not(1) nor Q_int(1);
Q_int(1) <= D_gated_not(0) nor Q_int(0);

```

```

Q <= Q_int;

```

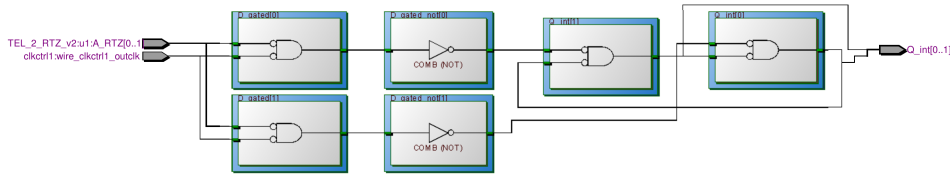


Figure 4.63. OR-gated NOR SR-latch post-synthesis and post-optimization in Altera Quartus II.

end architecture;

The last building block in the D³L sequential element is the *RTZ-to-TEL* converter, which provides the correct TEL signaling, imposing the nominal t_{eval} to the output signal. It does not require any special attribute, so the VHDL code is not reported here.

4.9.3 Generation of the Delayed Clock

In a TEL compatible logic, it is critical the length of the evaluation phase t_{eval} , since it implies the security level of the implementation, as we have discussed in this chapter. In Section 4.5.4, we have presented various possible solution to generate a secondary clock, with a certain time shift. In FPGA applications, the generation of a delayed clock, with the same frequency of the main clock, low jitter and high voltage/temperature stability, it is not a simple task. As we have discussed before, a general approach, that can be adopted in both ASIC and FPGA, can be the utilization of a *Phase-Locked Loop* (PLL), which is a commonly used strategy to derive multiple clocks with very stable performance. In FPGAs, PLLs are usually available as pre-implemented mixed signal primitives. Both Altera Cyclone-IV and the Xilinx Spartan-6 provide more than one PLL on-chip:

- ALTPLL primitive (Altera Quartus II 13.0);
- Clocking Manager IP-core (Xilinx ISE 14.1).

They can be configured to be fed with multiple input clock signals, and to generate up to 8 different clocks, with different frequency, duty cycle and phase. On both boards shown in Figure 4.58, on-board clock references have higher frequencies compared to our needs (50MHz for the Cyclone-IV and 60MHz for the Spartan-6). We have chosen a main clock of 2MHz on both FPGAs, and the PLLs have been set to provide an output clock signal with a frequency equal to 2MHz. The delayed clock *CKD* can be set with a phase shift between 0° and 180° respect to *CK*.

4.9.4 4-bit PRESENT Crypto-Core

To test the effectiveness of D³L style in counteracting PAAs on a real and physical platform, we have chosen to design the 4-bit PRESENT crypto-core as case study, adopting the same architecture designed for the simulations using the 40nm STMicroelectronics digital design kit (see Section 4.8). For both FPGAs, the synthesizer has been set to not flatten the cryptographic-processor hierarchy, in order to preserve the architecture presented in previous sections. The S-BOX has been synthesized with K-map synthesis, using only 2-inputs Boolean operands. We have chosen to synthesize bit per bit. This approach in synthesizing the S-BOX, allows to isolate logical cones. Each output bit has no sharing results with others, avoiding additive information leakage due to hazard phenomena. The post-synthesis and post-map results of the S-BOX for the two FPGAs are shown in Figure 4.64. It has to be noted that the critical path of the S-BOX is composed by four cascaded D³L gates, corresponding to a length of 8 in terms of CMOS gates.

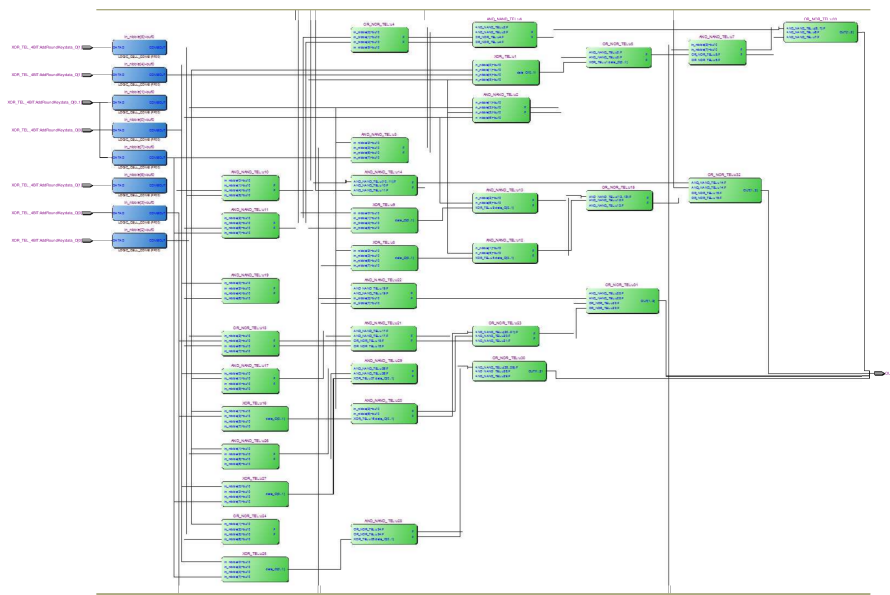
The *AddRoundKey* layer is reduced to a 4x4 bit XORing between the 4-bit input plaintext and the 4-bit key. In this case, only XOR/XNOR gates from the D³L library have been used.

The 4-bit PRESENT-based crypto-core, implementing the first round of the complete PRESENT-80 algorithm, has been designed as 2 stage, as shown in Figure 4.47. In this case, the XOR and the S-BOX are in the same pipeline stage, and since the input of the S-BOX has a huge fan-in, we have chosen to let the synthesizer to place buffers between the two building blocks. This way, we have ensured a proper driving stage to the output of the XOR/XNOR gates.

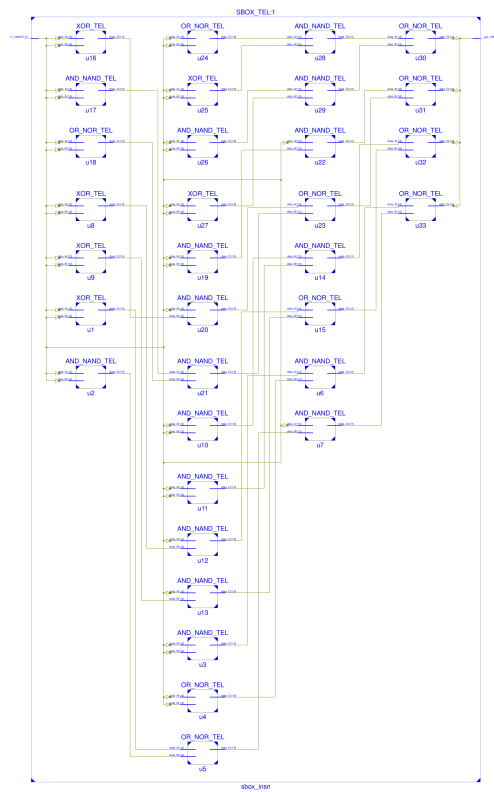
To allow the stimulation of the crypto-core, also glue logic has been designed in order to connect the device under attack to a computer. Since we need to provide both key and plaintext to the device under attack, we have designed a *UART interface*, which is able to provide the signaling of an asynchronous serial communication. The *UART interface* is fed by the main 2MHz clock signal, but internally, it reduces the frequency to adapt the speed to the specified baud rate, which has been set to 56.7kbaud. The communications settings are resumed in the following:

- 8-bit data;
- 1 stop bit;
- no parity check;
- 57.6kbaud.

The *UART interface* has been designed to accommodate different needs; therefore, it is possible to specify the number of bytes to be transmitted and received (independently) as a *generic* property on the VHDL code. In this case, we have set



(a)



(b)

Figure 4.64. RTL view of the implementation of the S-BOX after the synthesis and the map steps; (a) for the Altera Cyclone-IV and (b) for the Xilinx Spartan-6.

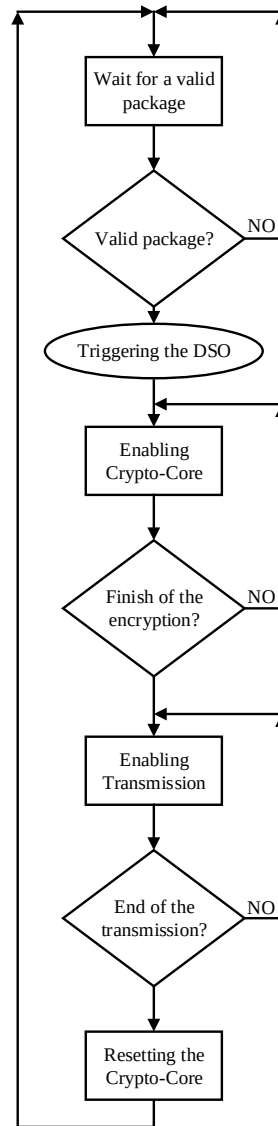


Figure 4.65. ASM diagram of the finite state machine that acts as controller for the 4-bit PRESENT crypto-core.

both to 1. For the scheduling and the control of the encryption and sending/receiving operations, a custom synchronous finite state machine has been designed. The scheduling of the operations to be handled can be resumed as follows:

1. waiting for the valid data package at the output of the *UART interface*.
2. enabling the crypto-core;
3. waiting for the end of the encryption operation;
4. enabling the *UART interface* to transmit data;

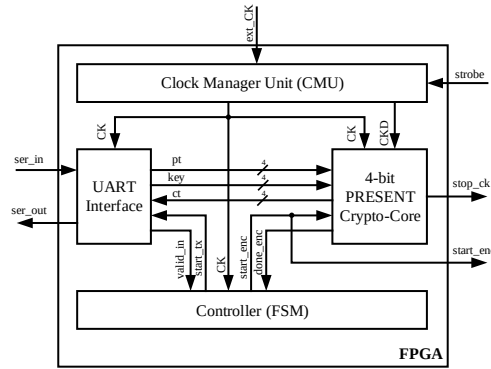


Figure 4.66. Block scheme of the testbed used for the implementation of the 4-bit PRESENT crypto-core on FPGA.

5. resetting the crypto-core, to prepare it for a new (and fresh) encryption.

In Figure 4.65, the scheduling of the operations performed by the controller unit is shown.

A block scheme of the FPGA implementation of the cryptographic processor is depicted in Figure 4.66. As we will discuss further, additional signaling has been added to synchronize measurement instruments to perform power analysis attacks (using both dynamic and static power consumption). *ser_in* and *ser_out* signals are connected to output pins of the target FPGA, and provide physical connections with a USB-FTDI daughter board, shown in Figure 4.67. The USB-FTDI daughter board allows to communicate with the PC through a UART interface using 3.3V signals through USB connection. In fact, the FTDI chip (e.g. FT-232RL [42]) is a USB to serial UART interface, and implements the USB's physical layer with the additional circuitry needed for the UART conversion. When a complete package of data has been received (specified in the number of bytes to receive in the *generic* declaration of the UART interface code), the UART interface asserts the *valid_in* signal, stating that valid data is available at its output port. At this point, the controller unit enables the 4-bit PRESENT crypto-core, asserting *start_enc*. At the end of the encryption, the crypto-core asserts *done_enc*, that forces the finite-state machine inside the controller to assert *start_tx* and starting the transmission of the 4-bit ciphertext *ct* through UART interface.

The *start_enc* signal assumes logical value '1' at the beginning of the encryption operation, and it is generated by the controller unit. *start_enc* is forwarded to an output pin of the target FPGA, providing a trigger signal for the DSO, in order to synchronize automated measurements on a common point in time. The *stop_clk* and *strobe* signals are used to perform AESP attacks, as we have already discussed in Section 3.8.3. In detail, when the *strobe* signal is high, it freezes both *CK* and *CKD* signals to their value, making the DC-picoammeter (see Chapter 3) to perform the measurement.

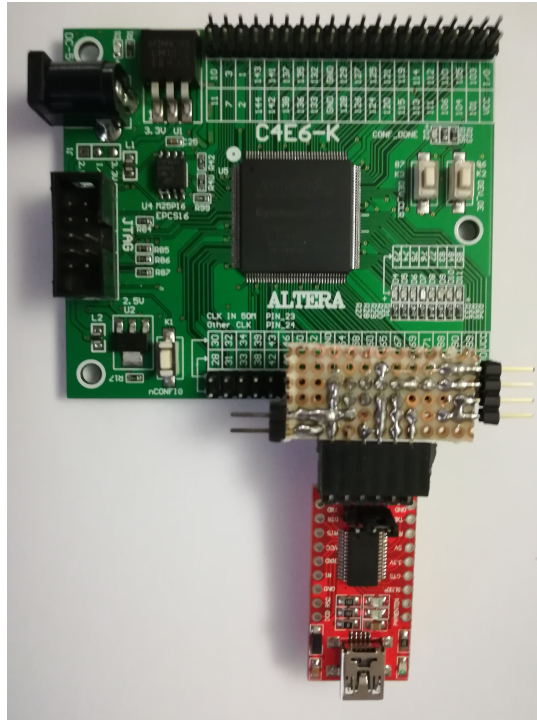


Figure 4.67. FTDI FT-232RL daughter board for USB-to-UART connection mounted on the Altera Cyclone-IV's evaluation board.

It is worth noting that the *Clock Manager Unit* (CMU) in Figure 4.66 refers to the PLL and timing circuitry described in Section 4.9.3.

Similarly to the AESP measurement setup described in Section 3.8, a Matlab script controls the scheduling of the operation and the DSO through TCP-IP connection. The oscilloscope used to acquire current traces is a LeCroy WaveSurfer MX-104B [88]; it has 1GHz of analog bandwidth and 10GS/s of sampling frequency. The current absorbed during the encoding operation is measured through the Tektronix CT-1 inductive current probe [140]. The probe is applied to the positive wire of the power supply of the part of the chip under attack, as shown in Figure 4.68. As previously mentioned, the acquisition system is automated by a custom Matlab script, performing the following tasks, in the same order in which they are mentioned below:

1. plaintext generation, which can be random or preset depending on the type of experiment to be carried out;
2. sending of the plaintext to the target FPGA;
3. traces acquisition from the oscilloscope through TCP-IP connection;
4. storing of the traces as a matrix in a *.mat* file.

After trace acquisition, data processing and PAAs are performed by means of

additional custom Matlab scripts.

In order to compare the security level of the 4-bit PRESENT crypto-core implemented using D³L with other logic styles, we have designed using the following logics:

- CMOS;
- WDDL;
- MDPL.

More in detail, we have used the same architecture of Figure 4.47 and Figure 4.66, adopting the same approach to implement the S-BOX function. Specific VHDL library has been designed for WDDL and MDPL styles. Since the MDPL needs the generation of a masking bit, we have designed also *Pseudo-Random Number Generator* (PRNG), based on a *LFSR* (Linear Feedback Shift Register). The long periodicity, compared to the length of the experiment, makes the bit stream generated by the LFSR to act as a random stream. The LFSR can be activated/deactivated by asserting/deasserting the *enable_PRNG* signal, which acts like a gating port for the clock that feeds the PRNG. The activation of the LFSR is demanded through the UART connection. In the MDPL implementation, the UART interface has been set to receive two bytes instead of one, making possible to remotely activate/deactivate the PRNG through the Matlab script. The *Chip Planner* view of Altera Cyclone-IV implementations are shown in Figure 4.70, Red boxes represent the *logic elements* used by the cryptographic circuit, while blue ones are referred to non-cryptographic circuitry. A resume of the resources usage with considered logic styles on the Altera Cyclone-IV FPGA is reported in Table 4.24.

Table 4.24. Resource usage for the Altera Cyclone-IV FPGA using Altera Quartus II 13.1.

Implementation	LUT only	Reg. only	LUT/Reg. Pair
CMOS	30	6	13
WDDL	154	0	30
MDPL*	784	34	62
D ³ L	486	0	6

It has to be noted that the MDPL requirements in terms of resources is the highest, and the synthesis becomes very large with MDPL implementation. It is worth noting that also in Figure 4.70, the MDPL implementation of the cryptographic processor is the largest one. The D³L implementation overhead lower than MDPL but larger than WDDL, since it requires more than double of logic gates. In addition, the D³L requires more logic element than WDDL also because registers have been designed according to the storage element described in Section 4.6, that do not use CMOS explicit flip-flops. Registers in D³L use only LUTs to store data, so it shows the smallest number of *LUT/Register pairs*, which is equal to 6. In fact, this value

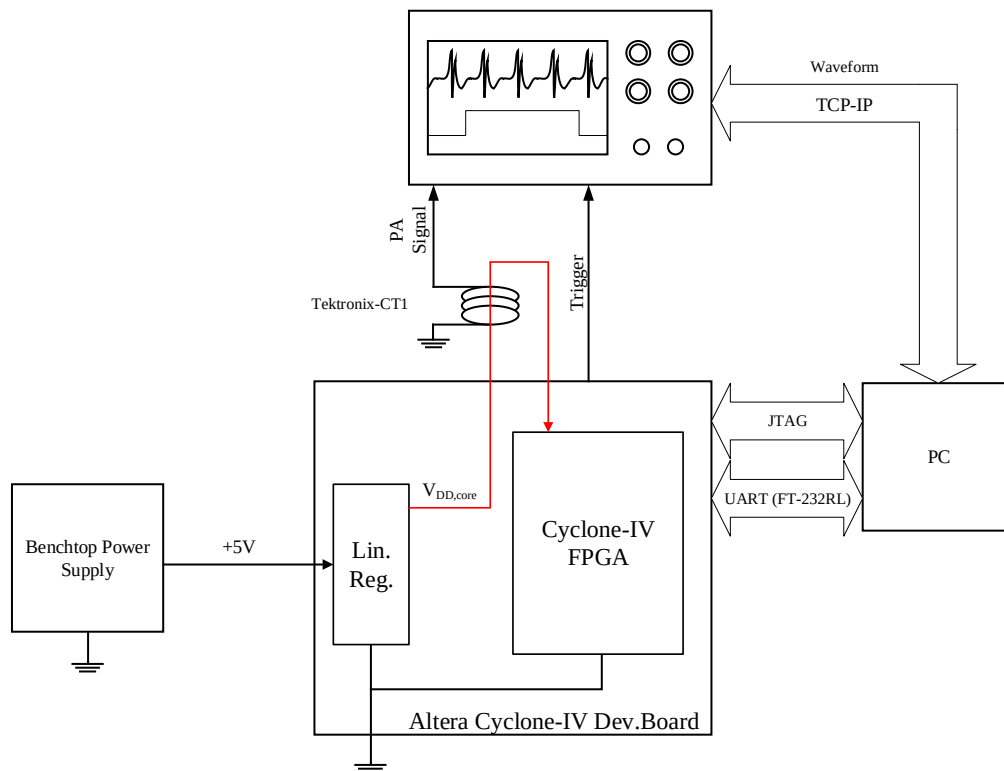


Figure 4.68. Block scheme of the dynamic power measurement setup.

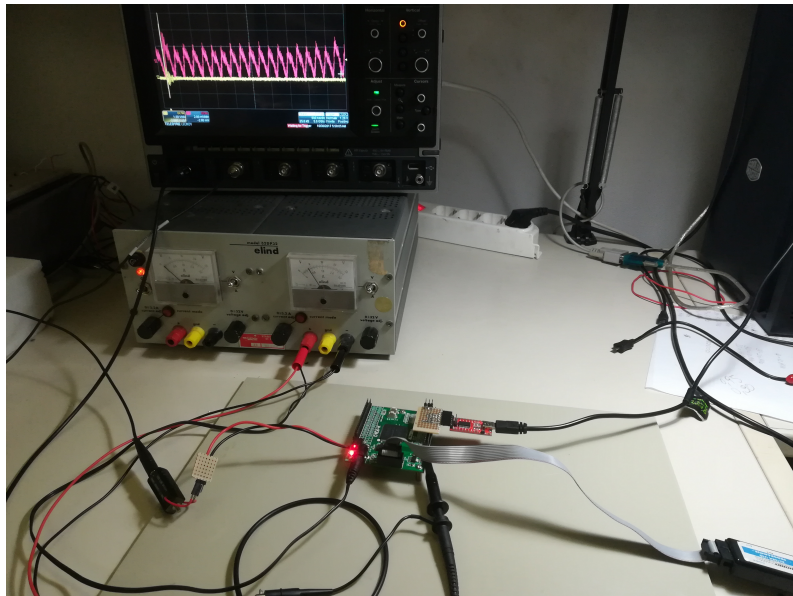


Figure 4.69. Dynamic power measurement setup.

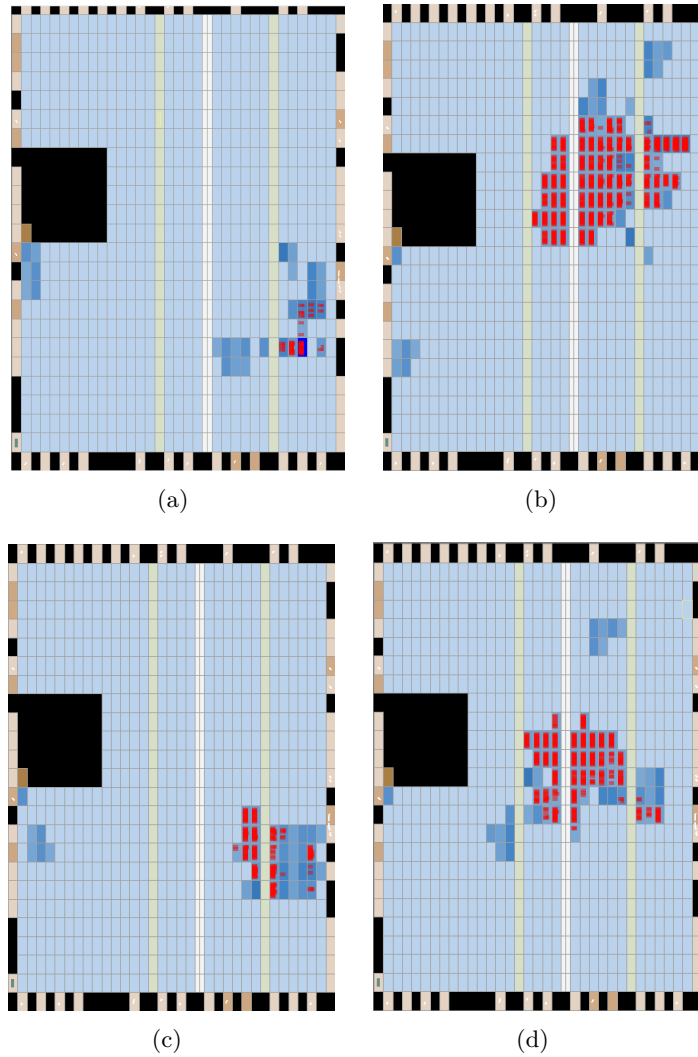


Figure 4.70. *Chip Planner* view of PRESENT crypto-cores' implementations on the Altera Cyclone-IV FPGA: CMOS (a), MDPL (b), WDDL (c) and D³L (d). Red boxes represent the *logic elements* used by the cryptographic circuit, while blue ones are referred to non-cryptographic circuitry.

refers to an internal counter of the crypto-core on a non-secured path plus additional registers for internal control.

The synthesis attributes and methodology presented in this section have been used to synthesize also to design WDDL and MDPL version of the cryptographic processor, in order to get *What You See Is What You Get* implementations. Our aim is to provide a simple way to design cryptographic processor, by means of a logic style which does not need of complex *place&route* constraints. As we have already discussed in this chapter, the presence of mismatch impact even more critically on FPGA platforms, because the granularity of the synthesis is very far from the approach used with ASICs. To provide a fair analysis, this comparison has been

carried out without changing settings on routing and placing engine.

4.9.5 Dynamic Power Analysis on FPGA Implementation of D³L PRESENT Crypto-Core

Experiments have been performed to analyze the information leaked through dynamic power consumption of the 4-bit PRESENT crypto-core in the implementation with D³L style. The same setup has been used for all experiments in this section, in order to get a fair comparison of the D³L with other DPL styles. Without loss of generality, we have used the Altera Cyclone-IV FPGA as device under attack, since the evaluation board we have used, as the minimum number of on-board components. It is worth noting that the power consumption has been measured after the linear regulator that feeds the FPGA's core. Inductor and filtering capacitors have been removed on this line, in order to get as much bandwidth as possible. The power supply voltage at the linear regulator's output is 1.2V, and since we have used the Tektronix-CT1 inductive probe, no voltage burden has been introduced. For each implementation, $2^{17} = 131072$ power traces have been collected, using a sampling period of 5GS/s, that corresponds to 200ps/sample. The clock frequency of each core has been set to 2MHz, whereas we have 2500 samples per cycle. t_{eval} has been set to 4.17ns, recorded in ~ 21 samples. The key has been set to $(6)_2$ in all experiments. The encryption takes three cycles. Current absorption in this time window are reported in Figure 4.72. NED and NSD values are reported in Table 4.25 and shown in Figure 4.71.

Table 4.25. NED and NSD values of dynamic power consumption of the 4-bit PRESENT crypto-core implementations.

Implementation	NED	NSD
CMOS	30.30%	10.32%
WDDL	21.95%	7.20%
MDPL-PRNGon	22.03%	6.85%
MDPL-PRNGoff	8.79%	2.66%
D ³ L	8.32%	2.87%

In Figure 4.72, *pre-charge* and *evaluation* phase are clearly distinguishable for WDDL and MDPL implementations. The dynamic power consumption tends to assume higher values during the *evaluation* phase, since all charging events occur at the rising edge of the clock (all DPL-RTZ cores have been designed according to the RTZ encoding scheme in Section 3.5). Regarding D³L's power trace, we can notice that it has almost a constant power consumption within three cycles. This simple power analysis is also supported by the NED and NSD analysis in Table 4.25. In fact, D³L implementation exhibits the lowest NED value among other implementations, remarking that the impact due to presence of mismatch (almost unavoidable on FPGA) is strongly reduced. The MDPL with PRNG enabled exhibits a very high NED and NSD values: it has been demonstrated that this logic style allows to

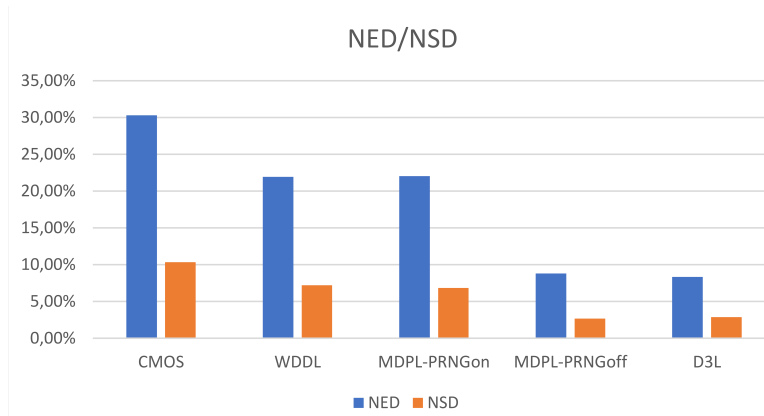


Figure 4.71. NED and NSD values of dynamic power consumption of the 4-bit PRESENT crypto-core implementations.

Table 4.26. Average power consumption of PRESENT-based cryptographic processors ($f_{CLK}=2MHz$ and $V_{DD,core}=1.2V$) on the Altera Cyclone-IV.

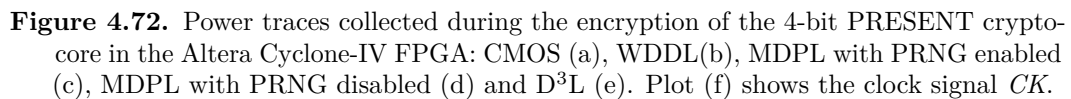
	CMOS	WDDL	MDPL-PRNGon	MDPL-PRNGoff	D ³ L
P _{AVG}	13.17mW	13.14mW	16.67mW	15.53mW	17.21mW

Table 4.27. Results of CPA attacks against various implementation of the 4-bit PRESENT crypto-core on Altera Cyclone-IV FPGA using dynamic power consumption.

Implementation	S-BOX			XOR		
	ρ_{corr}^{MAX}	SVI	MTD	ρ_{corr}^{MAX}	SVI	MTD
CMOS	0.0310	0.0290	> 32k	0.3194	+0.0298	750
WDDL	0.0379	+0.0008	54.5k	0.0379	-0.0200	> 132k
MDPL-PRNGon	0.0156	-0.0094	> 131k	0.1297	+0.0342	2.5k
MDPL-PRNGoff	0.0617	-0.0183	> 131k	0.0262	-0.0750	> 131k
D ³ L	0.0074	-0.0068	> 131k	0.0216	-0.0026	> 131k

relax the constraint on the unbalance in load capacitance, but it provides additional leakage due to early propagation effect [86] [139] [116]. An improved version of the MDPL (iMDPL) has been proposed in [82] that aims to solve this problem using an *evaluation-precharge detection unit* (EPDU) before majority gates to synchronize each input at the beginning of the evaluation phase (see also [109]).

CPA attacks results using the HW as power model are shown in Figure 4.73 and 4.74, using the output of the S-BOX and the output of the XOR respectively. It has to be noted that it is possible to attack only the WDDL implementation with 54.5k power traces using the output word of the S-BOX as target intermediate result. The WDDL implementation exhibits a correlation peak at the beginning of the third clock cycle, but the distance with the maximally ranked wrong key is very poor, providing a SVI of 0.0008. Attacks implying the output word of the XOR



provide better results, since the CMOS and the MDPL with PRNG enabled shows peaks of correlation coefficient related to the correct key when the XOR operation occurs (beginning of the second cycle). The CMOS implementation has an MTD value of ~ 750 power traces, while the MDPL with the PRNG enabled ~ 2500 . It is worth noting that the MDPL implementation has a different behavior with

the PRNG enabled or disabled. A possible explanation to the higher vulnerability enabling the PRNG is due to the fact of the early propagation effect, as mentioned previously in this section. The presence of not synchronized switching events implies higher unwanted data-dependency in the power consumption, as can be noted in Figure 4.73(c). Moreover, the MDPL implementation running with the PRNG enabled shows the maximum average power consumption, as it was expected. The D³L implementation has an MTD higher than the maximum number of power traces collected, and it was not possible to recover the secret key using CPA attacks with the target functions. A resume of the results of CPA attacks is reported in Table 4.27, and MTD diagrams are depicted in Figure 4.75-4.79.

The analysis of the information leakage has been performed also using the SNR [93] and the mutual information [91], presented in Chapter 2. In Figure 4.80, the SNR values as function of time are shown. It has to be mentioned that the encryption operation takes place only during the second clock cycle, and during the third one, the 4-bit ciphertext is forwarded to the output by means of the output register, according to Figure 4.47. For our purpose, it is sufficient to consider the SNR curves after sample no.2000. It should be noted that there is a strong relation between SNR curves in Figure 4.80 and CPA attacks' results in Figure 4.73-4.74. In fact, high values of SNR occur at the same time intervals of correct key's highest peaks of correlation coefficient in their respective implementations. In D³L implementation, the value of the SNR during the cryptographic operation is very small, and also if compared with the other implementations, it is significantly reduced. Low values of SNR remark that the data-dependent component of the overall power consumption is low compared to the noisy component's power.

Also the information theoretic approach using mutual information, reported in Figure 4.81, has remarked the same conclusion we had with the SNR analysis. During the processing of the secret key (from sample no.2000 to sample no.8000), the estimated mutual information curves are very similar in shape with their respective SNR ones, similarly to [54]. D³L implementation shows the minimum value of mutual information during the processing time window.

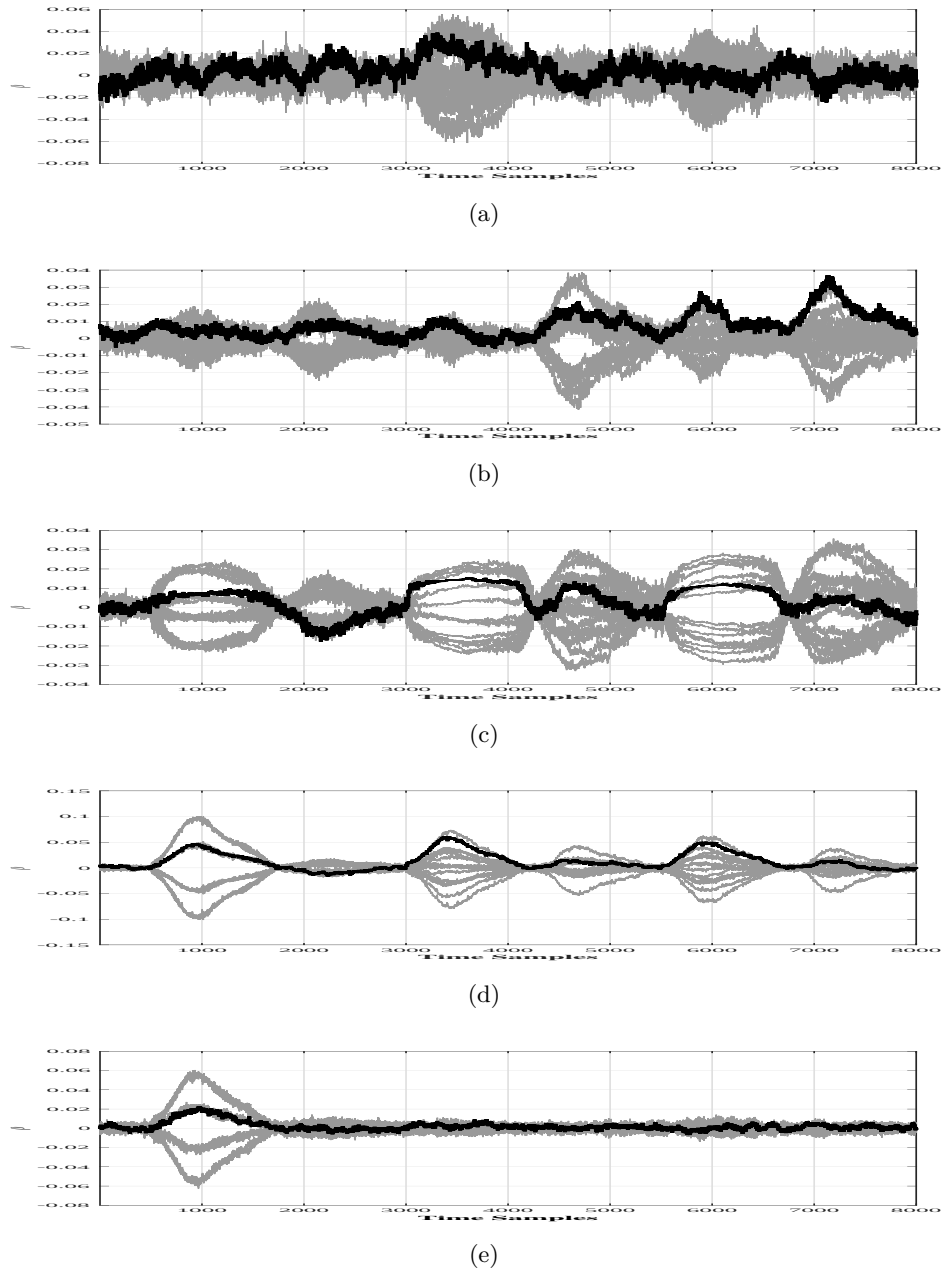


Figure 4.73. Plots of correlation coefficients for CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D³L (e) using the output word of the S-BOX and the HW as power model. Attacks have been performed using 2^{17} power traces. Black lines correspond to the correct key's correlation coefficients. Grey lines are referred to wrong keys' correlation coefficients.

A resume of SNR and mutual information performance of the implementations of the PRESENT-based cryptographic processor are reported in Table 4.28. The D³L implementation allows to reduce both SNR and mutual information peaks, thus, providing a better security performance when dynamic power exploitation.

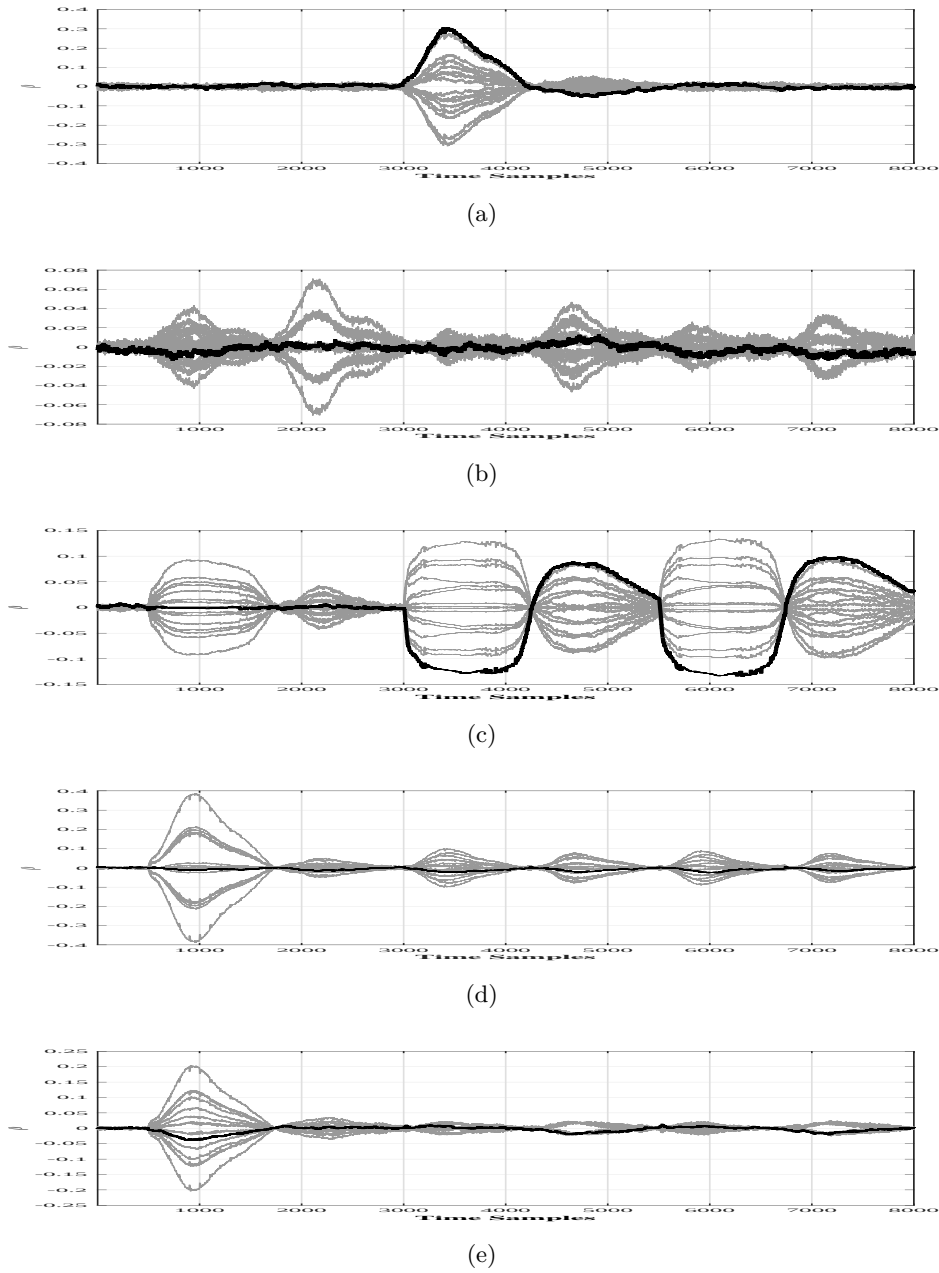
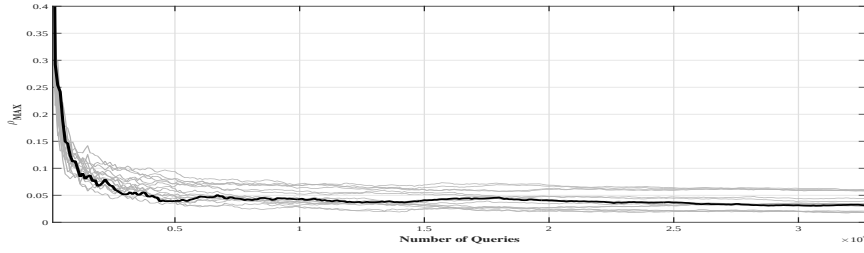
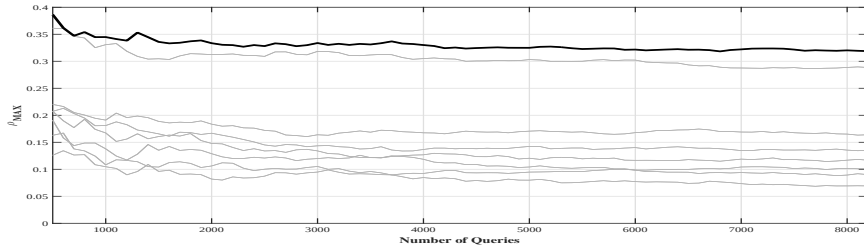


Figure 4.74. Plots of correlation coefficients for CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D³L (e) using the output word of the 4-bit XOR and the HW as power model. Attacks have been performed using 2^{17} power traces. Black lines correspond to the correct key's correlation coefficients. Grey lines are referred to wrong keys' correlation coefficients.

Compared to other state-of-the-art standard-cell based DPL styles, the D³L improves the SNR by a factor of 6, and the mutual information by a factor of 2. Comparing to MDPL, that is the only one that could not be broken using 131k power traces in our analysis (only with PRNG disabled), the D³L improves the most critical aspects

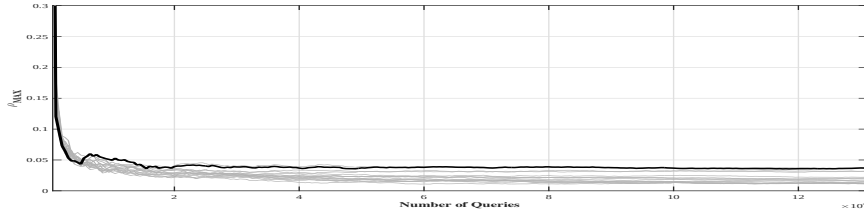


(a)

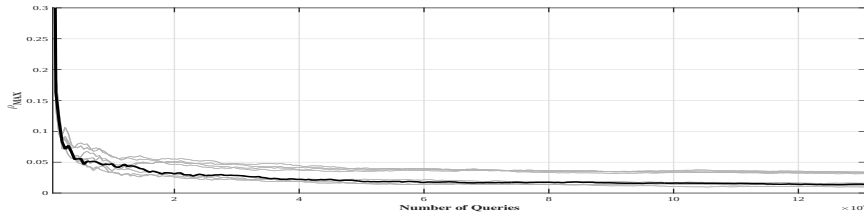


(b)

Figure 4.75. MTD diagrams on CMOS implementation: (a) using S-BOX and (b) using XOR.



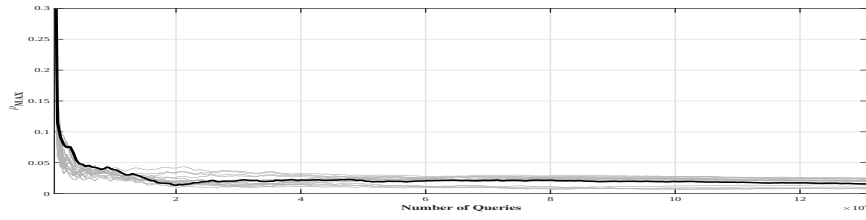
(a)



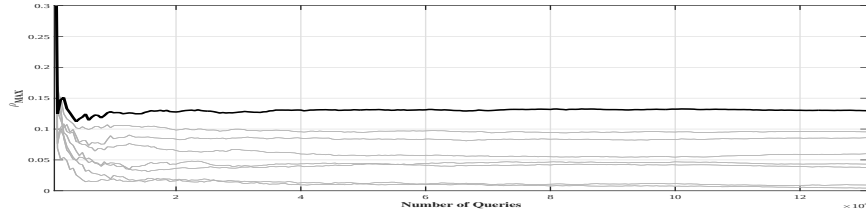
(b)

Figure 4.76. MTD diagrams on WDDL implementation: (a) using S-BOX and (b) using XOR.

in security applications: area and robustness to PAAs. The resource utilization is almost halved compared to MDPL, and the MTD is improved at least of three orders of magnitude compared to the CMOS reference. We want to remark that this comparison has been carried on synthesizing all cores **without balancing capacitive mismatches** through security-oriented *place&route* design steps. This

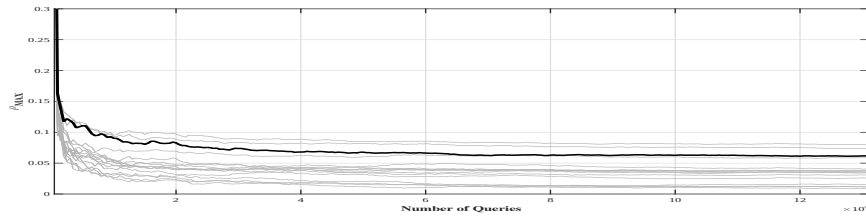


(a)

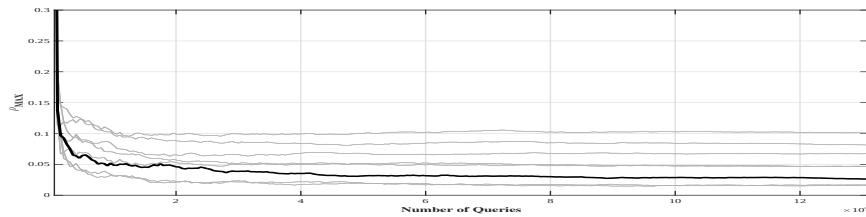


(b)

Figure 4.77. MTD diagrams on MDPL implementation with PRNG enabled: (a) using S-BOX and (b) using XOR.



(a)



(b)

Figure 4.78. MTD diagrams on MDPL implementation with PRNG disabled: (a) using S-BOX and (b) using XOR.

choice has been made to compare the security performance of D³L in a worst-case scenario, and providing a comparison with the state-of-the-art of FPGA-compatible DPL styles, synthesized in the same manner. The D³L style aims to provide an **easy-to-design** logic style without routing constraints, relaxing one of the most critical problem in security applications.

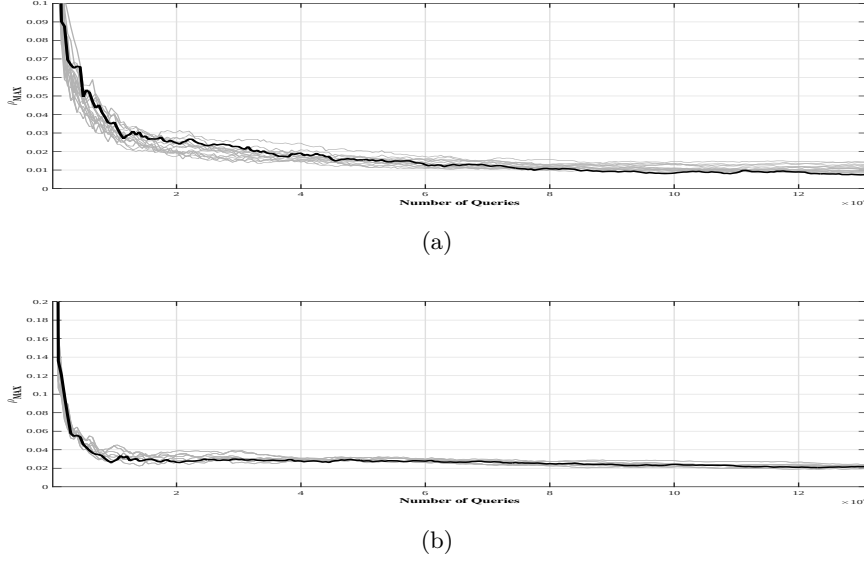


Figure 4.79. MTD diagrams on D³L implementation: (a) S-BOX and (b) using XOR.

Table 4.28. SNR and mutual information values on the PRESENT-based cryptographic processor within the processing time window (from sample no.2000 to sample no.8000).

Implementation	$\max(SNR)$	$\max(MI)$ [bit]
CMOS	169.90×10^{-3}	0.3950
WDDL	9.67×10^{-3}	0.0264
MDPL-PRNGon	23.24×10^{-3}	0.0418
MDPL-PRNGoff	20.48×10^{-3}	0.0465
D ³ L	1.73×10^{-3}	0.0136

4.9.6 AESP Attack on FPGA Implementation of D³L PRESENT Crypto-Core

In this evaluation, also the static power consumption has been taken into account to verify the security level of D³L. AESP attacks and information leakage through static power have been performed using the measurement setup in [16], presented also in Section 3.8. As previously mentioned, all PRESENT-based cores have been designed with synchronization signals for both dynamic and static exploitation, according to both measurement setups. In this section we will give a results of AESP attacks using the 4-bit output of the XOR and the S-BOX functions. All experiments have been performed at 65°C, since it is a reasonably higher working temperature to easily extract information leakage [48].

Since the encryption operation takes place in two clock cycles, we have collected power samples for each phases of the clock signal in the processing time window. Thus, we have four possible stopping moments:

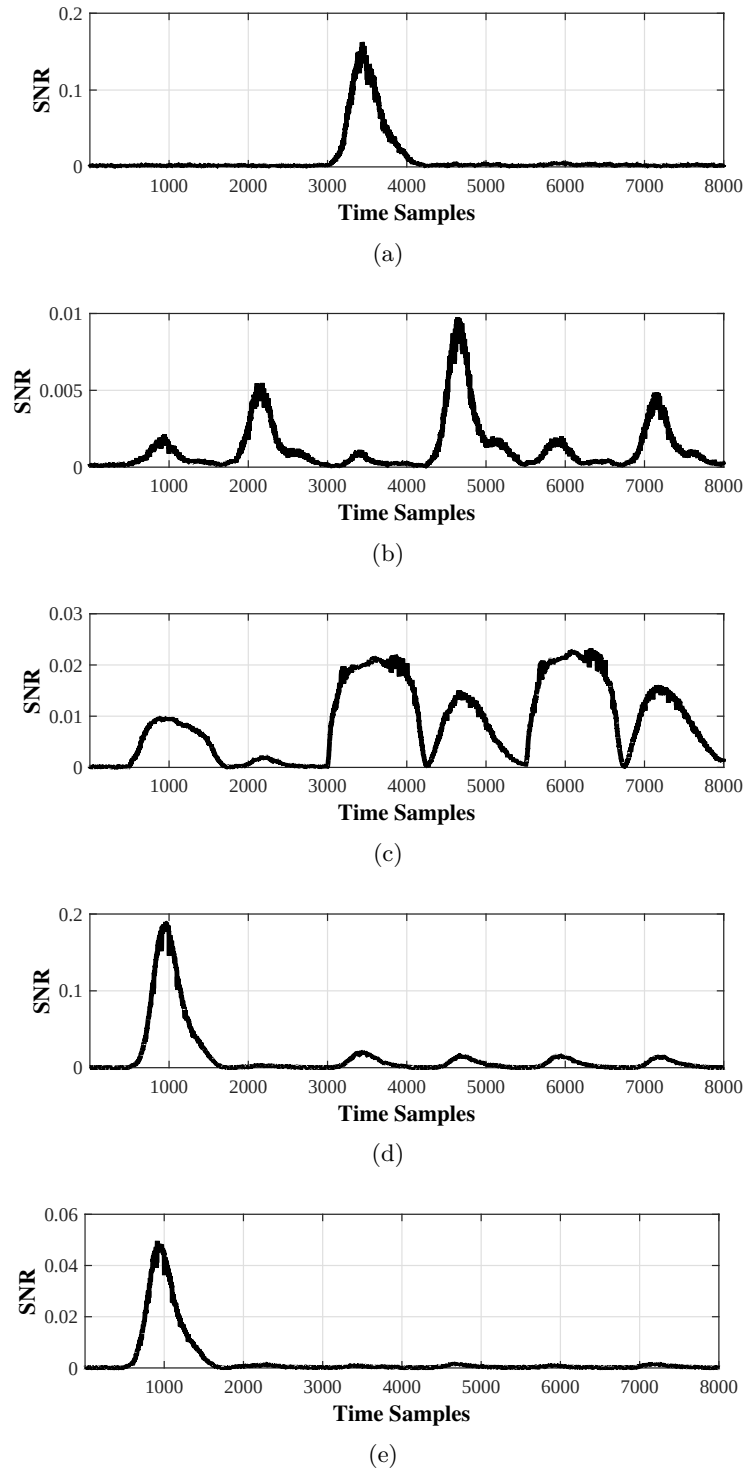


Figure 4.80. SNR curves as function of time: CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D³L (e).

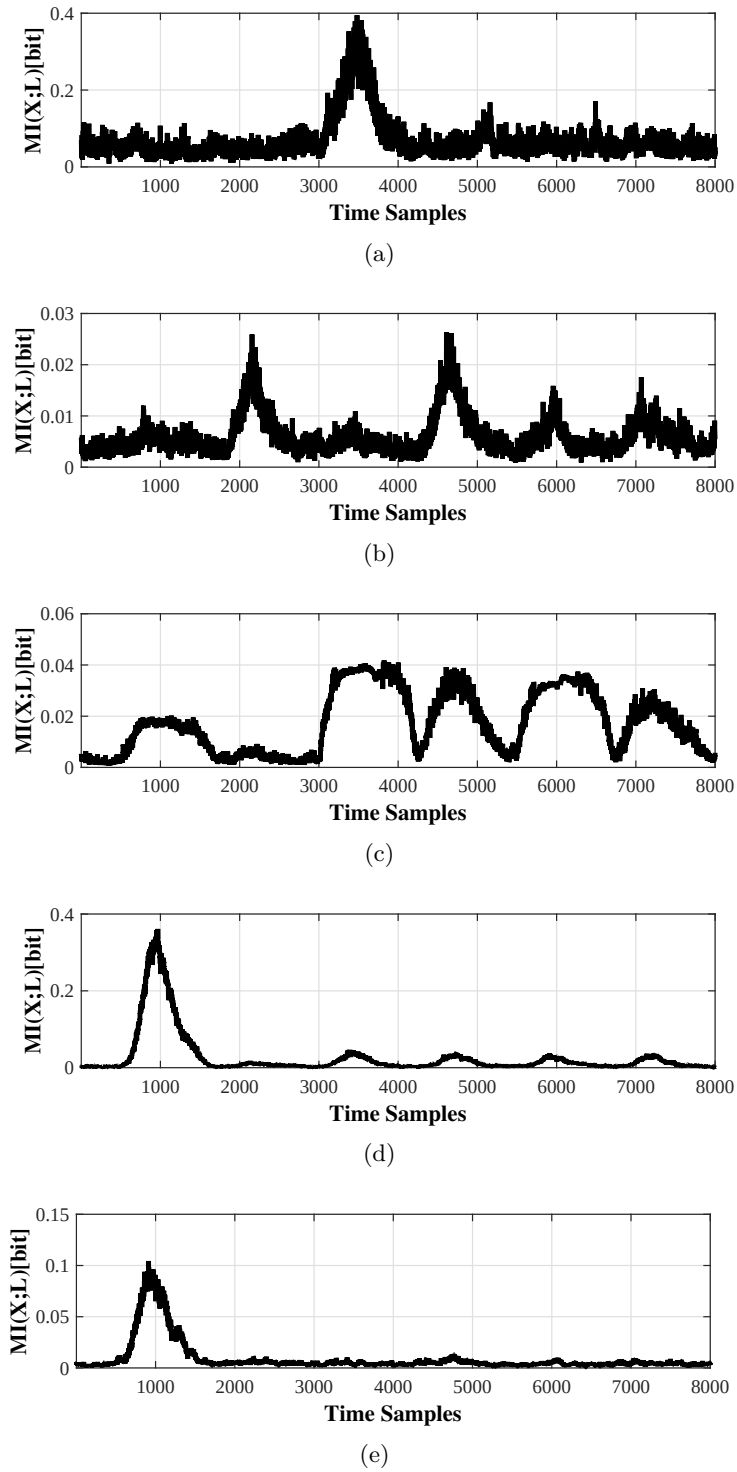


Figure 4.81. Mutual information curves as function of time: CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D³L (e).

Table 4.29. SNR, mutual information and σ_{data} of static power measurements collected during the 3rd clock cycle

Impl.	CK=0			CK=1		
	SNR[dB]	MI(X;L)[mbit]	$\sigma_{data}[nA]$	SNR [dB]	MI(X;L) [mbit]	$\sigma_{data}[nA]$
CMOS	-39.80	19.09	416	-36.29	28.54	537
WDDL	-48.21	7.27	259	-49.02	6.63	260
MDPL-PRNGon	-47.02	8.34	416	-51.53	4.97	302
MDPL-PRNGoff	-39.13	20.65	493	-36.04	29.39	568
D ³ L	-56.62	2.76	184	-55.39	3.18	199

1. 2nd cycle, $CK = 1$;
2. 2nd cycle, $CK = 0$;
3. 3rd cycle, $CK = 1$;
4. 3rd cycle, $CK = 0$.

After an initial stage, we have noticed that we could get better result using the 3rd cycle rather than the 2nd, and thus, we will present attacks performed on case 3 and 4. Adopting the AESP procedure, we have chosen the output of the 4-bit XOR as target function. 64k static samples for each core and for each case have been collected using the Keithley 6485 DC-picoammeter.

A preliminary analysis of the information leakage in the static consumption has been carried out using the SNR and the mutual information. It has been found that during the *evaluation phase*, the MDPL with PRNG disabled shows almost the same SNR and higher mutual information than the CMOS implementation. These results are in accordance with results presented in Chapter 3, for leakage assessment of standard-cell based DPL styles. In these experiments, we have found that the the D³L implementation shows the minimum values for SNR and mutual information compared to others. The SNR is reduced of 19dB compared to CMOS and also compared with MDPL and WDDL, the improvement is up to 10dB. The maximum value of the mutual information for the D³L is $3.18 \times 10^{-3} \text{bit}$ which is one order of magnitude smaller compared to CMOS and MDPL (with PRNG off). It has to be noted that these are first experimental results on the effectiveness of the TEL approach in thwarting also attacks exploiting static power, as suggested in [15]. In a TEL circuit, the very short duration of the *evaluation phase* allows to make reasonably unfeasible to separate the static power from dynamic power, since settling times of transient currents are usually longer than t_{eval} .

Results of AESP attacks as MTD diagrams for case 3 and 4 are shown in Figure 4.82-4.83 and summarized in Table 4.30. The correct key has been recovered only with CMOS and MDPL implementations. It has to be noted that the MDPL has been broken only with case 4 ($CK = 1$) and with PRNG enabled. During the evaluation phase, both storage elements and combinational cells have inputs set to their evaluation values. As a consequence, it will be easier for the adversary

Table 4.30. Results of AESP attacks on PRESENT-based crypto-cores ($T = 65$, 3rd cycle).

Impl.	CK=0				CK=1			
	ρ_{MAX}	SVI	SVI%	MTD	ρ_{MAX}	SVI	SVI%	MTD
CMOS	0.0836	+0.0180	+21.53%	2060	0.0960	+0.0286	+70.21%	411
WDDL	0.0119	-0.0274	-230.25%	> 64k	0.0337	-0.0051	-15.14%	> 64k
MDPL-PRNGon	0.0265	-0.0258	-97.36%	> 64k	0.0362	+0.0058	+83.98%	12.5k
MDPL-PRNGoff	0.0407	-0.0136	-33.41%	> 64k	0.0445	-0.0581	-130.56%	> 64k
D ³ L	0.0128	-0.0047	-36.71%	> 64k	0.0079	-0.0179	-213.92%	> 64k

to exploit information leaked through the static current, since there will be more data-dependent power consumption. Moreover, the presence of the PRNG is not enough

The D³L implementation cannot be broken with 64k measurements using the AESP procedure on both cases, reinforcing results in Table 4.29. To better analyze these result, we introduce the *normalized SVI%*, defined as follows:

$$SVI\% = \frac{SVI}{\max(\rho_{corr}, \rho_{wrong})} = \frac{\rho_{corr} - \rho_{wrong}}{\max(\rho_{corr}, \rho_{wrong})} \quad (4.51)$$

Using $SVI\%$, it is possible to better understand which is the improvement in the reduction of the value of the statistical distinguisher with a given countermeasure. Hence, the $SVI\%$ allows to make a fair comparison between different implementations and attack results.

When the adversary stops CK , and, consequently, CKD , all D³L combinational gates will assume the same internal and external states, neglecting the value of CK . As a result, D³L combinational gates provide theoretically zero mutual information through static power. The residual information that can be extracted in D³L's power consumption may be leaked only by storage elements in the architecture. Nevertheless, the exploitable information through static power in the D³L flip-flop is minimized by the symmetric architecture of the storage element. The presence of two symmetric and homogeneous branches for each sub-block in the flip-flop makes the information leakage through static power theoretically zero also for the flip-flop. In fact, for each possible TEL state of the input data, the number of transistor that are switched off/on is the same for each value of CK . As it can be seen in Table 4.30, $SVI\%$ is -213.92% in the best-case ($CK = 1$) and -36.71% in the worst-case ($CK = 0$) for the D³L, which outperforms the WDDL's worst-case. It is worth mentioning that the D³L implementation reaches the minimum correlation coefficient ($\rho_{corr} = 0.0079$) among all implementations.

4.10 Final Remarks on the Novel D³L Style

The Time-Enclosed Logic principle has been proposed to overcome the presence of additional information leakage in cryptographic hardware implementations due to unbalanced load capacitors at the output of differential gates. The classical Return-to-Zero protocol with dual rail pre-charge logic (DPL) approach has been found to be not sufficient to counteract Power Analysis Attacks (PAAs) due to non-idealities and electrical mismatches. In this chapter, the *Delay-based Dynamic Differential Logic* (DDDL or D³L) is proposed as novel logic style, capable to counteract PAAs also in the presence of capacitive mismatch at the output of differential gates. The new logic style aims to thwart PAAs at both protocol and gate-level, since it supports TEL-encoding with DPL approach. The D³L is based on a standard-cell design flow and it is suitable to be implemented on FPGAs without any routing constraint on the differential lines. A 4-bit PRESENT-based crypto-core has been designed using D³L for FPGA applications, and its security level has been compared with other gate-level countermeasures. Experiments in Section 4.9.5-4.9.6 have highlighted the ability of D³L logic style in thwarting power analysis attacks in a real implementation, using both dynamic and static power consumption. As a trade-off with regular implementation, the D³L requires higher area and power consumption, but the improvement in security level outperforms other DPL styles used to protect cryptographic circuit from PAAs also in the presence of mismatch.

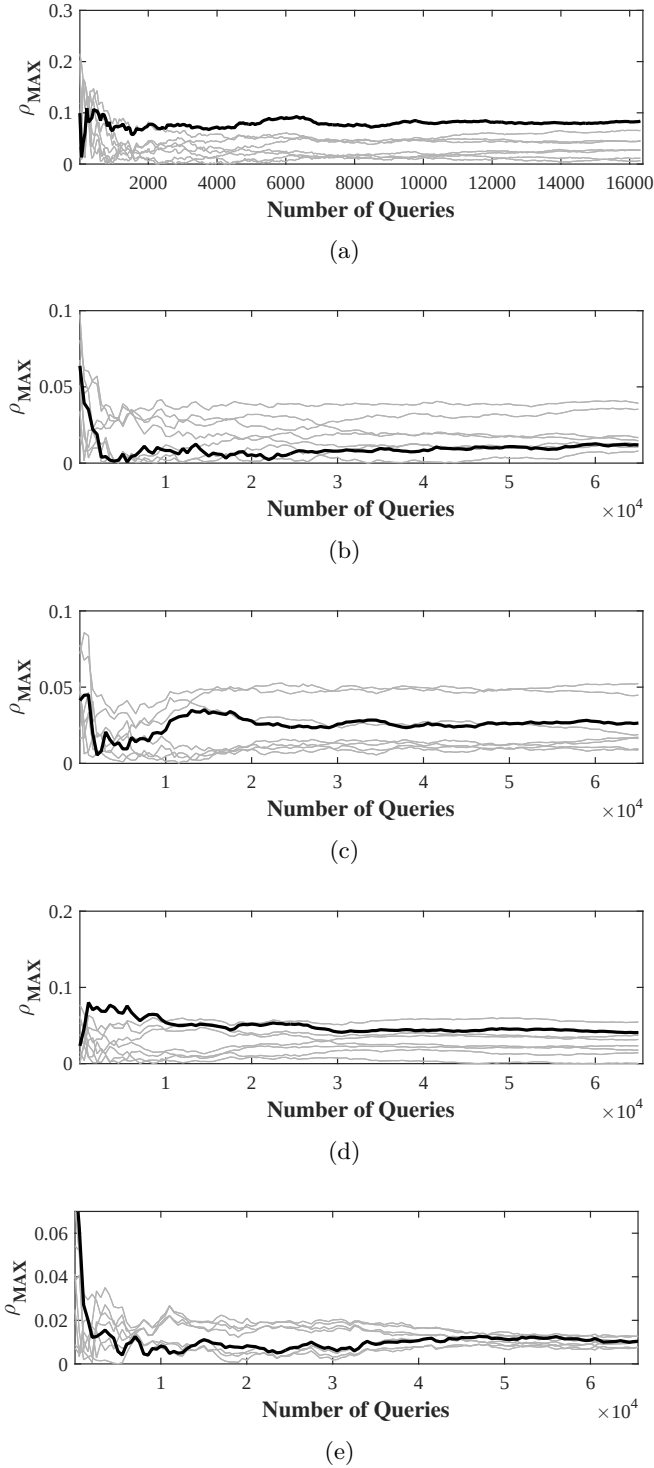


Figure 4.82. Correlation coefficient ρ_{MAX} as function of the number of measurements used to perform AESP attacks on 4-bit PRESENT crypto-cores, using the 3rd clock cycle with $CK = 0$: CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D³L (e). Black lines represent the correct key's correlation coefficient, while gray lines are referred to correlation coefficients of wrong keys.

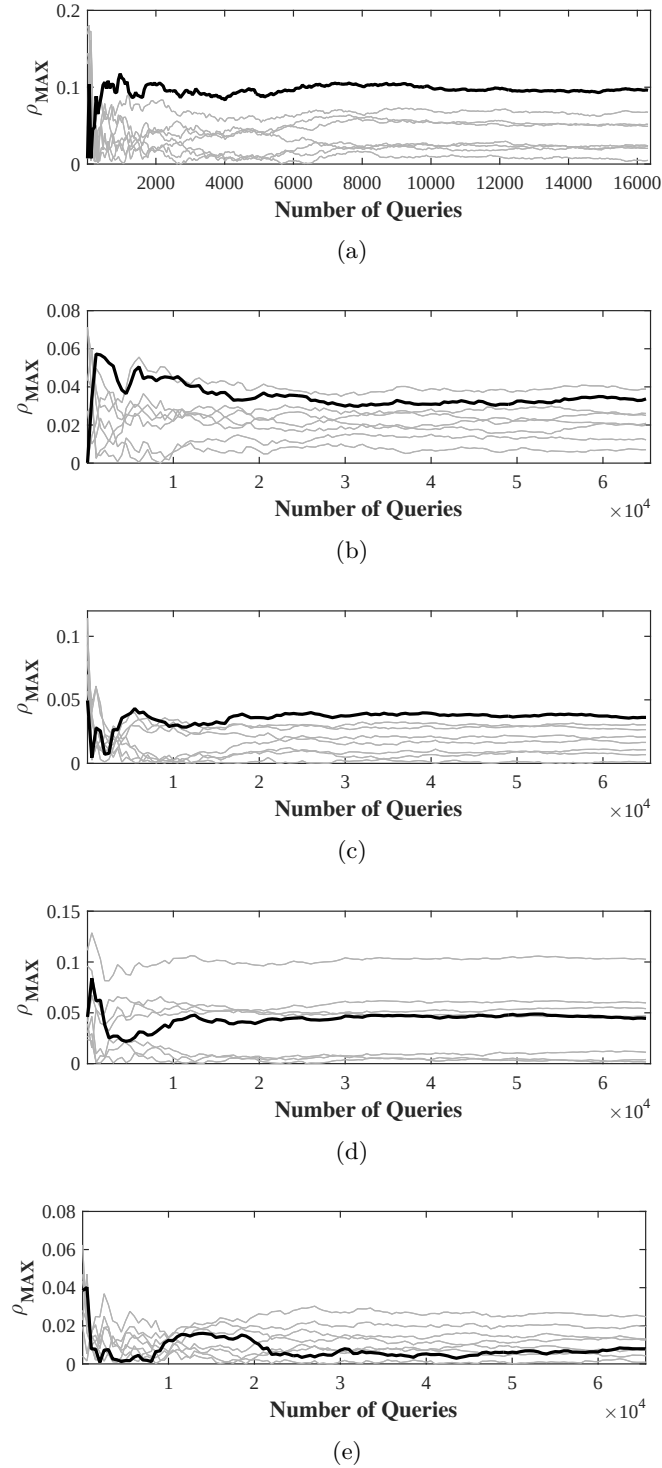


Figure 4.83. Correlation coefficient ρ_{MAX} as function of the number of measurements used to perform AESP attacks on 4-bit PRESENT crypto-cores, using the 3rd clock cycle with $CK = 1$: CMOS (a), WDDL (b), MDPL with PRNG enabled (c), MDPL with PRNG disabled (d) and D³L (e). Black lines represent the correct key's correlation coefficient, while gray lines are referred to correlation coefficients of wrong keys.

Chapter 5

Countermeasures based on Analog Current Equalizers

5.1 Introduction

As we have discussed in previous chapters, the protection of sensible data in a cryptographic hardware accelerator can be carried out transversely at each abstraction level of the implementation. The information leaked through the power consumption of a cryptographic device has been analyzed for twenty years. Since PAAs are basically non-invasive attacks, the adversary can measure only the off-chip power consumption, which may limit the information that he/she can recover. In Chapter 4, we have deeply analyzed a logic-level countermeasure, the D³L style, which can be considered a pure digital approach to power balancing and time enclosing of the information leaked through dynamic power consumption of a cryptographic implementation. The pure digital approach is the most used in the protection of the power signature of cryptographic accelerators, since it offers several advantages in the realization of the physical implementations, but, also non-digital approaches can be still effective.

System-level techniques have the purpose of preventing the exploitation of information leakage in the power consumption, and aim to de-correlate the consumption from the processed data. They require to adapt the regular implementation with additional logics, by changing the basic functions, and altering the order of execution of operations of the cryptographic algorithm. As we have discussed in previous chapters, at gate-level, there is the possibility to use other logic styles that are more resilient to power analysis compared to CMOS. These countermeasures aim to balance the power consumption per cycle, in order to provide a constant power consumption to an external observer. Many of them suffer of various problems related to non-idealities in the physical implementation of the hardware device. Issues like capacitive mismatches or early evaluation effects, cause the presence of unwanted leakage in the dynamic power consumption, that can be used to recover

sensible information, and they represent a weakness in protected implementations using such kind of countermeasures.

The less explored way to protect cryptographic implementation is the analog approach. We must consider that from the adversary point of view, the information leakage is contained in an analog signal, which is the actual current absorption of the cryptographic device. The idea behind the utilization of the analog approach to design a thwarting scheme is to provide an analog interface that is able to filter off the data-dependent component of the dynamic power consumption. Analog approach approaches can be used to develop countermeasures that are able to prevent information leakage through the observation of the dynamic power consumption of a cryptographic implementation. As well as many full custom DPLs, on-chip analog countermeasures cannot be directly implemented on FPGA platform, because of the presence of non-digital sub-blocks. In this chapter, we will introduce two on-chip analog countermeasures based on a current-mode approach to thwart power analysis attacks using the dynamic power consumption as source of information leakage.

5.2 State-of-the-Art of Analog Approach Countermeasures

The possibility to integrate analog circuitry in digital integrated circuits is often used to expand the set of features of modern electronic products, reducing production cost, and increasing performance and energy efficiency. Since it is a common approach to integrate analog blocks with digital circuitry on the same silicon die, it is possible to use analog processing to decouple the actual power consumption of a cryptographic device from the processed data. The analog approach approach can be considered as an hiding technique, since it will reduce the SNR by reducing the magnitude of the data-dependent power consumption.

In order to understand the application of analog processing on the signal that the adversary can measure to mount the attack, we must consider the block scheme in Figure 5.1. In fact, it is critical in which point of the circuit the adversary will place the SCA sensor, to collect the power traces. Let us assume that the adversary can place the SCA sensor before and after the off-chip filtering, which serves as low-pass filter for the power supply voltage fed to the chip. In the scenario depicted in Figure 5.1(a), the adversary places the SCA sensor before the off-chip filter. The collected current samples $i_{DD,off}$ will take into account the presence of the off-chip filter, which smooths the current peaks and limits the bandwidth available to the adversary. In this case, the data-dependent component of the measured power consumption can be reduced by the filtering effect provided by the off-chip filter, and the possibility to mount a successful attack may be reduced as well. In most cases, the off-chip filter can be removed or bypassed, since it is usually implemented using external capacitors and inductors, as depicted in Figure 5.1(b). In this scenario, the bandwidth available at the adversary can be strongly increased. Bypassing the off-chip filter, the adversary is able to capture the current absorption $i_{DD,on}$

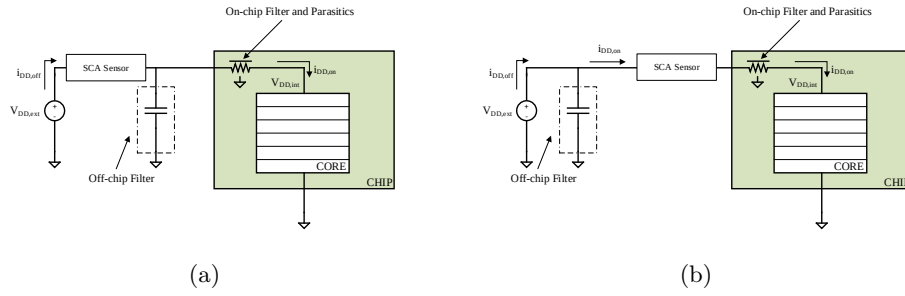


Figure 5.1. Realistic PAAs scenarios: (a) the SCA sensor is placed before the off-chip filter, (b) the SCA sensor is placed after off-chip filter.

that is absorbed by the chip. The current $i_{DD,on}$ is usually the measurable signal with the larger bandwidth that can or cannot have dependency with the processed data. The presence of an on-chip analog approach countermeasure that is able to decouple the $i_{DD,on}$ (and, in turns, $i_{DD,off}$) from the processed data will help the designer to protect the implementation also in the case that the off-chip filter is bypassed/removed.

In [150], authors have proposed an on-chip flattening circuit based on switched capacitor circuits. Thanks to the use of controlled decoupling stages, the cryptographic engine is not directly powered by the main V_{DD} pad. A precise sequence of charge-supply-discharge of the switching capacitor array is used to provide energy to the cryptographic core, in order to hide the real consumption to the malicious attacker. Based on a similar concept, Gornik *et al.* propose a three layers decoupling circuit, which provides energy to the target implementation [65]. It aims to flatten the power consumption, and uses CMOS switches and CMOS capacitors. Each gate of the cryptographic device is protected by the proposed decoupling cell, providing distributed filtering capability. Also in [97], a switching NMOS capacitor array is used to thwart PAAs on a cryptographic implementation. In this case, the charge/discharge of capacitor arrays is controlled by a specific unit (e.g. the charge control unit), that connects a subset of NMOS capacitors with a random pattern.

In [122], a different approach has been adopted. Using a *feedback loop* architecture, a dynamic current correction scheme suppresses differences in dynamic power consumption related to different processed data. Instantaneous current drawn by the cryptographic engine is sensed using a voltage-mode approach, and then, the proper additional current is shunted from the main power supply, in order to maintain the total current constant. Hence, the observable power consumption is approximately flat and unrelated to processed data. In [102], Mesquita *et al.*, propose a *Current Mask Generator* (CGM) circuit, which is used to provide the maximum value of power consumption of the cryptographic circuit at each clock cycle. The cryptographic circuit is powered by the CGM, which also measures its current absorption. The current draw is converted into a voltage signal and compared with a properly designed reference. Additional current is drawn to nullify the voltage error signal. In [111], an on-chip current flattening circuit is proposed to

protect the power consumption of a smart card accelerator from CPA/DPA attacks. The circuit makes use of a static current reference to compensate variations in current consumption due to data-dependency. The actual current drawn by the microcontroller is compared with the static reference; the difference is then used to drive a transconductance amplifier that will shunt an extra current to minimize the error signal.

Iokibe *et al.* propose an off-chip solution in [73], aiming to improve the tolerance to PAA of FPGA cryptographic implementations. An external decoupling circuit has been designed, in order to implement an off-chip filter on the power supply line. Anyway, this kind of protection can be easily bypassed or removed, as illustrated in Figure 5.1(b). In a real scenario, the off-chip filter is usually removed to mount the attack, and the presence of this such countermeasure will not really improve the security of the system, as it can be easily circumvented.

5.3 OCE: On-chip current equalizer

In literature, several voltage-mode analog countermeasures have been proposed [122], [111], [97]. The *The On-chip Current Equalizer* (OCE) is the first pure current-mode approach to design an analog countermeasure to thwart power analysis, and it has been proposed during the Ph.D. work in [20]. The current mode approach is widely used in many electronic applications, such as AD/DA converters, analog filters, etc., due to its compactness and speed.

The idea behind our approach is to set the same current drawn at each clock edge, in order to reduce the variability due to different input patterns. As we have said before, during the active edge of the clock, standard CMOS gates in a data-path perform output transitions and a certain current is drawn from the supply line. During the active clock edge, the current equalizer senses the current drawn by the logic and compares it with a reference current. If for the specific input pattern the current drawn is less than the reference current, current equalizer circuits shunts an extra current from the supply line, in order to hide to the attacker the real consumption of the logic circuit below. At each clock cycle, the same current is drawn and the power consumption is ideally constant. A block scheme that is able to implement our approach is shown in Figure 5.2.

A linearized and simplified model of the current equalizer is shown in Figure 5.3. We can express the relationship between I_{TOT} (total current) and I_{REF} (reference current) as function of I_{LOGIC} (current drawn by the logic):

$$I_{TOT} = I_{REF} \frac{R_0 G_M}{1 + R_0 G_M} + I_{LOGIC} \frac{1}{1 + R_0 G_M} \quad (5.1)$$

$$I_{TOT} = I_{SINK} + I_{LOGIC} \frac{1}{1 + R_0 G_M} \quad (5.2)$$

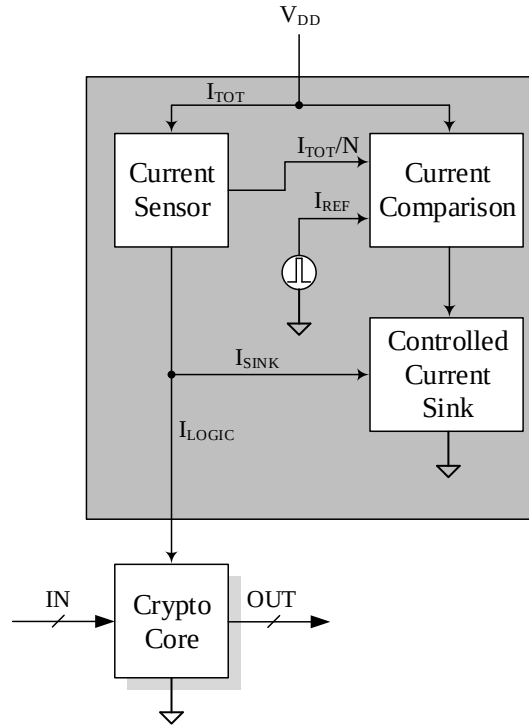


Figure 5.2. Block scheme of the OCE.

If the loop gain $R_0 G_M \gg 1$, the output of the current equalizer is expressed by:

$$I_{TOT}(t) = I_{SINK}(t) + I_{LOGIC}(t) = I_{REF} = \text{const} \quad (5.3)$$

where I_{LOGIC} is the data-dependent component and provides energy to the logic, and I_{SINK} is the current that is drawn by the equalizer to reach I_{REF} , which is constant. As we can see in Figure 5.2-5.3, the current equalizer is a feedback loop system. The input of the feedback loop is the current I_{REF} and the output is I_{TOT} , while I_{SINK} is the correction. The Current Comparison block compares I_{TOT} with the reference current I_{REF} , and produces a voltage signal, driving the Controlled Current Sink, which acts as a transconductance G_M and equalize the total current drawn by the system. The current I_{LOGIC} can be considered as a disturbance for I_{TOT} , and it has to be rejected. Since the reference current I_{REF} is constant, the I_{SINK} current has to dynamically correct the variability of I_{LOGIC} due to data-dependency.

In Figure 5.4, a circuit implementation of the current equalizer is shown. M_{1-7} senses the current I_{TOT} , and implements a current mirror with M_2 . M_{3-4} allows to invert the sign of the current and scales down its magnitude, in order to reduce the power consumption overhead. The reduction ratio of the sensed current can be set by properly designing the aspect ratio of the current mirror M_{3-4} . Transistor M_5 is the reference generator, which has to be sized and designed to provide the proper

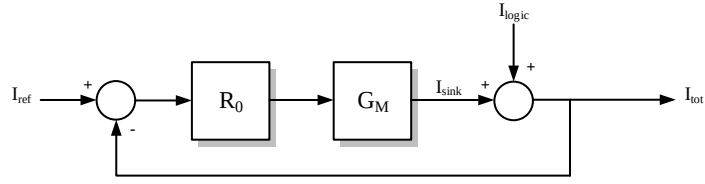


Figure 5.3. Simplified and linearized model of the current equalizer.

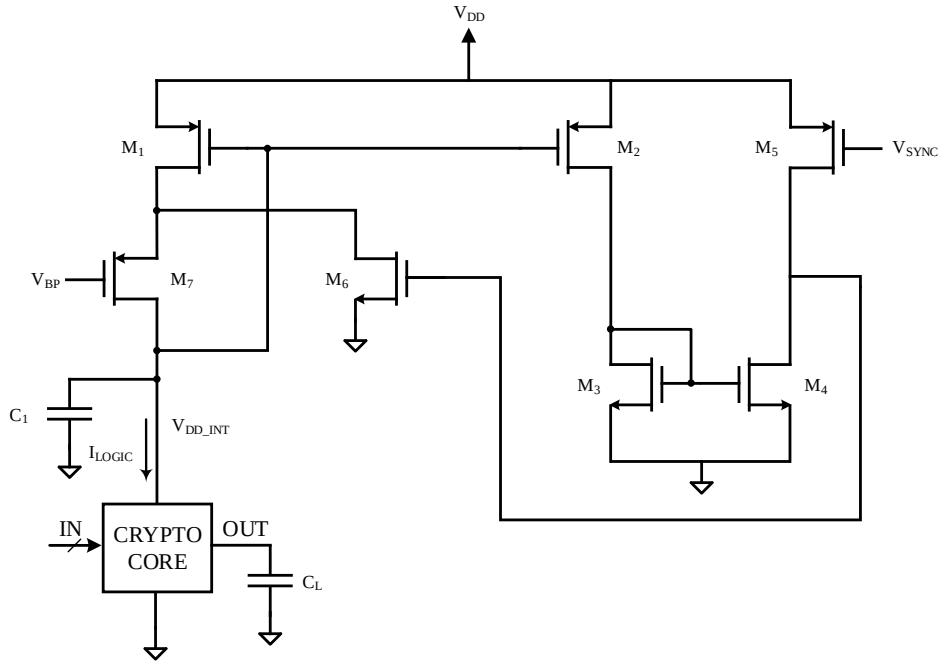


Figure 5.4. Circuit implementation of the proposed current equalizer.

reference current I_{REF} . The control voltage V_{sync} activates M_5 during the edge of the clock. During this short interval, M_5 is in saturation region and I_{REF} is drawn from V_{DD} . At the drain node of M_5 , the difference between the drain current of M_5 and M_4 produces a voltage swing on the total equivalent resistance R_0 at the node. This voltage swing drives M_6 , to shunt the I_{SINK} required to nullify the error current of the loop.

In order to provide enough power supply to the logic, it is necessary to use a cascode configuration of the input of the current mirror $M_{1,2,7}$. Thanks to the presence of M_7 , a low voltage drop is reached between V_{DD} and V_{DD_int} , due to the low impedance provided by the cascode current mirror.

V_{sync} signal, which is used to activate the reference generator M_5 , has to be generated from the clock signal. To reduce power consumption overhead, the

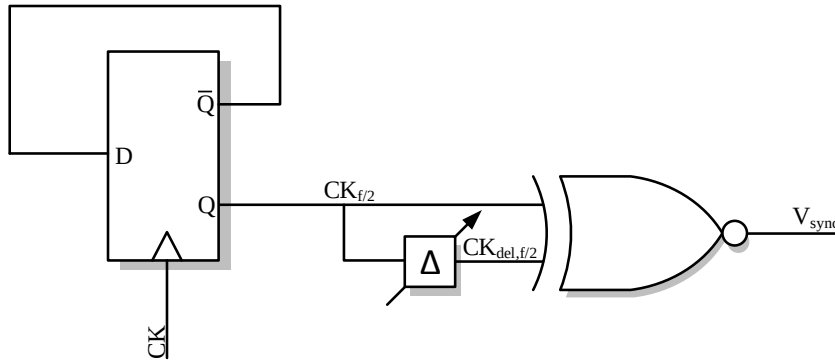


Figure 5.5. Circuit implementation of the V_{sync} signal. The delay element is implemented with a starved inverter.

correction on the current drawn by the logic is performed only around the active edge of the clock. In Figure 5.5, V_{sync} signal generator circuit is shown. A D flip-flop is used to get a clock signal at half of the frequency of the global clock. The delay element is obtained with a starved inverter [105]. As discussed in Chapter 4, the delay can be achieved also with other methods (e.g. PLL, DLL, etc), but we have chosen a compact and energy saving solution. The delay Δ can be set with the control voltage of a starved inverter, and allows to designers to choose the width of the pulse of V_{sync} . The value of Δ has to be chosen larger than the evaluation time t_{cp} required by the critical path to generate correct results, in order to guarantee that the power consumption is dynamically equalized during the switching:

$$t_{cp} < \Delta \quad (5.4)$$

Using V_{sync} instead of a constant reference allows to prevent a static power dissipation when the logic net is not switching. A timing diagram of the V_{sync} signal is depicted in Figure 5.6.

The capacitor C_I is used to help the stability of the loop, and it can be implemented using MOS capacitors or *decap cells*, since it is connected directly on the power rail of the digital core.

5.3.1 Performance on Single Logic Gates

To demonstrate the effectiveness of the proposed current-mode approach to thwart CPA attacks, basic combinational gates have been studied, and the power variability due to data-dependency has been analyzed using the on-chip current equalizer shown in Figure 5.4.

STMicroelectronics CMOS 40nm design library has been used to design both,

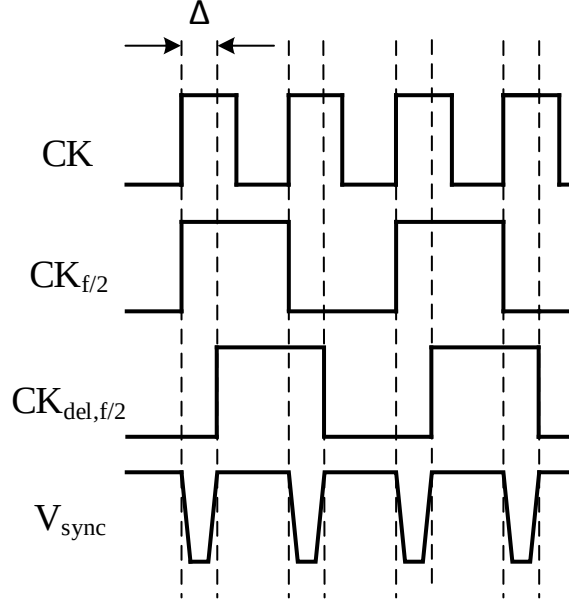


Figure 5.6. Timing diagram of the V_{sync} signal.

Table 5.1. Comparison of unprotected CMOS and protected CMOS using the OCE, in terms of NED and NSD for basic logic gates.

	Unprot. CMOS		Prot. CMOS	
	NED	NSD	NED	NSD
	[%]	[%]	[%]	[%]
NAND	0.81	0.55	0.09	0.04
NOR	0.80	0.58	0.07	0.03
NOT	0.81	0.80	0.05	0.03

the OCE and digital logic cells. The power supply voltage for CMOS gates has been fixed at 1V. V_{DD} for the current equalizer is fixed at 1.2V, in order to guarantee a $V_{DD_int} \approx 1V$ for protected gates. The clock frequency has been set to 20MHz. In Table 5.1, a comparison between standard CMOS gates and OCE-protected CMOS gates is reported.

Both NED and NSD of protected gates are 10-20 times smaller respect to unprotected implementations. It implies that the ability of the attacker to discriminate the peak value of the current consumption is reduced. The possibility of a successful DPA/CPA is strongly dependent on NSD of basic gates, and since they are reduced, the possibility to mount a successful attack is limited.

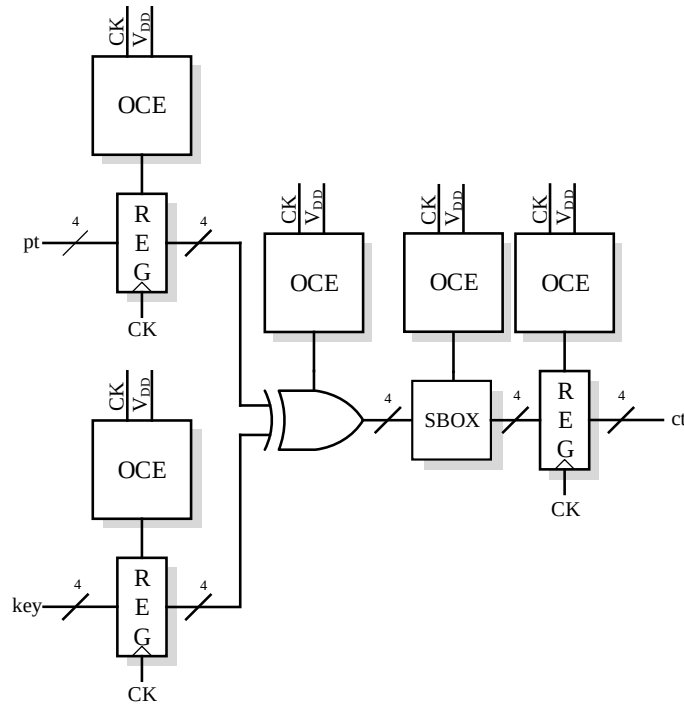
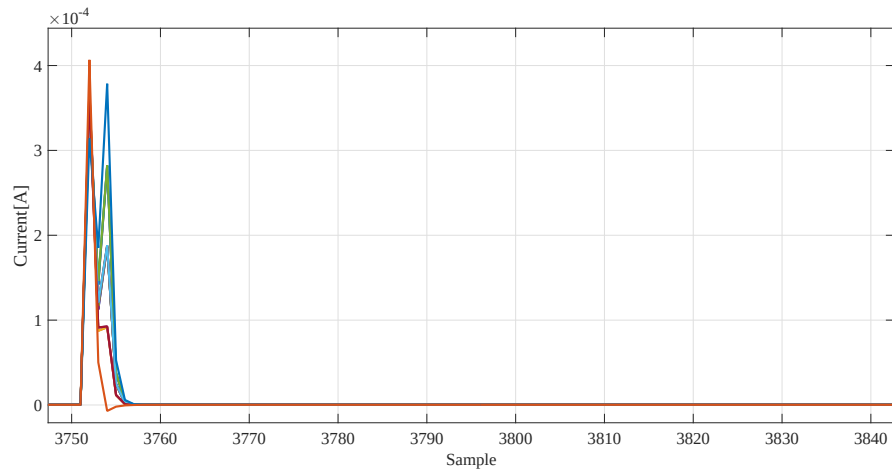


Figure 5.7. Protected implementation of the 4-bit PRESENT crypto-core. Each sub-block is protected locally by an on-chip current equalizer.

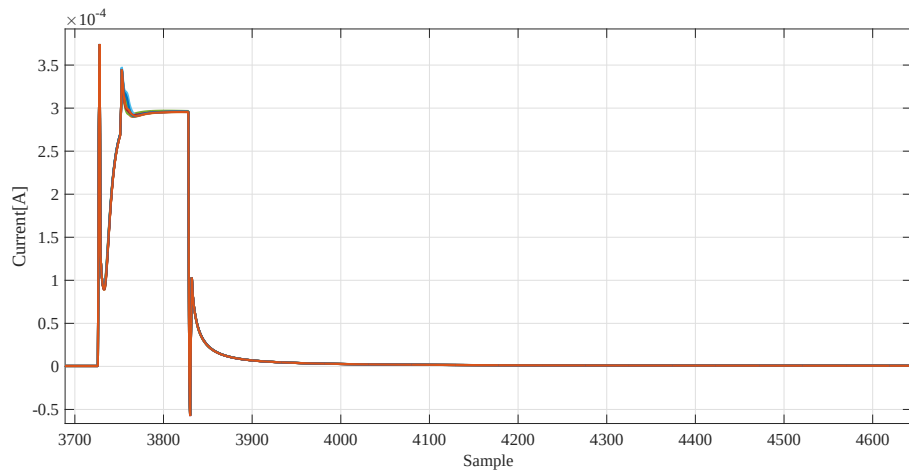
5.3.2 Case Study: Application of OCE on the 4-bit PRESENT Crypto-core

To test the effectiveness of the on-chip current equalizer, the proposed countermeasure has been implemented as analog approach protection to the 4-bit PRESENT crypto-core of Figure 3.18. The protected core has the same architecture of the unprotected one. Each sub-block of the 4-bit PRESENT crypto-core has its own current equalizer, to provide local protection and filtering at power supply node, as depicted in Figure 5.7. This choice allows to reduce the needs of large capacitor for C_I and let more degrees of freedom to the designer to customize current equalizers. The comparison is performed on unprotected and protected implementation of the case study. The measurements are collected on Cadence Virtuoso and the attack routine is executed on Matlab. For the sake of generality, Gaussian distributed noise has been added to simulation results, to simulate a real attack scenario [125]. A SNR of 6dB has been chosen as reference for measurements, and a maximum of 100k traces has been used as maximum storage capability. The key has been set to $(5)_2$, and Δ has been set to 500ps. A maximum of a 100k power traces has been chosen as maximum storage capability, as in a real attack scenario. The output of the S-BOX has been chosen as target intermediate value.

In Figure 5.8, the power traces of the unprotected and OCE-protected imple-



(a)



(b)

Figure 5.8. Power traces of unprotected (a) and protected (b) implementation of the 4-bit PRESENT crypto-core using the on-chip current equalizer with different plaintexts.

mentations are shown for different plaintexts. It is clear that the unprotected CMOS implementation exhibits a stronger variability in the power consumption, compared to the protected one. The on-chip current equalizer is able to suppress those differences, making the power signature almost independent from the processed data.

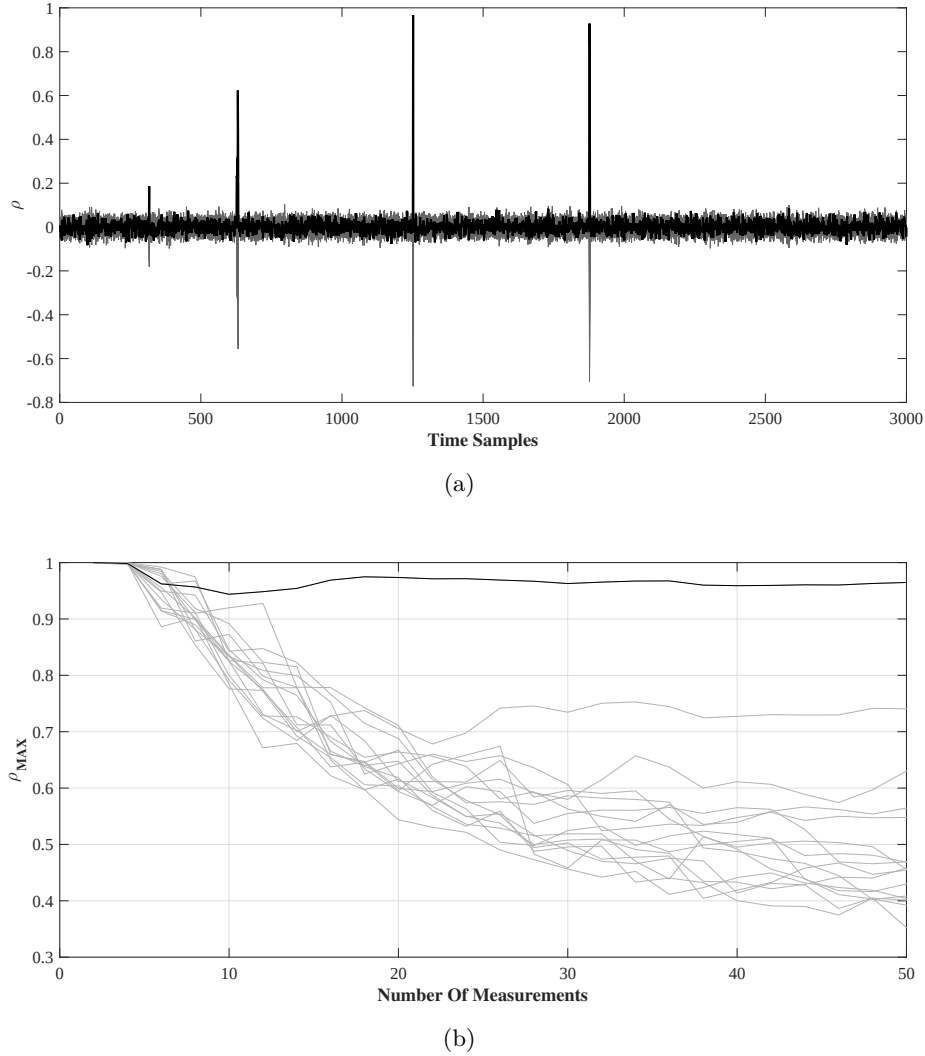
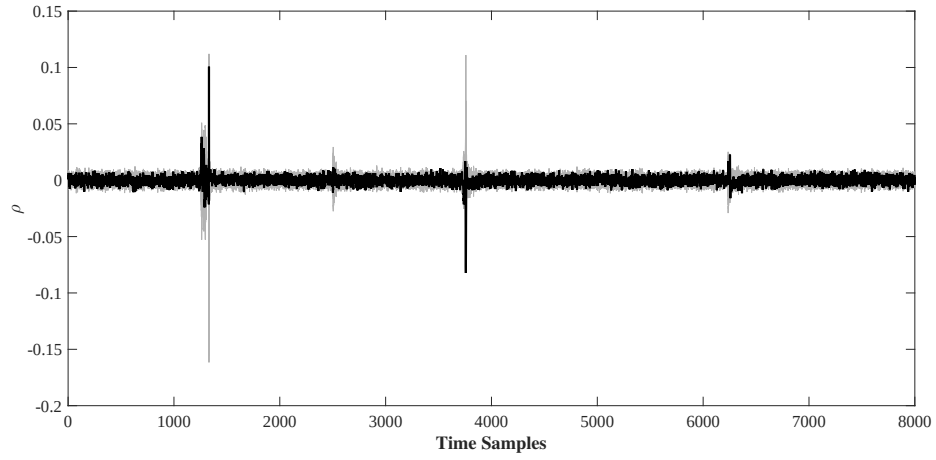
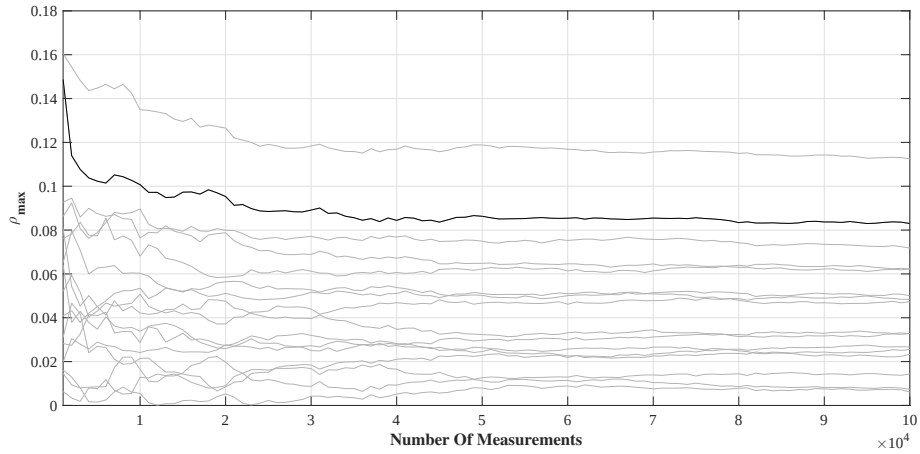


Figure 5.9. Plots of the CPA attack on the unprotected 4-bit PRESENT crypto-core. In (a), the correlation coefficient ρ vs. current traces time samples. In (b), the MTD diagram is shown. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

Results of CPA attack on both implementations are shown in Figure 5.9-5.10. The unprotected core has been successfully attacked with 8 traces. The protected core shows a robust behavior in counteracting PAA. In fact, the MTD of the protected PRESENT core is higher than 100k power traces. All simulated experiments on this core have not led to a successful attack, and the SVI is negative over the entire power



(a)



(b)

Figure 5.10. Plots of the CPA attack on the protected 4-bit PRESENT crypto-core, using the on-chip current equalizers as analog approach countermeasure. In (a) the correlation coefficient ρ vs. current traces time samples. In (b), the MTD diagram is shown. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

Table 5.2. Comparison between unprotected and protected implementation of the 4-bit PRESENT crypto-core.

	Area	P_{AV}	MTD	NED	NSD	Max SVI
	$[\mu m^2]$	$[\mu W]$		$[\%]$	$[\%]$	(@100k Meas.)
Unprot.CMOS	5.02	0.83	8	40.12	15.89	+0.25
Prot.CMOS	15.34	7.25	> 100k	7.53	2.28	-0.075

measurement set. This result remarks the capability of our design to counteract a dynamic power analysis attack. Note that the logic and registers of the two cores are the same, but in the protected one, current equalizers allow to avoid a physical attack that uses dynamic consumption as source of information leakage. The result of a CPA attack using the maximum storage capability is shown in Fig. 7. In Table 5.2, area and average power are shown for both implementations. In terms of silicon area, the protected core uses 3 times the area of the unprotected CMOS implementation, while the power consumption is almost 9 times.

Both NED and NSD values are strongly reduced in the protected implementation compared to standard CMOS, and no successful attack is possible within the storage capability. The improvement in security is more evident when the proposed countermeasure is used for logic sub-blocks. The use of current equalizers at gate-level leads to an inefficient design in terms of area, which even limits improvements in the security level. It has to be noted, that this kind of analysis is *pessimistic*, because, using simulations, we are considering a *Perfect Adversary model*, which has no limit in bandwidth. No filters have been designed on the main supply lines.

5.4 Improved OCE: an area and power efficient solution

As reported in Table 5.2, the required area of the protected core using the current-equalizer in Figure 5.4 is three times compared to unprotected one. In addition, also the average power overhead is $\times 8.7$. In order to make the current-mode approach compatible with demanding requirements of modern devices, such as IoT nodes, the countermeasure has to be improved, in order to reduce both area and power overheads.

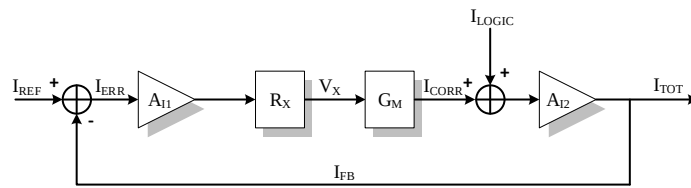


Figure 5.11. Simplified and linearized block scheme of the on-chip current-mode suppressor. I_{LOGIC} is considered as a disturbance to be rejected, in order to counteract a CPA attack.

An *improved on-chip current equalizer* (iOCE) is shown in Figure 5.11, which implements a current-mode feedback loop suppressor. The iOCE has been proposed during the Ph.D. work in [22]. The output current, which is namely the total current I_{TOT} , on the current sensor's branch, can be expressed as sum of two components as in Equations 5.1-5.3:

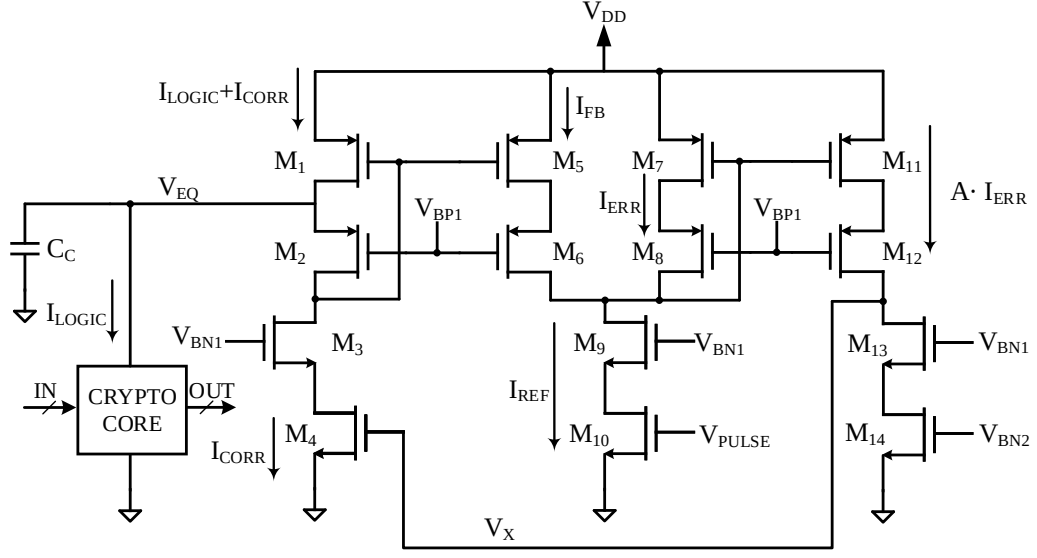


Figure 5.12. CMOS implementation of the improved on-chip current-mode suppressor. The protected crypto-core is fed through the suppressor circuit.

$$I_{TOT} = I_{REF} \frac{A_{I1} A_{I2} R_X G_M}{1 + A_{I2} A_{I1} R_X G_M} + I_{LOGIC}(pt, key) \frac{1}{1 + A_{I2} A_{I1} R_X G_M} \quad (5.5)$$

where I_{LOGIC} is the current drawn by the cryptographic processor, and represents the data-dependent signal exploited by the PAA. If the loop gain ensures the condition $A_{I1} A_{I2} R_X G_M \gg 1$, we have:

$$I_{TOT} \rightarrow I_{REF} \quad (5.6)$$

$$\Delta I_{TOT}(I_{LOGIC}(pt, key)) \rightarrow 0 \quad (5.7)$$

The CMOS implementation of the proposed on-chip current-mode suppressor is depicted in Figure 5.12. $M_{1,2}$ - $M_{4,5}$ implement a Flipped Voltage Follower Current Sensor (FVFCs) [39], which offers a current mirror, and a very low impedance at the drain node of M_1 , due to the shunt feedback provided by M_2 . The very low impedance helps to feed the supply voltage correctly to the cryptographic logics, without significant alteration of the nominal working condition. The output current of $M_{4,5}$, namely I_{FB} , is the sum of the current drawn by the logic I_{LOGIC} and the correction current I_{CORR} and it is compared with the reference current I_{REF} .

$M_{9,10}$ provide the reference current I_{REF} , which is not constant, but pulsed, in order to avoid an extra static power consumption. The iOCE is activated only

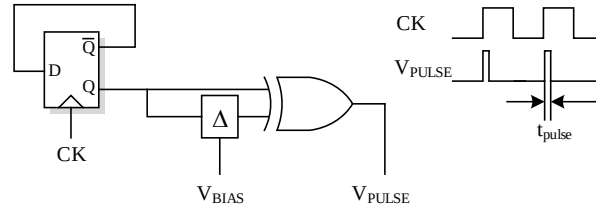


Figure 5.13. Implementation of the pulse generator, which generates the signal V_{PULSE} .

during the active edge of the clock signal, which the device leaks at its maximum level. According to Kirchhoff's law, the difference current I_{ERR} is mirrored by the high swing current mirror $M_{7,8,11,12}$, and it can be defined as follows:

$$I_{ERR} = I_{REF} - I_{FB} = I_{REF} - A_{I2} \cdot (I_{CORR} + I_{LOGIC}) \quad (5.8)$$

I_{ERR} is amplified by a proper sizing of the aspect ratio of the aforementioned high-swing current mirror. The difference current I_{ERR} is converted to a voltage signal V_X through the high impedance R_X that can be seen at the drain of M_{12} , which can be approximated as:

$$R_X \approx (r_{o,11}r_{o,12}g_{m12}) / (r_{o,14}r_{o,13}g_{m13}) \quad (5.9)$$

The signal V_X is used to control the gate voltage of M_4 , in order to obtain I_{CORR} . If we assume that the condition $A_{I1}A_{I2}R_XG_M \gg 1$ is satisfied, the I_{ERR} is negligible and the V_X is set to compensate the difference due to data-dependency of I_{LOGIC} . The control signal V_{PULSE} used to generate the pulsed I_{REF} , is generated by means of the circuit depicted in Figure 5.13. Also in this design, a starved inverter has been used as delay element. The width of the current pulse has to be chosen as a tradeoff between security requirements and the power consumption overhead according to the following constraint:

$$t_{cp} < t_{pulse} < \frac{t_{clk}}{2} \quad (5.10)$$

5.4.1 Case Study: 4-bit PRESENT Crypto-Core

In order to demonstrate the effectiveness of the improved on-chip current-mode feedback countermeasure, simulated experiments have been performed on the 4-bit PRESENT crypto-core, shown in Figure 3.18. In this case, the protected crypto-core has been designed using only one protection circuit. Thus, the main V_{DD} pin of the cryptographic logic is connected to the output of the iOCE unit. The external

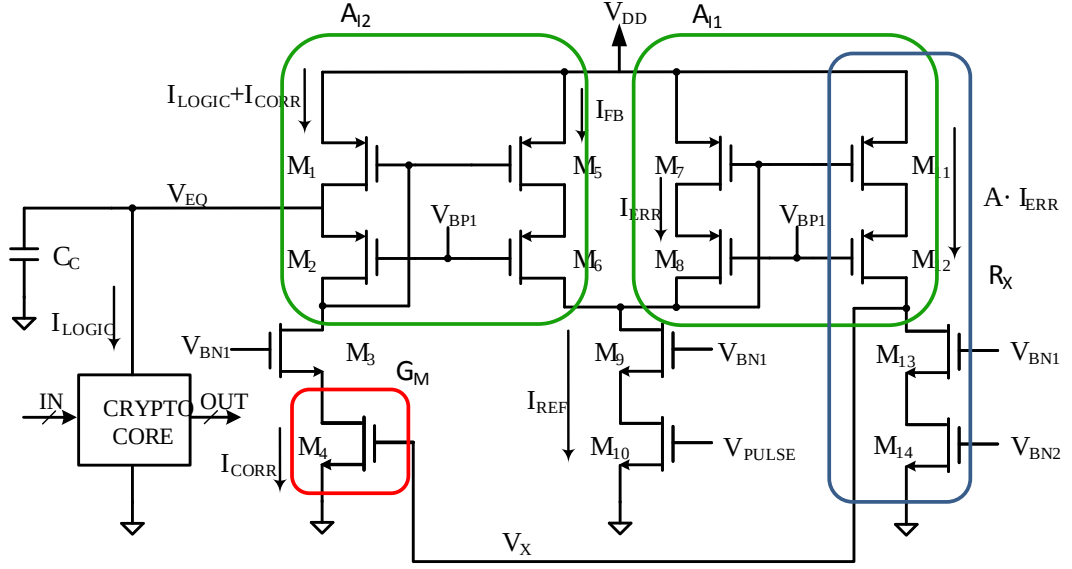


Figure 5.14. CMOS implementation of the improved on-chip current mode suppressor with each sub-system in Figure 5.11 highlighted.

power supply has been set to 1V, while the clock frequency has been set to 20MHz. Current consumption has been measured at the V_{DD} pin. A maximum of a 100k power traces has been chosen as maximum storage capability. Also in this case, the output of the S-BOX has been chosen as target intermediate value. The key has been set to $(5)_2$, and the t_{pulse} has been set to 1ns.

The noise-free power traces sample collected on the protected implementation of the 4-bit PRESENT are shown in Figure 5.15. The on-chip current-mode feedback equalizer is able to strongly reduce the power variability due to data-dependency of the CMOS crypto-core.

As we can notice from Figure 5.17(a), the protected core with the improved on-chip current-mode feedback suppressor does not exhibit the correct key with the maximum correlation coefficient, demonstrating the effectiveness of the countermeasure to thwart CPA. The correlation coefficient is reduced by a factor of 47. The MTD is 85 for the unprotected implementation, while the protected crypto-core has a MTD $>100k$. Regarding results in Section 5.3.2, different seeds have been used to generate additive Gaussian noise to perform simulated attacks. Thus, the MTD value on the unprotected core is slightly different in this section. A resume of the comparison between the two implementations is shown in Table 5.3.

Comparing the area and power consumption of the improved on-chip current suppressor with the protection circuit discussed in the previous section, we can notice that both design aspects have been improved too. Moreover, the correlation coefficient has been reduced by a factor of 47.

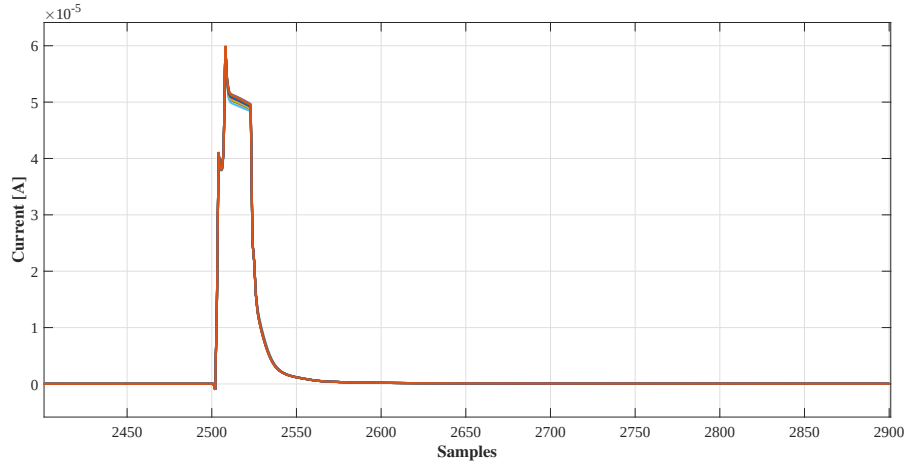


Figure 5.15. Power traces on the protected implementation of the 4-bit PRESENT crypto-core. The improved on-chip current-mode feedback equalizer is able to strongly reduce the power variability due to data-dependency of the CMOS crypto-core.

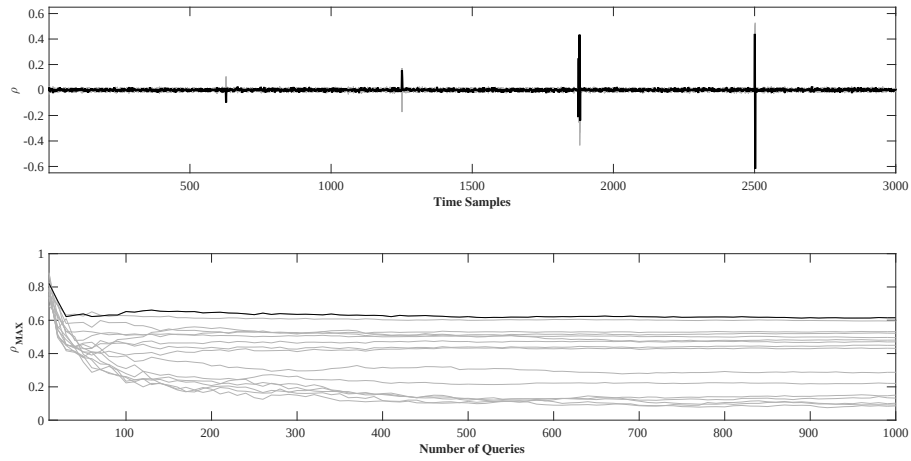


Figure 5.16. CPA attacks on unprotected PRESENT crypto-core. Top figure shows the correlation coefficient ρ vs. current traces time samples, using 1000 power traces. Bottoms figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

5.4.2 Full Implementation of the iOCE-Protected PRESENT-80

In order to better assess the effectiveness of the improved on-chip current equalizer, the complete CMOS implementation of the PRESENT-80 block cipher in Figure 3.19 has been adopted as additional case study. A single on-chip suppressor has been used to protect and feed the core, as in the previous case. External power supply voltage has been set to 1V and the clock frequency to 20MHz. The SNR has been set to 18dB. The higher SNR value is due to the fact that in this case the measured power

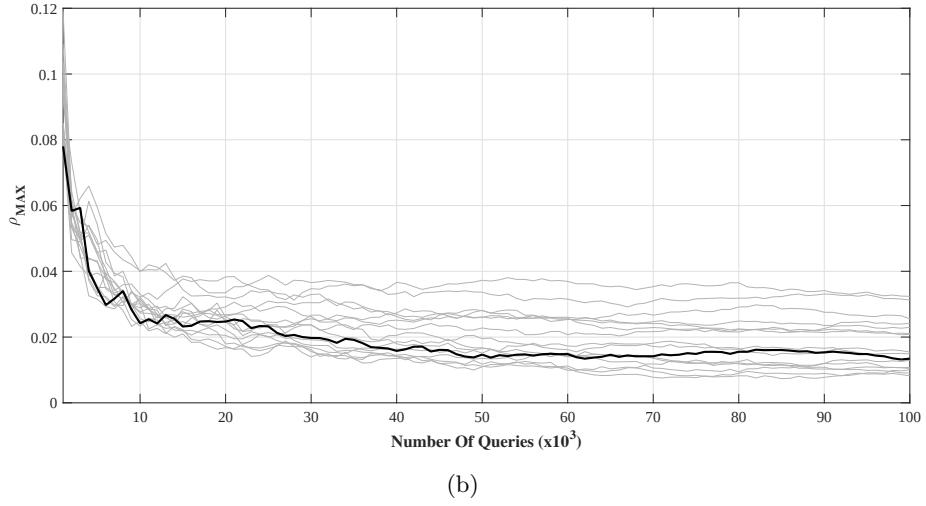
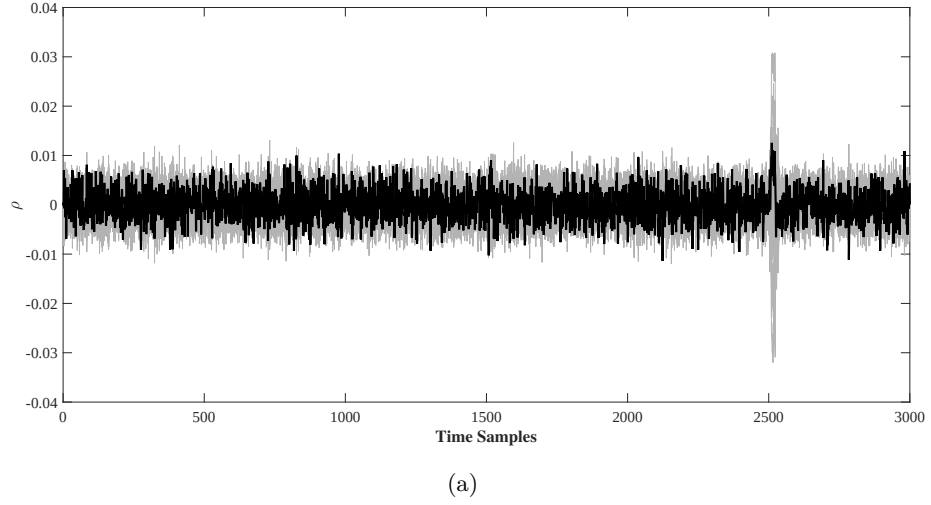


Figure 5.17. CPA attacks on the protected 4-bit PRESENT crypto-core implementation. The correlation coefficient ρ vs. current traces time samples, using 100k power traces, is shown in (a). The MTD diagram is shown in (b). The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

consumption takes into account also non-targeted sub-blocks of the cryptographic circuitry, and smaller noise power are required to simulate a realistic environment. Without loss of generality, the target function is the most significant nibble of the output of the *SubsLayer* at the first round, expressed by Equation 5.11.

$$ct_{63,62,61,60}^{round-1} = S - BOX \left(pt_{63,62,61,60} \oplus key_{79,78,77,76}^{round-1} \right) \quad (5.11)$$

Results of CPA attacks on both implementations are depicted in Figure 5.18-5.19, and a resume is reported in Table 5.4. CPA results on both implementations

Table 5.3. Comparison of the unprotected and protected implementation of the 4-bit PRESENT crypto-core, using the improved on-chip current equalizer.

	Area [μm^2]	P _{AV} [μW]	ρ_{MAX}	MTD
Unprot. CMOS	5.02	0.83	0.615	85
Prot. CMOS (iOCE)	5.40	1.20	0.013	> 100k

Table 5.4. Comparison of the unprotected versus protected implementation of the PRESENT-80 using the improved on-chip suppressor as protection circuit.

	Area [μm^2]	P _{AV} [μW]	MTD	NED [%]	NSD [%]	Max SVI (@100k meas.)
Unprotected	105.29	12.57	16	6.76	2.27	+0.132
Protected (with iOCE)	105.96	13.36	> 100k	1.85	0.50	-0.189

Table 5.5. Comparison of the iOCE feedback suppressor with other analog approach and gate-level CPA/DPA countermeasure in terms of area and average power overhead. Unprotected CMOS implementation is used as reference.

	CMOS	WDDL [147]	MDPL [117]	Gornik et al. [65]	OCE [20]	iOCE [21]
Area	1	3.1	4 – 5	10	3	1.004
Power	1	3.7	3 – 7	3.5	8.7	1.07

(standard CMOS and iOCE-protected CMOS) have shown that also in this case the sub-key can be recovered with only 16 power traces on the unprotected one, with a +0.132 of SVI. The improved on-chip current-mode suppressor provides an MTD greater than 100k measurements, and the SVI is always negative. The SVI using the maximum storage capability is -0.189. It has to be noted that also the rank of the key in the protected implementation (see Figure 5.19(b)) is fair distant from first places, remarking the real effectiveness of this improved on-chip suppressor to hide the information leakage through dynamic power consumption. In addition to that, the area overhead is very small compared to the on-chip current equalizer depicted in Figure 5.4 and to other CPA countermeasures, as shown in Table 5.5. Also the power consumption is very small, and it requires only +7% compared to the unprotected implementation of the PRESENT-80.

The iOCE has a very small footprint compared to the OCE unit. It requires only a +0.4% area overhead and a +7% power consumption overhead. This improved on-chip suppressor is fully suitable and implementable in secure IoT smart devices, since it is able to meet demanding requirements of area/power overhead, while providing a strong increase in level of security. It has to be considered that the presence of the on-chip current suppressor is compliant with several others PAA countermeasures, giving to designers the possibility to implement nested protections throughout different abstraction levels.

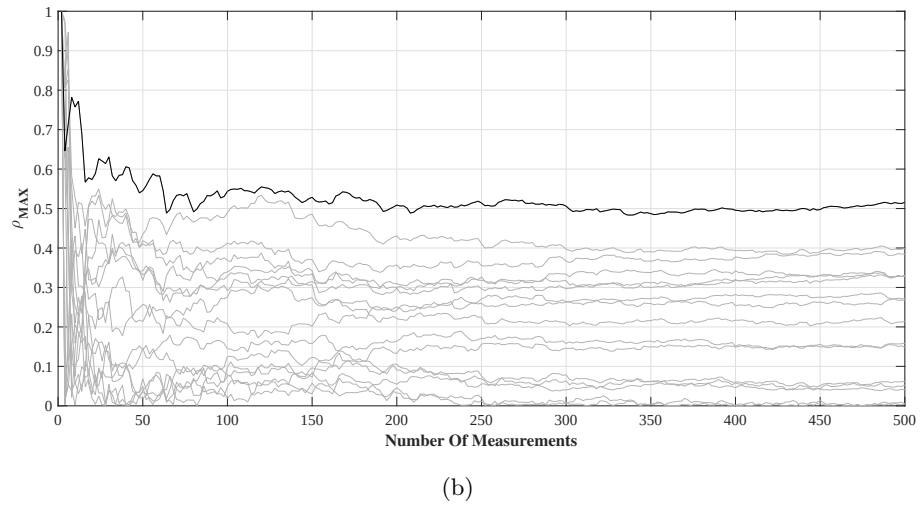
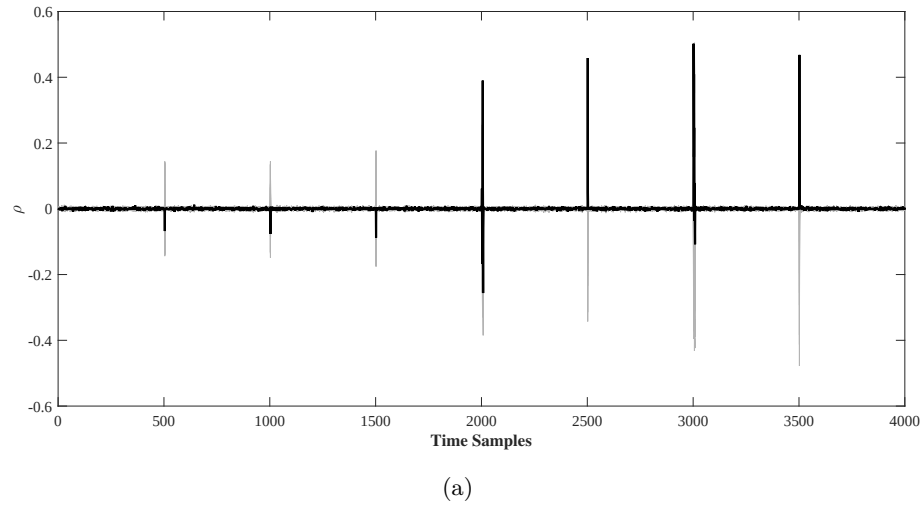
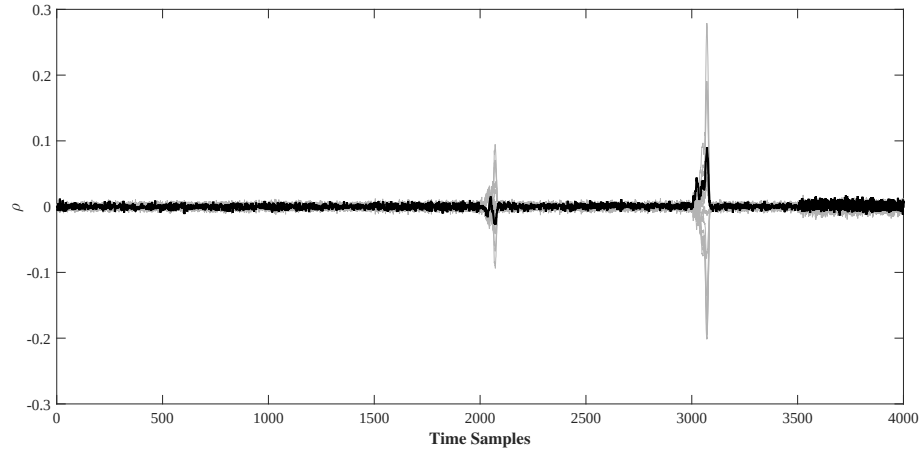
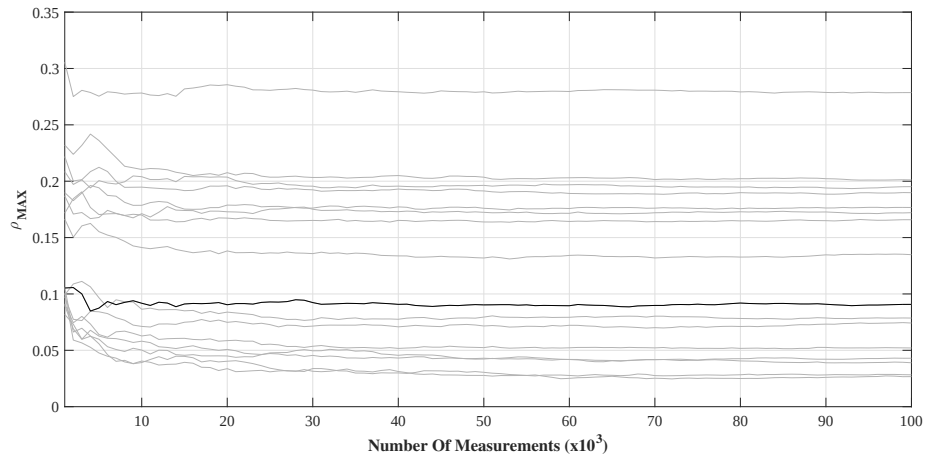


Figure 5.18. Plots of the CPA attack on the unprotected PRESENT-80. Figure in (a) shows the correlation coefficient ρ vs. current traces time samples. Figure in (b) shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

For the sake of completeness, the case study of the full implementation of the PRESENT-80 has been analyzed within the technology process corners, in order to take into account the presence of intra-die variations and their impact on the effectiveness of the proposed countermeasure. In Figure 5.20-5.21, a resume of CPA attacks on the PRESENT-80 with SS and FF process corners are shown. It has to be noted that also in both case, the countermeasure is effective and the MTD is greater than $100k$. The SVI in the FF case is -0.068 , and in the SS case is -0.111 , using the maximum storage capability. These results show that the improved on-chip current equalizer is able to counteract a CPA attack also in the presence of intra-die variation.



(a)



(b)

Figure 5.19. Plots of the CPA attack on the protected PRESENT-80 (nominal case), using the on-chip current-mode suppressor of Figure 5.12 as analog approach countermeasure. Figure (a) shows the correlation coefficient ρ vs. current traces time samples. Figure (b) shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

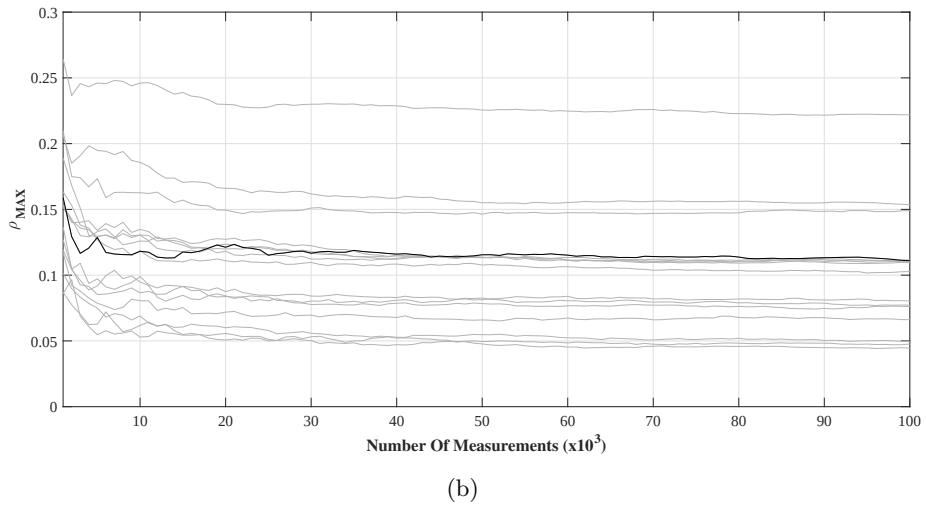
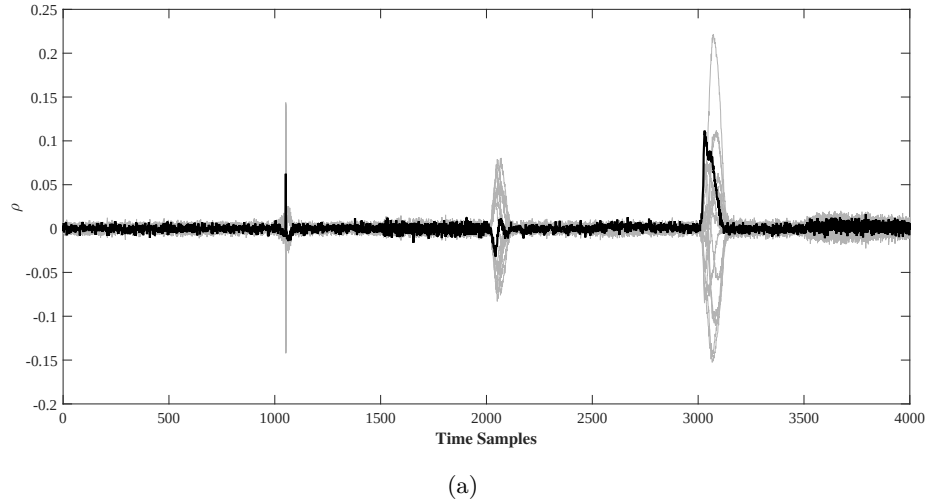
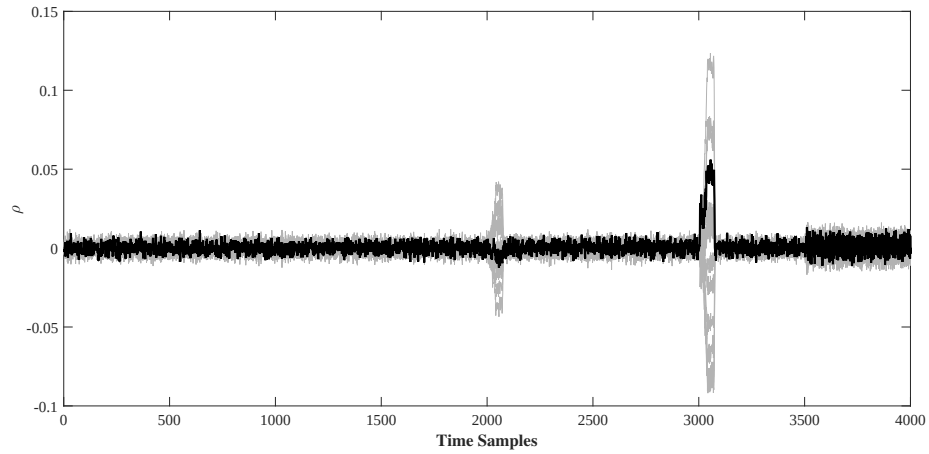
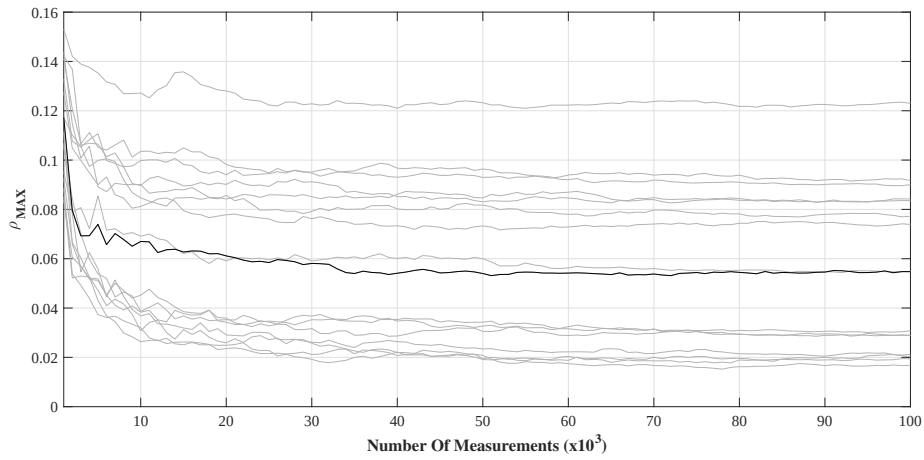


Figure 5.20. Plots of the CPA attack on the protected PRESENT-80 (SS corner), using the on-chip current-mode suppressor of Figure 5.12 as analog approach countermeasure. Figure (a) shows the correlation coefficient ρ vs. current traces time samples. Figure (b) shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.



(a)



(b)

Figure 5.21. Plots of the CPA attack on the protected PRESENT-80 (FF corner), using the on-chip current-mode suppressor of Figure 5.12 as analog approach countermeasure. Figure (a) shows the correlation coefficient ρ vs. current traces time samples. Figure (b) shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

Chapter 6

Test and Security Evaluation of the SERPAES Chip

6.1 Introduction

The analysis of a secure implementation has to cope with a physical evaluation after the manufacturing of the chip. The post-silicon verification is one of the most critical stage in the assessment of the information leakage that can be exploited to recover sensible data. Simulations are able to provide useful information on potential source of exploitable leakage, as, nowadays, the modeling of circuits in pre and post layout are very accurate compared to the past. Lower is the abstraction level of the simulations, higher will be the accuracy in the results. However, some unwanted effects, due to fabrication process, can threaten the physical security of the device and may not be evident in simulations. Hence, a measurement campaign on the real chip (attacks and leakage assessment) should be conducted to verify if security requirements are met. In this chapter, we will discuss about the evaluation of four out of seven crypto-cores, designed with RTL and gate-level countermeasure, and implemented on a dedicated ASIC, named SERPAES. The prototype SERPAES chip has been designed in our department (Centro Studi Giorgio Barzilai lab.), during 2013-2014, using the CMOS065SVTLP technology provided by STMicroelectronics. As we will discuss in this chapter, the SERPAES chip contains several crypto-cores based on two block cipher algorithms:

- AES-128 (also known as Rijndael);
- SERPENT.

The chip is divided in two macro-blocks, as shown in Figure 6.1. The smallest section has been implemented using full-custom cells, designed in SABL and iDDPL styles. These two logic styles have been used to implement two 4-bit crypto-cores based on SERPENT algorithm. The iDDPL implementation of this core is the

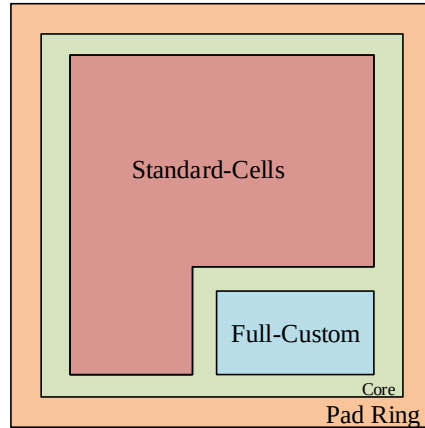


Figure 6.1. Macro-blocks in SERPAES chip.

first physical implementation of the logic family presented in [29], and mentioned in Chapter 4. Thus, the SERPAES could be considered as the first prototype of the iDDPL style. In addition, the SABL implementation has been designed as state-of-the-art of full-custom DPL style for cryptographic applications adopting the RTZ encoding. Most of the die's area is dedicated to five different implementations of the AES-128 algorithm, all of them using standard-cells only. Four cores have been designed using different RTL-level countermeasures, while a fifth one has been implemented unprotected, to be used as reference for PAAs evaluations and comparison. RTL-level countermeasures used in the SERPAES chip have been developed in our department during the last years as VHDL firmware for FPGA platforms [35], [36], [99], [101], [100]. Functional and security level assessments have been evaluated through FPGA experiments, using different FPGAs:

- Altera Cyclone;
- Xilinx Spartan-6.

A microphotograph of the SERPAES chip is shown in Figure 6.2.

In addition, also a custom printed circuit board has been designed to evaluate the SERPAES chip. The prototype board has been equipped with all the necessary circuitry (linear regulators and filtering capacitors) to provide the correct power supply required by the technology of the chip. A complete set of headers are used to measure the power consumption of both sections of the chip independently. SABL and iDDPL cores have additional headers and jumpers to measure individually the power consumption of sections of the core. On-board level-shifters provide voltage conversions for I/O interfacing. A serial interface has been embedded in the SERPAES chip, for data communications and chip programming. Sets of internal multiplexers have been designed to select the desired core to stimulate. An on-board

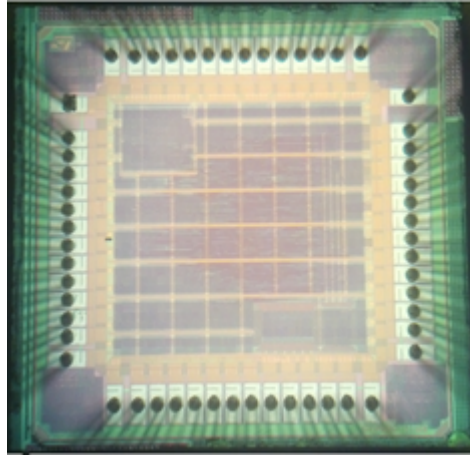


Figure 6.2. Microphotograph of the SERPAES chip.

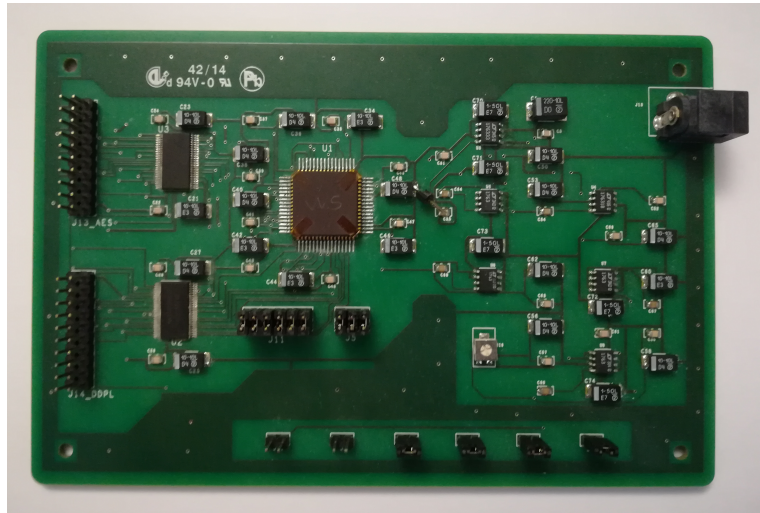


Figure 6.3. Printed circuit board with the SERPAES chip, power supply network and level shifters.

voltage regulator provides the desired V_{bias} for the iDDPL SERPENT crypto-core, to adjust the internal t_{eval} used by TEL-compatible circuitry.

During the PhD course, the SERPAES chip has been tested functionally, in order to provide a characterization of the performance of the chip as hardware accelerator in secure applications. Moreover, an intensive measurement campaign has been carried out to perform a security verification and evaluation of both standard-cells cores and full-custom designed cores. In this chapter, we present the results of PAA evaluations on one of the countermeasured AES-128 core. A comparison between the SABL and iDDPL implementations of the 4-bit SERPENT crypto-core is also given in terms of security level.

6.1.1 Securing RTL Implementation of Cryptographic Devices, State-of-the-Art

PAA countermeasures operating at register-transfer level (RTL) typically require a simpler design flow, as they do not have need of full-custom building blocks, and can be implemented also on reconfigurable hardware, such as FPGAs. One of the first RTL countermeasures proposed in the technical literature was the *Random Pre-charge Logic* (RPL) [35]. In RPL, dummy data generated by random number generators (RNG) are pre-charged in the combinational networks at the rising edge of the clock cycle and evaluated for half the clock cycle. In [99], authors showed an architectural technique to protect the *AddRoundKey* processing block of an AES crypto-engine, using a duplicated XOR data-path, with one side dedicated to real-data processing and the other to random-data processing, both in inverted and non-inverted form. The processing of real and random data takes place in a time-interleaved manner, to “obfuscate” dynamic power consumption and reduce its correlation with the input data. Authors in [101] have proposed the use of random clocks, generated with random number generators and phase shifters, to increase the randomness of the time behavior of the power traces, and thwart PAAs. In [89], the intra-cycle energy variation was exploited. A large variance in data-dependent delay was introduced to increase the randomness of power traces, reducing the probability of a successful attack. Authors in [12] proposed the *CMOS-based Blurring Gate* (CMOS-BG) embedded in a CMOS network. The CMOS-BG is an RTL-level countermeasure operating in both static and dynamic mode. The presence of a CMOS-BG in a combinational network provides random delay, as in [36], with the possibility to randomly pre-charge internal nodes of the network. The combination of these two techniques blurs the power profiles of the cryptographic device and randomize its initial conditions. These countermeasures focus on protecting the combinational logic, and have no effect on the power consumption of sequential logic (i.e. registers), which is a significant contribution to overall data-dependent current consumption. Furthermore, all the previously proposed RTL countermeasures [35], [99], [101], [89], [12], [36], have been validated referring to simulations and/or FPGA implementations and no measurement results on ASIC implementations can be found in technical literature.

6.2 RTL-Level Countermeasures for AES-128

The AES-128 is one of the most used block cipher, in both hardware accelerators and software implementations. The SERPAES chip contains five different implementations of the AES-128 block cipher encryption algorithm. These cryptographic cores have been intensively tested in our department as VHDL implementations for Altera Cyclone FPGA [100] [99] [101]. The chip has been designed to run only one AES-128 core at a time, in order to minimize coupling effects. The selection has been made through a 3-bit input word *AES_sel*. *AES_sel* is used to enable one core at a time and also to route forward five 128-bit ciphertext buses to the

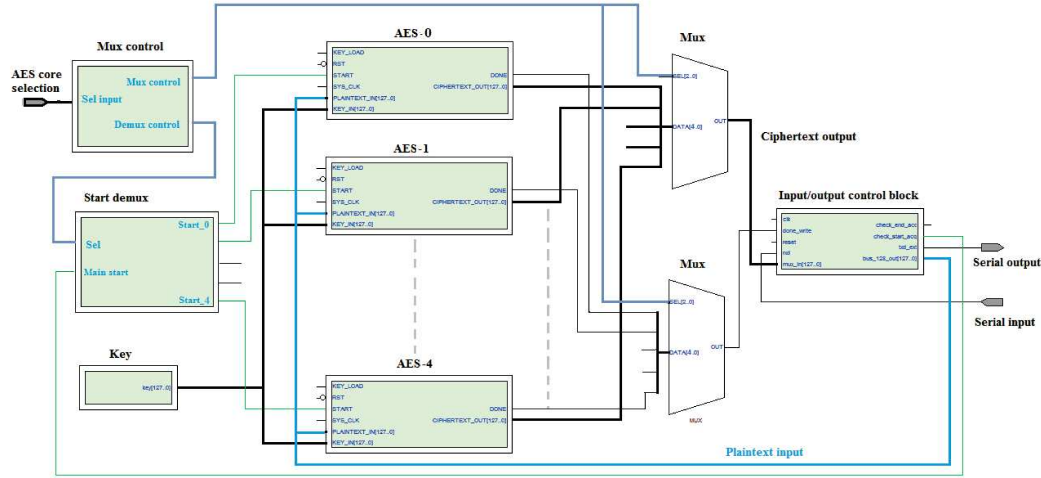


Figure 6.4. Simplified schematic of the SERPAES' standard-cell section with AES-128 implementations.

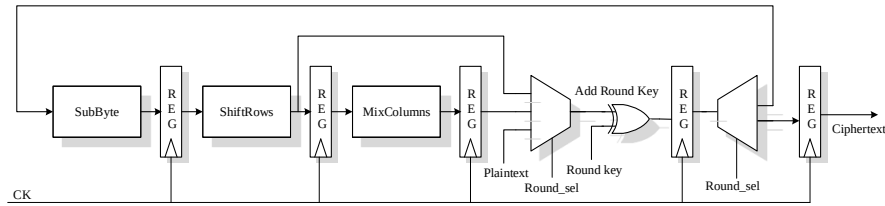


Figure 6.5. Data-path of the basic implementation of the AES-128 block cipher (AES-0).

serial interface. A simplified schematic diagram of the standard-cell section of the SERPAES chip is shown in Figure 6.4. It has to be noted that the also a *Random Number Generator* (RNG) has been designed and placed in this section of the chip, since RTL-countermeasures in SERPAES make use of random data. There a plethora of possible RNG design on ASIC. In this case, a simple *Linear Feedback Shift Register* (LFSR) has been used as pseudo-RNG. In this section, a brief description of AES-128 implementations is presented. We refer to AES-128 implementations with number, from 0 to 4, where AES-0 is the unprotected implementation. AES-4 implementation has been the target core of an intensive measurement campaign. Therefore, the analysis of the architecture of AES-4 will be more consistent than other cores.

6.2.1 Unprotected Reference Implementation (AES-0)

The basic AES-128 encryption processor implemented in the SERPAES, namely AES-0, has been designed according to the VHDL in [98]. The data-path of the architecture of AES-0 is shown in Figure 6.5. It is composed by the four basic operation of the AES-128 (see Appendix A.1):

- *AddRoundKey*;
- *SubByte*;
- *ShiftRows*;
- *MixColumn*.

They compose a pipeline of four stages. The entire pipeline can be assumed as a *round* of the AES algorithm. Each operation has been implemented with a combinational circuit. A key scheduler is also present in the core. A finite state machine (not shown in Figure 6.5) controls the routing of data through the pipeline, and allows to interface the core with external circuitry. The cryptographic processing of the input data is handled completely parallel, thus, each bus in Figure 6.5 is 128-bit wide. The entire encryption corresponds to 10 rounds plus a final 3-layers round, requiring 44 clock cycles to perform a complete encryption. Therefore, the throughput can be considered 3 bytes per clock cycle.

It has to be mentioned that the synthesis of the *SubByte* operation is critical for PAAs. It has been demonstrated that the PAA resistance of the AES-128 can be improved if the AES' S-BOX function (see Appendix A.1) is synthesized using combinational cells instead of look-up tables [151]. In this case, the *SubByte* operation has been synthesized using only combinational logic cells.

6.2.2 Random Pre-charged Interleaved Pipeline Countermeasure (AES-1)

Along with the classical sub-blocks in the architecture of AES-128 in Figure 6.5, it is possible to design several countermeasures operating at RTL-level. In AES-1 core, the *Random Pre-charged Interleaved* (RPI) pipeline has been adopted, as shown in Figure 6.6, which was presented in [35]. Each pipeline stage of AES-0 in Figure 6.5 has been modified according to Figure 6.6. In AES-1, each register in the architecture is doubled. A *commutator* routes alternatively the real data and a random data in two parallel registers. This unit can be implemented using a pair of multiplexers, as shown in Figure 6.7. When the real data is stored in one register, the other one will store a random vector, generated by the RNG. Output data of registers are forwarded to the combinational network of the pipeline stage through a multiplexer. *SEL* signal makes the combinational network to pre-charge at the value imposed by the random vector at the beginning of the clock cycle.

6.2.3 XOR-Series Countermeasure (AES-2)

AES-2 is based on a different approach. It is composed by two countermeasures at the same time, both at RTL-level. The structure of the countermeasure in AES-2 is shown in Figure 6.8. The first one acts to protect *AddRoundKey* at round-0, where

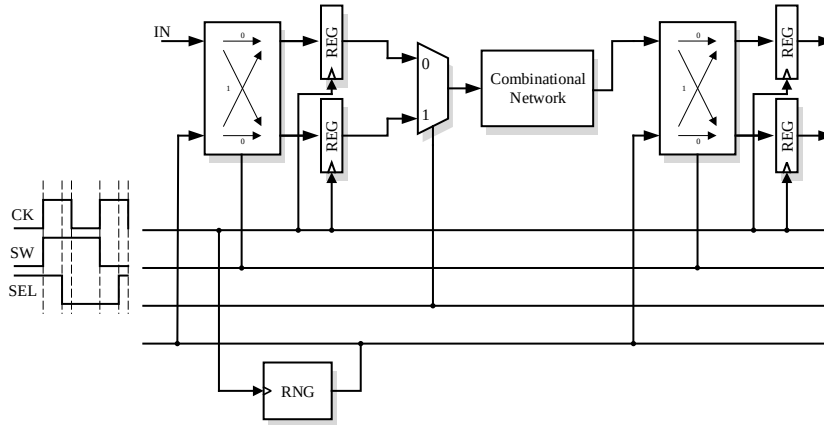


Figure 6.6. Random Pre-charged Interleaved pipeline countermeasure in AES-1.

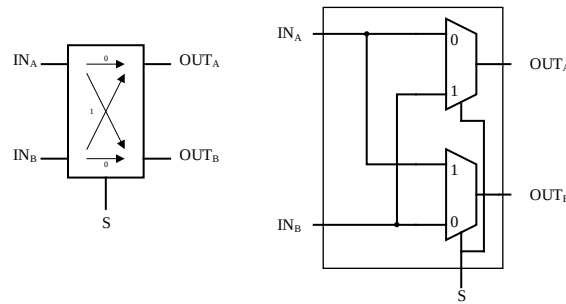


Figure 6.7. Commutator implementation.

the relevance of the original key is the highest. The *AddRoundKey* is based on the bitwise XORing of the data with the round key. In AES-2, the XOR is doubled, in order to combine data with the key and the inverted key. This solution acts as a replication of the dual-rail principle at RTL-level, aiming to balance the current consumption. The additional countermeasure doubles also the register at each stage of the pipeline. The data at the output of the double XOR is multiplexed with a random data (both direct and inverted) and processed in parallel by cascaded registers. The routing of datum is handled by *SEL*, that ensure data correctness alongside the pipeline. The random data is processed sequentially with the real data, and thus the clock frequency has to be doubled to maintain the same throughput of AES-0.

6.2.4 XOR-Parallel Countermeasure (AES-3)

AES-3 makes use of a modified version of the XOR-series countermeasure in AES-2. The input section is designed similar to AES-2, adopting the same XOR duplication to protect the *AddRoundKey* intermediate result at round-0. To enhance the randomness

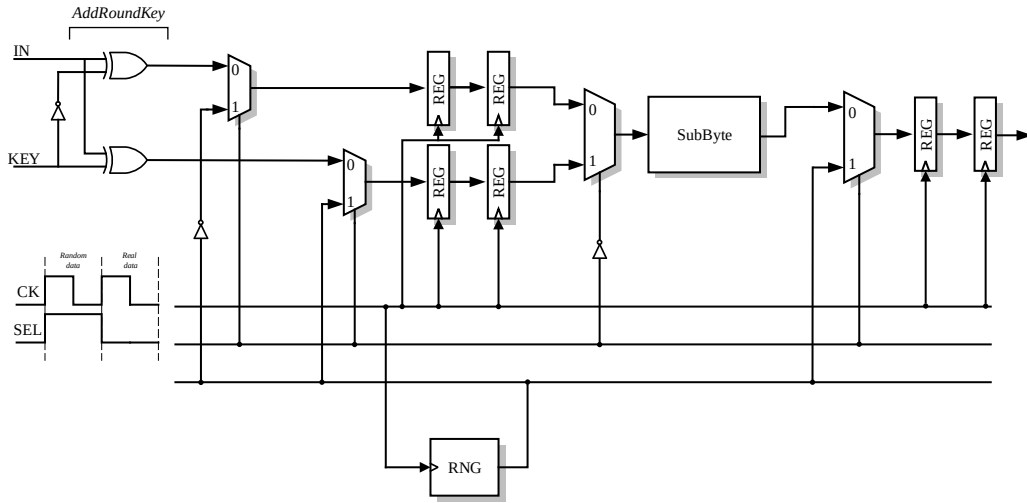


Figure 6.8. The XOR-series countermeasure in AES-2.

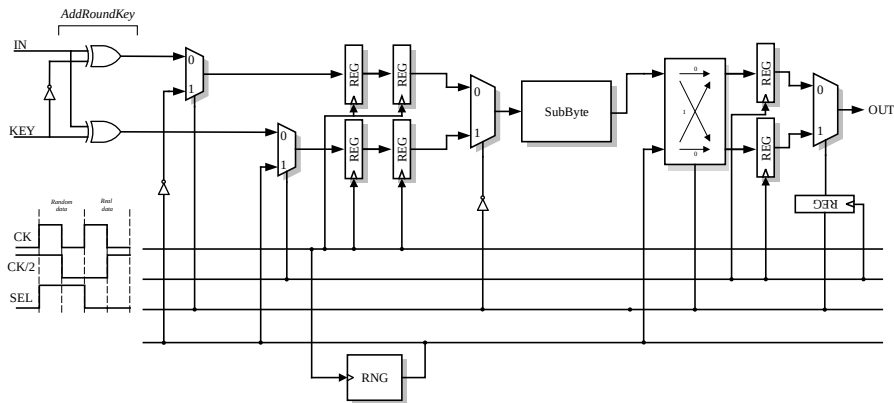


Figure 6.9. The XOR-parallel countermeasure in AES-3.

of the data processed, a commutator is added at the output of each combinational layer, providing a random pre-charge of next layers, as shown in Figure 6.9. In addition, the parallel registers at the output of the commutator provides the random pre-charge during the first semi-period of the clock [151], thanks to the presence of the final multiplexer.

6.2.5 Secure Double Rate Register (AES-4)

The last core in the standard-cell section of the SERPAES chip is AES-4. The architectural-level countermeasure used in AES-4 is based on a novel building block, called *Secure Double Rate Register*. The block scheme of the proposed *Secure Double Rate Register* (SDRR) is depicted in Figure 6.10. The SDRR is composed of two

cascaded registers and an input multiplexer which allows to select the input data to the first register. Flip-flops in the SDRR are clocked by the CK signal (whose frequency is doubled with respect to the CK signal in the reference architecture). The control (SEL signal) is used to select between real and random data. By using the SDRR in place of conventional registers the power consumption of both sequential and combinational gates can be randomized. In fact, when the real input datum is stored in one of the two registers of the SDRR, a random datum is stored in the other one and vice versa, allowing de-correlation of the power consumption, as described in the following.

AES-4 architecture is shown in Figure 6.11. It exploits a *pipelined* pre-charging technique to force both combinational and sequential logic to a random state S_r . For this purpose, conventional registers are replaced by SDRRs. In each stage of the pipeline, the SDRR feeds the combinational logic alternating the correct and the random data. In this way, correct data and random data are processed and stored simultaneously, exploiting the diffusion property of the cryptographic algorithm. To better explain this point, we refer to the power consumption model in [35]. According to this model the current $I_{DD}(t)$ drawn by a standard CMOS circuit is a function of the transition from an initial state S_k to a final state $S_{(k+1)}$:

$$I_{DD}(t) \propto \sum_i (i_{DD}(S_k(i) \rightarrow S_{k+1}(i), t)) \quad (6.1)$$

where $i_{DD}(S_k(i) \rightarrow S_{(k+1)}(i), t)$ is the current consumption of the i -th node of the circuit at time t . Equation 6.1 highlights a strong correlation between the current $I_{DD}(t)$ and the transitions due to changes in the internal state. Due to the presence of the double-rate registers in the SDRR, random states S_r and S_{r+1} force both sequential and combinational gates to consume randomly along with the consumption given by real initial and final states S_k and S_{k+1} , corrupting the correlation between the current consumption $I_{DD}(t)$ and the internal transitions:

$$\begin{aligned} I_{DD}(t) \propto & \sum_i (i_{DD}(S_k(i) \rightarrow S_r(i), t) + \\ & + i_{DD}(S_r(i) \rightarrow S_{k+1}(i), t - T_{CK/2}) + \\ & + i_{DD}(S_{k+1}(i) \rightarrow S_{(r+1)}(i), t - T_{CK})) \end{aligned} \quad (6.2)$$

In conventional CPA attacks the attacker is not supposed to know the hardware architecture and implementation of the device under attack, and his/her knowledge is limited to the adopted cryptographic algorithm. In *technology-based* attacks, which have been recently introduced in [12], the attacker is able to identify the sample t^* (or a narrow time window around it), in which the information leakage can be exploited through dynamic power consumption. Authors in [12] have shown that the conventional *Random Pre-charge Logic* (RPL) [35] offers a reduction of the SNR for the attacker, but this reduction depends strongly on the duration of the pre-charge phase. If the attacker gains knowledge of the duration of the pre-charge phase, he/she can retrieve the secret key by analyzing the correlation in a narrow time window around the switch from the *pre-charge* phase to the *evaluation* phase.

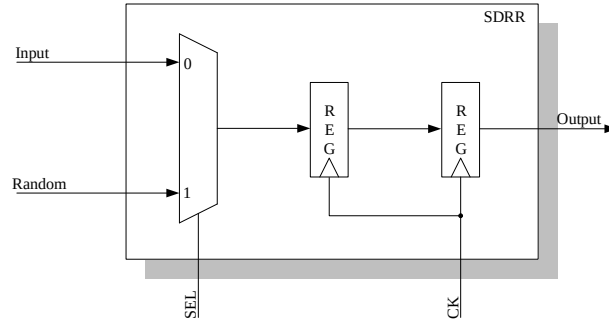


Figure 6.10. Block scheme of the *Secure Double Rate Register* in AES-4.

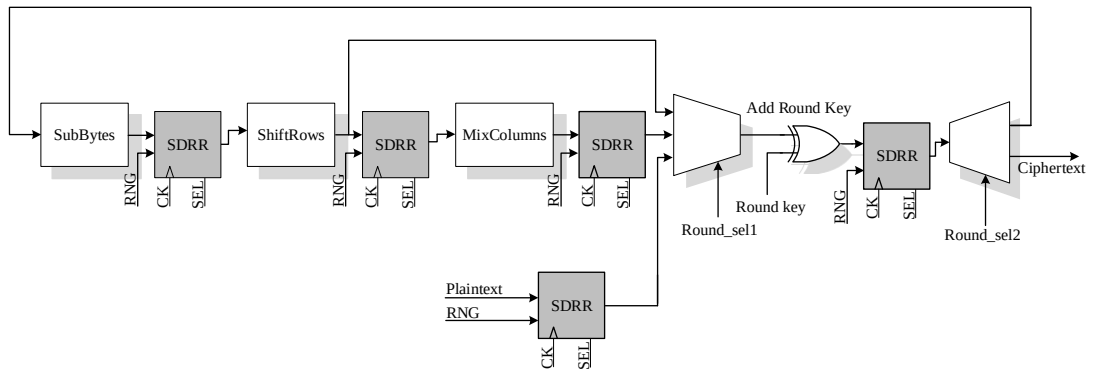


Figure 6.11. Block scheme of the architecture of AES-4 with SDRR units instead of regular registers.

The usage of the proposed SDRR blocks avoids this critical problem allowing the combinational path to evaluate random data throughout the entire clock cycle, and not only a portion of it. The adoption of the interleaved processing of random data along with real data ensures the protection of both combinational and sequential logic and offers a two-fold improvement:

- it removes memory effects on the combinational path of a stage of the pipeline;
- the presence of two registers in each SDRR unit ensures that the total consumption due to data-storage is randomized by means of the simultaneous storage of the random data alongside with real data.

It has to be pointed out that the proposed technique does not require the duplication of the data-path for the random datum, and limiting the area and power consumption overhead. Furthermore, the proposed architecture does not suffer from critical problems related to the imbalance of the fan-out, because the real and random data share the same data-path.

Table 6.1. FPGA implementation of AES-0 and AES-4 cores on a Xilinx Spartan-6 LX45.

	LUT	FFs	Avg. Overhead	Norm. Power	MTD
AES-0	1146	1040	—	1	< 256
AES-4	1476	1606	40%	2.9	> 100k

6.3 Security Level Evaluation of AES-4, a Case Study

In this section we present an evaluation of the security level of the AES-4 compared to unprotected AES-0. During the writing of the VHDL code, AES-4 has been tested on the Xilinx Spartan-6 LX45, mentioned in Chapter 3 and 4. After a functional level verification, the AES-4 has been attacked using CPA, in order to state the level of security of the protected implementation compared to AES-0. The post-silicon verification has been carried out similarly to the FPGA case, starting from a functional level test. The leakage assessment of the core has been deeply analyzed using actual and information theoretic security metrics, using the dynamic power consumption of the chip as side-channel.

6.3.1 FPGA Prototyping of AES-0 and AES-4

To provide a preliminary validation of the proposed protected AES architecture, we have implemented and tested AES-0 and AES-4 cores on a Xilinx Spartan-6 LX45 FPGA device. A summary of the FPGA implementation of AES-0 and AES-4 is shown in Table 6.1 (clock frequency are different in order to get the same throughput).

Also in the FPGA design, random data have been generated by means of a simple PRNG based on the same LFSR. AES-0 and AES-4 have been attacked through CPA (adopting HW power model). The aim of the attacks was to recover the encoding key, which was hard-wired in the FPGA design, along with other interface circuitry:

$$key = '9DAC5F7D56E8BE7B655A48912120BA77' \quad (6.3)$$

The clock frequency has been set to 10MHz (20MHz for AES-4) and the output of the S-BOX at the first round has been chosen as the target function for the attack. Results are shown in Figure 6.12 and 6.13. Notice that the number of queries on the bottom plots are different. The AES-0 core has proven to be vulnerable to correlation analysis. In fact, most of the key's bytes were successfully retrieved with less than 256 power traces and without any pre-processing. The correlation coefficient resulting from the CPA attack on AES-0 (top plot) and the MTD diagram (bottom plot), summarizing the maximum correlation coefficient versus the number of queries, are shown in Figure 6.12. The attack on AES-4 was not successful even with 100.000 traces. The experimental results can be seen in the correlation curves

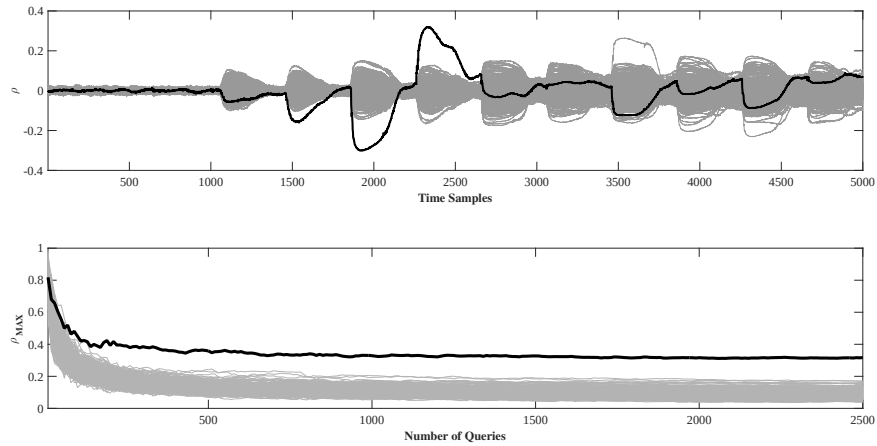


Figure 6.12. Plots of the CPA attack on AES-0 (FPGA implementation). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

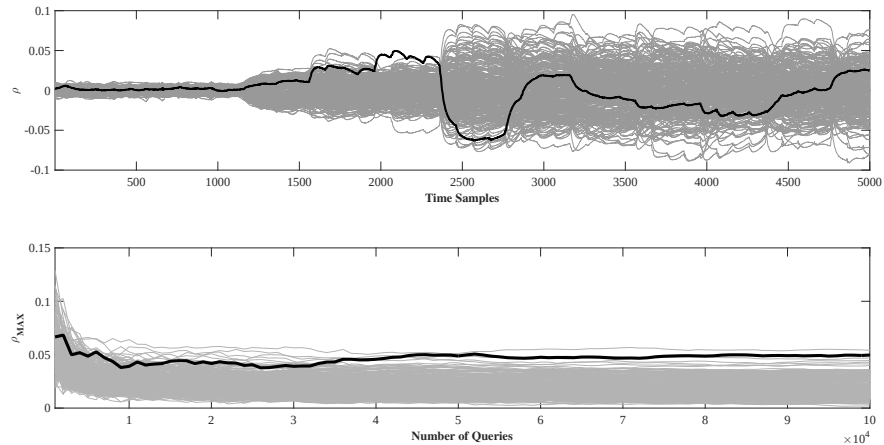


Figure 6.13. Plots of the CPA attack on AES-4 (FPGA implementation). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

of Figure 6.13.

6.3.2 Leakage Assessment on the SERPAES chip of AES-0 and AES-4.

The measurement setup adopted to carry out DPA and CPA attacks on AES-0 and AES-4 is depicted in Figure 6.14. The AES-128 test-chip has been mounted

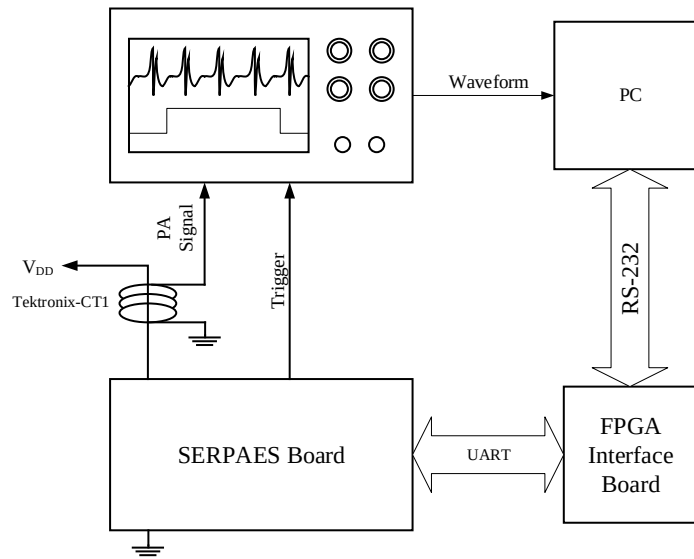


Figure 6.14. Block scheme of the measurement setup for SERPAES chip.

on a printed circuit board, which also contains the support circuitry: a set of bidirectional level shifters, needed for input-output interfacing and some step-down linear regulators. The power regulators provide separate power supplies for the different parts of the chip internal circuitry. The power supply for the AES crypto cores can be provided both via the on-board regulators or an external bench-top power supplier. Several jumpers allow feeding current only to specific parts of the chip and to measure power absorption through removable shunts.

The testchip board is connected to a personal computer via a FPGA board (Altera Cyclone-II), implementing the RS-232 interface and control functions. The interface allows bidirectional communication: the plaintext is sent from the PC to the chip while the ciphertext goes in the reverse direction. The FPGA also provides the *CK* and *SEL* signals for the AES cores and the trigger signal for the oscilloscope. The clock frequency has been set to 10MHz for AES-0 and 20MHz for AES-4 (see Section 6.2.5) in all the experiments. The oscilloscope used to acquire current traces is a LeCroy WaveSurfer MX-104B [88]; it has 1GHz bandwidth and 10GS/s sampling frequency. The current absorbed during the encoding operation is measured through the Tektronix CT-1 inductive probe [140]. The probe is applied to the positive wire of the power supply of the part of the chip under attack. The whole system is managed by a Matlab script, that performs the following tasks, in the same order in which they are mentioned below:

1. plaintext generation, which can be random or preset depending on the type of experiment to be carried out;
2. sending of the plaintext to the chip;
3. traces acquisition from the oscilloscope;

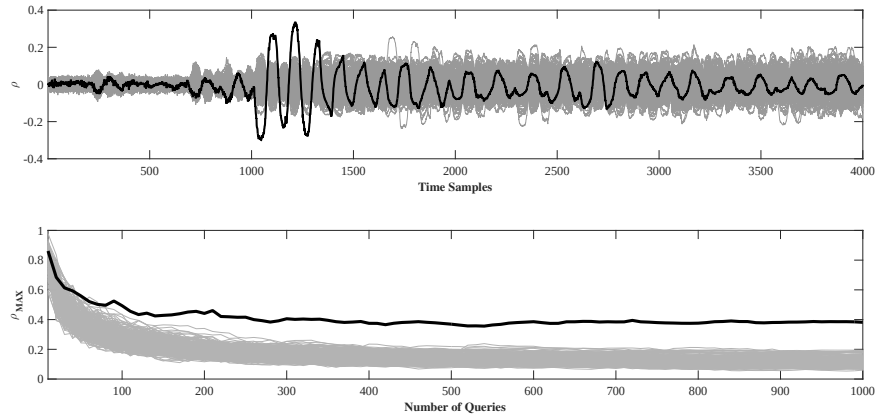


Figure 6.15. Plots of the CPA attack on AES-0 (SERPAES). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

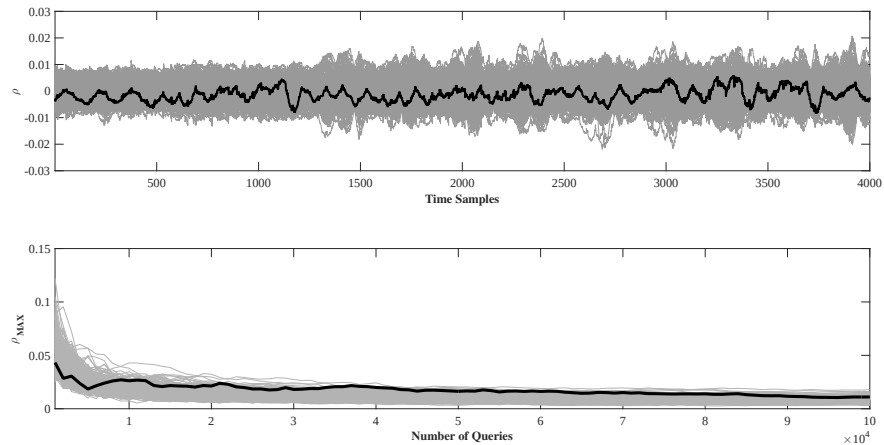


Figure 6.16. Plots of the CPA attack on AES-4 (SERPAES). Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

4. storing of traces as *.mat* files.

After trace acquisition, data processing and the PAAs are performed by means of additional custom Matlab scripts.

To compare the vulnerability to PAAs of AES-0 and AES-4 both CPA and DPA attacks techniques have been used. For each core, 100.000 current traces have been recorded and used to attack all the 16 bytes of the AES-128 key (one by one). Without loss of generality, we present the results obtained for byte 3, which resulted

the easiest to attack for AES-0. When performing CPA attacks, we have chosen the output of the S-BOX at the first round as target operation. With this assumption, the output of the S-BOX (out_{sb}) is a function of the sub-byte of the plaintext and the sub-byte of the secret key at first round:

$$out_{sb} = f(pt_{sb}, key_{sb}) = SBOX(pt_{sb} \oplus key_{sb}) \quad (6.4)$$

Results of the CPA attack on AES-0 are reported in Figure 6.15, showing how AES-0 can be successfully attacked exploiting CPA on byte 3 with only 72 power traces. Under the same conditions, AES-4 cannot be successfully attacked even with 100k measurements. Figure 6.16 shows that the correlation peak corresponding to the correct key is embedded in the “bulk”, proving an MTD of $> 100k$. The correct sub-key’s correlation coefficient is never large enough to make it distinguishable among wrong keys. As it is clear from experimental CPA attacks on the SERPAES testchip, in AES-4 there is a strong reduction of the correlation coefficient for the correct key. In the non-protected AES implementation, the *steady state*’s correlation coefficient value is $\rho_{AES-0} = 0.3816$, whereas for AES-4, using the maximum number of queries, it is about $\rho_{AES-4} = 0.011$.

Starting from these values and using the expression of the correlation coefficient as function of the minimum number of traces needed to recover the secret key reported in [93], i.e. $\rho^2 \propto 1/MTD$, we have estimated that AES-4 has an MTD greater than the MTD of AES-0 of a factor given by [54]:

$$n_{MTD} = \frac{MTD_{AES-4}}{MTD_{AES-0}} \approx \left(\frac{\rho_{AES-0}}{\rho_{AES-4}} \right)^2 = 1203 \quad (6.5)$$

This result is in accordance with the result of the CPA attack on AES-4 using the whole power traces set. By using the same power traces set, a DPA analysis on the two AES-128 cores has been carried out, showing very similar results in terms of vulnerability. In particular, for the sake of completeness, we have performed the DPA attack using each bit of byte 3 as a single-bit power model. For AES-0, the DoM coefficients of the correct key were always easily distinguishable from the ones corresponding to wrong keys. Regarding AES-4, DPA attacks using all the bits of byte 3 as single bit power models were carried out. Even using 100k traces, it was not possible to retrieve the correct key. Figure 4.46 shows the results of the DPA attack assuming the MSB as single bit power model.

As shown in Figure 6.16 and in Figure 6.17, neither conventional nor technology-based CPA and DPA attacks are effective on AES-4. In fact, the correlation coefficients and the DoM coefficients are hidden in the “noise floor” for all the relevant time samples, and it is not possible to retrieve the correct key, even assuming the attacker model proposed in [12].

Figure 6.18 shows the SNR for the AES-0 and AES-4 implementations. The reduction of the SNR is describe in Equation 6.6:

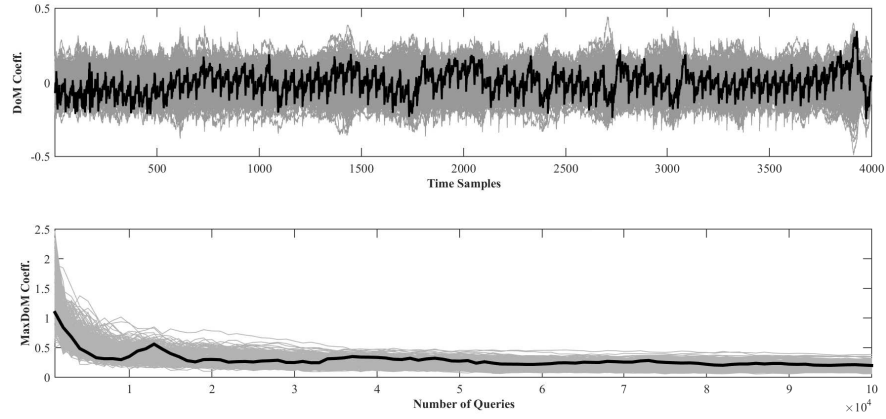


Figure 6.17. Plots of the DPA attack on AES-4 (SERPAES). Top figure shows the difference of mean (DoM) coefficient vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

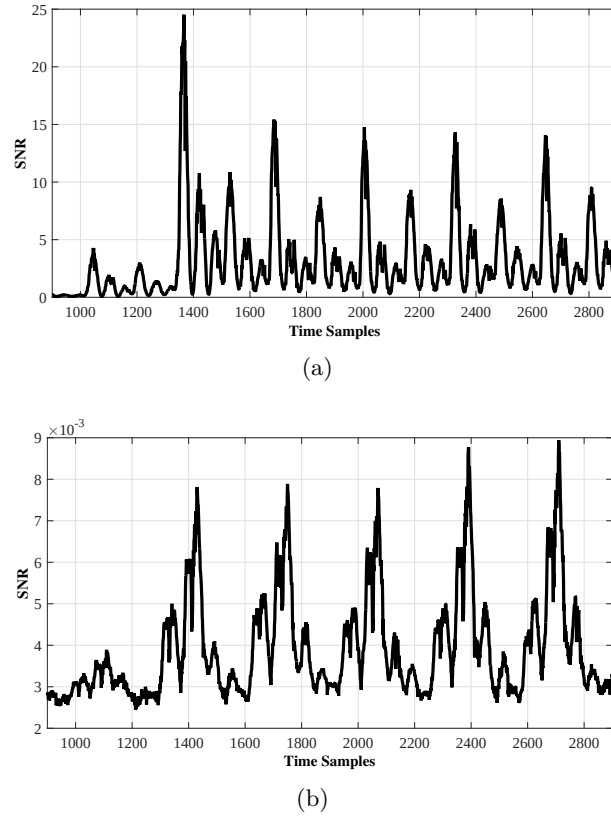


Figure 6.18. SNR curves for AES-0 (top) and AES-4 (bottom) at the first-round.

$$SNR_{ratio} = \frac{SNR_{AES-0}}{SNR_{AES-4}} = \frac{24.52}{0.0078} \approx 3205 \quad (6.6)$$

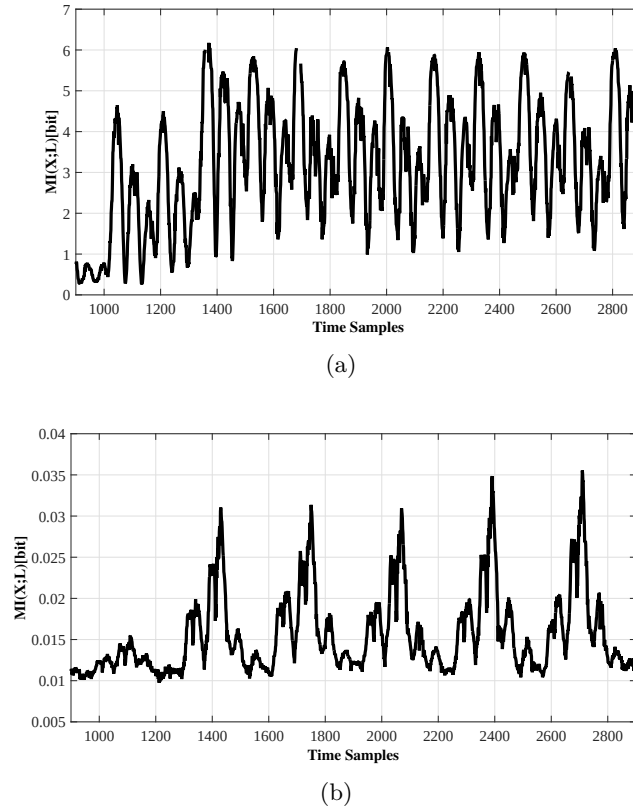
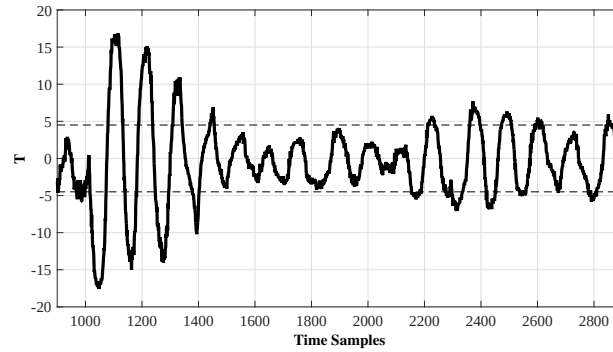


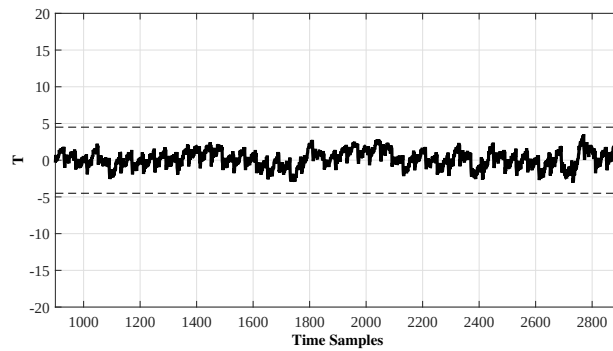
Figure 6.19. Mutual information curves for AES-0 (top) and AES-4 (bottom) at the first round.

The SNR is reduced by a factor of 3205, which is a three orders of magnitude improvement. In AES-4, the presence of the additional randomness introduced by SDRRs instead of regular registers, allows to maximize the contribution of the noise on both storage elements and combinational cells for all operations.

The mutual information curves are shown in Figure 6.19. As in [54], the MI curves are similar to the SNR curves. The reduction of the maximum value is 199, remarking the ability of the protected architecture to reduce the information leakage through dynamic power consumption. Mutual information assumes perfect knowledge of the statistical model of the device, so it represents the upper bound on what an adversary can extract from the chip. The Welch's t -test analysis of the first round, depicted in Figure 6.20, shows that there is a leakage reduction in the AES-4 implementation. As in [131], we have used the threshold value $|t[k]| > 4.5$ to reject the null hypothesis. The t -value does not exceed the threshold and is much lower than in the unprotected AES-0. This countermeasured architecture of the AES-128, which makes use of SDRR element, is effective in reducing the information leakage. A summary of the security metrics for AES-0 and AES-4 is reported in Table 6.2.



(a)



(b)

Figure 6.20. Welch's T-test with power samples from AES-0 (top) and AES-1 (bottom) at the first round.

Table 6.2. Actual and information theoretic security metrics of AES-0 and AES-4 cores on the SERPAES chip.

	SNR	Maximum Value			
		MI[bit]	T-test	ρ_{MAX}	DoM
AES-0	25.52	6.178	-17.600	0.3816	1.22
AES-4	0.0078	0.031	-2.670	0.0110	0.19

6.4 Full-Custom 4-bit SERPENT Crypto-cores

The SERPAES chip can be considered the first implementation of a cryptographic circuit using the iDDPL style, which was proposed by Bongiovanni *et al.* in 2013 [29], using the CMOS065SVTLP process from STMicroelectronics, mentioned at the beginning of this chapter. This section of the chip contains two full-custom designed crypto-cores based on the following logic styles:

- SABL;

Table 6.3. Comparison of performances of SABL and iDDPL 4-bit SERPENT-based crypto-cores.

	# Devices	Area Overhead	Active Area [μm^2]	P_{AV} 10MHz [μW]	$\max f_{CK}$ [MHz]	Throughput
CMOS	564	$\times 1.0$	n.a.	n.a.	n.a.	$\times 1$
SABL	1538	$\times 2.7$	1703	23.3	215	$\approx \times 0.5$
iDDPL	1983	$\times 3.5$	2323	36.1	380(240)	$\approx \times 0.5$

- iDDPL.

For both logic styles, a full-custom library has been designed in our laboratory using Cadence, using a top-down approach. Pre and post simulations have been used to carefully design both implementations and libraries, in order to get a fair comparison between the RTZ and TEL approach with the aforementioned logic styles. SABL and iDDPL libraries have been manually designed in Cadence and post-layout simulations have been used to generate technology files.

The two cores are placed side-by-side in a *macro* block, in the lower right corner of the chip's core area, as shown in Figure 6.1. The two implementations of the 4-bit SERPENT crypto-core share the same ground ring, but they have separated power nets. It has to be reminded that SERPAES is a prototype chip for PAA evaluations of iDDPL style. Hence, it has been designed to provide several *test points* for power analysis. In fact, the iDDPL has six different power nets, while SABL has only two power nets, providing the possibility to monitor power consumption of different sub-block in each implementation. Each power net is accessible from the outside by a specific pin, connected to a 2-pins header for testing. It has to be noticed that the printed circuit board designed for the SERPAES chip is featured with two additional set of headers, acting as main power nets, separately for iDDPL and SABL cores' power nets. This feature has been used to power independently each full-custom core, minimizing coupling effects.

In order to enhance the minimization of coupling effects between the SABL and iDDPL core, the full-custom macro has been designed to run only one core at a time, similarly to standard-cells side of the SERPAES chip. As it can be seen in Figure 6.21, a SEL signal is used to route 4-bit input plaintext and key to only one core at a time through a set of input demultiplexers. An output multiplexer route the 4-bit output ciphertext of the selected core through output pads. In addition, we also have two distinct input pads for clock signals. In the iDDPL implementation, a delayed replica of the clock signal needs to be generated on-chip, in order to guarantee a certain duration of the evaluation phase t_{eval} . The starved inverter in Figure 4.22 and presented in [27] has been used to as delay element in this design. The control voltage V_{bias} , provided externally, sets the delay to the desired value.

In this section, a security evaluation of SERPENT-based cores in SABL and iDDPL styles are discussed by means of PAAs. Further details on the design of the custom cores are reported in [28].

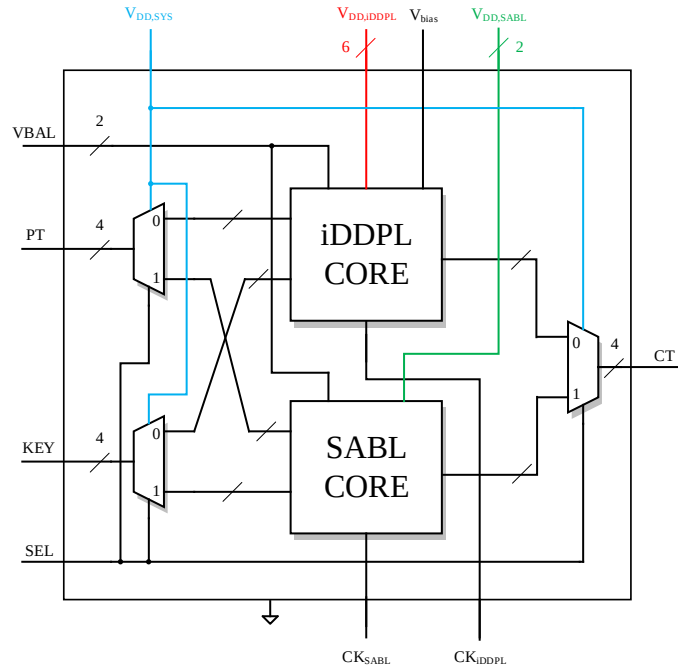


Figure 6.21. Architecture of the full-custom section of the SERPAES chip, containing two implementations of a 4-bit SERPENT-based crypto-core.

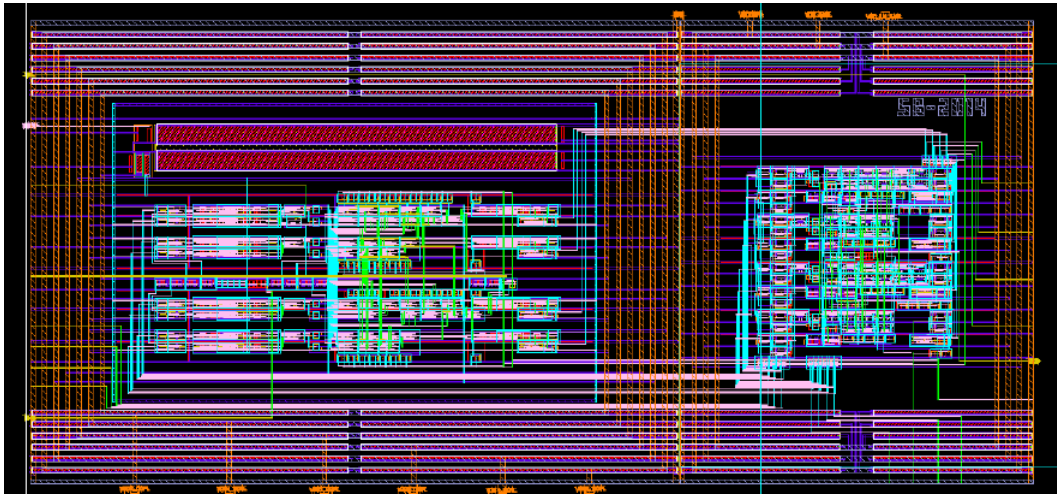


Figure 6.22. Layout of the SERPENT macro. The section on the left is the iDDPL implementation, while the one on the right is the SABL implementation.

6.4.1 Data-path of 4-bit SERPENT Crypto-Cores

Both cores share the same 4-bit architecture, implementing round-0 of the SERPENT block cipher. The block scheme of the 4-bit SERPENT-based crypto-core is depicted in Figure 6.23. The conversion of input data from CMOS to the respective

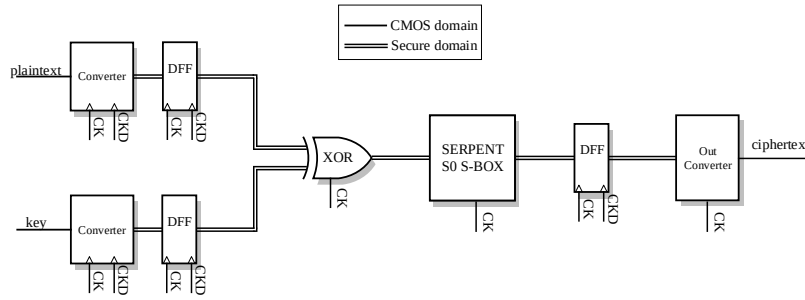


Figure 6.23. Block scheme of the 4-bit SERPENT-based crypto-cores in the SERPAES chip. The signal CKD is used only on the iDDPL core.

secure domain is performed by CMOS-to-RTZ and CMOS-to-TEL input converter respectively. The secure domain is composed by 2 pipelined stages. The first one performs bitwise XOR operation between the 4-bit input plaintext and the 4-bit key. The second stage implements the non-linear S-BOX S_0 function of the SERPENT algorithm (see Appendix A.3). The complete encryption requires 4 clock cycles to generate the correct ciphertext. A in-depth description of the design of the SABL and iDDPL 4-bit SERPENT-based crypto-cores is reported in [28].

6.4.2 Capacitive Mismatch Analysis

In Chapter 4, we have discussed on the impact that the capacitive mismatch has on the security level of a cryptographic devices protected with PAA-resilient DPLs. The TEL protocol adopted in the D³L implementation has been found to be effective in tolerating the presence of capacitive mismatch on different testbenches (FPGA and pre-layout simulation with 40nm CMOS process) if compared to RTZ-based DPLs. The full-custom section of the SERPAES prototype chip has been designed to minimize the capacitive mismatch, thanks to ad hoc routing. Nevertheless, a custom programmable load cell has been designed to emulate the presence of capacitive mismatch. The cell, shown in Figure 6.24, is composed by two capacitors activated by two n-MOS switches independently. The additive capacitance C_{add} is programmed with the 2-bit word $VSEL$, providing 4 different values:

- $VSEL = 00$, $C_{add} = 0fF$;
- $VSEL = 01$, $C_{add} = 3.2fF$;
- $VSEL = 10$, $C_{add} = 6.4fF$;
- $VSEL = 11$, $C_{add} = 9.6fF$.

Both cores have been designed including a programmable load cell connected at the *false* output of each combinational gate and sequential element in SABL

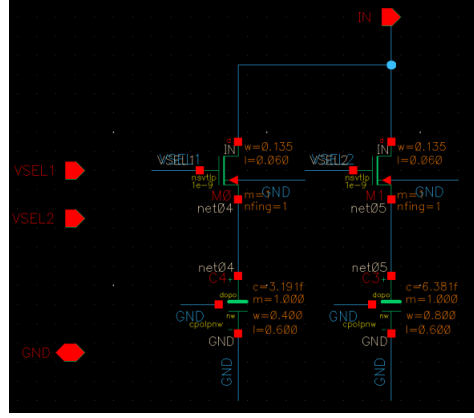


Figure 6.24. Programmable output load in SERPAES chip.

and iDDPL SERPENT-based crypto-cores. The 2-bit word $VSEL$ for capacitive mismatch selection is provided by external interface through dedicated input pins. We can redefine the real mismatch factor in these implementations taking into account the presence of C_{add} :

$$MF' = \frac{\max(C'_{true}, C'_{false})}{\min(C_{true}, C_{false})} = \frac{\max(C_{true}, C_{false}) + C_{add}}{\min(C_{true}, C_{false})} = MF + \frac{C_{add}}{\min(C_{true}, C_{false})} \quad (6.7)$$

6.5 Power Analysis Attacks on SERPENT-based Crypto-cores

The full-custom section of the prototype SERPAES chip has been intensively studied and analyzed through a measurement campaign. The PA conducted on SERPENT crypto-cores has been focused on the dynamic power consumption exploitability. The same measurement setup discussed for the AES side of the chip has been used to carry out the information leakage analysis. Minor changes in the measurement setup are due to the simpler interface between the control FPGA and the device under attack.

The core voltage has been set to 1.2V, according to foundry specifications for nominal voltage of the 65nm design-kit. We have set the external V_{bias} to 0.8V, which is the minimum value that guarantees the correct encryption on the iDDPL core. It corresponds internally to a t_{eval} equal to $\approx 1ns$ [28]. Both cores have been tested with a running frequency of 1MHz, using the LeCroy WaveSurfer MX-104B DSO with a sampling rate of 5GS/s and full analog-bandwidth (1GHz). Also in this case, we have used the Tektronix-CT1 inductive probe to sense the current absorption on main core power supply headers.

In order to mitigate coupling effects within crypto-cores, the main power supply pin of the unused one has been tied to ground. Coupling effects of adjacent cores are almost unavoidable if they are placed back-to-back on the same die, whereas a minimization of their magnitude is needed to improve the quality of measurements.

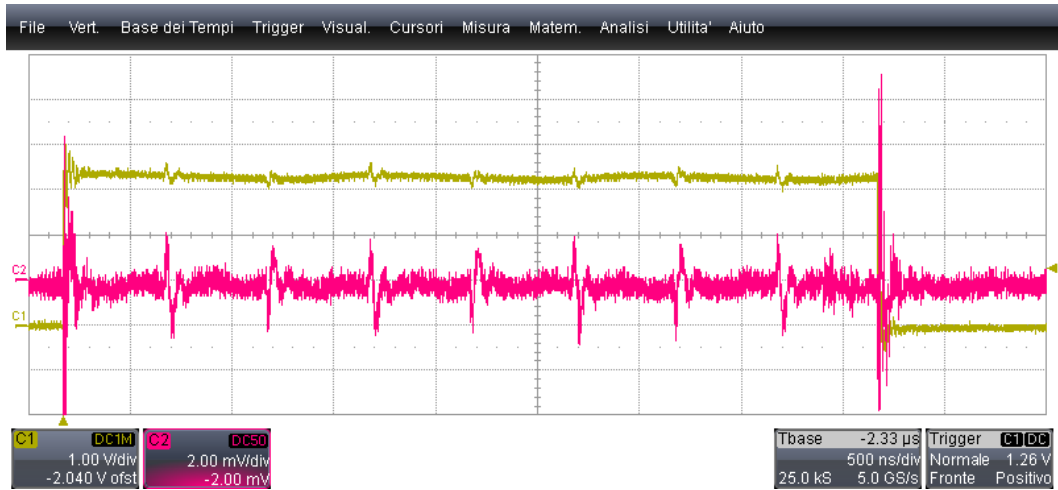
Power traces of the SABL and iDDPL crypto-cores are shown in Figure 6.25. It has to be noted that power trace collected on the SABL implementation appears more smooth than the respective iDDPL counterpart. In iDDPL implementation, the power trace appears more "ringing", with a pseudo-period of $\approx 50ns$, as can be clearly seen in Figure 6.25(b). Higher frequency effects are expected in TEL-compatible implementations, since the evaluation phase has a very short duration compared to the clock period. In the D³L FPGA implementation in Chapter 4, the presence of a huge parasitic capacitance between the supply rails may cut off resonant mode, and power traces appear smoothed. In this case, we have very low on-chip capacitance, since the prototype iDDPL (as SABL) SERPENT-based crypto-core is implemented on a small and isolated hard-macro inside the chip.

As previously mentioned, SABL and iDDPL implementations have been designed with multiple power supply pins, to provide access also to power consumption of different sub-blocks in the design. We have chosen to monitor only the power consumption of $SBOX + DFF_{OUT}$ combo. Therefore, the 4-bit output word of the S-BOX S_0 has been used as target intermediate function. This choice is justified by the fact that the S-BOX sub-block contains a large number of combinational gates. Addressing the S-BOX's output as target function provides us useful informations about the behavior of the SABL and iDDPL in the presence of capacitive mismatch. Moreover, excluding non-targeted sub-blocks, we can reduce the influence of switching noise, improving the quality of collected power traces. We want to remark that, according to Figure 6.23 and Figure 6.26, the S-BOX elaboration takes place during the second cycle of the encryption operation, and the 4-bit ciphertext is forwarded to the output at the third cycle.

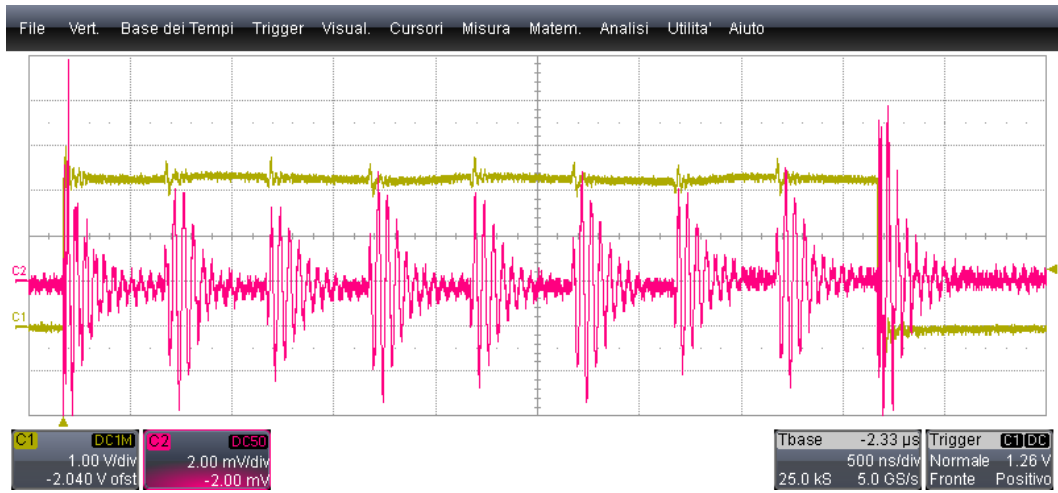
The investigation of the resistance to power analysis have been conducted repeating CPA (adopting HW power model) and DPA attacks with different level of capacitive mismatch between *true* and *false* output of each gate with the two implementations, according to Section 6.4.2. It has to be noted that the iDDPL implementation is the first full-custom designed TEL-compatible circuit to be tested on a real chip. Since TEL encoding has been proposed to overcome security issues due to capacitive mismatch, it is needed to characterize its behavior from no mismatch condition ($C_{add} = 0F$) to maximum mismatch ($C_{add} = 9.6fF$).

6.5.1 Evaluation of Security Metrics

In this section, an evaluation of the security metrics on both cores with different mismatch conditions. It has to be noted that, if $VBAL = 00$, a residual of mismatch is still present on both cores, due to non perfectly symmetric routing, which is reported to be under 1.5 for the S-BOX, and under 2.20 for the output register for



(a)



(b)

Figure 6.25. Current traces of the SABL (a) and iDDPL (b) 4-bit SERPENT-based crypto-cores collected on the respective main voltage supply pin, running at 1MHz, with 1.2V of core voltage. Yellow traces represent the trigger signal, while pink traces are current traces, measured with the Tektronix-CT1 inductive probe.

both implementations [28].

Results of SNR and mutual information with the four possible *VBAL* configurations on both cores are shown in Figure 6.27. Regarding SNR values, the iDDPL implementation exhibits a positive monotonic behavior increasing C_{add} , moving from 5.43 to 12.51, as expected. In SABL implementation, SNR peak values are always higher than iDDPL counterpart, in accordance with experimental results we have found for RTZ vs TEL FPGA implementation in Chapter 4. With $VBAL = 00$, the SNR is 50.41 for the SABL implementation, which is ten times higher respect to iDDPL (5.41). It is worth noting that a minimum of SNR value can be observed at $VBAL = 10$, that corresponds to $C_{add} = 6.4fF$. A possible explanation for

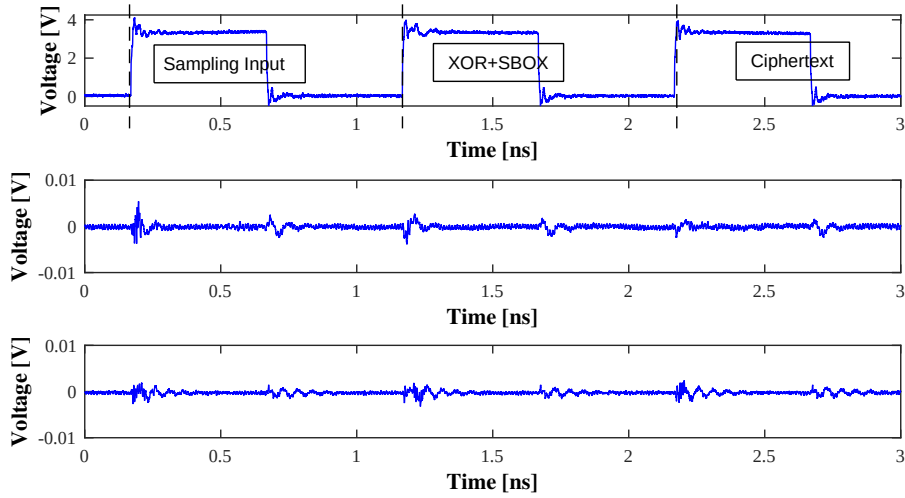


Figure 6.26. Time diagram of the encryption in SABL/iDDPL cores: clock signal (top), SABL current absorption (middle), iDDPL current absorption (bottom).

the presence of a minimum is reasonably due to a higher residual mismatch in SABL implementation compared to iDDPL. The presence of a certain value of C_{add} (reasonably between 5fF and 7fF) can help to provide balancing in capacitive loads on SABL implementation, and thus helping in reducing information leakage through dynamic power consumption. However, for all settings of V_{BAL} , SABL implementation exhibits higher values of SNR peaks, remarking the relevance of capacitive mismatch in determining the level of security for DPLs adopting RTZ signaling. Similarly to SNR, peak values of mutual information assume higher values in SABL implementation. If $V_{BAL} = 00$, the estimated mutual information for SABL core is 3.82bit, while for the iDDPL is 2.92bit. The spread between the two implementations of the 4-bit SERPENT-based crypto-core remains higher, but, also in this case, a minimum of SABL's mutual information value can be found at $V_{BAL} = 10$. At this value, the mutual information of the $S - BOX + DFF_{OUT}$ is practically the same.

The analysis of SNR and mutual information is reasonably in accordance with experimental findings in Chapter 4. The iDDPL, adopting TEL signaling, exhibits lower information leakage compared to RTZ-based SABL. Moreover, different mismatches does not impact severely on the information leaked by the iDDPL core. In the SABL implementation, the presence of a local minimum value for SNR and estimated mutual information remarks how the improvement in security of this logic style is sensible to capacitive mismatch.

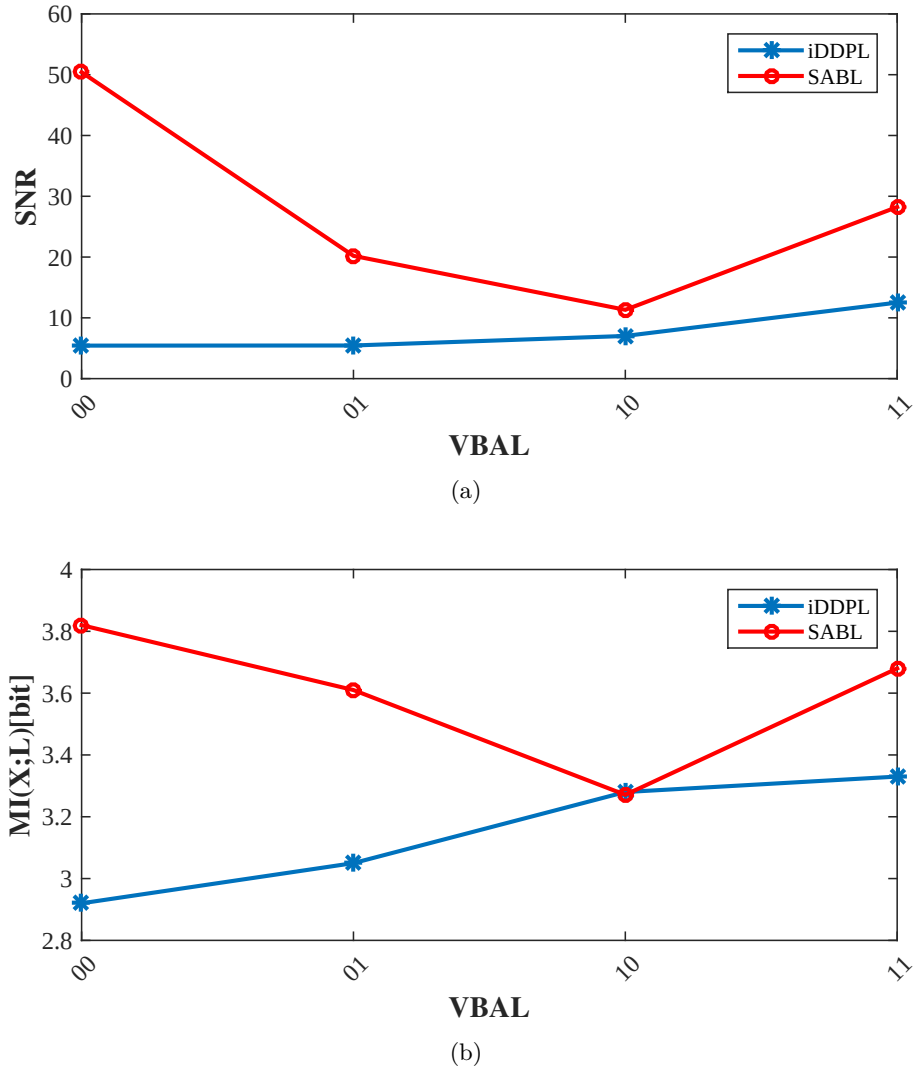


Figure 6.27. Peak values of SNR (a) and mutual information (b) regarding *VBAL* configurations.

6.5.2 CPA Attacks on SERPENT-based Crypto-Cores

Both cores have been attacked using CPA attacks adopting HW power model. Results of CPA attacks on SABL and iDDPL cores with all possible configurations of *VBAL* are shown in Figure 6.28. The iDDPL implementation exhibited an extreme resistance to multi-bit attack, and in all mismatch cases, it was not possible to recover the secret key. In fact, the MTD is always higher than 50k. Despite high values of correct key's correlation coefficient, the value of $SVI_{\%}$ tends to increase with C_{add} , remarking that the correct key tends to be hidden in the "bulk" even in the presence of mismatch. Regarding the SABL implementation, the CPA is not effective in recovering the correct key only with $VBAL = 10$, according to SNR and mutual information analysis mentioned previously. For all the remaining

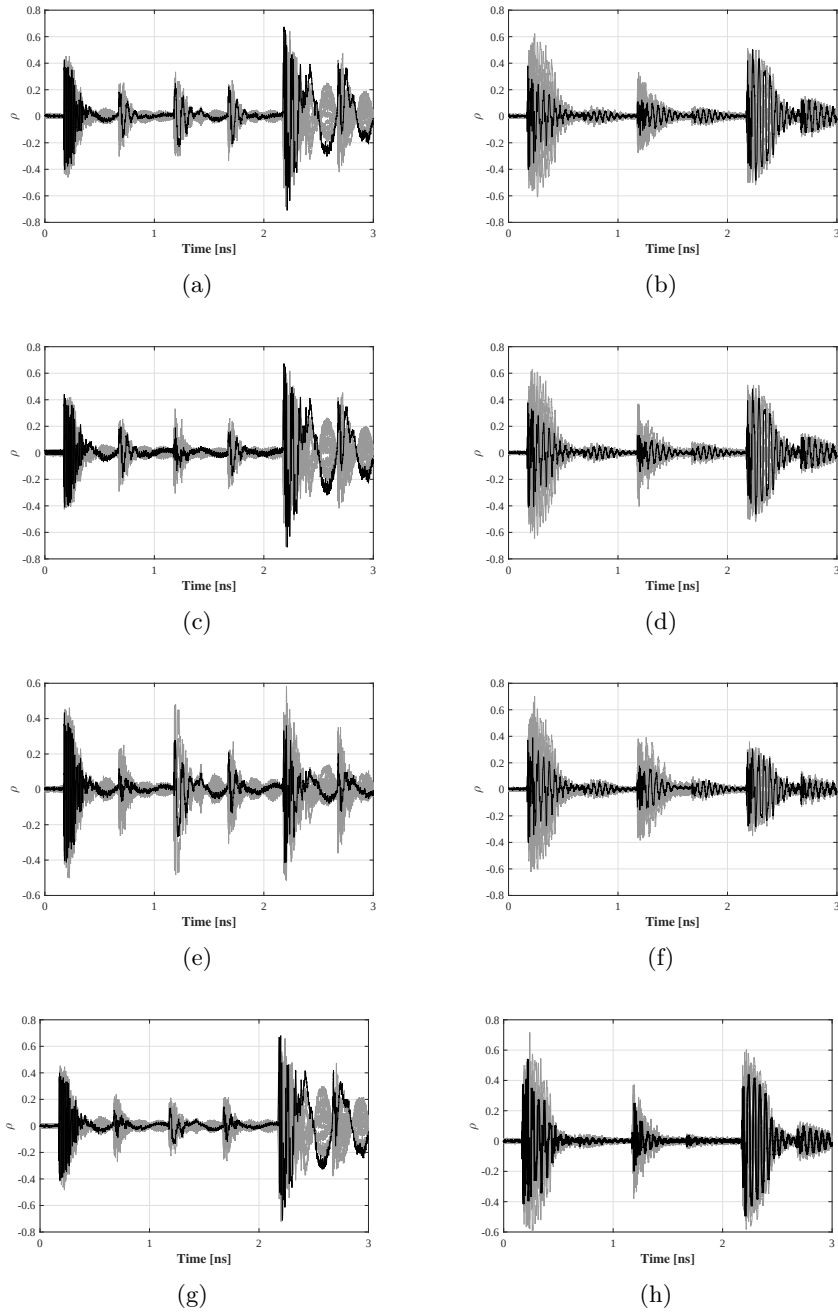


Figure 6.28. Plots of correlation coefficients for SABL (left column) and iDDPL (right column) implementations with $C_{add} = 0fF$ (a)-(b), $C_{add} = 3.2fF$ (c)-(d), $C_{add} = 6.4fF$ (e)-(f), $C_{add} = 9.6fF$ (g)-(h). Black lines correspond to the correct key's correlation coefficients. Grey lines are referred to wrong keys' correlation coefficients.

configurations of *VBAL*, the CPA is able to recover the secret key with a very small number of traces (from 40 to 670). MTD diagrams of CPA attacks are shown in Figure 6.29 and a summary of results are reported in Table 6.4.

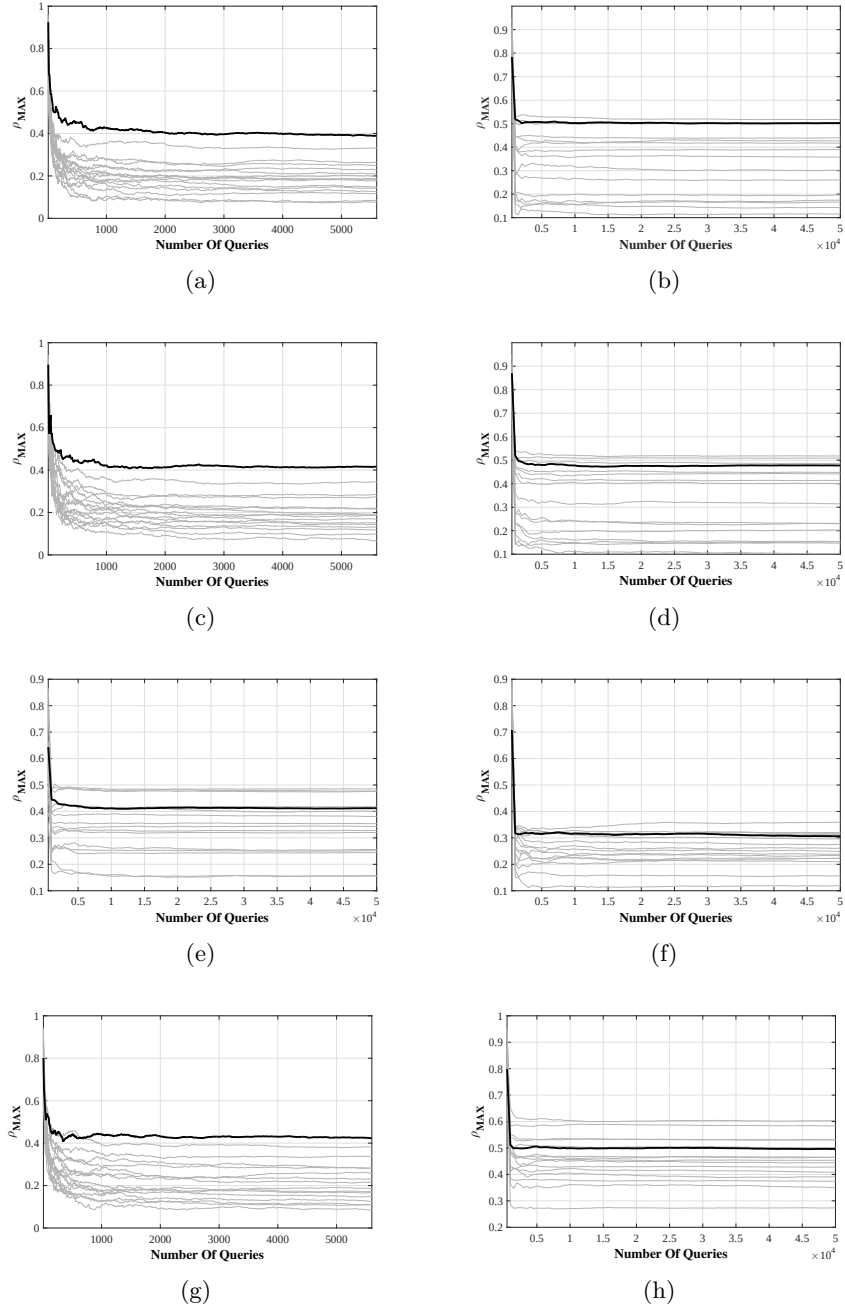


Figure 6.29. MTD diagrams for SABL (left column) and iDDPL (right column) implementations with $C_{add} = 0fF$ (a)-(b), $C_{add} = 3.2fF$ (c)-(d), $C_{add} = 6.4fF$ (e)-(f), $C_{add} = 9.6fF$ (g)-(h). Black lines correspond to the correct key's correlation coefficients. Grey lines are referred to wrong keys' correlation coefficients.

Table 6.4. CPA attacks results on iDDPL and SABL implementations of 4-bit SERPENT-based data-path.

	C_{add}	ρ_{MAX}	SVI	SVI%	MTD
iDDPL	$0fF$	0.5028	-0.0154	-2.97%	> 50k
	$3.2fF$	0.4775	-0.0406	-7.84%	> 50k
	$6.4fF$	0.3063	-0.0524	-14.6%	> 50k
	$9.6fF$	0.4959	-0.1078	-17.88%	> 50k
SABL	$0fF$	0.3889	+0.057	+14.66%	40
	$3.2fF$	0.4149	+0.0707	+17.04%	130
	$6.4fF$	0.1131	-0.0891	-78.78%	> 50k
	$9.6fF$	0.4229	+0.0402	+9.51%	670

6.5.3 DPA Attacks on SERPENT-based Crypto-Cores

In addition to CPA, we have also performed single-bit attacks using the classical DPA procedure. In this section, only results regarding the value of most significant bit (MSB) as single-bit power model are presented, since it gives most representative informations about the PAA-resilience of SABL and iDDPL implementations in SERPAES prototype chip.

Using the same data-set of CPA attacks in previous section, both SABL and iDDPL implementation have been attacked adopting the DPA procedure. Results of DPA attacks are shown in Figure 6.30. It has to be mentioned that difference of means plots targeting the MSB of the S-BOX' output word in both implementations provide results quiet similar to classic output results of CPA/DPA attacks using XOR. In fact, we have obtained symmetric curves for each $(key, \overline{key})$, as it can be generically found adopting the output word of the XOR as target intermediate result. For the iDDPL implementation, the attack ended unsuccessfully for $C_{add} = 0fF$ and $C_{add} = 3.2fF$. Increasing the mismatch, it has been possible to recover the secret key for $C_{add} = 6.4fF$ and $C_{add} = 9.6fF$, with a MTD value of ≈ 30 power measurements. Regarding the SABL implementation of the SERPENT crypto-core, DPA attacks show almost the same behavior of CPA. In fact, it has been possible to recover clearly the secret key for all values of C_{add} , with MTD values between 20 and 40 power measurements, expect $C_{add} = 6.4fF$, corresponding to $VBAL = 10$. As previously discussed, SABL implementation exhibits a minimum of SNR and mutual information at $VBAL = 10$, and also the CPA attack did not succeed in recovering the key with this configuration. Further considerations about the behavior the information leaked during the encryption can be given looking at Figure 6.30. It has been noted that in iDDPL, maximum values of DoM coefficients can be found only during the rising edge of the clock at the beginning of the third cycle ([2ns, 2.5ns]), remarking that a critical point leaking information is due to the output register and not from the combinational gates of the S-BOX. In addition, falling edges on the second and third clock cycles do not provide relevant informations. In SABL implementation, not negligible leakage can be observed during the falling edge of

the third cycle ([2.5ns,3ns]).

6.6 Conclusions

In this chapter, security evaluations and tests on the 65nm SERPAES prototype chip have been presented. The prototype chip has been designed at our laboratory and fabricated by STMicroelectronics that provides us also the CMOS065SVTLP design-kit. The chip contains five implementations of the popular AES-128 block cipher and two full-custom designed cores based on the SERPENT algorithm. AES-128 implementations have been designed using only standard-cells, and the synthesis has been led with the help of VHDL codes. Four implementations have been designed with RTL-level countermeasures, aiming to break the physical link between power consumption and processed data through randomization, plus an unprotected version of core has been placed for reference. In this context, the Secure Double Rate Register (SDRR), implemented in AES-4 core, have been in-depth analyzed through PAAs, using actual and information theoretic security metrics in addition to CPA and DPA attack procedures. We have found that the AES-128 architecture where each register has been substituted by a SDRR unit is able to resist to PAAs, improving (at least) of three orders of magnitude the number of measurements needed to break the unprotected implementation. Regarding the full-custom cores, they have been conceived to fairly compare state-of-the-art of full-custom designed DPLs: SABL and iDDPL. The latter one makes use of TEL principle for differential signaling. The TEL encoding scheme has been proposed to overcome issues due to capacitive mismatch in modern CMOS processes, due to non-perfectly symmetric routing. In fact, the comparison "SABL vs. iDDPL" can be seen also under the perspective of "RTZ vs. TEL" encoding, since RTZ has been found to be inadequate in presence of capacitive mismatch. Results concerning PAAs procedure and information leakage evaluation have confirmed that TEL-based iDDPL implementation is able to tolerate multi-bit attacks also in presence of extreme unbalancing in capacitive loads. Also adopting a single-bit power model, the SABL has been found very sensitive to unbalance.

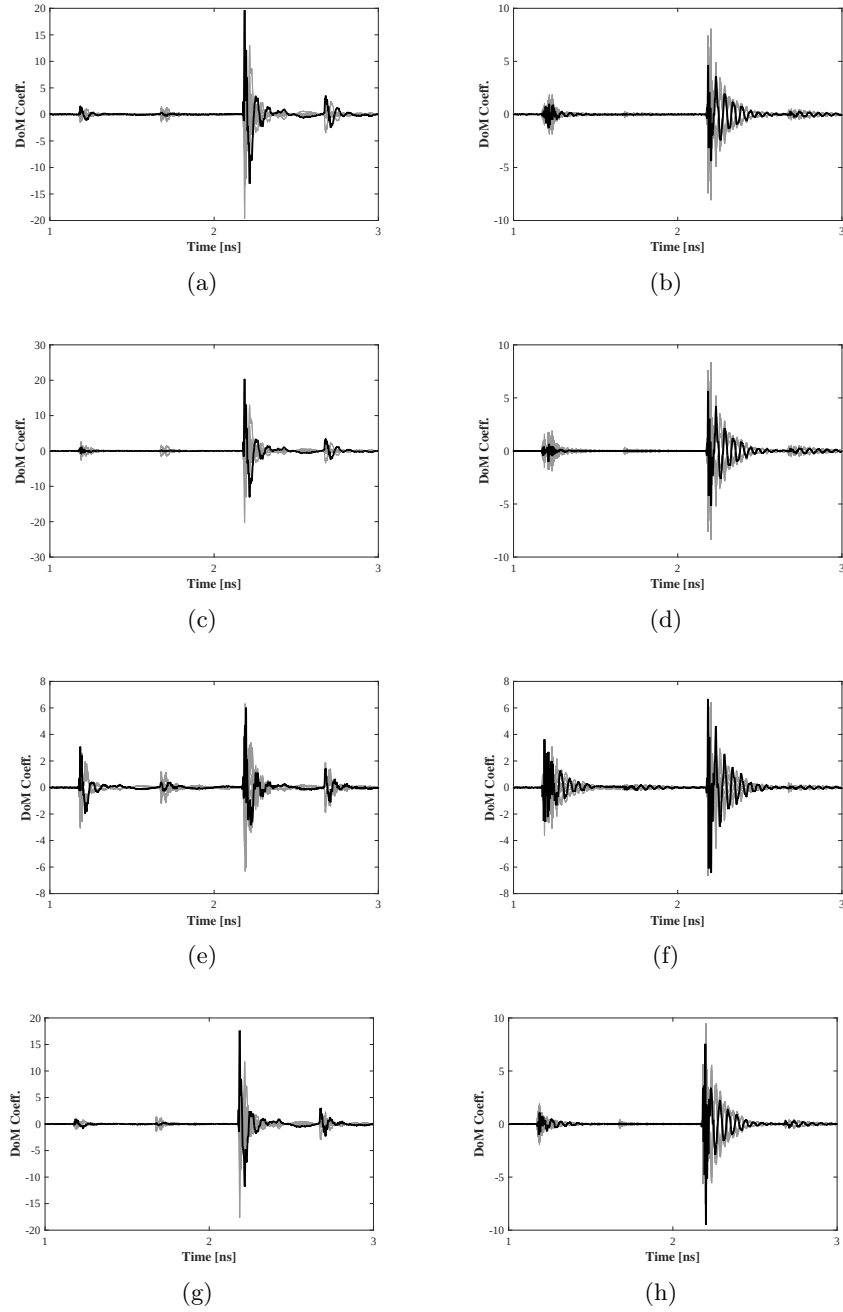


Figure 6.30. Plots of difference of means for SABL (left column) and iDDPL (right column) implementations with $C_{add} = 0fF$ (a)-(b), $C_{add} = 3.2fF$ (c)-(d), $C_{add} = 6.4fF$ (e)-(f), $C_{add} = 9.6fF$ (g)-(h). Black lines correspond to the correct key's DoM coefficient. Grey lines are referred to wrong keys' DoM coefficient.

Chapter 7

Conclusions and Future Developments

7.1 Summary of the Research Contributions

In this thesis, several topics in the context of Power Analysis Attacks have been studied and discussed. The onset of new technologies and the arise of nanometer CMOS processes have highlighted new issues in terms of physical security. The analysis of security issues of cryptographic circuits manufactured with nanometer CMOS processes has been the focus of this thesis work, where the power consumption is used as source of information leakage. Moreover, a great effort has been made in defining new countermeasures and design methodologies against PAAs, also under the new perspective of exploiting static power. The research contributions are summarized as follows:

- Study and analysis of information leakage in static power consumption of cryptographic circuits in deep sub-micron technologies, as novel frontier of physical observable security. The formalization of Attack Exploiting Static Power (AESP) as two-fold procedure, to attack and evaluate robustness of cryptographic circuits against parasitic leakage currents exploitation, have provided a methodology to assess security issues arisen with deep scaled processes.
- Analysis of security issues of Dual-rail Pre-charge Logic (DPL) styles, commonly adopted to counteract Power Analysis Attacks exploiting dynamic power, under the perspective of using the static power consumption as source of information leakage. AESP analysis, adopting actual and information theoretic security metrics, have highlighted that such gate-level countermeasures conceived to avoid any steal of information from power consumption are still vulnerable if static power is adopted as side-channel. It has been found that many CMOS-based DPLs do not offer any protection if the adversary takes advantage of

data-dependency in parasitic static consumption.

- Analysis of the temperature-dependency of the information leaked through static power consumption, based on the physical phenomena of parasitic static currents in CMOS technology. Each contribution to static power consumption in CMOS technology has an exponential (or quasi-exponential) relation with temperature. If the working temperature of a cryptographic device changes, also the information that an adversary could extract may change. Analysis with AESP procedure conducted on simulated cryptographic implementations (using 40nm design kit provided by STMicroelectronics) at different working temperatures have highlighted that the adversary could tolerate higher noise power if the temperature on the device under attack is increased to extract the same amount of information. Also simulated AESP attacks have validated this results. In fact, the MTD of univariate AESP attacks decreases if the working temperature of the device is increased.
- A novel multivariate approach in exploiting static power has been developed, based on temperature-dependency of parasitic leakage currents in CMOS technology. Analysis conducted on Monte Carlo generated circuit samples of a 4-bit PRESENT-based crypto-core have shown that the average outcome of perceived information's peaks adopting multiple temperature-points is increased by +44% respect to univariate best-case. On a randomly picked sample from the Monte Carlo's pool (namely chip no.46), the multivariate analysis with two temperature points has been able to double the perceived information with the same noise standard deviation, respect to the univariate best-case, remarking a strong increase in probability to get a successful attack within the same scenario.
- A novel attack procedure has been developed, in order to extend profiling attacks with the exploitation of static power consumption: *Template Attack Exploiting Static Power* (TAESP). Unlike classical Template Attack, TAESP makes use of static power samples to mount the attack, and it can be considered intrinsically a univariate attack procedure. Moreover, we have also proposed to extend the univariate TAESP attack to a multivariate approach, adopting the working temperature as additional domain. The TAESP attack procedure has been tested successfully on 100 Monte Carlo generated circuit samples of the 4-bit PRESENT crypto-cores, and the multivariate approach in the range $[20^{\circ}C; 60^{\circ}C]$ exhibited best results in terms of MTD.
- Design of a novel measurement setup to perform AESP/LPA and vulnerability analysis using static power as side-channel. The use of not expansive and dedicated instrument to measure DC current instead of DSOs, helps to maximizes the SNR. In order to minimize the effect of temperature on static current, we designed a controlled heater system using only off-the-shelf components and a commercial Peltier Cell as heater. The system is able to fine control the working temperature of the device under attack, allowing to set precisely the working temperature of the device under attack. To verify the effectiveness of the measurement setup, a 4x4 crypto-core based on PRESENT-80 has been

implemented on a Xilinx Spartan-6 FPGA. AESP has been performed to evaluate the MTD of the implementation at 65°C. It has been found that 547 static current samples are sufficient to recover the correct key with the novel measurement setup.

- Design of a novel gate-level PAA-countermeasure, named *Delay-based Dynamic Differential Logic* (DDDL or D³L), adoptable in a standard digital design-flow, and based on the *Time Enclosed Logic* principle for differential signaling. The new logic style is completely implementable with standard-cells, since it does not need any custom design digital primitive. The aim of this new logic is to provide an easy-to-use DPL which is capable of counteracting PAAs also in the presence of capacitive mismatch, that is a major concern in the context of DPLs as gate-level PAA-countermeasures.
- Design and analysis of a D³L library using a 40nm CMOS design-kit provided by STMicroelectronics. The combinational cells have been implemented adopting a NAND-approach for each 2-input Boolean operands. Moreover, also the sequential element, which is a TEL-compatible D-type flip-flop, has been designed using the same design-kit, adopting a Master-Slave architecture, with RTZ/TEL/RTZ interfacing. Combinational cells and flip-flop have been characterized in order to evaluate their robustness against PAAs, adopting physical security metrics as NED, NSD and standard deviation of the data-dependent consumption, even in the presence of unbalanced load capacitance. Same building blocks have been designed in other standard-cells based DPLs (WDDL, MDPL and CMOS, used as base reference), in order to compare performance with literature. The D³L allows to improve all main figures of merits compared to reference cases. Also recently proposed frequency-domain security metrics have been evaluated on the D³L library, since the TEL encoding has a direct impact on the frequency spectrum of the information leaked through dynamic consumption.
- Design and comparison of 4x4 PRESENT-based crypto-cores, implemented with D³L and WDDL styles in Cadence Virtuoso. Both cores have been compared under the same working condition. The physical security evaluation has been performed adopting the modeling of different attack capabilities. Since D³L requires demanding constraints on a minimum sampling rate and bandwidth that the adversary should have theoretically to mount an attack, three realistic situations have been taken into account: 10GS/s, 1GS/s and 500MS/s. Simulated CPA attacks, considering the presence of additive Gaussian noise on simulated power traces, have been performed on D³L and WDDL crypto-cores in given attack scenarios. It has been found that even with a low-grade Digital Storage Oscilloscope (DSO) (500MS/s), unbalanced WDDL implementation can be attacked successfully, while the D³L implementation needs a superior attack capability to be broken. In addition, shorter is the duration of the evaluation phase in D³L, higher is the minimum sampling rate and bandwidth needed to mount the attack.
- Design of a D³L VHDL library, that can be easily adapted to FPGA and

ASIC applications. The VHDL library has been used to synthesize all D³L primitives in two different FPGAs from different vendors: Xilinx Spartan-6 (45nm technology) and Altera Cyclone-IV (65nm technology). In addition, also WDDL and MDPL VHDL libraries have been written, in order to fairly compare the D³L other popular gate-level solutions to protect cryptographic circuits on FPGAs. The D³L VHDL library has been used to design the 4x4 PRESENT crypto-core for the Altera Cyclone-IV without routing constraints. CMOS, WDDL and MDPL implementations have been also designed, using their respective VHDL libraries and adopting the same design-flow used for the D³L implementation.

- Test and attacks of various implementation (D³L, WDDL, MDPL and CMOS) of 4x4 PRESENT-based crypto-cores on the Altera Cyclone-IV FPGA, exploiting dynamic power (CPA with HW power model). We have found that the D³L implementation has been able to resist to CPA attacks, with 120k power traces. Experiments carried on other implementations have highlighted that also in a real attack, the TEL principle, embodied within D³L, is able to tolerate capacitive mismatch (due to unconstrained routing), remarking that the RTZ signaling is not suitable to design secure implementations with a standard design-flow. Also SNR and mutual information analysis on collected power traces have confirmed that D³L, enforced with TEL signaling, is able to reduce the information leaked through dynamic power adopting a standard digital design flow.
- Test and attacks of various implementation (D³L, WDDL, MDPL and CMOS) of 4x4 PRESENT-based crypto-cores on the Altera Cyclone-IV FPGA, adopting AESP procedure. The evaluation of the information leaked through static power consumption has shown that the D³L exhibits lower mutual information and SNR compared to other considered DPLs. This is the first time that a TEL-compatible logic is tested against static power exploitation, and experimental results confirm that TEL is able to reduce also data-dependency in static current absorption. In fact, AESP attacks on PRESENT-based crypto-cores have shown that also in this case, it is not possible to recover the secret key exploiting the D³L implementation, since its MTD has been found higher than the collected static samples.
- Development and design of a novel analog-approach countermeasure against PAAs, based on a feedback-loop architecture. The *On-chip Current Equalizer* (OCE) takes advantage of a current-mode approach to obtain a constant power consumption that is independent from processing data. The OCE circuit senses the current drawn by a cryptographic circuit, and compares it with a properly sized pulsed current reference. The error signal, converted through a voltage signal, is used to drive a transconductance amplifier. The latter shunts an extra current, zeroing the error signal, and providing constant current consumption. The OCE has been tested on a PRESENT-based crypto-circuit on Cadence Virtuoso. Simulated attacks have been performed, adding Gaussian white noise in Matlab. The OCE is able to protect a CMOS implementation avoiding the possibility to recover the secret key. The protection ability is traded-off

with not negligible area/power overhead.

- Design and development of an improved version of the OCE, called iOCE. This improved version makes use of a Flipped Voltage Follower (FVF) current mirror as current sensing cell, which acts also as a very low impedance buffer to provide power supply to the cryptographic circuit. The comparison with a pulsed current is done differently respect to the aforementioned OCE, since it is done by a current subtractor circuit. The error current is firstly amplified, by means of a properly sized current mirror. After that, it is converted to a voltage signal through the high-impedance offered by a cascode stage. Also in this case, the voltage signal, representing the error between the current drawn by the logic (that is data-dependent) is used to drive a transconductance amplifier. The transconductance amplifier shunts an extra current that is needed to suppress the error signal, to make the overall power consumption data-independent. The feedback loop architecture of the OCE has been designed to consider the data-dependent current drawn by the logic as a disturbance to suppress. The iOCE has been tested on the 4x4 PRESENT crypto-core and on a complete implementation of the PRESENT-80 in Cadence Virtuoso, simulating real attack experiments. The iOCE has been able to protect aforementioned cryptographic circuits, since PAAs has not succeed with maximum storage capabilities with given scenarios. Compared to the OCE circuit, the area and power overhead required by iOCE protection circuit is negligible, since it requires a +0.4% of area and +7% of power respect the full implementation of the PRESENT-80.
- Security evaluations and experimental activities on the 65nm SERPAES prototype chip. The SERPAES contains different PAA-protected implementations of AES and of a 4×4 SERPENT-based circuits, developed in our department and implemented as independent cores. AES cores have been designed with architecture-level PAA-countermeasures, and implemented using only standard-cells from CMOS065SVTLP design kit from STMicroelectronics. The experimental activity on standard-cell side of the SERPAES chip has been focused on the test of the AES-4 core, where each register has been replaced with a Secure Double Rate Register (SDRR), especially designed to randomize the power consumption of both combinational network and registers. AES-4 has been characterized with CPA and DPA attacks, and also physical and information theoretic security metrics have been estimated. The protected implementation has been found to be strongly PAA-resistant compared to unprotected AES (also implemented in the SERPAES chip). The unprotected core has been attacked with only 72 power traces, while AES-4 has a MTD greater than the number of collected power traces ($> 100k$). The presence of SDRR allows to reduce each considered security metric (SNR, mutual information and Welch's T-test) compared to unprotected implementation, remarking its ability to avoid stealing of information through power consumption. Security evaluations have been carried out also on the two prototype SERPENT-based cores on the custom designed side of the chip. They have been designed at our laboratory with two state-of-the-art DPLs, conceived to protect cryptographic

circuits from PAAS: SABL and iDDPL. Results concerning PAAs procedure and information leakage evaluation have confirmed that TEL-based iDDPL implementation is able to tolerate multi-bit attacks also in presence of extreme unbalancing in capacitive loads. Also adopting a single-bit power model, the RTZ-based SABL has been found very sensitive to unbalance. Experiments performed on SABL and iDDPL implementations are in accordance with findings highlighted during the experimental activity on FPGA for D³L vs. RTZ-based DPLs implementations of the 4x4 PRESENT crypto-core.

7.1.1 Additional Research Activities

In addition to research conducted in the context of PAAs, also non inherent topics have been treated during the Ph.D. course. Main off-topic research fields and main results are summarized as follows:

- design of a novel low-voltage high-speed D-latch circuit suitable for nanometer CMOS technologies [132]. The proposed topology is compared against the low-voltage triple-tail D-latch and its advantages are demonstrated both by simulations, under different performance/power consumption tradeoffs with a 40nm CMOS technology, and theoretically, thanks to a simple model of the propagation delay derived for both low-voltage topologies. In order to further demonstrate the advantages of the proposed topology, it has also been used to design a D flip-flop (DFF), where thanks to the feature to need just 1 clock differential pair; a further speed improvement is achieved over the conventional triple-tail topology. Indeed, by comparing a two-stage frequency divider designed using both the triple-tail DFF and the proposed folded DFF, a 54% improvement in the maximum operating frequency is found when using the proposed folded DFF.
- design and test of VHDL implementation of the Frisch-Waugh-Lovell (FWL) Recursive Least Squares (RLS) algorithm [18], successfully implemented on a Xilinx Virtex-7 FPGA. The FWL-RLS algorithm has a complexity of $L^2 + O(L)$ products, instead of $1.5L^2 + O(L)$ products as in the conventional RLS algorithms. Because it removes all matrix operations separating an L input vector problem into L separate scalar problems, it is stable and often faster in fixed-point arithmetic than conventional RLS. An RLS filter with L inputs is composed of L stages, and the i -th stage ($i = 1, 2, \dots, L$) has $L + 2 - i$ inputs and $L + 1 - i$ outputs. The implementation is based on two blocks: a scalar estimation block (EB), which is instantiated once for every layer, and $L + 1 - i$ identical filtering blocks (FB). For a L -input RLS model, there are L EBs and $L(L + 1)/2$ FBs. Adding an input involves instantiating one additional EB and $L + 1$ FBs. Removing one input requires the removal of the first layer. The VHDL structure is modular and can be easily adjusted for different values of L . We also present estimated hardware costs over a wide range of L values.

7.2 Future Works

On the basis of results contained in this thesis work, there are several open points and suggestions, encouraging possible future developments and further investigations. First of all, the exploitation of data-dependency of static power consumption offer is still at first stages, since most of the PAA literature is focused on dynamic power analysis. In deep scaled CMOS processes, the static power consumption plays a key role in the overall power budget, and considerations about physical security must be taken into account also on this side. Multivariate analysis in the temperature domain and TAESP have exhibited encouraging results in increasing the quantity of information that can be extracted from parasitic static consumption. To further validate these methodologies, real experiments should be conducted on a physical device. For example, the SERPAES chip could be an interesting case study to investigate, since it has been implemented with a "not-so-old" 65nm technology.

Regarding the novel D³L style, a further validation of its capability to tolerate capacitive mismatch would be an implementation on a ASIC based on such logic style, implementing an entire block cipher, such as the AES-128, the PRESENT-80/128 or the SERPENT, using a standard digital design-flow, without routing constraints. The presence of electrical mismatch is unavoidable, but the D³L implementation has been found to be very effective in counteracting PAA also without any balancing in differential routing. Results collected on FPGA and with simulated PAAs have shown that D³L can be a suitable candidate for an easy-to-use protection strategy, that does not require additional effort to minimize unwanted leakage, whilst typically needed with other DPLs.

In Chapter 5, the analog approach to design a PAA-countermeasure has been explored. The utilization of the OCE and iOCE on a CMOS implementation of a cryptographic circuit, allowed a strong reduction of the information leaked through dynamic power consumption. Regarding the iOCE, which has been found to provide an effective solution with a negligible impact on area/power overhead, a possible and interesting future development could be its application alongside with other digital approach countermeasures, in order to further increase the security level through a nested protection scheme. In fact, the adoption of other possible countermeasures can provide additional protection from other physical emissions exploitation, such as electromagnetic radiation, not investigated in this work.

Appendix A

Introduction to Modern Lightweight Cryptography

In the last ten years, newest technologies made possible to strongly reduce the power consumption while increasing the density on chip. The "Moore's Law" should need to be reinterpreted in order to be aligned with newer needs and possibilities. The upcoming philosophy in design electronic circuits and devices is the "More Than Moore", which can be considered as the solution to the nearly end (or at least, linearization) of the "Moore's Law". The "More than Moore" approach is characterized by high density of functions per unit of silicon area, meaning that with the "same" number of transistors, the features of the device are increased with respect to the past. Heterogeneous sub-blocks are implemented on the same die:

- microprocessor;
- memory;
- A/D and D/A converters;
- I/O interfaces;
- sensors;
- cryptographic primitives;
- DSP units;
- etc.

One of the best examples of the "More Than Moore" are "Internet of Things" (IoT) devices and networks. An IoT device is a "smart node", which is able to collect real world data through sensors, elaborate them locally, and provide connectivity with similar devices. These devices have demanding constraints since are often battery powered or take advantage of energy harvesting, thus the power budget

plays a critical role in their design flow. Moreover, long idle times are dominant in the lifetime of the device, and a designer should take into account that static power consumption can be a problem in terms of battery life and also in terms on self-heating. Other interesting devices that are heavily constrained are RFIDs, that are extremely diffused in many foreseen applications, such as public transport cards, company badges, etc. It has to be noted that the collected/stored data in such smart devices are constrained to some protection strategy, since it is possible that they contain private and sensible informations, such as health-monitoring and biometric data or ID. Hence, those tight constraints are usually reflected also on cryptographic circuits and protection strategies that aim to maintain secure sensible data. In general, it is referred with the term *lightweight cryptography* all cryptographic algorithms that provide suitable solutions for this purpose [51]. In *lightweight cryptography*, designers have to deal with those demanding constraints, and a trade-off between area, power and security is needed to provide cryptographic primitives for such smart devices.

In this work, design methodologies and analysis of cryptographic circuits in terms of physical security against Power Analysis Attacks (PAAs) have been discussed. As case study, three block cipher algorithms have been taken into account:

- AES-128;
- PRESENT-80;
- SERPENT.

The wide utilization of block ciphers in several applications has been enforced by the effort that several cryptographic designers have made to provide low hardware cost solutions. In recent years, several works in this direction have been published, providing a plethora of solutions that differ from length of key, length of data-blocks, hardware requirements, and, of course, security level. In this Appendix, three popular symmetric key cipher algorithms are discussed, as representative cases of modern and *lightweight* solutions to data protection.

A.1 Advanced Encryption Standard: AES-128 Block Cipher

The Advanced Encryption Standard (AES) [114] is a symmetric key block cipher, adopted by the US National Institute for Standard and Technology (NIST) as official block cipher for secure applications, supporting key of length 128, 192 and 256 bits. The original formulation of the AES is the Rijndael algorithm [45], which was the finalist and the winner of the NIST competition in 2000 to update the classical Data Encryption Standard (DES) and triple-DES. In 2003, its relevance has been enforced by the US National Security Agency (NSA), after the adoption of AES-128 as ciphering algorithm for SECRET level files. Moreover, the AES (with longer

keys) has been chosen also for protecting TOP SECRET files. The approval of the NSA established a solid credibility in AES features in protecting data. In fact, the AES became a standard not only for the US government, but also industries and foreign administrations adopted the AES for encryption. As we have said before, the AES is available for three possible key length: 128, 192 and 256 bits. We refer to the first one, as it is the most used as case study in the PAAs literature.

The AES-128 algorithm encrypts 128-bit of data-block with 128-bit key. Encryption consists in iterated operations, known as “rounds” on a 4×4 column-major order matrix of bytes, called the *state matrix*. Each round is composed of sub-operations on the state matrix, working on a single byte of the matrix and known as “layers”. The AES-128 is composed of 11 rounds, which are in turn composed of 4 layers (except Round-0 and Round-10):

- **SubstituteBytes (SubBytes):** each byte of the state matrix is mapped into another byte according to a specific calculation in $GF(28)$ which involves a non-linear operation: the inverse element calculus in $GF(28)$. It is possible to describe this step as an associative 16x16 table, where each input byte is divided into two nibbles: the first nibble is the row index i while the second nibble is the column index j of the table; then, the element ij is the output byte of the substitution phase. This table is called substitution box (S-BOX), and it can be efficiently implemented in hardware using look-up tables or hardwired logics.
- **ShiftRows:** in this layer, the rows of the state matrix are shifted to the left: in general, the i -th row is shifted by $i - 1$ positions to the left ($i = 1, 2, 3, 4$).
- **MixColumns:** the bytes of the state matrix are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with *ShiftRows*, *MixColumns* provides the propriety of confusion of the algorithm in order to resist high-order cryptanalytic attacks.
- **AddRoundKey:** in this layer, each byte of the matrix is exclusively summed to each byte of the 128-bit round key. A round key is calculated through the function *ExpandKey* of the Key Scheduler device, which takes as input the k -th round key and generates the $(k + 1)$ -th round key using nonlinear operations which involve again the usage of S-BOXes.

The encryption process is shown in Figure A.1, where the different elaboration steps are shown. Round-0 is made up only of the *AddRoundKey* layer, where the key is combined directly to the input block. Rounds 1-9 are composed of all the four layers and at each round, the XOR operation is executed between the bytes of the state matrix and the round key generated by the Key Scheduler. Finally, in Round 10 the *MixColumns* layer is not present. The four operations/layers required in AES-128 are shown also in Figure A.2.

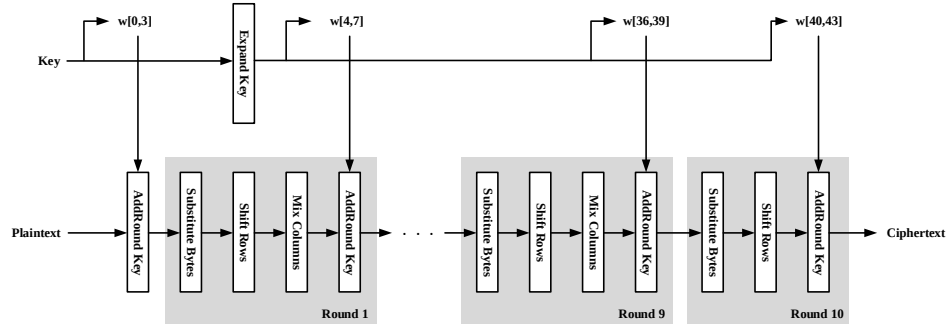


Figure A.1. Different elaboration steps of the encoding procedure of AES-128.

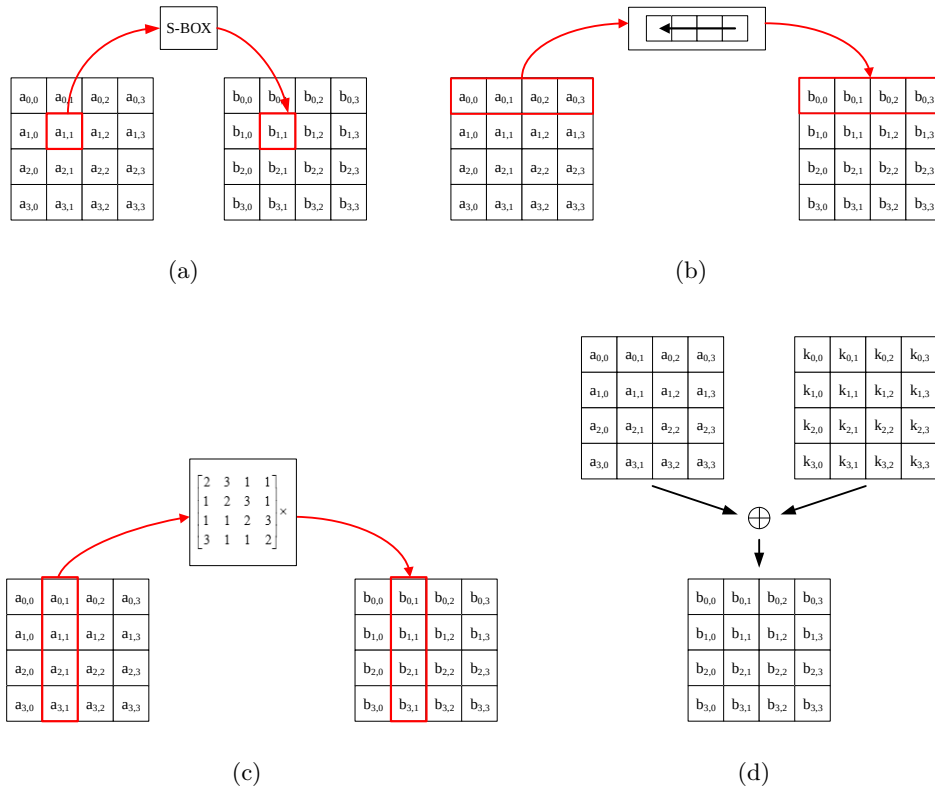


Figure A.2. Basic operations on state matrix in AES-128: *SubBytes* (a), *ShiftRows* (b), *MixColumns* (c) and *AddRoundKey* (d).

A **Key Schedule** expands the key, generating at each round a new 128-bit round key. The key expansion can be efficiently computed, since require less computation than the encryption itself, and for each possible key, there is one and only one possible expansion set. In this case, the key schedule performs three basic operations: rotation (8-bit left shift), SubBytes and bitwise XOR with a 8-bit vector called *Rcon*, the value of which depends on the round.

Table A.1. S-BOX of PRESENT regarding the input value.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SBOX[x]	12	5	6	11	9	0	10	13	3	14	15	8	4	7	1	2

A.2 PRESENT

On the legacy of AES block cipher, several other alternative design of symmetric key algorithms, based on the *substitution-permutation network* (SPN) paradigm, meeting cryptanalysis-resilience, throughput and demanding constraints based on hardware needs have been presented in the last fifteen years. The PRESENT block cipher algorithm (ISO/IEC 29192-2:2012 standard) proposed by Bogdanov *et al.* in [25], is considered as a lightweight cryptographic algorithm, since it requires down to half of hardware resources needed for AES-128 [51] [77], and can operate on 64-bit data-blocks. The algorithm has been conceived with the perspective to work with 80-bit or 128-bit keys. In this section, we will focus on the PRESENT-80 version, which is the most adopted in PAAs literature. The main algorithm has been designed with simplicity in mind, since it requires very low-computational effort compared to other popular symmetric key cipher (e.g. DES, AES). The main goal of Bogdanov *et al.* was to reduce the hardware cost of the implementation, to make it suitable for ultra-constrained applications.

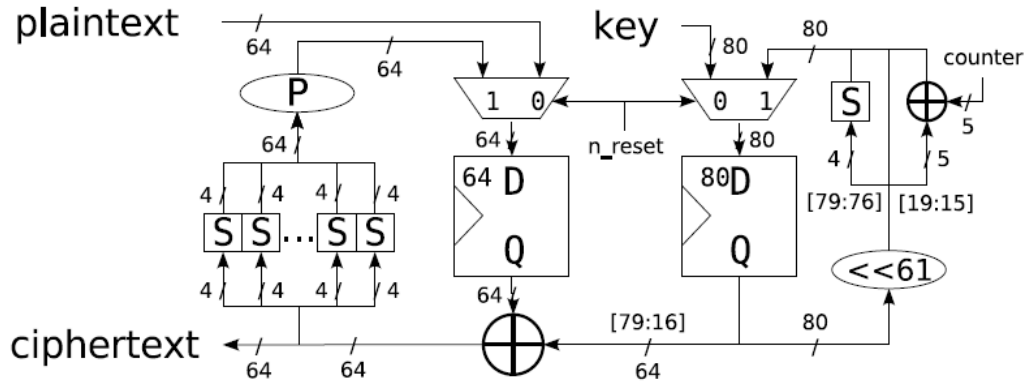
The algorithm is composed by 31 rounds, structured as follows:

- **AddRoundKey:** the 64-bit round key is XORed with the 64-bit round ciphertext;
- **SubsLayer:** 16 identical 4×4 -bit S-BOXes (see Table A.1) perform the non-linear function, providing *diffusion*. The S-BOX in the PRESENT is a bijective function $SBOX : GF(4) \rightarrow GF(4)$, ;
- **PermLayer:** a linear permutation is performed after the non-linear operation, and the round ciphertext is stored in the status register (see Table A.2). The aim of the linear permutation is to ensure avalanche effect together with *SubsLayer* in the following round. This layer can be hardwired with *wire-swapping*.

Only the last round is different from the others, and it is composed only by the *AddRoundKey*. All the round keys are obtained from the secret key, by using a *KeyScheduler*. At each round, only the most significant 64-bit of the round key are XORed with the round ciphertext. The final ciphertext is captured at the output of the *AddRoundKey* layer at the end of the last round. As it is clear, the core of the algorithm can be considered as a simplification of the AES, in order to reduce the hardware footprint. The *KeyScheduler* is very simple, and not too far from AES key schedule. It is composed by a 61-bit rotation of the round key, a single 4×4 S-BOX and an addition with the round counter.

Table A.2. Permutation rule in *PermLayer* of PRESENT.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(i)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

**Figure A.3.** Data-path of the PRESENT-80 in [25].

A.2.1 Design of the PRESENT S-BOX

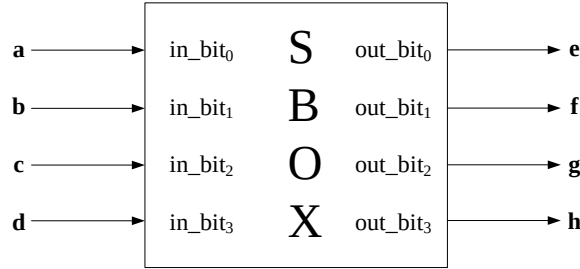
Throughout this thesis work, the 4×4 S-BOX used for PRESENT-80 and 4-bit PRESENT-based crypto-cores has been implemented using a K-map synthesis, in order to have independent logic cone for each bit. Thus, each output path is independent, and their design can be better controlled, since the S-BOX is a critical sub-block in a cryptographic circuit. In the following, equations for the internal processing of the PRESENT S-BOX are given. In this 2-input Boolean synthesis with K-map, the PRESENT S-BOX needs 47 instruction to be computed. If we consider to share only input bits and their complementary values, the number of instruction falls to 37.

A.3 SERPENT

The SERPENT block cipher proposed by Anderson *et al.* in [10] as possible candidate for Advanced Encryption Standard in 1998. It is based on a 32 rounds substitute-permutation network, operating on 128-bit data word, with key of length 128, 192 or 256 bits, similarly to the Rijndael. The SERPENT algorithm ranked second, just

Table A.3. Boolean equations describing the PRESENT 4×4 S-BOX using only 2-input Boolean operands.

$p_1 = \bar{a} \oplus b$	$p_{11} = c \cdot \bar{d}$	$p_{21} = p_{17} \cdot p_{18}$	$g = p_{14} + p_{15}$
$p_2 = b \cdot c$	$p_{12} = \bar{b} \cdot p_8$	$p_{22} = d \cdot p_{19}$	$h = p_6 + p_7$
$p_3 = \bar{c} \cdot d$	$p_{13} = \bar{c} \cdot p_9$	$p_{23} = p_{20} + p_{21}$	
$p_4 = a + b$	$p_{14} = p_{10} \cdot p_{11}$	$p_{24} = b + \bar{c}$	
$p_5 = p_1 + p_2$	$p_{15} = p_{12} + p_{13}$	$p_{25} = a \oplus d$	
$p_6 = p_3 \cdot p_4$	$b \oplus d$	$p_{26} = \bar{b} \cdot c$	
$p_7 = \bar{d} \cdot p_5$	$p_{17} = \bar{a} \cdot b$	$p_{27} = \bar{a} \oplus d$	
$p_8 = \bar{c} \oplus d$	$p_{18} = \bar{c} \oplus \bar{d}$	$p_{28} = p_{24} \cdot p_{25}$	
$p_9 = a \oplus b$	$p_{19} = a \cdot c$	$e = p_{28} + p_{29}$	
$p_{10} = a \cdot b$	$p_{20} = \bar{c} \cdot p_{16}$	$f = p_{22} + p_{23}$	
No. of Instruction		47	

**Figure A.4.** PRESENT S-BOX.

after the Rijndael algorithm, thus, it was not elected as the AES. The algorithm is well suited to be implemented in a parallel fashion, adopting 32-bit slices. It takes advantage of a $8 \times 4 \times 4$ S-BOX, that are smaller than Rijndael's 8×8 S-BOX. The encryption operation in the SERPENT block cipher can be summarized as follows:

1. an initial permutation IP ;
2. 32 rounds, consisting in a key mixing operation, substitution through S-BOXes, and a linear transformation, except the last round. In the last round, the linear transformation is replaced by an additional key mixing;
3. a final permutation FP .

It has to be pointed out that in SERPENT, there are eight S-BOXes (S_0 to S_7) that are used in parallel in 32 copies. They are chosen in according with the number of the round, more precisely:

$$round = i \rightarrow S - BOX_i = S_{i \bmod 8} \quad (\text{A.1})$$

Thus, in 32 rounds, each S-BOX is used four times. Their designs have been inspired by RC4 algorithm, as mentioned by authors in [10], and the starting point for them has been DES S-BOXes. It has to be noted that the first formulation of the SERPENT algorithm, reported in [24], made use of DES S-BOXes, but, in the latter version of [10], a different and determinist design has been adopted. More details of the implementation of SERPENT S-BOX S_0 are reported in [28].

Bibliography

- [1] ABDOLLAHI, A., FALLAH, F., AND PEDRAM, M. Leakage current reduction in cmos vlsi circuits by input vector control. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, **12** (2004), 140. doi:10.1109/TVLSI.2003.821546.
- [2] ALIOTO, M., BONGIOVANNI, S., DJUKANOVIC, M., SCOTTI, G., AND TRIFILETTI, A. Effectiveness of leakage power analysis attacks on dpa-resistant logic styles under process variations. *IEEE Transactions on Circuits and Systems I: Regular Papers*, **61** (2014), 429. doi:10.1109/TCSI.2013.2278350.
- [3] ALIOTO, M., BONGIOVANNI, S., SCOTTI, G., AND TRIFILETTI, A. Leakage power analysis attacks against a bit slice implementation of the serpent block cipher. In *2014 Proceedings of the 21st International Conference Mixed Design of Integrated Circuits and Systems (MIXDES)*, pp. 241–246 (2014). doi:10.1109/MIXDES.2014.6872193.
- [4] ALIOTO, M., CONSOLI, E., AND PALUMBO, G. *Flip-Flop Design in Nanometer CMOS: From High Speed to Low Energy*. EBL-Schweitzer. Springer International Publishing (2014).
- [5] ALIOTO, M., GIANCANE, L., SCOTTI, G., AND TRIFILETTI, A. Leakage power analysis attacks: Well-defined procedure and first experimental results. In *2009 International Conference on Microelectronics - ICM*, pp. 46–49 (2009). doi:10.1109/ICM.2009.5418592.
- [6] ALIOTO, M., GIANCANE, L., SCOTTI, G., AND TRIFILETTI, A. Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits. *Trans. Cir. Sys. Part I*, **57** (2010), 355. Available from: <http://dx.doi.org/10.1109/TCSI.2009.2019411>, doi:10.1109/TCSI.2009.2019411.
- [7] ALIOTO, M. AND PALUMBO, G. Feature - power-aware design techniques for nanometer mos current-mode logic gates: a design framework. *IEEE Circuits and Systems Magazine*, **6** (2006), 42. doi:10.1109/MCAS.2006.264841.
- [8] ALTERA. Logic elements and logic array blocks in cyclone iv devices. Available from: https://www.altera.com/en_US/pdfs/literature/hb/cyclone-iv/cyiv-51002.pdf.

- [9] AMOURI, E., MARRAKCHI, Z., AND MEHREZ, H. Differential pair routing to balance dual signals of wddl designs in cluster-based mesh fpga. In *6th International Workshop on Reconfigurable Communication-Centric Systems-on-Chip (ReCoSoC)*, pp. 1–4 (2011). doi:10.1109/ReCoSoC.2011.5981528.
- [10] ANDERSON, R., BIHAM, E., AND KNUDSEN, L. Serpent: A proposal for the advanced encryption standard.
- [11] ARCHAMBEAU, C., PEETERS, E., STANDAERT, F. X., AND QUISQUATER, J. J. *Template Attacks in Principal Subspaces*, pp. 1–14. Springer Berlin Heidelberg, Berlin, Heidelberg (2006). ISBN 978-3-540-46561-4. Available from: http://dx.doi.org/10.1007/11894063_1, doi:10.1007/11894063_1.
- [12] AVITAL, M., LEVI, I., KEREN, O., AND FISH, A. Cmos based gates for blurring power information. *IEEE Transactions on Circuits and Systems I: Regular Papers*, **63** (2016), 1033. doi:10.1109/TCSI.2016.2546387.
- [13] BADDAM, K. AND ZWOLINSKI, M. *Divided Backend Duplication Methodology for Balanced Dual Rail Routing*, pp. 396–410. Springer Berlin Heidelberg, Berlin, Heidelberg (2008). ISBN 978-3-540-85053-3. Available from: http://dx.doi.org/10.1007/978-3-540-85053-3_25, doi:10.1007/978-3-540-85053-3_25.
- [14] BATINA, L., HOGENBOOM, J., AND VAN WOUDENBERG, J. G. J. *Getting More from PCA: First Results of Using Principal Component Analysis for Extensive Power Analysis*, pp. 383–397. Springer Berlin Heidelberg, Berlin, Heidelberg (2012). ISBN 978-3-642-27954-6. Available from: https://doi.org/10.1007/978-3-642-27954-6_24, doi:10.1007/978-3-642-27954-6_24.
- [15] BELLIZIA, D., BONGIOVANNI, S., MONSURRÒ, P., SCOTTI, G., AND TRIFILETTI, A. Univariate power analysis attacks exploiting static dissipation of nanometer cmos vlsi circuits for cryptographic applications. *IEEE Transactions on Emerging Topics in Computing*, **5** (2017), 329. doi:10.1109/TETC.2016.2563322.
- [16] BELLIZIA, D., CELLUCCI, D., STEFANO, V. D., SCOTTI, G., AND TRIFILETTI, A. Novel measurements setup for attacks exploiting static power using dc pico-ammeter. In *2017 European Conference on Circuit Theory and Design (ECCTD)*, pp. 1–4 (2017). [to be published].
- [17] BELLIZIA, D., DJUKANOVIC, M., SCOTTI, G., AND TRIFILETTI, A. Template attacks exploiting static power and application to cmos lightweight crypto-hardware. *International Journal of Circuit Theory and Applications*, **45** (2017), 229. CTA-16-0162.R1. Available from: <http://dx.doi.org/10.1002/cta.2286>, doi:10.1002/cta.2286.
- [18] BELLIZIA, D., MONSURRÒ, P., AND TRIFILETTI, A. Vhdl implementation of fwl rls algorithm. In *2017 European Conference on Circuit Theory and Design (ECCTD)*, pp. 1–4 (2017). [to be published].

- [19] BELLIZIA, D., SCOTTI, G., AND TRIFILETTI, A. Implementation of the present-80 block cipher and analysis of its vulnerability to side channel attacks exploiting static power. In *2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems*, pp. 211–216 (2016). doi:10.1109/MIXDES.2016.7529734.
- [20] BELLIZIA, D., SCOTTI, G., AND TRIFILETTI, A. On-chip analog current equalizer as a countermeasure against side-channel attacks in cmos nanometer technology. In *2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems*, pp. 229–234 (2016). doi:10.1109/MIXDES.2016.7529737.
- [21] BELLIZIA, D., SCOTTI, G., AND TRIFILETTI, A. On-chip current-mode approach to thwart cpa attacks in cmos nanometer technology. *International Journal of Microelectronics and Computer Science*, **7** (2016), 147.
- [22] BELLIZIA, D., SCOTTI, G., AND TRIFILETTI, A. Fully integrable current-mode feedback suppressor as an analog countermeasure against cpa attacks in 40nm cmos technology. In *2017 13th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME)*, pp. 349–352 (2017). doi:10.1109/PRIME.2017.7974179.
- [23] BHASIN, S., GUILLEY, S., FLAMENT, F., SELMANE, N., AND DANGER, J.-L. Countering early evaluation: An approach towards robust dual-rail precharge logic. In *Proceedings of the 5th Workshop on Embedded Systems Security*, WESS '10, pp. 6:1–6:8. ACM, New York, NY, USA (2010). ISBN 978-1-4503-0078-0. Available from: <http://doi.acm.org/10.1145/1873548.1873554>, doi:10.1145/1873548.1873554.
- [24] BIHAM, E., ANDERSON, R., AND KNUDSEN, L. *Serpent: A New Block Cipher Proposal*, pp. 222–238. Springer Berlin Heidelberg, Berlin, Heidelberg (1998). ISBN 978-3-540-69710-7. Available from: https://doi.org/10.1007/3-540-69710-1_15, doi:10.1007/3-540-69710-1_15.
- [25] BOGDANOV, A., KNUDSEN, L. R., LEANDER, G., PAAR, C., POSCHMANN, A., ROBshaw, M. J. B., SEURIN, Y., AND VIKKELSOE, C. *PRESENT: An Ultra-Lightweight Block Cipher*, pp. 450–466. Springer Berlin Heidelberg, Berlin, Heidelberg (2007). ISBN 978-3-540-74735-2. Available from: https://doi.org/10.1007/978-3-540-74735-2_31, doi:10.1007/978-3-540-74735-2_31.
- [26] BONGIOVANNI, S., CENTURELLI, F., SCOTTI, G., AND TRIFILETTI, A. Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ics from side-channel attacks. *Journal of Cryptographic Engineering*, **5** (2015), 269. Available from: <http://dx.doi.org/10.1007/s13389-015-0096-z>, doi:10.1007/s13389-015-0096-z.
- [27] BONGIOVANNI, S., OLIVIERI, M., SCOTTI, G., AND TRIFILETTI, A. A power-balanced sequential element for the delay-based dual-rail precharge logic style.

- International Journal of Microelectronics and Computer Science*, **4** (2013), 129.
- [28] BONGIOVANNI, S., SCOTTI, G., AND TRIFILETTI, A. Design techniques for secure cryptographic circuits in deep submicron technologies. In PhD Thesis.
- [29] BONGIOVANNI, S., SCOTTI, G., AND TRIFILETTI, A. Security evaluation and optimization of the delay-based dual-rail pre-charge logic in presence of early evaluation of data. In *2013 International Conference on Security and Cryptography (SECRYPT)*, pp. 1–12 (2013).
- [30] BOUESSE, G. F., SICARD, G., BAIXAS, A., AND RENAUDIN, M. Quasi delay insensitive asynchronous circuits for low emi. In *4th International Workshop on Electromagnetic Compatibility of Integrated Circuits (EMC Compo'04)*. Angers, France (2004). Available from: <https://hal.archives-ouvertes.fr/hal-01392544>.
- [31] BOWMAN, K. A., TANG, X., EBLE, J. C., AND MEINDL, J. D. Impact of extrinsic and intrinsic parameter variations on cmos system on a chip performance. In *Twelfth Annual IEEE International ASIC/SOC Conference (Cat. No.99TH8454)*, pp. 267–271 (1999). doi:10.1109/ASIC.1999.806517.
- [32] BRIER, E., CLAVIER, C., AND OLIVIER, F. *Correlation Power Analysis with a Leakage Model*, pp. 16–29. Springer Berlin Heidelberg, Berlin, Heidelberg (2004). ISBN 978-3-540-28632-5. Available from: https://doi.org/10.1007/978-3-540-28632-5_2, doi:10.1007/978-3-540-28632-5_2.
- [33] BUCCI, M., GIANCANE, L., LUZZI, R., SCOTTI, G., AND TRIFILETTI, A. Delay-based dual-rail pre-charge logic. In *2009 16th IEEE International Conference on Electronics, Circuits and Systems - (ICECS 2009)*, pp. 53–56 (2009). doi:10.1109/ICECS.2009.5410921.
- [34] BUCCI, M., GIANCANE, L., LUZZI, R., AND TRIFILETTI, A. *Three-Phase Dual-Rail Pre-charge Logic*, pp. 232–241. Springer Berlin Heidelberg, Berlin, Heidelberg (2006). ISBN 978-3-540-46561-4. Available from: https://doi.org/10.1007/11894063_19, doi:10.1007/11894063_19.
- [35] BUCCI, M., GUGLIELMO, M., LUZZI, R., AND TRIFILETTI, A. *A Power Consumption Randomization Countermeasure for DPA-Resistant Cryptographic Processors*, pp. 481–490. Springer Berlin Heidelberg, Berlin, Heidelberg (2004).
- [36] BUCCI, M., LUZZI, R., GUGLIELMO, M., AND TRIFILETTI, A. A countermeasure against differential power analysis based on random delay insertion. In *Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on*, pp. 3547–3550. IEEE (2005).
- [37] BUTZEN, P. F. AND RIBAS, R. P. Leakage current in sub-micrometer cmos gates (2008).
- [38] CARMON, E., SEIFERT, J. P., AND WOOL, A. Photonic side channel attacks against rsa. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 74–78 (2017). doi:10.1109/HST.2017.7951801.

- [39] CARVAJAL, R. G., RAMIREZ-ANGULO, J., LOPEZ-MARTIN, A. J., TORRALBA, A., GALAN, J. A. G., CARLOSENA, A., AND CHAVERO, F. M. The flipped voltage follower: a useful cell for low-voltage low-power circuit design. *IEEE Transactions on Circuits and Systems I: Regular Papers*, **52** (2005), 1276. doi:10.1109/TCSI.2005.851387.
- [40] CHANDRAKASAN, A. P., BOWHILL, W. J., AND FOX, F. *Design of High-Performance Microprocessor Circuits*. Wiley-IEEE Press, 1st edn. (2000).
- [41] CHARI, S., RAO, J. R., AND ROHATGI, P. *Template Attacks*, pp. 13–28. Springer Berlin Heidelberg, Berlin, Heidelberg (2003). ISBN 978-3-540-36400-9. Available from: http://dx.doi.org/10.1007/3-540-36400-5_3, doi:10.1007/3-540-36400-5_3.
- [42] CHIP, F. Ftdi ft-232rl datasheet. Available from: http://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT232R.pdf.
- [43] CHOUDARY, O. AND KUHN, M. G. *Efficient Template Attacks*, pp. 253–270. Springer International Publishing, Cham (2014). ISBN 978-3-319-08302-5. Available from: https://doi.org/10.1007/978-3-319-08302-5_17, doi:10.1007/978-3-319-08302-5_17.
- [44] COMBLOCK. Com-1500 specifications. Available from: <https://www.comblock.com/download/com1500.pdf>.
- [45] DAEMEN, J. AND RIJMEN, V. Aes proposal: Rijndael (1999).
- [46] DANGER, J. L., GUILLEY, S., BHASIN, S., AND NASSAR, M. Overview of dual rail with precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors. In *2009 3rd International Conference on Signals, Circuits and Systems (SCS)*, pp. 1–8 (2009). doi:10.1109/ICSCS.2009.5412599.
- [47] DEBANDE, N., SOUISSI, Y., AABID, M. A. E., GUILLEY, S., AND DANGER, J. L. Wavelet transform based pre-processing for side channel analysis. In *2012 45th Annual IEEE/ACM International Symposium on Microarchitecture Workshops*, pp. 32–38 (2012). doi:10.1109/MICROW.2012.15.
- [48] DJUKANOVIC, M., BELLIZIA, D., SCOTTI, G., AND TRIFILETTI, A. *Multivariate Analysis Exploiting Static Power on Nanoscale CMOS Circuits for Cryptographic Applications*, pp. 79–94. Springer International Publishing, Cham (2017). ISBN 978-3-319-57339-7. Available from: http://dx.doi.org/10.1007/978-3-319-57339-7_5, doi:10.1007/978-3-319-57339-7_5.
- [49] DURVAUX, F., STANDAERT, F.-X., AND DEL POZO, S. M. *Towards Easy Leakage Certification*, pp. 40–60. Springer Berlin Heidelberg, Berlin, Heidelberg (2016). ISBN 978-3-662-53140-2. Available from: https://doi.org/10.1007/978-3-662-53140-2_3, doi:10.1007/978-3-662-53140-2_3.
- [50] DURVAUX, F., STANDAERT, F.-X., AND VEYRAT-CHARVILLON, N. *How to Certify the Leakage of a Chip?*, pp. 459–476. Springer Berlin Heidelberg, Berlin,

- Heidelberg (2014). ISBN 978-3-642-55220-5. Available from: https://doi.org/10.1007/978-3-642-55220-5_26, doi:10.1007/978-3-642-55220-5_26.
- [51] EISENBARTH, T., KUMAR, S., PAAR, C., POSCHMANN, A., AND UHSADEL, L. A survey of lightweight-cryptography implementations. *IEEE Design Test of Computers*, **24** (2007), 522. doi:10.1109/MDT.2007.178.
- [52] EISENBARTH, T., PAAR, C., AND WEGHENKEL, B. *Building a Side Channel Based Disassembler*, pp. 78–99. Springer Berlin Heidelberg, Berlin, Heidelberg (2010). ISBN 978-3-642-17499-5. Available from: https://doi.org/10.1007/978-3-642-17499-5_4, doi:10.1007/978-3-642-17499-5_4.
- [53] ELGHARBAWY, W. M. AND BAYOUMI, M. A. Leakage sources and possible solutions in nanometer cmos technologies. *IEEE Circuits and Systems Magazine*, **5** (2005), 6. doi:10.1109/MCAS.2005.1550165.
- [54] ENDER, M., WILD, A., AND MORADI, A. *SafeDRP: Yet Another Way Toward Power-Equalized Designs in FPGA*, pp. 83–101. Springer International Publishing, Cham (2017).
- [55] EVANS., D. The internet of things – how the next evolution of the internet is changing everything. Available from: https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
- [56] FAHN, P. N. AND PEARSON, P. K. *IPA: A New Class of Power Attacks*, pp. 173–186. Springer Berlin Heidelberg, Berlin, Heidelberg (1999). ISBN 978-3-540-48059-4. Available from: https://doi.org/10.1007/3-540-48059-5_16, doi:10.1007/3-540-48059-5_16.
- [57] FAN, G., ZHOU, Y., ZHANG, H., AND FENG, D. *How to Choose Interesting Points for Template Attacks More Effectively?*, pp. 168–183. Springer International Publishing, Cham (2015). ISBN 978-3-319-27998-5. Available from: https://doi.org/10.1007/978-3-319-27998-5_11, doi:10.1007/978-3-319-27998-5_11.
- [58] FANT, K. M. AND BRANDT, S. A. Null convention logictm: a complete and consistent logic for asynchronous digital circuit synthesis. In *Application Specific Systems, Architectures and Processors, 1996. ASAP 96. Proceedings of International Conference on*, pp. 261–273 (1996). doi:10.1109/ASAP.1996.542821.
- [59] FERGUSON, N., SCHNEIER, B., AND KOHNO, T. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley Publishing (2010). ISBN 0470474246, 9780470474242.
- [60] GENKIN, D., SHAMIR, A., AND TROMER, E. *RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*, pp. 444–461. Springer Berlin Heidelberg, Berlin, Heidelberg (2014). ISBN 978-3-662-44371-2. Available from: https://doi.org/10.1007/978-3-662-44371-2_25, doi:10.1007/978-3-662-44371-2_25.

- [61] GHOSH, S. AND ROY, K. Parameter variation tolerance and error resiliency: New design paradigm for the nanoscale era. *Proceedings of the IEEE*, **98** (2010), 1718. doi:10.1109/JPROC.2010.2057230.
- [62] GIERLICH, B., BATINA, L., TUYLS, P., AND PRENEEL, B. *Mutual Information Analysis*, pp. 426–442. Springer Berlin Heidelberg, Berlin, Heidelberg (2008). ISBN 978-3-540-85053-3. Available from: https://doi.org/10.1007/978-3-540-85053-3_27, doi:10.1007/978-3-540-85053-3_27.
- [63] GIERLICH, B., LEMKE-RUST, K., AND PAAR, C. *Templates vs. Stochastic Methods*, pp. 15–29. Springer Berlin Heidelberg, Berlin, Heidelberg (2006). ISBN 978-3-540-46561-4. Available from: https://doi.org/10.1007/11894063_2, doi:10.1007/11894063_2.
- [64] GIORGETTI, J., SCOTTI, G., SIMONETTI, A., AND TRIFILETTI, A. Analysis of data dependence of leakage current in cmos cryptographic hardware. In *Proceedings of the 17th ACM Great Lakes Symposium on VLSI, GLSVLSI '07*, pp. 78–83. ACM, New York, NY, USA (2007). ISBN 978-1-59593-605-9. Available from: <http://doi.acm.org/10.1145/1228784.1228808>, doi:10.1145/1228784.1228808.
- [65] GORNIK, A., MORADI, A., OEHM, J., AND PAAR, C. A hardware-based countermeasure to reduce side-channel leakage: Design, implementation, and evaluation. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **34** (2015), 1308. doi:10.1109/TCAD.2015.2423274.
- [66] GUILLEY, S., HOOGVORST, P., MATHIEU, Y., AND PACALET, R. *The “Backend Duplication” Method*, pp. 383–397. Springer Berlin Heidelberg, Berlin, Heidelberg (2005). ISBN 978-3-540-31940-5. Available from: http://dx.doi.org/10.1007/11545262_28, doi:10.1007/11545262_28.
- [67] HAIDER, S. I. AND NAZHANDALI, L. Utilizing sub-threshold technology for the creation of secure circuits. In *2008 IEEE International Symposium on Circuits and Systems*, pp. 3182–3185 (2008). doi:10.1109/ISCAS.2008.4542134.
- [68] HALPERIN, D., HEYDT-BENJAMIN, T. S., RANSFORD, B., CLARK, S. S., DEFEND, B., MORGAN, W., FU, K., KOHNO, T., AND MAISEL, W. H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pp. 129–142 (2008). doi:10.1109/SP.2008.31.
- [69] HASAN, M. Z. AND BIRD, M. Energy reductions for embedded processors in reconfigurable hardware. In *2011 IEEE INTERNATIONAL CONFERENCE ON ELECTRO/INFORMATION TECHNOLOGY*, pp. 1–8 (2011). doi:10.1109/EIT.2011.5978617.
- [70] HE, W., OTERO, A., DE LA TORRE, E., AND RIESGO, T. Automatic generation of identical routing pairs for fpga implemented dpl logic. In *2012 International Conference on Reconfigurable Computing and FPGAs*, pp. 1–6 (2012). doi:10.1109/ReConFig.2012.6416733.

- [71] HOGENBOOM, J. Principal component analysis and side-channel attacks - master thesis.
- [72] IOKIBE, K., AMANO, T., OKAMOTO, K., AND TOYOTA, Y. Equivalent circuit modeling of cryptographic integrated circuit for information security design. *IEEE Transactions on Electromagnetic Compatibility*, **55** (2013), 581. doi:10.1109/TEM.2013.2250505.
- [73] IOKIBE, K., AMANO, T., AND TOYOTA, Y. On-board decoupling of cryptographic fpga to improve tolerance to side-channel attacks. In *2011 IEEE International Symposium on Electromagnetic Compatibility*, pp. 925–930 (2011). doi:10.1109/ISEMC.2011.6038441.
- [74] JOHNSON, H. W. AND GRAHAM, M. *High-speed Digital Design: A Handbook of Black Magic*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA (1993). ISBN 0-13-395724-1.
- [75] JOVANOVIĆ, B. AND JEVTIĆ, M. Static and dynamic power consumption of arithmetic circuits in modern technologies. In *ETRN, National Conference*, pp. EL3–6 (2011).
- [76] JOVANOVIĆ, G. S. AND STOJČEV, M. Linear current starved delay element. *Proc. of ICEST*, (2005).
- [77] KATAGI, M. AND MORIAI, S. Lightweight cryptography for the internet of things.
- [78] KEITHLEY. Keithley 6485/6487 user manual. Available from: [http://www.sal.wisc.edu/manga/archive/public/datasheets/keithley/6487-900-01%20\(C%20-%20Mar%202011\)\(User\).pdf](http://www.sal.wisc.edu/manga/archive/public/datasheets/keithley/6487-900-01%20(C%20-%20Mar%202011)(User).pdf).
- [79] KIM, H., HONG, S., PRENEEL, B., AND VERBAUWHEDE, I. Binary decision diagram to design balanced secure logic styles. In *22nd IEEE International Symposium on On-Line Testing and Robust System Design, IOLTS 2016, Sant Feliu de Guixols, Spain, July 4-6, 2016*, pp. 239–244 (2016). Available from: <https://doi.org/10.1109/IOLTS.2016.7604710>, doi:10.1109/IOLTS.2016.7604710.
- [80] KIM, M. K., HAN, D. G., RYOO, J. C., AND YI, O. Cpa performance enhancement based on spectrogram. In *2012 IEEE International Carnahan Conference on Security Technology (ICCST)*, pp. 195–200 (2012). doi:10.1109/CCST.2012.6393558.
- [81] KIM, N. S., AUSTIN, T., BAAUW, D., MUDGE, T., FLAUTNER, K., HU, J. S., IRWIN, M. J., KANDEMIR, M., AND NARAYANAN, V. Leakage current: Moore’s law meets static power. *Computer*, **36** (2003), 68. doi:10.1109/MC.2003.1250885.
- [82] KIRSCHBAUM, M. AND POPP, T. Evaluation of a dpa-resistant prototype chip. In *2009 Annual Computer Security Applications Conference*, pp. 43–50 (2009). doi:10.1109/ACSAC.2009.14.

- [83] KNIGHT, K. *Mathematical Statistics*. Chapman & Hall/CRC Texts in Statistical Science. CRC Press (1999). ISBN 9781584888567.
- [84] KOCHER, P., JAFFE, J., AND JUN, B. *Differential Power Analysis*, pp. 388–397. Springer Berlin Heidelberg, Berlin, Heidelberg (1999). ISBN 978-3-540-48405-9. Available from: https://doi.org/10.1007/3-540-48405-1_25, doi:10.1007/3-540-48405-1_25.
- [85] KOCHER, P. C. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '96, pp. 104–113. Springer-Verlag, London, UK, UK (1996). ISBN 3-540-61512-1. Available from: <http://dl.acm.org/citation.cfm?id=646761.706156>.
- [86] KULIKOWSKI, K. J., KARPOVSKY, M. G., AND TAUBIN, A. Power attacks on secure hardware based on early propagation of data. In *12th IEEE International On-Line Testing Symposium (IOLTS'06)*, pp. 6 pp.– (2006). doi:10.1109/IOLTS.2006.49.
- [87] KULIKOWSKI, K. J., SU, M., SMIRNOV, A., TAUBIN, A., KARPOVSKY, M. G., AND MACDONALD, D. Delay insensitive encoding and power analysis: a balancing act [cryptographic hardware protection]. In *11th IEEE International Symposium on Asynchronous Circuits and Systems*, pp. 116–125 (2005). doi:10.1109/ASYNC.2005.18.
- [88] LECROY, T. Lecroy wavesurfer mx-104b datasheet. Available from: http://cdn.teledynelecroy.com/files/pdf/wavesurfer_mxs-b_datasheet.pdf.
- [89] LEVI, I., KEREN, O., AND FISH, A. Data-dependent delays as a barrier against power attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, **62** (2015), 2069.
- [90] LIU, W., WU, L., ZHANG, X., AND WANG, A. Wavelet-based noise reduction in power analysis attack. In *2014 Tenth International Conference on Computational Intelligence and Security*, pp. 405–409 (2014). doi:10.1109/CIS.2014.103.
- [91] MACÉ, F., STANDAERT, F.-X., AND QUISQUATER, J.-J. *Information Theoretic Evaluation of Side-Channel Resistant Logic Styles*, pp. 427–442. Springer Berlin Heidelberg, Berlin, Heidelberg (2007). ISBN 978-3-540-74735-2. Available from: http://dx.doi.org/10.1007/978-3-540-74735-2_29, doi:10.1007/978-3-540-74735-2_29.
- [92] MANGARD, S. *Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness*, pp. 222–235. Springer Berlin Heidelberg, Berlin, Heidelberg (2004). ISBN 978-3-540-24660-2. Available from: https://doi.org/10.1007/978-3-540-24660-2_18, doi:10.1007/978-3-540-24660-2_18.
- [93] MANGARD, S., OSWALD, E., AND POPP, T. *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA (2007). ISBN 0387308571.

- [94] MARLOW. Marlow rc3-8-01ls thermoelectric cooler datasheet. Available from: http://www.marlow.com/downloads/dl/file/id/237/product/143/rc3_8.pdf.
- [95] MATHER, L., OSWALD, E., BANDENBURG, J., AND WÓJCIK, M. Does my device leak information? an a priori statistical power analysis of leakage detection tests. In *Part I of the Proceedings of the 19th International Conference on Advances in Cryptology - ASIACRYPT 2013 - Volume 8269*, pp. 486–505. Springer-Verlag New York, Inc., New York, NY, USA (2013). ISBN 978-3-642-42032-0. Available from: http://dx.doi.org/10.1007/978-3-642-42033-7_25, doi:10.1007/978-3-642-42033-7_25.
- [96] MATSUI, M., HARA, H., UETANI, Y., KIM, L.-S., NAGAMATSU, T., WATANABE, Y., CHIBA, A., MATSUDA, K., AND SAKURAI, T. A 200 mhz 13 mm² 2-d dct macrocell using sense-amplifying pipeline flip-flop scheme. *IEEE Journal of Solid-State Circuits*, **29** (1994), 1482. doi:10.1109/4.340421.
- [97] MAYHEW, M. AND MURESAN, R. On-chip nanoscale capacitor decoupling architectures for hardware security. *IEEE Transactions on Emerging Topics in Computing*, **2** (2014), 4. doi:10.1109/TETC.2014.2303934.
- [98] MCCOY, C. Vhdl source code of basic aes-128 encryption unit. Available from: https://github.com/inmcm/HDL_Ciphers/tree/master/AES/Basic_AES_128_Cipher.
- [99] MENICOCCHI, R., TRIFILETTI, A., AND TROTTA, F. A logic level countermeasure against cpa side channel attacks on aes. In *Proceedings of the 20th International Conference Mixed Design of Integrated Circuits and Systems - MIXDES 2013*, pp. 403–407 (2013).
- [100] MENICOCCHI, R., TRIFILETTI, A., AND TROTTA, F. Random interleaved pipeline countermeasure against power analysis attacks. In *Proceedings of the 2013 9th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME)*, pp. 145–148 (2013).
- [101] MENICOCCHI, R., TRIFILETTI, A., AND TROTTA, F. Experiments on two clock countermeasures against power analysis attacks. In *2014 Proceedings of the 21st International Conference Mixed Design of Integrated Circuits and Systems (MIXDES)*, pp. 215–219 (2014).
- [102] MESQUITA, D., TECHER, J.-D., TORRES, L., ROBERT, M., CATHEBRAS, G., SASSATELLI, G., AND MORAES, F. G. *Current Mask Generation: an Analog Circuit to Thwart DPA Attacks*, pp. 317–330. Springer US, Boston, MA (2007). ISBN 978-0-387-73661-7. Available from: https://doi.org/10.1007/978-0-387-73661-7_20, doi:10.1007/978-0-387-73661-7_20.
- [103] MESSERGES, T. S., DABBISH, E. A., AND SLOAN, R. H. *Power Analysis Attacks of Modular Exponentiation in Smartcards*, pp. 144–157. Springer Berlin Heidelberg, Berlin, Heidelberg (1999). ISBN 978-3-540-48059-4. Available from: https://doi.org/10.1007/3-540-48059-5_14, doi:10.1007/3-540-48059-5_14.

- [104] MICALI, S. AND REYZIN, L. *Physically Observable Cryptography*, pp. 278–296. Springer Berlin Heidelberg, Berlin, Heidelberg (2004). ISBN 978-3-540-24638-1. Available from: https://doi.org/10.1007/978-3-540-24638-1_16, doi: 10.1007/978-3-540-24638-1_16.
- [105] MOKHTAR, S. M. A. B. AND ABDULLAH, W. F. H. W. Memristor based delay element using current starved inverter. In *RSM 2013 IEEE Regional Symposium on Micro and Nanoelectronics*, pp. 81–84 (2013). doi:10.1109/RSM.2013.6706478.
- [106] MOOS, T., MORADI, A., AND RICHTER, B. Static power side-channel analysis of a threshold implementation prototype chip. In *Design, Automation Test in Europe Conference Exhibition (DATE), 2017*, pp. 1324–1329 (2017). doi:10.23919/DATE.2017.7927198.
- [107] MORADI, A. *Side-Channel Leakage through Static Power*, pp. 562–579. Springer Berlin Heidelberg, Berlin, Heidelberg (2014). ISBN 978-3-662-44709-3. Available from: http://dx.doi.org/10.1007/978-3-662-44709-3_31, doi:10.1007/978-3-662-44709-3_31.
- [108] MORADI, A., EISENBARTH, T., POSCHMANN, A., AND PAAR, C. *Power Analysis of Single-Rail Storage Elements as Used in MDPL*, pp. 146–160. Springer Berlin Heidelberg, Berlin, Heidelberg (2010). ISBN 978-3-642-14423-3. Available from: https://doi.org/10.1007/978-3-642-14423-3_11, doi: 10.1007/978-3-642-14423-3_11.
- [109] MORADI, A., KIRSCHBAUM, M., EISENBARTH, T., AND PAAR, C. Masked dual-rail precharge logic encounters state-of-the-art power analysis methods. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, **20** (2012), 1578. doi:10.1109/TVLSI.2011.2160375.
- [110] MUKHOPADHYAY, S., MAHMOODI-MEIMAND, H., NEAU, C., AND ROY, K. Leakage in nanometer scale cmos circuits. In *2003 International Symposium on VLSI Technology, Systems and Applications. Proceedings of Technical Papers. (IEEE Cat. No.03TH8672)*, pp. 307–312 (2003). doi:10.1109/VTSA.2003.1252615.
- [111] MURESAN, R. AND GREGORI, S. Protection circuit against differential power analysis attacks for smart cards. *IEEE Transactions on Computers*, **57** (2008), 1540. doi:10.1109/TC.2008.107.
- [112] NASSIF, S., BERNSTEIN, K., FRANK, D. J., GATTIKER, A., HAENSCH, W., JI, B. L., NOWAK, E., PEARSON, D., AND ROHRER, N. J. High performance cmos variability in the 65nm regime and beyond. In *2007 IEEE International Electron Devices Meeting*, pp. 569–571 (2007). doi:10.1109/IEDM.2007.4419002.
- [113] NIKOLIC, B., OKLOBDIJA, V. G., STOJANOVIC, V., JIA, W., CHIU, J. K.-S., AND LEUNG, M. M.-T. Improved sense-amplifier-based flip-flop: design and measurements. *IEEE Journal of Solid-State Circuits*, **35** (2000), 876. doi:10.1109/4.845191.

- [114] OF STANDARD, N. I. AND TECHNOLOGY. Advanced encryption standard. *NIST FIPS PUB 197*, (2001).
- [115] PARK, A., HAN, D. G., AND RYOO, J. Cpa performance comparison based on wavelet transform. In *2012 IEEE International Carnahan Conference on Security Technology (ICCST)*, pp. 201–206 (2012). doi:10.1109/CCST.2012.6393559.
- [116] POPP, T., KIRSCHBAUM, M., ZEFFERER, T., AND MANGARD, S. *Evaluation of the Masked Logic Style MDPL on a Prototype Chip*, pp. 81–94. Springer Berlin Heidelberg, Berlin, Heidelberg (2007). ISBN 978-3-540-74735-2. Available from: https://doi.org/10.1007/978-3-540-74735-2_6, doi:10.1007/978-3-540-74735-2_6.
- [117] POPP, T. AND MANGARD, S. *Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints*, pp. 172–186. Springer Berlin Heidelberg, Berlin, Heidelberg (2005). ISBN 978-3-540-31940-5. Available from: http://dx.doi.org/10.1007/11545262_13, doi:10.1007/11545262_13.
- [118] POZO, S. M. D., STANDAERT, F. X., KAMEL, D., AND MORADI, A. Side-channel attacks from static power: When should we care? In *2015 Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 145–150 (2015).
- [119] QUISQUATER, J.-J. AND SAMYDE, D. *ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards*, pp. 200–210. Springer Berlin Heidelberg, Berlin, Heidelberg (2001). ISBN 978-3-540-45418-2. Available from: https://doi.org/10.1007/3-540-45418-7_17, doi:10.1007/3-540-45418-7_17.
- [120] RABAEY, J. M., CHANDRAKASAN, A., AND NIKOLIC, B. *Digital Integrated Circuits*. Prentice Hall Press, Upper Saddle River, NJ, USA, 3rd edn. (2008). ISBN 0132219107, 9780132219105.
- [121] RAKERS, P., CONNELL, L., COLLINS, T., AND RUSSELL, D. Secure contactless smartcard asic with dpa protection. *IEEE Journal of Solid-State Circuits*, **36** (2001), 559. doi:10.1109/4.910496.
- [122] RATANPAL, G. B., WILLIAMS, R. D., AND BLALOCK, T. N. An on-chip signal suppression countermeasure to power analysis attacks. *IEEE Transactions on Dependable and Secure Computing*, **1** (2004), 179. doi:10.1109/TDSC.2004.25.
- [123] RECHBERGER, C. AND OSWALD, E. *Practical Template Attacks*, pp. 440–456. Springer Berlin Heidelberg, Berlin, Heidelberg (2005). ISBN 978-3-540-31815-6. Available from: https://doi.org/10.1007/978-3-540-31815-6_35, doi:10.1007/978-3-540-31815-6_35.
- [124] REGAZZONI, F., ET AL. *Evaluating Resistance of MCML Technology to Power Analysis Attacks Using a Simulation-Based Methodology*, pp. 230–243.

- Springer Berlin Heidelberg, Berlin, Heidelberg (2009). ISBN 978-3-642-01004-0. Available from: http://dx.doi.org/10.1007/978-3-642-01004-0_13, doi:10.1007/978-3-642-01004-0_13.
- [125] RENAULD, M., STANDAERT, F.-X., VEYRAT-CHARVILLON, N., KAMEL, D., AND FLANDRE, D. *A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices*, pp. 109–128. Springer Berlin Heidelberg, Berlin, Heidelberg (2011). ISBN 978-3-642-20465-4. Available from: http://dx.doi.org/10.1007/978-3-642-20465-4_8, doi:10.1007/978-3-642-20465-4_8.
- [126] ROLFES, C., POSCHMANN, A., LEANDER, G., AND PAAR, C. *Ultra-Lightweight Implementations for Smart Devices – Security for 1000 Gate Equivalents*, pp. 89–103. Springer Berlin Heidelberg, Berlin, Heidelberg (2008).
- [127] ROY, K., MUKHOPADHYAY, S., AND MAHMOODI-MEIMAND, H. Leakage current mechanisms and leakage reduction techniques in deep-submicrometer cmos circuits. *Proceedings of the IEEE*, **91** (2003), 305. doi:10.1109/JPROC.2002.808156.
- [128] SARAVANAN, P., KALPANA, P., PREETHISRI, V., AND SNEHA, V. Power analysis attack using neural networks with wavelet transform as pre-processor. In *18th International Symposium on VLSI Design and Test*, pp. 1–6 (2014). doi:10.1109/ISV DAT.2014.6881059.
- [129] SCHAUMONT, P. AND TIRI, K. *Masking and Dual-Rail Logic Don't Add Up*, pp. 95–106. Springer Berlin Heidelberg, Berlin, Heidelberg (2007). ISBN 978-3-540-74735-2. Available from: https://doi.org/10.1007/978-3-540-74735-2_7, doi:10.1007/978-3-540-74735-2_7.
- [130] SCHIMMEL, O., DUPLY, P., BOHL, E., HAYEK, J., AND ROSENSTIEL, W. Correlation power analysis in frequency domain. In *COSADE 2010 - First International Workshop on Constructive Side-Channel Analysis and Secure Design* (2010).
- [131] SCHNEIDER, T. AND MORADI, A. Leakage assessment methodology - a clear roadmap for side-channel evaluations. Cryptology ePrint Archive, Report 2015/207 (2015).
- [132] SCOTTI, G., BELLIZIA, D., TRIFILETTI, A., AND PALUMBO, G. Design of low-voltage high-speed cml d-latches in nanometer cmos technologies. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, **PP** (2017), 1. doi:10.1109/TVLSI.2017.2750207.
- [133] SHAMIR, A. *Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies*, pp. 71–77. Springer Berlin Heidelberg, Berlin, Heidelberg (2000). ISBN 978-3-540-44499-2. Available from: https://doi.org/10.1007/3-540-44499-8_5, doi:10.1007/3-540-44499-8_5.
- [134] SHANNON, C. A mathematical theory of communication. *Bell System Technical Journal*, Vol 27, pp. 379–423, (1949).

- [135] SOUISSI, Y., AABID, M. A. E., DEBANDE, N., GUILLEY, S., AND DANGER, J.-L. Novel applications of wavelet transforms based side-channel analysis (2011).
- [136] STANDAERT, F.-X. *Introduction to Side-Channel Attacks*, pp. 27–42. Springer US, Boston, MA (2010). ISBN 978-0-387-71829-3. Available from: https://doi.org/10.1007/978-0-387-71829-3_2, doi:10.1007/978-0-387-71829-3_2.
- [137] STANDAERT, F.-X., MALKIN, T. G., AND YUNG, M. A unified framework for the analysis of side-channel key recovery attacks. In *Proceedings of the 28th Annual International Conference on Advances in Cryptology: The Theory and Applications of Cryptographic Techniques*, EUROCRYPT '09, pp. 443–461. Springer-Verlag, Berlin, Heidelberg (2009). ISBN 978-3-642-01000-2. Available from: http://dx.doi.org/10.1007/978-3-642-01001-9_26, doi:10.1007/978-3-642-01001-9_26.
- [138] STANDAERT, F.-X., XAVIER ST, F., MALKIN, T. G., AND YUNG, M. A formal practice-oriented model for the analysis of side-channel attacks (2006).
- [139] SUZUKI, D. AND SAEKI, M. *Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style*, pp. 255–269. Springer Berlin Heidelberg, Berlin, Heidelberg (2006). ISBN 978-3-540-46561-4. Available from: https://doi.org/10.1007/11894063_21, doi:10.1007/11894063_21.
- [140] TEKTRONIX. Tektronix ct-1, ct-2 and ct-6 datasheet. Available from: https://www.tek.com/sites/default/files/media/media/resources/60W_12572_2.pdf.
- [141] TI. Texas instruments lm-35 temperature sensor datasheet. Available from: <http://www.ti.com/lit/ds/symlink/lm35.pdf>.
- [142] TI. Texas instruments lmx58-n low-power, dual-operational amplifier datasheet. Available from: <http://www.ti.com/lit/ds/symlink/lm158-n.pdf>.
- [143] TIAN, Q., O'NEILL, M., AND HANLEY, N. Can leakage models be more efficient? non-linear models in side channel attacks. In *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 215–220 (2014). doi:10.1109/WIFS.2014.7084330.
- [144] TIRI, K., AKMAL, M., AND VERBAUWHEDE, I. A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards. In *Proceedings of the 28th European Solid-State Circuits Conference*, pp. 403–406 (2002).
- [145] TIRI, K., HWANG, D., HODJAT, A., LAI, B.-C., YANG, S., SCHAUMONT, P., AND VERBAUWHEDE, I. *Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment*, pp. 354–365. Springer Berlin Heidelberg, Berlin, Heidelberg (2005). ISBN 978-3-540-31940-5. Available from: https://doi.org/10.1007/11545262_26, doi:10.1007/11545262_26.

- [146] TIRI, K. AND VERBAUWHEDE, I. A dynamic and differential CMOS logic style to resist power and timing attacks on security ic's. *IACR Cryptology ePrint Archive*, **2004** (2004), 66. Available from: <http://eprint.iacr.org/2004/066>.
- [147] TIRI, K. AND VERBAUWHEDE, I. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proceedings of the Conference on Design, Automation and Test in Europe - Volume 1*, DATE '04, pp. 10246–. IEEE Computer Society, Washington, DC, USA (2004). ISBN 0-7695-2085-5. Available from: <http://dl.acm.org/citation.cfm?id=968878.969036>.
- [148] TIRI, K. AND VERBAUWHEDE, I. *Place and Route for Secure Standard Cell Design*, pp. 143–158. Springer US, Boston, MA (2004). ISBN 978-1-4020-8147-7. Available from: http://dx.doi.org/10.1007/1-4020-8147-2_10, doi:10.1007/1-4020-8147-2_10.
- [149] TIRI, K. AND VERBAUWHEDE, I. Design method for constant power consumption of differential logic circuits. *CoRR*, **abs/0710.4756** (2007). Available from: <http://arxiv.org/abs/0710.4756>.
- [150] TOKUNAGA, C. AND BLAAUW, D. Securing encryption systems with a switched capacitor current equalizer. *IEEE Journal of Solid-State Circuits*, **45** (2010), 23. doi:10.1109/JSSC.2009.2034081.
- [151] TROTTA, F., MENICOCCHI, R., AND TRIFILETTI, A. Rtl countermeasures against power analysis attacks implemented on fpga. In PhD Thesis.
- [152] WHITNALL, C., OSWALD, E., AND MATHER, L. *An Exploration of the Kolmogorov-Smirnov Test as a Competitor to Mutual Information Analysis*, pp. 234–251. Springer Berlin Heidelberg, Berlin, Heidelberg (2011). ISBN 978-3-642-27257-8. Available from: https://doi.org/10.1007/978-3-642-27257-8_15, doi:10.1007/978-3-642-27257-8_15.
- [153] XILINX. Spartan-6 fpga configurable logic block - user guide (ug384, v1.1, february 23,2010). Available from: https://www.xilinx.com/support/documentation/user_guides/ug384.pdf.

List of Publications

- Bellizia, D., Bongiovanni, S., Monsurrò, P., Scotti, G., and Trifiletti, A., "Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications". *IEEE Transactions on Emerging Topics in Computing*, 5 (2017), pp. 329-339.
- Bellizia, D., Cellucci, D., Stefano, V. D., Scotti, G., and Trifiletti, A., "Novel measurements setup for attacks exploiting static power using DC pico-ammeter". *2017 European Conference on Circuit Theory and Design (ECCTD)*, Catania, 2017, pp. 1-4.
- Bellizia, D., Djukanovic, M., Scotti, G., and Trifiletti, A., "Template Attacks Exploiting Static Power and Application to CMOS Lightweight Cryptohardware". *International Journal of Circuit Theory and Applications*, 45 (2017), pp.229-241.
- Bellizia, D., Monsurrò, P., and Trifiletti, A., "VHDL implementation of FWL RLS algorithm". *2017 European Conference on Circuit Theory and Design (ECCTD)*, Catania, 2017, pp. 1-4.
- Bellizia, D., Scotti, G., and Trifiletti, A., "Implementation of the PRESENT-80 Block Cipher and Analysis of Its Vulnerability to Side Channel Attacks Exploiting Static Power". In *2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems*, pp. 211–216 (2016).
- Bellizia, D., Scotti, G., and Trifiletti, A., "On-chip Analog Current Equalizer as a Countermeasure Against Side-Channel Attacks in CMOS Nanometer Technology". In *2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems*, pp. 229–234 (2016).
- Bellizia, D., Scotti, G., and Trifiletti, A., "On-chip Current-mode Approach to Thwart CPA Attacks in CMOS Nanometer Technology". *International Journal of Microelectronics and Computer Science*, 7 (2016), 147.
- Bellizia, D., Scotti, G., and Trifiletti, A., "Fully Integrable Current-mode Feedback Suppressor as an Analog Countermeasure Against CPA Attacks in 40nm CMOS Technology". In *2017 13th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME)*, pp. 349–352 (2017).

- Djukanovic, M., Bellizia, D., Scotti, G., and Trifiletti, A., "Multivariate Analysis Exploiting Static Power on Nanoscale CMOS Circuits for Cryptographic Applications", pp. 79–94. Springer International Publishing, Cham (2017).
- Scotti, G., Bellizia, D., Trifiletti, A., and Palumbo, G., "Design of Low-Voltage High-Speed CML D-Latches in Nanometer CMOS Technologies". IEEE Transactions on Very Large Scale Integration (VLSI) Systems, PP (2017), 1.
- Bellizia, D., Bongiovanni, S., Monsurrò, P., Scotti, G., Trifiletti, A., and Trotta, F. "Secure Double Rate Registers as an RTL Countermeasure against Power Analysis Attacks". IEEE Transactions on VLSI (TVLSI). [To Be Published]
- Bellizia, D., Scotti, G., and Trifiletti, A. "Secure Implementation of TEL-compatible Flip-Flops using a Standard-Cell Approach". ISCAS-2018 Conference. [To Be Published]
- Bellizia, D., Scotti, G., and Trifiletti, A., "Delay-based Dynamic Differential Logic: a Novel PAA and Mismatch Tolerant Logic Style for Cryptographic Implementations". for IEEE Transactions on VLSI (TVLSI). [Writing]
- Bellizia, D., Palumbo, G., Scotti, G., and Trifiletti, A. "A Novel Very Low Voltage Topology to implement MCML XOR Gates. for ISICAS-2018 Conference". [Writing]
- Bellizia, D., Scotti, G., and Trifiletti, A., "TEL Logic Style as a Countermeasure Against Side-Channel Attacks: Secure Cell Library in 65nm CMOS and Experimental Results". for IEEE TCAS-I. [Writing]
- Levi, I., Bellizia, D., and Standaert, F.-X. "The Extent of Time Domain Countermeasures and Multi-Dimensional Side-Channel Leakage Distribution". [Writing]
- Bellizia, D., Djukanovic, M., Scotti, G., and Trifiletti, A., "Univariate and Multivariate Template Attacks Exploiting Static Power using DC Pico-ammeter". [Writing]

Acknowledgments

I would like to express all my gratitude to:

- *my family, that has been the column of my whole life: my parents, my brother and his partner Cristina. All challenges I have faced during these years have been supported by their solid trust and unconditional love. Without them, all of this could never happen.*
- *my tutor Prof. Giuseppe Scotti, for the continuous support in all these years at university, since our collaboration started almost five years ago, for his patience, motivation and immense knowledge and experience. He was not only my tutor, but a true friend. He helped me to become firstly an engineer, and then, a researcher, standing beside me as an older brother. During my Ph.D., his presence meant everything to me. I could not have imagined having a better mentor than him. Honestly: thank you so much!*
- *my grandparents, since they are the root of what I am. I must look back to look ahead. This thesis work is dedicated to the memory of my grandfather Costantino.*
- *my band (Out of Grace plus Leo), that has been the "safety valve" for the frantic years of my Ph.D.. Guys, you will always have a special place in my heart! Wish you all the best!*
- *my Ph.D. colleagues, Danilo, Andrea, Felice, Stefano, Rosa and Gaetano, that have shared this adventure with me. The hard work at university has been less heavy with them on my side. I wish them the best!*
- *my dear friend, Prof. Milena Djukanovic, for her support in working on side-channel attacks that has been so precious.*
- *the staff of the Centro Studi Giorgio Barzilai (Prof. Centurelli, Prof. Monsurrò, Prof. Tommasino, Dr. Trotta and Dr. Bongiovanni), for their wonderful technical support.*
- *Valerio Di Stefano and Danilo Cellucci, for helping me in performing experiments and supporting activities inherently to side-channel attacks. I would wish them a bright future in engineering.*
- *last, but not least, my girlfriend, for her loving support in facing the challenges that this Ph.D. offered to me. Thanks for being on my side!*

In addition, I would also to thank Prof. Domenico Caputo, Prof. Alessandro Trifiletti, Prof. Olivieri and Prof. Guglielmo D'Inzeo for their precious advices during these three years, and Prof. Tommaso Addabbo and Prof. Davide De Caro for the reviewing process of this work.