# SC-DDPL: a novel Standard-Cell based Approach for Counteracting Power Analysis Attacks in Presence of Unbalanced Routing

Davide Bellizia, Simone Bongiovanni, Mauro Olivieri, *Senior Member, IEEE* and Giuseppe Scotti, Senior *Member, IEEE*

***Abstract*—In this paper we present the Standard Cell Delay-based Dual-rail Pre-charge Logic (SC-DDPL), a novel logic style which is able to counteract Power Analysis Attacks (PAAs) also in the presence of capacitive mismatch at the output of dual-rail gates. The SC-DDPL is based on a standard-cell design flow and it is suitable to be implemented on ASICs or FPGAs without any routing constraint on differential lines, supporting the Time Enclosed Logic protocol along with a DPL structure. The security provided by SC-DDPL has been firstly investigated in simulation on some basic logic gates, which have been designed referring to a commercial 40nm CMOS technology, and then validated with experimental results on a real cryptography circuit implemented on a 65nm Intel FPGA. Simulated experiments have highlighted the capability of SC-DDPL gates to guarantee a high level of security also in presence of extreme capacitive mismatch, exhibiting strongly reduced NED/NSD metrics, as well as a reduction of the FED, compared to a reference RTZ-based WDDL implementation. In order to compare the proposed logic style against other state of the art countermeasures we have implemented a 4bit PRESENT crypto core adopting several logic styles and we have evaluated different security metrics on the same Intel Cyclone-IV FPGA. Experimental results have confirmed that the SC-DDPL outperforms other gate-level countermeasures in terms of security metrics with a reasonable area and power consumption overhead.**

***Index Terms*— power analysis attack; CMOS; DDPL, WDDL; FPGA; cryptography; side channel attack; TEL; ASIC, security.**

## I. Introduction

Since Kocher demonstrated in [1] that it is possible to use physical emissions of CMOS implementations of cryptographic algorithms or functions as source of information leakage, Side Channel Attacks (SCAs) have gained a key role in the design of such secure devices. Many physical emissions have been analyzed in the context of SCAs, such as time execution [1], electro-magnetic emission [2] and power consumption [3]. Power Analysis Attacks (PAAs) are considered to be the most common and used among the others, since they require no expensive equipment to be performed. PAAs are based on the strong relationship between input/output transitions and power consumption in CMOS circuits, which can be exploited by means of statistical tools. In literature, there are several PAA procedures that are actually used to recover secret information from a device, such as Differential Power Analysis (DPA) [3] and Correlation Power Analysis (CPA) [4]. In the context of thwarting PAAs, several approaches have been proposed, acting at each abstraction layer of a cryptographic implementation design. The leading philosophy is to make the power consumption independent from the processed data, breaking the possibility to recover information through de-correlation. To achieve this result, one of the most popular approach is to use Dual-rail Pre-charge Logic (DPL) styles, which aim to provide a constant power consumption at each clock cycle at gate-level using differential signaling. In literature, there are several DPL styles used to de-correlate power consumption from the processed data; such as Wave Dynamic Differential Logic (WDDL) [5], Sense Amplifier Based Logic (SABL) [6] Masked DPL (MDPL) [7]. Recently dual-spacer dual-rail delay-insensitive asynchronous logic [8] and Dynamic and Differential Swing-Limited Logic (DDSLL) [9] have been also proposed.

All these logic styles require special attentions during the design flow, since their capability to protect and balance the power consumption is limited by several factors, such as electrical mismatch due to capacitive unbalance [10]-[11]. To overcome the issue of capacitive unbalance due to imperfect routing without any constraint on the routing of complementary wires, in [12] authors propose the Delay-based Dual-rail Pre-charge Logic (DDPL). The DDPL makes use of DPL approach using the Time Enclosed Logic (TEL) [13] signaling instead of the classical Return-to-Zero (RTZ). In TEL protocol, the datum is encoded in the time domain instead of the differential logic level domain, which is able to provide higher immunity to capacitive unbalance compared to RTZ. A recent work presents an improved version, namely improved DDPL (iDDPL) [14],

D. Bellizia is with ICTEAM-Crypto Group of Université Catholique de Louvain, Louvain-la-Neuve, 1348 Belgium (e-mail: davide.bellizia@uclouvain.be ).

S. Bongiovanni is with the Digital Security System department of Infineon Technologies Austria (e-mail: simone.bongiovanni@infineon.com )

M. Olivieri and G. Scotti are with Dipartimento di Ingegneria Elettronica e Telecomunicazioni (DIET) of Sapienza University of Rome, Rome, 00184 Italy (e-mail: mauro.oliveri@uniroma1.it ; giuseppe.scotti@uniroma1.it ).

where the effectiveness of the TEL to tolerate capacitive mismatch has been demonstrated on an experimental 65nm ASIC.

In this paper we propose and evaluate, from a security perspective, a novel logic style named *Standard Cell Delay-based Dual-rail Pre-charge Logic* (SC-DDPL). SC-DDPL is based on a standard-cell DPL approach using TEL encoding scheme to process the data. Being based on a standard-cell design flow, SC-DDPL is suitable to be implemented on ASICs or FPGAs without any routing constraint on differential lines, supporting the Time Enclosed Logic (TEL) protocol along with a DPL structure and a synchronous behavior (evaluation starts always at the rising edge of the clock signal).

In Section II, the TEL protocol is briefly reviewed, along with the underlying assumptions on the adversary capabilities. The SC-DDPL logic gates are introduced in Section III. An analysis of energy metrics on combinational gates is presented in Section IV. The security evaluation of SC-DDPL gates and of a 4-bit PRESENT S-BOX is presented in Section V, considering different measurement setups and adversary capabilities. The FPGA implementation of a 4-bit PRESENT crypto-core referring to different PAA resistant logic styles is presented in Section VI. Experimental results, adopting real-world CPA attacks, are discussed in this section, along with Signal-to-Noise Ratio, Mutual Information analysis and t-test on real traces, comparing the SC-DDPL against WDDL and MDPL implementations. Finally, conclusions are reported in Section VII.

## II. Review of The Time Enclosed Logic Protocol

The Time Enclosed Logic (TEL) principle, firstly introduced in [12] and then formalized in [13], has the purpose to mitigate the influence of the electrical mismatches on the data dependence of the current consumption in a dual rail design. In DPL implementations, the presence of capacitive mismatches on two differential wires (see Fig. 1) impacts critically on the security level of the device, since information leakage still exists through dynamic power. Denoting as $C_{L1}$ and $C_{L2}$ the total parasitic capacitance at the *true* and *false* output nodes of a logic gate respectively and referring to Fig. 1, it is evident that unbalanced routing and mismatches in active devices result in $C_{L1} \neq C_{L2}$, and then:

$$V_{DD}^2 f_{ck} C_{L1} \neq V_{DD}^2 f_{ck} C_{L2}. \quad (1)$$

Differently from the conventional RTZ protocol adopted in DPL implementations which encodes the logic value as an amplitude level, the logic value is encoded as a time difference (more specifically the sign of the time distance between the edges of the two dual rail signals) when adopting the TEL protocol. The operation of this signaling style is based on three phases for each clock cycle:

- Pre-charge phase, with time duration $t_{pre}$;
- Evaluation phase, with time duration $t_{eval}$;
- Post-evaluation phase, with time duration $t_{post}$.

Referring to Fig. 2, during $t_{pre}$, both signals $A$ and $\bar{A}$ are low and all parasitic capacitances are at the same voltage.

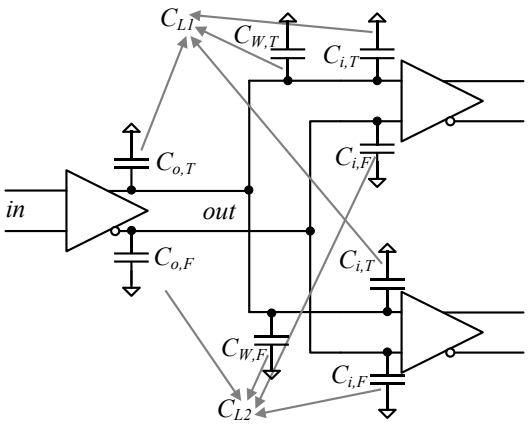



Fig. 1. Capacitive mismatch on a RTZ-based DPL logic gate.

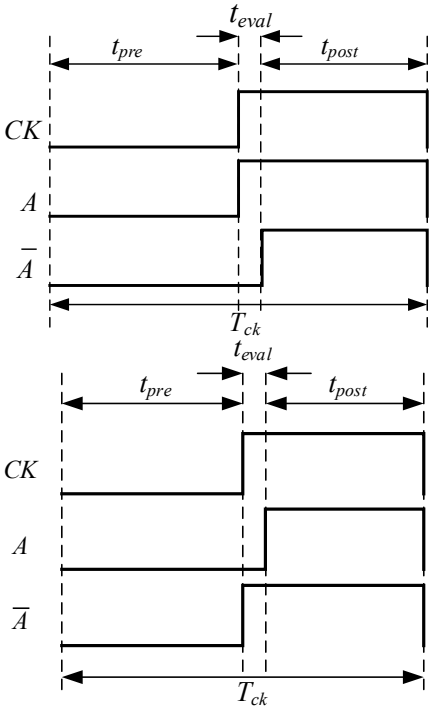



Fig. 2. TEL signaling for logical '1' (a), logical '0' (b).

During $t_{eval}$, both signals $A$ and $\bar{A}$ make a low to high transition encoding a logic '1' if $A$ rises before $\bar{A}$ (see Fig. 2a) and a logic '0' if $A$ rises after $\bar{A}$ (see Fig. 2b). Finally, during $t_{post}$, both $A$ and $\bar{A}$ remain high. Thanks to this post-evaluation phase information leakage due to memory effect is ideally avoided.
TABLE I shows the comparison of the dynamic power consumption over a clock cycle for RTZ and TEL encoding for $C_{L1} \neq C_{L2}$, ($Y$ and $\bar{Y}$ denote the true and false outputs of a generic dual rail logic gate, $P_{dyn}^{1st}$, $P_{dyn}^{2nd}$ and $P_{dyn,TOT}$ denote the power consumption during the first semiperiod, the second semiperiod and the whole clock cycle respectively).

As we can notice from TABLE I, the TEL encoding allows to ensure a constant dynamic power consumption $P_{dyn,TOT}$ over a clock period, providing the power balancing also in presence of capacitive mismatch due to unbalanced routing.

TABLE I.
COMPARISON OF THE DYNAMIC POWER CONSUMPTION OVER A CLOCK CYCLE FOR RTZ AND TEL ENCODING IN THE PRESENCE OF CAPACITIVE MISMATCH ($C_{L1} \neq C_{L2}$)

| | $(Y, \overline{Y})$ | 1st Semiperiod | | 2nd Semiperiod | |
|---|---|---|---|---|---|
| | | $Y$ | $\overline{Y}$ | $Y$ | $\overline{Y}$ |
| **RTZ** | (0,1) | $0 \rightarrow 0$ | $0 \rightarrow 1$ | $0 \rightarrow 0$ | $1 \rightarrow 0$ |
| | (1,0) | $0 \rightarrow 1$ | $0 \rightarrow 0$ | $1 \rightarrow 0$ | $0 \rightarrow 0$ |
| **TEL** | (0,1) | $0 \rightarrow 1$ | $0 \rightarrow 1$ | $1 \rightarrow 0$ | $1 \rightarrow 0$ |
| | (1,0) | $0 \rightarrow 1$ | $0 \rightarrow 1$ | $1 \rightarrow 0$ | $1 \rightarrow 0$ |

| | $P_{dyn}^{1st}$ | $P_{dyn}^{2nd}$ | $P_{dyn,TOT}$ |
|---|---|---|---|
| **RTZ** | 0 | $V_{DD}^2 C_{L2} f_{ck}$ | $V_{DD}^2 C_{L2} f_{ck}$ |
| | $V_{DD}^2 C_{L1} f_{ck}$ | 0 | $V_{DD}^2 C_{L1} f_{ck}$ |
| **TEL** | $V_{DD}^2 C_{L1} f_{ck}$ | $V_{DD}^2 C_{L2} f_{ck}$ | $V_{DD}^2 (C_{L1} + C_{L2}) f_{ck}$ |
| | $V_{DD}^2 C_{L1} f_{ck}$ | $V_{DD}^2 C_{L2} f_{ck}$ | $V_{DD}^2 (C_{L1} + C_{L2}) f_{ck}$ |

The most important property of the TEL encoding is that all the relevant information leakage is enclosed in the duration of the evaluation phase $t_{eval}$. To better clarify this point, let us assume that that the attacker has limited resources in terms of time resolution (and bandwidth) for monitoring the power consumption of the cryptographic device, as will be further discussed in Section V-C. If the sampling period of the Digital Storage Oscilloscope (DSO) used to record the current traces is greater than $t_{eval}$, no relevant power samples can be captured, and the attacker will not be able to get useful information. This simple consideration can be enforced by the presence of other low-pass effects (e.g. power grid RC parasitics), which can filter off relevant information directly on-chip or on-board.

From the above discussion it is evident that in order to maximize the security level we have to design $t_{eval}$ to be as short as possible.

To understand the factors that limit the possibility to shorten $t_{eval}$, we have to focus on the behavior of the TEL flip flop and on the concept of critical path of a time encoded logic [13].

The behavior of a TEL flip flop can be summarized as follows:

- The TEL flip flop detects the TEL datum ('1' if $D$ rises before $\overline{D}$ '0' if $D$ rises after $\overline{D}$);
- The TEL flip flop regenerates the TEL datum at the output (the time distance between $Q$ and $\overline{Q}$ is set to the nominal $t_{eval}$ at the output of the flip flop).

According to this definition it is evident that the "setup time" of a TEL flip flop is related to the ability of discriminating which signal rises first between D and $\overline{D}$. If we consider a certain number N of cascaded gates between two TEL flip flops (i.e. a combinatorial path), at each level of logic we have that the effective $t_{eval}$ can be reduced with respect to the nominal $t_{eval}$ due to process variations and mismatch effects. In this context the critical path is defined as the path which results in the minimum value of the effective $t_{eval}$ across the whole design. A TEL design operates properly if the effective $t_{eval}$ of the critical path is sufficient for a TEL flip flop to detect the logic value encoded in time domain.

Therefore, the nominal $t_{eval}$ of a TEL design represents a sort of time margin which is degraded across a logic path: for a given technology node, reducing $t_{eval}$ reduces the maximum number of gates which can be reliably cascaded in a combinatorial path.

## III. STANDARD CELL DELAY-BASED DUAL-RAIL PRE-CHARGE LOGIC

In the literature, two logic styles that are based on the TEL principle have been previously presented: the DDPL [12] and iDDPL [14][15]. Both these logic styles are intended to be implemented in ASICs, since they require full custom cells to be compatible with the TEL signaling. The proposed SC-DDPL style aims to provide a solution for thwarting PAAs at gate-level, being TEL compatible and standard-cell based.

### A. TEL Compliance

The TEL encoding scheme requires that the logic circuitry has to meet the property of completeness. The *completeness* is the property of a logic circuit to be represented by symbolically complete logic expression, and a set of Boolean function is said *functionally complete* if and only if all other Boolean functions can be constructed from this set [16]. 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, (TEL *NULL* value is when both complementary wires have the same value throughout the entire clock cycle), 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 [16].

The property of completeness implicitly requires that each gate has to satisfy following Eq. (2):

$$\begin{cases} out = F_1(D_1, D_2, \dots, D_n, \overline{D_1}, \overline{D_2}, \dots, \overline{D_n}) \\ \overline{out} = F_2(D_1, D_2, \dots, D_n, \overline{D_1}, \overline{D_2}, \dots, \overline{D_n}) \end{cases} \quad (2)$$

and that each signal has both a low to high and a high to low transition in a clock cycle. These requirements can be satisfied if the NAND operator is used as basic function to derive every Boolean function needed in a cryptographic device. In [5], a simpler expression is used for RTZ-based WDDL, where $F_1$ depends only on non-asserted inputs and $F_2$ depends only on asserted inputs. As additional requirement [5], functions $F_1$ and $F_2$ have to be *positive monotonic* [17].

If Eq. (2) is satisfied, 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 logic '0', the output values of $F_1$ and $F_2$ are '0'. In the post-evaluation, all input values are set to logic '1', and the output values are set, in turns, to '1'. In TEL encoding, all signals have 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 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 operator, and since the NAND function is the minimum complete function, it can be adopted to design a self-synchronized TEL-based gate.

### B. Standard-cell based TEL implementation

Since the NAND function is able to provide a suitable basis for building a TEL-compatible gate, we have chosen to design SC-DDPL gates using the NAND function as building block. In order to satisfy Eq. (2), the SC-DDPL combinational gate template is designed on two evaluation levels using all-NANDs approach, as shown in Fig. 3. Basic Boolean operands are re-written using *product of products*, by means of DeMorgan's equivalences. In the following, the AND/NAND functions are given to better explain the philosophy behind the SC-DDPL gate design:

$$F_1 = \overline{\overline{A \cdot B}} = A \cdot B = AND \tag{3}$$

$$\begin{aligned} F_2 &= \overline{\overline{(\bar{A} \cdot \bar{B})} \cdot \overline{(\bar{A} \cdot B)} \cdot \overline{(A \cdot \bar{B})}} = \\ &= \overline{[(A+B) \cdot (\bar{A}+B) \cdot (A+\bar{B})]} = \\ &= \overline{[A + A \cdot (B+\bar{B})] \cdot (\bar{A}+B)} = \\ &= \overline{A \cdot \bar{A} + A \cdot B} = \overline{A \cdot B} = NAND \end{aligned} \tag{4}$$

Eq. (4) represents the equivalence of non-minimal NAND function, using formalism in Eq. (2). Using Eq. (3)-(4), we can design the AND/NAND in SC-DDPL style, adopting all-NAND design. The first evaluation level will be composed by four 2-inputs NAND (namely NAND2), that will compute the NAND of each combination of the single-ended inputs composing TEL pairs. The second evaluation level can be implemented using 2 3-inputs NAND (namely NAND3). The resulting design is shown in Fig. 4. On the $F_1$ branch, the NAND3 has been adopted to preserve the symmetry of the design. It has to be noted that the AND/NAND operator is designed using minimum NAND2 and NAND3 CMOS gates.

It has to be noted that this design is not able to guarantee internal symmetry in terms of propagation delay between the two output paths. In fact, the NAND2 that computes $\overline{A \cdot B}$ has a fan-out which is three times greater than the fan-out of the others NAND2 gates' one. In order to make the AND/NAND gate internally symmetric, the design in Fig. 4 has been modified according to Fig. 5a. This fan-in balancing technique is similar to the load-balance DIMS in asynchronous logic [8]. Anyway, it is worth noting that SC-DDPL exhibits a synchronous behavior (evaluation starts at the rising edge of the clock) and fan-in balancing is not used to guarantee the correct functional behavior of the logic, but to improve the symmetry in order to allow a very short $t_{eval}$ thus moving the leakage at very high frequencies [13] (where it can be filtered out by means of on chip capacitances) as specified by the TEL protocol.

At functional level, the presence of $V_{DD}$ on two unused inputs of the NAND3 on $F_1$ branch will not alter the functionality of the gate while providing the correct internal uniformity of the output time constant on the 1st evaluation layer. Therefore, the OR/NOR and XOR/XNOR gates have been designed accordingly, and their schematic are reported in Fig. 5b-c respectively.

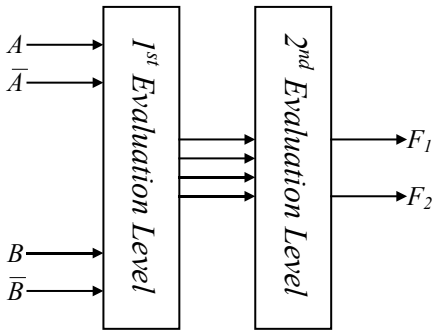



Fig. 3. SC-DDPL 2-inputs combinational gate template.

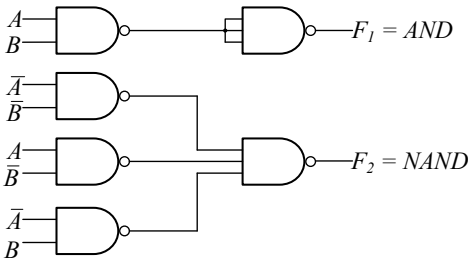



Fig. 4. SC-DDPL AND/NAND gate designed with the formulation in Eq.(3)-(4).

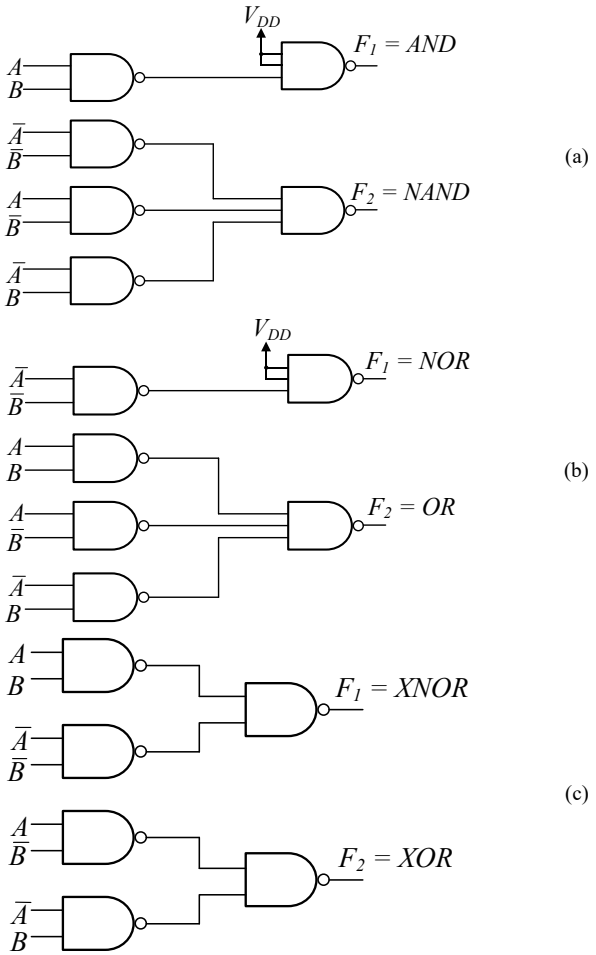
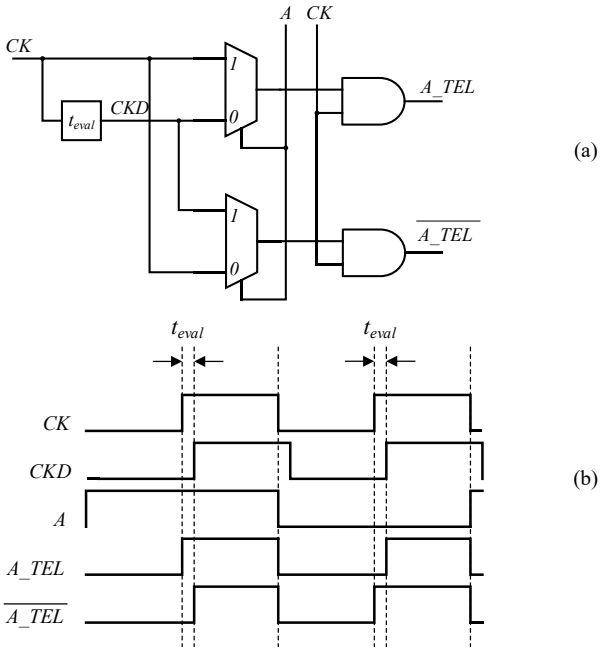
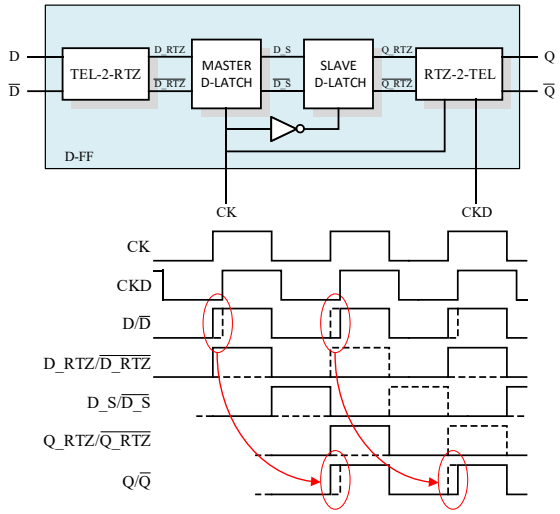



Fig. 5. SC-DDPL basic 2-input combinational gates, with internally balanced time constants: AND/NAND (a), OR/NOR (c) and XOR/XNOR (c).




(a) (b)

Fig. 6. CMOS-to-TEL converter and time diagram.




(a) (b)

Fig. 7. Block scheme (a) and time diagram (b) of the SC-DDPL flip-flop in [18].

### C. CMOS-to-TEL Standard-cell converter

A simple solution to design a CMOS-to-TEL converter is depicted in Fig. 6. The single rail signal *A* is used as selection signal for two 2:1 multiplexers, that receive *CK* and *CKD* as inputs, in a cross-coupled fashion. The signal *CKD* is a shifted replica of *CK*. The time delay between *CK* and *CKD* is set to $t_{eval}$. Depending on the value of signal *A*, the output of the two multiplexers will be *CK*/*CKD* or *CKD*/*CK*. Two AND2 gates perform the Boolean product of these multiplexed signals with *CK*, providing the synchronization needed for a correct TEL encoding of converted signals *A_TEL* and $\overline{A\_TEL}$.

### D. SC-DDPL Flip-flop

To complete the library, we briefly recall the structure of the adopted standard-cell TEL-compatible flip-flop, which has been previously presented by some of the authors in [18]. The flip-flop is composed by 4 cascaded layers, as shown in Fig. 7, delivering a master-slave sequential element. The first layer is a NAND SR-latch, which maps the incoming TEL signal into a RTZ pair. The second and the third layers are designed as OR-gated NOR SR-latches, driven by opposite phases of master clock *CK*. An output layer will reconstruct the TEL signaling, by OR-ing and AND-ing the signal with *CKD* and *CK* respectively.

## IV. Energy And Frequency Security Metrics

The design of a secure implementation has to be evaluated through the assessment of the information leakage. In the context of gate-level countermeasures, it is useful to analyze the power variability due to data-dependency through an energy analysis throughout the clock cycle. In this work, we have adopted both energy and frequency domain security metrics to evaluate the capability of the SC-DDPL combinational gates to counteract PAAs.

In the literature, one of the most 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 as:

$$E = \int_0^{t_{ck}} V_{DD} i(t) dt \tag{5}$$

Using the definition in [6], we define the Normalized Energy Deviation (NED) as follows:

$$NED = \frac{\max(E) - \min(E)}{\max(E)} \tag{6}$$

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):

$$NSD = \frac{\sigma_E}{E_{AV}} \tag{7}$$

where $E_{AV}$ and $\sigma_E$ are the average and standard deviation of the energy per cycle respectively.

Since the SC-DDPL is a TEL-based logic style, it is necessary to evaluate the frequency contents of the information leakage. In [13], Bongiovanni *et al.* have introduced a new criterion 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 a reference gate (e. g. inverter or XOR) for the two data transitions:

$$\Delta FFT = |FFT_0 - FFT_1|^2 \tag{8}$$

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

$$FED = [\sigma_1\ \sigma_2\ \dots\ \sigma_f\ \dots\ \sigma_F] \quad (9)$$

$$\sigma_f = \frac{1}{N}\sqrt{\sum_{i=1}^{N}[FFT_i(f) - \overline{FFT}(f)]^2} \quad (10)$$

where $f=1,2,\dots f\dots,F$ are the frequency bins at which the FFT of the current consumption traces is computed and $\sigma_f$ is the generic sample $f$ of the FED vector computed as in (10). The one dimensional vector $\overline{FFT}$ contains the averages over the $N$ input vectors of the points of the FFT of the current traces. According to this definition, the FED represents a trace made up of F bins in which each bin is the standard deviation in the frequency domain of the information leakage in the dynamic power consumption due to data-dependency.

## V. Evaluation of the Security Level of the SC-DDPL

### A. Logic Gates

A first evaluation of the security level of the proposed SC-DDPL gates has been carried out by accurate simulations in Cadence Virtuoso, using the 40nm STMicroelectronics design kit, which supports BSIM4 models for the best accuracy. Schematics in Fig. 5 have been implemented using only standard-cells from the CMOS standard cell 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 [13], [19], [20], [21]. The time resolution of the simulation has been set to 10ps, providing a bandwidth of 50GHz. In order to simulate capacitive mismatch, output load capacitors have been varied according to the Mismatch Factor (MF) defined as follows:

$$MF = \frac{C_{L2}}{C_{L1}} \quad (11)$$

with MF varying from 1 to 4 and $C_{L1}$ set to 1fF. MF=1 represents no mismatch condition, while MF=4 represents extreme mismatch. To get a fair comparison, we have adopted the WDDL [5] as DPL standard-cell-based reference. Also WDDL combinational gates have been designed using standard cells from the same library, adopting the same simulation setup.

Results for NED and NSD values for both logic families are reported in TABLE II and TABLE III. It has to be noted that also for MF=1, both NED and NSD for SC-DDPL are strongly reduced compared to WDDL. The presence of mismatch impacts critically on WDDL implementation, since both NED and NSD increase significantly as MF increases. In the SC-DDPL implementation, the NED and NSD is approximatively constant with increasing MF, remarking the capability of the proposed logic style to limit the possibility to mount a successful PAAs even in the presence of capacitive mismatch. The maximum values of the NED and NSD for SC-DDPL are 2.87% and 1.30% respectively, which means a meaningful reduction compared to WDDL.

The simulation testbench used for the evaluation of $\Delta FFT$ and FED metrics is shown in Fig. 8.

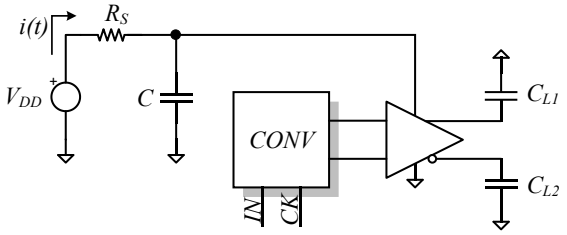



Fig. 8. Testbench used to evaluate $\Delta FFT$ and FED plots.

TABLE II
NED and NSD values for SC-DDPL combinational gates

| | MF=1 | MF=2 | MF=3 | MF=4 |
|---|---|---|---|---|
| | | **NED** | | |
| 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% |
| | | **NSD** | | |
| 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 III
NED and NSD Values for WDDL Combinational Gates

| | MF=1 | MF=2 | MF=3 | MF=4 |
|---|---|---|---|---|
| | | **NED** | | |
| 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% |
| | | **NSD** | | |
| 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% |

Since there are no explicit inverter gates in SC-DDPL and WDDL, we have used the XOR/XNOR gate to compare the $\Delta FFT$, 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 to compute the FFT of current traces from the simulations. $\Delta FFT$ plots are shown in Fig. 9 and Fig. 10 for different mismatch conditions.

At low frequency, $\Delta FFT$ is around -115dB for SC-DDPL 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 that some lobes are visible at multiple of 1GHz, due to higher order effects, which are not relevant for our analysis.

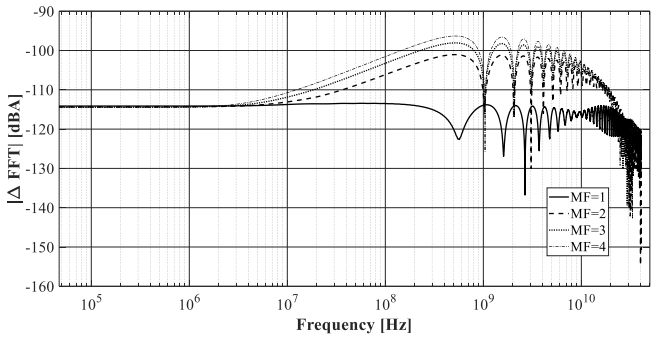



Fig. 9. $\Delta FFT$ vectors for SC-DDPL XOR/XNOR gate used as inverter, with $t_{eval}$=1ns.

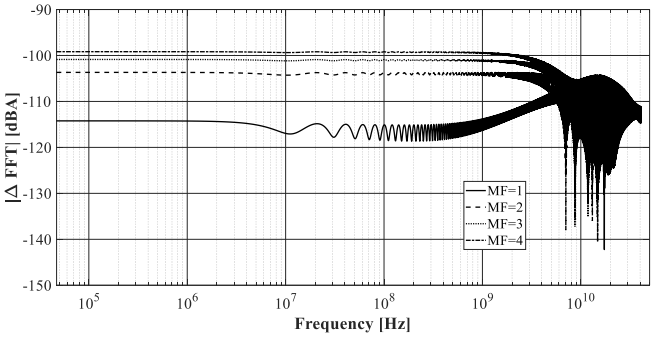



Fig. 10. $\Delta FFT$ vectors for WDDL XOR/XNOR gate used as inverter.

The WDDL shows approximately the same $\Delta FFT$ value of the SC-DDPL at low frequency in no mismatch condition. If MF>1, $\Delta FFT$ plots shows higher values even at low frequency (+10dB).

At extreme condition (MF=4), the low frequency $\Delta FFT$ is approximately -99dB, which is significantly higher than the respective SC-DDPL. These results are in accordance with TABLE II and TABLE III since it is sufficient a slight mismatch (MF≥2) to strongly increase information leakage that the adversary can exploit from dynamic consumption. Moreover, the low-frequency side of $\Delta FFT$ is extremely relevant from the adversary point of view [13].

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 SC-DDPL, we can implement a simple low-pass filter with the aim to flatten the $\Delta FFT$ plots with MF>1.

Assuming $R_s = 100\Omega$ in the testbench of Fig. 8, the minimum value of the on-chip capacitor to flatten $\Delta FFT$ plots is expressed according to [13] as:

$$C = C^{opt} \approx \frac{1}{2\pi f_c R_s} \cong 53pF \qquad (12)$$

As a further validation we have carried out 500 Monte Carlo mismatch simulations in the ADE XL environment and using accurate statistical models of MOS transistors provided by the IC manufacturer. In these simulations the nominal $t_{eval}$ has been set to 1ns (by setting the delay between the CK and CKD signals at the input of the SC-DDPL Gates), and the output evaluation time for SC-DDPL AND/NAND, OR/NOR and XOR/XNOR gates has been analyzed.

TABLE IV
$\overline{t_{eval}}$ AND $\sigma_{t_{eval}}$ OF SC-DDPL GATES

| | AND/NAND | OR/NOR | XOR/XNOR |
|---|---|---|---|
| $\overline{t_{eval}}$ | 998.51ps | 995.12ps | 992.02ps |
| $\sigma_{t_{eval}}$ | 5.83ps | 5.48ps | 4.49ps |
| CV | 0.58% | 0.55% | 0.45% |

TABLE V
$\overline{NED}/\overline{NSD}$ AND $\sigma_{NED}/\sigma_{NSD}$ OF SC-DDPL GATES

| MF=1 | AND/NAND | OR/NOR | XOR/XNOR |
|---|---|---|---|
| $\overline{NED}$ | 0.036 | 0.041 | 0.033 |
| $\sigma_{NED}$ | 0.0012 | 0.0079 | 0.0051 |
| $\overline{NSD}$ | 0.0134 | 0.0158 | 0.0151 |
| $\sigma_{NSD}$ | 0.0012 | 0.0033 | 0.0025 |
| MF=3 | AND/NAND | OR/NOR | XOR/XNOR |
| $\overline{NED}$ | 0.0366 | 0.0373 | 0.0347 |
| $\sigma_{NED}$ | 0.0114 | 0.0076 | 0.0098 |
| $\overline{NSD}$ | 0.0142 | 0.0145 | 0.0149 |
| $\sigma_{NSD}$ | 0.0043 | 0.0031 | 0.0042 |

The average $\overline{t_{eval}}$ and the standard deviation $\sigma_{t_{eval}}$ of the output evaluation time of the aforementioned combinational gates, as well as its coefficient of variation (CV) are reported in TABLE IV. Additional Monte Carlo simulations have been carried out in order to thoroughly extend the analysis for intra-gate mismatch. The NED/NSD of the SC-DDPL gates under process variations have been collected over a sample of 500 Monte Carlo runs for two different values of MF. TABLE V reports the average values $\overline{NED}/\overline{NSD}$ and the standard deviations $\sigma_{NED}/\sigma_{NSD}$ of the *NED/NSD* security metrics for *MF*=1 and *MF*=3. The results in TABLE V highlight the robustness of SC-DDPL gates to mismatch variations.

### *B. Present S-BOX*

To compare SC-DDPL and WDDL on a cryptographic function we have implemented the S-BOX in PRESENT-80 algorithm [22] in both logic styles. The S-BOX has been designed adopting K-map synthesis and using only 2-input Boolean operands. For this comparison we have chosen MF=3 since it can be suitable to model the two following scenarios [18]:

- ASIC implementations without routing constraints;
- FPGA implementations without optimized *place&route*.

The testbench used for the evaluation of FED is the same of Fig. 8. Results of the FED analysis are shown in Fig. 11. It has to be noted that the behavior of the SC-DDPL implementation of the S-BOX is similar to $\Delta FFT$ plots in Fig. 9. 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 SC-DDPL (+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 SC-DDPL versus the WDDL implementation of the Present S-BOX is reported in TABLE VI.

### *C. Adversary modeling*

The use of highly accurate SPICE-level simulations is very important from a pre-silicon assessment perspective [23].

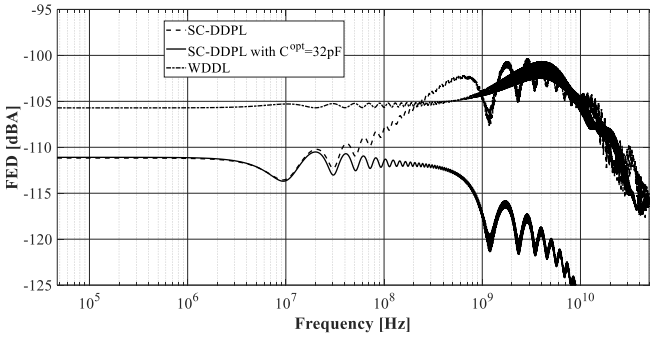



Fig. 11. FED plots of the implementation of the PRESENT-80 S-BOX in SC-DDPL (blue), SC-DDPL with $C^{opt}$=32pF (green) and WDDL (red) style for MF=3.

Nevertheless, such high-accuracy simulations allow the designer to evaluate the capability of a *Perfect Adversary* to extract information from the device. The *Perfect Adversary* model has the following properties:

- Infinite bandwidth in collecting the specific side-channel.
- Infinite storage capability (unbounded sampling complexity).

However, this model does not hold in practice, since the entire measurement equipment and the device itself (e.g. presence of on-chip filter and/or analog countermeasures [24]) provide a limited bandwidth from an adversarial point of view. Furthermore, regarding the measurement setup, a Digital Storage Oscilloscope (DSO) used to collect and digitize the power consumption of the device under test/attack, is equipped with a real analog front-end, that has a limited bandwidth. Moreover, the DSO's analog-to-digital converter has a limited time resolution and number of bits to represent the sampled data, that implies limited ability to observe fast phenomena and upper bounded minimum detectable signal. In addition, the sampling complexity of a *real* adversary is always limited, and thus it limits the possibility to filter-off noise by averaging. For all these reasons, in the context of TEL signaling, our assumptions on the adversary model are more realistic and closer to a real-world scenario: the adversary has limited resources in time resolution and bandwidth.

Leveraging on this aspect, we have performed simulations with a time resolution of 20ps (50GS/s) on the 4-bit crypto-core based on the first round of PRESENT-80 reported in Fig. 12 and implemented with the proposed SC-DDPL and with WDDL, as reference. Registers have been implemented according to the secure standard-cell TEL-compatible in [18].

We distinguished three practical scenarios, that aim to represent typical DSO limitations:

- Case 1: high-grade DSO, with sampling rate of 10GS/s;
- Case 2: mid-grade DSO, with sampling rate of 1GS/s;
- Case 3: low-grade DSO, with sampling rate of 500MS/s.

The working conditions have been set as in Section V-A, and we have chosen MF=3 as in Section V-B. No additional capacitance has been added on the supply line, to guarantee a simple interpretation of the results. The evaluation phase $t_{eval}$ for the SC-DDPL has been set to 1ns.

TABLE VI
AREA AND POWER CONSUMPTION COMPARISON FOR THE PRESENT-80 S-BOX IMPLEMENTATION.

| Implementation | # Device | Area Overhead | $P_{AV}$ (@10MHz) | Power Overhead |
|---|---|---|---|---|
| CMOS | 132 | x1 | 0.60μW | x1 |
| WDDL | 360 | x2.72 | 1.02μW | x1.7 |
| SC-DDPL (This work) | 948 | x7.18 | 2.52μW | x4.2 |

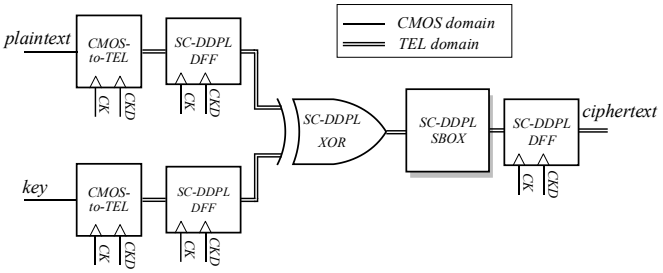



Fig. 12. RTL-level schematic of the implementation of the 4-bit PRESENT crypto-core.

For both implementations, the key has been set to $(5)_2$ and the output value of the S-BOX has been used as target for the CPA attacks adopting the Hamming Weight power model:

$$out = SBOX(key \oplus plaintext) \quad (13)$$

We generated 100k traces for each core and for each case study. It has to be noted that we did not consider explicitly the presence of timing uncertainty of the DSO, which may represent a source of additional limitation to the adversary's capability in extracting information. We left this point as an open question for future research.

*1) Case 1:* the sampling rate has been reduced by a factor of 5 before mounting the CPA attack. The final time resolution is 100ps/pts, which allows the attacker to collect 10 samples for the evaluation phase. The CPA attack yields to a successful attack with ~37k measurements for the SC-DDPL core and with ~1000 for WDDL, as shown in Fig. 13. It has to be mentioned that for the SC-DDPL core, the correct key's peak can be observed exactly on during the evaluation phase (9 samples out of 10), which confirms TEL's properties in Section II. In the WDDL implementation, we have two correlation peaks, but the relevant one takes place during the transition from the evaluation to the pre-charge phase.

*2) Case 2:* In the mid-grade DSO case study, the sampling rate is reduced down to 1GS/s, which means a time resolution of 1ns/pts. Case 2 can be considered as the DSO common choice (1GS/s DSOs have a cost in the range 5-10k€). The evaluation phase for the SC-DDPL implementation is now sampled with only a single time sample. In fact, in this case, the CPA attack is still successful at ~77k traces, but the margin between the correct key and the highest ranked wrong key is very small, as shown in Fig. 14. We believe that the DSO jitter performance could have a strong impact in this case, since the evaluation phase is sampled with the minimum number of time samples

possible. The WDDL crypto-core has shown a distinct peak for the correct key with ~1100 traces.

*3) Case 3:* the final sampling rate has been reduced to 500MS/s, which means no relevant time samples have been captured for the SC-DDPL implementation. DSOs with similar sampling rates are widely diffused, since they do not have a prohibitive cost. As expected, the CPA attack was not able to retrieve the correct key within the data set generated for the simulated experiment (measurement to disclosure higher than 100k), as shown in Fig. 15. According to TEL assumptions in Section II, the sampling rate of the simulated DSO in Case 3 is not enough to capture data-dependency in the SC-DDPL implementation. Moreover, the correlation coefficient of the correct key is way lower compared to the first ranked wrong key. Regarding the WDDL implementation, we have found that the number of traces needed to recover successfully the key is ~6.6k. This result is perfectly in accordance with the FED analysis, where the WDDL shown higher date-dependency at low-frequency compared to the TEL-compatible circuit. In the SC-DDPL, the correlation coefficient of the correct key has been found reduced of a factor of 6.43 compared to its WDDL counterpart.

We have then performed additional simulated attacks on the 4-bit crypto-core in Fig. 12, adopting a reduced nominal $t_{eval}$, which has been set to 500ps. With $t_{eval}$ set to 500ps the mid-grade DSO with sampling rate of 1GS/s is not adequate to reveal the secret key. It has to be noted that the MTD does not change with high-grade oscilloscope (sampling rate of 10GS/s), which corresponds to 38k traces in this case. This last experiment showed, as expected, that a reduction of the evaluation period leads to a more demanding minimal sampling rate that the adversary shall use to perform a successful attack.

## VI. FPGA Implementation and Experimental Results

To evaluate and assess the security of the proposed SC-DDPL by means of experimental results, the 4-bit crypto-core based on the first round of PRESENT-80 shown in Fig. 12 has been implemented in FPGA referring to SC-DDPL , WDDL and MDPL logic styles. An additional implementation referring to the conventional CMOS logic style has been considered as reference.

Secure designs for FPGAs suffer from several problems related to the intrinsic nature of these reprogrammable devices. In fact, the degrees of freedom for designers are quite limited compared to the ASIC world, enforcing our choice of using a FPGA platform for the validation and comparison of the proposed standard-cell approach.

In literature, several solutions have been proposed to balance capacitive load for dual-rail secure designs. In [11], authors presented a methodology to get a balanced routing on Xilinx FPGAs 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.

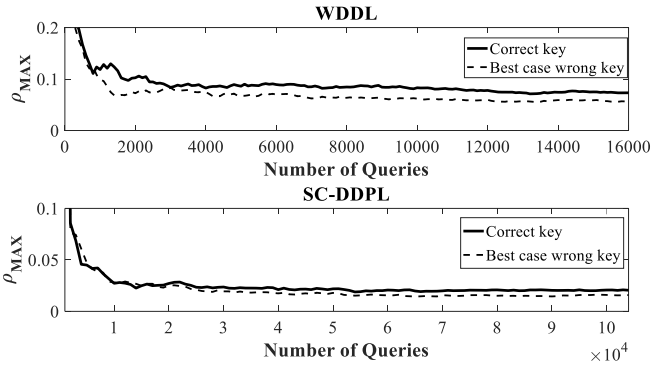



Fig. 13. Correlation coefficient curves versus number of measurements for WDDL and SC-DDPL implementations, adopting the output of the S-BOX as target intermediate function with sampling rate 10GS/s.

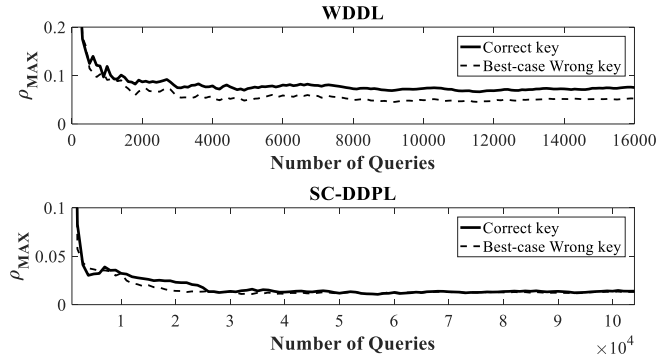



Fig. 14. Correlation coefficient curves versus number of measurements for WDDL and SC-DDPL implementations, adopting the output of the S-BOX as target intermediate function with sampling rate 1GS/s.

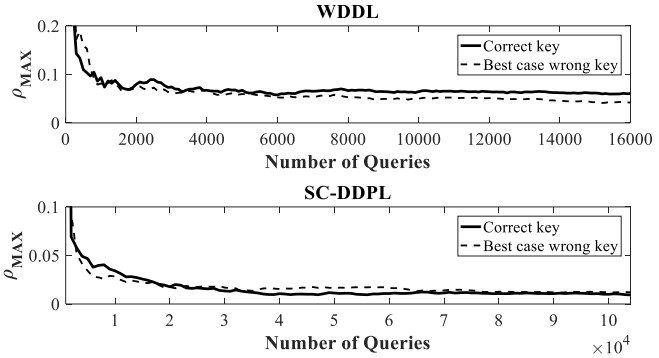



Fig. 15. Correlation coefficient curves versus number of measurements for WDDL and SC-DDPL implementations, adopting the output of the S-BOX as target intermediate function with sampling rate 500MS/s.

The set of APIs implemented in RapidSmith can be used only for a limited set of devices, as the output .XDL file can be interpreted by Xilinx products. Amouri et al. [25], propose a methodology for mesh-style FPGA similar to the "fat wire" method proposed in [10] for ASIC applications. However, the outcome of these methods will formally not ensure a good balancing in terms of security for deep-scaled FPGAs, since they still suffer the same (and most probably, even worst) critical problem of intra-die variations observed with ASICs. So, it appears clear that FPGAs are the best (and fastest) benchmark to test effectiveness of SC-DDPL to deal with unavoidable capacitive mismatches due to routing unbalance.

As target FPGA device, we have used an Intel Cyclone-IV (65nm technology). To avoid redundancy needed to implement the PRESENT core in SC-DDPL implementation, we have used

*syn_keep* attribute on internal signals of combinational gates, *dont_touch* and *REMOVE_DUPLICATE_LOGIC_OFF* on NAND3 instances. To implement SC-DDPL Flip Flops we rely on the architecture presented in [18]. The Latches required by the architecture in [18] have been implemented by means of interconnections of combinational elements to build a macro structure of NAND SR latches and NOR SR latches thus avoiding the usage of DFF primitives. The generation of *CLK* and *CLKD* has been delegated to the on-chip PLL macro, taking advantage of the capability of this building block to provide a stable phase shift.

It has to be noted that no *place & route* constraints have been taken into account for DPL implementations, in order to guarantee a good coverage of the worst-case scenario, where the capacitive mismatch occurs at its most.

The summary of the resource usage and power consumption for the three designs is reported in TABLE VII. Compared to WDDL, SC-DDPL requires more resources and more power consumption. Compared to the demanding MDPL, the SC-DDPL requires half of the resources (it has to be noted that no fabric registers/flip-flops have been used) and 15% less power. A block scheme of the measurement setup is shown in Fig. 16; we measured the current absorption of the device under test at the core $V_{DD}$ pin, using a Tektronix CT1 inductive probe and a LeCroy WaveSurfer MX-104b, providing a sampling rate of 5GS/s (that corresponds to 200ps/sample). It has to be noted that we have removed every filtering component on the FPGA's board (mostly capacitors), that could filter off PAA signal. For each implementation we have collected $2^{17}$ traces, running each implementation at 2MHz, with a core power supply of 1.2V. The $t_{eval}$ of the SC-DDPL core has been set to 4.17ns, that corresponds to ~21 time samples at 5GS/s. The 4-bit key has been set to $(6)_2$ on all implementations.

Current absorption traces collected on the implementations are shown in Fig. 17 (the encryption takes three cycles). The clock signal in Fig. 17 has been added as a time reference to identify the pre-charge, evaluation and post evaluation (only for SC-DDPL logic style). When the clock signal is low all logic styles are in the pre-charge phase, whereas the evaluation phase starts at the rising edge of the clock signal. For all logic styles except the SC-DDPL the evaluation phase ends at the falling edge of the clock signal. In case of the SC-DDPL logic style, the evaluation phase starts at the rising edge of the clock, its duration time is $t_{eval}$, and after the evaluation phase we have the post-evaluation phase which lasts until the falling edge of the clock. As expected, the dynamic current absorption tends to assume higher values at the beginning of the *evaluation* phase, since all charging events occur at the rising edge of the clock. In WDDL and MDPL implementations we can notice that the current traces are different in the three different clock cycles showing a data dependence. Regarding the SC-DDPL implementation, we can notice that the current absorption tends to not vary from a cycle to another. This aspect can be expected observing that in a TEL implementation, every signal has the same switching activity of the clock signal, ensuring the power balancing property.

TABLE VII
RESOURCE USAGE AND POWER CONSUMPTION FOR THE ALTERA CYCLONE-IV FPGA

| Implementation | LUT Only | Reg. Only | LUT/Reg. Pair | $P_{dyn}^{AVG}$ (@1V2, 2MHz) |
|---|---|---|---|---|
| CMOS | 30 | 6 | 13 | 81.25µW |
| WDDL | 154 | 0 | 30 | 85.95µW |
| MDPL | 784 | 34 | 62 | 268.47µW |
| SC-DDPL (This work) | 486 | 0 | 6 | 228.68µW |

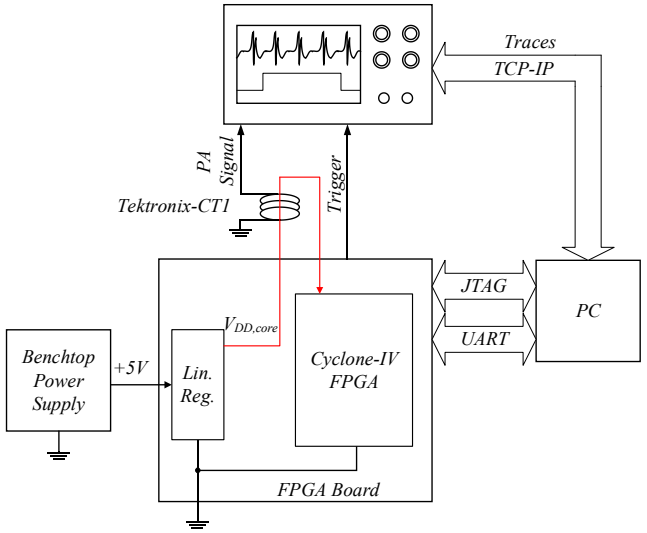



Fig. 16. Block scheme of the measurement setup.

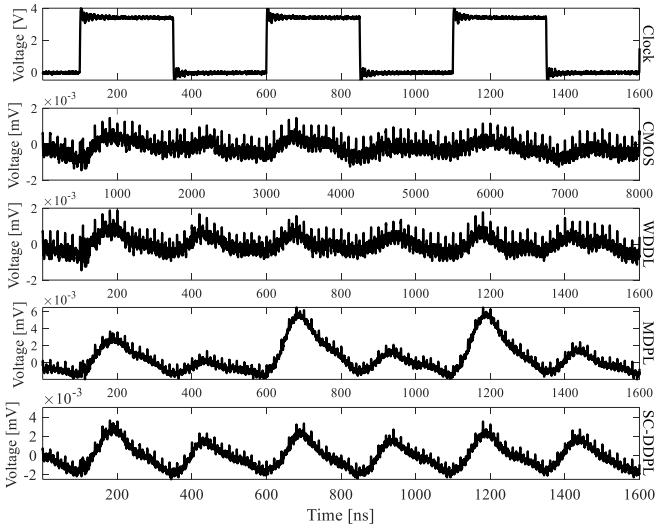
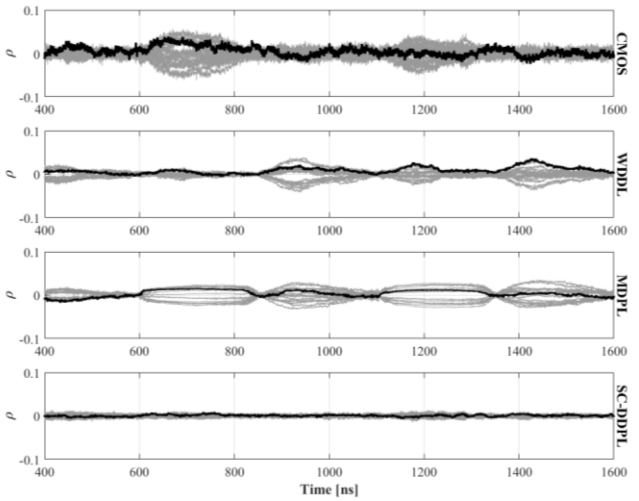



Fig. 17. Measurements on FPGA implementations of the 4-bit PRESENT crypto core (clock signal as temporal reference). The current absorption is converted to a voltage signal through the transresistance of the inductive probe.

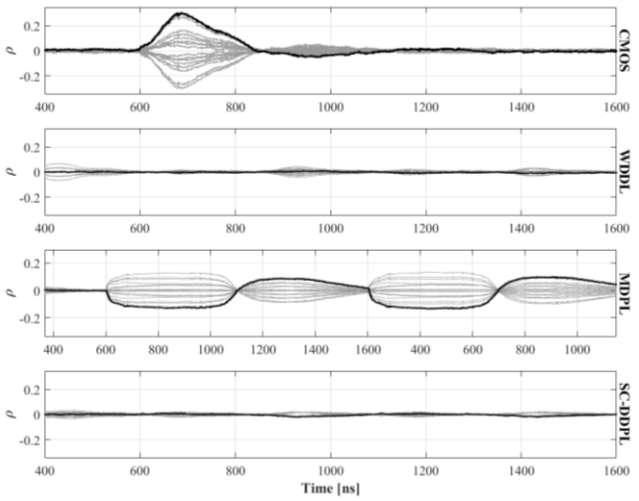
This simple power analysis is supported with practical evaluation of the NED and NSD values reported in TABLE VIII. We can notice that the SC-DDPL implementation exhibits lowest values for both NED and NSD compared to RTZ-based implementations, remarking that the effect of mismatches (unavoidable on FPGA) is strongly reduced.

TABLE VIII
SECURITY METRICS ON THE INTEL CYCLONE-IV FPGA

| Implementation | NED/NSD [%/%] | Min. Meas. To key recovery | max(MI) [bit] | max(SNR) |
|---|---|---|---|---|
| CMOS | 30.30/10.32 | ~750 | 0.395 | 0.162 |
| WDDL | 21.95/7.20 | ~54.5k | 0.022 | 0.010 |
| MDPL | 22.03/6.85 | ~2500 | 0.040 | 0.023 |
| SC-DDPL (This work) | 8.32/2.87 | >132k | 0.013 | 0.002 |




(a)




(b)

Fig. 18. Correlation coefficient curves versus time for CMOS, WDDL, MDPL and SC-DDPL implementations, adopting the output of the S-BOX (a) and output of the XOR (b) as target intermediate function, using 100k traces. Correct key's correlation coefficient curve is plotted in black, while wrong keys' correlation curves are plotted in grey.

CPA attacks results, adopting the output of the S-BOX and the output of the XOR as intermediate values and the Hamming Weight as power model (as widely used in literature [14][26]), are shown in Fig. 18-Fig. *20*. It has to be noted that, using the S-BOX as intermediate value, only the WDDL core has been attacked successfully, with a minimum number of traces for exhibiting the correct key of ~54.5k.

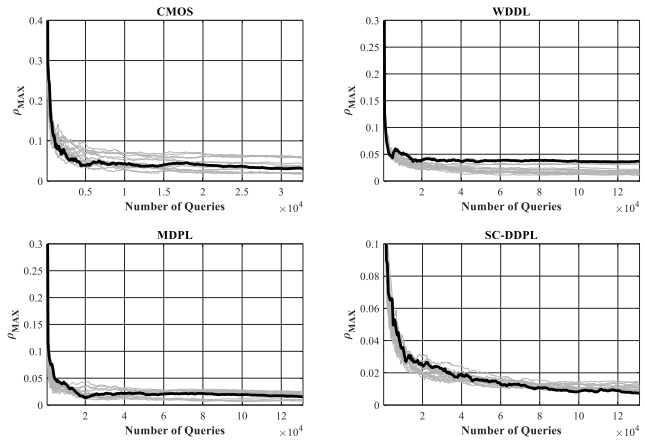



Fig. 19. Plots of correlation coefficient versus number of measurements for CMOS, WDDL, MDPL and SC-DDPL crypto-cores, adopting the output of S-BOX as target intermediate value: correct key's correlation coefficient curve is plotted in black, while wrong keys' correlation curves are plotted in grey.

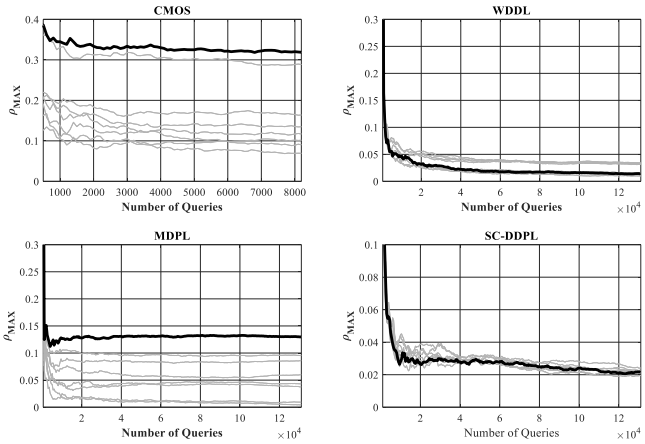



Fig. 20. Plots of correlation coefficient versus number of measurements for CMOS, WDDL, MDPL and SC-DDPL crypto-cores, adopting the output of XOR as target intermediate value: correct key's correlation coefficient curve is plotted in black, while wrong keys' correlation curves are plotted in grey.

In this case, the correlation peak appears at the beginning of the third clock cycle with a maximum around 1.4µs, even if the distance with the best ranked wrong key is very poor ($8x10^{-4}$). Attacks implying the output of the XOR have provided better results. In fact, we have successfully attacked the CMOS and the MDPL implementation at the beginning of the second cycle (the XOR operation is computed in that point in time, along with the S-BOX). The minimum number of traces needed to obtain the correct key in this setup is ~750 for the CMOS and ~2500 for the MDPL. The SC-DDPL has not been successfully attacked in the two CPA setups even adopting the full dataset collected, exhibiting a strong PAA-resistance compared to reference WDDL and MDPL.

For the sake of completeness also a DPA [3] attack has been carried out on all the four bits of the target word of the FPGA implementations. TABLE IX reports the MTD for the attack on each bit for all the considered FPGA implementations and shows that the SC-DDPL is robust also against single bit attacks.

TABLE IX
DPA ATTACK ON THE INTEL CYCLONE-IV FPGA

| | $Bit_0$ (LSB) | $Bit_1$ | $Bit_2$ | $Bit_3$ (MSB) | Max abs. T-test |
|---|---|---|---|---|---|
| CMOS | 3.8k | >132k | >132k | >132k | 26.7 |
| WDDL | 7k | >132k | >132k | >132k | 55.5 |
| MDPL | 24.5k | >132k | >132k | >132k | 15.5 |
| SC-DDPL | >132k | >132k | >132k | >132k | 3.4 |

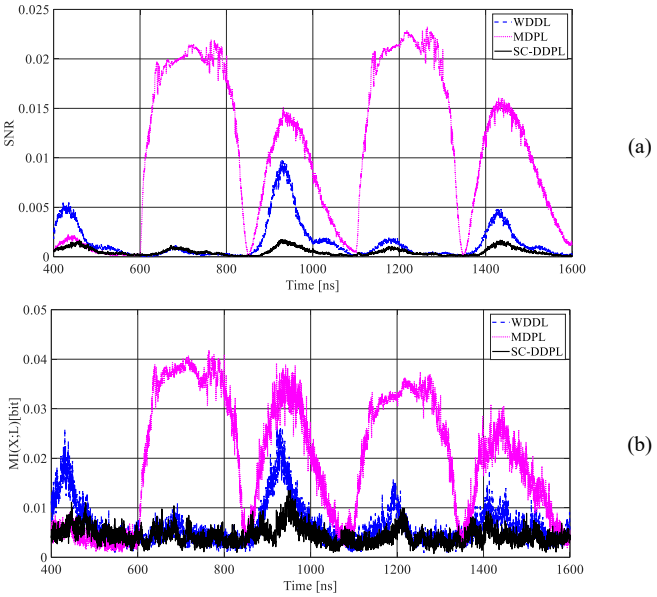



Fig. 21. SNR (a) and estimated mutual information (b) curves for WDDL, MDPL and SC-DDPL implementations.

Further investigation and analysis of the SC-DDPL as a gate-level countermeasure against PAA has been conducted adopting the signal-to-noise ratio (SNR) [17], information theoretic metric, the mutual information (MI) [27] and the popular t-test from the TVLA methodology [28].

- SNR: it is defined as the ratio between the variance of data-dependent power consumption $\sigma^2_{data}$ and the variance of the noise $\sigma^2_{noise}$:

$$SNR = \frac{\sigma^2_{data}}{\sigma^2_{noise}} \tag{14}$$

- MI: it quantifies the amount of information leaked by hardware implementation of a cryptographic algorithm, making use of the definition of Shannon's conditional entropy, assuming Gaussian distributed power samples:

$$MI(X;L) = H[X] - \sum_{x\epsilon X} \Pr(x) \sum_{l\epsilon L} \Pr_{chip}(l|x) \log_2 Pr_{chip}(x|l) \tag{15}$$

where *H[X]* is the entropy of the secret key *X*, $Pr(x)$ the probability of the secret key $x\epsilon X$, and $Pr_{chip}(l|x)$ is the probability of the leakage *l* given the key *x*. $Pr_{chip}(x|l)$ can be derived from $Pr_{chip}(l|x)$ by means of Bayes' theorem.

- T-test: it allows to efficiently assess the presence of data-dependency based on a standardized difference of means (also known as Welch's t-test). The comparison is performed on two classes A and B as follows:

$$t = (\overline{L_A} - \overline{L_B}) \Big/ \sqrt{\frac{\sigma_A^2}{N_A} + \frac{\sigma_B^2}{N_B}} \tag{16}$$

where $\overline{L_A}$ (resp. $\overline{L_B}$) and $\sigma_A^2$ (resp. $\sigma_B^2$) represent the sample mean and sample variance of class A (resp. B), and $N_A$ (resp. $N_B$) represents the cardinality of class A (resp. B). If, for a certain amount of traces, $|t| > 4.5$ the device is considered as leaky. The partition of the traces between class A and B can be done following the *fixed versus random* approach [28] or with the *fixed versus fixed* approach [29].

SNR and MI plots for the DPL implementations are shown in Fig. 21. As we can see, the resulting curves of SNR and MI tend to be very similar, as seen in other works [26][30]. It is clear that the SC-DDPL is able to reduce both metrics, thus, confirming the efficiency in the data-dependency reduction also in presence of capacitive unbalance. The MDPL implementation exhibits higher values of SNR and MI compared to WDDL and SC-DDPL, especially in the interval 600-1100ns, where the input and the key are processed together. Compared to reference WDDL, the SC-DDPL improves the SNR by a factor of 5, and the mutual information by a factor of 2. The t-test leakage assessment has been carried on adopting the fixed versus fixed approach in [29] for efficiency reasons. The maximum absolute values we have obtained for the four implementations are reported in TABLE IX. The SC-DDPL has shown a t-score lower than the conventional 4.5 threshold, while the other three implementations have been found leaky with the same amount of traces ($2^{17}$ in this case).

## VII. CONCLUSION

A novel standard-cell PAA resilient and mismatch tolerant logic style has been presented in this work. The new logic style, named Standard cell, Delay-based Dynamic Differential Logic (SC-DDPL), has been designed adopting the TEL signaling instead of the classical RTZ, used in most common DPL gate-level countermeasures. The TEL encoding makes use of a very short evaluation phase duration to deal with security weakness due to capacitive mismatches on differential wires, which are unavoidable in deep scaled nanometer technologies. Since the evaluation phase is very short, the data-dependent component in the dynamic power consumption is relevant only at very high frequencies, as $\Delta FFT$ and FED analysis have shown. In the case of SC-DDPL, high frequency data-dependent leakage can be easily eliminated by means of proper on-chip filtering, as shown in Section V, or taking advantage of on-chip capacitances, by means of *decap* cells, MIM capacitors and other on-chip circuitry's parasitics. A simulated comparative analysis adopting energy and frequency security metrics is given in the paper, performed on 40nm STMicroelectronics design kit, using the WDDL style as RTZ-based DPL reference. It has been shown that capacitive mismatches compromise the ability of WDDL to counteract PAAs. The SC-DDPL exhibits strongly reduced NED (down to a factor x42) and NSD (down to a factor x64) metrics, remarking its ability to tolerate electrical mismatches. The analysis performed by means of frequency-based metrics has confirmed the capability of the

proposed approach to move the residual data-dependency in the power consumption to high frequency also in presence of mismatch. Within this framework, we have simulated different attack scenarios, regarding an adversary with limited bandwidth and sampling rate. Our investigation has highlighted that the SC-DDPL is able to explicitly counteract PAAs, assuming that the adversary has some concrete (and practice in the real world) limitations, due to non-ideal measurement setups.

As a further validation, we have implemented on a Intel Cyclone IV FPGA a 4-bit crypto-core based on the first round of PRESENT-80 referring to SC-DDPL, WDDL and MDPL logic styles. An extensive measurement campaign, comparing the proposed implementation against WDDL and MDPL counterparts, has shown that the proposed SC-DDPL outperforms both reference DPLs in the two CPA setups investigated. More specifically, the SNR and MI metrics are reduced by a factor of 5 and 2, compared to WDDL, which has shown the best performance among the two RTZ-based DPL cores. This confirms also under a leakage assessment perspective that the SC-DDPL can be considered PAA and mismatch tolerant.

The resource utilization of SC-DDPL is about 2.7 times higher than that of WDDL, but it is almost halved compared to the demanding MDPL; power consumption of SC-DDPL is also about 2.7 times higher than that of WDDL, but it is 15% lower compared to the MDPL implementation.

## APPENDIX A

For the sake of completeness and to further validate the proposed approach, we have designed and compared a full implementation of the PRESENT-80 algorithm with a loop-iterative architecture and 64-bit parallel data-path, as in [20], adopting the technology in Section V. We have compared a WDDL and a SC-DDPL (with $t_{eval}$ set at 1ns) design. We have also designed a non-cryptographic core, that is the s349 circuit from the ISCAS'89 benchmark, referring to both WDDL and SC-DDPL logic styles. This specific circuit is made up of a 4x4bit add-shift multiplier. The gate count and the power consumption results, as well as the energy security metrics for both designs are reported in TABLE X. The overhead of the proposed logic style compared to WDDL is slightly less than x1.7 for the gate count and x2.8 in power consumption, but it delivers a strongly increased capability to mitigate data-dependency in the power consumption.

TABLE X
ASIC results on full implementation of PRESENT-80 block cipher and ISCAS'89 s349 circuit

| Design | Logic Style | Gate Count [kG] | $P_{AV}$ (@10MHz) | NED/NSD [%]/[%] |
|---|---|---|---|---|
| PRESENT-80 | WDDL | 10.20 | 141 | 0.13/0.030 |
| | SC-DDPL | 17.54 | 372 | 0.02/0.007 |
| ISCAS'89 s349 | WDDL | 0.86 | 13.53 | 2.83/0.65 |
| | SC-DDPL | 1.45 | 38.49 | 0.27/0.006 |

## REFERENCES


[1] P.C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," In Proc. of Advances in cryptology, CRYPTO '96. Lect. Notes in Computer Science, vol. 1109, pp. 104–13, Springer; 1996.

[2] J. J. Quisquater and D. Samyde, Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In Smart Card Programming and Security (pp. 200-210). Springer Berlin Heidelberg (2001).

[3] P.C. Kocher, *et al.*, Differential Power Analysis. In Proceedings of Advances in Cryptology, CRYPTO '99, Lect. Notes in Computer Science, vol.1666, pages 388-397.Springer, 1999.

[4] E. Brier, et al., "Correlation power analysis with a leakage model", Proc. CHES-04, vol. 3156, pp.16 -29, 2004.

[5] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," In Proc. of *DATE'04*, pp. 246-251, 2004.

[6] K. Tiri, *et al.*, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards," In Proc. of *ESSCIRC '02*.

[7] T. Popp and S. Mangard, "Masked Dual-Rail Pre-charge Logic: DPA Resistance Without Routing Constraints," in Proc. of *CHES'05*, ser. LNCS, vol. 3659. Springer, Sept 2005, pp. 172-186., Edinburgh, Scotland, UK.

[8] W. Cilio, M. Linder, C. Porter, J. Di, D. R. Thompson, S. C.Smith, "Mitigating power- and timing-based side-channel attacks using dual-spacer dual-rail delay-insensitive asynchronous logic," Microelectronics Journal vol. 44, 2013, pp. 258–269.

[9] K. Nawaz, et al., "Scaling Trends for Dual-Rail Logic Styles Against Side-Channel Attacks: A Case-Study,", *COSADE 2018*.

[10] K. Tiri, and I. Verbauwhede, "Place and Route for Secure Standard Cell Design,", in *Smart Card Research and Advanced Applications VI* pp. 143–158. Springer US, Boston, MA (2004).

[11] W. He, *et al.*, "Automatic generation of identical routing pairs for FPGA implemented DPL logic," In 2012 *International Conference on Reconfigurable Computing and FPGAs*, pp. 1–6 (2012).

[12] M. Bucci, et al., "Delay based dual-rail precharge logic", in *IEEE Trans. on VLSI* (TVLSI), 1147–1153 (2011).

[13] S. Bongiovanni, *et al.*, "Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks", in J. of Crypt.Eng., Springer Berlin Heidelberg, April 2015.

[14] D. Bellizia, *et al.*, "TEL Logic Style as a Countermeasure Against Side-Channel Attacks: Secure Cells Library in 65nm CMOS and Experimental Results", in *IEEE Transactions on Circuits and Systems I*, vol. 65, no. 11, pp. 3874-3884, 2018.

[15] S. Bongiovanni, *et al*., "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).

[16] K.M. Fanta and S.A. Brandt, "Null convention logic: a complete and consistent logic for asynchronous digital circuit synthesis," In Proc. Of ASAP 1996, pp.261–273 (1996).

[17] S. Mangard et al., Power analysis attacks: Revealing the secrets of smart cards., Springer Science& Business Media, 2008.

[18] D. Bellizia, et al., "Secure Implementation of TEL-compatible Flip-Flops using a Standard-Cell Approach," in Proc. Of International Symposium of Circuits and Systems 2018 (ISCAS'18), May 2018.

[19] D. Bellizia, *et al.*, "Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications," in *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 3, pp. 329-339, July-Sept. 1 2017.

[20] D. Bellizia, *et al.*, "Implementation of the PRESENT-80 block cipher and analysis of its vulnerability to Side Channel Attacks Exploiting Static Power," in Proc. Of *MIXDES 2016*, Lodz, 2016, pp. 211-216.

[21] C. Rolfes, *et al.*, "Ultra-Lightweight Implementations for Smart Devices – Security for 1000 Gate Equivalents", 8th IFIP WG 8.8/11.2 Int. Conference, *CARDIS 2008*, London, UK, September 8-11, 2008.

[22] A. Bogdanov, et al., "PRESENT: An Ultra-Lightweight Block Cipher Cryptographic Hardware and Embedded Systems-*CHES 2007*. " Vol. 4727, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 450-466.

[23] K. Iokibe, et al., "Equivalent Circuit Modeling of Cryptographic Integrated Circuit for Information Security Design," in *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 581-588, June 2013.

[24] D. Bellizia, *et al.*, "On-chip current-mode approach to thwart CPA attacks in CMOS nanometer technology." International Journal of Microelectronics and Computer Science 7.4 (2016).

[25] E. Amouri, *et al.*, "Differential pair routing to balance dual signals of wddl designs in cluster-based mesh FPGA," in Proc. of 6th International Workshop on Reconfigurable Communication-Centric Systems-on-Chip (ReCoSoC), pp. 1–4 (2011).
[26] D. Bellizia, *et al.*, "Secure Double Rate Registers as an RTL Countermeasure Against Power Analysis Attacks," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 7, pp. 1368-1376, July 2018.
[27] F. Macé, *et al.*, "Information Theoretic Evaluation of Side-Channel Resistant Logic Styles," in *CHES 2007*, pp. 427–442. Springer Berlin Heidelberg, Berlin, Heidelberg (2007).
[28] J. Cooper, *et al*., Test Vector Leakage Assessment (TVLA) Methodology in Practice. International Cryptographic Module Conference, 2013.
[29] F. Durvaux, and F.X. Standaert, From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces, in EUROCRYPT 2016. Lecture Notes in Computer Science, vol 9665. Springer, Berlin, Heidelberg
[30] M. Ender, *et al.*, "SafeDRP: Yet Another Way Toward Power-Equalized Designs in FPGA", in Proc. *COSADE*, Paris, France, Apr. 2017, pp.83-101.

**Davide Bellizia** was born on June 20th 1989. He received the M.S. degree (summa cum laude) in Electronic Design and the Ph.D. degree in Electronics Engineering from University "La Sapienza" of Rome (Italy), respectively in 2014 and 2018. In 2014 he received the "Laureato Eccellente" award for the best graduate student of the year. In 2017, he joined to the Crypto Group of Université Catholique de Louvain (UCLouvain), Louvain-la-Neuve, Belgium, as postdoc researcher. His research interests include the design of cryptographic ICs for counteracting power analysis attacks, and VLSI design for DSP algorithm implementations.

**Simone Bongiovanni** was born in Rome in 1983. He received the Bachelor's degree in electronic engineering and the Master of Science degree (summa cum laude) in electronic systems for telecommunications from the University of Rome "La Sapienza", in 2007 and 2010 respectively. In 2010, after a collaboration with the Communications Department of the Ministry of Economic Development of Italy and the "Ugo Bordoni" Foundation, he discussed a thesis on the study of the hardware security of smart cards for mobile payments applications. In 2015 he received the Ph.D. degree in electronic engineering from the University of Rome "La Sapienza", after discussing a thesis on the design of techniques for secure IC's devices for cryptographic applications, with a particular focus on power analysis attacks. In 2015 he joined the Digital Security System department of Infineon Technologies Austria, as Digital Design Engineer.

**Mauro Olivieri** (M'98) received the Master (Laurea) degree in electronic engineering "cum laude," in 1991 and the Doctorate degree in electronic and computer engineering in 1994 from the University of Genoa, Genoa, Italy, where he was an Assistant Professor from 1995 to 1998. In 1998, he joined Sapienza University, Rome, Italy, where he is currently an Associate Professor, teaching digital electronics and VLSI system architectures. His current research interests include digital system-onchip design, microprocessor core design, and digital nanoCMOS circuits. He authored more than 100 research papers and a textbook in three volumes. He is a Reviewer for several IEEE Transactions and is in the technical program committee of the IEEE DATE Conference. He is an Evaluator for the Joint Technology Initiative of the European Commission on Nanoelectronics (ENIAC Joint Undertaking).

**Giuseppe Scotti** was born in Cagliari, Italy, in 1975. He received the M.S. and Ph.D. degrees in electronic engineering from the University of Rome "La Sapienza", Rome, Italy, in 1999 and 2003, respectively. In 2010, he became a Researcher (Assistant Professor) at the DIET department of the University of Rome "La Sapienza" and in 2015 he was appointed Associate Professor in the same department. He teaches undergraduate and graduate courses on basic electronics and microelectronics. His research activity was mainly concerned with integrated circuits design and focused on design methodologies able to guarantee robustness with respect to parameter variations in both analog circuits and digital VLSI circuits. In the context of analog design his research activity was concerned with circuit topologies for the realization of low-voltage analog building blocks using ultra-short channel CMOS technology, whereas in the context of cryptographic hardware his focus has been on novel PAAs methodologies and countermeasures. He has been also involved in R&D activities held in collaboration between "La Sapienza" University and some industrial partners, which led, between 2000 and 2015, to the implementation of 13 ASICs. He has coauthored more than 45 publications in international Journals, about 70 contributions in conference proceedings and is the co-inventor of 2 international patents.