IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Novel Clock Gating Approach for the Design of Low-Power Linear Feedback Shift Registers

GIANLUCA GIUSTOLISI[1], (Senior Member, IEEE), ROSARIO MITA[1], GAETANO PALUMBO[1], (Fellow, IEEE), and GIUSEPPE SCOTTI[2], (Senior Member, IEEE)

[1]DIEEI, Università degli Studi di Catania, 95125, Catania, Italy. (e-mail: gianluca.giustolisi@unict.it)
[2]DIIET, Università degli Studi di Roma "La Sapienza", 00184, Roma, Italy (e-mail: giuseppe.scotti@uniroma1.it)e

Corresponding author: Gianluca Giustolisi (e-mail: gianluca.giustolisi@unict.it).

This work was supported in part by…

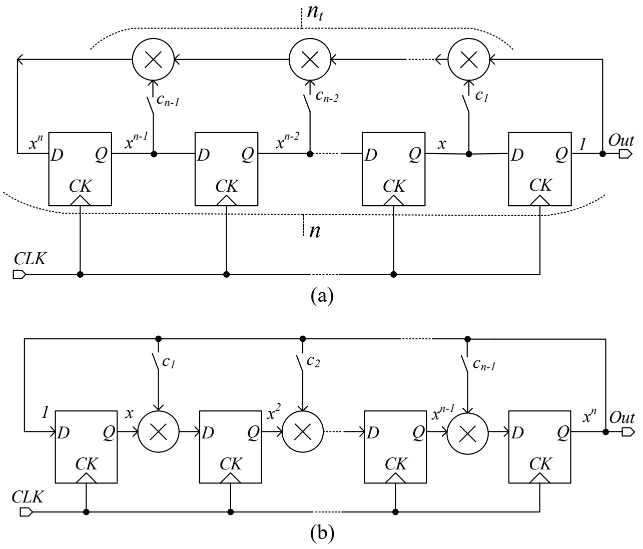
ABSTRACT This paper presents an efficient solution to reduce the power consumption of the popular linear feedback shift register by exploiting the gated clock approach. The power reduction with respect to other gated clock schemes is obtained by an efficient implementation of the logic gates and properly reducing the number of XOR gates in the feedback network. Transistor level simulations are performed by using standard cells in a 28-nm FD-SOI CMOS technology and a 300-MHz clock. Simulation results show a power reduction with respect to traditional implementations, which reaches values higher than 30%.

INDEX TERMS Complementary pass-transistor logic (CPL), gated clock, linear feedback shift register (LFSR), low-power design, transmission gate (TG)

I. INTRODUCTION

Today, linear feedback shift registers (LFSRs) are widely used in many electronics equipment that require very fast generation of a pseudo-random sequence, such as built-in test of digital circuits [1]-[5], where the minimization of area, power and delay are the most important figures of merit. LFSRs are also fundamental building blocks in stream ciphers for secure communications used in GSM and LTE applications [6], and in lightweight stream ciphers for embedded systems [7]. Word-based LFSRs were introduced to efficiently use the structure of modern word-based processors. Such LFSRs are used in a variety of stream ciphers, most notably in the SNOW series of stream ciphers [8] and in image encryption applications [9]. LFSRs are also used to generate an approximation of white noise for parameters estimation and system identification purposes [10], and in the Global Positioning System where an LFSR is used to rapidly transmit a sequence that indicates high-precision relative time offsets [11]. LFSRs are also widely used in direct sequence spread spectrum (DSSS) systems [12], and error detection and correction by implementing BCH (Bose, Chaudhuri, Hocquenghem) and CRC (cyclic redundancy codes) encoder and decoder circuits [13]-[15]. Recently LFSR have been also exploited to build strong physical unclonable functions (PUFs) for cryptographic applications [16,17].

Hardware implementation of linear feedback shift registers can be obtained by adopting two alternative configurations, both depicted in Fig. 1, each generating the same output bit stream. The configurations are named Fibonacci configuration (Fig. 1a) also known as standard, many-to-one or external XOR gates, and the Galois configuration (Fig. 1b) also known as modular, one-to-many or internal XOR gates [18].



(a)

(b)

FIGURE 1. Generic *n*-bit LFSR: Fibonacci or standard configuration (a) and Galois or modular configuration (b).

These topologies are very simple to build, but since the clock-path of all flip-flops toggles at every clock cycle, they waste a non-negligible amount of power.

Although the LFSR power consumption has been extensively addressed in literature [19]-[21], the proposed solutions reduced power consumption at the cost of an increased circuit complexity, thus obscuring the major advantage of the LFSRs. A gated clock solution to reduce power consumption of the LFSRs has been also proposed by one of the authors in [22], where the analysis demonstrated that the power reduction strongly depends on the technological characteristics of the employed gates.

Moreover, in the same paper it has been found that a relationship involving technology parameters has to be satisfied in order to achieve a power reduction with respect to a traditional (non-gated clock) LFSR. In particular, even if the above relationship involving technology parameters gets satisfied, the maximum power reduction allowed by the approach in [22] with respect to a traditional (non-gated clock) LFSR is below 10%.

In this paper we propose a more efficient gated clock design approach for LFSRs, which greatly reduce power consumption without unduly complicating the traditional simple topology. With respect to other gated clock schemes, the proposed approach allows more power saving, thanks to a power efficient implementation of the logic gates that implement the clock gating network, and by properly reducing the number of XOR gates in the feedback path. Indeed, the proposed approach has resulted in a power reduction that can reach values higher than 30%.

II. BACKGROUND

A. LINEAR FEEDBACK SHIFT REGISTER

A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state.

By referring to the standard implementation in Fig. 1, LFSR is realized with an array of flip-flops (FFs) with a linear feedback performed by several XOR gates.

The initial value of the LFSR is called the seed, and since the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current state. Although LFSRs are very simple to implement, they are based on a rather complex mathematical theory [23]. However, they can be efficiently described through the n^{th}-order polynomial

$$p_c = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + 1 \qquad (1)$$

where the binary coefficients c_i $(i = 1,2, \dots n-1)$, define the well-known characteristic polynomial (p_c), which set the length of the pseudo-random sequence and the other statistical properties of the bit generator.

By defining P_{FF} and P_{XOR} the power consumption of the FFs and the XOR gates, respectively, the power consumption of the conventional LFSR in Fig. 1 can be modeled as

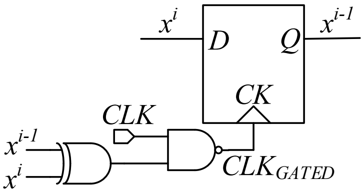


FIGURE 2. Traditional gated clock circuit for FFs without enable signal.

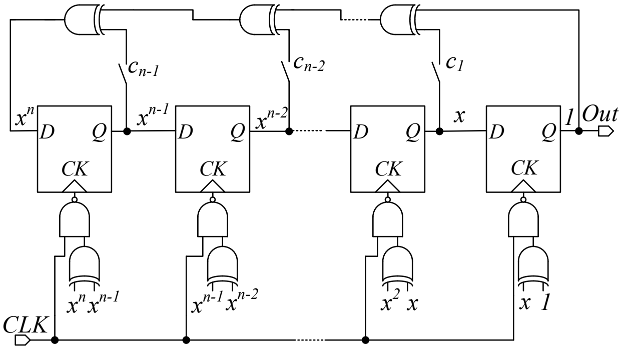


FIGURE 3. Gated clock LFSR implementation.

$$P_{Conv} = nP_{FF} + n_t \alpha P_{XOR} \qquad (2)$$

where n is the register length (i.e., the order of the generator), n_t is the number of the inner taps (i.e., the number of the terms of the polynomial characteristic except x^n and 1), α is the switching activity at the inner nodes, which, in a LFSR with $n \geq 6$ and assuming maximum period, is approximately equal to 0.5 [22].

From (2), it appears that for the topologies in Fig. 1 the clock path toggles at every clock cycle, thus dissipating a significant amount of power especially at high clock rates.

Vice versa, power consumption of FF D-path and XOR gates depend on the switching activity and hence its value is reduced by 50% with respect to the maximum value.

B. DYNAMIC POWER MANAGEMENT

Dynamic Power Management (DPM) is a commonly adopted strategy to reduce power consumption in a digital system. It consists in disabling the logic circuits that are not performing functional operations during a particular time frame.

At circuit level, this strategy is known as “gated clock approach” [24, 25] and, for flip-flops with no enable signal, it consists in their activation only when the input signal is different from the actual output value, according to the scheme depicted in Fig. 2.

A modified LFSR that takes advantage of the gated clock strategy is shown in Fig. 3. The topology reduces the flip-flop power consumption, P_{FF}, at the price of additional power consumption due to the extra gates required to implement the gated clock approach.

Therefore, for the gated clock LFSR in Fig. 3, the power consumption in (2) turns into

$$P_{GC} \approx n\alpha P'_{FF} + (n + n_t)\alpha P_{XOR} + n\alpha P_{NAND} \qquad (3)$$

where the term $n \cdot \alpha \cdot P'_{FF}$ represents the dissipation of the FFs with the new load conditions (i.e., the extra XOR gates).

In [22], to further reduce the power consumption of the extra gates, the authors proposed a single CMOS XORNAND gate to drive the clock terminals of the FFs. The power dissipation was estimated in

$$P_{GC[22]} \approx n\alpha P'_{FF} + n_t \alpha P_{XOR} + n\alpha P_{XORNAND} \qquad (4)$$

but, the reduction in the overall power dissipation with respect to a traditional (non-gated clock) LFSR was no better than 10%, thus limiting the benefit of the proposed topology.

III. IMPROVED GATED CLOCK IMPLEMENTATION

A. EFFICIENT LOGIC GATE IMPLEMENTATION

Reducing the overall power dissipation can be accomplished by reducing the power consumption of the term $P_{XORNAND}$ in (4). This can be done by means of the power-aware solution depicted in Fig. 4, which combines the benefits of the complementary pass transistor logic (CPL-XOR/XNOR) with the transmission gate approach (TG-MUX) [26]. It is worth noting that the complementary signals required by the CPL-XOR/XNOR section are easily available as output signals of many FF standard cells. Moreover, the complementary outputs of the CPL-XOR/XNOR section are perfectly tailored to drive the TG-MUX section since they guarantee a full voltage swing at the output node of the XORAND gate without any additional level restoring transistors.

The power consumption of a gated clock LFSR implemented using the XORAND circuit in fig. 4 can be modeled as

$$P_{CPT\_TG} \approx n\alpha P''_{FF} + n_t \alpha P_{XOR} \qquad (5)$$

where the power consumption of the gated circuit, P_{XORAND}, is virtually eliminated and the FFs power consumption, P''_{FF}, accounts for the smaller capacitive effects due to both CPL and TG circuits.

B. REDUCED XOR NUMBER

To further cut down the LFSR power consumption, we propose an additional strategy to reduce the number of XOR gates in the feedback path, n_t, by taking advantage of the CPL-XOR/XNOR section in Fig. 4. Indeed, at the output of this CPL gate we have a binomial $x^{i+1} \oplus x^i$, with index i from 0 to $n-2$, which can be used to save XORs in the feedback path. For example, considering the polynomial $x^7+x^3+x^2+x+1$, instead of using three XORs in the feedback path to implement $x^3 \oplus (x^2 \oplus (x \oplus 1))$, we can simply do the XOR of the binomials $x^3 \oplus x^2$ and $x \oplus 1$ available at the outputs of the CPL gates. Moreover, in case of non-adjacent taps, we can exploit the property $x^i \oplus x^i = 0$.

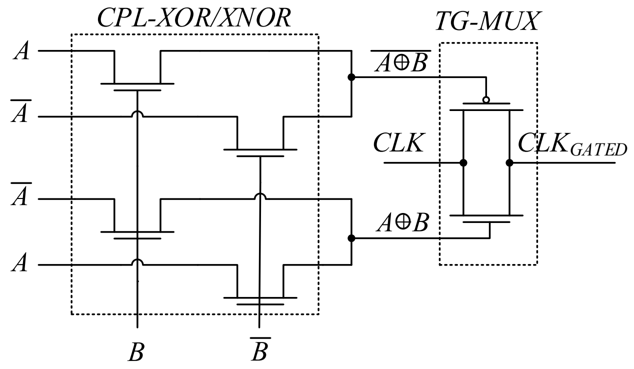


FIGURE 4. Power-aware XORAND for gated clock implementation.

For example, the polynomial x^5+x^2+1, which needs only one XOR in the traditional topology, can be implemented again with only one XOR whose inputs are the binomials (x^2+x) and $(x+1)$ available at the outputs of the CPL-XOR/XNOR.

To derive the number of XOR gates required in the feedback network by using the proposed strategy, let us consider the ordered m-elements array, a_i, of the taps exponent (for example, for the polynomial $x^{10}+x^4+x^3+x+1$ the array elements are $a_1=1$, $a_2=3$, $a_3=4$ and $a_4=10$). Then, the number of the XOR required in the feedback network is given by

$$n'_t = a_1 - 1 + \sum_{i=1}^{\frac{m}{2}-1} (a_{2i+1} - a_{2i}) \qquad (6)$$

Note that in (6) a_1 is the lowest exponent of the polynomial characteristic, and terms in the sum are couple of close taps exponents, without the highest one.

By inspection of relationship (6), it is apparent that the minimum number of XOR is required when the characteristic polynomial contains the term x, and all the couple of taps are also adjacent.

Table I summarizes the number of XOR gates necessary to implement the feedback circuit of some characteristic polynomials both in the traditional topology, n_t (i.e., number of the inner taps), and by adopting the proposed strategy, n'_t evaluated through relationship (6).

If we now focus on Table I, it is apparent that the proposed strategy does not always need a lower number of XOR gates. Thus, to achieve a further reduction on the number of XOR gates, we can efficiently use together the outputs of the CPL-XOR/XNOR sections (i.e., the terms $x^{i+1} \oplus x^i$), and the terms x^i at the outputs of the FFs.

Thus, a further reduction on the number of XOR gates in the feedback path is achieved, since it results equal to

$$n''_t = n_t - m_c \qquad (7)$$

where m_c is the number of adjacent taps couples, but considering each tap in only one couple. For example, in the polynomial $x^{10}+x^4+x^3+x+1$ the couples of adjacent taps, m_c, are 2, that is, the couples (x^4+x^3) and $(x+1)$.

TABLE I
NUMBER OF XORS IN THE LINEAR FEEDBACK PATH OF SOME LFSRS

Polynomial characteristic	n_t	n'_t	n''_t	$n''_t - n_t$
$x^5 + x^2 + 1$ [1]	1	1	1	0
$x^5 + x^3 + x^2 + x + 1$	3	1	1	–2
$x^7 + x^3 + 1$ [2]	1	2	1	0
$x^7 + x^3 + x^2 + x + 1$	3	1	1	–2
$x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$	5	2	2	–3
$x^{10} + x^3 + 1$	1	2	1	0
$x^{10} + x^4 + x^3 + x + 1$	3	1	1	–2
$x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$	5	2	2	–3
$x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	7	3	3	–4
$x^{16} + x^5 + x^3 + x^2 + 1$	3	3	2	–1
$x^{16} + x^5 + x^4 + x^3 + x^2 + x + 1$	5	2	2	–1
$x^{16} + x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$	7	3	3	–4
$x^{16} + x^{15} + x^{11} + x^9 + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ [3]	9	9	6	–3

[1] Used in CRC-5-USB token packets
[2] Used in CRC-7 Telecom systems, ITU-T G.707, ITU-T G.832, SD/MMC
[3] Used in CRC-16-T10-DIF SCSI DIF

Note that now, unlike for relationship (6), the term x^0 is also included to find the adjacent couples.

By inspection of Table I, where also the number of XOR gates required by adopting this strategy, n''_t, is reported, it is apparent that now the number of XOR gates in the feedback path is always lower (or equal) than n_t thus providing an overall power reduction on the feedback network contribution.

Finally, it has to be remarked that, in the feedback network, where XOR gates have to drive FFs instead of TGs, it is not convenient to implement XOR gates with the CPL topology. Indeed, the highest output voltage value of CPL is equal to $V_{DD} - V_{tn}$ (i.e., a weak logical '1').

This value may not be sufficiently high to switch off the PMOS transistors at the input of the FFs, and a static power consumption contribution may arise.

Thus, unless additional transistors to provide level restoring are included, CPL-XOR/XNOR gates in feedback network result inefficient with respect to the traditional CMOS implementation [27].

IV. DESIGN EXAMPLES AND SIMULATION RESULTS

We have compared the power consumption among the LFSRs designed with the proposed gated clock approach, with the traditional implementation and with the solution given in [22]. We remark that the proposed approach allows to reduce power consumption without severely affecting the critical path of the circuit and thus without limiting the speed of the serial LFSR, which exhibits the lowest critical path delay among all the LFSR architectures. Recently parallel approaches [13]-[15], have been proposed, specifically targeted for BCH and CRC encoders, but due to the very different architecture, a comparison between the LFSR presented in this paper and these parallel approaches is not fair, therefore we do not include parallel approaches in the comparison.

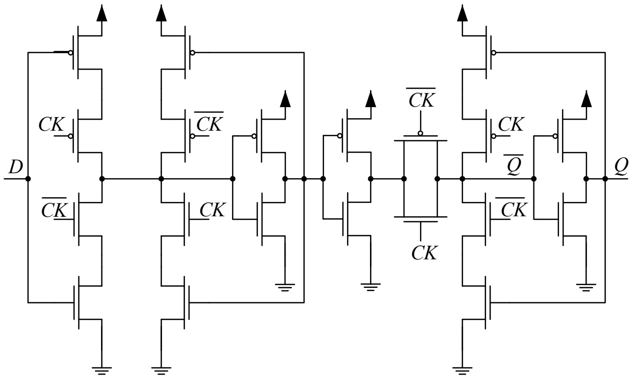


FIGURE 5. Simplified schematic of the used D-type Flip-Flop.

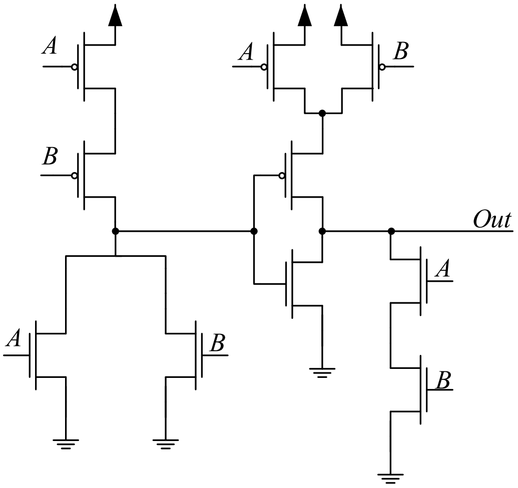


FIGURE 6. Simplified schematic of the speed-optimized XOR gate included in the STM standard-cell library.

Specifically, using a commercial 28-nm CMOS FD-SOI technology process in the Cadence simulation environment, we have run several transistor level simulations on the topologies having the characteristic polynomials in Table I. For the digital blocks, we used the master-slave positive edge triggered D-type Flip-Flop depicted in Fig. 5 and the two-input speed-optimized XOR gate in Fig. 6, both included in a standard threshold voltage, low-power option standard cells library. In addition, for the circuits reported in [26] and in Fig. 4, we used the thin oxide N-type and P-type MOSFETs with low threshold voltage and minimum channel length of 28-nm, included in the same design kit. All circuits have been clocked at 300 MHz and powered at 1 V.

The simulation results of the LFSRs designed with the different approaches are summarized in Table II. By comparing the approach proposed in [22] with respect to the traditional implementation, we note that the power consumption of the FFs is reduced by nearly 25% after applying the clock gated design, but the overall power reduction is only lower than 8% since extra gates are introduced to implement the gated circuit. In other words, the XORNAND gates contribute with 12-18% of the overall power consumption with an inverse dependence on the number of the taps.

On the other hand, as expected, the proposed solution, as reported in Table II and plotted in Fig. 7, allows a significant power saving, which is typically higher than 20% and often (especially for higher order polynomials) reaching values around 30%.

Finally, it is worth noting that, unlike the strategy in [22], the overall power saving of the proposed gating approach is proportional to the number of taps. Indeed, by increasing the number of taps, although the capacitive effects of the feedback network also increase, there is, according to (7), an increased probability to find couples of adjacent taps that reduce the number of the XOR gates.

For area and delay estimation purposes, we have coded in VHDL and synthesized by using the Cadence Genus^{TM} tool the 16 bits LFSRs reported in Table II, considering both the conventional and the gated clock implementation in [22]. To estimate area and delay of the LFSRs exploiting the approach proposed in this paper, we have implemented also the full custom layout of the power-aware XORAND circuit in Fig. 4. The area of the LFSRs has then been estimated by summing the area of the standard cells and the area of the power-aware XORAND exploited in the different 16 bits LFSRs implementations.

Table III summarizes the area and critical path delays of the 16 bits LFSRs reported in Table II, confirming how the proposed approach does not affect the critical path delay, which is, in all cases, set by the feedback path. The area estimations suggest also that the proposed approach results not only in a significant power consumption saving, but also in a slight area reduction with respect to the approach in [22].

TABLE II.
POWER CONSUMPTION (EXPRESSED IN μW) OF THE SIMULATED LFSRS

	Conventional Eq. (2)		Gated Clock [22] Eq. (4)			Proposed approach Eq. (5)	
	nP_{FF}	$n_t \alpha P_{XOR}$	$n\alpha P'_{FF}$	$n_t \alpha P_{XOR}$	$n\alpha P_{XORNAND}$	$n\alpha P''_{FF}$	$n''_t \alpha P_{XOR}$
x^5+x+1	7.93	0.21	5.98	0.24	0.93	6.39	0.27
	P_{Conv}=8.14		***$P_{GC[22]}$=7.15 (-12.2%)***			***$P_{CPL\_TG\_imp}$=6.65 (-18.3%)***	
$x^5+x^3+x^2+x+1$	8.11	0.798	6.17	0.84	0.95	6.34	0.36
	P_{Conv}=8.91		***$P_{GC[22]}$=7.97 (-10.7%)***			***$P_{CPL\_TG\_imp}$=6.70 (-24.9%)***	
x^7+x^3+1	11.08	0.78	8.22	0.23	1.28	8.73	0.26
	P_{Conv}=11.99		***$P_{GC[22]}$=10.48 (-12.6%)***			***$P_{CPL\_TG\_imp}$=9.10 (-24.2%)***	
$x^7+x^3+x^2+x+1$	11.20	0.361	8.38	0.82	1.28	8.74	0.35
	P_{Conv}=11.56		***$P_{GC[22]}$=10.48 (-9.4%)***			***$P_{CPL\_TG\_imp}$=9.10 (-20.5%)***	
$x^7+x^5+x^4+x^3+x^2+x+1$	11.51	1.64	8.56	1.68	1.28	8.80	0.70
	P_{Conv}=13.14		***$P_{GC[22]}$=11.53 (-12.3%)***			***$P_{CPL\_TG\_imp}$=9.50 (-27.8%)***	
$x^{10}+x^3+1$	15.78	0.201	11.69	0.23	1.84	12.51	0.26
	P_{Conv}=15.98		***$P_{GC[22]}$=13.77 (-13.9%)***			***$P_{CPL\_TG\_imp}$=12.77 (-20.2%)***	
$x^{10}+x^4+x^3+x+1$	15.94	0.77	11.86	0.81	1.81	12.39	0.35
	P_{Conv}=16.71		***$P_{GC[22]}$=14.49 (-13.4%)***			***$P_{CPL\_TG\_imp}$=12.75 (-23.8%)***	
$x^{10}+x^6+x^5+x^3+x^2+x+1$	16.10	1.63	12.02	1.66	1.84	12.47	0.70
	P_{Conv}=17.73		***$P_{GC[22]}$=15.53 (-12.5%)***			***$P_{CPL\_TG\_imp}$=13.18 (-25.8%)***	
$x^{10}+x^7+x^6+x^5+x^4+x^3+$	16.59	2.84	12.92	2.90	1.79	13.29	0.99
x^2+x+1	***P_{Conv}=19.43***		***$P_{GC[22]}$=17.62 (-9.4%)***			***$P_{CPL\_TG\_imp}$=14.28 (-26.5%)***	
$x^{16}+x^5+x^3+x^2+1$	25.55	0.78	18.58	0.81	2.96	19.64	0.70
	P_{Conv}=26.33		***$P_{GC[22]}$=22.35 (-15.2%)***			***$P_{CPL\_TG\_imp}$=20.35 (-22.8%)***	
$x^{16}+x^5+x^4+x^3+x^2+x+1$	25.76	1.65	18.79	1.60	2.97	19.68	0.69
	P_{Conv}=27.41		***$P_{GC[22]}$=23.36 (-14.8%)***			***$P_{CPL\_TG\_imp}$=20.38 (-25.7%)***	
$x^{16}+x^8+x^7+x^5+x^4+x^3+$	26.61	2.82	20.48	2.84	2.97	19.66	1.02
x^2+x+1	***P_{Conv}=29.43***		***$P_{GC[22]}$=26.29 (-10.7%)***			***$P_{CPL\_TG\_imp}$=20.69 (-29.7%)***	
$x^{16}+x^{15}+x^{11}+x^9+x^8+x^7+$	27.03	4.39	20.69	4.78	2.97	19.73	2.0916
$x^5+x^4+x^2+x+1$	***P_{Conv}=31.42***		***$P_{GC[22]}$=28.45 (-9.5%)***			***$P_{CPL\_TG\_imp}$=21.83 (-30.6%)***	

TABLE III.
AREA AND CRITICAL PATH DELAY OF THE 16 BIT SIMULATED LFSRS

	Conventional LFSR		Gated Clock [22]		Proposed approach	
	Area (μm^2)	Delay (ns)	Area (μm^2)	Delay (ns)	Area (μm^2)	Delay (ns)
$x^{16}+x^5+x^3+x^2+1$	47.64	0.133	66.77	0.133	56.68	0.133
$x^{16}+x^5+x^4+x^3+x^2+x+1$	49.28	0.154	68.41	0.154	55.93	0.154
$x^{16}+x^8+x^7+x^5+x^4+x^3+x^2+x+1$	50.91	0.154	70.04	0.154	56.36	0.154
$x^{16}+x^{15}+x^{11}+x^9+x^8+$ $x^7+x^5+x^4+$ x^2+x+1	52.55	0.182	71.68	0.182	59.20	0.182

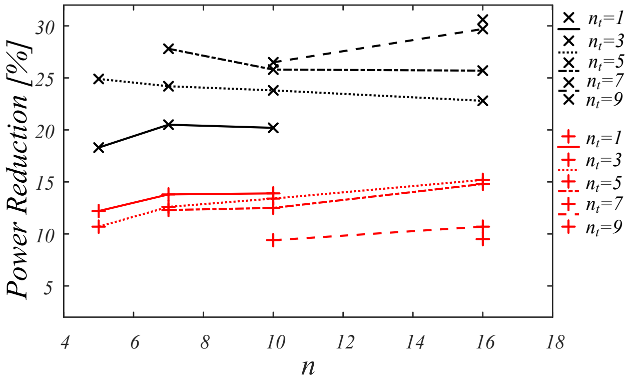


FIGURE 7. Power reduction of the proposed LFSR (×) and solution given in [22] (+) with respect to the traditional implementation.

V. CONCLUSION

An efficient solution to reduce the power consumption of the popular linear feedback shift register has been presented and discussed in detail. The approach uses in some parts CPL design style and benefits from using the gated clock also to implement the feedback network, thus allowing to reduce the number of XOR gates. The proposed design approach has been validated by simulations in a 28 nm CMOS technology and, compared to traditional implementation, has been shown to lead to a power reduction up to 30%, without increasing area and critical path delay.

REFERENCES

[1] C. P. de Souza, F. M. de Assis, R. C. S. Freire,” A New Architecture of Test Response Analyzer Based on the Berlekamp–Massey Algorithm for BIST,” *IEEE Transactions on Instrumentation and Measurement*, Vol. 59 , No. 12, pp. 3168 – 3173, December 2010.

[2] R. Oommen, M. K. George and S. Joseph, "Study and Analysis of Various LFSR Architectures," *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, 2018, pp. 1-6.

[3] M. Mohan and S. S. Pillai, "Review on LFSR for Low Power BIST," *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, 2019, pp. 873-876.

[4] K. -J. Lee, Z. -Y. Lu and S. -C. Yeh, "A Secure JTAG Wrapper for SoC Testing and Debugging," in *IEEE Access*, vol. 10, pp. 37603-37612, 2022.

[5] Murugan, S.V., Sathiyabhama, B. “Bit-swapping linear feedback shift register (LFSR) for power reduction using pre-charged XOR with multiplexer technique in built in self-test.” Journal of Ambient Intelligence Humanized Computing 12, 6367–6373 (2021).

[6] D. Rupprecht, K. Kohls, T. Holz and C. Pöpper, "Breaking LTE on Layer Two," *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1121-1136.

[7] Manifavas, C., Hatzivasilis, G., Fysarakis, K., and Papaefstathiou, Y. (2016) A survey of lightweight stream ciphers for embedded systems. Security Comm. Networks, 9: 1226– 1246.

[8] S. Nandi, S. Krishnaswamy, B. Zolfaghari and P. Mitra, "Key-Dependent Feedback Configuration Matrix of Primitive σ–LFSR and Resistance to Some Known Plaintext Attacks," in *IEEE Access*, vol. 10, pp. 44840-44854, 2022.

[9] J. Choi and N. Y. Yu, "Secure Image Encryption Based on Compressed Sensing and Scrambling for Internet-of-Multimedia Things," in *IEEE Access*, vol. 10, pp. 10706-10718, 2022.

[10] F. M. Mwaniki and H. J. Vermeulen, "Characterization and Application of a Pseudorandom Impulse Sequence for Parameter Estimation Applications," in *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 6, pp. 3917-3927, June 2020

[11] F. Zanier, G. Bacci, M Luise, “Criteria to Improve Time-Delay Estimation of Spread Spectrum Signals in Satellite Positioning,” *IEEE Journal of Signal Processing*, Vol. 3, No. 5, pp. 748-763, October 2009.

[12] Y. Kim, J. Kim, J. Song and D. Yoon, "Blind Estimation of Self-Synchronous Scrambler Using Orthogonal Complement Space in DSSS Systems," in *IEEE Access*, vol. 10, pp. 66522-66528, 2022.

[13] G. Hu, J. Sha and Z. Wang, "High-Speed Parallel LFSR Architectures Based on Improved State-Space Transformations," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 1159-1163, March 2017.

[14] X. Zhang, "A Low-Power Parallel Architecture for Linear Feedback Shift Registers," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 3, pp. 412-416, March 2019.

[15] X. Zhang and Z. Xie, "Efficient Architectures for Generalized Integrated Interleaved Decoder," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 10, pp. 4018-4031, Oct. 2019.

[16] S. Hou, Y. Guo and S. Li, "A Lightweight LFSR-Based Strong Physical Unclonable Function Design on FPGA," in *IEEE Access*, vol. 7, pp. 64778-64787, 2019.

[17] S. Baek, G. -H. Yu, J. Kim, C. T. Ngo, J. K. Eshraghian and J. -P. Hong, "A Reconfigurable SRAM Based CMOS PUF With Challenge to Response Pairs," in *IEEE Access*, vol. 9, pp. 79947-79960, 2021.

[18] M. Goresky, A. M. Klapper, “Fibonacci and Galois representations of feedback-with-carry shift registers,” *IEEE Transactions on Information Theory*, Vol. 48 , No. 11, pp. 2826 – 2836, Nov. 2002.

[19] M. E. Hamid, C. H. Chen, “A Note to Low-Power Linear Feedback Shift Register,” *IEEE Transaction on Circuits and Systems – II*, Vol. 45, No. 9, September 1998.

[20] R. S. Katti, X. Ruan, H. Khattri, “Multiple-Output Low-Power Linear Feedback Shift Register Design,” *IEEE Transaction on Circuits and Systems – I*, Vol. 53, No. 7, pp. 1487-1495, July 2006.

[21] Mehta, D. S., Mishra, V., Verma, Y. K., & Gupta, S. K. “A Hardware Minimized Gated Clock Multiple Output Low Power Linear Feedback Shift Register,” Advances in VLSI, Communication, and Signal Processing, 2020, pp. 367-376. Springer, Singapore.

[22] W. Aloisi, R. Mita, “Gated-Clock Design of Linear-Feedback Shift Registers”, *IEEE Transaction on Circuits and Systems – II*, Vol. 55, No. 6, June 2008

[23] R. David, *Random Testing of Digital Circuits. Theory and Application*, Marcel Dekker, New York, 1998.

[24] L. Benini, A. Bogliolo, G. De Micheli, “A Survey of Design Techniques for System-Level Dynamic Power Managment,” *IEEE Transaction on VLSI Systems*, Vol. 8, No. 3, pp. 299-316, June 2000.

[25] G. Palumbo, F. Pappalardo, S. Sannella, “Evaluation on power reduction applying gated clock approach,” in *Proc. ISCAS 2002*, Vol. 44, pp. IV85-IV88, May 2002.

[26] J. M. Rabay, M. Pedram, Low Power Design Methodologies, Kluver Academic Publishers, Boston, 1997.

[27] R. Zimmermann, W. Fichtner, “Low-power logic styles: CMOS versus pass-transistor logic,” IEEE Journal of Solid-State Circuits, Vol. 32, No. 7, pp. 1079 – 1090, July 1997.

GIANLUCA GIUSTOLISI (M'99–SM'17) was born in Catania, Italy, in 1971. He received the Laurea degree (summa cum laude) in electronic engineering and the Ph.D. degree in electrical engineering from the University of Catania in 1995 and 1999, respectively. Currently, he is Associate Professor at the "Dipartimento di Ingegneria Elettrica Elettronica e Informatica" (DIEEI), University of Catania. Since 2003 he has been teaching courses on electronic devices and analog electronics in undergraduate and postgraduate degrees.

His main research interests reflect his teaching activity in analog circuits with particular emphasis on feedback circuits, compensation techniques, voltage regulators, bandgap voltage references, low-voltage circuits and device modeling.

He is author of more than 100 scientific papers in referred international journals and conferences. He is author of the italian course-book Introduzioneai Dispositivi Elettronici, published by Franco Angeli.

ROSARIO MITA (M'07) received the Laurea degree in electronic engineering and the Ph.D. degree in electrical engineering from the University of Catania, Catania, Italy, in 1998 and 2002, respectively.

He has been aggregate professor with the Dipartimento di Ingegneria Elettrica Elettronica e dei Sistemi, University of Catania, where he taught the electronic's course with the Faculty of Engineering. His research interests include low-voltage CMOS circuits and frequency-compensation techniques of multistage amplifiers, modeling and design of CMOS high-performance digital circuits, low-power digital circuits and systems for pseudorandom bit generation, and the behavioral description of common digital and analog blocks.

GAETANO PALUMBO (F'07) received the Laurea degree in Electrical Engineering in 1988 and the Ph.D. degree in 1993 from the University of Catania. In 1994 he joined the University of Catania, where he is full professor. His primary research interests are in analog and digital circuits. He is the author of more than 400 scientific papers on referred international journals (170+) and conferences. Moreover he is co-author of several patents, four books by Kluwer Academic Publishers and Springer, (published in 1999, 2001, 2005, 2014 respectively), and a textbook on electronic devices (2005).

He served as an Associate Editor of the *IEEE Transactions on Circuits and Systems–part I* in 1999-2001, 2004-2005 and 2008-2011, and of the *IEEE Transactions on Circuits and Systems–part II* in 2006-2007. In 2005 he was one of the 12 panelists in the scientific area 09-industrial and information engineering of the CIVR (Committee for Evaluation of Italian Research), aimed to evaluate the Italian research in the above area for the period 2001-2003.

In 2003 he received the *Darlington Award*. In the period 2011-2013 he served as a member of the Board of Governors of the IEEE CAS Society.

In 2015 he was a panelist of GEV (Group of Evaluation Expert) in the scientific area 09-industrial and information engineering of the ANVUR for the Evaluation of Italian Research Quality in 2011-2014.

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 70 publications in international Journals, about 70 contributions in conference proceedings and is the co-inventor of 2 international patents.