cryptography

MDPI

Article

SC-DDPL as a Countermeasure against Static Power Side-Channel Attacks

Davide Bellizia [1,*], Riccardo Della Sala [2] and Giuseppe Scotti [2]

[1] ICTEAM/ELEN Crypto Group, Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium
[2] Dipartimento di Ingegneria Elettronica e Telecomunicazioni (DIET), Sapienza Università di Roma, 00185 Rome, Italy; riccardo.dellasala@uniroma1.it (R.D.S.); giuseppe.scotti@uniroma1.it (G.S.)
* Correspondence: davide.bellizia@uclouvain.be

Abstract: With the continuous scaling of CMOS technology, which has now reached the 3 nm node at production level, static power begins to dominate the power consumption of nanometer CMOS integrated circuits. A novel class of security attacks to cryptographic circuits which exploit the correlation between the static power and the secret keys was introduced more than ten years ago, and, since then, several successful key recovery experiments have been reported. These results clearly demonstrate that attacks exploiting static power (AESP) represent a serious threat for cryptographic systems implemented in nanometer CMOS technologies. In this work, we analyze the effectiveness of the Standard Cell Delay-based Precharge Logic (SC-DDPL) style in counteracting static power side-channel attacks. Experimental results on an FPGA implementation of a compact PRESENT crypto-core show that the SC-DDPL implementation allows a great improvement of all the security metrics with respect to the standard CMOS implementation and other state-of-the-art countermeasures such as WDDL and MDPL.

Keywords: static power; side-channel attacks; cryptographic hardware; nanometer CMOS; countermeasure; PRESENT; IoT

check for updates

Citation: Bellizia, D.; Della Sala, R.; Scotti, G. SC-DDPL as a Countermeasure against Static Power Side-Channel Attacks. *Cryptography* **2021**, *5*, 16. https://doi.org/10.3390/cryptography5030016

Academic Editor: Jim Plusquellic

Received: 5 May 2021
Accepted: 25 June 2021
Published: 28 June 2021

1. Introduction

Advances in semiconductor technology have been extremely beneficial for the development of new trends in electronics, as modern integrated circuits provide better performance, lower power consumption and much higher integration level. Along with advances in semiconductor technology, security features are increasingly required, especially in applications where sensitive data are handled (e.g., healthcare devices, smartphones, credit cards and IoT nodes). Apart from classical mathematical methodologies to break security schemes, in 1996, Kocher et al. formalized a new approach to recover secret keys from a physical implementation without bruteforcing the algorithm in a seminal paper [1]. The work of Kocher et al. gave rise to a new branch of research in the context of security, known as Side-Channel Analysis (SCA), which became one of the pillars of physical security in a broader sense. In SCA, an adversary would not leverage mathematical weaknesses of a cryptographic algorithm to recover sensible data, while making use of physical emissions, or side channels, directly from the device, such as power consumption [2], execution time [1] and electromagnetic emission [3]. The rationale behind SCA is based on the fact that those physical emissions can be related to the data processed within the device. Clearly, in the last two decades, SCA has become a serious threat in security and a critical issue for the designers of cryptographic hardware, therefore becoming a focal point in the development of secure products.

In the era of nanometer CMOS technologies, the role of the leakage currents of MOS transistors resulting in static power dissipation has become increasingly important in the power balance of digital integrated circuits, especially when referring to ultra-constrained applications. In addition to the technological problem due to static power consumption, an important security issue was formulated and addressed by Alioto et al. in 2010 [4]. In this context, it is important to notice that the static power of CMOS integrated circuits strongly depends on the input vectors, and the exploitation of the correlation between input data and static power paved the way for a new class of side-channel attacks. Conventional power analysis leverages dynamic power consumption, which in the past has been historically dominant in CMOS integrated circuits. Many countermeasures have been proposed against conventional power analysis attacks, mainly summarized into two categories: hiding, where the dynamic data-dependent consumption is hidden within physical and algorithmic noise, and masking, where random and independent data are processed along the real ones in order to mask the overall physical observation from the exploitable ones. The first category aims to reduce the exploitable signal compared to noise, while the second one aims to increase the algorithmic noise that the adversary can measure/observe. Clearly, in digital integrated circuits design flow, hiding and masking countermeasures can be applied at different abstraction levels. A popular way to reduce the data-dependent component of dynamic power consumption at gate-level is based on the adoption of Dual-rail Pre-charged Logics (DPLs). DPLs aim to balance the switching activity factor for each gate in a design in order to deploy an overall power consumption that is independent from processed data by means of differential gates and (differential) Return-to-Zero (RTZ) encoding. Common DPLs that have been investigated in the literature to decorrelate the power consumption from manipulated data include Wave Dynamic Differential Logic (WDDL) [5], Masked DPL (MDPL) [6], Dynamic and Differential Swing-Limited Logic (DDSLL) [7] and Sense Amplifier Based Logic (SABL) [8].

The aforementioned logic styles are theoretically secure, but, in practice, their effectiveness is strongly limited by technological issues concerning a balanced routing assumption that is hardly reachable in practice. In fact, in the presence of electrical mismatches in the capacitive (and resistive) load of complementary outputs of DPL gates, their effectiveness in counteracting power analysis attacks is heavily reduced [9], as well as in the presence of tight routing constraints. Their applicability to sub-micron technologies is worsened by the increasing and dominant role of routing in the capacitive contribution and almost impossible in FPGA, where the possibility to effectively balance the routing is strongly reduced compared to ASIC. Bucci et al. [10] proposed the Delay-based DPL (DDPL) as a power analysis-resistant logic style that is insensitive to imperfect routing. The DDPL makes use of an alternative data encoding protocol, called Time Enclosed Logic (TEL) [11]. In the TEL protocol, the datum represented by a pair of complementary wires is encoded in their time of arrival in the 0 → 1 transition, which, in other words, corresponds to the time difference of the two wires in reaching V_{DD}. As this time difference decreases, the effect of unbalanced capacitive loads is pushed towards high frequencies, so that it can be easily cut-off by means of on-chip power-rail decoupling capacitances. An improved implementation of DDPL (namely, iDDPL) is proposed in [12], where the effectiveness of the TEL protocol in thwarting conventional power analysis attacks even in presence of imperfect routing is demonstrated on a prototype 65 nm CMOS ASIC. Both DDPL and iDDPL require a full-custom design, which inevitably impacts on the development cost of a secured hardware macro. Recently, a novel TEL-compliant standard-cell logic style has been proposed, namely Standard-Cell Delay-based DPL (SC-DDPL) [13]. SC-DDPL is insensitive to routing unbalance and offers a portable solution to protect cryptographic circuits against power analysis including on FPGA platforms. Bellizia et al. [13] reported a remarkable ability of the SC-DDPL to withstand conventional power analysis attacks based on the exploitation of dynamic power consumption.

The idea that TEL protocol may provide protection against Attacks Exploiting Static Power (AESP) techniques, as this encoding scheme strongly reduces the time interval in which data can leak, was introduced for the first time by Bellizia et al. [14], and a preliminary study of the capability of SC-DDPL to withstand AESP was presented by Bellizia [15].

In this work, we analyze in detail the resilience of the SC-DDPL against AESP, providing a twofold contribution:

- We validate the robustness of the TEL protocol to static power analysis, according to Bellizia et al. [14].
- We validate the SC-DDPL as an effective countermeasure to this kind of attacks by means of a full set of experimental results on a reprogrammable device.

The paper is organized as follows. In Section 2, a review of AESP and the related evaluation methodologies is presented. In Section 3, we briefly recall the TEL protocol and describe the SC-DDPL operation principles and circuits. Experimental results in which AESP were carried out on several FPGA implementations of a compact PRESENT crypto-core are reported and discussed in Section 4. Finally, conclusion are drawn in Section 5.

2. Review of Attacks Exploiting Static Power

In this section, we briefly recall the AESP as an approach to recover sensible information from a nanometer CMOS implementation of a cryptographic circuit exploiting its static power consumption as a source of information leakage. With the aggressive scaling of MOS transistors channel lengths in the nanometer regime, several second-order effects such as reverse bias-pn junction leakage, sub-threshold leakage, drain-induced barrier lowering and threshold voltage (V_{TH}) roll off are no longer negligible and result in a continuous increase of static current dissipation of CMOS integrated circuits (ICs). Since the static current is correlated to the input data of CMOS cryptographic ICs, it can be considered as an additional side channel that an attacker can exploit to infer the secret keys. Among several physical effects, sub-threshold leakage currents represent the most dominant one in modern deep-scaled technologies (<100 nm). The sub-threshold leakage current I_{sub} of MOS devices depends on several factors and a comprehensive model of this current is given by [16]:

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

where W and L are the gate width and length, respectively; V_{TH} is the threshold voltage; and V_{GS}, V_{DS} and V_{SB} denote the gate-source voltage, the drain-source voltage and the source-body voltage, respectively. K, η and γ are technology-dependent constants and V_T is the thermal voltage defined as follows:

$$V_T = \frac{kT}{q} \tag{2}$$

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

As observed in [17], the magnitude of the static current of a circuit can be correlated with the data processed within the circuit itself. Research activity dealing with the relationship between the static power consumption of CMOS ICs and their input data has been triggered, at the beginning of this century, by the necessity to reduce the static power consumption of microprocessors implemented in nanometer CMOS processes. These studies have found that there is a strong relationship between the value of the static power dissipation of a digital CMOS circuit and the input state of the different CMOS logic gates upon which it is built. Starting from 2007, several studies have shown that the correlation between the static power consumption and the input vectors of cryptographic ICs can be exploited by a novel class of attacks firstly denoted as "Leakage Power Analysis Attacks" and then renamed as "Attacks Exploiting Static Power" (AESP) [14]. AESP are able to infer the secret keys through the exploitation of the correlation between the static power of a CMOS implementation of a cryptographic algorithm and its input data, which can be controlled by a malicious attacker. Most hardware implementations of cryptographic algorithms are based on bit-sliced circuits, in which the static power of the whole circuit can be computed as the sum of the static powers of the m-bit slices. The static power of each bit-slice is assumed to be equal to the high (or low) value of the static power P_H (or

P_L) according to the value '1' or '0' of the corresponding input bit [4]. Then, remembering that the number of '1's in the input vector represents its Hamming Weight (HW) w, the static power consumption of a m-bit slice is easily found to be:

$$P_{stat} = w \cdot P_H + (m - w) \cdot P_L = w \cdot (P_H - P_L) + m \cdot P_L \tag{3}$$

The above model expresses the linear dependency of the static power of a slice on the HW of its input vector [18,19].

Leveraging on the linear relationship between the static power and the Hamming Weight of input vectors of a circuit, an AESP makes use of the Pearson's correlation coefficient to exploit the data-dependency and recover sensible information. The correlation coefficient of a key guess k using l static power samples is computed as follows:

$$\rho_k = \frac{\sum_{i=1}^{l}(H_{i,k} - \overline{H_i}) \cdot (P_{stat,i} - \overline{P_{stat}})}{\sqrt{\sum_{i=1}^{l}(H_{i,k} - \overline{H_i})^2 \cdot (P_{stat,i} - \overline{P_{stat}})^2}} \tag{4}$$

where $H_{i,k}$ is the Hamming Weight of a intermediate function of the input with index i and key guess k (e.g., the output value of the XOR between key and input plaintext), H_i is the average Hamming Weight value, $P_{stat,i}$ is the static power due to the input with index i and $\overline{P_{stat}}$ is the average static power value.

2.1. Threat Model

In the context of AESP, it is common to assume that the adversary has the ability to control the clock signal and, in particular, to stop it freely (see Figure 1). This assumption is widely used in the literature, as recently discussed by Moos [20]. Moos noted that this assumption may not be needed in all cases, and it could be sufficient that the target intermediate variable is stable for some time (it is reported as a "certain number of cycles") to be exploited, even in the presence of algorithmic noise. Therefore, we can safely assume that performing experiment with such strong assumption would lead to a worst-case analysis from the security point of view.

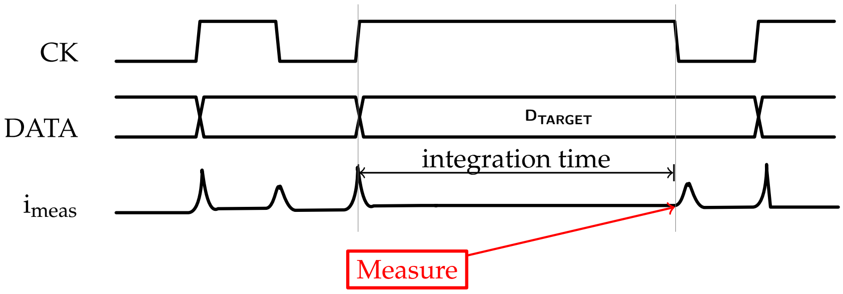


Figure 1. Stopping clock signal to extract a static current measurement.

2.2. Related Works on AESP

After a hiatus of some years, the hardware security community has recently started again to investigate on AESP and to analyze security issues due to this particular side channel. Djukanovic et al. [21] discussed the role of temperature as a dimension to increase the informativeness of static current, through simulated experiments at various temperature, also considering a multivariate approach. In [22], Moradi demonstrated the feasibility of AESP attacks over three different FPGA technologies, also adopting a protected AES-based crypto-core. These results were extended by Moos [20], presented at *CHES'19*, to different ASIC technologies, giving also an insight on vulnerabilities of Boolean masked implementations to AESP. Another paper presented at *CHES'19*, by Karimi et al. [19], proposes a study of the impact of device aging on the exploitability of static power, based on measurements taken on 65 nm prototype ASICs. This study shows that the degradation of an integrated circuit due to aging effects reduces the informativeness of static currents, hence increasing the effort for their exploitation. In [18], Moos et al. proposed a survey of the impact of several measurement factors on the outcome of an AESP, such as temperature (as in [21]), power supply voltage and integration time, providing results on a 150 nm ASIC prototype chip.

It has to be noted that the analysis of DPLs as gate-level countermeasures against attacks exploiting static power was only investigated from a simulated perspective by Bellizia et al. [14]. In addition, none of the available TEL-compatible logics have been studied experimentally under this point of view.

2.3. Security Metrics

In accordance with previous works [23,24], we compliment our AESP attacks with a leakage assessment based on the adoption of the *Signal-to-Noise Ratio* (*SNR*) proposed by Mangard [25], which allows an intuitive quantification of the side-channel signal strength against the observed noise. *SNR* is computed as the ratio between the variance of the data-dependent component of the power consumption σ^2_{data}, in this case static power, and the variance of the observed noise σ^2_{noise}:

$$SNR_{naive} = \frac{\sigma^2_{data}}{\sigma^2_{noise}} \tag{5}$$

Usually, the *SNR* in static power measurements is much lower compared to dynamic ones. Therefore, we make use of a logarithmic transformation of the *SNR* for practical reasons:

$$SNR = 10 \cdot \log_{10}\left(\frac{\sigma^2_{data}}{\sigma^2_{noise}}\right) \tag{6}$$

In our AESP evaluation, we use also an information theoretic approach, leveraging the concept of *mutual information* (*MI*). *MI* [26] is based on Shannon's conditional entropy and quantifies the amount of information leaked by the hardware implementation under test, considering the side channel as a noisy channel. It is defined as follows:

$$MI(X;L) = H[X] - \sum_{x \in X} \Pr(x) \sum_{l \in L} \Pr_{\text{chip}}(l|x) \log_2 \Pr_{\text{chip}}(x|l) \tag{7}$$

where $H[X]$ is the entropy of the secret variable (key) X, $\Pr(x)$ is the probability of the secret variable $x \in X$ and $\Pr_{\text{chip}}(l|x)$ is the probability of the leakage l given the secret x. Clearly, $\Pr_{\text{chip}}(x|l)$ can be derived using the Bayes's theorem. In our analysis, we use the Gaussian model assumption on the distributions, as, in previous observations, it was found that this model is sound and therefore applicable.

In addition to SNR and mutual information, we also perform the Test Vector Leakage Assessment (TVLA) [27] based on Welch's t-test on our static power analysis of the SC-DDPL. The t-test is a statistical test that allows verifying if two classes of samples A and B belong to the same population by means of comparing their first-order statistics, also called null hypothesis. The t-test is widely diffused in the SCA literature, and it has recently been intensively used also for AESP leakage assessment. Usually, a threshold value of the t-test score $|t| > 4.5$ (the value of 4.5 is used to ensure a statistical confidence higher than 0.9999) means that classes A and B do not belong to the same population (thus, rejecting the null hypothesis), remarking the presence of data-dependent leakage in the side-channel samples. The t-test score can be evaluated as follows:

$$t = \frac{(\overline{L_A} - \overline{L_B})}{\sqrt{\frac{\sigma^2_A}{N_A} + \frac{\sigma^2_B}{N_B}}} \tag{8}$$

where $\overline{L_A}$ (respectively, $\overline{L_B}$) represents the mean value of the static power samples of Class A (respectively, Class B), σ^2_A (respectively, σ^2_B) represents variance of Class A (respectively, Class B) and N_A (respectively, N_B) is the cardinality of Class A (respectively, Class B).Classes

A and B can be partitioned according to a *fixed versus random* approach [27] or with the *fixed versus fixed* one [28].

3. TEL Protocol and SC-DDPL

In this section, we briefly recall the TEL protocol and describe the SC-DDPL operation principles and circuits.

3.1. TEL Protocol

In the last two decades, Dual-rail Pre-charge Logics (DPLs) have been widely studied as gate-level countermeasures against conventional power analysis attacks. Most DPLs, such as WDDL, SABL and MDPL, are based on the Return-to-Zero (RTZ) protocol for encoding data processed within a secure circuit. In the RTZ protocol, a clock cycle is divided into two phases, called *pre-charge* and *evaluation* phases. During the *pre-charge* phase, both wires of a dual-rail pairs are pre-charged to a known value (0 or 1), while, during the *evaluation* phase, they assume the informative value 0/1 or 1/0 (see Table 1). Ideally, the presence of a complementary value on a dual-rail pair would allow achieving data-independent power consumption. However, this goal is hard to be reached in practice, as RTZ-based DPLs require perfect capacitive load balance. One of the main causes of capacitive unbalance is the routing between secure gates, which is usually hard to balance in deep-scaled technologies. Especially on FPGAs, where designers do not have a full control on layout results, this effect is particularly critical for the effectiveness of RTZ-based DPLs in counteracting power analysis [9]. In addition, some DPLs, such as WDDL, make use of inherently asymmetric combinational gates, providing an additional source of unbalancing, also under a static power point of view.

In order to cope with these issues, the Time Enclosed Logic (TEL) protocol was introduced in 2011 [10] and later formalized in 2015 [11]. The TEL protocol encodes data in the time of arrival of the two wires in a dual-rail pair, as shown in Figure 2. The clock period T_{CK} is divided into three phases:

- Pre-charge phase (t_{pre}): Both wires are pre-charged to 0.
- Evaluation (t_{eval}): One of the wires reaches V_{DD} before the other, according to the representation of the data in Figure 2 and Table 1.
- Post-charge phase (t_{post}): Both wires reach V_{DD} and keep this level to the end of the clock period.

It is straightforward to observe the following:

$$T_{CK} = t_{pre} + t_{eval} + t_{post} \tag{9}$$

In particular, the evaluation phase length is very critical from a security perspective. In fact, to reduce the information leakage due to capacitive unbalance, t_{eval} has to be kept really short. In other words,

$$t_{eval} \ll T_{CK} \tag{10}$$

This condition is deeply investigated in [11,13]. In fact, as the evaluation phase is reduced, the effect of capacitive unbalance in terms of information leakage's frequency content is moved to high frequencies (in the range of hundreds of MHz). From a designer perspective, this effect allows the information leakage to be filtered off (e.g., by low-pass effect of the on-chip power grid's parasitic capacitance or by explicit on-chip filtering). The value of t_{eval} depends on several factors, such as the technology node, design requirements and security constraints. Of course, the value of t_{eval} depends on several factors. It is evident that the value of this parameter is technology dependent, as newer technologies can support shorter evaluation phase, due to shorter propagation delay. However, this value is also design-dependent, as it is limited by the pipeline architecture, according to the time enclosed principle introduced in [11] (typical values for t_{eval} are in the range of hundreds of picoseconds to nanoseconds, in order to shift the informative leakage frequency in the range of hundreds of MHz to GHz) and by security requirements.

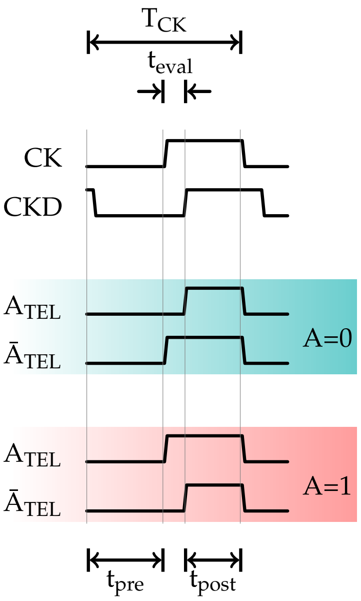


Figure 2. TEL encoding timing diagram.

Table 1. RTZ and TEL dual-rail encoding.

	RTZ Protocol		TEL Protocol		
Log.Value	**Pre-Charge**	**Evaluation**	**Pre-Charge**	**Evaluation**	**Post-Charge**
A	(A_{RTZ},$\bar{A}_{RTZ}$)	(A_{RTZ},$\bar{A}_{RTZ}$)	(A_{TEL},$\bar{A}_{TEL}$)	(A_{TEL},$\bar{A}_{TEL}$)	(A_{TEL},$\bar{A}_{TEL}$)
0	(0,0)	(0,V_{DD})	(0,0)	(0,V_{DD})	(V_{DD},V_{DD})
1	(0,0)	(V_{DD},0)	(0,0)	(V_{DD},0)	(V_{DD},V_{DD})
NULL	(0,0)	(0/V_{DD},0/V_{DD})	(0,0)	(0/V_{DD},0/V_{DD})	(V_{DD},V_{DD})

3.2. SC-DDPL Operation

Recently, Bellizia et al. proposed the Standard-Cell Delay-based Dual-rail Pre-charge Logic (SC-DDPL) as the first standard-cell based logic style that can support the TEL protocol [13]. In order to be compliant with the TEL protocol, the SC-DDPL has been designed to fulfill the *completeness* property [29]. Inspecting the Table 1, we can clearly observe that in a TEL circuit the dual-rail information is encoded as a mutually exclusive value in asserted domain; thus, only one wire of the pair is asserted during the evaluation phase. Moreover, the *NULL* value is used to guarantee that the Boolean logic is symbolically complete, which implies the *completeness* of the set. This *completeness* is relevant as it allows the synchronization of the output signals of a TEL gate [29]. In order to guarantee the *completeness* property, each gate has to be designed according to the following requirements:

$$\begin{cases} out = F_1(A_1, A_2, ..., A_n, \overline{A_1}, \overline{A_2}, ..., \overline{A_n}) \\ \overline{out} = F_2(A_1, A_2, ..., A_n, \overline{A_1}, \overline{A_2}, ..., \overline{A_n}) \end{cases} \tag{11}$$

It has to be noted that each signal of a gate has to perform the ’0’ to ’1’ and the ’1’ to ’0’ transitions in the same clock cycle. According to Tiri and Verbauwhede [5], Bellizia et al. [13], the latter requirement for security and TEL-compliance concerns F_1 and F_2, which have to be *positive monotonic*. The NAND operator is able to satisfy all these requirements, and it has served as base function to design each SC-DDPL combinational gate. For example, the AND/NAND function can easily be derived from Equation (11) adopting a product-of-product approach:

$$F_1 = \overline{\overline{A \cdot B}} = A \cdot B = AND \tag{12}$$

$$F_2 = \overline{\overline{(\overline{A}\cdot\overline{B})}\cdot\overline{(\overline{A}\cdot B)}\cdot\overline{(A\cdot\overline{B})}} = \overline{A\cdot B} = NAND \tag{13}$$

Equations (12) and (13) represent the equivalence of non-minimal AND and NAND, respectively, built upon a two-stage template. It has to be noted that a straightforward implementation in static CMOS gates of Equations (12) and (13) would lead to an asymmetric architecture of the secure SC-DDPL gate (details in [13]), and therefore Equation (12) is adapted as follows:

$$F_1 = \overline{\overline{(A\cdot B)}\cdot 1\cdot 1} = AND \tag{14}$$

With Equations (13) and (14), the AND/NAND function in SC-DDPL is obtained using standard-cell NAND2 and NAND3 gates, as depicted in Figure 3. It is easy to observe that from a power analysis perspective such construction allows a good balancing. Other combinational gates can be derived easily. It has to be noted that this architecture does not require any custom logic, as only static NAND2 and NAND3 gates are used (usually available in all design kits). Moreover, this architecture is easily portable to FPGA, as it is possible to design it using only LUTs. This feature represents a strong point compared to DDPL/iDDPL.

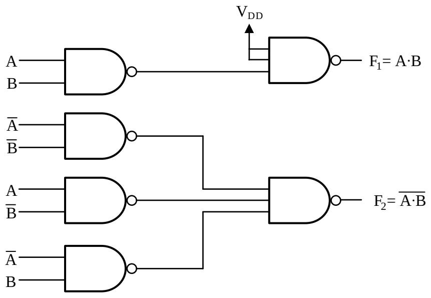


Figure 3. SC-DDPL AND/NAND gate with symmetric architecture.

As a remark, we must notice that the SC-DDPL, as any other TEL-compliant logic styles, requires the use of a second clock, namely *CKD* (see Figure 2), which is a delayed version of the nominal clock signal *CK*. Its delay corresponds to the nominal t_{eval}, and it is distributed to input converters and flip-flops. Such delayed replica can be easily generated on-chip, reducing the attack surface to a stronger SCA adversary.

3.3. SC-DDPL Effectiveness against AESP

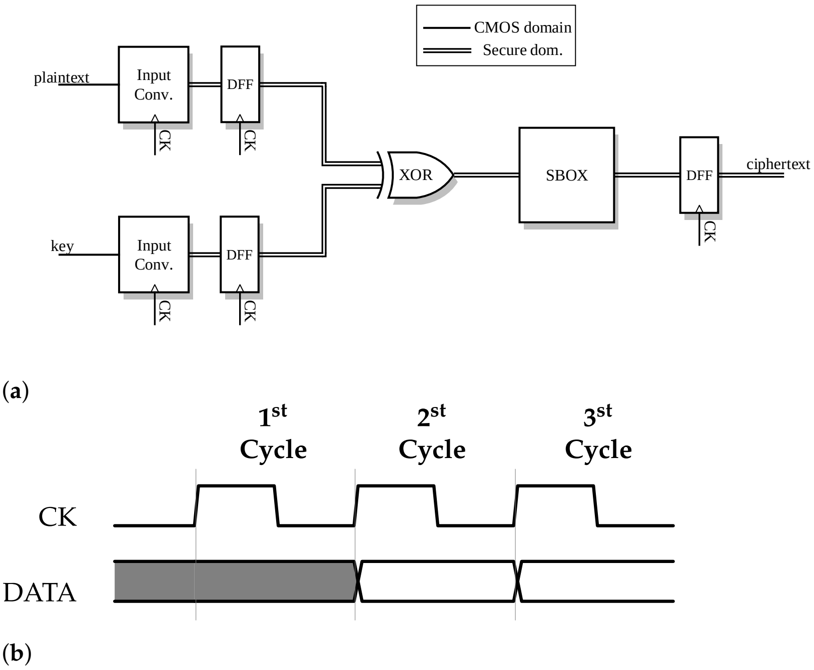
SC-DDPL was studied and tested along with other DPLs from a dynamic power exploitability viewpoint by Bellizia et al. [13], exhibiting stronger resilience against conventional power analysis attacks compared to other logic styles referring to both 40 nm CMOS simulations and real experiments on FPGA platforms. Bellizia et al. [14] discussed about potential vulnerability issues of DPLs regarding AESP. More precisely, mutual information analysis as a function of noise standard deviation has shown that MDPL and WDDL (both standard-cell based DPLs) exhibit a *leakier* behavior than static CMOS, remarking that only the full-custom SABL approach outperforms the CMOS unprotected implementation. Bellizia et al. [14] reported only a preliminary discussion about the possibility of using TEL-based logic styles as countermeasures against AESP. As an additional remark, we observe here that, since the TEL protocol encodes the information in the difference of the arrival time of two complementary wires, no potential leaks can be observed in the static power consumption if the clock is stopped. Being SC-DDPL based on the TEL protocol, we focus on the investigation and analysis of its resilience against AESP.

4. Experimental Results

In previous works, the possibility to use the TEL encoding as a countermeasure against AESP has only been suggested, and no experimental or simulated results are provided to support this claim. In this section, we report first experimental results on the AESP resilience of a TEL-compliant SC-DDPL FPGA implementation of a compact PRESENT crypto-core, alongside with a comparison with other RTZ-based DPLs.

4.1. Case Study — 4-bit PRESENT Crypto-Core

As a case study, we considered the 4-bit cryptographic core in [13], as shown in Figure 4a, based on a nibble slice of the first round of the PRESENT algorithm [30]. PRESENT is a lightweight block cipher designed for constrained applications (e.g., RFID tags and IoT nodes) and part of the ISO/IEC 29192-2:2012 standard. The circuit implements the 4-bit XOR between the input plaintext and the key, an instance of the PRESENT 4-bit SBOX and input/output registers. We implemented four different cores, based on CMOS logic, WDDL, MDPL (the MDPL core requires randomness that we generated by means of a linear-feedback shift register, used as Pseudo-Random Number Generator (PRNG)) and SC-DDPL, in order to compare their resistance against AESP and extend the analysis in [13] to the static power domain. Clearly, input converters were added in the protected versions of the 4-bit core to allow interfacing the unsecured static CMOS domain with the secured circuitry. As Device Under Attack (DUA), we used an Intel Cyclone-IV FPGA (65 nm technology). Along with the cryptographic module, we implemented an UART interface on the FPGA, in order to deploy a communication channel with the external environment. The *CKD* clock replica required by the SC-DDPL was generated by the on-chip PLL and set to 4 ns.



(**a**)

(**b**)

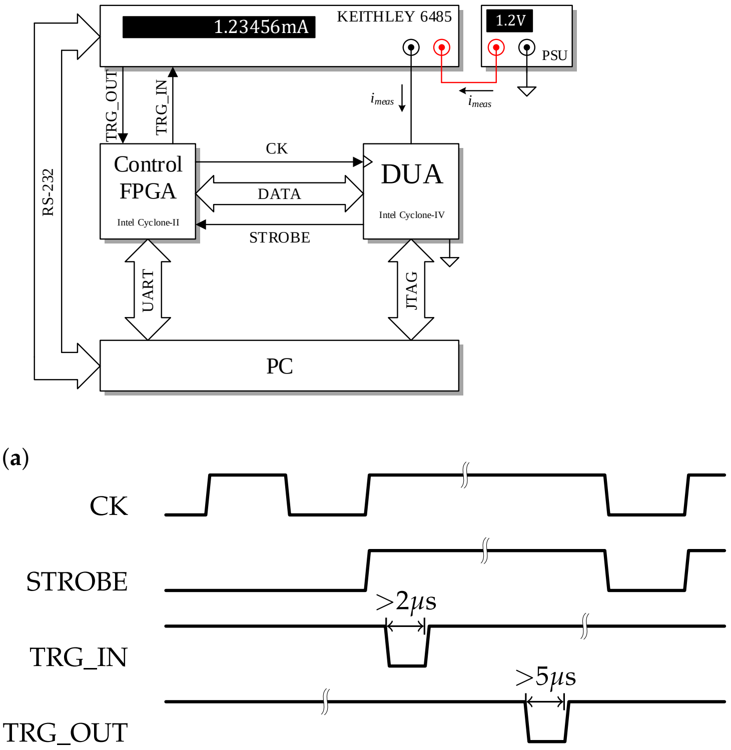
Figure 4. The 4-bit PRESENT crypto-core circuit (**a**) and timing diagram (**b**). Note that the architecture is clocked on the rising-edge for all considered logic styles.

4.2. Measurement Setup

In accordance with Bellizia et al. [31], we used a measurement setup based on the utilization of a picoammeter in place of the conventional digital storage oscilloscope, widely used in the literature to carry out attacks exploiting dynamic power. Adopting such strategy allows a direct current measurement, bypassing the need of voltage-to-current conversion, amplifiers and low-pass filters [18], hence simplifying the setup itself while avoiding unwanted distortions. As picoammeter, we used a Keithley 6485, which is designed to perform high-precision static current measurement.

In previous works, it has been demonstrated that performing experiments at higher (than room) temperature leads to more informative measurements [18,21]. Therefore, we adopted the same heating system used in [31], setting the working temperature of the DUA at 65 °C. The power supply voltage of the DUA's core was set to 1.2 V by using a bench-top power supply.

The measurement setup was controlled by a *Matlab* script, which provides/reads input/output data to/from the target and collects static current samples from the picoammeter. The target handled the triggering sequence of the Keithley for performing the measurement using a trigger handshake (TRG_IN and TRG_OUT signals) with the instrument. The trigger handshake was partially implemented on a control FPGA (i.e., an Intel Cyclone-II development board). A block scheme of the measurement setup and a timing diagram of the triggering sequence is depicted in Figure 5. As also suggested in [18], the integration time (also shown in Figure 1) was set as a trade-off between speed, in terms of sample collected per unit of time and noise. In our experiments, a good trade-off was found for a 0.25 power-line cycle, corresponding to 5 ms of integration time.



(**a**)

(**b**)

Figure 5. Measurement setup block diagram (**a**) and triggering sequence (**b**).

The encryption operation takes place in three clock cycles, being the first one consumed only for loading the input plaintext and key into the core. Therefore, only the second and third cycles are meaningful for our analysis, as they are the two involved in the real cryptographic operation. Adopting the threat model in Section 2.1, and therefore assuming that the adversary has full control on the main clock signal *CK*, static current values were recorded for each value of the stable clock signal (*CK* = '0' and *CK* = '1') in the third cycle (see Figure 4b), hence collecting two samples of the static current. In order to perform the attack, the output nibble of the XOR operator was chosen as the target function. Then, for each value of the stable clock signal (*CK* = '0' and *CK* = '1'), 64 k values of static current were acquired for the countermeasure cores, whereas only 16k values were acquired for the CMOS core.

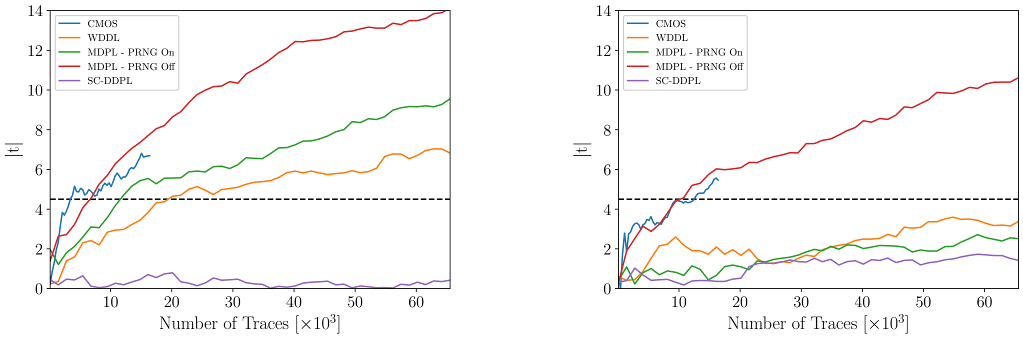
4.3. Leakage Assessment

The first analysis that we carried out is related to the comparison between the MDPL core and the unprotected CMOS core. The results of our evaluations referring to the *evaluation phase* of the MDPL core with PRNG disabled show that it exhibits an *SNR* about equal to the one of the CMOS implementation, whereas the mutual information of the MDPL core was found higher than the one of the unprotected CMOS core. These results are in partial agreement with those of Bellizia et al. [14]. Then, we compared all the countermeasure cores in terms of *SNR* and mutual information, showing that the SC-DDPL core exhibits the best values for both these metrics compared to other countermeasures. In particular, we found that the *SNR* is about 10 dB lower than the one of the CMOS core, whereas it is at least 5 dB lower than those of MDPL and WDDL cores. The SC-DDPL core exhibits a mutual information of 3.18×10^{-3} bit, which is one order of magnitude lower than the mutual information of the CMOS and MDPL (with PRNG off) implementations. All the above results (summarized in Table 2) confirm the claims reported in [14].

Table 2. Summary of the security metrics computed from static current values measured during the third clock cycle.

Impl.	**CK = ’0’**			**CK = ’1’**		
	SNR [dB]	**MI(X;L) [$\times 10^{-3}$]**	**σ_{data} [nA]**	**SNR [dB]**	**MI(X;L) [$\times 10^{-3}$]**	**σ_{data} [nA]**
CMOS	−19.90	19.09	416	−18.15	28.54	537
WDDL	−24.11	7.27	259	−24.51	6.63	260
MDPL-PRNGon	−23.51	8.34	416	−25.77	4.97	302
MDPL-PRNGoff	−19.57	20.65	493	−18.02	29.39	568
SC-DDPL	−28.31	2.76	184	−27.70	3.18	199

As most of the considered case studies are non-masked, we performed the *fixed versus fixed t*-test, as suggested in [28], to find the evidence of leakage through this widely adopted assessment methodology. The results of the *t*-test analysis as a function of the number of traces are reported in Figure 6a for *CK* = ’0’ and Figure 6b for *CK* = ’1’. The CMOS implementation is reported as a reference for comparison against protected cores. WDDL and MDPL show a meaningful *t*-test score already with a limited number of traces on the case with *CK* = ’0’, as the threshold value of 4.5 is exceeded at ∼10 k, as the CMOS in the same setting. The SC-DDPL does not show any meaningful leakage in both cases with *CK* = ’0’ and *CK* = ’1’. The value at 64 k traces is 0.4 for *CK* = ’0’ and 1.42 for *CK* = ’1’. These results are partially in line with the findings in [14] concerning RTZ-based DPLs, and they show how the TEL encoding is able to suppress the informativeness of the leakage through static power analysis.



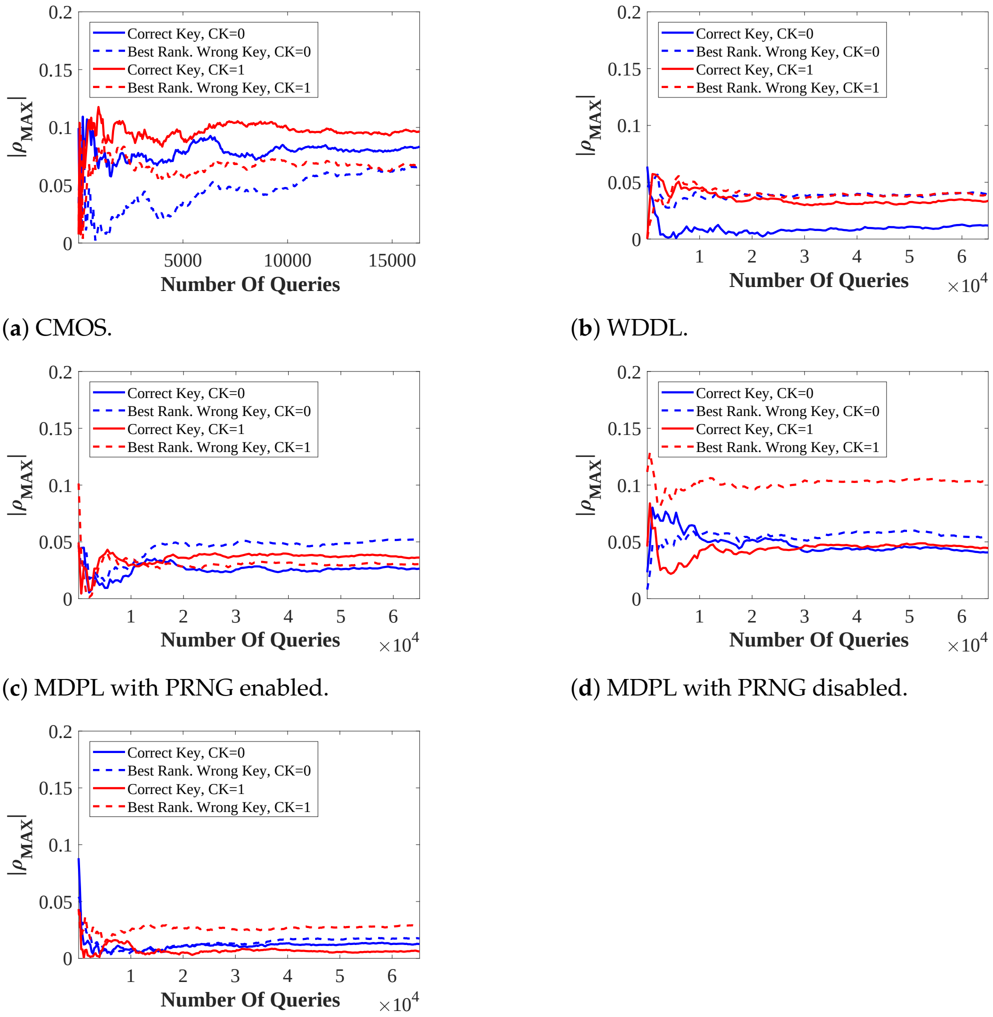
(**a**) *CK*=’0’.

(**b**) *CK*=’1’.

Figure 6. Absolute *T*-test score versus number of traces for PRESENT core implementations at third cycle with: *CK* = ’0’ (**a**); and *CK* = ’1’ (**b**).

4.4. AESP Results

The outcomes of the AESP attacks are reported in Figure 7 and summarized in Table 3 in terms of measurements-to-disclosure (MTD) for both *CK* = ’0’ and *CK* = ’1’. The AESP attacks succeeded in retrieving the secret key only for the CMOS and MDPL implementations. In particular, the correct key of the MDPL implementation was recovered only with *CK* = ’1’ and the PRNG enabled. A possible explanation of this result can be found noting that, in the RTZ countermeasures, during the evaluation phase, the inputs of both the combinational gates and the flip-flops are set to their evaluation values. This is similar to what can be observed in the CMOS implementation, in which the inputs are always set to their evaluation values. Therefore, in all the above cases, there is a strong correlation between the input data and the static current which can be exploited by the attacker. The results of the AESP on the MDPL countermeasure (see Figure 7c) also demonstrate that the adoption of the PNRG in the MDPL is not able to counteract the effectiveness of the AESP.



(**a**) CMOS.

(**b**) WDDL.

(**c**) MDPL with PRNG enabled.

(**d**) MDPL with PRNG disabled.

(**e**) SC-DDPL.

Figure 7. Absolute correlation coefficient $|\rho_{MAX}|$ vs. the number of queries used to perform AESP: CMOS (**a**); WDDL (**b**); MDPL with PRNG enabled (**c**); MDPL with PRNG disabled (**d**); and SC-DDPL (**e**).

Table 3. Summary of AESP attacks on the different PRESENT cores (T = 65 °C).

Impl.	**CK = '0'**				**CK = '1'**			
	MTD	$\vert\rho_{MAX}\vert$	**SVI**	**SVI%**	**MTD**	$\vert\rho_{MAX}\vert$	**SVI**	**SVI%**
CMOS	2060	0.0836	+0.0180	+21.53%	411	0.0960	+0.0286	+70.21%
WDDL	>64*k*	0.0119	−0.0274	−230.25%	>64*k*	0.0337	−0.0051	−15.14%
MDPL-PRNGon	>64*k*	0.0265	−0.0258	−97.36%	12.5*k*	0.0362	+0.0058	+83.98%
MDPL-PRNGoff	>64*k*	0.0407	−0.0136	−33.41%	>64*k*	0.0445	−0.0581	−130.56%
SC-DDPL	>64*k*	0.0128	−0.0047	−36.71%	>64*k*	0.0079	−0.0179	−213.92%

As shown in Figure 7e and Table 3, the SC-DDPL implementation was not broken, even with the maximum number of measurements, confirming its capability to withstand AESP.

A further analysis of AESP outcomes can be carried out by considering the *Success Value Indicator* (SVI), defined as the difference between absolute correlation coefficient values of the correct key ρ_{corr} and wrong key that exhibits the highest (absolute) correlation coefficient ρ_{wrong}. To achieve a fair comparison among different implementations with different absolute values of the correlation coefficients, we also adopted the *normalized* $SVI_{\%}$, defined as follows:

$$SVI_{\%} = \frac{SVI}{\max(|\rho_{corr}|, |\rho_{wrong}|)} \cdot 100 = \frac{|\rho_{corr}| - |\rho_{wrong}|}{\max(|\rho_{corr}|, |\rho_{wrong}|)} \cdot 100 \qquad (15)$$

$SVI_{\%}$ is a useful metric to quantify the effective reduction of the value of the statistical distinguisher allowed by a given countermeasure. As shown in Table 3, the SC-DDPL approach results in a $SVI_{\%}$ of −213.92% for CK = '1' and −36.71% for CK = '0', thus outperforming other DPLs. Another important result achieved by the SC-DDPL implementation is that it exhibits the lowest correlation coefficient ($|\rho_{corr}|$ = 0.0079) among all other implementations.

The motivation behind these good results can be found by noting that, when the attacker stops the *CK* signal (and consequently stops also *CKD*), all combinational gates are in the pre-charge or post-evaluation phase, thus assuming the same input and output states regardless of the value of *CK*. Therefore, the mutual information leaked by SC-DDPL combinational gates is theoretically zero. The only information that can be reliably extracted by measuring the static power of SC-DDPL implementation is related to storage elements (e.g., flip-flops) of the system. However, the symmetric architecture of the SC-DDPL storage elements allows minimizing the information which they can leak through static power. More specifically, the presence of two symmetric and homogeneous branches for each sub-block in the flip-flop and the fact that, for each possible TEL state of the input data, the number of transistors that are switched off/on is the same for each value of *CK* also make the information leakage through static power of the flip-flops ideally zero.

4.5. Discussion

According to the leakage assessment and AESP outcomes, we can observe that the TEL-compatible SC-DDPL outperforms all considered RTZ-based DPLs. These results confirm the intuitions in [14] regarding the ability of TEL-compatible logics to withstand a static power adversary. The possibility to confine the information leakage in a (very) short time window that is not under control of the adversary along with intra-gate homogeneity allows designing a secure circuit that is not vulnerable to static (nor dynamic) power analysis. The outcome of this investigation suggests that TEL encoding is a valuable approach in securing circuits from SCA, also considering an adversary that is able to control the main clock. Even considering the latest findings of Moos [20], if we relax the needs of full control on the clock signal from an adversarial perspective, we expect that SC-DDPL, and in general TEL-compatible DPLs such as iDDPL, would not exhibit any meaningful informative leakage as static power consumption.

A summary of the resource utilization of the crypto-cores is reported in Table 4. It is straightforward to notice that the SC-DDPL requirements are in between those of MDPL and WDDL, making it suitable for many area-constrained applications where security against dynamic and static power analysis is required.

Table 4. Utilization of the various implementations of the PRESENT crypto-core on the Intel Cyclone-IV FPGA and design characteristics. Note that the average static power consumption is reported for the whole core power supply, and thus not used resources also contribute to the overall absorption.

Impl.	CMOS	WDDL	MDPL *	SC-DDPL
RTZ	-	✓	✓	✓
TEL	-	✗	✗	✓
Need Randomness	-	✗	✓	✗
Tolerance Cap. Unbalance	-	✗	✗	✓
LUTs	30	154	784	486
Regs	6	0	34	0
LUT-Reg Pair	13	30	62	6
$\mathbf{P_{dyn}^{AVG}}$ **(@1.2 V, 2 MHz)**	81.25	85.85	268.74	228.68
$\mathbf{P_{stat}^{AVG}}$ **(@1.2 V, 65 °C)**	11.89	11.74	12.01	13.49

* PRNG not included.

5. Conclusions

In this paper, we carry out and in-depth analysis of the effectiveness of the TEL-compliant SC-DDPL logic style as a countermeasure against static power side-channel attacks. Experimental results referring to a 4-bit PRESENT crypto-core implemented on an Intel Cyclone-IV FPGA device show that the proposed SC-DDPL countermeasure outperforms standard-cell and RTZ-based dual-rail logic styles, namely WDDL and MDPL. The evaluation was carried out by means of AESP attacks and thorough leakage assessment, adopting SNR, mutual information and *t*-test. The SC-DDPL implementation showed a strong improvement of all the security metrics compared to reference RTZ-based DPLs and the ability to withstand AESP attacks. These experimental results confirm that the TEL encoding represents a suitable approach in counteracting AESP at gate-level, offering an additional level of protection to this less investigated (but not less important) side channel.

Author Contributions: Conceptualization, D.B. and G.S.; data curation, R.D.S.; investigation, D.B.; methodology, D.B., R.D.S. and G.S.; supervision, G.S.; validation, D.B. and R.D.S.; writing—original draft, D.B.; writing—review & editing, R.D.S. and G.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available in article.

Conflicts of Interest: The authors declare a conflict of interest in regards of Itamar Levi, as he is a frequent collaborator.

References

1. Kocher, P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Advances in Cryptology—CRYPTO '96, Proceedings of the 16th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 1996*; Lecture Notes in Computer Science; Koblitz, N., Ed.; Springer: Berlin/Heidelberg, Germany, 1996; Volume 1109, pp. 104–113.
2. Kocher, P.C.; Jaffe, J.; Jun, B. Differential Power Analysis. In *Advances in Cryptology—CRYPTO '99, Proceedings of the 19th Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 1999*; Lecture Notes in Computer Science; Wiener, M.J., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1666, pp. 388–397.
3. Quisquater, J.; Samyde, D. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In Proceedings of the Smart Card Programming and Security, International Conference on Research in Smart Cards, E-smart 2001, Cannes, France, 19–21 September 2001; Lecture Notes in Computer Science; Attali, I., Jensen, T.P., Eds.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2140, pp. 200–210.
4. Alioto, M.; Giancane, L.; Scotti, G.; Trifiletti, A. Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2010**, *57-I*, 355–367. [CrossRef]

5. Tiri, K.; Verbauwhede, I. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. In Proceedings of the 2004 Design, Automation and Test in Europe Conference and Exposition (DATE 2004), Paris, France, 16–20 February 2004; IEEE Computer Society: Washington, DC, USA, 2004; pp. 246–251.
6. Popp, T.; Mangard, S. Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints. In *Cryptographic Hardware and Embedded Systems—CHES 2005, Proceedings of the 7th International Workshop, Edinburgh, UK, 29 August–1 September 2005*; Lecture Notes in Computer Science; Rao, J.R., Sunar, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3659, pp. 172–186.
7. Nawaz, K.; Kamel, D.; Standaert, F.; Flandre, D. Scaling Trends for Dual-Rail Logic Styles Against Side-Channel Attacks: A Case-Study. In Proceedings of the Constructive Side-Channel Analysis and Secure Design—8th International Workshop, COSADE 2017, Paris, France, 13–14 April 2017; Revised Selected Papers; Lecture Notes in Computer Science; Guilley, S., Ed.; Springer: Cham, Switzerland, 2017; Volume 10348, , pp. 19–33.
8. Tiri, K.; Akmal, M.; Verbauwhede, I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. In Proceedings of the 28th European Solid-State Circuits Conference, Florence, Italy, 24–26 September 2002; pp. 403–406.
9. He, W.; Otero, A.; de la Torre, E.; Riesgo, T. Automatic generation of identical routing pairs for FPGA implemented DPL logic. In Proceedings of the 2012 International Conference on Reconfigurable Computing and FPGAs, ReConFig 2012, Cancun, Mexico, 5–7 December 2012; pp. 1–6.
10. Bucci, M.; Giancane, L.; Luzzi, R.; Scotti, G.; Trifiletti, A. Delay-Based Dual-Rail Precharge Logic. *IEEE Trans. Very Large Scale Integr. Syst.* **2011**, *19*, 1147–1153. [CrossRef]
11. Bongiovanni, S.; Centurelli, F.; Scotti, G.; Trifiletti, A. Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks. *J. Cryptogr. Eng.* **2015**, *5*, 269–288. [CrossRef]
12. Bellizia, D.; Scotti, G.; Trifiletti, A. TEL Logic Style as a Countermeasure Against Side-Channel Attacks: Secure Cells Library in 65 nm CMOS and Experimental Results. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *65-I*, 3874–3884. [CrossRef]
13. Bellizia, D.; Bongiovanni, S.; Olivieri, M.; Scotti, G. SC-DDPL: A Novel Standard-Cell Based Approach for Counteracting Power Analysis Attacks in the Presence of Unbalanced Routing. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2020**, *67-I*, 2317–2330. [CrossRef]
14. Bellizia, D.; Bongiovanni, S.; Monsurrò, P.; Scotti, G.; Trifiletti, A. Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications. *IEEE Trans. Emerg. Top. Comput.* **2017**, *5*, 329–339. [CrossRef]
15. Bellizia, D. Design Methodologies for Cryptographic Hardware with Countermeasures against Side Channel Attacks. Ph.D. Thesis, Sapienza Università di Roma, DIET, Rome, Italy, 2018. Available online: http://hdl.handle.net/11573/1094643 (accessed on 27 May 2021).
16. Chandrakasan, A.P.; Bowhill, W.J.; Fox, F. *Design of High-Performance Microprocessor Circuits*, 1st ed.; Wiley-IEEE Press: Hoboken, NJ, USA, 2000.
17. Narendra, S.G.; Chandrakasan, A. *Leakage in Nanometer CMOS Technologies*; Series on Integrated Circuits and Systems; Springer: Berlin/Heidelberg, Germany, 2005.
18. Moos, T.; Moradi, A.; Richter, B. Static Power Side-Channel Analysis—An Investigation of Measurement Factors. *IEEE Trans. Very Large Scale Integr. Syst.* **2020**, *28*, 376–389. [CrossRef]
19. Karimi, N.; Moos, T.; Moradi, A. Exploring the Effect of Device Aging on Static Power Analysis Attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, *2019*, 233–256. [CrossRef]
20. Moos, T. Static Power SCA of Sub-100 nm CMOS ASICs and the Insecurity of Masking Schemes in Low-Noise Environments. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, *2019*, 202–232. [CrossRef]
21. Djukanovic, M.; Bellizia, D.; Scotti, G.; Trifiletti, A. Multivariate Analysis Exploiting Static Power on Nanoscale CMOS Circuits for Cryptographic Applications. In Proceedings of the Progress in Cryptology—AFRICACRYPT 2017—9th International Conference on Cryptology in Africa, Dakar, Senegal, 24–26 May 2017; Lecture Notes in Computer Science; Joye, M., Nitaj, A., Eds.; Springer: Cham, Switzerland, 2017; Volume 10239, pp. 79–94.
22. Moradi, A. Side-Channel Leakage through Static Power—Should We Care about in Practice? In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2014—16th International Workshop, Busan, South Korea, 23–26 September 2014; Lecture Notes in Computer Science; Batina, L., Robshaw, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8731, pp. 562–579.
23. Bellizia, D.; Scotti, G.; Trifiletti, A. Implementation of the PRESENT-80 block cipher and analysis of its vulnerability to Side Channel Attacks Exploiting Static Power. In Proceedings of the 2016 MIXDES—23rd International Conference Mixed Design of Integrated Circuits and Systems, Lodz, Poland, 23–25 June 2016; pp. 211–216.
24. Pozo, S.M.D.; Standaert, F.; Kamel, D.; Moradi, A. Side-channel attacks from static power: When should we care? In Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, DATE 2015, Grenoble, France, 9–13 March 2015; Nebel, W., Atienza, D., Eds.; ACM: New York, NY, USA, 2015; pp. 145–150.
25. Mangard, S. Hardware Countermeasures against DPA? A Statistical Analysis of Their Effectiveness. In Proceedings of the Topics in Cryptology—CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, 23–27 February 2004; Lecture Notes in Computer Science; Okamoto, T., Ed.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2964, pp. 222–235.

26. Macé, F.; Standaert, F.; Quisquater, J. Information Theoretic Evaluation of Side-Channel Resistant Logic Styles. In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2007, 9th International Workshop, Vienna, Austria, 10–13 September 2007; Lecture Notes in Computer Science; Paillier, P., Verbauwhede, I., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4727, pp. 427–442.
27. Becker, G.; Cooper, J.; DeMulder, E.; Goodwill, G.; Jaffe, J.; Kenworthy, G.; Kouzminov, T.; Leiserson, A.; Marson, M.; Rohatgi, P.; et al. Test Vector Leakage Assessment (TVLA) Methodology in Practice. In Proceedings of the International Cryptographic Module Conference 2013, Gaithersburg, MD, USA, 24–26 September 2013.
28. Durvaux, F.; Standaert, F. From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces. In Proceedings of the Advances in Cryptology—EUROCRYPT 2016—35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, 8–12 May 2016; Proceedings, Part I; Lecture Notes in Computer Science; Fischlin, M., Coron, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9665, pp. 240–262.
29. Fant, K.M.; Brandt, S.A. NULL Convention Logic/sup TM/: A Complete And Consistent Logic For Asynchronous Digital Circuit Synthesis. In Proceedings of the 1996 International Conference on Application-Specific Systems, Architectures, and Processors (ASAP '96), Chicago, IL , USA, 19–23 August 1996; IEEE Computer Society: Washington, DC, USA, 1996; pp. 261–273.
30. Bogdanov, A.; Knudsen, L.R.; Leander, G.; Paar, C.; Poschmann, A.; Robshaw, M.J.B.; Seurin, Y.; Vikkelsoe, C. PRESENT: An Ultra-Lightweight Block Cipher. In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2007, 9th International Workshop, Vienna, Austria, 10–13 September 2007; Lecture Notes in Computer Science; Paillier, P., Verbauwhede, I., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4727, pp. 450–466.
31. Bellizia, D.; Cellucci, D.; Stefano, V.D.; Scotti, G.; Trifiletti, A. Novel measurements setup for attacks exploiting static power using DC pico-ammeter. In Proceedings of the 2017 European Conference on Circuit Theory and Design, ECCTD 2017, Catania, Italy, 4–6 September 2017; pp. 1–4.

Short Biography of Authors

Davide Bellizia was born on 20 June 1989. He received the M.S. degree (summa cum laude) and 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 main research interests include the design and evaluation of circuits for hardware security, with particular attention to development of countermeasures against side-channel attacks, PUFs and RNGs.

Riccardo Della Sala was born on 23 April 1996. In 2020 he received the M.S. degree (summa cum laude) in Electronics Engineering from the University of Rome “La Sapienza” (Italy). His main research interests include the design and development of analog and digital PUFs for hardware security. Furthermore, in the context of analog design, his research activity is focused on ultra-low voltage ultra-low power topology for IOT and biomedical applications.

Giuseppe Scotti received the M.S. and Ph.D. degrees in electronic engineering from the University of Rome “La Sapienza”, 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. 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 cryptographic hardware his focus has been on novel PAAs methodologies and countermeasures. He has coauthored more than 60 publications in international Journals, about 70 contributions in conference proceedings and is the co-inventor of 2 international patents.