Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations

Massimo Alioto, Simone Bongiovanni, Milena Djukanovic, Giuseppe Scotti, and Alessandro Trifiletti

***Abstract*—This paper extends the analysis of the effectiveness of Leakage Power Analysis (LPA) attacks to cryptographic VLSI circuits on which circuit level countermeasures against Differential Power Analysis (DPA) are adopted. Security metrics used for assessing the DPA-resistance of crypto core implementations, such as the minimum number to disclosure (MTD) and the asymptotic correlation coefficient, have been extended to the case of LPA. The LPA-resistance has been evaluated in terms of MTD as a function of the on chip noise. Noise variances up to 10000 times greater than the signal variance have been taken into account and LPA attacks have been successfully executed for all the logic styles under analysis using less than 100000 measurements. Moreover the role of process variations has been investigated through extensive Monte Carlo simulations in order to evaluate their impact on the leakage model for the logic styles under analysis. Results show that LPA attacks can be successfully carried out on the different anti-DPA logic styles even in presence of process variations. To the best of our knowledge, this work proves for the first time the effectiveness of LPA attacks in a real scenario where on chip noise and process variations are taken into account.**

***Index Terms*—Cryptography, differential power analysis, leakage power analysis, security, side-channel attack, smart card, VLSI.**

I. Introduction

MICROPROCESSOR-BASED Smart Cards are frequently used in the consumer market as cryptographic devices to provide secure authentication and storage of secret data. Evidently, security issues play a central role in Smart Cards and add design constraints at all levels of abstraction. In recent years, a large amount of attention has been given to a whole class of attacks developed to extract the secret key through the analysis of the information leaked by the hardware implementation of cryptographic cores. This class of attacks are often referred to as Side-Channel Analysis (SCA's) [1], [2] [3].

In this context Differential Power Analysis (DPA) attacks [4] have been widely demonstrated to be a very powerful technique for stealing information from a cryptographic circuit and hence a major threat to the security of an embedded system. DPA exploits the dependence of dynamic power consumption on the processed data (including the secret key) that is observed in CMOS logic circuits, and can be counteracted through a number of countermeasures at various levels of abstraction.

At the transistor level, which is the main focus of this work, countermeasures are based on the adoption of logic styles whose power consumption is constant or independent of the processed data, which is typically obtained through differential signaling and pre-charged logic.

Wave Dynamic Differential Logic (WDDL) is an example of a state-of-the-art DPA-resistant logic style that can be implemented with a standard CMOS cell library [5], [6] . Randomizing the dynamic power consumption is also a suitable technique for masking the actual dependence between power and processed data. It consists of pre-processing input data in order to obtain masked signals which are a function of original data and a random internally-generated mask. Attacker can only correlate masked data and power consumption but he/she cannot extract information about original data. Masked Dual-rail Precharge Logic (MDPL) is an example of masked CMOS standard-cell based DPA-resistant logic style [7].

On the other hand, more resistant logic styles are built by adopting a custom cell library, as in the case of Sense Amplifier Based Logic (SABL) [8], which requires a perfectly balanced capacitive load at the two nodes of each differential pair, which is not trivial to obtain during synthesis, placement and routing. As an even more secure logic style that relaxes the constraint of perfect load balance, the Three-phase Dual-rail Pre-charge Logic (TDPL) has also been proposed [9]. Finally as an improvement of TDPL, Delay-based Dual-rail Pre-charge Logic Style has been presented [10]. It introduces a new data encoding concept which allows enhancing the benefits of TDPL with less constraints.

In literature the above mentioned transistor level countermeasures are also referred to as Dual-rail Pre-charge Logic (DPL) styles. DPLs were specifically implemented with the aim of de-correlating the dependence of the dynamic power consumption on the logic data transitions by balancing the energy for each clock cycles and data input.

In sub-100 nm technologies, leakage power is well known to be comparable to the dynamic power, and is expected to become an even larger portion of the chip power budget in the future [12]. Hence, the leakage (static) supply current can reveal a significant amount of information on the secret key, due to the strong dependence of leakage on the input of digital blocks [13], [14] . Therefore, power analysis attacks based on leakage are expected to be increasingly effective in downscaled technologies.

Manuscript received January 10, 2013; revised May 27, 2013; accepted June 17, 2013. Date of publication August 23, 2013; date of current version January 24, 2014. This paper was recommended by Associate Editor H.-C. Chang

M. Alioto is with the Department of Electrical and Computer Engineering, National University of Singapore, 117576 Singapore (e-mail: malioto@ieee.org).

S. Bongiovanni, G. Scotti, and A. Trifiletti are with the DIET, Università di Roma "La Sapienza," 00184 Roma, Italy (e-mail: bongiovanni@die.uniroma1.it; scotti@die.uniroma1.it; trifiletti@die.uniroma1.it).

M. Djukanovic is with the Faculty of Electrical Engineering, University of Montenegro, 81000 Podgorica, Montenegro (e-mail: djukanovicmilena@yahoo.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2013.2278350

1549-8328 © 2013 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

These attacks have been proposed very recently in the literature, and will be referred to as Leakage Power Analysis (LPA). As opposed to DPA attacks ([16] and [17]), these recently proposed attacks are not well understood yet, and deserve further investigation to understand their effectiveness in realistic conditions, i.e., in the presence of process variations and countermeasures to DPA attacks (which have to be adopted in applications requiring a high level of security). Until now, only some basic concepts on LPA attacks have been introduced in [18]–[21], where the leakage dependence on the input data was discussed and simulated, and attacks of simple circuits were presented. Only very recently, a well-defined procedure to perform LPA attacks was introduced in [21]. There was shown that leakage power measurements can be even simpler to carry out than dynamic power measurements. Impact of process parameter variations on LPA attacks effectiveness has been recently analyzed in [22] and [23] referring to standard CMOS logic style, and some preliminary work has been done in [24].

This work presents a complete analysis of the success rate of LPA attacks for a crypto core implemented in the state of the art anti-DPA logic styles taking into account on chip noise and process variations. The LPA resistance of the above mentioned anti-DPA logic styles is evaluated and compared to the leakage model which has been adopted. In Section II the fundamentals of LPA attacks and the leakage model are briefly reviewed. In Section III a preliminary analysis of leakage power has been presented for combinatorial gates implemented in the different anti-DPA logic styles. In Section IV a deeper investigation of the leakage model for a cryptographic non-bit slice structure is performed and related to the leakage model, and LPA attacks are performed on real crypto-core implementations in presence of on-chip noise. The effect of process variations on LPA attacks is discussed in Section V. Finally, conclusions are drawn in Section VI.

II. Review of LPA Attacks

The weakness of static CMOS logic style for what concern static power analysis attacks is well known in literature, and has been deeply analyzed [13], [14] .

In a practical power measurement scenario, LPA attacks aim to recover the secret key k of a cryptographic device where the processed data X under attack is a function (or a portion) of k through the analysis of the leakage consumption. Recently, these attacks were rigorously defined along with a clear five-step procedure [21], which is briefly recalled in the following.

In the first step of LPA attacks, the adversary chooses an internal m-bit signal X that is physically generated within the cryptographic circuit under attack. In the second step, the adversary applies 2^m different input values I_i (with $i = 1 \dots 2^m$), and measures the corresponding leakage current $I_{leak,i}$ of the cryptographic chip at the point of time in which X is physically evaluated. In the third step, the physical value of X within the chip is estimated for each input I_i and for each possible guess k_j of the secret key (with $j = 1 \dots 2^m$), thereby generating a 2D array of possible results $X_{ij} = f(I_i, k_j)$ (where X_{ij} is the value of X for the i-th input and j-th key guess). In the fourth step, the leakage current of the block generating X is estimated by the Hamming weight $H(X)$ of X, and the adversary generates a 2D array $H_{ij} = H(X_{ij})$ (where H_{ij} is the estimated leakage for the i-th input and j-th key guess and represents the selection function of the attack). In the fifth step, the measured leakage $I_{leak,i}$ and the estimated leakage H_{ij} are compared through the evaluation of their Pearson correlation coefficient $\rho(I_{leak,i}, H_{ij})$. The correct guess of k is that leading to the highest value of $\rho(I_{leak,i}, H_{ij})$ among all possible guesses k_j.

This procedure has been analytically described for bit-sliced circuits (i.e., circuits with m -bit inputs that are made up of m identical replicas of the same building block), such as arithmetic logic units, registers, register files and bus drivers [21]. For this kind of circuits, the relation between the Hamming weight $w = H(X_i)$ and $I_{leak,i}$ is expressed by (1):

$$\begin{aligned} I_{\mathrm{leak,TOT}} &= w \cdot I_H + (m - w) \cdot I_L \\ &= w \cdot (I_H - I_L) + m \cdot I_L \end{aligned} \tag{1}$$

where $\mathrm{I_H}$ and $\mathrm{I_L}$ are the leakage current for a high level and a low level in the corresponding input bit, respectively. According to (1), leakage $\mathrm{I_{leak,TOT}}$ exhibits a linear dependence on the Hamming weight w, rather than the specific value of each input bit. Note that Pearson correlation coefficient measures the linear dependence between two variables, so it can be used as statistical distinguisher for exploiting the linear relationship (1) between static current $\mathrm{I_{leak,i}}$ and data X, making LPA attacks effective.

As pointed out in [21], one of the most challenging aspect is carefully performing the leakage measurements when performing LPA. When the input is applied to a logic gate, its leakage current is well known to have a transient variation and finally settles to the steady-state value after a period ranging from less than 1 ns to a few tens of nanoseconds according to the technology node. In [21] many measurements of the settling time for different standard logic gates are presented. In such cases authors conclude that the settling times are generally comparable or greater than the period required to observe the steady-state leakage for deep submicron technologies. As a consequence, usually, the adversary is not required to stop the clock for performing leakage analysis. These results cannot be extended immediately to the case of DPLs where the settling times are influenced by the initial conditions at each internal node. Anyway, it is worth noting that the exact clock period in which a selection function inside the chip is evaluated can be easily found if the adversary has sufficient knowledge of the circuit implementation of the algorithm. Even in cases where the adversary does not exactly know this clock cycle but knows that it is among a limited number of clock cycles, he/she can reiterate the above described procedure for each period and then evaluate the maximum correlation coefficients for each of the periods under analysis. Since the static current of the crypto core is strongly correlated with the input state of the registers the adversary can increase the effectiveness of the LPA attack by stopping the clock after an appropriate number of clock cycles so that the correlation between the static current and the key is maximized, as it will be shown in Section IV-B.

III. Leakage Current in Combinatorial Gates

Transistor level countermeasures led to the design of new ad hoc logic styles based on hiding (i.e., making constant) the dynamic power consumption for each data transition within a clock cycle [5], [8] , or on masking it by randomizing the values

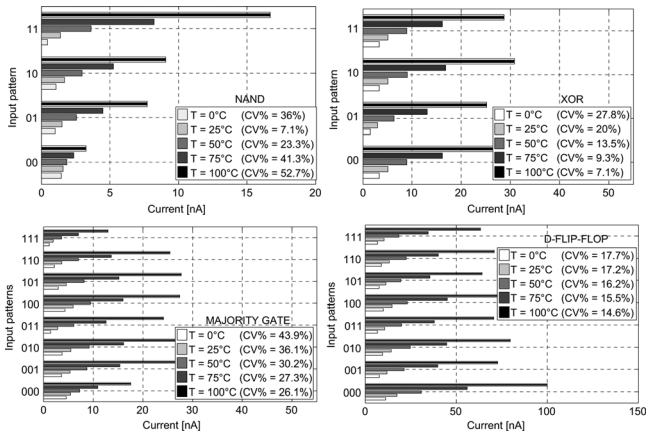


Fig. 1. Leakage current distribution for CMOS gates.

of the power samples through a pre-processing operation on internal signals [7], [15] . In this work some of the most popular DPA-resistant logic styles will be used as case studies for LPA.

Following the theoretical background on leakage power analysis attacks [21] and taking into consideration the first state-of-the-art experimental results [13], [14] , in this section a leakage analysis is conducted in the most used combinatorial gates as case studies for some anti-DPA style. We use the coefficient of variation (CV) [26] as metric to evaluate the dependence of the leakage on the input patterns. It is calculated as the ratio between the standard deviation and the mean of the n measured currents I_j, thus the larger the coefficient the larger the dependency of leakage on the input.

$$CV = \frac{\alpha}{m} = \frac{\sqrt{\frac{1}{n}\sum_{j=1}^{n}(I_j - m)^2}}{\frac{1}{n}\sum_{j=1}^{n} I_j}. \qquad (2)$$

In the remainder of the paper all simulations have been performed in Cadence environment using a CMOS 65-nm cell library from STMicrolectronics. Experiments were performed by adopting High Voltage Threshold General Purpose (HVTGP) BSIM4 model transistors with standard-library sizing factors.

A. Standard CMOS Logic

Each NMOS and PMOS transistor of a CMOS cell exhibits a static power consumption which contributes to the total leakage of the cell itself. This power consumption is due to the currents flowing in a single transistor when it is switched off (i.e., no dynamic transition is applied). However for each data combination there is a different value of the overall leakage current, being the threshold voltages of NMOS and PMOS different between each other. Indeed according to the topology and the number of NMOS and PMOS transistors, correlating each value of the leakage current to a specific input data combination is possible for each logic cell. In Fig. 1 simulation results for NAND, XOR, majority gates and flip-flop are reported for different temperatures. The value of CV confirms a remarkable dependence of the leakage current on the input data.

It has to be noted that for what concerns the input pattern of the flip-flop, the first bit in Fig. 1 is the clock, whereas the second and the third ones are data at the clock cycles i and i-1 respectively. We use this convention also in next subsections, where simulations are repeated for DPLs.

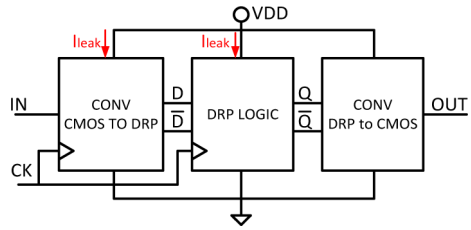


Fig. 2. Simulation testbench for measuring the leakage of DPLs.

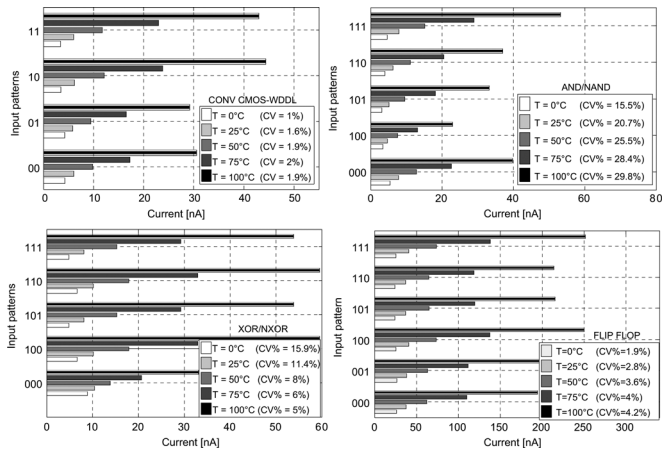


Fig. 3. Leakage current distribution for WDDL gates.

For DPLs we have to define a different testbench, because DPL gates require an input stage for converting static signals from the single-rail to the dynamic dual-rail domain. As shown in Fig. 2, the leakage current has been measured on the VDD pin of the input converters and the internal DRP logic.

B. Standard-Cell Based Dual-Rail Logics

Wave Dynamic Differential Logic (WDDL) is a DPA-resistant dual-rail logic style fully designed through CMOS standard-cells and suitable for building secure cryptographic cores even on FPGAs [5]. Moreover unlike CMOS the range of possible input patterns is limited by the input converters: for instance, during the pre-charge phase (CK=0) dual-rail signals $(D, \overline{D})$ are both forced to be low irrespective of input data. This is an important factor to be accounted for when performing static current measurements.

We expect that WDDL gates exhibit an analogous dependence between leakage and input as seen in CMOS. Simulation results are reported in Fig. 3, and actually confirm our expectation, even though the variation is slightly reduced. Note that during the pre-charge, all signals are always low, and for combinatorial gates only the pattern (0,0) is admitted. As anticipated in the previous subsection this is due to the input converters which force signals to be logic-0.

C. Masked Dual-Rail Pre-Charge Logic

Masking is another countermeasure against DPA attacks and it is based on the randomization of the intermediate value of the cryptographic device by pre-processing input data. Masked Dual-Rail Pre-charge Logic (MDPL) is a DPL style which elaborates masked values as a function of data d and a random mask value m. Similarly to WDDL it is also standard-cell based logic style, which potentially suffers on the input dependence

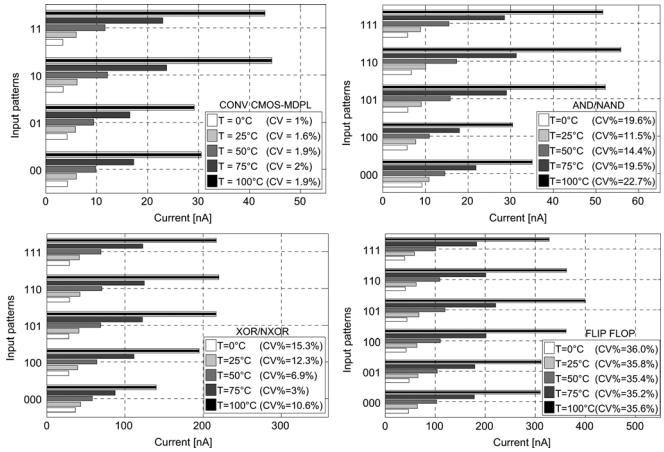


Fig. 4. Leakage current distribution for MDPL gates.

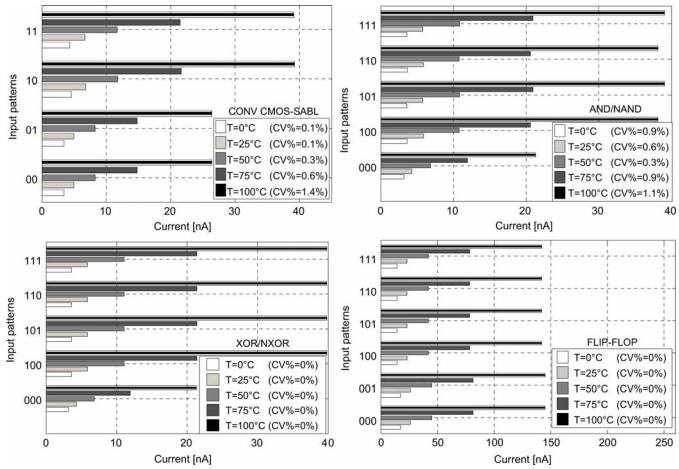


Fig. 5. Leakage current distribution for SABL gates.

of its static consumption. We consider MDPL gates where data are XORed with the mask, being logic XOR the most simple masking function:

$$d_m = f(d, m,) = d \oplus m. \tag{3}$$

Results are shown in Fig. 4, and confirm that also in MDPL the values of CV highlights a certain dependence between original input data and leakage current. It is worth noting that CV is calculated by averaging the values obtained by using m=0 and m=1.

We conclude that even if masking helps to de-correlate power consumption and input patterns, it is not effective for preventing correlation between input and static power because the latter does not depend on the value of the mask m. The MDPL gates are built with majority gates available in the standard library [7], whose leakage is strongly related to the input pattern as shown in Fig. 1.

D. Full Custom Dual-Rail Dynamic Logics

Full custom Dual-Rail Pre-charge (Dynamic) Logics (DPL) are widely used for counteracting DPA on cryptographic devices for ASIC applications. They allow to make the dynamic power consumption of a logic cell constant for each clock cycle, thanks to an optimized dual-rail circuit topology and a dynamic pre-charge/evaluation clocking phase which forces only one logic data transition for each cycle. In a dynamic elaboration the clock period is subset into an evaluation and a pre-charge phase, thanks to the presence of transistors acting like charged capacitances at the different clock semi-periods. The charge and discharge of these capacitances provides the transient response of a dynamic cell at the output nodes [25].

Extending LPA attacks to dynamic logics is not a trivial task. As recalled in the previous section, once an input data is applied to a logic gate, the current adsorbed from the power supply is well known to have a transient variation and finally settles to the steady-state value after a period depending on the technology node. But waiting for the transient to be elapsed means measuring the adsorbed current after the dynamic data encoding has occurred.

The hypothesis that the clock period is comparable or even greater than the period required to observe the steady-state leakage in a nanometer technology [21] may be not more valid for dynamic logic families and must be verified in order to perform a LPA attack. For this reason it must be ensured that the steady-state condition is satisfied so to measure the static power consumption of a dynamic logic.

Sense Amplifier Based Logic (SABL) has been one of the first full custom DPA-resistant logic styles to exploit the above described dynamic and dual-rail behavior [8]. SABL data encoding is based on a spatial domain conception for which data are in a complementary logic state for all the duration of the evaluation period. This information is useful to practically implement an LPA analysis because the static power consumption can be measured before the ending of the evaluation phase, obviously waiting for the steady-state condition to be satisfied, according to the settling time of the devices in a given technology and for different inputs.

Following these considerations, transient simulations on SABL gates have been performed. The clock frequency has been lowered so that after the ending of the evaluation phase all signals settle to the steady-state value as occurs in a real attack scenario. Finally leakage currents have been measured for each possible input data combination. Simulation results are shown in Fig. 5. It is clear that SABL shows a remarkable intrinsic robustness against leakage analysis, being CV of the leakage distribution very low. However a slight dependence between input and leakage can be detected for the AND/NAND gate due to the asymmetry of the cell.

As a second case study we considered the Delay-Based Dual-Rail Pre-Charge Logic (DDPL) family. DDPL is a DPA resistant logic style which is based on a time domain data encoding: each complementary line is charged (evaluation) and discharged (pre-charge) once in a clock cycle, and a datum is encoded according to a fixed delay Δ between the complementary lines.

A DDPL cell requires a special conversion of the dual-rail signals in order to generate the delay Δ at the evaluation edge [10]. Unlike standard-cell-based DPLs, which are built with static gates, and SABL, which can be considered a semi-dynamic logic being the state of the combinatorial gate kept by a sense-amplifier-based evaluation network during a semi-period, in DDPL data encoding is fully dynamic and it is affected by leakage measurements. When simulating a transient analysis by stopping the clock after the evaluation phase, the output of the converter goes to the invalid dynamic value (1,1), being the

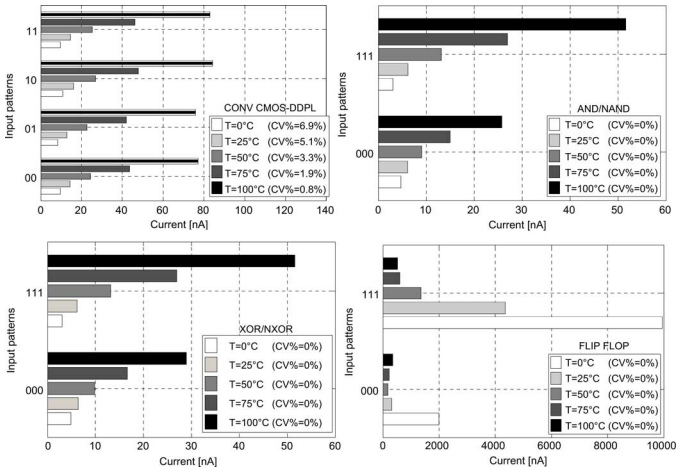


Fig. 6. Leakage current distribution for DDPL gates.

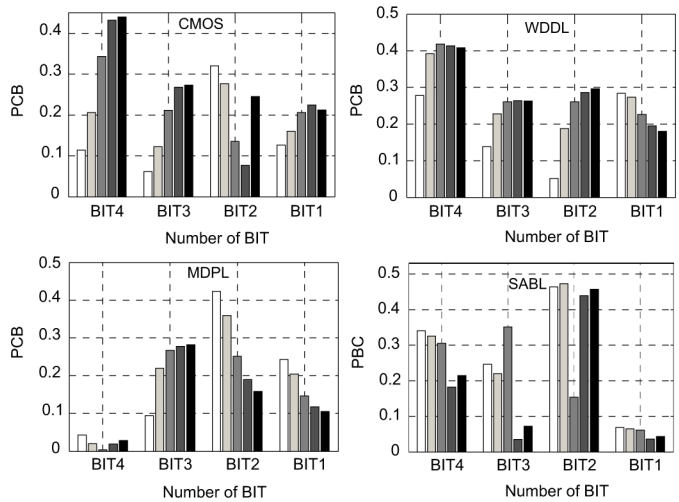


Fig. 7. PBCs between leakage and output bits of DPL S-Boxes.

settling time typically higher than Δ for nanometer technologies [10], [21] , and the following logic gates are always in the same state irrespective of the inputs.

In a real DDPL test chip the delay Δ (typically lower than 1ns) is chosen *a-priori* in order to have a certain level of security and it is not dependent on the clock frequency. Namely lowering the clock frequency in a transient analysis simulation (i.e., stopping the clock signal in a real attack scenario) causes the invalidation of the dynamic data encoding which results to be de-correlated from the input and the key.

Simulation results are shown in Fig. 6. A Spice-level analysis of the waveforms confirms that the output of the converters is not a valid DDPL dual-line (i.e., logic value (1,1)) when clock is stopped at logic-1, confirming the above considerations. Thus the only leakage source in DDPL logic is due to the input converters, whose static current directly depend on the input patterns. This will be demonstrated in the next section.

IV. LPA Attacks on a Crypto Core Implementation

A. Investigation of the Leakage Model For Non-Bit-Sliced Logic Circuits

The leakage model presented in [21] and recalled in Section II holds for a bit sliced structure, being the overall static consumption equal to the sum of the leakages of all the bit slices. The linear dependence between the input Hamming weight distribution and the leakage has been shown for some registers implementation in simulation and confirmed by measurements [21].

Results presented in the previous section show that for standard based flip-flops, which are designed using CMOS flip-flops, like WDDL and MDPL, the dependence law still holds. Thus registers are good candidates to be considered a leakage source of the circuit when a LPA attack is mounted on a crypto core implementation.

However there are different parts of a chip that are typically not-bit sliced, such as the non-linear S-Box used in many cryptographic algorithms. These sub-blocks randomly impact the data dependence of the overall leakage current of the chip and this must be taken into account in the LPA model. Simulations were performed on a 4-input Serpent S-Box implemented with a standard CMOS library [29]. The S-Box was designed using a CMOS 65-nm cell library from STMicroelectronics and was synthesized in Cadence environment using an automated design flow.

Equation (1) states that the leakage of a bit sliced structure has a linear dependence on the Hamming weight of its inputs. In order to investigate if the input pattern of a S-Box and its leakage current distribution are somehow correlated, we use the point biserial correlation coefficient (PBC) [28] which estimates the correlation when one variable is dichotomous (i.e., each bit of the output of the S-Box).

$$\mathrm{PBC} = \frac{\mathrm{M_0} - \mathrm{M_1}}{\mathrm{S_n}} \sqrt{\frac{\mathrm{n_0 n_1}}{\mathrm{n^2}}}. \tag{4}$$

The PBC is calculated for each of the four bits at the output of the S-Box. Leakages are subset into two groups according to the value of the selected bit. $\mathrm{M_0}(\mathrm{M_1})$ is the mean value on the leakages when bit is 0 (1), $\mathrm{n_0}(\mathrm{n_1})$ is the number of leakages of the group associated to bit 0 (1), $\mathrm{S_n}$ is the standard deviation of the leakages distribution. PBC estimates the level of correlation between the input and the output of a n-bit logic.

In a bit sliced circuit (i.e., a n-bit register) PBC is expected to be high for each single bit, whereas in a non-bit sliced circuit it does not. The values of PBC for each bit and for different temperatures are shown in Fig. 7 for the DPL S-Boxes.

Simulation results show that each DPL S-Box exhibits a different law of dependence. For instance BIT4 of the MDPL S-Box is poorly correlated to the leakage, similarly as BIT1 of the SABL S-Box, whereas CMOS and WDDL bits are well correlated to the leakage current.

It is not a trivial task to understand the results in Fig. 7 under the perspective of LPA. PBC is mathematically equivalent to the Pearson's correlation coefficient, thus it assesses the linear dependence between leakage and data when one bit is chosen as selection function.

The simulated S-Box implementation was built with DPL combinational gates, thus PBC gives an estimation of the data dependence of the leakage of each sub-circuit which elaborates the selected bit.

However in the context of LPA we are not interested in the correlation between the Hamming weight of the output word of a circuit and its power consumption, but on its impact on the

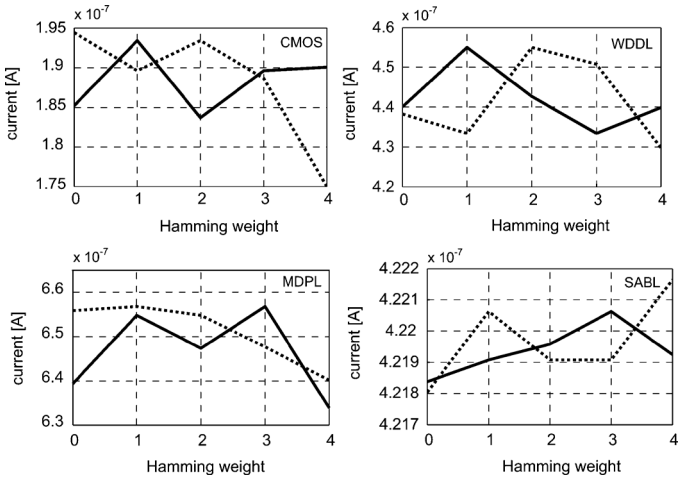


Fig. 8. Leakage current as a function of the Hamming weight of the input (dotted line) and the output (straight line) words of the S-Box.

overall static power consumption with respect to the Hamming weight of a datum inside the chip.

Therefore it makes sense to simulate the leakage of the S-Boxes and depict it as a function of the leakage current, in order to perform a deeper investigation of the leakage model of the S-Box. In Fig. 8 the plots of the leakage currents as a function of the Hamming weight are reported, comparing the input and the output words.

From Fig. 8 it is clear that each S-Box changes the law of data dependence of the leakage in a different way. For instance in the MDPL S-Box the output word is less correlated to the leakage with respect to the input word, according to the low PBC of BIT4, whereas actually in SABL the low PBC of BIT1 enhances the correlation level (see Fig. 7). Namely in a random logic circuit the correlation between a single bit and the overall leakage may impact in a different way the LPA effectiveness, depending on the architecture of the logic circuit. However if PBC is high, it is very likely that the effect of de-correlation by the random block is light.

Unlike CPA which directly assesses and detects the linear dependence between the Hamming weight of the elaborated data and the dynamic power at certain time instants within the clock cycle, the success of LPA depends on the possibility to extract information on the leakage of a sub-circuit by correlating it to its input patterns (e.g., the state of a register of the data path of a crypto core when the clock is stopped).

Therefore we guess that if the combinational logic preceding the bit sliced circuit under attack is random, as it is in a real chip, it exhibits a static consumption which may de-correlate the overall static consumption from the selection function, reducing the effectiveness of LPA. Namely in a LPA attack it is critical to choose a convenient selection function so that the effect of de-correlation between leakage and data due to the combinational logic is low.

B. Exploring the Leakage Dependence for a Case Study Crypto Core Designed With Random Combinational Logics

As the dependence of the correlation coefficient on the variations of all leakage contributions is not easy to grasp in general, we considered a lightweight cryptographic circuit as a case study for performing the LPA attack strategy.

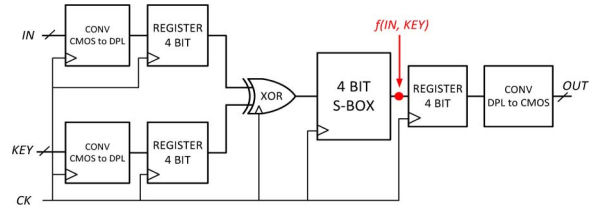


Fig. 9. Data path of the crypto core designed for mounting LPA attacks.

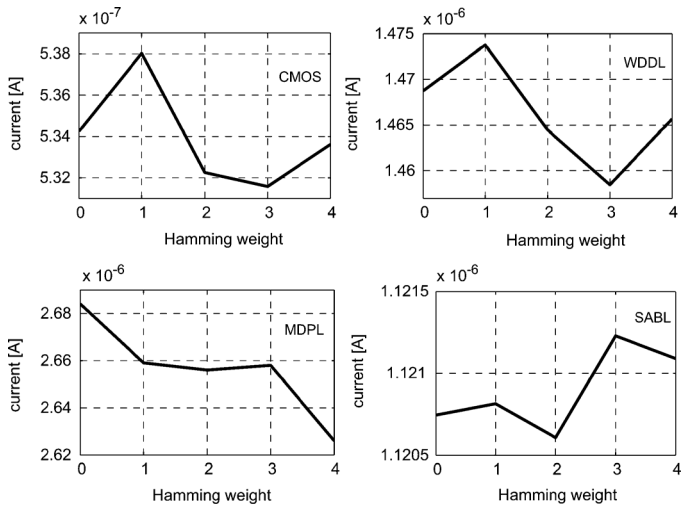


Fig. 10. Leakage current as a function of the selection function w = f(IN, Key).

The core was implemented using the logic gates analyzed in the previous sections. More specifically the previously described S-Box is used as a representative example of a random block that is vulnerable to power analysis attacks. In Fig. 9 the hardware architecture of the crypto core is presented. Basically the core represents a subset of the cryptographic algorithm Serpent [29], in which the 4-bit S-Box S_0 takes as input the XOR between data and key. It was implemented as a 4-bit architecture with two stages of registers, and takes three clock cycles for processing a datum. The secret key of the crypto-core was set to $(5)_2 = (0101)$.

In our simulations the clock signal was stopped after the evaluation edge of the second clock cycle, in order to allow the output registers to set in the steady state, and the Hamming weight HW of the word at the output of the S-Box (i.e., the input of the registers) is chosen as selection function. In Fig. 9 the selection function is indicated as f(IN, Key).

Following the considerations of the previous section, we expect that in this implementation more correlated the leakage of the S-Box to the Hamming weight of the selection function, more feasible the LPA on the overall leakage of the crypto core due to the bit sliced registers. Analogous considerations were made in the past for traditional DPA/CPA attacks on the dynamic power consumption, which were extended to random logic blocks in a very similar way [1]. Interestingly, in this respect LPA and DPA/CPA attacks are similar, as the linear model of power consumption in (1) generally applies.

However a fundamental difference between DPA/CPA and leakage arises, as seen in Fig. 10, where simulation results are presented for the DPL crypto-core under analysis.

In the figures the trend of the static current is presented as a function of the selection function HW(w). It is worth noting that the sub-part of the overall leakage which is correlated to the

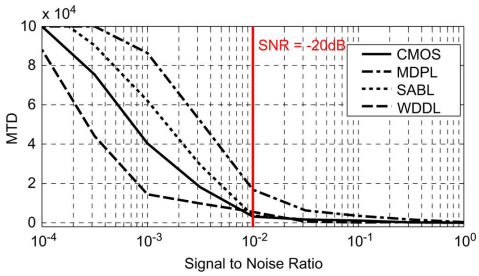


Fig. 11. Minimum number to disclosure as a function of the SNR.

selection function is mainly due to the static consumption of the second stage of registers.

Indeed the S-Box block de-correlates the state of these registers to the state of the first level of registers and introduces a contribution which is randomly correlated to the selection function (as seen in Fig. 8 in the previous section). Thus when the leakage model is applied, we expect that a linear dependence can be still detectable and exploitable mainly due to the leakage of the second stage of registers. All the other contributions represent correlated noise in the LPA model.

Indeed the plots in Fig. 10 confirm that a residual linear correlation still holds, which makes LPA effective also in presence of the S-Box.

C. Performing LPA Attacks With the Linear Model

The LPA attack was performed following the procedure in Section II: for each key hypothesis, the correlation coefficient between the leakage current distribution and the selection function $\mathrm{w} = \mathrm{f}(\mathrm{IN}, \mathrm{KEY})$ was evaluated. Note that the leakage distribution is an one-dimension vector where each element is the steady state current measured on the $\mathrm{V_{DD}}$ pin of the chip for a given plaintext, unlike DPA/CPA where the leakage measurements are a matrix of time samples.

The number of measurements to disclosure (MTD) has been introduced in [30] and used in a lot of works as an actual security metric for quantifying the resistance of a crypto implementation against DPA/CPA in terms of minimum number of plaintexts for discover the key. Thus we also adopt MTD for assessing the effectiveness of LPA.

After having simulated static current traces from Cadence environment at an operating temperature of 50° C, we elaborated the traces by adding a Gaussian noise in order to take into account the on-chip noise [31]. By using this approach the on-chip noise accounts also for all the other logic blocks which are instantiated on the chip and contribute to the overall static current consumption, but their power consumption is not correlated with the key.

The LPA procedure was repeated increasing the noise standard deviation step by step. We used a maximum capacity of the attack equal to 100000 measurements. In Fig. 11 the MTD as a function of the Signal to Noise Ratio (SNR) is depicted.

It must pointed out that under the perspective of a real LPA scenario, leakage measurements are rather insensitive to ac additive noise since they are based on measurements averaged over a sufficiently long period of time, as any other dc measurement [21].

By using 100000 measurements and averaging the noisy traces in order to reduce the noise for each plaintext, the correct key was disclosed up to a SNR almost equal to nearly -40 dB

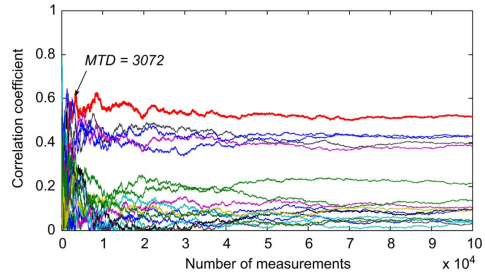


Fig. 12. Correlation coefficients as a function of the number of measurements for CMOS (the curve of the correct key is in red).

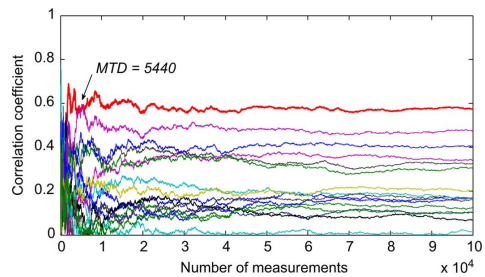


Fig. 13. Correlation coefficients as a function of the number of measurements for WDDL (the curve of the correct key is in red).

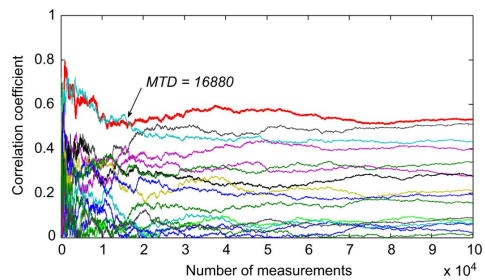


Fig. 14. Correlation coefficients as a function of the number of measurements for MDPL (the curve of the correct key is in red).

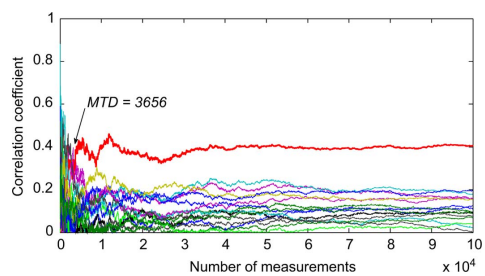


Fig. 15. Correlation coefficients as a function of the number of measurements for SABL (the curve of the correct key is in red).

for all the logic styles under analysis, which corresponds to a maximum noise variance 10000 times greater than the signal variance. This demonstrates that it is possible to detect hardware leakage through a static power analysis even in presence of noise.

As a second set of simulations, we plotted in Figs. 12–15 the correlation coefficient for all the correct key guesses with a fixed level of noise (i.e., $\sigma_N^2 = 100 \cdot \sigma_S^2$, which corresponds to $\mathrm{SNR} = -20$ dB) in order to evaluate the MTD for each crypto implementation.

In Table Iρ_{correct} is the value of the correlation coefficient of the correct key guess for 100000 measurements, which is a good estimation of the correlation when an unbounded attack is mounted (i.e., the value of the correlation coefficients calculated

TABLE I
ACTUAL SECURITY METRICS FOR THE DPL CRYPTO-CORES ($\mathrm{SNR} = -20$ dB).

	CMOS	WDDL	MDPL	SABL	DDPL
MTD	3072	5440	16880	3656	>100000
$\rho_{correct}$	0.529	0.578	0.545	0.391	0.009
$\max[\rho_{wrong}]$	0.431	0.479	0.489	0.201	0.516
$G(N\to\infty)$	1.227	1.207	1.115	1.945	~ 0

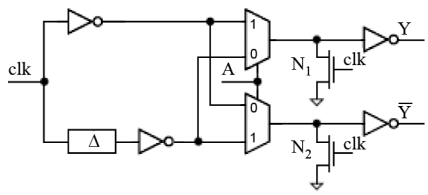


Fig. 16. Circuit for the conversion of a CMOS signal into the DDPL domain.

when the number of traces is high enough to obtain the convergence towards an asymptotical value [32]). Instead $\max[\rho_{\mathrm{wrong}}]$ is the maximum asymptotical value calculated among all the wrong keys. The asymptotical gain G is calculated as the ratio between ρ_{correct} and $\max[\rho_{\mathrm{wrong}}]$ and gives an estimation of the leakage resistance of an implementation.

D. LPA Attack Against DDPL

As anticipated in Section III-D, when the clock is stopped during a leakage measurement the output of the CMOS-DDPL converters at the interface of the DDPL crypto-core, which should convert the signals according to a time difference between the dual-rail pair, are forced to be in an invalid logic state (1,1). In Fig. 16 the circuit architecture of the converter is depicted [10].

When clock is maintained in a certain logic state, the output lines are forced to be always at the same values. For instance, when clock is '0' (pre-charge), the input pair of both multiplexers is (1,1) and the signal output pair is pre-charged to (0,0) irrespective of the single-ended datum A, whereas when clock is '1' (evaluation) the output are always forced to be (1,1). Namely, the output does no more depend on the information to be encoded. According to the hardware architecture in Fig. 9, actually the dynamic data encoding has been deleted at the beginning of the elaboration path, and if we suppose to stop the clock at logic '1' during the evaluation phase, signals (1,1) propagate along the logics at the output of each gates. Thus the overall static leakage is constant for each data input and the leakage model adopted for LPA cannot be effective (i.e., the correlation is zero) as shown in Table I.

The unfeasibility of the LPA attack procedure against the DDPL core requires a further analysis. Consider again the model reviewed in Section II and reported in (5):

$$\mathrm{I}_{\mathrm{leak,TOT}} = \mathrm{w}\cdot \mathrm{I}_{\mathrm{H}} + (\mathrm{m}-\mathrm{w})\cdot \mathrm{I}_{\mathrm{L}}. \tag{5}$$

Suppose that the multiplexers of the input converters, which are the only blocks contributing to the leakage are bit-slice circuits. Their leakage depends on the Hamming weight of the input pattern. The total leakage in the DDPL chip is given by (6):

TABLE II
LEAKAGE CURRENTS MEASURED FOR THE DDPL CRYPTO-CORE AS A FUNCTION OF THE INPUT PATTERN.

IN	HW(IN)	$I_{leak,TOT}$	$I_{leak,CONV}$	I_{const}
0000	0	21.374	0.213	21.161
0001	1	21.372	0.211	21.161
0010	1	21.372	0.211	21.161
0011	2	21.370	0.209	21.161
0100	1	21.372	0.211	21.161
0101	2	21.370	0.209	21.161
0110	2	21.370	0.209	21.161
0111	3	21.369	0.208	21.161
1000	1	21.372	0.211	21.161
1001	2	21.370	0.209	21.161
1010	2	21.370	0.209	21.161
1011	3	21.369	0.208	21.161
1100	2	21.370	0.209	21.161
1101	3	21.369	0.208	21.161
1110	3	21.369	0.208	21.161
1111	4	21.367	0.206	21.161

$$\begin{aligned}\mathrm{I}_{\mathrm{leak,TOT}} &= \mathrm{I}_{\mathrm{leak,CONV}} + \mathrm{I}_{\mathrm{const}}\\ &= \mathrm{w}_{\mathrm{data}}\cdot \mathrm{I}_{\mathrm{H}} + \mathrm{w}_{\mathrm{key}}\cdot \mathrm{I}_{\mathrm{H}} + (\mathrm{m}-\mathrm{w}_{\mathrm{data}})\cdot \mathrm{I}_{L}\\ &\quad + \ (\mathrm{m}-\mathrm{w}_{\mathrm{key}})\cdot \mathrm{I}_{\mathrm{H}} + \mathrm{I}_{\mathrm{const}}\\ &= \mathrm{w}_{\mathrm{key}}\cdot(\mathrm{I}_{\mathrm{H}}-\mathrm{I}_{\mathrm{L}}) + \mathrm{w}_{\mathrm{data}}\cdot(\mathrm{I}_{\mathrm{H}}-\mathrm{I}_{\mathrm{L}})\\ &\quad + 2\mathrm{m}\cdot \mathrm{I}_{\mathrm{L}} + \ \mathrm{I}_{\mathrm{const}}\\ &= \mathrm{w}_{\mathrm{key}}\cdot(\mathrm{I}_{\mathrm{H}}-\mathrm{I}_{\mathrm{L}}) + \mathrm{w}_{\mathrm{data}}\cdot(\mathrm{I}_{\mathrm{H}}-\mathrm{I}_{\mathrm{L}}) + \mathrm{I}'_{\mathrm{const}}.\end{aligned} \tag{6}$$

$\mathrm{I}_{\mathtt{leak,CONV}}$ is the fraction of the total leakage which depends on the Hamming weight of both input data and key words passing through the converters, whereas $\mathrm{I}_{\mathtt{const}}$ is a constant fraction which depends on the internal DDPL gates which are always stimulated by the not valid signal pair (1, 1).

Equation (6) shows that the overall leakage linearly still depends on the Hamming weights of data, with a coefficient of variation of the leakage in the order of 4–5% for the possible input patterns (see Fig. 6). However the current $\mathrm{I}_{\mathtt{leak,CONV}}$, as reported in Table II in the next page, is around 210nA by considering the sum of the leakages of the eight input converters.

This is only a low fraction of the overall static power consumption of the chip (less than 1%). Moreover, the leakage of the four converters of the 4-data input word is fully uncorrelated to the leakage of the four converters of the 4-bit keys, as seen in (6), and it depends only on the Hamming weight $\mathrm{w}_{\mathrm{data}}$ of the input words. Namely it is very hard to exploit the leakage model, being the leakage source only a very low fraction of the overall static consumption ($\mathrm{CV} = 0.008\%$).

The absence of an actual selection function inside the chip which relates leakage and key for each input plaintext makes actually impossible to distinguish which part of the leakage depends solely on the key.

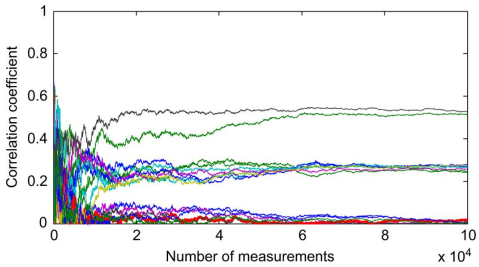


Fig. 17. Correlation coefficients as a function of the number of measurements for DDPL (the curve of the correct key is in red).

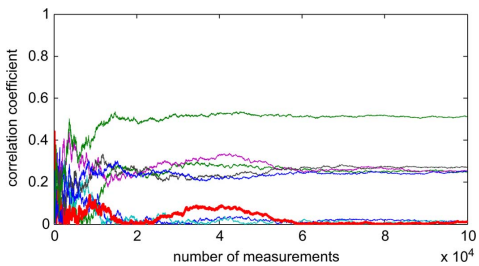


Fig. 18. Correlation coefficients as a function of the number of measurements for DDPL using the output of the XOR as selection function (the curve of the correct key is in red).

Moreover it is possible to design LPA-resistant multiplexers in the CMOS-DDPL converters so that also the leakage current $\mathrm{I}_{\mathtt{leak,CONV}}$ can be definitively de-correlated from the key.

On the basis of these considerations, we mounted LPA attack against the DDPL implementation similarly as the other DPLs. In Fig. 17 the results of the attacks are shown.

LPA was still performed with an on-chip noise with a variance $\sigma_N^2 = 100 \cdot \sigma_S^2$, and at a temperature equal to $50°\mathrm{C}$. The plot of the correlation coefficients in Fig. 17 confirms that LPA attack is not effective in the DDPL test chip, leading to high correlation coefficients for the wrong key guesses, whereas the correlation coefficient of the correct one is almost zero, revealing that no correlation exists between key and the measured overall static consumption in our implementation.

The LPA attack was also mounted by choosing the output of the XOR logic, which is a bit-slice block, as a different selection function. Nevertheless (see Fig. 18) LPA is still unsuccessful and leads to the wrong key guess $(0)_2$.

In the DPLs the pre-charge and the evaluation phases alternate within the clock semi-periods, thus when the clock signal is stopped DPL behaves similarly to the static logic. Instead in DDPL no correlation exists between input data, hardwired key and static power, because the information is encoded during the dynamic time interval Δ and it is lost when the steady state is reached. Therefore by using this measurement setup for evaluating the leakage static consumption of the test chips, the role of the input converters is fundamental: it is enough to balance the energy consumption of the multiplexers in order to break the residual correlation between key and static power.

V. Evaluation of the LPA Effectiveness With Power Variability Issues

A. Intra-Die and Inter-Die Process Variations in the Actual Security Metrics Adopted in LPA

In general, VLSI circuits are subject to both inter-die and intra-die process variations [27]. *Inter-die* comprise not only process variations affecting all the chips on one single wafer, but also the variations on different wafers, and even on different lots. Actually, these comprise all possible variations between the standard process corners. Accordingly inter-die variations are expected to have the same effect on the value of the overall consumption of the chip, and in particular the leakage $\mathrm{I}_{\mathrm{leak}}$ due to the bit slices sub-circuits is shifted according to the same (random) factor. Therefore the correlation coefficient between $\mathrm{I}_{\mathrm{leak}}$ and the Hamming weight of the input data that determines the outcome of the LPA attack is not affected by inter-die variations.

On the other hand *intra-die* variations represent the mismatch of devices which are located close to each other (i.e., adjacent), and which should match as closely as possible. This kind of variations affects all devices within a chip in a different manner. For this reason intra-die process variations are expected to have an impact on the outcome of LPA attacks, as they differently affect the leakage $I(H)(I_L)$ for different bit slices (see (1)), thereby impacting the resulting correlation coefficient both in the case of bit sliced and random logic blocks [21]. As a consequence, logic gates exhibit a different leakage consumption in presence of intra-die variations even when the same inputs are applied. Because in this case the leakage depends on the specific value of the input (not only on its Hamming weight), a slight deviation from the linear trend in (1) is also expected.

The effect of the intra-die process variations can be modeled as a Gaussian variable which causes an uncertainty on the value of the correlation coefficients calculated in the previous section.

Namely the asymptotic value of the correlation coefficients for each key guess is also a Gaussian variable with mean ρ and a standard deviation depending on the process variations. Thus the extension of the uncertainty ranges and so their overlapping (or not) depends on the range of random variability of the technology process which should be investigated at a given technology node. Even if intra-die process variations might cause a LPA attack strategy to be ineffective, the attack is still feasible if the value ρ under the correct key guess can be distinguished from that under a wrong guess. Thus it must be ensured that the uncertainty ranges of the corresponding correlation coefficients do not overlap. If a sample circuit exhibits a correlation coefficient for the correct key guess less than the correlation coefficient for one wrong key guess, the LPA fails.

It has been demonstrated [21] that by simulating a circuit instantiation under small to moderate process variations in a CMOS 65-nm technology node, the key guesses with input Hamming distances (to correct key) higher than one cannot cause an overlapping correlation coefficient distribution. So a LPA attack can identify the correct key in the most cases, or find at most a one-wrong-bit key with an high probability. Namely the standard deviation due to the process spread is higher than the uncertainty of a LPA attack in distinguishing a one wrong bit to the correct one, but lower than the uncertainty of a LPA attack in distinguishing a two wrong bit to the guess one. Thus LPA attacks under intra-die variations are expected to be successful in current and future technology generations and in the next sections we will demonstrate these preliminary results by simulating LPA attack on the case study crypto-core.

Observe that such overlap might lead to an attack failure or not, i.e., such overlap does not convey information on the LPA effectiveness. Indeed, the presence of a correlation coefficient

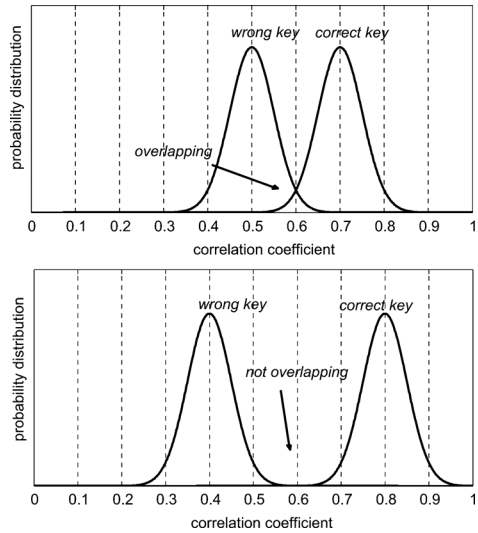


Fig. 19. Statistical distribution of the correlation coefficient under high intra-die variations (success rate ¡1) (upper) and moderate intra-die variations (success rate = 1) (lower).

ρ for the wrong key $(4)_2$ that is higher than the correct key $(5)_2$ for different realizations does not indicate any attack failure (an attack fails only if ρ for key $(4)_2$ is higher than $(5)_2$ in the same realization). In other words, the statistical distribution of the correlation coefficient for different keys is not sufficient to deduce the effectiveness of a LPA attack.

According to the above considerations, the impact of variations on the effectiveness of LPA can be understood only by evaluating the percentage of realizations such that the correct key is actually associated with the highest correlation coefficient, and assessing the LPA resistance in terms of mean and standard deviation of the actual security metrics as MTD.

B. Impact of Intra-Die Variation on the Leakage Model

Before performing LPA attacks on the crypto core, it makes sense to investigate how the leakage model of the chip is affected by the intra-die variations. For this purpose we performed the attack on 100 samples of the circuit, each one generated by means of Monte Carlo simulations.

The 100 sample circuits generated in each experiment were all affected by mismatch variations. Note that each of 100 Monte Carlo iterations represents a realization of the circuit under test with a particular configuration of process random variables. The operating temperature is equal to $50°$ C. BSIM4 models with statistical parameters provided by the foundry were used [33], which were previously validated on silicon over a large number of commercial integrated circuits.

The distribution have been subset in five groups, according to the value of the selection function (i.e., the Hamming weight $\mathrm{w} = \mathrm{f}(\mathrm{IN}, \mathrm{Key})$).

In Figs. 20–23 the leakage current trend versus the Hamming weight is plotted, both for mean and standard deviation. As expected the linear trend is still visible for the mean leakage, and fits well the trend in nominal case plotted in Fig. 10. Moreover the coefficient of variation has been calculated for each Hamming weight of the DPLs and shown in Table III. It stays within the range of $1 \div 3$, confirming that moderate process variations have a rather limited impact on the LPA model.

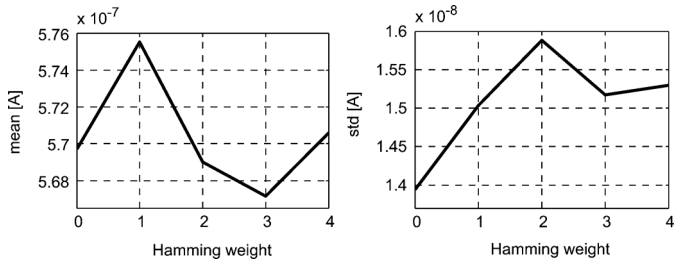


Fig. 20. Mean and standard deviation of the leakage current distribution versus input Hamming weight over 100 CMOS sample circuits.

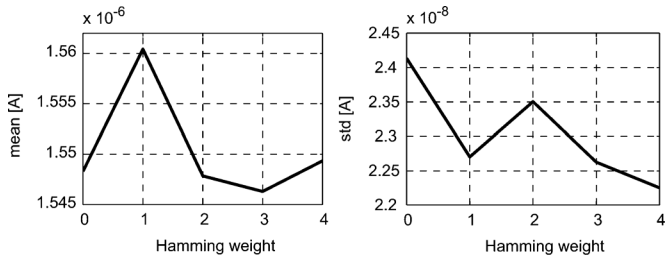


Fig. 21. Mean and standard deviation of the leakage current distribution versus input Hamming weight over 100 WDDL sample circuits.

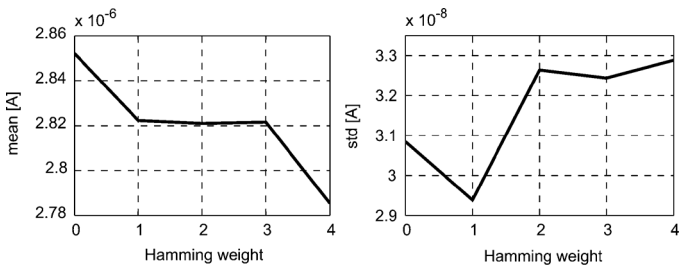


Fig. 22. Mean and standard deviation of the leakage current distribution versus input Hamming weight over 100 MDPL sample circuits.

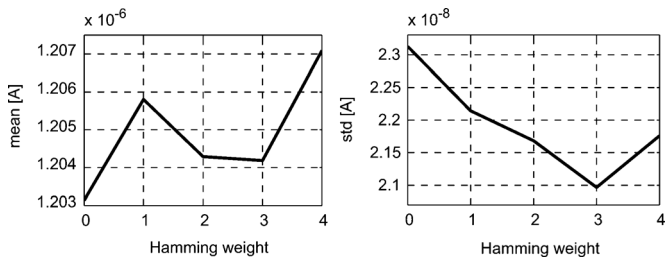


Fig. 23. Mean and standard deviation of the leakage current distribution versus input Hamming weight over 100 SABL sample circuits.

For instance, for MDPL the CV% is lower than the others, so we expect that LPA in presence of process variations could be more effective with respect to CMOS and SABL. Instead for the latter the mismatches have a stronger effect in terms of variance on the linear model.

C. Performing LPA Attacks on the Crypto-Core in Presence of Noise and Process Variations

Under the perspective of a real LPA attack, the intra-die variability of a chip must be quantified by using a deterministic metric.

As suggested in [31], the resistance of a crypto core against power analysis can be assessed in the worst case by profiling and attacking the same chip. Each sample circuit exhibits a different leakage depending on the impact of process mismatches

TABLE III
COEFFICIENT OF VARIATION (%) FOR THE STATIC CURRENTS DISTRIBUTION MEASURED FOR THE 100 CRYPTO CORE SAMPLE CIRCUITS DESIGNED WITH DPLS.

HW	0	1	2	3	4	μ
CMOS	2.447	2.612	2.791	2.675	2.681	**2.641**
WDDL	1.559	1.455	1.519	1.463	1.436	**1.486**
MDPL	1.082	1.041	1.157	1.150	1.180	**1.122**
SABL	1.922	1.836	1.801	1.741	1.803	**1.821**

on the LPA model, according to the mean and the standard variation described in the previous section. Thus we evaluated the impact of intra-die process variations by mounting LPA against all the sample circuits and calculating the MTD and the asymptotic correlation coefficient for the correct key guess for each realization. We use the success rate as a metric to evaluate the effectiveness of LPA on the sample circuits, defined in this scenario as the number of sample circuits which were successfully atacked with a $\mathrm{MTD} \leq \mathrm{N}$:

$$\begin{aligned} \mathrm{SR_i} &= \Pr\{\mathrm{Exp}=1\} = \Pr(\rho_{\mathrm{corr}} > \rho_{\mathrm{wrong}}) \\ &= \begin{cases} 0, \mathrm{MTD} > N \\ 1, \mathrm{MTD} \leq \mathrm{N} \end{cases} \\ \mathrm{SR}\ \% &= \sum_{\mathrm{i}=1}^{100} \mathrm{SR_i}. \end{aligned} \tag{7}$$

After having simulated static current traces from Cadence environment at an operating temperature equal to 50° C, simulated traces were post-processed by adding a Gaussian noise in order to consider also the on chip noise as done in the nominal case. We considered again $\sigma_N = 100 \cdot \sigma_S$, which leads to a $\mathrm{SNR} = -20$ dB.

LPA attacks were mounted with a maximum number of traces equal to 100000. As seen in Section IV, by considering this noise variance the correlation coefficient of the key guesses for a LPA with 100000 traces is considered a good approximation of the asymptotical correlation.

The overall effect of intra-die variation can be modeled as a statistical variation in the security metrics used in previous section for assessing the effectiveness of LPA attacks. For instance, if we consider the MTD, which is defined as the minimum number of measurements for which the curve of the correlation coefficient ρ of the correct key guess crosses over the curve of the maximum correlation coefficient of the wrong keys and asymptotically maintains a value higher than the others key guesses [30], it can be seen as a Gaussian variable centered on its nominal value and with a range of uncertainty around it (see Fig. 19). Thus it must be assured that the distribution of MTD does not overstep the boundary due to the maximum number of measurements for not increasing the complexity of the attack.

The MTD was calculated for all the sample circuits which were successfully attacked by LPA. In Figs. 24–27 the distribution of the MTD is depicted for all the logic styles.

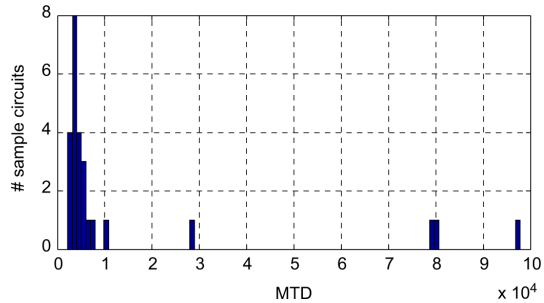


Fig. 24. Distribution of the MTD for the successful LPA attacks against the CMOS sample circuits.

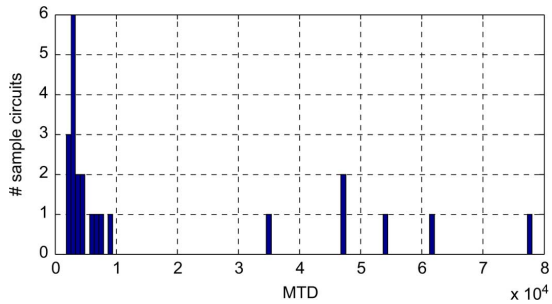


Fig. 25. Distribution of the MTD for the successful LPA attacks against the WDDL sample circuits.

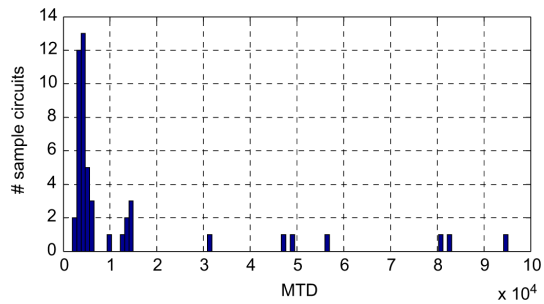


Fig. 26. Distribution of the MTD for the successful LPA attacks against the MDPL sample circuits.

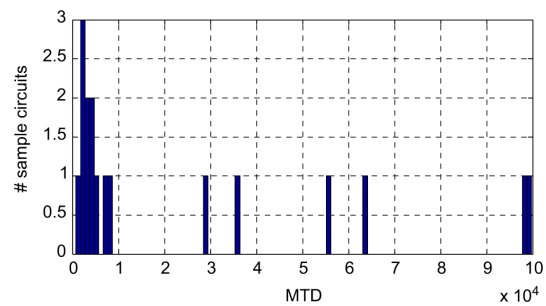


Fig. 27. Distribution of the MTD for the successful LPA attacks against the SABL sample circuits.

As anticipated, MTD exhibits a Gaussian distribution around a mean value which is very similar to the value calculated in the nominal case (around 3000–4000 measurements). However, the MDPL crypto core exhibits a lower standard deviation which confirms the low impact of process variations in the leakage model for this DPL logic style. Instead SABL exhibits a higher variance which highlights a bigger impact of process variations on the leakage model, mainly due to the symmetry of the cells which aims at balancing the dynamic power consumption.

TABLE IV
ACTUAL SECURITY METRICS FOR THE DPL CRYPTO-CORES SUCCESSFULLY ATTACKED WITH A LPA PROCEDURE ($\mathrm{SNR} = -20$ dB).

	CMOS	WDDL	MDPL	SABL
SR%	26 (51)	23 (38)	49 (70)	17 (32)
max[MTD]	97792	78048	95200	99728
mean[MTD]	14770	17075	13876	24978
mean[$\rho_{correct}$]	0.522	0.529	0.584	0.495
mean[G]	1.299	1.296	1.255	1.276

Results of LPA attacks against the crypto cores are reported in Table IV in the next page.

For the success rate, the number of successfully attacked circuits when the one-bit wrong key is also considered and reported between brackets.

The values of the mean asymptotical correlation coefficient for the correct key guess and the mean correlation gain agree to the nominal values reported in Table I.

Results confirm that LPA is still effective against the most popular cryptographic logic styles adopted for balancing dynamic consumption and designed with nanoscale devices, even when physical variability due to the on-chip noise and the process mismatches are taken into account. Inevitably process variations impact the effectiveness of LPA depending on the specific architecture of each logic style, but the leakage model is still exploitable for all the logics under analysis.

VI. CONCLUSION

In this paper, LPA attacks to the logic gates used in cryptographic circuits have been deeply investigated with the aim of better understanding their effectiveness in practical cases where physical variability due to the presence of on-chip noise and process mismatches are observed, and countermeasures to DPA are employed. Analysis has shown that the Hamming weight of a selected data word inside the chip can be adopted as leakage power model even in the real case of crypto-core designed with a mix of bit sliced and not-bit sliced circuits (e.g., S-Boxes). An investigation of the variation of the hypothesized leakage model for LPA has been extensively performed for some DPLs crypto-core implementations, where random logic blocks are always present.

Results of LPA attacks demonstrate that, even if transistor level countermeasures developed for thwarting DPA on a cryptographic circuit have been implemented for balancing the overall dynamic consumption, an attacker is enabled to exploit the fraction of the overall consumption due to the static power, which keeps on exhibiting a dependence on the data input. When a maximum capacity of the attack of 100000 measurements is adopted, LPA was effective for all the DPLs under analysis in the case of on-chip noise variance up to 10000 times greater than the signal variance, which corresponds to a SNR equal to -40 dB.

We used actual security metrics introduced for DPA/CPA for assessing the LPA resistance of each implementation, such as the minimum number of measurements for disclosure (MTD). The MTD for LPA attacks is very low for the DPLs under analysis: when a SNR equal to -20 dB is considered, for CMOS, WDDL and SABL MTD is within $3000 \div 6000$ traces, whereas for MDPL it is higher but within the attack capacity (~17000). The only logic style which reveals a strong resistance against LPA resulted to be DDPL.

Moreover Monte Carlo simulations have been performed in order to take into account the impact of process variations in a real scenario. Results showed that actually intra-die variations have an influence on the outcome of LPA attacks. For standard cells based DPLs, process mismatches do not reduce the effectiveness of LPA, leading to a success rate equal to 1 for an intolerably high percentage of sample circuits (i.e., $23 \div 50\%$) when a SNR equal to -20 dB has been considered. Furthermore if we consider the one-bit wrong key guess in a second order attack strategy, the percentage increases up to 70%. Instead for a full custom logic as SABL, the static power consumption is more sensitive to process variations with respect to the nominal case, mainly due to the symmetry of the logic gates; in this case the success rate is slightly lower (i.e., 17%), demonstrating that also anti-DPA full custom logic styles are potentially vulnerable to LPA attacks.

More in general, the design of transistor and gate level countermeasures for power analysis must take into account also the need of breaking correlation between the static power, and the input data. To the best of our knowledge, no specific countermeasures against LPA have been presented in the literature. This work proves that, even if the anti-DPA countermeasures prevent power analysis on the differential power consumption, many logic styles which are considered as "secure" against DPA can be violated using LPA, in some cases also exploiting process mismatches. This means that the body of work focused on countermeasures to DPA attacks does not solve the security issues arising with power analysis attacks and research efforts must address toward anti-LPA countermeasures.

The aim of this study is also to promote the design of novel countermeasures which are secured both against DPA/CPA and LPA. Hence, in the future a significant research effort will be required to devise appropriate solutions and countermeasures against LPA that keeps the security level to the current standards, provided that different leakage models can also been investigated by eventually exploiting a non-linear dependence between input data and static power, and other statistical distinguishers can be adopted, such as mutual information analysis [34] and template attacks [35].

REFERENCES

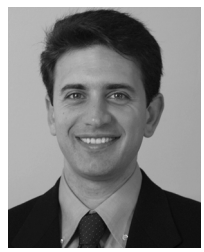
[1] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, 2002.

[2] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York, NY, USA: Springer-Verlag, 2007.

[3] K. Tiri and I. Verbauwhede, "Simulation models for side-channel information leaks," in *Proc. 42nd Design Automation Conference (DAC)*, 2005, pp. 228–233.

[4] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Proc. CRYPTO'99*, pp. 388–397, 1999.

[5] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Design, Automation Test Eur. Conf. Expo. (DATE '04)*, 2004, pp. 246–251.
[6] K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.*, vol. 25, no. 7, pp. 1197–1208, 2006.
[7] T. Popp and S. Mangard, "Masked Dual-Rail Pre-charge logic: DPA resistance without routing constraints ," in *Proc. CHES'05*, Scotland, UK, Sep. 2005, vol. 3659, pp. 172–186.
[8] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. ESSCIRC 02*, 2002, pp. 403–406.
[9] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Pre-Charge logic," in *Proc. Cryptographic Hardware and Embedded Syst.—CHES 2006, 8th Int. Workshop, Lecture Notes in Computer Sci. Springer*, Yokohama, Japan, Oct. 10–13, 2006.
[10] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay-Based Dual-Rail precharge logic," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 7, pp. 1147–1153, 2011.
[11] L. Lin and W. P. Burleson, "Analysis and mitigation of process variation impacts on Power-Attack Tolerance," in *Proc. Design Automation Conf. (DAC)*, 2009, pp. 238–243.
[12] Int. Tech. Roadmap for Semiconductors. (2008) [Online]. Available: http://public,itrs.net
[13] A. Abdollahi, F. Fallah, and M. Pedram, "Leakage current reduction in CMOS VLSI circuits by input vector control," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 12, no. 2, pp. 140–154, 2004.
[14] L. Lin and W. Burleson, "Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2008, pp. 252–255.
[15] H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, and W. Zhang, "Masking the energy behavior of des encryption," in *Proc. IEEE Design, Automation Test Europe Conf. Exhibition—DATE*, 2003, pp. 84–89.
[16] M. Alioto, M. Poli, and S. Rocchi, "A general power model of differential power analysis attacks to static logic circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 5, pp. 711–724, May 2010.
[17] M. Alioto, M. Poli, and S. Rocchi, "Differential power analysis attacks to precharged busses: a General analysis for symmetric-key cryptographic algorithms," *IEEE Trans. Dependable Secure Comput.*, vol. 7, no. 3, pp. 226–239, Sep. 2010.
[18] J. Giorgetti, G. Scotti, A. Simonetti, and A. Trifiletti, "Analysis of data dependence of leakage current in CMOS cryptographic hardware," in *Proc. Great Lake Symp. VLSI (GSLVLSI 2007)*, Stresa, Italy, Mar. 11, 2007, p. 78.
[19] L. Giancane, M. Jovanovich, G. Scotti, and A. Trifiletti, "Leakage power analysis of cryptographic devices implemented in nanometer CMOS technologies," in *Proc. Konferencija 9-a 07: Konferencija za Elektroniku, Telekomunikacije, Racunarstvo, Automatiku i Nuklearnu Tehniku, Herceg Novi (Montenegro)*, Jun. 2007, pp. 355–367.
[20] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: Well-defined procedure and first experimental results," in *Proc. Int. Conf. Microelectron. (ICM)*, 2009, pp. 46–49.
[21] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A Novel class of attacks to nanometer cryptographic circuits," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 2, pp. 355–367, Feb. 2010.
[22] M. Djukanovic, L. Giancane, G. Scotti, and A. Trifiletti, "Impact of process variations on LPA attacks effectiveness," in *Proc. Int. Conf. Computer Elect. Eng. (ICCEE09)*, 2009, pp. 102–106.
[23] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: Theoretical analysis and impact of variations," in *Proc. 16th IEEE Int. Conf. Electronics, Circuits, Syst. (ICECS)*, 2009, pp. 85–88.
[24] M. Djukanovic, L. Giancane, G. Scotti, A. Trifiletti, and M. Alioto, "Leakage power analysis attacks: Effectiveness on DPA resistant logic styles under process variations," in *Proc. ISCAS 2011*, Rio de Janeiro, Brazil, May 2011, pp. 2043–2046.
[25] J. M. Rabaey, A. Chandrakasan, and B. Nikolic, *Digital Integrated Circuits—A design perspective*2 ed. Englewood Cliffs NJ, USA, Prentice Hall, Jan. 3, 2003.
[26] W. A. Hendricks and K. W. Robey, "The sampling distribution of the coefficien of variation," *Ann. Math. Stat.*, vol. 7, no. 3, pp. 129–132, 1936.
[27] S. R. Nassif, "Modeling and forecasting of manufacturing variations," *Proc. ASP-DAC*, pp. 145–150, 2001.
[28] U. Olsson, F. Drasgow, and N. J. Dorans, "The polyserial correlation coefficient," *Psychometrika*, vol. 47, no. 3, pp. 337–347, 1982.
[29] R. Anderson, E. Biham, and L. Knudsen, "Serpent: A proposal for the advanced encryption standard," *Nat. Inst. Standards Technol.*, 1998.
[30] K. Tiri, D. Hwang, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "Prototype IC with WDDL and differential Routing—DPA resistance assessment," in *Proc. CHES '05, ser. LNCS Springer*, Edinburgh, U.K., Sep. 2005, vol. 3659, pp. 354–365.
[31] M. Renauld, F.-X. Standaert, N. Veyrat-Charvillon, D. Kamel, and D. Flandre, "A formal study of power variability issues and side-channel attacks for nanoscale devices," in *Proc. EUROCRYPT 2011 LNCS 6632 Springer*, Tallinn, Estonia, May 15–19, 2011, pp. 129–138.
[32] F. X. Standaert, T. G. Malkin, and M. Yung, "A unified framework for the analysis of Side-Channel key recovery attacks," in *Proc. EUROCRYPT 2009 LNCS 5479 Springer 2009*, Cologne, Germany, Apr. 26–30, 2009, pp. 443–461.
[33] [Online]. Available: http://www-device.eecs.berkeley.edu/bsim3/bsim4.html
[34] B. Gierlichs, L. Batina, P. Tuyls, and Preneel, "Mutual information Analysis—a generic Side-Channel distinguisher," in *Proc. CHES '08 LNCS*, Washinghton, DC, USA, Aug. 2008, vol. 5154, pp. 426–442.
[35] S. Chari, J. R. Rao, and P. Rohatagi, "Template attacks, proc. of ches '02 lncs," in *Proc. CHES '02 LNCS*, San Francisco, CA, USA, Aug. 2002, vol. 2523, pp. 13–28.



Massimo Alioto (M'01–SM'07) was born in Brescia, Italy, in 1972. He received the Laurea (M.Sc.) degree in electronics engineering and the Ph.D. degree in electrical engineering from the University of Catania, Catania, Italy, in 1997 and 2001, respectively.

He is currently an Associate Professor at the Department of Electrical and Computer Engineering, National University of Singapore. Previously, he was Associate Professor at the Department of Information Engineering of the University of Siena (2002–2013). In the summer of 2007, he was a Visiting Professor at EPFL—Lausanne (Switzerland). In 2009–2011, he held a Visiting Professor position at BWRC—UCBerkeley, investigating on next-generation ultra-low power circuits and wireless nodes. In 2011–2012, he was Visiting Professor at University of Michigan, investigating on active techniques for resiliency in near-threshold processors, error-aware VLSI design for wide energy scalability, self-powered circuits. In 2013 he was Visiting Scientist at Intel Labs—CRL (Oregon) to work on ultra-scalable microarchitectures. He has authored or co-authored about 180 publications on journals (60+, mostly IEEE TRANSACTIONS) and conference proceedings. Two of them are among the most downloaded TVLSI papers in 2007 (respectively 10th and 13th). He is co-author of two books: *Flip-Flop Design in Nanometer CMOS—from High Speed to Low Energy* (Springer, 2013) and *Model and Design of Bipolar and MOS Current-Mode Logic: CML, ECL and SCL Digital Circuits* (Springer, 2005). His primary research interests include ultra-low power VLSI circuits, self-powered and wireless nodes, near-threshold circuits for green computing, error-aware and widely energy-scalable VLSI circuits, circuit techniques for emerging technologies.

Prof. Alioto was a member of the HiPEAC Network of Excellence (EU) and the MuSyC FCRP Center (US). In 2010–2012 he was the Chair of the "VLSI Systems and Applications" Technical Committee of the IEEE Circuits and Systems Society, for which he was also Distinguished Lecturer in 2009–2010 and member of the DLP Coordinating Committee in 2011–2012. He currently serves as Associate Editor in Chief of the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, and served as Guest Editor of various journal special issues (including the issue on "Ultra-Low Voltage Circuits and Systems for Green Computing" published in December 2012 on IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS). He also serves or has served as Associate Editor of a number of journals (ACM *Transactions on Design Automation of Electronic Systems*, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, *Microelectronics Journal, Integration—The VLSI journal, Journal of Circuits, Systems, and Computers, Journal of Low Power Electronics, Journal of Low Power Electronics and Applications*). He was Technical Program Chair of the ICECS 2013, NEWCAS 2012 and ICM 2010 conferences, and Track Chair in a number of conferences (ICCD, ISCAS, ICECS, VLSI-SoC, APCCAS, ICM).

Simone Bongiovanni was born on June 4th 1983. He received the B.S. degree in electronic engineering and the M.A. degree (*summa cum laude*) in electronic systems for telecommunications from Università di Roma "La Sapienza," Rome, Italy, in 2007 and 2010, respectively.

In 2011 he was with the R&D division of General Impianti—Loccioni Group where he worked in the statistical analysis based on multivariate techniques applied on electronically acquired signals. He is currently attending a Ph.D. course at the Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni of the university "La Sapienza". His research interests include the design of cryptographic ICs for counteracting power analysis attacks, and more in general the digital VLSI design.

Milena Djukanovic was born in Podgorica, Montenegro, in 1983. She graduated from the the Faculty of Electrical Engineering, University of Montenegro, in 2006. During her studies she received scholarships from Ministry of Science and Municipality of Podgorica, Montenegro, as being one of the best students in her generation. She received the M.Sc. and the Ph.D. degree sin electronics engineering from the University of Montenegro in 2007 and 2012, respectively.

She is working as a Teaching Assistant at the Faculty of Electrical Engineering, Podgorica, University of Montenegro, from 2007. She received scholarships, funded by European Commission for master and doctoral studies, to spend a year at the University of Rome 'La Sapienza', carrying out research activities in the field of crypto processor analysis and design. She has also received a staff scholarship funded by European Commission to spend one month at the University of Bologna, where she gave lessons and presentations about her research work. She is engaged as a Research Assistant at two Scientific Projects supported by Ministry of Science of Montenegro. She was a member of Tempus team Project 'Development of Regional Interdisciplinary Mechatronic Studies—DRIMS', just as FP7 team Project 'Promote, mobilize, reinforce and integrate wireless sensor networking research and researchers: Towards pervasive networking of WBC and the EU—PROSENSE', both supported by European Commission. She is a leader of a research group from University of Montenegro for COST project (2012–2016). She has authored or co-authored about 20 publications on international journals and conference proceedings. Also, she is first author of one university book *Introduction to Mechatronics*, (2013), and co-author of one scientific monograph (2013).

Dr. Djukanovic serves as part of Editorial Board for two International Journals*: International Journal of Engineering & Technical Research, International Journal of Modern Communication Technologies & Research*. She also serves as Reviewer of a number of journals (ACM T*ransactions on Design Automation of Electronic Systems,* IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION SYSTEMS, *Elsevier Integration—The VLSI Journal, World Scientific Journal of Circuits, Systems, and Computers, IJENS International Journals of Engineering and Sciences*).

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.

He is currently Assistant Professor in the scientific field "Elettronica" (ING-INF/01) in the Department DIET at the same University. From 2003 to 2010 he was Professor of Digital Electronics at "La Sapienza" University, and since 2006 he teaches a course in Theory of Electronic Circuits at "La Sapienza" University. From 2004 to 2006 he participated in the European project SCARD (Side Channel Attacks Resistant Design), and from 2007 to 2009 he was involved in the European Integrated Project SHAPES (Scalable Software Hardware Application Platform for Embedded Systems). 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 (radio frequency and microwave applications) and digital VLSI circuits. In the context of analog design his research activity was concerned with circuit topologies for the realization of analog functions using low-voltage ultra-short channel CMOS technology and with the development of current mode building blocks. He has been also involved in research/design activities held in collaboration between "La Sapienza" University and some industrial partners which led, between 2000 and 2012, to the implementation of 12 ASICs. He has coauthored more than 100 publications in international journals and conferences and is the co-inventor of 2 international patents.

Dr. Scotti conducts peer reviews for IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, and TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS), Wiley and Elsevier journals.

Alessandro Trifiletti was born in Rome, Italy, in 1959. He received the Laurea degree in electronic engineering from the Università di Roma "La Sapienza," Rome, Italy.

In 1991, he joined the Dipartimento di Ingegneria Elettronica, Università di Roma "La Sapienza," as a Research Assistant where he is currently an Associate Professor. His research interests include high speed circuit design techniques and III-V device modeling.