On-chip Current-Mode Approach to Thwart CPA Attacks in CMOS Nanometer Technology

Davide Bellizia, Giuseppe Scotti, and Alessandro Trifiletti

***Abstract*—The protection of information that reside in smart devices like IoT nodes is becoming one of the main concern in modern design. The possibility to mount a non-invasive attack with no expensive equipment, such as a Power Analysis Attack (PAA), remarks the needs of countermeasures that aims to thwart attacks exploiting power consumption. In addition to that, designers have to deal with demanding requirements, since those smart devices require stringent area and energy constraints. In this work, a novel analog-level approach to counteract PAA is presented, taking benefits of the current-mode approach. The kernel of this approach is that the information leakage exploited in a PAA is leaked through current absorption of a cryptographic device. Thanks to an on-chip measuring of the current absorbed by the cryptographic logic, it is possible to generate an error signal. Throughout a current-mode feedback mechanism, the data-dependent component of the overall consumption can be compensated, making the energy requirement constant at any cycle and thwarting the possibility to recover sensible information. Two possible implementations of the proposed approach are presented in this work and their effectiveness has been evaluated using a 40nm CMOS design library. The proposed approach is able to increase the Measurements to Disclosure (MTD) of at least three orders of magnitude, comparing to the unprotected implementation. It has to be pointed out that the on-chip current-mode suppressor, based on the proposed approach, is able to provide a very good security performance, while requiring a very small overhead in terms of silicon area (x1.007) and power consumption (x1.07).**

***Index Terms*—IoT, Power Analysis Attacks, smart card, CPA, current-mode, Side Channel Analysis, CMOS, Cryptography, PRESENT.**

I. Introduction

THE protection of sensible data is one of the main concerns in most recent applications. Several secured devices (e.g smartphones, smart-card, etc.) are frequently used to exchange private informations, such as ID and bank account credentials. Given the benefit of the newest technology, in addition to the "More Than Moore" approach to the design of electronic devices, the Internet of Things (IoT) paradigm had an incredible growth, since its first appearance during the 1998. IoT allows to interconnect several "smart devices" or "nodes", in order to collect real-world data and thanks to network connectivity. Typically, this intelligent networks are based on the identification of smart devices, and the exchanged data are actually private and sensible (such as in medical and healthcare applications). It is clear that data stream has to be protected, in order to avoid the possibility to be hijacked or sniffed [1][3].

A Side-channel Attack (SCA) is a class of procedures that have the aim to recover sensible information, such as the secret key, from cryptographic devices, by exploiting the information that is leaked by the implementation itself, while the algorithm is executed [1]. The feasibility of a SCA, demonstrated in 1999 by Kocher *et al.*, represents a critical issue for secure application, due to its simplicity. In fact, not expensive equipment is required to perform a successful attack, which outlines the needs of countermeasures. Many physical emissions can be used as leakage source, such as electromagnetic emission [5], execution time [1] and power consumption [6]. Power Analysis Attacks (PAAs) are the most used methodologies in SCA, and it exploits the power consumption of cryptographic devices as side-channel [6]. Thanks to PAA, it is possible to relate the power consumption of a CMOS logic to the processed data. Then by means of statistical distinguishers, the input of a digital gate can be recovered by monitoring its power consumption. Well known procedures to perform a PA are Differential Power Analysis (DPA) [6] and Correlation Power Analysis (CPA) [7]. They make use of the data-dependent component of dynamic consumption of a cryptographic device to exploit sensible information. With the help of a proper leakage model and a statistical distinguisher, the secret key can be recovered. The possibility to use the static power consumption of cryptographic circuits as an additional side channel has been analyzed in [8], [9] and [10].

In literature, several countermeasures have been proposed at each level of abstraction to counteract attacks to dynamic power consumption. System-level techniques have the purpose of preventing the physical observation of the power consumption, and aim to de-correlate the consumption from the processed data. At gate-level, many countermeasure can be implemented by using both standard cell and full custom design. Widely used gate level countermeasures use Dual-Rail Pre-charged Logic (DPL) styles, such as Wave Dynamic Differential Logic (WDDL) [11], Sense Amplifier Based Logic (SABL) [12] and Masked DPL (MDPL) [13]. They aim to balance the difference in dynamic power consumption between 0→1 and 1→0 output

D. Bellizia, G. Scotti and A. Trifiletti are with DIET, Università degli Studi di Roma "La Sapienza", Rome, Italy (e-mails: {bellizia, scotti, trifiletti}@diet.uniroma1.it)

ISSN 2080-8755

transition, providing both transitions at each clock cycle, by using differential signaling. Differential signaling requires special attention to get the capacitive load on each wire of an interconnection matched, because the balancing in power consumption depends on the pairwise balancing of the capacitive parasitics of complementary wires. To overcome this challenge, Delay-based Differential Pre-charge Logic (DDPL) has been proposed in [14]. DDPL uses a different data encoding; it is based on TEL (Time Enclosed Logic) encoding [15], which relies on the data encoding in the time domain instead on the differential logic level domain.

Analog, circuit level approaches can be used to develop countermeasures able to prevent information leakage through the observation of the dynamic power consumption of a cryptographic implementation. As well as many full custom DPL styles, on-chip analog countermeasures cannot be directly implemented on FPGA platform, because of the presence of non-digital (standard-cell) sub-blocks. In [16], the authors have proposed an on-chip *current equalizer* based on switched capacitor circuits. Thanks to the use of controlled decoupling stages, the cryptographic engine is not directly powered by the main V_{DD} pad. A precise sequence of charge-supply-discharge of the switching capacitor array is used to provide energy to the secure core, in order to hide the real consumption to the malicious attacker. Based on similar concepts, in [17], a three layers decoupling circuit provides energy to the target implementation, to flatten the power consumption, and uses CMOS switches and CMOS capacitors. Each gate of the cryptographic device is protected by the proposed decoupling cells. In [18], a different approach is used. Using a *feedback loop* approach, a dynamic current correction scheme suppresses differences in dynamic power consumption related to different processed data. Instantaneous current drawn by the cryptographic engine is sensed using a *voltage mode approach*, and then, the proper current is shunted from the main power supply, in order to maintain the total current constant. Hence, the observable power consumption is approximately flat and unrelated to processed data.

In this paper, we propose a novel analog-level approach to counteract CPA attacks exploiting dynamic power consumption. The novel approach is based on a *current-mode* suppression scheme. The proposed approach is intended to be a compact and power-aware solution, in order to make it suitable for ultraconstrained IoT devices. The paper is organized as follows. *Section II* briefly presents the background of the DPA and CPA. *Section III* outlines the proposed scheme, as building block for secure applications. *Section IV* discusses the application of the proposed circuit for the protection of the single gates or of cryptographic sub-blocks. *Section V* highlights the results of simulated attacks on the unprotected and protected implementation of PRESENT-80 algorithm. In *Section VI*, an improved version of the building block presented in *Section III* is presented, providing an efficient countermeasure with a smaller area and power overhead. In *Section VII*, a simulated attack on a 40nm CMOS implementation of the entire PRESENT-80 block cipher protected by the improved current-mode suppressor circuit.

II. Background of CPA/DPA Attack

The aim of PA is to recover the secret key of a device by monitoring and analyzing its power consumption during the execution of the cryptographic algorithm. Each PA attack procedure requires the use of a specific power model of the device, as a prediction of the real power consumption, by targeting a certain operation of the algorithm. Then, a comparison between actual consumption and power model is executed by using the proper statistical distinguisher.

The dynamic power consumption of a CMOS circuit, which can be used as side-channel, can be expressed by the sum of two main components [19]:

$$P_{dyn} = P_{sw} + P_{sc} \tag{1}$$

where P_{sw} is the switching power and P_{sc} is the short-circuit power. They have the following expressions:

$$P_{sw} = V_{DD}^2 \cdot C_L \cdot f \cdot \alpha_t \tag{2}$$

$$P_{sc} = V_{DD} \cdot I_{peak} \cdot t_{sc} \cdot f \cdot \alpha_t \tag{3}$$

In a simple gate as the CMOS inverter, we can see 1→0 and 0→1 output transitions have two different power consumptions. During 1→0 transition, the C_L is discharged internally and only short-circuit power is consumed. In 0→1 transition the total power consumption is larger because not only short-power is consumed, but also C_L must be charged, and it requires current from the power supply. This simple consideration is typical of CMOS gates, and the attacker can use this difference to recover sensible information.

In DPA attacks [6] the attacker chooses a single bit of a word processed by the device. Then the attacker divides the collected set into two sets according to the value of the chosen bit. In this case, the power model is the simple bit value. The guess on the correct key is obtained by using the *difference of means test* as statistical distinguisher. Highest is the difference of means for a certain key hypothesis at sample *j*, highest is the correlation between the power model and the actual measurements. If we consider the binary matrix *H*, with *n* rows and *K* columns, as the power model matrix related to the target bit for each key hypothesis, and *T* the power measurements set for *n* plaintexts, each composed by *N* samples, we compute the *difference of means* for key hypothesis k_i as:

$$R_{DPA,i}[j] = \frac{\sum_{l=1}^{n} h_{l,i} \cdot t_l[j]}{\sum_{l=1}^{n} h_{l,i}} - \frac{\sum_{l=1}^{n} (1 - h_{l,i}) \cdot t_l[j]}{\sum_{l=1}^{n} (1 - h_{l,i})} \tag{4}$$

with j=1,2,…N and i=1,2,…K. Equation (4) can be written as:

$$R_{DPA,i}[j] = M_{1,i}[j] - M_{0,i}[j] \tag{5}$$

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

$$k^* = argmax_i\{|R_{DPA,i}|\} \tag{6}$$

In CPA attacks [7] the attacker chooses a word processed by the device, and not a single bit like in DPA attacks. For each key hypothesis, the hypothetical word value is computed and a matrix V of size $n \times K$, where n is the number of queries and K is the cardinality of the sub-key space, is created. Usually, for the hypothetic power consumption model, the *Hamming Weight* (HW) or the *Hamming Distance* (HD) are very common to model the power consumption in CMOS logics. In bit-slice or memory-based architectures, these simple models can fit very well the real consumption. HW/HD models make a strong assumption on the power consumption of a multi-bit structure: the power consumption related to every bit contributes to total power consumption equally. The matrix V is used to compute the hypothetical power consumption matrix H, which has the same size of V, following the chosen power model.

$$H = f(V) \tag{7}$$

The matrix H is then compared with the power traces set T, by using the *Pearson's correlation coefficient* as statistical distinguisher:

$$R_{CPA,i}[j] = \frac{\sum_{l=1}^{n}\left(h_{l,i} - \bar{h}_i\right) \cdot \left(t_l[j] - \overline{t[j]}\right)}{\sqrt{\sum_{i=1}^{N}\left(h_{l,i} - \bar{h}_i\right)^2 \cdot \sum_{i=1}^{N}\left(t_l[j] - \overline{t[j]}\right)^2}} \tag{8}$$

The matrix R_{CPA} has size $K \times N$. The key hypothesis k^* which maximizes the correlation coefficient is chosen as guessed key.

$$k^* = argmax_i\{|R_{CPA,i}|\} \tag{9}$$

III. On-chip Current Equalizer

In literature, several *voltage mode* analog countermeasures have been proposed [18], [20]. To the best of our knowledge, the proposed design is the first analog countermeasure based on a *current mode approach*. The current mode approach is widely used in many electronic applications, such as AD/DA converters, analog filters, etc., due to its compactness and speed.

The idea behind our approach is to set the same current drawn at each clock edge, in order to reduce the variability due to different input patterns.

As we have said before, during the active edge of the clock, standard CMOS gates in a data-path perform output transitions and a certain current is drawn from the supply line. During the active clock edge, the current equalizer senses the current drawn by the logic and compares it with a reference current. If for the specific input pattern the current drawn is less than the reference current, the current equalizer circuits shunts an extra current from the supply line, in order to hide to the attacker the real consumption of the logic below. At each clock cycle, the same current is drawn and the power consumption is ideally constant. A block scheme that is able to implement our approach is shown in Fig. 1.

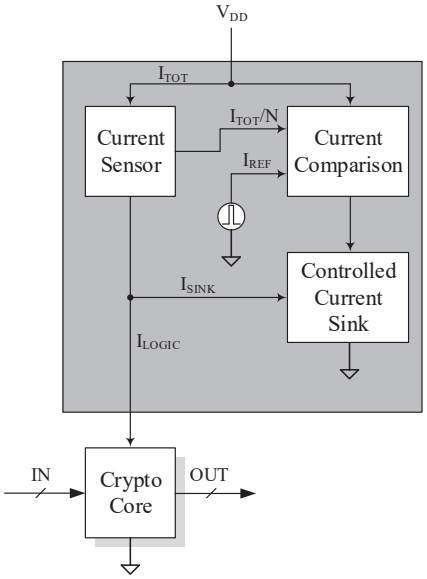

Fig. 1. Block scheme of the current equalizer.

A linearized and simplified model of the current equalizer is shown in Fig. 2. We can express the relationship between I_{TOT} (total current) and I_{REF} (reference current) as function of I_{LOGIC} (current drawn by the logic):

$$I_{TOT} = I_{REF}\frac{R_0 G_M}{1 + R_0 G_M} + I_{LOGIC}\frac{1}{1 + R_0 G_M} \tag{10}$$

$$I_{TOT} = I_{SINK} + I_{LOGIC}\frac{1}{1 + R_0 G_M} \tag{11}$$

If the loop gain $R_0 G_M \gg 1$, the output of the current equalizer is expressed by:

$$I_{TOT}(t) = I_{LOGIC}(t) + I_{SINK}(t) = I_{REF} \tag{12}$$

where I_{LOGIC} is the data-dependent component and provides energy to the logic, and I_{SINK} is the current that is drawn by the equalizer to reach I_{REF}, which is constant. As we can see in Fig. 1-2, the current equalizer is a feedback loop. The input of the feedback loop is the current I_{REF} and the output is I_{TOT}, while I_{SINK} is the correction. The *Current Comparison* block compares I_{TOT} with the reference current I_{REF}, and produces a voltage signal, driving the *Controlled Current Sink*, which acts as a transconductance G_M and equalize the total current drawn by the system. The current I_{LOGIC} can be considered as a disturbance for I_{TOT}, and it has to be rejected. Since the reference current I_{REF} is constant, the I_{SINK} current has to dynamically correct the variability of I_{LOGIC} due to data-dependency.

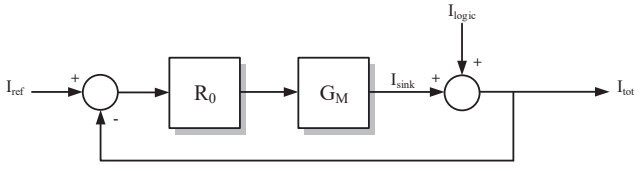

Fig. 2. Simplified and linearized model of the current equalizer.

In Fig. 3, a circuit implementation of the current equalizer is shown. As we can see, M_1-M_7 senses the current I_{TOT}, and implement a current mirror with M_2. M_3-M_4 permits to invert the sign of the current and scales down its magnitude, in order to reduce the power consumption overhead. The reduction ratio of the sensed current can be set by properly designing the aspect ratio of the current mirror M_3-M_4. Transistor M_5 is the reference generator. The control voltage V_{sync} activates M_5 during the edge of the clock. During this short interval, M_5 is in saturation region and I_{REF} is drawn from V_{DD}. At the drain node of M_5, the difference between the drain current of M_5 and M_4 produces a voltage swing on the total equivalent resistance R_0 at the node. This voltage swing drives M_6, to shunt the I_{sink} required to nullify the error current of the loop.

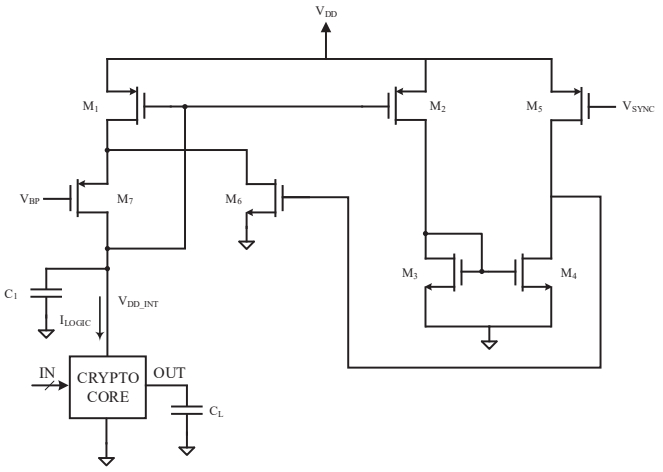

Fig. 3. Circuit implementation of the proposed current equalizer.

In order to provide enough power supply to the logic, it is necessary to use a cascode configuration of the input of the current mirror $M_{1,2,7}$. Thanks to the presence of M_7, a low voltage drop is reached between V_{DD} and V_{DD_int}, due to the low impedance provided by the cascode current mirror.

V_{sync} signal has to be generated from the clock signal. To reduce power consumption overhead, the correction on the current drawn by the logic is performed only around the active edge of the clock. In Fig. 4, V_{sync} signal generator circuit is shown. A D flip-flop is used to get a clock signal at half of the frequency of the global clock. The delay element is obtained with a starved inverter [21]. The delay Δ can be set with the control voltage of the starved inverter, and allows to designers to choose the width of the pulse of V_{sync}. Using V_{sync} instead of a constant reference permits to prevent a static power dissipation when the logic net is not switching. A timing diagram of the V_{sync} signal is depicted in Fig. 5.

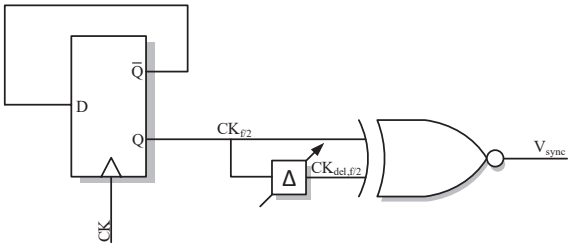

Fig. 4. Circuit implementation of the V_{sync} signal. The delay element is implemented with a starved inverter.

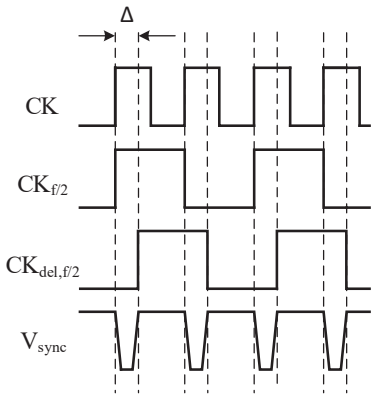

Fig. 5. Timing diagram of the V_{sync} signal.

IV. Evaluation on Logic Gates

To demonstrate the effectiveness of the proposed current-mode approach to thwart CPA attacks, basic combinational gates have been studied, and the power variability due to data-dependency has been analyzed using the on-chip current equalizer shown in Fig. 3.

For this reason, adopted metrics have to measure the power-balancing ability. Higher is the dispersion of the power over the input space, weaker to DPA is the implementation. To measure this dispersion, the *energy per cycle* is widely used as reference:

$$E = \int_0^{T_{cycle}} V_{DD} I_{tot}(t) dt \tag{13}$$

To have a fair comparison between different architectures, the following metrics have been adopted in this work [12]:

- **Normalized Energy Deviation (NED):**

$$NED = \frac{\max(E) - \min(E)}{\max(E)} \tag{14}$$

  min(E) and *max(E)*are the minimum and the maximum of the energy per cycles.

- **Normalized Standard Deviation (NSD):**

$$NSD = \frac{\sigma_E}{E_{AV}} \tag{15}$$

  E_{AV} and σ_E are the average and the standard deviation of the distribution of the energy per cycle respectively.

STMicroelectronics CMOS 40nm design library has been used for this work. The power supply voltage for CMOS gates is fixed at 1V, which is even the V_{DD_int} voltage of the protected gates. V_{DD} for the current equalizer is fixed at 1,2V. The clock frequency has been set to 20MHz.

In Table I, a comparison between standard CMOS gates (a) and standard CMOS gates protected with the proposed current equalizer (b) is shown.

As we can see, both NED and NSD of protected gates are 10-20 times smaller respect to unprotected implementations. It implies that the ability of the attacker to discriminate the peak value of the current consumption is reduced. The possibility of a successful DPA/CPA is strongly dependent on NSD value of both combinational and sequential gates.

TABLE I.
COMPARISON OF STANDARD CMOS (A) AND CMOS WITH THE PROPOSED CURRENT EQUALIZER (B) GATES AND FLIP-FLOP IN TERMS OF NED AND NSD.

CMOS	*NED*	*NSD*
NAND	0,81	0,55
NOR	0,80	0,58
NOT	0,81	0,80

a)

CMOS+CE	*NED*	*NSD*
NAND	0,0898	0,0373
NOR	0,0730	0,0334
NOT	0,0466	0,0255

b)

V. A CASE STUDY

Algorithm like PRESENT [22], SERPENT [23] and TEA [24] are now very popular on several commercial devices, because they offer a good mathematical security and lower design effort compared to classic AES. For this work, we choice a minimized version of the PRESENT algorithm, which is the 4x4 bit data-path of the regular PRESENT engine. It is composed by a 4-bit XOR layer and one 4-bit SBOX, as shown in Fig. 6.

$$ct = SBOX(pt \oplus key) \tag{16}$$

The comparison is performed on unprotected and protected implementation of the case study. The measurements are collected on Cadence Virtuoso and the attack routine is executed on Matlab. For the sake of generality, Gaussian distributed noise is added to simulation results, to simulate a real attack scenario [25].

The protected core has the same architecture of the unprotected one. Each sub-block shown in Fig. 6, has its own current equalizer, to provide local protection and filtering at power supply node. This choice allows to reduce the needs of large capacitor for C_l and let more degrees of freedom to the designer to customize current equalizers.

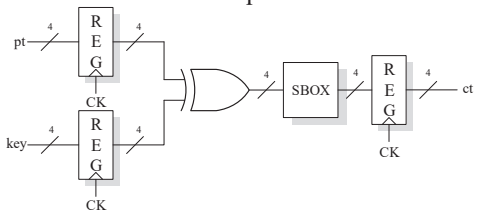

Fig. 6. 4x4 bit data-path of the PRESENT engine used as case study.

To simulate a real attack scenario, Gaussian white noise has been added to simulated power traces. In this work, 6dB of SNR has been chosen as reference for measurements, and a maximum of 100k traces has been used as maximum storage capability.

To assess the capability of the proposed current equalizer to protect a secure core from PAs, we use the Measurements Trace to Disclosure (MTD) [26] and the Success Value Indicator (SVI) [20], which is given by the CPA procedure. The SVI is equal to maximum difference between the peak of the correlation value for the correct key and the maximum peak of the correlation coefficient for the other possibilities. Note that the negative value of SVI represents unsuccessful attack.

$$SVI = \max(\rho_{ck}) - \max(\rho_{wk}) \tag{17}$$

The unprotected core has been successfully attacked with 8 traces. This result has confirmed what is already known in literature, but it is important for a good evaluation of the CMOS architecture protected by the proposed design.

The protected core shows a robust behavior to PA. In fact, the MTD of the protected PRESENT core is higher than 100k power traces. All simulated experiments on this core have not led to a successful attack, and the SVI is negative over the entire power measurement set. This result remarks the capability of our design to counteract a dynamic power analysis attack. Note that the logic and registers of the two cores are the same, but in the protected one, current equalizers allow to avoid a physical attack that uses dynamic consumption as information leakage source. The result of a CPA attack using the maximum storage capability is shown in Fig. 7.

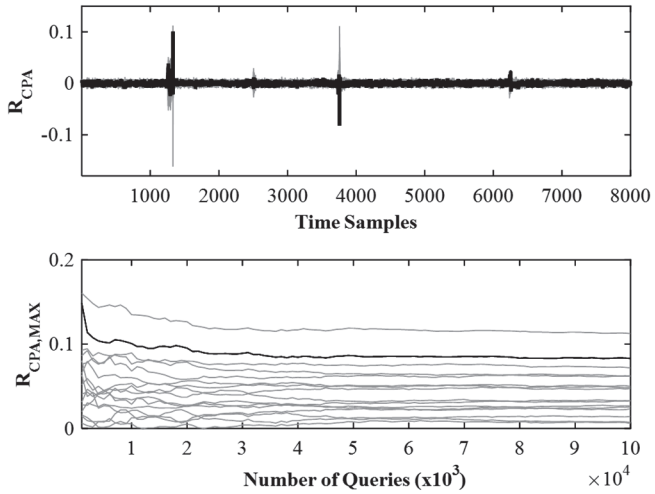

Fig. 7. Plots of the CPA attack on the protected 4x4 bit PRESENT crypto-core, using on-chip current equalizers as analog-level countermeasure. Top figure shows the correlation coefficient RCPA vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

In Table II, area and average power are shown for both implementations. In terms of silicon area, the protected core uses 3 times the area of the unprotected CMOS implementation, while the power consumption is almost 9 times.

TABLE II.
COMPARISON BETWEEN UNPROTECTED AND PROTECTED IMPLEMENTATION OF THE 4X4 BIT PRESENT CORE.

	Area [µm²]	P_{AV} [µW]	MTD	NED [%]	NSD [%]	Max SPI (@100k meas.)
CMOS	5,02	0,83	8	40,12	15,89	+0,25@100 meas.
CMOS+CE	15,34	7,25	>100k	7,53	2,28	-0,075@100k meas.

As we can see, NED and NSD values are strongly reduced in the protected implementation compared to standard CMOS, and no successful attack is possible within the storage capability. The improvement in security is more evident when the proposed countermeasure is used for logic sub-blocks. The use of current equalizers at gate-level leads to an inefficient design in terms of area, which even limits improvements in the security level.

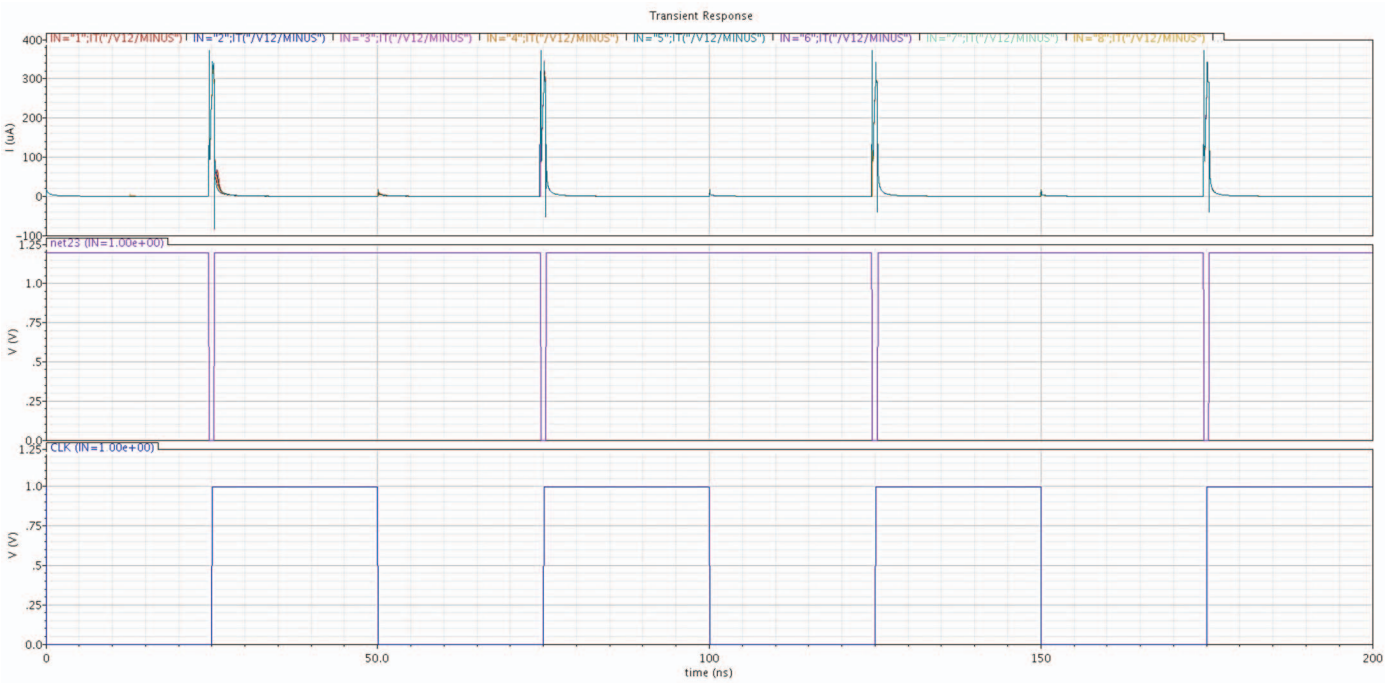

Fig. 8. Power consumption of the protected PRESENT module. The second and third plot shows V_{sync} and clock signals respectively.

VI. Improved On-chip Current-Mode Suppressor

As we can notice from TABLE II, the required area of the protected core using the current-equalizer in Fig. 3 is three times compared to unprotected one. In addition to that, also the average power overhead is x8.7. In order to make the *current-mode* approach compatible with demanding requirements of IoT devices, an improved on-chip current-mode suppressor is also presented in this work.

The block scheme of the improved on-chip current-mode feedback loop is shown in Fig. 9. The output current, which is namely the total current on the current sensor's branch, can be expressed as sum of two components as in Eq.(10)-(12):

$$I_{TOT} = I_{REF}\frac{A_{I1}A_{I2}R_X G_M}{1 + A_{I2}A_{I1}R_X G_M} + I_{LOGIC}(pt, key)\frac{1}{1 + A_{I2}A_{I1}R_X G_M} \quad (18)$$

where I_{TOT} is the total current, and I_{LOGIC} the current drawn by the cryptographic processor, which is the data-dependent signal exploited by the PAA. If the loop gain ensure the condition $A_{I1}A_{I2}R_X G_M \gg 1$, we have:

$$I_{TOT} \rightarrow I_{REF} \quad (19)$$

$$\Delta I_{TOT}(I_{LOGIC}(pt, key)) \rightarrow 0 \quad (20)$$

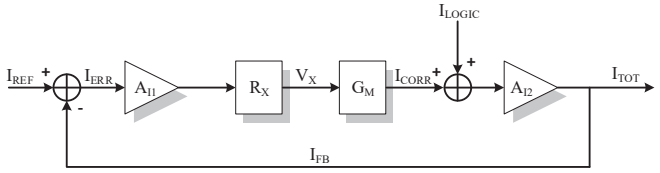

Fig. 9. Block scheme of the improved on-chip current-mode suppressor. I_{LOGIC} is considered as a disturbance to be rejected, in order to counteract a CPA attack.

The CMOS implementation of the proposed on-chip current-mode suppressor is depicted in Fig. 10. $M_{1,2}$-$M_{4,5}$ implement a Flipped Voltage Follower Current Sensor (FVFCS) [27], which offers a current mirror, and a very low impedance at the drain node of M_1, due to the shunt feedback provided by M_2. The very low impedance helps to feed the supply voltage correctly to the cryptographic logics, without no significant alteration of the nominal working condition. The output current of $M_{4,5}$, namely I_{FB}, is the sum of the current drawn by the logic I_{LOGIC} and the correction current I_{CORR} and it is compared with the reference current I_{REF}. $M_{9,10}$ provide the reference current I_{REF} which is not constant, but pulsed, in order to avoid an extra static power consumption.

In fact, CMOS digital circuits have a significant power consumption only during the active clock edge. According to Kirchhoff's law, the difference current I_{ERR} is mirrored by the high swing current mirror $M_{7,8,11,12}$, and it is defined as follow:

$$I_{ERR} = I_{REF} - I_{FB} = I_{REF} - A_{I2}\cdot(I_{CORR} + I_{LOGIC}) \quad (21)$$

I_{ERR} is amplified by a proper sizing of the aspect ratio of the aforementioned high swing current mirror, and it is converted to a voltage signal V_X through the high impedance that can be seen at the drain of M_{12}, which can be approximated as:

$$R_X \approx \left(r_{o,11}r_{o,12}g_{m12}\right)//\left(r_{o,14}r_{o,13}g_{m13}\right) \quad (22)$$

The signal V_X is used to control the gate voltage of M_4, in order to obtain I_{CORR}. If we assume the condition $A_{I1}A_{I2}R_X G_M \gg 1$ is satisfied, the I_{ERR} is negligible and the V_X is set to compensate the difference due to data-dependency of I_{LOGIC}. The control signal V_{PULSE} used to generate the pulsed I_{REF}, is generated by means of the circuit depicted in Fig. 11. Also in this design, a starved inverter has been used as delay element.

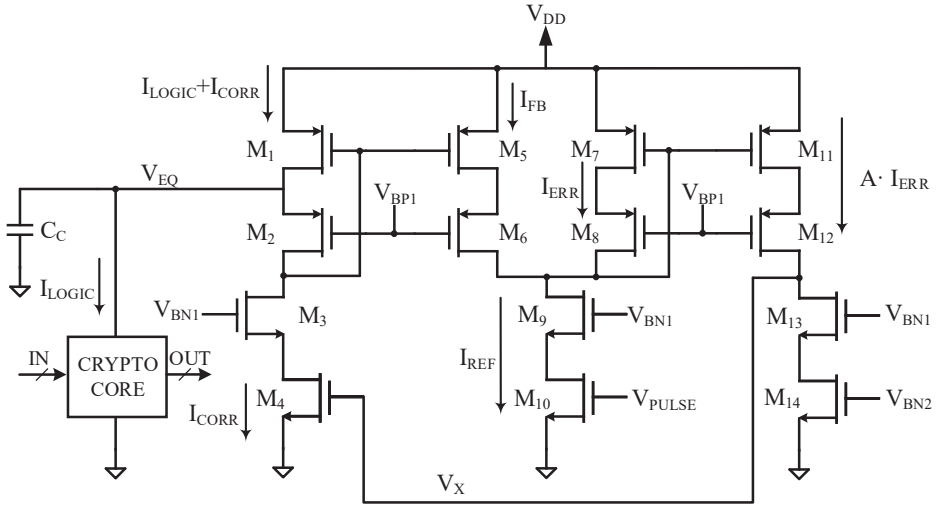

Fig. 10. CMOS implementation of the improved on-chip current-mode suppressor. The protected crypto-core is fed through the suppressor circuit.

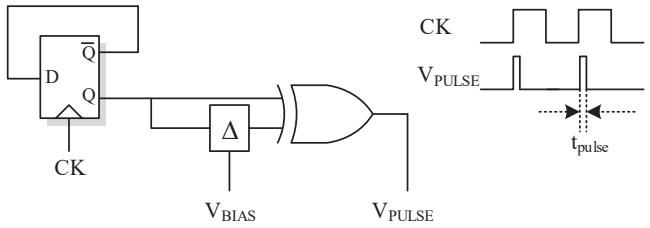

Fig. 11. Implementation of the pulse generator, which generates the signal V_{PULSE}.

VII. Evaluation of the Improved On-chip Current-Mode Suppressor

In order to better assess the effectiveness of the improved on-chip current-mode suppressor, a complete CMOS implementation of the PRESENT-80 block cipher [22] has been adopted as case study, as depicted in Fig. 12. Also in this case, a 40nm CMOS STMicroelectronics design library has been used to implement both the suppressor and the cryptographic core. A single on-chip suppressor has been used to protected and feed the core, in order to save as much area and power consumption as possible, while providing a good level of security. Power supply voltage has been set to 1V and the clock frequency to 20MHz. The SNR has been set to 18dB (uncorrelated noise due to other on-chip sub-systems and measurement equipment noise). Without loss of generality, the target function is the most significant nibble of the output of the *SubsLayer* at the first round, which can be expressed as follows:

$$ct_{63,62,61,60}^{round,1} = SBOX(pt_{63,62,61,60} \oplus key_{79,78,77,76}^{round,1}) \quad (23)$$

where $ct_{63,62,61,60}^{round,1}$ is the intermediate result, $pt_{63,62,61,60}$ is the most significant nibble of the plaintext, and $key_{79,78,77,76}^{round,1}$ is the most significant nibble of the key at round 1.

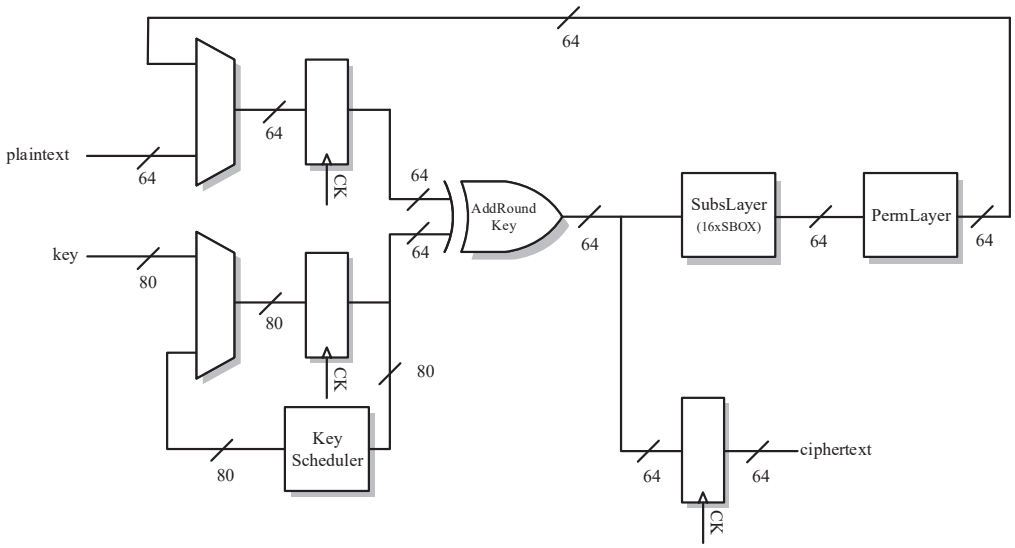

Fig. 12. Register-Transfer Level of the complete implementation of the PRESENT-80 block cipher used as case study in Section VII.

The CPA attack on both the protected and unprotected implementations has shown that also in this case the sub-key can be recovered with 16 power traces on the unprotected implementation, with a +0.132 of SVI. The improved on-chip current-mode suppressor provides an MTD greater than 100k measurements, and the SVI is always negative. The SVI using the maximum storage capability is -0.189. Results of CPA attack on both implementations are depicted in Fig. 13-14, and a resume is reported in Table III.

It has to be noted that also the rank of the key in the protected implementation (bottom plot of Fig. 14) is fair distant from first places, remarking the real effectiveness of this improved on-chip suppressor to hide the information leakage through dynamic power consumption. In addition to that, the area overhead is very small compared to the on-chip current equalizer depicted in Fig. 3 and to other CPA countermeasures, as shown in Table IV. Also the power consumption is very small, and it requires only +7% compared to the unprotected implementation of the PRESENT-80.

TABLE III.
COMPARISON OF UNPROTECTED VS. PROTECTED (WITH IMPROVED ON-CHIP SUPPRESSOR) COMPLETE PRESENT-80 CRYPTO-CORE.

	Area [μm²]	P_{AV} [μW]	MTD	NED [%]	NSD [%]	Max SPI (@100k meas)
Unprotected	105,59	12.57	16	6.76	2.27	+0.132
Protected (improved suppressor)	105,96	13.36	>100k	1.85	0.50	-0.189

TABLE IV.
COMPARISON BETWEEN THE OVERHEAD FACTORS FOR AREA AND AVERAGE POWER.

Implementation	*Area*	*Power*
CMOS	1	1
WDDL [26]	3.1	3.7
MDPL [13]	4-5	3-7
Gornik et al.[17]	≈10	≈3.5
This work	3	≈8.7
This work (improved vers.)	1.004	1.07

For the sake of completeness, the case study has been analyzed within the technology process corners, in order to take into account the presence of die to die variations and their impact on the effectiveness of the proposed countermeasure. CPA attacks on the PRESENT-80 with SS and FF process corners show that the countermeasure is effective and the MTD is greater than 100k. The SVI in the FF case is -0.068, and in the SS case is -0.111, using the maximum storage capability. These results demonstrate that the on-chip current equalizer is able to counteract a CPA attack also in the presence of die to die variations.

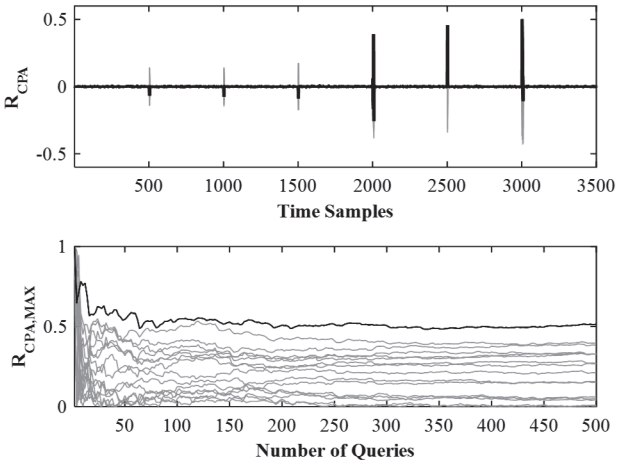

Fig. 13. Plots of the CPA attack on the unprotected PRESENT-80. Top figure shows the correlation coefficient R_{CPA} vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

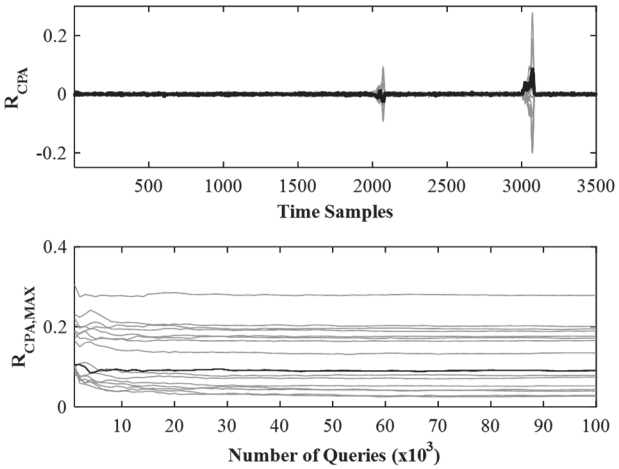

Fig. 14. Plots of the CPA attack on the protected PRESENT-80, using the on-chip current-mode suppressor as analog-level countermeasure. Top figure shows the correlation coefficient R_{CPA} vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

VIII. CONCLUSION

In this work, a novel, analog circuit based, approach to counteract CPA attacks has been presented. The concept behind the two designs presented in this paper is to hide to the malicious attacker the actual power consumption of a cryptographic device by compensating differences in power consumption with an analog current-mode feedback loop. The aim of the current-mode feedback loop is to get the same current drawn at each clock edge in spite of the input pattern. It allows to reduce the possibility to use the dynamic power consumption as a source of information leakage, because of the presence of the current equalizer sub-block.

The on-chip current equalizer allows to strongly reduce the possibility to mount a successful attack exploiting dynamic power. In fact, with 4x4 bit PRESENT crypto-core, the MTD is

increased at least of three orders of magnitude. However, the area and the power consumption overhead does not make it suitable to be implemented in an ultraconstrained secure design, like IoT smart device. In order to provide a suitable implementation of the current-mode approach to counteract CPA attacks, an improved design, namely the improved on-chip current-mode suppressor, has been presented in this work.

By using the proposed improved on chip current suppressor, and referring to the power consumption of the complete implementation of the PRESENT-80 block cipher, both NED and NSD are strongly reduced. Furthermore, simulated CPA attacks, using additive Gaussian distributed white noise, have been performed to evaluate the real effectiveness of the approach in a complete implementation. The MTD has been increased at least of three orders of magnitude, comparing the unprotected PRESENT-80.

The improved on-chip current-mode suppressor has a very small footprint compared the on-chip current equalizer. It provides a x1.004 area overhead and a x1.07 power consumption overhead. This improved on-chip suppressor is fully suitable and implementable in secure IoT smart devices, since it is able to meet demanding requirements of area/power overhead, while providing a strong increase in the level of security. It has to be considered that the presence of the on-chip current suppressor is compliant with several others PAA countermeasures, giving to designers the possibility to implement nested protections throughout different abstraction levels.

REFERENCES

[1] Dave Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," Cisco White Paper, April 2011.

[2] M. Wolf, A. Weimerskirch, and T. Wollinger, "*State of the art: Embedding security in vehicles,*" EURASIP Journal on Embedded Systems, vol. 2007, no. 1, pp. 1–16, 2007.

[3] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "*Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,*" in Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008, pp. 129–142.

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

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

[6] P.C.Kocher, J.Jaffe, and B.Jun.Differential Power Analysis.In Proceedings of Advances in cryptology, CRYPTO '99.Lect.Notes in Computer Science, vol.1666, pages 388-397.Springer, 1999.

[7] E. Brier , C. Clavier and F. Olivier , "Correlation power analysis with a leakage model" , *Proc. CHES* , vol. 3156 , pp.16 -29 , 2004.

[8] M. Alioto, L. Giancane, G. Scotti, A. Trifiletti, *"Leakage Power Analysis Attacks: a Novel Class of Attacks to Nanometer Cryptographic Circuits"*, In IEEE Transaction on Circuits and Systems-part I, vol. 57, no. 2, pp. 355-367, Feb. 2010.

[9] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti, "*Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations*," IEEE Trans. Circuits Syst. I, Reg. Papers, 2014, vol. 61, pp. 429-442.

[10] D. Bellizia; S. Bongiovanni; P. Monsurro; G. Scotti; A. Trifiletti, "Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications," in IEEE Transactions on Emerging Topics in Computing , vol.PP, no.99, pp.1-1

[11] K. Tiri and I. Verbauwhede. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. In Proc. of Design, Automation and Test in Europe Conference and Exposition (DATE '04), pp. 246-251, 2004.

[12] 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. of ESSCIRC '02.

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

[14] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, *"Delay based dual-rail precharge logic"*, VLSI Syst. IEEE Trans., 1147–1153 (2011).

[15] Bongiovanni,F. Centurelli, G. Scotti, A. Trifiletti, "*Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks*", in J.of Crypt.Eng., Springer Berlin Heidelberg, April 2015.

[16] Tokunaga, C.; Blaauw, D., "Securing Encryption Systems With a Switched Capacitor Current Equalizer," in *Solid-State Circuits, IEEE Journal of* , vol.45, no.1, pp.23-31, Jan. 2010.

[17] Gornik, A.; Moradi, A.; Oehm, J.; Paar, C., "A Hardware-Based Countermeasure to Reduce Side-Channel Leakage: Design, Implementation, and Evaluation," in *Computer-Aided Design of Integrated Circuits and Systems, IEEE Trans. on* , vol.34, no.8, pp.1308-1319, Aug. 2015.

[18] Ratanpal, G.B.; Williams, R.D.; Blalock, T.N., "An on-chip signal suppression countermeasure to power analysis attacks," in *Dependable and Secure Computing, IEEE Trans. on* , vol.1, no.3, pp.179-189, July-Sept.2004.

[19] S. Mangard, E. Oswald, and T. Popp, "*Power Analysis Attacks: Revealing the Secrets of Smart Cards"*, Springer-Verlag, 2007.

[20] R. Muresan and S. Gregori, ``Protection circuit against differential power analysis attacks for smart cards," *IEEE Trans. Comput.*, vol. 57, no. 11, pp. 1540_1549, Nov. 2008.

[21] Binti Mokhtar, S.M.A.; Abdullah, W.F.H.W., "Memristor based delay element using current starved inverter," in *Micro and Nanoelectronics (RSM), 2013 IEEE Regional Symposium on* , vol., no., pp.81-84, 25-27 Sept. 2013.

[22] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, *"PRESENT: An Ultra-Lightweight Block Cipher Cryptographic Hardware and Embedded Systems-CHES 2007. "* Vol. 4727, P. Paillier and I. Verbauwhede, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 450-466.

[23] Ross Anderson, Eli Biham and Lars Knudsen , "Serpent: A Proposal for the Advanced Encryption Standard" , *submitted to NIST as an AES candidate*.

[24] David J. Wheeler and Roger M. Needham, *"TEA, a tiny encryption algorithm."* Proc.First International Conference on Security in Pervasive Computing, Boppard, Germany, March 12-14, 2003.

[25] 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.

[26] K. Tiri, D. Hwang, et al. Prototype IC with WDDL and differential routing - DPA resistance assessment. In Proceedings of CHES 2005, pp. 354-36.

[27] R. G. Carvajal *et al*., "The flipped voltage follower: a useful cell for low-voltage low-power circuit design," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 52, no. 7, pp. 1276-1291, July 2005.

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

Davide Bellizia was born on June 20th 1989. He received the Bacherlor's Degree in Electronic Engineering and the Master's Degree (summa cum laude) in Electronic Design from University "La Sapienza" of Rome (Italy), respectively in 2011 and 2014. In 2014 he received the "Laureato Eccellente" award for the best graduated student of the year. He is currently attending a Ph.D. course at the Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni of the University "La Sapienza" of Rome. His research interests include the design of cryptographic ICs for counteracting power analysis attacks, and VLSI design for DSP algorithm implementations.

Alessandro Trifiletti was born in Rome, Italy, in 1959. He received the Laurea degree in electronic engineering from the Università di Roma "La Sapienza." In 1991, he joined the Dipartimento di Ingegneria Elettronica, Università di Roma "Sapienza" as a Research Assistant, where he is now engaged as Associate Professor. His research interests include high speed circuit design techniques, III-V device modeling, DSP techniques to enhance analog circuit performance, techniques to improve resilience to security attacks in VLSI ICs and robust design methodologies. He has published over 70 international journal papers and 120 contributions in conference proceedings.