TEL Logic Style as a Countermeasure Against Side-Channel Attacks: Secure Cells Library in 65nm CMOS and Experimental Results

Davide Bellizia, Giuseppe Scotti, and Alessandro Trifiletti

***Abstract*— This paper presents experimental results on a dual-rail pre-charge logic family whose power consumption is insensitive to unbalanced load conditions. The proposed logic family is based on the time enclosed logic (TEL) encoding and can be viewed as an improvement of the delay based dual rail pre-charge logic (DDPL) logic style. The DDPL logic gates have been redesigned to avoid the early evaluation effect and to reduce area and power consumption. A library of TEL secure gates and flip-flops has been implemented in a 65 nm CMOS process. The developed library allows adopting a semi-custom design flow (automatic place and route) without any constraint on the routing of the complementary wires. A four bit lightweight crypto core has been implemented on a 65 nm CMOS testchip by using the developed TEL library and compared against a SABL implementation of the same crypto core on the same chip. Comparisons have been carried out by means of extensive transistor level simulations and measurements on the 65 nm testchip which allowed to evaluate a wide set of security metrics. Experimental results have shown a strong reduction of the information leakage with respect to the sense amplifier based logic logic style under mismatched load conditions with an improvement in the measurements to disclosure of more than three orders of magnitude.**

***Index Terms*— Cryptography, security, power analysis attacks (PAAs), dual-rail logic, sense amplifier-based logic (SABL), delay-based dual-rail pre-charge logic (DDPL).**

I. Introduction

THE protection of information manipulated by electronic devices is considered one of the most challenging tasks in electronic products (e.g. smartphones, ID cards, IoT smart nodes). Modern devices providing cryptographic functions, such as authentication, encryption, etc., have been demonstrated to be unsecure against physical attacks, namely, Side-Channel Attacks (SCAs). In fact, SCAs allow a malicious attacker to disclose confidential information (IDs, PIN codes, etc.) without demanding needs of cryptanalytic attacks [1]. SCAs take advantage of the dependency of physical emissions, such as power consumption, electro-magnetic emission, time execution, of a device performing cryptographic operations. In the design of cryptographic devices, these dependencies have to be carefully minimized, since they represent a concrete threat to the protection of sensible data [2].

The physical security of devices providing cryptographic features against SCAs has become more and more relevant in the last twenty years, since the publication of Differential Power Analysis (DPA) [2] in 1999. The possibility to reveal secret information through the exploitation of the power consumption represents a severe threat, since it does not require expensive laboratory equipment [3].

In the technical literature, a huge effort has been made towards the development of countermeasures against attacks exploiting power consumption. In this paper, we focus on transistor level countermeasures, which aim at minimizing the correlation between the power consumption and the processed data. Dual-Rail Pre-charged Logic (DPL) styles based on the Return to zero (RTZ) data encoding, such as Wave Dynamic Differential Logic (WDDL) [4], Sense Amplifier Based Logic (SABL) [5], and Masked DPL (MDPL) [6] have been proposed in the past to reduce differences in dynamic power consumption due to data-dependency by exploiting differential signaling and dynamic operation.

The main issue behind the use of differential logic styles is the limited effectiveness due to not properly balanced parasitic capacitance of complementary wires. In the technical literature, semi-custom design flows, supporting differential signaling and dynamic operation, have been proposed in order to achieve a more accurate balance of differential lines parasitic capacitance. In [7], a routing methodology for DPL styles has been introduced as the "fat wire" method to minimize mismatches on differential interconnections. In [8], Guilley *et al.* have proposed the "back-end duplication" method to overcome capacitive mismatches issues in dual-rail implementations. The main idea is to use a regular design flow on a single-ended netlist, taking care to leave enough free space on the core section of the floorplan to make possible the place and route of the duplicated part of the netlist. These approaches do not take into account the dependence of the capacitive load on a line on the logic state of the adjacent wires and, furthermore, introduce additional constraints for the routing tool thus limiting its efficiency and, likely, causing an area

Manuscript received March 30, 2018; revised July 12, 2018; accepted July 25, 2018. Date of publication August 20, 2018; date of current version October 2, 2018. This paper was recommended by Associate Editor A. Cilardo. *(Corresponding author: Giuseppe Scotti.)*

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

G. Scotti and A. Trifiletti are with the Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni, Sapienza Università di Roma, 00185 Rome, Italy (e-mail: scotti@diet.uniroma1.it).

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.2018.2861738

overhead especially if only few metal layers are available for the inter-cell routing. In addition, in modern nanometer CMOS technologies, random process variations cannot be neglected and they are the limiting factor for the load matching accuracy.

An alternative strategy has been reported in [9]: a logic insensitive to unbalanced routing capacitances is obtained by introducing a three-phase dual-rail pre-charge logic (TDPL) with an additional discharge phase where the output, which is still high after the evaluation phase, is discharged as well. Since both outputs are pre-charged to V_{DD} and discharged to 0V, a TDPL gate shows a constant energy consumption over its operating cycle. The main drawback of this solution is the additional area and power consumption overhead for the routing of the three clock signals.

To overcome this problem, Bucci *et al.* [10] and Bongiovanni *et al.* [11] have proposed the Delay-based Differential Pre-charge Logic (DDPL) in which data encoding is based on the use of a time domain signaling, which can be tolerant, from a security point of view, to the capacitive imbalance of gate interconnections.

An important limitation of all the above countermeasures is due to the early evaluation effect. The early evaluation is a transistor-level effect, which causes a logic gate to evaluate before all inputs are valid. This effect is directly linked to the logic function and is mapped into the physical implementation. It is very critical for a DPL combinational gate because it produces a dependence of the adsorbed current on the arrival times of the input signals, resulting in a data dependent power consumption even for DPA-resistant circuits implemented with perfectly balanced internal and output capacitances. There is a number of papers in which authors describe this vulnerability in the DPA-resistant DPL logic families, both theoretically [12], [13] and experimentally [14], [15].

In this paper we present an improved version of the DDPL logic style (iDDPL) which is not prone to the early evaluation effect and in which the area and power consumption overhead have been reduced. We present also the design and implementation of a library of secure cells in a commercial 65nm CMOS technology which is then used to build a secure cryptographic core on a testchip for validation purposes.

In the following, section II discusses the TEL signaling concept and the topology of iDDPL cells. Section III focuses on the implementation of the secure cells library and section IV introduces the 65nm CMOS testchip designed with the aim of validate the secure cells library. Measurements results are reported in section V and conclusions are drawn in section VI.

II. TEL Concept and iDDPL Gates

During the design phase of a secure implementation, it is important to make the proper assumptions on the power consumption model that the adversary can exploit in a real attack scenario. The main assumption behind the practical application of TEL data encoding is that the adversary has limited resources in time resolution and bandwidth of the measurement setup [11].

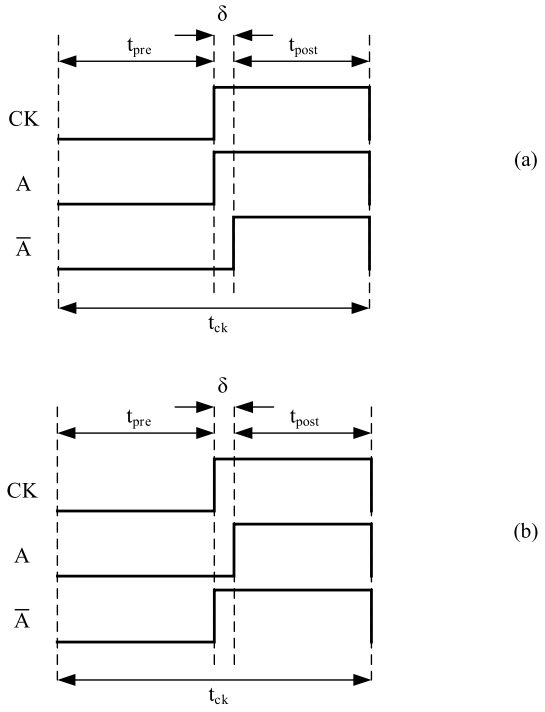

Fig. 1. TEL signaling for logical '1' (a), logical '0' (b).

A. Time Enclosed Logic Principle

The main difference between the TEL and the RTZ data encoding is that the TEL datum is encoded in the time-domain, and not in the differential voltage amplitude-domain.

In TEL encoding, the clock cycle is divided in three subsequent phases: pre-charge phase (t_{pre}), evaluation phase(δ), post-evaluation phase (t_{post}). The period of the clock signal can be expressed as the sum of the duration of the three phases:

$$t_{ck} = t_{pre} + \delta + t_{post} \tag{1}$$

During the pre-charge phase, both wires of a complementary pair assume the same value, for example "0". In this phase, all transistors are pre-charged at the corresponding voltage value, and the complementary output of each cell assumes the logic value "0". In this way, the entire combinational path is pre-charged and all internal capacitances of the combinational gates are at the same voltage value. In the evaluation phase, the complementary pair assumes its differential value, and the logic nets evaluate the results. After the evaluation phase, all the signals are forced to the logic value "1" (post-evaluation phase t_{post}). The presence of this third phase allows to avoid information leakage due to memory effect, which is typical of most standard-cell based logic styles using the RTZ encoding. The signaling used in TEL protocol is depicted in Figure 1 (a)-(b), respectively for the logical "1" and "0". For the invalid logic value, both complementary wires have the same value throughout the entire clock cycle. A resume of the value of both wires in each phase for each logic value, is reported in Table I.

In TEL encoding the relevant information is enclosed in the duration of the evaluation phase δ, and all the information that is leaked by the hardware implementation can be captured

TABLE I

TEL VALUES AND VOLTAGES FOR EACH PHASE OF A CLOCK CYCLE

Pre-Charge		Evaluation		Post-Evaluation		TEL Enc.	Logical Value
A	$\overline{A}$	A	$\overline{A}$	A	$\overline{A}$	$(A,\overline{A})$	IN
0	0	0	V_{DD}	V_{DD}	V_{DD}	(0,1)	0
0	0	V_{DD}	0	V_{DD}	V_{DD}	(1,0)	1
0	0	V_{DD}	V_{DD}	V_{DD}	V_{DD}	NULL	Invalid

TABLE II

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

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

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

only during the time window δ. To increase the security level the duration of evaluation phase δ has to be minimized with respect to the duration of both the pre-charge and post-evaluation phases: $\delta \ll t_{pre}$ and $\delta \ll t_{post}$.

In fact, if the sampling period of the Digital Storage Oscilloscope (DSO) used to carry out the measurements for the attack is greater than δ, no relevant power samples can be captured, and the adversary will not be able to recover information from the device's consumption.

The two main requirements for TEL circuits can be summarized as follows:

- The average current on a clock cycle is balanced (property of energy balancing).
- The instantaneous current exhibits a limited time interval in which the leakage could be potentially detectable (property of timing enclosing).

A summary of the dynamic power consumption of RTZ and TEL encoding schemes is reported in Table II.

In Table II, C_{L1} and C_{L2} denote the parasitic capacitances at the output of two complementary wires and the expression of $P_{dyn,TOT}$ highlights the robustness of TEL encoding with respect to mismatches in the load capacitances of the gates.

B. iDDPL Logic Gates as a Template for TEL Circuits

The iDDPL logic style presented here has been conceived as an improvement of the conventional DDPL style, which cannot be directly used as template for TEL circuits. Indeed, one drawback of the conventional DDPL style is that even if the energy on a clock cycle is balanced, as proved by Bucci *et al.* [10], the instantaneous power consumption may still depend on the processed data. More specifically, the dynamic peaks in the current traces may have a certain time length, and this depends on the electrical mismatches, causing

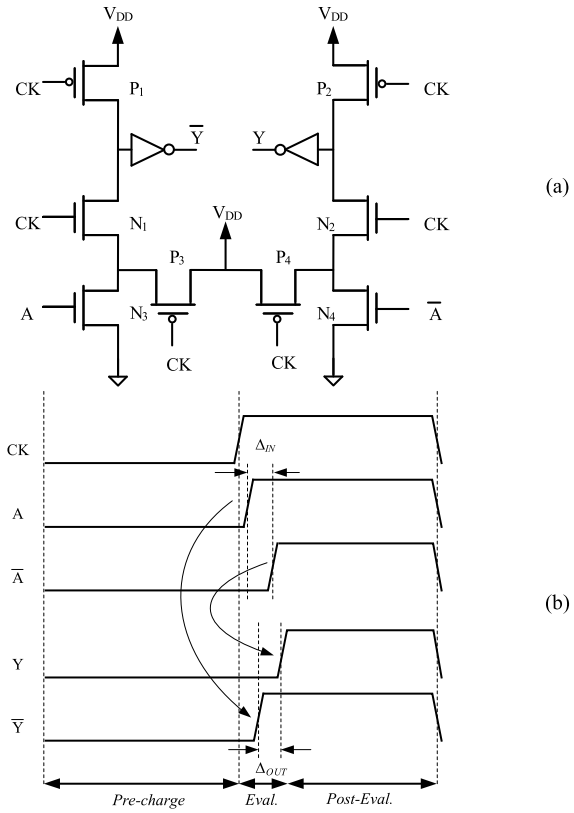

Fig. 2. iDDPL buffer/inverter gate (a) and timing diagram (b).

the leakage to be visible also outside the interval δ, both in the evaluation and in the pre-charge phase. We must notice that the gate can propagate its logical output value without waiting that all input signals are valid. In fact, in the DDPL proposed in [10], the *evaluation depth*, which corresponds to the number of transistor in series between the supply line and the output internal capacitance, is not the same for the two branches of AND/NAND gates. Early propagated transitions provide data-dependent power consumption, which the adversary can exploit to recover secret information from the device. So far, the DDPL style does not meet the requirement on timing enclosing defined for TEL circuits, and the schemes presented by Bucci *et al.* [10] cannot be adopted to build circuits implemented in a TEL fashion.

The iDDPL style proposed in this work has the aim of balancing not only the energy in a clock cycle, but also the instantaneous power consumption.

Unlike DDPL, the iDDPL style meets the two main requirements of TEL circuits discussed in the previous section: (property of energy balancing and property of timing enclosing).

The basic iDDPL inverter (BUFF/INV) is shown in Figure 2 (a). We refer as n-type (p-type) to a dynamic circuit in which the evaluation network is the pull-down (pull-up). The cell library we will describe in this work is composed of n-type iDDPL gates, in order to take advantage of reduced area and higher carrier mobility compared to p-type gates. The pulldown network has a direct connection with the ground line, saving the area overhead due to foot-transistor in TDPL. When *CK* is low, the combinational logic is in pre-charge

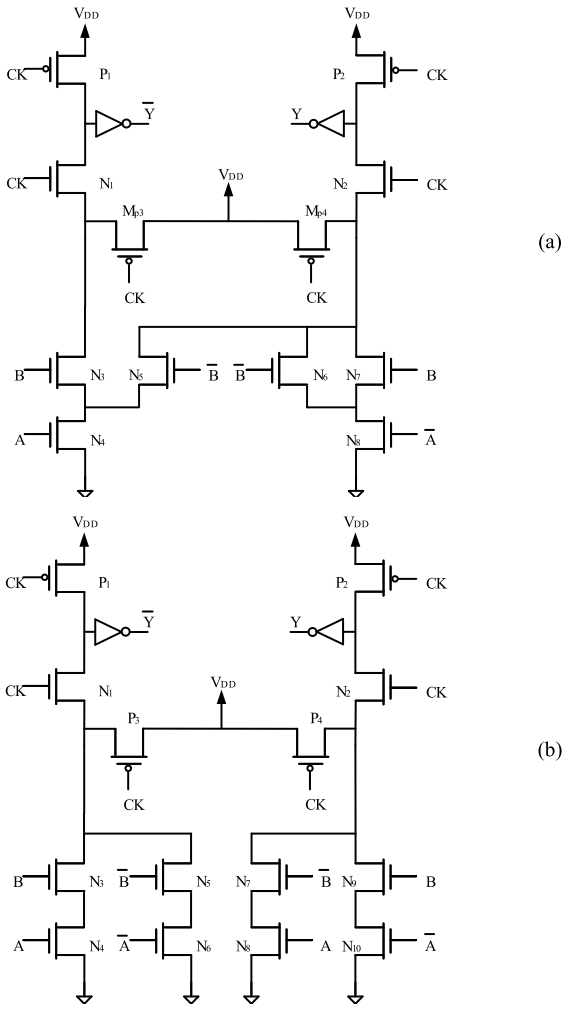

Fig. 3. iDDPL n-type AND/NAND (a) and XOR/XNOR (b) gate.

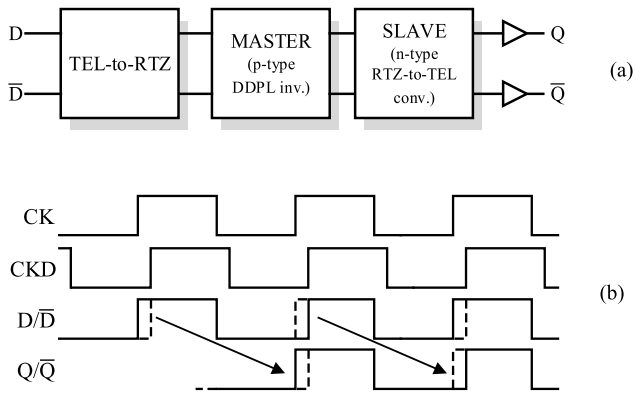

Fig. 4. Block scheme of the iDDPL sequential element (a) and timing diagram (b).

phase, and input and output signals of each gate are set to 0V, due to transistors $P_{1,2}$ which force the inputs of the CMOS inverters to V_{DD}. During the evaluation phase, assuming the input value $(A, \bar{A}) = (1, 0)$, as shown in the timing diagram in Figure 2 (b) the output signal Y is charged after $\bar{Y}$, providing the correct TEL value $(Y, \bar{Y}) = (0, 1)$ at the output of the gate. After the evaluation, both input signals are charged to V_{DD}, and consequently, both output lines are set to V_{DD}. The two transistor $P_{3,4}$ have been inserted to avoid the memory effect due to internal capacitance of the pull-down network, during the pre-charge phase. At the beginning of each pre-charge phase, the upper nodes of the pull-down network are both charged to V_{DD}. The presence of these two additional transistors respect to the DDPL combinational template in [10] and [11], allows to achieve a better balancing in the energy per cycle, making the consumption of each gate throughout the clock cycle independent from the input pattern.

An interesting strategy to achieve a more symmetric structure for an AND/NAND gate at the expense of a few more transistors can be found in [16].

The iDDPL AND/NAND gate has been redesigned using a NAND *approach*, as shown in Figure 3 (a). The presence of additional transistors in the evaluation network allow to equalize the resistive path during the evaluation phase, avoiding, the occurrence of the *early evaluation* effect.

This approach, similarly to the fully connected SABL in [17], allows to balance the propagation times for each possible input pattern. The XOR/XNOR gate scheme is reported in Figure 3 (b).

C. iDDPL Flip-Flop

The typical approach to the design of flip-flops for DPL style is based on three basic operations:

1. a specific differential signal pair is sampled at the clock rising edge;
2. the signals are then held for a clock period;
3. these signals are finally used to regenerate the original data-encoding in correspondence to the clock rising edge of the following cycle.

In [18], a balanced flip-flop that is compatible for TEL data encoding has been proposed, according to the block scheme and timing diagrams depicted in Figure 4. The DDPL flip-flop uses the master-slave architecture of the SABL flip-flop in [3] and share the same "p-type+n-type" inverter paradigm. The flip-flop in DDPL (and more in general for TEL compatible logic styles) needs of additional sub-systems that convert the signal from/to the TEL domain to/from the RTZ domain. A self-timed pulse clock latch is used to convert the TEL signal to an RTZ signal. A transistor schematic of the self-timed pulse clock latch in [18] is depicted in Figure 5 (a). A p-type DDPL inverter is used as master latch, while the slave device has been implemented using the n-type RTZ-to-TEL converter shown in Figure 5 (b), which acts as a latch and allows to restore the TEL encoding. The architecture proposed in [18] is able to tolerate higher capacitive mismatch compared to other DPL flip-flops, remarking the ability of the TEL encoding to increase the level of security also in the presence of strong mismatches.

Recently a different approach to implement TEL compatible flip flops has been proposed in [19]. The approach proposed in [19] is focused on an FPGA compatible implementation which, we consider out of the aim of this work.

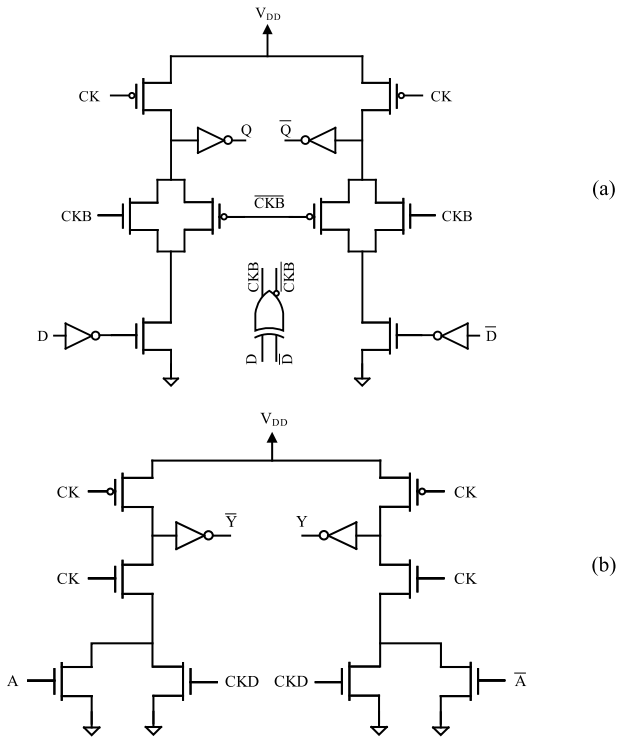

Fig. 5. In (a), the self-timed pulse clock latch used as TEL-to-RTZ converter in iDDPL flip-flop architecture. In (b), the n-type RTZ-to-TEL latch/converter.

TABLE III

SUMMARY OF THE DDPL065 SECURE LIBRARY FOR EXTREME MISMATCH MF = 4 (TRANSISTORS OVERHEAD COMPARED TO CMOS065 LIBRARY)

iDDPL065	No. of Transistors	Transistors Overhead	Max(E_{AV}) [fJ]	Max[NED] [%]
BUFF/INV	6N + 6P	x6.0	9.76	0.20
AND/NAND	10N + 6P	x4.0	14.04	1.56
OR/NOR	10N + 6P	x4.0	14.04	1.56
XOR/XNOR	12N + 6P	x1.5	14.71	1.31
MUX	30N + 18P	x4.0	35.07	1.21
FLIP-FLOP	36N + 25P	x4.3	45.54	1.55

III. FULL-CUSTOM IMPLEMENTATION OF TEL SECURE LIBRARY IN 65nm CMOS

In this section, we present the *iDDPL065* prototype library (see Table III) built upon the CMOS065SVTLP process from STMicroelectronics. The library is composed of iDDPL gates with minimum fan-in, designed according to the analysis done in the previous section. The parameters reported in Table III are obtained through post-layout SPICE simulations (adopting accurate BSIM4 models of transistors provided by the foundry).

According to these values, the area overhead is calculated dividing the number of transistors used for the iDDPL gate by the number of transistors used for the correspondent CMOS gate in the standard cell library. The layout area for the different cells is reported in Table IV for iDDPL and SABL implementations. According to the values in Table IV and Table IV the iDDPL circuit template impacts the area overhead as well as the power consumption of a factor less than 4 with respect to the CMOS counterpart.

TABLE IV

SUMMARY OF THE IDDPL AND SABL SECURE LIBRARY LAYOUT AREA (AREA OVERHEAD COMPARED TO CMOS065 LIBRARY)

Layout cell	iDDPL Area (μm^2)	SABL Area (μm^2)	iDDPL overhead	SABL overhead
BUFF/INV	17,93	13,99	7,37	5,75
AND/NAND	20,42	19,19	6,85	6,445
OR/NOR	20,42	19,19	6,85	6,445
XOR/XNOR	22,85	19,19	4,17	3,505
MUX	61,28	57,59	11,19	10,52
FLIP-FLOP	88,8	50,64	9,18	5,23

In this section, we introduce the *mismatch factor* (*MF*) as a measure of unbalancing between the load capacitor charged by the two differential signals at the output of a given gate. For a generic DPL cell, we could define a *mismatch factor* *MF* as follows:

$$MF = \frac{C_{false}}{C_{true}} \tag{2}$$

where C_{false} and C_{true} are the nominal load capacitance of the *false* and *true* outputs respectively. A $MF \neq 1$ should be expected also in a manually routed design, since mismatches are unavoidable in nowadays technologies.

In PAAs, the adversary takes advantage of the data-dependency in the power consumption for recovering sensible information. We consider the definition of *energy per cycle* E_{cycle} as the amount of energy requested by a circuit to process data within a clock period, as indicated in Eq. (3) [5]:

$$E_{cycle} = \int_0^T V_{DD} i\,(t)\,dt \tag{3}$$

where V_{DD} is the power supply voltage (assumed constant), $i(t)$ is the current absorbed by the circuit (the measured/simulated signal) and T is the clock period.

Since$i(t)$ is data-dependent, also E_{cycle} will follow this dependency as well. Upon the definition in Eq.(3), the *Normalized Energy Deviation* (*NED*) [5] is defined as:

$$NED = \frac{\max\left(E_{cycle}\right) - \min(E_{cycle})}{\max(E_{cycle})} \tag{4}$$

where $\max\left(E_{cycle}\right)$ and $\min\left(E_{cycle}\right)$ represents the maximum and minimum energy per cycle within the possible input vectors. The usage of the *NED* helps in estimating the variability of the power consumption of the device under test (gate or circuit) due to data-dependency. The evaluation of the iDDPL library regarding the power variability is performed in a worst-case scenario. In fact, the *NED* is calculated in the case of extreme unbalance ($MF = 4$), which is a considerably high value for small compact designs.

For each element of the iDDPL library presented above (combinatorial, sequential, converters and additional sub-blocks), we have created the views needed for the synthesis and place & route steps, (i. e. .dB, .lib and .LEF files). This library can be used in a semi-custom design flow similar to the

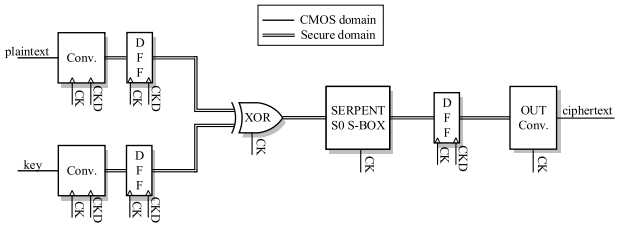

Fig. 6. Block scheme of the 4-bit SERPENT-based crypto-cores in the SERPAES chip. The signal CKD is used only on the iDDPL core.

one reported in [20], [21], and [22]. First, the technology mapping is executed by using the iDDPL library, in substitution of the technology library provided by the foundry in the PDK; for this purpose, the wires of the synthesized netlist are duplicated in accordance to a differential architecture. In conventional secure semi-custom design-flows for RTZ DPL-based designs, the next step would be the optimization of the routing to obtain a minimization of the capacitive mismatch between complementary wires (in [20], [21], and [22]). In our flow, this step is not needed and the place & route does not require such optimization due to the properties of the TEL encoding.

IV. Test Chip Design: TEL vs SABL Comparison

In this section, we discuss the implementation of a 4-bit cryptographic processor, based on the SERPENT algorithm [23] by using the presented iDDPL secure library, along with implementation of the same core by using a reference fully-connected SABL logic style. The motivation behind this choice relies on the observation that the SABL has been considered one of the most reliable gate-level countermeasures for ASIC implementations, thus we consider the latter as state-of-the-art of DPLs for secure applications. Also for the SABL implementation, a secure full-custom library has been designed, according to [3] and [17].

Both cores share the same 4-bit architecture, implementing round-0 of the SERPENT block cipher [23]. The block scheme of the 4-bit SERPENT crypto-core is depicted in Figure 6. The conversion of input data from CMOS to the respective secure domain is performed by CMOS-to-RTZ and CMOS-to-TEL input converter respectively. The secure domain is composed by two pipelined stages. The first one performs bitwise XOR operation between the 4-bit input plaintext and the 4-bit key.

The second stage implements the non-linear *S0* S-BOX function of the SERPENT algorithm and the complete encryption requires three clock cycles.

The testchip, shown in Figure 7, has been manufactured using the aforementioned process from STMicroelectronics, and contains five standard-cells implementations of the AES-128 block cipher [24] along with the aforementioned iDDPL and SABL crypto-cores. The two cores are placed side-by-side in a *macro* block, in the lower right corner of the chip's core area, as shown in Figure 7. The two implementations of the 4-bit SERPENT crypto-core share the same ground ring, but they have separated power nets. It has to be noted that to allow full PAA evaluation of the crypto cores, several *test points* for power analysis have been placed on the testchip.

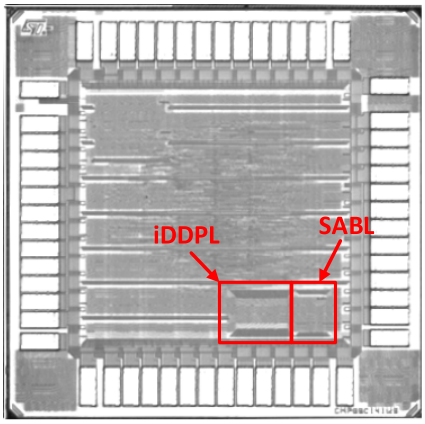

Fig. 7. Microphotograph of the SERPAES chip. In red, the SERPENT-based crypto-cores presented in this work.

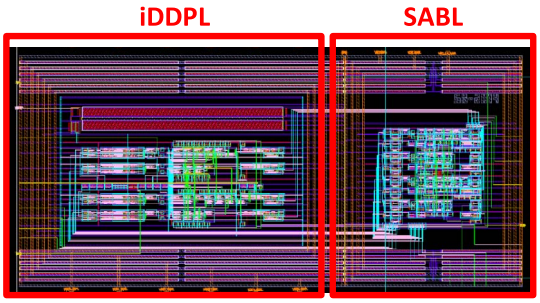

Fig. 8. Layout of the SERPENT macro. The section on the left is the iDDPL implementation, while the one on the right is the SABL implementation.

TABLE V
VBAL Values vs. Additive Capacitance (C_{add})

V_{BAL}	'00'	'01'	'10	'11'
C_{add}	0fF	3.2fF	6.4fF	9.6fF

Separate power nets provide the possibility to monitor power consumption of different sub-blocks in each implementation and each power net is accessible from the outside by a specific external pin. To enforce the isolation, a multiplexer system allows the operation of one of the two cores at a time.

The layout of both crypto-core implementations is shown in Figure 8. A custom programmable load cell has been designed to emulate the presence of capacitive mismatch on all the differential lines in the crypto cores. The programmable load cell is composed by two capacitors activated by two n-MOS switches independently and the additive capacitance C_{add} can be programmed with the 2-bit word V_{BAL}, providing 4 different values, according to Table V.

In order to take into account the presence of C_{add} on the *false* output, we could define the *total mismatch factor* $MF_{tot}[V_{BAL}]$ as follows:

$$MF_{tot}[V_{BAL}] = MF + \frac{C_{add}[V_{BAL}]}{\min(C_{true}, C_{false})} \tag{5}$$

where MF is the nominal mismatch factor defined in Eq. (2).

In this way, it is possible to emulate four mismatch conditions, according to the 2-bit word V_{BAL} value, allowing to

TABLE VI
COMPARISON OF THE SABL AND IDDPL IMPLEMENTATIONS

	No. of Transistors	Area Overhead	Active Area [μm^2]	P_{AVG}@1MHz [μW]	Max f_{CK} [MHz]
CMOS	564	x1.0	n.a.	n.a.	n.a.
SABL	1538	x2.7	1703	2.33	215
iDDPL	1983	x3.5	2323	3.61	380

analyze and fairly compare the performance of SABL and iDDPL in the presence of mismatch in a real attack scenario. It has to be noted that, if $V_{BAL} = 00$, a residual of mismatch is still present on both cores, due to unavoidable non-perfectly symmetric routing. *MF* has been estimated to be under 1.5 for the S-BOX, and under 2.20 for the output register.

A comparison between the SABL and iDDPL cores in terms of area, power consumption and maximum allowed clock frequency is reported in Table VI showing that the iDDPL implementation requires more area and power consumption than the SABL one. It has to be pointed out also that the maximum clock frequency supported by the iDDPL core is higher than the SABL counterpart. The absence of the foot-transistor in iDDPL cells allows to shorten the path towards to ground, achieving a faster switching and thus relaxing the constraints of minimum clock period.

A. Generation of δ

The generation of δ requires the presence of two clock signals: a nominal clock *CK*, and a δ-shifted replica of the nominal clock *CKD*. A priori, one can design the architecture of the cryptographic processor to route two clock signals, skewed exactly of δ, but this solution requires a careful generation of two clock trees, that must be consistent for the sake of TEL behavior. Moreover, in some cases, the area/power overhead due to doubling the clock tree can be not compliant with some physical constraints or requirements. Another simple solution is to implement a delay line using the propagation delay of a chain of inverters. This solution suffers from a high dependency of the propagation time of the single inverter cell from the power supply voltage and from the working temperature of the device, making it not suitable for security applications. Moreover, it requires a large number of inverter stages to achieve a reasonable δ value in the order of hundreds of picoseconds in nowadays technologies. In ASIC implementations, another possible solution to generate longer delay is to use the linear current starved delay element proposed in [25]. The delay element is implemented using a starved inverter circuit with linearized biasing scheme.

In this design, a starved inverter in which the control voltage V_{CTRL} is applied only to the upper p-channel transistor has been used to generate the nominal δ for the iDDPL implementation. The tuning range of the δ value according to an external bias voltage V_{CTRL} has been designed to be from about 150ps to 2ns. This solution avoids the presence of long chains of inverters or doubling the *place&route* of a second low skew clock tree. In fact, the generation of the *CKD* is derived locally at each TEL-regenerative interface (CMOS-to-TEL converters and flip-flops), and thus, only the DC signal V_{CTRL} has been routed, allowing a reduction of area and power overhead. To guarantee a δ value which is stable under PVT variation a delay locked loop can be used to generate the control voltage V_{CTRL}.

V. EXPERIMENTAL VALIDATION OF THE TEL SECURE LIBRARY

The analysis of a secure implementation has to cope with the physical evaluation after the manufacturing of the chip. The post-silicon verification is one of the most critical phases in the assessment of the information leakage that can be exploited to recover sensible data. Simulations are able to provide useful information on potential source of exploitable leakage, as, nowadays, the modeling of circuits in pre and post layout are very accurate compared to the past. However, some unwanted effects, due to fabrication process, can threaten the physical security of the device and may not be evident in simulations [27]. Hence, a measurement campaign on the real chip (attacks and leakage assessment) should be conducted to verify if security requirements are met [26].

A. Measurement Setup

The measurement setup adopted to carry out the security evaluations is based on the testchip mounted on a custom designed printed circuit board, containing also all the support circuitry, such as level-shifters and step-down linear power regulators. The testchip board is connected to a personal computer via a FPGA board (Altera Cyclone-II), implementing the UART interface and all the discussed control functions of the SERPENT cores. The core supply voltage has been set to 1.2V according to foundry specifications for nominal voltage of the CMOS065 technology. We have set the external V_{CTRL} to 0.75V to guarantees a value of δ of about 1ns in the iDDPL core. Both cores have been tested with a running frequency of 1MHz, using a LeCroy WaveSurfer MX-104B DSO with a sampling rate of 5GS/s and full analog-bandwidth (1GHz). A Tektronix-CT1 inductive probe has been used to sense the current absorption of the secure part of the architecture in Figure 6. The 4-bit key has been set, without loss of generality, to $(7)_2$ on both cores. Current traces of the SABL and iDDPL crypto-cores are shown in Figure 9. It has to be noted that the current trace collected on the SABL implementation appears smoother than the respective iDDPL counterpart. In iDDPL implementation, the current trace appears more "ringing" as can be seen in Figure 9. Higher frequency effects are expected in TEL-compatible implementations since the evaluation phase has a very short duration compared to the clock period.

B. Security Metrics

1) Signal to Noise Ratio (SNR): The SNR [3] in the context of PAAs is defined as follows:

$$SNR = \frac{\sigma^2_{data}[j]}{\sigma^2_{noise}[j]} \tag{6}$$

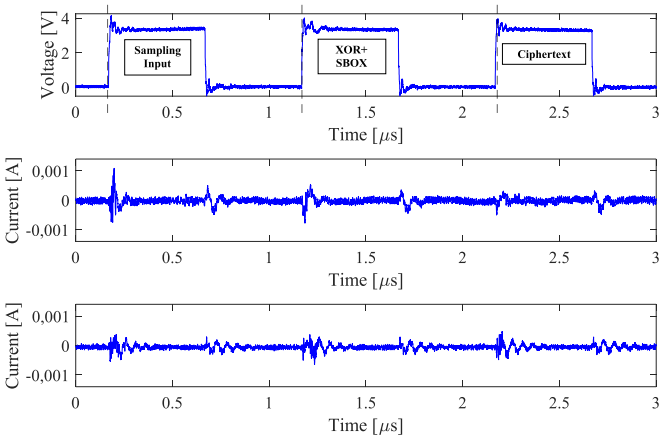

Fig. 9. Time diagram of the encryption in SABL/iDDPL cores: clock signal (top), SABL current absorption (middle), iDDPL current absorption (bottom).

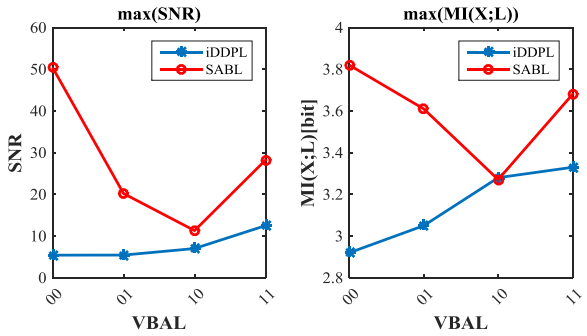

Fig. 10. Peak values of SNR (left) and mutual information (right) regarding VBAL configurations. Maximum leaky points (and in this case points which give maximum SNR and MI) in time are around the rising edge of clock at the third cycle (~2.15ns) in Figure 9.

where $\sigma^2_{data}[j]$ represents the variance of the data-dependent part of the power consumption for the j-th sample in a power trace, and $\sigma^2_{noise}[j]$ represents the variance of the noisy component in the overall power consumption.

Regarding maximum SNR values shown in Figure 10, the iDDPL implementation exhibits a positive monotonic behavior with the increasing of C_{add}, moving from 5.43 to 12.51, as expected. In SABL implementation, SNR peak values are always higher than iDDPL counterpart. In particular, setting $V_{BAL} = 00$, the SNR is 50.41 for the SABL implementation, which is one order of magnitude higher than the iDDPL one. It is worth noting that a minimum of the SNR value can be observed setting $V_{BAL} = 10$, that corresponds to $C_{add} = 6.4$fF. A possible explanation for the presence of a minimum for $V_{BAL} = 10$ is the unavoidable mismatch in the SABL implementation which is balanced for a certain value of C_{add}. However, for all settings of V_{BAL}, SABL implementation exhibits higher values of SNR, remarking the relevance of capacitive mismatch in determining the level of security for DPLs adopting RTZ signaling.

2) Mutual Information (MI): Introduced in [28], the MI quantifies the amount of information leaked by a hardware implementation of a cryptographic algorithm. It is able to quantify the information leaked by the crypto core using the

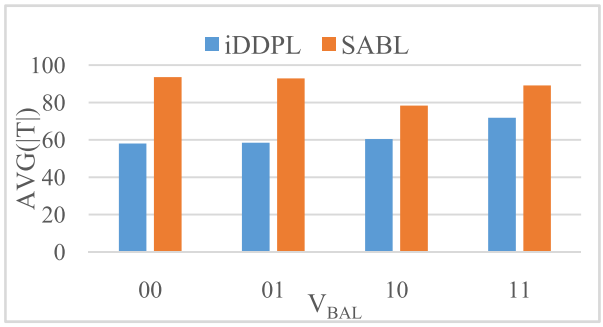

Fig. 11. Average absolute values of the T-test as a function of V_{BAL} adopting all the possible input value as "fixed class".

conditional entropy, by means of probability density functions (PDFs), assuming a Gaussian distribution for the power samples and can be expressed as follows:

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

where X is the secret variable (e.g. the secret key), $H[X]$ its entropy, $Pr(x)$ the probability of $x \in X$ and L is the observed leakage. The probability $Pr_{chip}(x|l)$ is derived from $Pr_{chip}(l|x)$ by means of Bayes' theorem. The underlying assumption is based on the fact that the adversary (the evaluator in this case) has a perfect knowledge of the distribution $Pr_{chip}(x|l)$. Therefore, the MI represents the upper-bound of the amount of information that can be extracted from a hardware implementation.

Similarly to SNR, peak values of mutual information in Figure 10 have been found higher in SABL implementation compared to iDDPL. Setting $V_{BAL} = 00$, the estimated mutual information for SABL core is 3.82bit, while for the iDDPL is 2.92bit. The spread between the two implementations of the 4-bit SERPENT-based crypto-core remains higher, but, also in this case, a minimum of SABL's mutual information value can be found at $V_{BAL} = 10$. At this value (which reasonably correspond to the best matched condition for the SABL core), the mutual information values for the two implementations are very similar to each other.

3) Test Vector Leakage Assessment (TVLA): TVLA has been introduced in [29] as a security metric whose results may highlight the amount of information that leaks from a cryptographic implementation. The theory behind this metric does not depend on any specific power model.

We performed the TVLA evaluation using the approach suggested in [29] on both iDDPL and SABL implementations for different load unbalance conditions and results are reported in Figure 11. We obtained that again the T-test statistic on the SABL returns a higher value compared to the iDDPL counterpart. This result is perfectly in accordance with the SNR plot in Figure 10, where the aforementioned tests have been performed for each mismatch configuration.

4) Frequency Energy Deviation (FED): In [11], Bongiovanni *et al.* have introduced new criteria for assessment

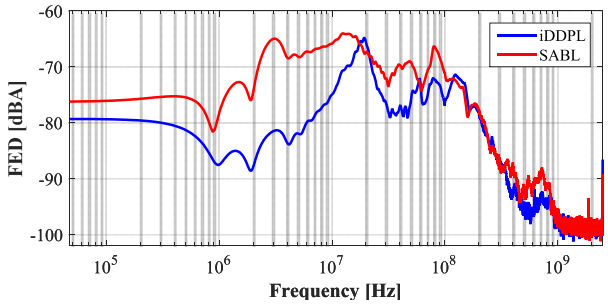

Fig. 12. Plot of the FED security metrics for iDDPL (blue) and SABL (red), for $V_{\mathrm{BAL}} = 11$.

TABLE VII

SUMMARY OF RESULTS OF THE CPA ATTACKS ON IDDPL AND SABL IMPLEMENTATION OF THE SERPENT-BASED CRYPTO-CORES

	V_{BAL}	C_{add}	$\max\{\rho_{corr}\}$	SVI	$SVI_{\%}$	MTD
iDDPL	00	0fF	0.503	-0.015	-2.97%	> 50k
	01	3.2fF	0.478	-0.041	-7.84%	> 50k
	10	6.4fF	0.306	-0.052	-14.60%	> 50k
	11	9.6fF	0.496	-0.108	-17.88%	> 50k
SABL	00	0fF	0.389	+0.057	+14.66%	40
	01	3.2fF	0.415	+0.071	+17.04%	130
	10	6.4fF	0.113	-0.089	-78.78%	>50k
	11	9.6fF	0.423	+0.040	+9.51%	670

of the information leakage in the frequency domain. We adopt the FED as an estimation of the power variability due to data-dependency in the frequency domain. Relying on the computation of the Fast-Fourier Transform (FFT) on power traces, the FED for N input vectors defined as in [11] represents the variance in the frequency domain of the information leaked through the power consumption side channel.

In the evaluation (and especially in the design) of a hardware implementation of a cryptographic primitive, assumptions on the bandwidth that the adversary can practically exploit to mount the attack should be considered.

To achieve an high level of security, the FED should be bounded by the (hypothesized) frequency response of the adversary's measurement chain.

The *FED* of the iDDPL (in blue) and SABL (in red) as a function of frequency is reported in Figure 12 for $\mathrm{V_{BAL}} = 11$. At low-frequencies (e. .g. below 1MHz), the *FED* for the iDDPL core tends to be about 4/5 dB lower than SABL implementation, showing the effectiveness of the TEL encoding. At high-frequencies (e. g. above 1MHz), the difference in the *FED* values for the two implementations becomes even more evident. In fact, at 3MHz the iDDPL core shows a *FED* value which is about 16dB lower than the SABL one.

This is a crucial result, because, a "conventional" real-world adversary will cut-off frequencies above four/five times the clock frequency to achieve better SNR [3]. So far, the reduction of the *FED* in this zone is remarkably important to protect cryptographic cores from malicious attackers, and it highlights the capability of the TEL signaling to tolerate unbalancing in load capacitors better than RTZ encoding.

As expected by [11], the high-frequency behavior of the iDDPL due to TEL encoding is perfectly visible in Figure 12, where a positive ramp of the FED around approximately 6MHz can be observed for the iDDPL implementation. It has to be pointed out that these results can be even enforced when implementing more complex crypto cores, since the algorithmic noise tends to push down all the values, and to flatten the *FED* curves, due to higher parasitic capacitance on V_{DD} lines.

As reported in [11], the *FED* analysis can be used to properly design the power supply network on-chip, by means of adding additional capacitance, in order to flatten the positive ramp, and thus, increasing the level of security. It has to be noticed that in this design, no additional capacitance on V_{DD} line has been added to allow the accurate evaluation of this effect.

C. CPA Attacks

The iDDPL and SABL implementation have then been attacked using Correlation Power Analysis (CPA) [30] adopting the Hamming Weight power model. We have chosen the output word of the SBOX as target function for the CPA attack:

$$out = S_0(plaintext \oplus key) \tag{8}$$

We have adopted also the *Success Value Indicator* (*SVI*), introduced in [31], and defined as follows for CPA attacks:

$$SVI = \max\{|\rho_{corr}|\} - \max|\rho_{wrong}|\} \tag{9}$$

where $\max\{|\rho_{\mathrm{corr}}|\}$ is the maximum value of the correct key's correlation coefficient and $\max\{|\rho_{\mathrm{wrong}}|\}$ is the highest value of the correlation coefficients corresponding to the best ranked wrong key. The *SVI* provides a useful tool to evaluate how the correct key can be distinguished from wrong keys. To enforce this aspect, we introduce also the *normalized SVI* ($SVI_{\%}$), defined as follows:

$$SVI_{\%} = \frac{SVI}{\max\left\{|\rho_{corr}|, |\rho_{wrong}|\right\}} \tag{10}$$

Figure 13 and Figure 14 show the correlation coefficient and the Measurement to Disclosure (*MTD*), (defined as the minimum number of measurements needed to recover the secret key [32]), computed during the CPA attack on the iDDPL and SABL cores. Results of CPA attacks for all possible configurations of V_{BAL} are summarized in Table VII. The iDDPL implementation exhibited an extreme resistance to multi-bit attack, and in all mismatch cases, it was not possible to recover the secret key.

In fact, the *MTD* resulted to be higher than 50k in all cases. Despite high values of correct key's correlation coefficient, the value of $SVI_{\%}$ tends to increase with C_{add}, remarking that the correct key tends to be hidden in the "bulk" even in the presence of mismatch. Regarding the SABL implementation, the CPA is not effective in recovering the correct key only with $V_{BAL} = 10$, in agreement with the SNR and mutual information analysis mentioned previously. For all the remaining configurations of V_{BAL}, the CPA attack was able to recover the secret key with a very small number of traces (from 40 to 670).

Without loss of generality, we have presented the results obtained for key '6', which resulted the easiest to attack for

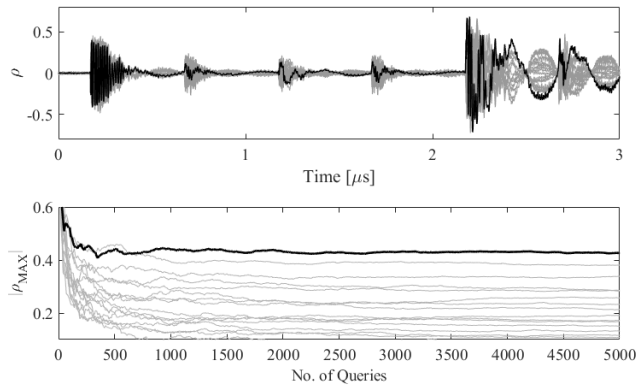

Fig. 13. Plots of the CPA attack on SABL implementation. Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

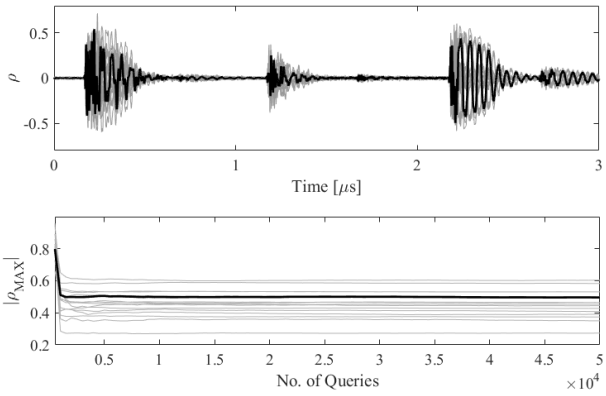

Fig. 14. Plots of the CPA attack on iDDPL implementation. Top figure shows the correlation coefficient ρ vs. current traces time samples. Bottom figure shows the MTD diagram. The black solid line represents the correlation coefficient of the correct key. Grey lines are referred to the correlation coefficient of wrong keys.

the SABL core. Similar results have been obtained for all the 16 possible keys.

VI. Conclusion

In this paper we have presented experimental results on a secure cells library based on the iDDPL logic style exploiting the TEL encoding and implemented in a 65nm CMOS technology. The developed library allowed adopting a semi-custom design flow (automatic place and route) without any constraint on the routing of the complementary wires.

A four bit lightweight crypto core has been implemented on a 65nm CMOS test-chip by using the developed TEL library and compared against a SABL implementation of the same crypto core on the same chip.

A measurement campaign on the test chip allowed to evaluate a set of security metrics and to quantify the improvement of the proposed approach with respect to the SABL implementation. In particular a reduction of *SNR* from 50.41 to 12.51 and of MI from 3.8 to 3.3 in the worst case mismatch conditions have been measured.

TABLE VIII

Comparison Against the State of the Art in Terms of Area/Power Overhead and Tolerance to Mismatch in the Routing of Complementary Wires

	Area Overhead	Power Overhead	Platform	Protocol	Routing Mismatch Tolerant
CMOS	x1	x1	FPGA/ASIC	-	-
WDDL	X3.1	X3.7	FPGA/ASIC	RTZ	NO
MDPL	X4-5	X3-7	FPGA/ASIC	RTZ	NO
SABL	X2.7	X3.3	ASIC	RTZ	NO
iDDPL	X3.5	X4.4	ASIC	TEL	YES

The evaluation of the *FED* on the two implementations highlighted a reduction of about 16dB at three times the clock frequency for the iDDPL with respect to SABL.

CPA attacks on the measured current traces have shown an improvement in *MTD* of about two to three orders of magnitude with respect to the state of the art in all the considered mismatch conditions.

This improvement in terms of robustness to PAAs has been achieved with an overhead with respect to SABL in terms of silicon area and power consumption of a factor of 1.4 and 1.5 respectively.

A comparison of different state of the art secure logic styles is reported in Table VIII. Table VIII shows that the proposed approach is the only one able to guarantee tolerance with respect to the routing unbalance of complementary wires thus allowing a standard semi-custom design flow for DRP logics without the routing matching optimization step. The area and power consumption overhead of iDDPL is in line with the other secure logic styles.

Acknowledgment

Authors would like to thank the UCL Welcome Lab for the support and assistance.

References

[1] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1996, pp. 104–113.

[2] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1999, pp. 388–397.

[3] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, 2008.

[4] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Design, Automat. Test Eur. Conf. Expo. (DATE)*, 2004, pp. 246–251.

[5] 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*, Sep. 2002, pp. 403–406.

[6] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *Proc. CHES*, Edinburgh, U.K., in Lecture Notes in Computer Science, vol. 3659. Springer, Sep. 2005, pp. 172–186.

[7] K. Tiri and I. Verbauwhede, "Place and route for secure standard cell design," in *Proc. Smart Card Res. Adv. Appl. IFIP Conf. (CARDIS)*, 2004, pp. 143–158.

[8] S. Guilley, P. Hoogvorst, Y. Mathieu, and R. Pacalet, *The 'Backend Duplication' Method*. Berlin, Germany: Springer, 2005, pp. 383–397.

[9] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, in Lecture Notes in Computer Science, vol. 4249. Springer-Verlag, 2006, pp. 232–241.
[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, Jul. 2011.
[11] S. Bongiovanni, F. Centurelli, G. Scotti, and A. Trifiletti, "Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks," *J. Cryptograph. Eng.*, vol. 5, no. 4, pp. 269–288, Apr. 2015.
[12] K. J. Kulikowski, M. G. Karpovsky, and A. Taubin, "Power attacks on secure hardware based on early propagation of data," in *Proc. IOLTS*, vol. 6, Jun. 2006, pp. 131–138.
[13] M. Saeki and D. Suzuki, "Security evaluations of MRSL and DRSL considering signal delays," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 91, no. 1, pp. 176–183, 2008.
[14] S. Bhasin, S. Guilley, F. Flament, N. Selmane, and J. L. Danger, "Countering early evaluation: An approach towards robust dual-rail precharge logic," in *Proc. 5th Workshop Embedded Syst. Secur.*, Oct. 2010, Art. no. 6.
[15] A. Moradi and V. Immler, "Early propagation and imbalanced routing, how to diminish in FPGAs," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)* in (Lecture Notes in Computer Science), vol. 8731. Berlin, Germany: Springer, 2014, pp. 598–615.
[16] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, "DPA-secured quasi-adiabatic logic (SQAL) for low-power passive RFID tags employing s-Boxes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 1, pp. 149–156, Jan. 2015.
[17] K. Tiri and I. Verbauwhede, "Design method for constant power consumption of differential logic circuits," in *Proc. Design Automat. Test Eur. (DATE)*, 2005, pp. 628–633.
[18] S. Bongiovanni, M. Olivieri, G. Scotti, and A. Trifiletti, "A power-balanced sequential element for the delay-based dual-rail precharge logic style," *Int. J. Microelectron. Comput. Sci.*, vol. 4, no. 4, p. 129, 2013.
[19] D. Bellizia, G. Scotti, and A. Trifiletti, "Secure implementation of TEL-compatible flip-flops using a standard-cell approach," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2018, pp. 1–5.
[20] K. Tiri and I. Verbauwhede, "Place and route for secure standard cell design," in *Smart Card Research and Advanced Applications VI. IFIP International Federation for Information Processing*, vol. 153, J. J. Quisquater, P. Paradinas, Y. Deswarte, and A. A. El Kalam, Eds. Boston, MA, USA: Springer, 2004.
[21] S. Guilley, P. Hoogvorst, Y. Mathieu, and R. Pacalet, "The back-end duplication method," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 3659, J. R. Rao and B. Sunar, Eds. Berlin, Germany: Springer, 2005.
[22] K. Baddam and M. Zwolinski, "Divided backend duplication methodology for balanced dual rail routing," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 5154, E. Oswald and P. Rohatgi, Eds. Berlin, Germany: Springer, 2008.
[23] E. Biham, R. Anderson, and L. Knudsen, "Serpent: A new block cipher proposal," in *Proc. 5th Int. Workshop Fast Softw. Encryption*, 1998, pp. 222–238.
[24] D. Bellizia, S. Bongiovanni, P. Monsurrò, G. Scotti, A. Trifiletti, and F. B. Trotta, "Secure double rate registers as an RTL countermeasure against power analysis attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 7, pp. 1368–1376, Jul. 2018, doi: 10.1109/TVLSI.2018.2816914.
[25] G. S. Jovanović and M. Stojčev, "Linear current starved delay element," in *Proc. ICEST*, 2005, pp. 1–4.
[26] T. Schneider and A. Moradi, "Leakage assessment methodology—A clear roadmap for side-channel evaluations," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 9293. Berlin, Germany: Springer, 2015, pp. 495–513.
[27] D. Kamel, M. Renauld, D. Flandre, and F.-X. Standaert, "Understanding the limitations and improving the relevance of SPICE simulations in side-channel security evaluations," *J. Cryptograph. Eng.*, vol. 4, no. 3, pp. 187–195, 2014.
[28] F. MacÃ©, F.-X. Standaert, and J.-J. Quisquater, *Information Theoretic Evaluation of Side-Channel Resistant Logic Styles*. Berlin, Germany: Springer, 2007, pp. 427–442.
[29] J. Cooper, E. De Mulder, G. Goodwill, J. Jaffe, G. Kenworthy, and P. Rohatgi, "Test vector leakage assessment (TVLA) methodology in practice," in *Proc. Int. Cryptograph. Module Conf.*, 2013. [Online]. Available: http://icmc-2013.org/wp/wp-content/uploads/2013/09/goodwillkenworthtestvector.pdf
[30] E. Brier, C. Clavier, and F. Olivier, *Correlation Power Analysis With a Leakage Model*. Berlin, Germany: Springer, 2004, pp. 16–29.
[31] 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.
[32] K. Tiri *et al.*, "Prototype IC with WDDL and differential routing—DPA resistance assessment," in *Proc. CHES*, 2005, pp. 354–365.

Davide Bellizia was born in 1989. He received the M.D. degree *(summa cum laude)* in electronic design and the Ph.D. degree in electronics engineering from the University of Rome La Sapienza, Italy, in 2014 and 2018, respectively. In 2017, he joined the Crypto Group, Université Catholique de Louvain, Louvain-la-Neuve, Belgium, as a Post-Doctoral Researcher. His research interests include the design of cryptographic ICs for counteracting power analysis attacks, and VLSI design for DSP algorithm implementations. In 2014, he received the Laureato Eccellente Award for the best graduate student of the year.

Giuseppe Scotti was born in Cagliari, Italy, in 1975. He received the M.S. and Ph.D. degrees in electronic engineering from the Sapienza Università di Roma, Rome, Italy, in 1999 and 2003, respectively. In 2010, he became a Researcher (Assistant Professor) with the DIET Department, Sapienza Università di Roma, where he was appointed as an Associate Professor in 2015. He teaches undergraduate and graduate courses on basic electronics and microelectronics. 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 over 45 publications in international Journals, about 70 contributions in conference proceedings, and is the co-inventor of two international patents. His research activity was mainly concerned with integrated circuits design and focused on design methodologies able to guarantee robustness with respect to parameter variations in both analog circuits and digital VLSI circuits. In the context of analog design his research activity was concerned with circuit topologies for the realization of low-voltage analog building blocks using ultra-short channel CMOS technology, whereas in the context of cryptographic hardware his focus has been on novel PAAs methodologies and countermeasures.

Alessandro Trifiletti was born in Rome, Italy, in 1959. He received the Laurea degree in electronic engineering from the Sapienza Università di Roma. In 1991, he joined the Dipartimento di Ingegneria Elettronica, Sapienza Università di Roma, as a Research Assistant where he is currently a Full Professor. His research interests include high-speed circuit design techniques and cryptographic hardware.