J Cryptogr Eng (2015) 5:269–288
DOI 10.1007/s13389-015-0096-z

REGULAR PAPER

Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks

Simone Bongiovanni[1] · **Francesco Centurelli**[1] · **Giuseppe Scotti**[1] · **Alessandro Trifiletti**[1]

Received: 6 September 2014 / Accepted: 21 March 2015 / Published online: 4 April 2015

Abstract Electrical and capacitive mismatches are outstanding issues in modern submicron technologies, and must be considered already during the design steps. In this work, we propose a novel hardware countermeasure based on the combination of a circuit- and a system-level methodology, which helps to reduce the data dependence of the instantaneous power consumption of cryptographic circuits. Accordingly, we define a specific design methodology, which is based on a novel data encoding and on the insertion of an on-chip filter implemented through capacitances in the layout. The new countermeasure, called *time-enclosed logic* (*TEL*), is able to hide the data dependence in a very short time interval (in the order of 100 ps in modern submicron technologies), constraining the minimum amount of bandwidth required from the attack setup. As a second and parallel contribution, we present a novel design time metric for validating our design, named *frequency energy deviation*, which is based on the investigation of the deviation of the frequency patterns of the current traces. By simulating a basic cell template under unbalanced capacitive condition, we show that standard *dual-rail precharge logics* exhibit a resilient leakage already at lower frequencies, whereas in TEL circuits the data dependence is shifted toward high frequencies. As a case study, we designed a TEL-featured cryptographic circuit using a 65-nm technology node, without any assumption on the routing of the logic gates. *Correlation power analysis* attacks with a Gaussian model have been then mounted against the circuit. Simulation results show that the proposed countermeasure can help to mitigate the electrical mismatches occurring in submicron technologies, offering a promising perspective for the design of power analysis resistant circuits.

Keywords Side-channel attacks · Correlation power analysis · Decoupling capacitor · Fast Fourier transform · Serpent S-Box · VLSI

1 Introduction

Side-channel attacks (*SCAs*) [1] are a serious threat for the security of cryptographic circuits, because they aim at extracting information (e.g. the key of a cryptographic algorithm) by exploiting the unintentional physical emissions of the device (e.g. power, electromagnetic field, light, etc.) without leaving any trace of their activity. *Power analysis attacks* (*PAA*) [2,3] represent one of the most effective and dangerous SCAs, because they are simple to be performed in practical applications and relatively low cost. For many years, the hardware cryptography community intensified efforts toward the development of novel countermeasures for balancing the switching activity of digital logic circuits, both on system and circuit level, to break any correlation between data and power. Decoupling [4,5], shuffling [6], shielding [7], de-synchronization [8,9], randomization [10], and noise insertion [2,11] are examples of system-level hardware. Among them, decoupling has been one of the first countermeasures to be adopted since PAAs were discovered. A decoupling capacitor acts as an intermediate storage element which filters out the high-frequency noise components superimposed on the supply voltage. Therefore, the presence

Electronic supplementary material The online version of this article (doi:10.1007/s13389-015-0096-z) contains supplementary material, which is available to authorized users.

✉ Simone Bongiovanni
bongiovanni@die.uniroma1.it

[1] Department of Information, Electrical and Telecommunication Engineering, University of Rome "La Sapienza", Rome, Italy

of some capacitance on the power supply line of an integrated circuit is mandatory to guarantee the correct functionality, and each EDA tool provides insertion of some decoupling capacitors during the back-end design flow. In literature, there are examples of failed PAAs mounted against cryptographic cores which are implemented on off-chip filtered boards, as for example in [4]. This led to the wrong belief that decoupling capacitance represents an intrinsic design methodology to protect a chip from PAAs, as concluded in [4]. On the contrary, more recent works proved that off-chip decoupling capacitances represent an unintentional source of leakage which can be efficiently exploited by an attacker, not only in PAAs [12] but also in an *electromagnetic analysis attacks* (*EMA*) [13] scenario.

Indeed, since PAAs are based on monitoring the switching transitions at the power supply line, the presence of decoupling capacitors can be a first effective countermeasure against PAAs provided that the attacker is prevented to measure the power consumption in the point between the capacitance and the internal pins of the chip; otherwise, he/she has still the possibility to detect the information leakage in the current traces, by exploiting for example the energy exchanged among the chip peripheral impedance at the resonance frequencies. Thus, to better exploit the properties of decoupling capacitors as countermeasure against PAAs, with the adoption of ever more scaled technologies new countermeasures which adopt on-chip rather than off-chip decoupling capacitors were presented [14–16].

Hardware countermeasures can be also implemented at circuit level. Basically these countermeasures are based on the duplication of the signal through a differential design and the insertion of redundant circuitry in the logic gates. *Dual-rail precharge logic* (*DPL*) styles are an outstanding example. The implementation of new specific DPL styles as *SABL* [17], *TDPL* [18], and *DDPL* [19] offers an enhanced level of security, at the expenses of an increased overhead of area occupation and power consumption. Furthermore, these architectures involve changes in the standard digital design flow, leading to a customized design which unavoidably enhances cost and time requirements. Other DPL styles are based on the compound of static CMOS gates, as *WDDL* [20] and *MDPL* [21]; they can be integrated in a standard digital flow, but have the drawback of being extremely sensitive to the electrical mismatches [17].

However, the trend of technology scaling in modern electronic circuits leads to novel subtle leakage sources with which a designer has to deal: for example, the electrical mismatches of the signals propagating inside the electronic circuit reveal a data dependence that cannot be detected by earlier power models. Today, capacitive [22] and timing [23,24] mismatches represent challenging issues to face already during the design steps of cryptographic circuits in modern submicron technologies. Several works were published where these leakage sources have been successfully exploited for stealing information from a device [23,25,26], as well as novel mitigation techniques have been presented. For example, some back-end optimization techniques have been proposed for overcoming capacitive mismatches [22,27,28]; these techniques have the advantage of being adoptable in combination with other previously published as well as novel countermeasures. Anyway, obtaining a perfect balance during the hardware design through a layout optimization is a very hard-working task which very often leads to imprecise results. Besides the electrical mismatches, the static consumption is another preeminent issue in the design of secure circuit with modern submicron technologies. The dependence of the static power consumption on the input data in sub-100nm CMOS technologies has been proved through extensive simulations for different case studies in [29]; then, *leakage-based differential power analysis* (*LDPA*) [30] and *leakage power analysis* (*LPA*) [31] have been proposed as well-defined analytical attack methodologies in a similar way as standard DPA and CPA were introduced for the case of the dynamic power. Further improvements and theoretical considerations on static power attacks against real cryptographic circuits have been then executed [32,33], so that the side-channel emission due to the static power consumption has been finally acknowledged by the SCA community as a real danger also in practical applications.

The above-discussed issues prove that several earlier countermeasures against PAAs revealed to be suboptimal, having been designed on the basis of inaccurate models, and the level of security they offered was only apparent. A parallel issue for hardware cryptographic designers is to determine a useful metric for evaluating the level of actual security of a circuit during the design phases. Among the possible implementations, integrated circuits designed for specific applications (ASIC) are the hardest to be validated in terms of SCA resistance: once a chip has been fabricated, it is actually impossible to patch any kind of vulnerability, and thus a more precise way for defining the weaknesses of the device already at simulation level must be adequately defined. Therefore, extensive tests of a prototype chip must be performed before the tape-out, to provide an effective validation of the security margin of the device.

2 Main contribution and methodology used in this work

Our work provides two different contributions with respect to the state-of-the-art. As a first contribution, we propose a countermeasure against PAA based on the combination of a logic-level and a system-level methodology, which helps to reduce the dependence of the instantaneous power consumption of a crypto-circuit on the processed data, even

when the electrical mismatches due to the internal capacitive unbalances of the interconnect wires are taken into account. Accordingly, we define a novel data encoding which implements the paradigm of hiding information in the time domain; in combination to the new logic protocol, we propose a design methodology based on the insertion of an on-chip filter which aims at eliminating the high-frequency components due to the electrical mismatches. The purpose of the new countermeasure is to give a two-dimensional protection against PAAs by guaranteeing that the pattern of the instantaneous current traces of a cryptographic circuit is always flattened. As a second contribution, we define a novel design time metric based on the analysis of the energy distribution of the current traces in the frequency domain with the aim of investigating the physical leakage emitted by the circuit already during the design steps. By estimating the energy deviation at each frequency sample, it is possible to assess the amount of internal capacitance needed for implementing the on-chip filter and ultimate the design. All the experiments presented in this work have been done with SPICE-level simulations performed in Cadence environment. Electrical schemes were designed using low power standard voltage threshold transistors from the 65 nm-CMOS technology library provided by STMicroelectronics. The advantage of using SPICE simulations is to provide the designer with a fine-grain analysis of the leakage, which allows a very accurate estimation of the power consumption profile with a fine timescale; furthermore, the collected traces are noise-free and perfectly aligned, which is actually impossible in practical measurements, but in our validation this usefully provides a conservative approach for validating the circuit implementation. Anyway, it must be pointed out that SPICE-level simulations are really meaningful if an adequate testbench which comprises also peripherals circuitry is taken into account, as discussed in [34].

With the aim of considering the worst-case scenario for validating the level of security of an implementation through PAAs, we consider the model of perfect attacker defined in [35], which is in accordance to the precision provided by the simulated noise-free traces exported by Cadence. Following this model, the assumptions we do are the following: (1) the attacker has full knowledge of the data path of the circuit; (2) the attacker can build an accurate power model of the leakage by knowing the power characteristics of the DPLs circuit and the exact instants in which leakage samples occur inside a clock cycle; (3) the attacker can profile the power consumption of the circuit using an unbounded profiling phase, which in simulation means collecting the noise-free traces corresponding to each possible input.

The strategy of considering a profiled acquisition phase corresponds to the situation in which the attacker owns a clone of the target device and builds a template of the device itself. The only hypothesis we do is on the bandwidth of the measurement setup. We started our work by an observation: if a cryptographic device can be characterized through its power traces, the device cannot be considered secure any more, since an attacker can always model the power consumption of the device and build power templates to extract information at any time instant. A perfect attacker is guessed to have unbounded sources in terms of time, bandwidth, and memory for performing an attack. The only hypothesis we do in our work is to relax the constraints on the bandwidth of the acquisition.

The effectiveness of the countermeasure we present in this work is based on the hypothesis that in practical applications the attacker has a measurement setup with a limited resolution [36]; therefore, if the observable leakage is hided in the time domain beyond the time resolution of an oscilloscope, the acquisition fails at collecting relevant time samples and no leakage can be detected, irrespective of the strength of the statistical distinguisher. After having validated the data dependence of the power consumption of a case study cryptographic circuit using the above-described attack model, we perform more realistic *correlation power analysis* (*CPA*) attacks [3] based on the Hamming Weight model, using the Gaussian model for the superimposed noise [37], which is in accordance to the formalized analysis done in [38] and the simulation methodology applied in [39] for the case of nanoscaled chips.

The paper is structured as follows: in Sect. 3 the fundamentals of a novel data encoding are described. In Sect. 4 we define a new metric based on the calculation of the *fast Fourier transform* (*FFT*) of the current traces. Then, in Sect. 5 a case study cryptographic circuit is designed. Simulations are presented in Sect. 6, where CPA attacks are executed. Finally, a discussion on the possibility to extend this countermeasure also to thwart EMA attacks is provided in Sect. 7, and the conclusions to this work are discussed in Sect. 8.

3 Description of time-enclosed logic circuits

3.1 Signal convention in DPL styles

Dual-rail precharge logic (*DPL*) [36] is a family of circuits with two basic properties: the information is encoded using two differential wires; the clock period is divided into a *precharge* and an *evaluation* phase. DPLs have been widely adopted as a countermeasure against PAAs thanks to their property of balancing the dynamic power consumption by guaranteeing that the switching factor of a logic gate is always 1. The *return to zero* (*RTZ*) logic circuits are a special class of DPLs widely used in the context of cryptography; in the RTZ data encoding both differential signals are reset to the minimum voltage supply (0 V) during the precharge, and

Table 1 Description of the data encoding for the new cryptographic logic family

Voltage						New logic domain	CMOS mapping
Discharge		Evaluation		Postcharge			
A	$\bar{A}$	A	$\bar{A}$	A	$\bar{A}$	$(A, \bar{A})$	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

only one of them evaluates V_{DD} according to the bit to be processed. In this kind of logics, the clock of the circuit is routed into the flip-flops as well as the combinational gates, and the data path is doubled. An interface circuit is provided to convert the single-rail (SR) signal from the CMOS circuit section into the dual-rail (DR) domain. The processed differential signals are represented using the formalism $(A, \bar{A})$. The data encoding is done in the voltage domain, according to which line is charged, and each wire stays at a voltage (0 or V_{DD}) for a period equal to $\frac{T_{CK}}{2}$: if $(A, \bar{A}) = (1, 0)$, wire A is charged at V_{DD} and a bit-1 is processed; on the contrary, if $(A, \bar{A}) = (0, 1)$ the processed bit is 0. The time interval $\frac{T_{CK}}{2}$ represents the relevant period of the data encoding, that is, the interval of time in which the information is visible and can be potentially detected by an attacker.

3.2 Basic principle of TEL circuits

Time-enclosed logic (*TEL*) circuits adopt a different methodology for encoding a bit: the SR signal is converted into a differential signal pair so that, after the precharge phase, one of them is again charged at V_{DD}, whereas the other wire stays at 0; but after a short time interval δ, the latter is also charged to V_{DD}. This data encoding is done in the time domain, because the voltages on the differential wires differ only during the time interval δ, which represents the relevant period of the new logic, unlike RTZ logics in which the relevant period is $\frac{T_{CK}}{2}$. In a time-domain data encoding, there are three possible states for a differential pair $(A, \bar{A})$: the discharge phase, in which both wires are at the precharge value 0; the evaluation phase, in which one line is at V_{DD} and the other stays at 0; the postcharge phase, in which both the lines are at the voltage V_{DD}. The data encoding scheme is represented in Table 1.

The time-domain data encoding has been introduced in [18] and studied in [40]. On the basis of the above-defined data protocol, a bit is encoded according to the order in which the differential signals are charged during the evaluation phase; there are three possible situations for the differential time diagram: if rail A is charged after rail $\bar{A}$, then the time-domain encoding maps a logic-0 according to the SR domain, on the contrary a logic-1 is mapped; no information is encoded when $\delta = 0$ (see Fig. 1).

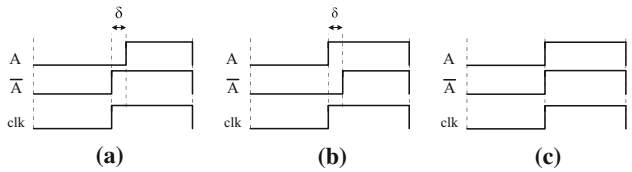

Fig. 1 Timing diagram of logic-0 (**a**), logic-1 (**b**), invalid (**c**) signal

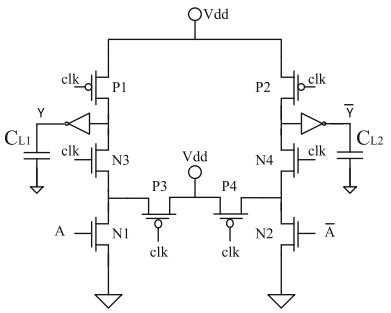

Fig. 2 Cell template of a time-enclosed logic inverter

3.3 A cell template for TEL circuit implementations

In this section, we describe a cell template which enforces the data encoding of TEL circuits. The cell of a TEL buffer/inverter (BUFF/INV) is shown in Fig. 2. It is a dynamic differential domino logic gate. When clk is low, the precharge is global thanks to the keeper transistors which activate simultaneously and force the internal nodes to V_{DD}. The outputs are then driven to 0 by the inverters for the following gate as in a domino logic. At the clock rising edge, keeper transistors are open and the internal nodes are discharged by the signals flowing in the differential paths. The reason for the insertion of keeper transistors P3–P4 is due to the memory effect on the internal nodes, which is critical for the energy balancing activity of the cell when the internal capacitances are unbalanced [22]. In Fig. 3 also the circuit of a *sense amplifier-based logic* (*SABL*) inverter is shown [17], which is an example of RTZ logic.

3.4 A first-order model of the power consumption

The main drawback of RTZ logic is that even if the switching factor is always 1, the dynamic power consumption is highly

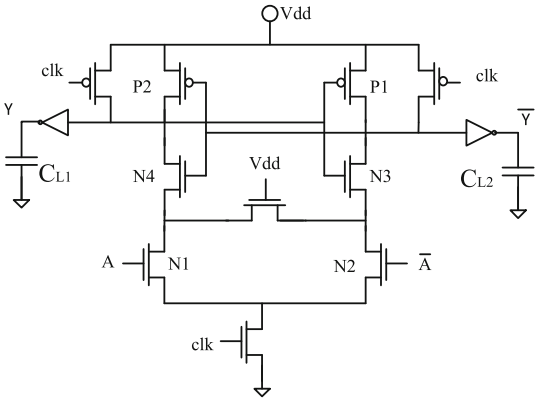

Fig. 3 Cell template of a sense amplifier-based logic inverter

sensitive to the differential capacitive mismatch [41]. With the technology scaling, the interconnect wires have a strong impact on the overall capacitance, and thus under the perspective of an automatic routing procedure the differential load capacitances are expected to be different, as shown in Figs. 2 and 3. According to the data encoding defined in Table 1 and the timing diagram of the signals depicted in Fig. 1, the current trace of a TEL circuit is composed of three peaks: the first occurs at the precharge, the other ones are related to the evaluation and the postcharge, respectively, and are separated from a time equal to δ. Through the time-enclosed data encoding, each capacitance is charged and discharged once in the clock cycle; therefore unlike the case of RTZ logics where the dynamic power depends on the values of the differential capacitances, in TEL circuits it depends only on their sum (Table 2).

The property of TEL data encoding is that the relevant information is enclosed inside a time period δ, and each electrical mismatch gives origin to a deviation of the current pattern only during this time window: if the sampling period of an oscilloscope is greater than δ, no relevant samples are captured during the acquisition phase, and thus PAAs are unfeasible. For instance, if an attacker uses an oscilloscope with a sampling rate of 2 GS/s (with a maximum bandwidth of 1 GHz due to the Nyquist's limit), which is rather common in a practical PAA scenario, an interval δ less than 500 ps, reasonably achievable in common submicron technologies, is sufficient for preventing PAAs. The value of δ is chosen by the designer to guarantee a certain level of security in a given technology. In the following, we use the mismatch factor for indicating the degree of unbalance, defined in [27] as the ratio between the differential capacitances:

$$\mathrm{MF} = \frac{C_{\mathrm{Lmax}}}{C_{\mathrm{Lmin}}} \tag{1}$$

3.5 Timing constraints of a TEL circuit

In this section, we define the timing specifications of TEL circuits. TEL circuits are based on a hybrid synchronization scheme: on a side, the precharge is globally synchronized with the clock edge; on the other side, the evaluation is also synchronized with the clock but the postcharge is asynchronous and depends on the propagation times of the signal along the combinational path. With reference to the multi-stage circuit in Fig. 4, the SR signal is first converted into a TEL differential pair with a nominal δ. In accordance to the data encoding defined in Table 1 and Fig. 1, the differential signals propagate along the pipeline at different time instants. At the output of each gate, the time interval δ is not equal to the nominal δ; these timing mismatches are intrinsic to the asymmetry of the logic cells implementing a combinational function.

This phenomenon is known as *early evaluation effect* and has been demonstrated to be a problem in several DPLs [23,24]. In [40] authors propose a circuit-level optimization for balancing the time of propagation of a logic cell in the *delay-based DPL* (*DDPL*) style, to avoid early evaluation errors. In the case of TEL circuits, the main drawback of early evaluation is the variation of the length of the time interval δ. To prevent any timing violations and guarantee at the same time that the level of security is preserved, the circuit in Fig. 4 must meet three fundamental requirements:

1. δ can decrease at the output of a combinational logic, but cannot increase ($\delta_{\mathrm{CL}} < \delta$).
2. δ can decrease down to the setup time of the flip-flop ($t_{\mathrm{SUP}} > \delta$)
3. δ must be regenerated by the flip-flop ($\delta_{\mathrm{FF}} = \delta$).

These conditions are translated in a timing constraint on the critical path of the circuit. The propagation time of a TEL gate

Table 2 Model of the power consumption for a TEL and a SABL inverter cell with an unbalanced load

	$(Y, \bar{Y})$	1st semiperiod		2nd semiperiod		$P^{(1)}_{\mathrm{dyn}}$	$P^{(2)}_{\mathrm{dyn}}$	P_{dynTOT}
		Y	$\bar{Y}$	Y	$\bar{Y}$			
RTZ	(0, 1)	$0 \to 0$	$0 \to 1$	$0 \to 0$	$1 \to 0$	0	$V^2_{\mathrm{DD}} C_{\mathrm{L2}} f$	$V^2_{\mathrm{DD}} C_{\mathrm{L2}} f$
	(1, 0)	$0 \to 1$	$0 \to 0$	$1 \to 0$	$0 \to 0$	$V^2_{\mathrm{DD}} C_{\mathrm{L1}} f$	0	$V^2_{\mathrm{DD}} C_{\mathrm{L1}} f$
TEL	(0, 1)	$0 \to 1$	$0 \to 1$	$1 \to 0$	$1 \to 0$	$V^2_{\mathrm{DD}} C_{\mathrm{L1}} f$	$V^2_{\mathrm{DD}} C_{\mathrm{L2}} f$	$V^2_{\mathrm{DD}} (C_{\mathrm{L1}} + C_{\mathrm{L2}}) f$
	(1, 0)	$0 \to 1$	$0 \to 1$	$1 \to 0$	$1 \to 0$	$V^2_{\mathrm{DD}} C_{\mathrm{L1}} f$	$V^2_{\mathrm{DD}} C_{\mathrm{L2}} f$	$V^2_{\mathrm{DD}} (C_{\mathrm{L1}} + C_{\mathrm{L2}}) f$

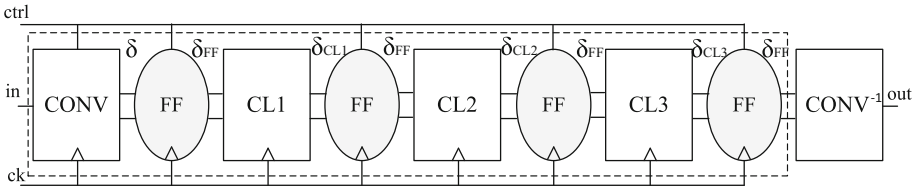

Fig. 4 A pipelined circuit template in which the information is enclosed inside a time interval δ

Table 3 Roadmap of the estimated propagation times for different submicron technologies

Tech mode (nm)	t_{pMAX} (ps)		t_{SUP} (ps)	δ_{MIN} (ps)
	CMOS IVX2	TEL AND/NAND		
90	50	100	180	380
65	25	50	90	190
45	12	25	45	95
28	6	12	20	48

t_P is defined as the difference $\delta_{IN} - \delta_{OUT}$, and depends on the technology: more scaled is the technology, lower is expected to be t_P because the propagation times of the signals decrease. According to the analysis in [40], it is always possible to build logic gates with balanced times of propagation of the differential signals; thus, we assume that condition 1 can be met by an adequate design of the pull-up network of the logic gates. The propagation time of the critical path t_{CP} is defined as the difference between the delay δ_{CP} at the output of the last gate in the path and the delay at the input of the first gate (i.e. the nominal δ):

$$t_{CP} = \delta - \delta_{CP}. \tag{2}$$

The propagation time of the critical path depends on the number of stages N and can be calculated as the sum of the propagation times of the N gates of the path:

$$t_{CP} = \sum_{i=1}^{N} t_{p_i} = N \cdot \bar{t}_p \tag{3}$$

where $\bar{t}_p$ is the average propagation time of the TEL combinational gates in the path in a certain technology. We point out that t_p depends on the input data configuration. The timing constraint on the critical path delay δ_{CP} is determined by the setup time t_{SUP} of the flip-flop at the final stage of the critical path:

$$\delta_{CP} = \delta - t_{CP} = \delta - N \cdot \bar{t}_p \geq t_{SUP} \tag{4}$$

which provides a condition on the number of logic stages in a TEL pipeline when δ is set:

$$N \leq \frac{\delta - t_{SUP}}{\bar{t}_p} \tag{5}$$

The maximum number of stages can be calculated in the worst-case situation that each logic gate has the maximum propagation time t_{pMAX}, which occurs for a specific input data configuration, as above mentioned, and represents the critical path of the design. Thus, the equation:

$$N_{MAX} = \frac{\delta - t_{SUP}}{t_{pMAX}} \tag{6}$$

poses a constraint on the maximum number of stages that can be inserted in a combinational TEL circuit in a given technology node, and depends on the value of δ, which is chosen for security issues, and t_{SUP} and t_{pMAX}, which are implementation and technology dependent.

As stated before, the designer chooses the value of the nominal δ according to the level of security he/she wants. However, the minimal value of δ which a designer could choose in a given technology is defined by the limits of the technology itself (i.e. by the propagation times of the logic cells). To have a better idea about the minimum value of δ that a designer can set, and so the maximum level of security that can be obtained using TEL circuits, let us consider the case of a critical path composed of only two combinational gates between registers (e.g. two AND/NAND gates). In this case, the minimum value of δ_{MIN} can be calculated by Eq. 5 as:

$$\delta_{MIN} = 2 \cdot t_{pMAX} + t_{SUP} \tag{7}$$

Accordingly, it is possible to define a road map for the dependence of δ_{MIN} with the technology scaling, which gives an idea about the level of security at different technology nodes: for different submicron technologies, at each step the propagation time is estimated to be halved, as well as the setup time and thus δ_{MIN} (Table 3).

The value chosen for δ poses a constraint on the maximum frequency f'_{MAX} for a TEL circuit, as described in Appendix A, but does not have a direct impact on the maximum working

frequency to guarantee functionality, which on the contrary depends on the propagation times of the logic gates, in a similar way as conventional RTZ logics.

The simulations proposed in this work have been executed on a specific implementation of a TEL circuit template, using the logic cells proposed in [40] and [42], designed in a CMOS 65-nm technology. According to the value in table, δ_{MIN} for a TEL implementation designed in a CMOS 65-nm technology is around 200 ps. An attacker could be able to detect information leakage inside this time windows if he/she has a setup measurement with a minimum resolution given by the following equation:

$$f_{\mathrm{sMIN}} = \frac{1}{\delta} = \frac{1}{200\,\mathrm{ps}} = 5\,\mathrm{GSample/s} \tag{8}$$

This represents a rough estimation which does not take into account all the electrical effects inside the circuit (e.g. filtering, noise, etc.), but provides a good idea about the level of security that can be reached by TEL circuits. Furthermore, in practical attacks, both the noise in the sampling and in the amplitude of the current sample must be also considered; therefore, the minimum resolution required from the attack setup can be even greater.

The tradeoff is in the choice of the number N of logic gates in a combinational path and the value of δ: lower is δ for security issues, smaller must be the maximum number of logic gates in the critical path, according to Eq. 5. In practical applications, for example in lightweight cryptography for ultra-constrained devices (e.g. RFID tags, smart cards, etc.) area and power are the most important requirements. The trend is to design ever smaller combinational S-Boxes for lightweight hardware-optimized block ciphers (e.g. 3×3 or 4×4 S-Boxes), which can be implemented with a very low number of logic gates (in the order of $10 \div 15$ [43]), with a critical path of around four logic gates, and this allows to obtain values very close to those predicted in Table 3. Consider for example that a combinational 8×8 S-Box from AES may require more than 100 logic gates [44], with a critical path usually higher than 10 cascaded gates. Indeed, TEL has been conceived to run on embedded devices where the increased level of security with respect to a conventional RTZ implementation is outstanding, as it will be shown in next sections, but it could be even extended to protect more modern cryptographic processors which run at maximum frequencies and are in general not area-optimized, requiring in this case a reduction of the critical path length by inserting intermediate registers (see Appendix A).

3.6 Second-order effects: transient leakage

The model described in Sect. 3.4 neglects the transient effects of the current traces due to the electrical mismatches in a circuit, for example, the charge/discharge settling times of the output capacitances. These transient effects have components at higher frequencies and are usually filtered out by the off-chip capacitances, omnipresent on the *power supply network* (*PSN*) of digital circuits. Earlier security metrics like *normalized energy deviation* (*NED*) [17,41] give an estimation of the ability of a circuit of balancing the energy in a clock cycle by integrating the current traces in a clock cycle, doing the implicit assumption on the presence of a low-pass filter. However, several papers demonstrated that depending on the device under attack, an attacker can even remove the off-chip capacitances and exploit these mismatches for attacking the circuit, as for example in [45]. Therefore, balancing the energy in a cycle is not sufficient for enhancing the resistance of circuit against PAAs, and NED usually overestimates the actual level of security.

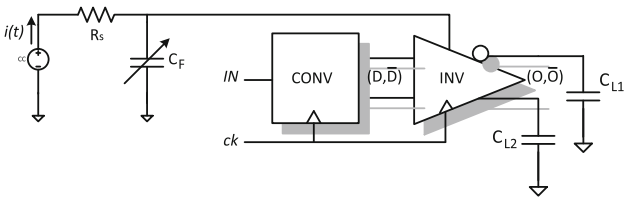

Fig. 5 Testbench for the simulations of the TEL inverter cell with an unbalanced load and a variable RC filter on the PSN

Consider for example the testbench in Fig. 5, in which the instantaneous current trace of the TEL inverter is measured considering a MF equal to 3: if one, say C_{L1}, is fixed to 1 fF, the other one, say C_{L1}, is equal to 3 fF. The model of the PSN is simple: a capacitance C_{F} together with a source resistor R_{S} (100 Ω), which acts as low-pass filter for the current drawn from the source generator. We measure the current when different values of the filtering capacitance C_{F} are considered. The clock frequency is chosen equal to 10 MHz, which is compatible with the typical frequencies adopted for cryptographic applications in embedded devices (e.g. smart cards), whereas the V_{DD} voltage is equal to 1.2 V and the time window δ to 500 ps. Note that the same results can be obtained using smaller values for δ and higher working frequencies, even in the order of GHz, as discussed in previous section and in Appendix A.

Simulations are repeated using different values for the capacitance C_{F} (no capacitance, 10 pF, 100 pF, 1 nF). The filtered instantaneous current traces $i(t)$ related to the two cases $(1, 0) \rightarrow (0, 1)$ and $(0, 1) \rightarrow (1, 0)$ exhibit the same peak during the discharge event, whereas the peaks at the evaluation and the postcharge times differ according to the value of the load capacitances. The traces are then exported from Cadence SPECTRE, obtaining the sample sequences $i[k]$, with $k = 1, 2 \ldots T$. The sampling period is equal to 1 ps, which results in a number of samples $T = 100{,}000$ per cycle. In Fig. 6, the standard deviation of the sequences $i_{0\rightarrow 1}[k]$ and

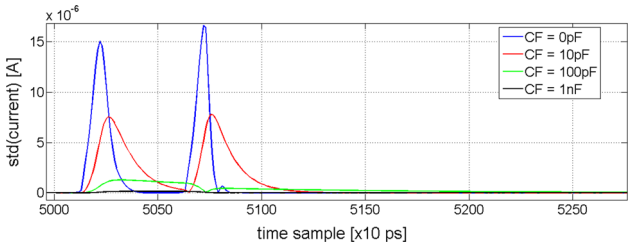

Fig. 6 Current peaks during the evaluation phase for the unbalanced TEL inverter, with a variable filtering capacitance

Table 4 NED as a function of the capacitance C_F

C_F	NED
0	0.855
10	0.807
100	0.869
1000	0.871

$i_{1\to 0}[k]$ is plotted for each value of C_F; the figure shows only the current during the evaluation and the postcharge phases, where the traces differ.

When no capacitances are inserted, the peaks are separated of about 500 ps, as expected (blue curve). With a decoupling capacitance of 10 pF, the peaks extend beyond the nominal interval δ, creating a transient leakage (red curve). Increasing C_F up to 100 pF, the transient leakage is integrated in time, but it is still visible outside the interval δ (green curve). Finally, with a value of 1 nF, the transient leakage is almost completely filtered and the standard deviation of the traces, which represents the exploitable power in the power analysis scenario [36], is flattened. Even if the energy (i.e the area under the curve) is always the same and NED is almost constant (Table 4), the relevant time extends beyond δ. If we consider a pipelined circuit as that shown in Fig. 4, transient leakage adds up along the combinational path, violating the timing constraints of a TEL circuit. Even if transient effects are reduced by the EDA processor, which in the automatic placing procedure selects minimum fanout cells from the technology library for driving the output capacitances of the interconnect wires, this is not sufficient for eliminating the mismatch due to the automatic routing.

4 A balancing act: frequency analysis of the current trace

In this paragraph, we present a novel methodology which can be adopted in combination with TEL gates. This technique is based on the insertion of a filter for removing the high-frequency components of the transient leakage highlighted by simulations of last section as depicted in Fig. 6. This solution guarantees an adequate filtering of the high frequencies

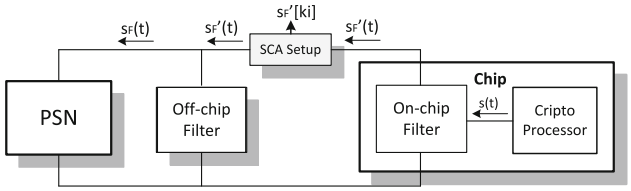

Fig. 7 PAAs scenario for a TEL circuit, with the insertion of an on-chip filter for removing the high-frequency components directly at layout level

already at layout level, irrespective of the presence of an off-chip filter.

4.1 Insertion of an on-chip filter in a TEL circuit

With reference to Fig. 7, the best situation for an attacker is when he/she has direct access to the pin of the package, under the hypothesis of removing the off-chip capacitances. This way the attacker can measure only the trace $s'_F(t)$, which is low-pass filtered; thus, provided that the on-chip filter is adequately designed, the transient effects of the internal signal $s(t)$ cannot be detected outside the package of the chip.

This methodology represents a back-end optimization which, if combined to the adoption of TEL data encoding allows to mitigate the effect of electrical mismatches and to efficiently flatten the instantaneous current irrespective of the peripherals of the chip, as it will be shown in next sections. The back-end step can be efficiently implemented for example by inserting some capacitance in the layout of the chip. It must be pointed out that the presence of on-chip decoupling capacitors is already implicit in the IC design, due to the fact that during the digital back-end flow some decoupling capacitors are always inserted by the automatic place and route engine. Polysilicon capacitances are available in common digital libraries as macrocells which are automatically inserted by the CAD engine. However, they have a limited capacitance per area unit (in the order of some fF/um^2) and are inserted to guarantee the functionality of the circuit, without any requirements regarding the security issues. The presence of a specific block in Fig. 7 indicates that a minimal amount of on-chip capacitance must be guaranteed according to the transient leakage to be filtered off.

4.2 A new frequency-based metric

In this section, we provide a method for estimating the bandwidth of the filter in Fig. 7. We use the *FFT* for deducing information on the energy distribution of the current traces in the frequency spectrum. Previously published works exploited FFT as a novel leakage source, and novel PAAs based on the frequency domain have been also presented [46,47]. Following the results in [48], where authors pro-

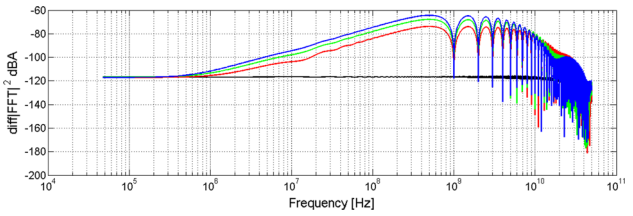

Fig. 8 **ΔFFT** vector for the TEL inverter for different values of the mismatch factor ($\delta = 500$ ps): MF = 1 (*black*), 2 (*red*), 3 (*green*), and 4 (*blue*) (color figure online)

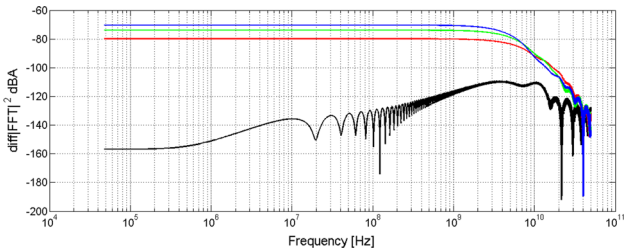

Fig. 9 **ΔFFT** vector for the SABL inverter for different values of the mismatch factor: MF = 1 (*black*), 2 (*red*), 3 (*green*), and 4 (*blue*) (color figure online)

pose a leakage frequency model for improving the strength of SCAs though a selective filtering of the traces of a synchronous design, in this work we use the properties of FFT for defining a general metric for assessing the leakage distribution at the design steps. With reference to the testbench in Fig. 5, we have measured the non-filtered current traces for the two data transitions. Simulations were repeated for different values of C_{L2}, from 1 fF (MF = 1, perfect balance) and 4 fF (MF = 4, high unbalance), with steps of 1 fF. $\mathbf{FFT}_0$ and $\mathbf{FFT}_1$ denote the one-dimensional vectors containing the F-points of the FFT of the current traces associated to 0 and 1 as input data, respectively. The current traces have been exported with a sampling period of 10 ps ($f_S = 100\,\mathrm{GS/s}$) and according to the Nyquist condition the maximum frequency of the FFT is 50 GHz. The number of points F is around 2M, which leads to a resolution of about 50 kHz in the frequency domain. The squared absolute value of the difference of the FFTs is:

$$\boldsymbol{\Delta}\mathbf{FFT} = |\mathbf{FFT_0} - \mathbf{FFT_1}|^2 \tag{9}$$

The plot of **ΔFFT** (Fig. 8) provides some useful information regarding the leakage distribution of the circuit. First, there is a flatten bandwidth in the energy deviation equal to about -120 dB irrespective of the amount of output unbalance. Then, after $f_0 \approx 1$ MHz, the plots increase, and some lobes at frequencies multiple of 1 GHz are visible. This frequency is related to $\delta = 500$ ps, where the maximum amount of leakage due to the capacitive mismatch is concentrated: higher the output unbalance, higher the transient effects on the current peaks, higher the lobes of the plot, as visible in Fig. 8.

For removing the transient leakage due to the capacitive unbalance, the on-chip low-pass filter must be in the order of 1 MHz; f_0 is named cutoff frequency of TEL circuit. With the setup of Fig. 5, where we assume a fixed input resistance R_S equal to 100 Ω, the minimum value for the on-chip capacitance can be estimated as:

$$C_F^{\mathrm{opt}} = \frac{1}{2\pi R_S f_0} \approx 1.6\,\mathrm{nF} \tag{10}$$

which is in accordance with the value of 1 nF found with transient simulations (Fig. 6): if a capacitance lower than C_F^{opt} is used, the on-chip filter cannot remove completely the high-frequency components due to the mismatch, and some relevant samples fall outside δ. The same set of simulations has been repeated for a SABL inverter (Fig. 9).

Unlike the case of TEL, in a SABL circuit, which is based on a synchronous evaluation, there is no possibility of identifying a cutoff frequency. The energy deviation strongly depends on the capacitive unbalance also at low frequencies, and there is no possibility of removing the data-dependent leakage by low passing the traces. Note that already for a moderate mismatch (MF = 2, red curve) **ΔFFT** is in the order of -80 dBA at low frequencies, which is 40 dB higher than the leakage of TEL.

The metric in Eq. 9 can be generalized to the more general case of N input vectors. We define the *frequency energy distribution* (*FED*) as the one-dimensional vector of the variances of the frequency samples at the discrete frequency f of the FFTs of all the possible current traces N.

$$\mathbf{FED} = [\sigma_1\ \sigma_2\ \ldots \sigma_F] \tag{11}$$

$$\sigma_f = \left[\frac{1}{N}\sum_{i=1}^{N}\sqrt{[\overline{\mathrm{FFT}}[f]^2 - \mathrm{FFT}[f]_i^2]}\right]^2 \tag{12}$$

with $f = 1, 2 \ldots F$. The one-dimensional vector $\overline{\mathbf{FFT}} = \left[\overline{\mathrm{FFT}}[1]\ \overline{\mathrm{FFT}}[2]\ \ldots \overline{\mathrm{FFT}}[F]\right]$ contains the averages of the points of the FFT; a sample $\overline{\mathrm{FFT}}[f]$ is calculated as:

$$\overline{\mathrm{FFT}}[f] = \frac{1}{N}\sum_{j=1}^{N}\mathrm{FFT}_j[f] \tag{13}$$

4.3 Relation between δ and f_0 in a TEL gate

In this section, we execute an analytical calculation to find a relation between δ and f_0 in a TEL gate. We consider the most simple case of a TEL inverter (Fig. 2), but this calculation can be extended to the case of any TEL circuit. To extrapolate the relation between δ and f_0, the absolute value of the difference of the Fourier transforms of the current traces in correspondence to the two possible input configurations of the inverter can be calculated as:

$$|\Delta S(f)| = |S_1(f) - S_0(f)| = 2\sqrt{2\pi}\,|\sin(\pi\delta f)| \cdot \left| I_1\sigma_1\, \mathrm{e}^{-(\pi\sqrt{2}\sigma_1 f)^2} - I_0\sigma_0\, \mathrm{e}^{-(\pi\sqrt{2}\sigma_0 f)^2} \right| \quad (14)$$

Further details on the calculation executed to obtain Eq. 14 are described in Appendix B. $S_0(t)$ and $S_1(t)$ are the Fourier Transforms of the current traces $s_0(t)$ and $s_1(t)$ for the two input configurations.

The last factor in Eq. 14 represents the difference of the Gaussian pulses when there is no delay; in the ideal case of MF = 1, we have $I_0 = I_1$ and $\sigma_0 = \sigma_1$, thus $|\Delta S(f)| = 0$ at each frequency, independently from δ. However as previously discussed, in submicron technologies it is hard to guarantee a perfect balance between C_{L1} and C_{L2}; therefore, we consider the realistic case of MF $\neq 1$. From Eq. 14, we see that the dependence of $|\Delta S(f)|$ on δ is sinusoidal, and there is an infinite number of local minima and maxima, as shown in Fig. 8. If we consider $\delta \neq 0$, $I_0 \neq I_1$ and $\sigma_0 \neq \sigma_1$, we have:

$$\max |\Delta S(f)| = 2\sqrt{2\pi} \left| I_1\sigma_1 \mathrm{e}^{(-\pi\sqrt{2}\sigma_1 f)^2} - I_0\sigma_0 \mathrm{e}^{(-\pi\sqrt{2}\sigma_0 f)^2} \right| \iff \sin(\pi\delta f) = 1 \quad (15)$$

$$f_m^{\max} = \frac{1+2m}{2\delta}, \quad m \in \mathbf{Z} \quad (16)$$

$$\min |\Delta S(f)| = 0 \iff \sin(\pi\delta f) = 0 \quad (17)$$

$$f_m^{\min} = \frac{m}{\delta}, \quad m \in \mathbf{Z} \quad (18)$$

The frequency pattern of $|\Delta S(f)|$ shifts toward the right (left) part of the frequency axis if δ decreases (increases). Fixed $m = m'$, $f_m'^{(\min)}$ and $f_m'^{(\max)}$ have a inverse relation with δ. The first minimum and the first maximum can be found for $m = 0$ at the frequencies $f_0^{(\min)} = 0$ and $f_0^{(\max)} = \frac{1}{2\delta}$. For the case $\delta = 500$ ps, the values are in accordance to the plot in Fig. 8. The cutoff frequency f_0 is located in the frequency range bounded by $f_0^{(\min)}$ and $f_0^{(\max)}$ where the function is monotonically decreasing, thus also f_0 has an inverse dependence with δ. Relaxing the condition in Eq. 15, we obtain

$$\min |\Delta S(f_0)| \approx 0 \iff \sin(\pi\delta f_0) \approx 0 \iff f_0 \ll \frac{1}{\pi\delta} \quad (19)$$

as expected. This relation is experimentally confirmed by repeating the simulations of previous section with different values of δ in the range of 100 ps $\div$ 5 ns. The plot of f_0 as a function of δ is reported in Fig. 10:

As shown in Figs. 11 and 12 for the cases of $\delta = 100$ ps and $\delta = 5$ ns respectively the frequency spectrum shifts in the frequency axis. The domain of the curve in Fig. 10 is given by the minimum (i.e. δ_{MIN} defined in Eq. 7) and the maximum value of δ (i.e. $\delta_{MAX} = \frac{T_{CK}}{2}$) in a given technology and for a certain clock frequency. If δ tends to δ_{MAX}, the TEL gate works similarly as the SABL inverter, and the

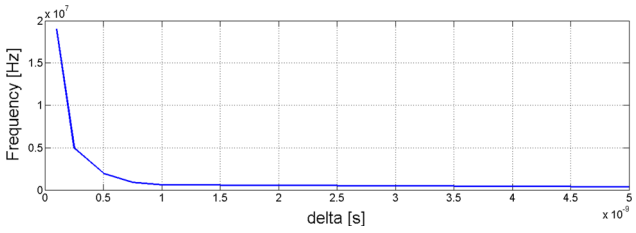

Fig. 10 Plot of the frequency f_0 as a function of δ

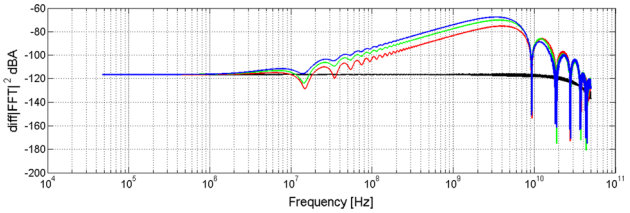

Fig. 11 **ΔFFT** vector for the TEL inverter for $\delta = 100$ ps

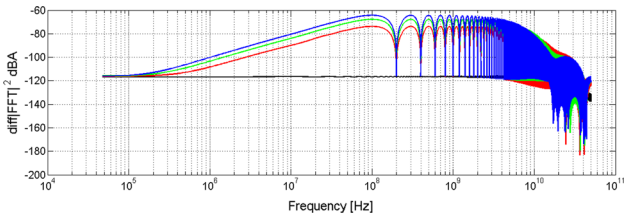

Fig. 12 **ΔFFT** vector for the TEL inverter for $\delta = 5$ ns

cutoff frequency f_0 tends to 0, invalidating the benefits of the time-enclosed encoding. We point out that modeling a current peak as a Gaussian pulse neglects the tail lobes in the spectrum, which instead must be considered for example in the case of many logic gates switching at the same clock cycle. In this case, the current trace is composed of several peaks and the pattern has not a Gaussian shape (see Fig. 14 in next section). Furthermore, in each current trace the static power consumption is superimposed to the dynamic peak. In a symmetric gate as TEL inverter, the static consumption is balanced for both the transitions; the residual leakage in the plot of **ΔFFT** (in the order of −120 dB) is probably due to the numeric error done by the simulator.

5 Design of a cryptographic TEL-protected cryptoprocessor

5.1 Description of the architecture tested in simulation

We have designed a 4-bit cryptographic circuit, which implements a 4-bit-slice unit of the *Serpent* processor, as target circuit in PAAs. *Serpent* is one of the finalists of the AES contest [49], and is based on 4 × 4 S-Boxes. We have chosen a single unit of the processor because a full design verifi-

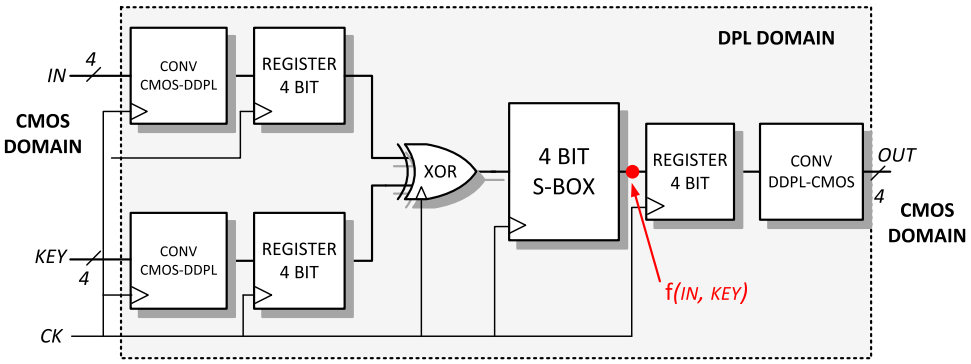

Fig. 13 Data path of a DPL-featured 4-bit unit implementing the first round of *Serpent* processor

cation of the entire 128-bit processor would have required a very long time for simulating all possible input vectors in Cadence. The data path of the circuit is reported in Fig. 13

The choice of reducing the span of the attack to 4-bit words is compatible with the bit-slice structure of *Serpent*: if we consider for instance the first round of the encryption, the power consumption of the logic is the sum of the power consumption of 32 identical parallel bit-slice units [50], which switch at the same time. Therefore, power analysis simulations can be simplified by analyzing the resistance of one of these bit-slice units, and considering the other switching circuits as on-chip noise. Then, by exploiting the leakage of the target bit-slice it is possible to recover 4 bits of the key word, and replying the same attacks for the other bit-slice units for recovering the whole key word, as in a *divide and conquer* strategy.

The circuit in Fig. 13 processes a nibble of the 128-bit data word in a two-stage pipeline. In the pipeline stages, a 4-bit data word is first converted and stored in a register, then it is XORed with a nibble of the round key, processed by the 4×4 S-Box S0 block and finally stored in an output register. The hardware description of the S-Box S0 was done using the Synopsys Design Compiler, which generated a netlist of combinational gates, and exported into Cadence environment. The data path in Fig. 13 has been implemented using TEL data encoding, with a relevant time $\delta = 1$ ns. For this purpose, we have used the improved architecture of the combinational delay-based DPL gates described in [40], which have the circuit template presented in Fig. 2, and the flip-flop presented in [42], which meets the timing requirements described in Sect. 3.5.

5.2 Estimation of the cutoff frequency f_0 of the circuit

The first step is the characterization of the leakage of the circuit by collecting the current traces related to all the possible 256 input combinations before doing the layout of the chip. The clock frequency is chosen equal to 10 MHz which is typical for smart card applications, the V_{DD} voltage to 1.2 V and the time window δ of the TEL circuit to 1ns. We have inserted at the output of each logic gate two capacitances which simulate the capacitances of the differential interconnect wires. We have collected the current traces in the case of low unbalance (MF $\approx$ 1) and in the case of high unbalance (MF = 3). The latter case is reported in Fig. 14, where several peaks due to the presence of several logic gates switching at the same time can be identified, as well as an amount of static power.

We have repeated the frequency analysis done for the TEL inverter gate. For taking into account all possible inputs, we have used the metric FED defined in Eqs. 11 and 12 for determining the amount of bandwidth required for designing the on-chip filter. In this set of simulations, the PSN is modeled as an ideal voltage source and the current drawn by the circuit is sampled with a time resolution of 20 ps. The simulation setup is equivalent of gathering measurements on the actual circuit with a sampling frequency equal to 50 GSample/s, which poses a constraint on the maximum bandwidth (equal to 25 GHz for the Nyquist's limit). The number of points of the FFT is around 200k, which corresponds to a resolution of about 400 kHz. Higher values are outside of the memory of MATLAB and cannot be processed. The FED is plotted in Fig. 15 for the two cases of low unbalance of the differential wires (MF $\approx$ 1) and high unbalance (MF = 3).

In Fig. 14, at low frequencies the FED is in the order of -80 dB, which indicates a higher variation of the static power consumption with respect to the case of a single inverter. The main lobe of the FED is at 500 MHz, in agreement with

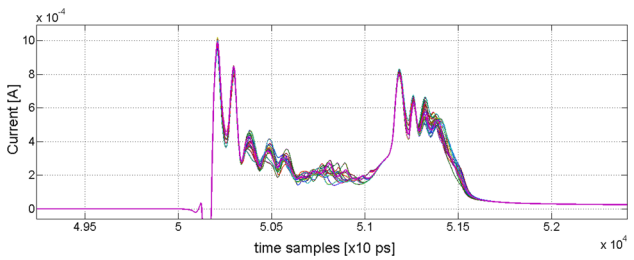

Fig. 14 Current traces for each of the 256 input combinations of the TEL circuit in the evaluation and post-evaluation phases of the third clock cycle

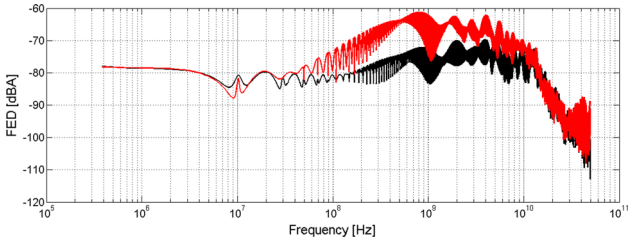

Fig. 15 FED vector for TEL circuit with low unbalance on the interconnect wires (*black curve*) and with a maximum unbalance ($MF = 3$) (*red curve*) (color figure online)

equations Eq. 16, whereas the frequency f_0 is around 30 MHz by visual inspection. Apart from a constant term due to the static consumption and several tail lobes in the FFTs of the traces, the Gaussian model described in Sect. 4 still holds and the inverse relation between of f_0 and δ depicted in Fig. 10 is also confirmed. The static consumption cannot be eliminated by the PSN filter and represents a resilient leakage which does not depend on the dynamic power model and is uncorrelated to the key; thus, f_0 is the just cutoff frequency of the filter, which must be designed to eliminate all the lobes at higher frequencies that correspond to the transient leakage.

6 SCA security evaluation of the TEL circuit

6.1 Discussion on the PAAs methodology for simulations

In this section, we perform PAAs against a TEL implementation of the previously described architecture, in a more realistic simulation model where also the effect of the impedance of hypothetical chip peripherals is taken into account. The Pearson's correlation coefficient vector $v = [\rho_1 \rho_2 \ldots \rho_T]$ used in standard *correlation power analysis* (*CPA*) attacks [3] reveals important information regarding the time instants in which the correlation between current samples and intermediate values is high. For this reason, after having supposed that the adversary knows exactly the relevant time interval, the correlation coefficient vector is used as statistical distinguisher to discriminate the correct key guess. We point out that even if there are more advanced security metrics to assess the information leaked by a hardware implementation [38,51,52] and statistical distinguishers to exploit this information [37,53], we used the correlation coefficient because it provides a direct estimation of the linear relation between current traces and processed data directly in the time domain, which is very useful to fairly compare an amplitude-domain logic as RTZ and a time-domain logic as TEL.

Simulations have been performed in Cadence environment, and the current traces have been measured by considering the presence of the decoupling capacitance $C_F = 100$ pf,

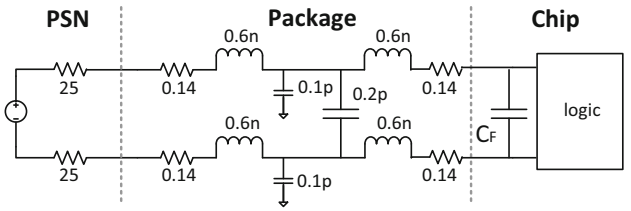

Fig. 16 Equivalent circuit model for the testbench in Cadence simulations [23]

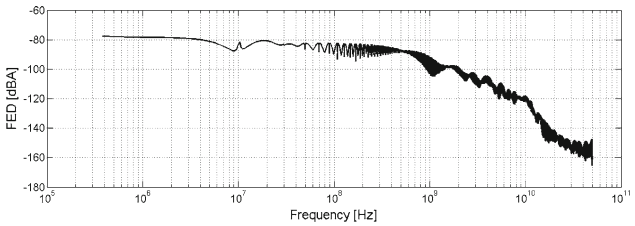

Fig. 17 FED vector for the TEL circuit calculated after having filtered the current traces ($f_0 = 30$ MHz)

as calculated in previous section. Experiments have been then repeated on a SABL implementation of the same architecture. Current samples have been exported from Cadence with different values of the sampling period, as it will be shown in Sects. 6.4 and 6.5

6.2 Design of the on-chip filter considering chip peripherals

As discussed by authors in [34], to have realistic SPICE simulations, a good model for the chip peripherals must be taken into account. Thus, in accordance to the model defined in [34], for the simulation testbench we use the same equivalent circuit which includes the package impedance of the chip as the only sources of impedance that must be included and cannot be removed by an adversary in a non-invasive attack. The effects of the external environment (e.g. socket, cable, etc.) are included in the model of the PSN, which is represented as a generic voltage source with a series resistor $R_S = 50\,\Omega$. We collected the 256 current traces of the circuit after post-layout simulations, using the simulation parameters described in previous section.

According to the pattern of Fig. 14 and the impedance model of Fig. 16, the capacitance C_F must be at least equal to 100 pF to obtain a cutoff frequency of about 30 MHz. With this value, we have repeated post-layout simulations of the circuit and calculated again the FED vector (Fig. 17).

The lobes are almost completely removed and the FED is nearly flattened; a residual variation at the multiple of the clock frequency is still visible, but it is below the value at low frequencies.

Table 5 Performances of the designed SABL and TEL circuits (post-layout)

	# Transistors	Area overhead	Active area (μm^2)	max[P_{AV}]@10 MHz (μW)	max[f_{CK}] (MHz)
CMOS	564	×1.0	n.a.	n.a.	n.a.
SABL	1538	×2.7	1703	23.3	215
TEL	1983	×3.5	2123	36.1	380 (240)

6.3 Area overhead of the countermeasure

Time-enclosed logic gates have been abutted using a rail-to-rail place methodology and routed using the Automatic Routing Tool of Virtuoso. The design occupies an active area of about 2.100 μm^2, which compared to the SABL implementation (1.703 μm^2) leads to an additional overhead of about 25 %. In Table 5 a comparison of the performances of CMOS, TEL, and SABL is reported (note that the layout of the CMOS implementation has not been performed and we reported only the number of transistors). Through a parasitic extraction we verified that MF <3 after the automatic routing procedure for all the differential interconnect wires, according to the assumption done during the design steps.

The area overhead reported in Table 5 takes into account only the active area of the logic cells. For the TEL implementation, frequencies f'_{max} and f_{max} (see Appendix A) are 240 and 380 MHz respectively, which are comparable to RTZ operating frequency. In the layout, we left some free room which in a standard semi-custom design flow would be filled with decoupling capacitances and filler cells. Anyway, in the simulation model of Fig. 16 we have considered the on-chip capacitance as a discrete component. In real cases, it is implemented using the decoupling capacitance cells of the technology library during the back-end design flow. Part of the capacitance can be also implemented by inserting CMOS polysilicon capacitors directly on the V_{DD} global metal wires in the layout. To have a total capacitance equal to 100pF, if we consider a capacitance per area unit of 13 fF/μm^2, in accordance to the specifications of the 65nm technology we have chosen, an area of about 7.700 μm^2 is required. The overall area estimation of the TEL chip with the polysilicon capacitances would be of about 10.000 μm^2.

Using more scaled technologies, it is possible to obtain lower values for the on-chip capacitance and reduce the area overhead: for instance, with reference to Eq. 4 and to Table 3, if we consider the same circuit implementation, which has a critical path of 8 stages ($N_{MAX} = 8$), using a 28-nm technology δ_{MIN} can be estimated equal to about 150 ps; thus, using a reasonable value $\delta = 200$ ps which is five times lower than δ used in the 65-nm implementation, and according to the circuit components in Fig. 16 the cutoff frequency f'_0 would be equal to $5 \cdot f_0 = 150$ MHz, which can be obtained with $C_F = 20$ pF and a strong reduction of area penalty. In any case, we would like to point out that typical values for the density in VLSI design obtained after the placement of the standard cells is around 70 %, and the remaining area is automatically filled by the CAD processor using the *decap* and *filler* cells in the tech library, which are essential to guarantee chip functionality and represent on average about one-third of the entire design. Thus, the expected amount of decoupling capacitances which must be inserted in the layout of a submicron TEL chip is in accordance with a standard procedure and cannot be counted as additional area overhead with respect to other implementations.

Please note that the high number of combinational stages used in this specific implementation has been intentionally chosen during the synthesis of the 4 × 4 S-Box, which is not optimized with the purpose to simulate the TEL circuit in a pessimistic situation of long critical path and verify the timing constraints in post-layout. As mentioned in previous paragraphs, the S-Box can be synthesized with a smaller number of logic gates in the critical path, leading to a further reduction of δ and area overhead.

6.4 Correlation power analysis of the noise-free traces

Before mounting CPA attacks against the cryptographic circuit, in this section we investigate the distribution of the leakage in the current traces when an ideal measurement setup is adopted, and we compare the result to the case of the SABL circuit. We calculate the correlation between the key guesses and the noise-free traces simulated in Cadence and sampled with a resolution of 10 ps, which corresponds to an unrealistic situation of attack setup with a remarkable time resolution of 100 GSample/s (Fig. 18).

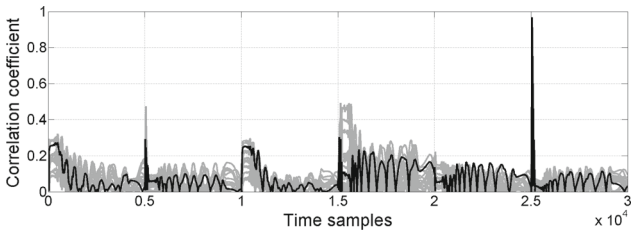

Fig. 18 Correlation coefficient plot of the 256 simulated traces of the TEL circuit as a function of time (no noise and extreme acquisition); correct key is indicated in *bold black line*

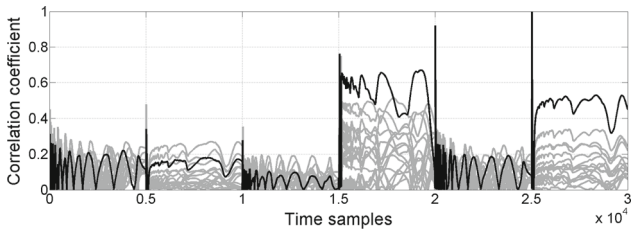

Fig. 19 Correlation coefficient plot of the 256 simulated traces of the SABL circuit as a function of time (no noise and extreme acquisition); correct key is indicated in *bold black line*

As expected, higher values of the correlation coefficient are detected only during the relevant time δ for the effect of the capacitive unbalances. The high-frequency components of the transient leakage have been removed so that the current pattern in the time domain is completely de-correlated from the intermediate value outside the relevant time.

As a fair comparison, we have designed a SABL implementation of the same circuit, with a capacitive mismatch on the internal differential wires equal to the unbalance considered for the TEL circuit. The correlation coefficient has been then calculated (Fig. 19). As seen in Fig. 19, the correlation coefficient of the correct key is high during the second and the third cycle of the elaboration, highlighting a strong sensitiveness of SABL circuit to capacitive mismatches.

In accordance to the plot in Fig. 9, the insertion of a low-pass filter does not help to break the correlation between the instantaneous current and the key because there is a resilient leakage at low frequencies. In other words, the weakness of SABL circuits which has been detected in the frequency domain causes the extension of the information leakage for the entire relevant time $\frac{T_{CK}}{2}$. On the contrary, the TEL circuits, which are based on a dynamic data encoding in a short relevant time, efficiently hide the information visibility in the time domain, forcing the attacker to use more costly measurement setups to detect any leakage.

6.5 CPA attacks with Gaussian noise and limited acquisition rate

As a final step, in this section we perform CPA attacks considering noise and a more realistic measurement setup. According to the Gaussian template model, a normally distributed noise has been considered. To perform attacks in a reasonable time (in the order of some hours), we have neglected the quantization noise due to the AD conversion. The traces have been then sampled using a sampling period of 1 ns to emulate the sampling of a basic oscilloscope with a limited time resolution of 1 GSample/s and a bandwidth in the order of few hundreds of MHz. At the same time, the sampling period has been considered to be not constant because of the random sampling imprecision of a real oscilloscope. The sampling time instants are not strictly multiple of 1ns for the presence of a uniformly distributed random jitter in the acquisition, due to the thermal noise, flicker noise, and shot noise contributions inside the oscilloscope. We have considered a peak-to-peak total jitter of about 100 ps. Furthermore, we have not considered the filtering effect of the probe impedance, being the traces already low-pass filtered by the presence of the decoupling capacitance (i.e. $f_0 = 30$ MHz). These post-processing phases have been implemented using a MATLAB script that we have specifically developed for this testbench and that could be also rearranged for other applications. After the elaboration, the number of points is equal to 100 for each clock cycle (i.e. 300 for a three-clock-cycle elaboration).

For a fixed level of noise, CPA attacks have been mounted with an increasing number of traces, up to 1M. Then, we have calculated the *minimum number of measurements to disclose the key* (*MTD*) as the crossover point in the correlation coefficient plot. According to the definition of MTD given in [28], MTD is the minimum number of traces needed before the correct key is clearly distinguishable. Attack have been executed on TEL and SABL implementations, increasing the number of input traces step by step.

As done for any other countermeasure implementations tested in simulation, a critical value of Gaussian noise σ^{CR}_{noise} can be determined. It is defined as the maximum value of Gaussian noise beyond which an attacker cannot discriminate the correct key with fixed sources in terms of memory and time. Obviously, lower is σ^{CR}_{noise}, higher is the PAAs resistance of the circuit implementation. The noise is given by the sum of electronic and switching noise, and at simulation level it is summed to the noise-free traces. PAAs have been repeated using different values of σ_{noise}, and at each step the MTD is calculated as a function of σ_{noise}.

In Fig. 20 the correlation coefficient plot as a function of the number of input plaintexts is depicted for all the possible keys for the TEL implementation, in the case of $\sigma_{noise} \approx 2{\cdot}10^{-4} > \sigma^{CR}_{noise}$. The correlation coefficient plot as a function of the time samples is showed in Fig. 21. From these figures, it is evident that the attack is not successful with the adopted

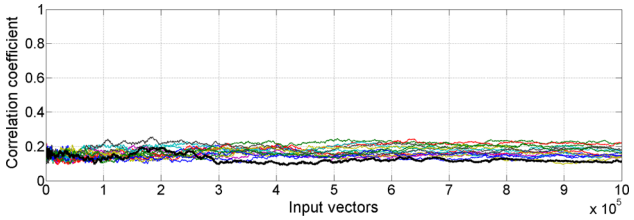

Fig. 20 Correlation coefficient plot as a function of the number of inputs, in the case of unsuccessful attack for the TEL circuit with 1M input vectors (with noise and limited acquisition rate); correct key is indicated in *bold black line*

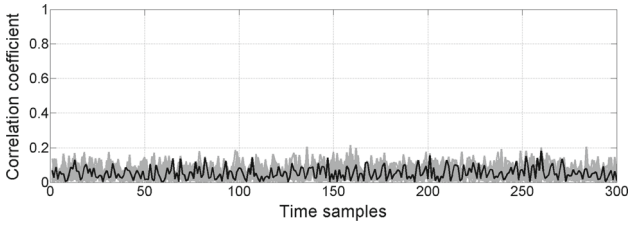

Fig. 21 Correlation coefficient plot as a function of time in the case of unsuccessful attack for TEL circuit with 1M input vectors (with noise and limited acquisition rate); correct key is indicated in *bold black line*

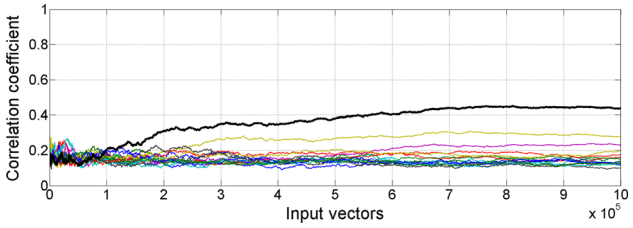

Fig. 22 Correlation coefficient plot as a function of the number of inputs, in the case of successful attack for the SABL circuit with 1M input vectors; (with noise and limited acquisition rate) correct key is indicated in *bold black line*

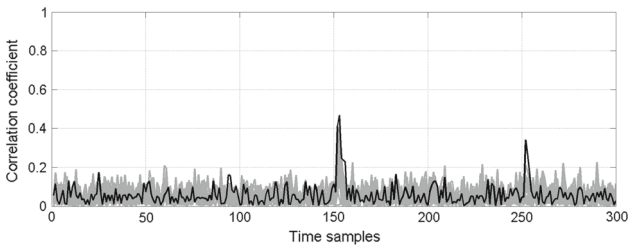

Fig. 23 Correlation coefficient plot as a function of time in the case of successful attack for the SABL circuit with 1M input vectors (with noise and limited acquisition rate); correct key is indicated in *bold black line*

PAAs setup, and the correlation peak detected in the ideal scenario is not more visible.

The same level of noise has been used to mount PAAs against the SABL circuit to have a fair comparison between the two implementations. The correlation coefficient plot as a function of the number of input plaintexts and the correlation coefficient plot as a function of the time samples are showed in Figs. 22 and 23, respectively. From these figures, it is clear that the SABL circuit can be attacked with less than 100k input traces, confirming to have a low resistance to PAAs.

According to the definition of critical noise, we calculate this value for both the TEL and the SABL implementations by repeating PAAs reducing the value of the Gaussian noise step by step. In Fig. 24 the plot of the MTD as a function of noise is reported; the critical noise $\sigma_{\text{noise}}^{\text{CR}}$ represents just the value in the x axis which corresponds to MTD = 1M (i.e., the maximum value of noise beyond which it is not possible

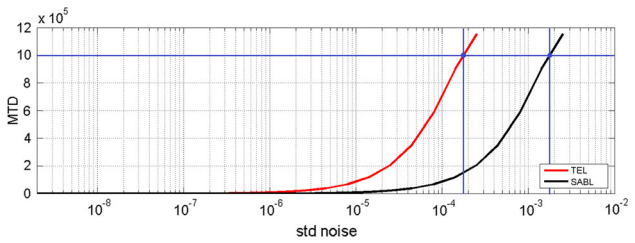

Fig. 24 MTD as a function of the noise standard deviation for TEL and SABL circuits after the PAAs experiments

to distinguish the correct key with the maximum number of traces).

The most important thing that can be deduced from Fig. 24 is that the MTD of the TEL implementation is about 1 order of magnitude higher than the correspondent SABL implementation. With the aim of recovering the correct key of the TEL circuit, the number of input plaintexts must be much higher than 1M input vectors; the critical noise is in the order of about $2 \cdot 10^{-4}$, which represents a relatively low value of noise if compared for example to the values found in simulations for other logic styles [54]. To have a better idea of the level of the noise compared to the intensity of the exploitable signal, in our application the critical noise corresponds to a SNR equal to about 10^{-2}. In practical cases, noise can be even more relevant; therefore, the SNR is typically lower than this value.

The simulation results presented in this section show unequivocally that the TEL data encoding, combined to the design methodology presented in previous section to design the on-chip capacitance, can help to mitigate the electrical mismatches in submicron circuits, enhancing the robustness of the implementation in terms of number of traces for disclosing the key (more than one million) in a PAAs scenario, where the power template of the circuit is perfectly known by the adversary and the correlation coefficient is adopted as statistical distinguisher. If compared to other state-of-the-art logic styles, like RTZ families, which are widely adopted in the context of PAAs, with the same level of noise and number of traces as attack parameters, and under the assumptions that the value of δ is chosen to be smaller than the resolution of the attacker, the security level can be increased at least of an order of magnitude in the real case of mismatched design.

7 A perspective on the effectiveness of EMA attacks against TEL circuits

In this paragraph, we discuss the possibility to adopt TEL circuits also to counteract EMA attacks. We point out that TEL circuits have been explicitly conceived to thwart PAAs. Basically, unlike other implementations TELs aim at allocating the information leakage due to the electrical mismatches

at high frequencies, in accordance to the value of δ, as predicted by the model in Sect. 4, and finally at removing these HF components by low-pass filtering at layout level.

EM leakage can be divided in two main categories: direct emissions and unintentional emissions [55]. Direct emissions are due to the several switching currents inside the circuit, whose amplitude depends on the sharp rising/falling edges of the signals; they have components in the whole frequency spectrum and in general do not depend on the clock frequency. The most dangerous and relevant components are those at low and intermediate frequencies, as argued in [46,56] and confirmed by [48], given that HF components have a lower amplitude because the rising/falling edges of the signals are not ideally zero. On the contrary, unintentional emissions are due to the cross-talk and coupling effects which induce a modulation effect on the near wires, both on amplitude and phase: an example is the clock signal, which is detectable as a signal carrier on each internal signal wire, thus they can be typically detected in the frequency analysis as noise around clock harmonics. In accordance to the architecture under attack, direct emissions and unintentional emission can be more or less predominant. For example, in [55] authors conclude that the most dangerous components are the unintentional emissions generated by the modulation effect of the clock signal carrier propagating on the internal wires, and thus selectively removing the most noisy clock harmonics helps to reduce the EM information leakage. On the contrary, in [48] authors adopt a synchronous schemes and state that the most relevant information leakage is not strictly allocated around the clock harmonics, thus implicitly revealing that direct emissions due to the switching currents inside the circuit do not depend on the clock and can be even more meaningful in EMA attacks.

The hybrid synchronization scheme of TELs, which are actually clock-driven in the discharge phase and asynchronous in the evaluation/postcharge phases, allow to assume that if the evaluation/postcharge phases of each differential pair are strictly allocated within δ, the direct emissions arising from the switching currents are forced to be beyond a specific cutoff frequency, which in turns depends on the value of δ; namely, unlike the case of synchronous logics as RTZ where switching currents are strongly sensitive on the electrical mismatches and have components in the whole frequency spectrum, which are typically exploitable in the low-frequency range, TEL signals are potentially exploitable only using the EM emission in the high-frequency range. However, the insertion of decoupling capacitances directly on the VDD wires of the standard cells in the layout of the chip has the purpose to eliminate these HF components just from the original physical spot where they arise, whereas the LF emissions are flattened thanks to the time-domain data encoding and do not contain relevant information, as visible in the plot of FED in the mismatched case. Furthermore, the coupling effects which generate the unintentional emissions are also prevented thanks to the fact that the capacitances are inserted very close to the TEL standard cells (i.e. on the VDD internal wires), and this allows to reduce the intermodulation effects between near wires.

Even if EMA attacks have not been still mounted against TELs, our intuition is that the level of security of a TEL circuit against EMA attacks is reasonably at least not lower than the level of security of the same circuit implemented using a standard RTZ protocol. The distribution of the FED in the presence of electrical mismatches highlights that TEL circuits eliminate the information leakage at low frequency where EMA attacks are more dangerous and prevent intermodulation among adjacent wires using on-chip decaps, whereas RTZ logics fail at doing so. The investigation of FED confirms the intuition that the information leakage in the frequency domain strongly depends on the implementation, which in turns depends on the logic data protocol, the architecture of the circuit, and the layout.

8 Conclusion

The relevance of this work is double: first, a bi-dimensional hardware countermeasure against PAAs is proposed; then a new design methodology, based on the analysis of the frequency distribution of the leakage of the current traces, is presented. The first important result is that TEL circuits overcome standard synchronous DPLs thanks to their hybrid logic data encoding, which makes this logic family intrinsically tolerant to the electrical mismatches, always present in submicron circuits, and consequently more resistant against PAAs. A back-end optimization is required to remove the high-frequency components directly at layout level, but it can be easily done by the EDA tool during the digital design flow, without requiring a sub-micrometric precision as required for other techniques [22,27,28] or other additional efforts.

Anyway, TEL circuits are perfectly compatible for being implemented also together with one of these techniques for very high secure processors, at the expenses of the design complexity. Furthermore, this work proves that a frequency leakage analysis is fundamental already during the design steps, considering that novel SCAs like *electromagnetic analysis attacks* (*EMAs*) rely on the data dependence in the frequency spectrum and are particularly critical also for DPLs. Future research must be addressed toward the design of robust circuit templates for implementing the TEL data encoding, both for ASIC design and FPGA applications, and toward the proposal of more precise power models which take into account time and frequency leakage at the same time, even adopting information theoretic metrics [38,54]. Furthermore, the TEL-featured cryptographic circuit analyzed

in this work will be manufactured as an ASIC for validating the power analysis resistance.

Appendix A: Analysis of the operating frequency regions of a TEL circuit as a function of δ

In this paragraph, we calculate the condition on the maximum clock frequency of a TEL circuit. It will be shown that the TEL data encoding provides an enhanced level of security with respect to an RTZ implementation, without impacting functionality.

Let us suppose that the waveforms in Fig. 25 represent the differential signals at the input/output of a TEL combinational path. The value $T_{\mathrm{CK-Q}}$ represents the delay between the clock and the asserted signal at the output of the flip-flop in [42]. Assuming that the waveforms (O1, O2) in Fig. 25 are the signals at the output of the critical path, the maximum frequency can be calculated in this way. When the clock period is reduced, if $T_{\mathrm{CK}} < 2 \cdot (T_{\mathrm{CK-Q}} + \delta + T_2) = T'_{\mathrm{MAX}}$, the discharge falling edge of the clock comes first than the rising edge of the non-asserted signal O2 and the postcharge phase is lost: in this case, the circuit continues working but with an RTZ-like data encoding on the signal (O1, O2) and a degraded margin of security. When the clock period is decreased to such an extent that the time margin on the asserted rising edge is less than t_{SUP}, the flip-flop at the output of the critical is not able to recognize the logic data, and the functionality of the circuit is compromised. Therefore, the minimum clock period which ensures the correct functionality is given by the relation $T_{\mathrm{CK}} < 2 \cdot (T_{\mathrm{CK-Q}} + T_1 + t_{\mathrm{SUP}}) = T_{\mathrm{MAX}}$, which does not depend on δ and is just the same relation occurring in a conventional RTZ pipeline.

In summary, once the nominal δ is fixed, three different working regions can be distinguished, and the value of the frequency is

$$f_{\mathrm{CK}} \begin{cases} < f'_{\mathrm{MAX}} & \text{TEL working} \\ \in [f'_{\mathrm{MAX}}, f_{\mathrm{MAX}}] & \text{RTZ working} \\ > f_{\mathrm{MAX}} & \text{no working,} \end{cases} \tag{20}$$

where

$$f'_{\mathrm{MAX}} = \frac{1}{2 \cdot (T_{\mathrm{CK-Q}} + \delta + T_2)} = \frac{1}{2 \cdot (T_{\mathrm{CK-Q}} + T_1 + \delta_{\mathrm{OUT}})} \tag{21}$$

$$f_{\mathrm{MAX}} = \frac{1}{2 \cdot (T_{\mathrm{CK-Q}} + T_1 + t_{\mathrm{SUP}})} \tag{22}$$

where $\delta > \delta_{\mathrm{OUT}} > t_{\mathrm{SUP}}$ and $T_1 > T_2$ to meet the timing constraints.

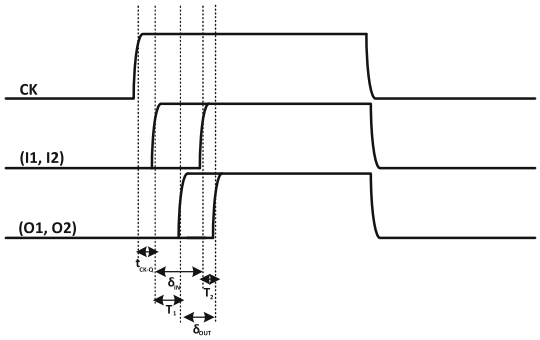

Fig. 25 Timing of the signals at the input/output of a generic combinational path

It is clear that the maximum working frequency of the TEL encoding has a direct dependance on the security margin of the circuit due to the presence of δ, but it does not impact directly the functionality of the chip. In other words, the presence of δ provides the designer with an additional degree of freedom to enhance the level of security of the chip, without impacting the maximum working frequency with respect to a RTZ implementation with the same number of N logic gates in the critical path (i.e. f_{max} in a TEL implementation is very similar to RTZ, because it depends on the propagation time T_1 of the asserted signals and on the setup time of the flip-flop, but not on δ). As discussed in Sect. 3.5, the values δ_{MIN}, t_{SUP}, $t_{\mathrm{CK-Q}}$ and $T_{1,2}$ are technology dependent: in more scaled technologies, it is expected that δ_{MIN} and the propagation times of the logic cells scale down to some tenths of picoseconds, and this is compatible with operating frequencies in the order of some GHz. This value is in accordance to the typical operating frequencies of modern general-purpose processors; thus, the TEL data encoding can be efficiently adopted also for high-performance cryptoprocessors with an expected increase of area overhead.

Appendix B: Calculation of $\Delta S(f)$ using a Gaussian model

For the sake of simplicity, let us consider the current trace of a TEL inverter gate (Fig. 2) during a clock cycle. In accordance to the leakage model presented in Table 2, the current trace of the cell is composed of three peaks: the first peak occurs at the falling edge of the clock at the beginning of the discharge phase; the second peak occurs after the rising edge of the clock at the beginning of the evaluation phase, just at the rising edge of the asserted signal; the third peak occurs at the rising of the non-asserted (delayed) signal, after a time interval equal to δ.

In presence of (0, 1) as input data (i.e. a logic 0 in the static domain), a specific current pattern is assigned; on the contrary, in presence of (1, 0) as input data (i.e. a logic 1

in the static domain) a different current pattern is assigned. The differences between the current patterns can be detected only during the evaluation and postcharge phases, when the switching current adsorbed by the power supply line is dependent on the value of the output capacitance. During this semi-period, the clock signal is at V_{DD}.

At this point, we consider only the portion of the current traces during the evaluation and the postcharge phases, where a logic gate is more sensitive on mismatches, as seen by calculating the standard deviation in Fig. 6. We do the assumption that the current peaks in evaluation and postcharge can be approximated as two Gaussian pulses; then, the current trace during this semi-period can be modeled as the sum of these two Gaussian peaks. If we call $s_0(t)$ and $s_1(t)$ the current trace in the case of input (0, 1) and (1, 0), respectively, we have

$$s_0(t) = I_0 \cdot \mathrm{e}^{-\frac{t^2}{2\sigma_0^2}} + I_1 \cdot \mathrm{e}^{-\frac{(t-\delta)^2}{2\sigma_1^2}} \tag{23}$$

$$s_1(t) = I_1 \cdot \mathrm{e}^{-\frac{t^2}{2\sigma_1^2}} + I_0 \cdot \mathrm{e}^{-\frac{(t-\delta)^2}{2\sigma_0^2}}. \tag{24}$$

The origin of the t axis has been set to the center of the first pulse, which is associated to the asserted signal. Then, the other peak one is centered on δ. I_0 (I_1) and σ_0 (σ_1) are the amplitude and the standard deviation of the current peak which charges the capacitance C_{L1} (C_{L2}): higher the output capacitance, higher the amplitude and the standard deviation of the pulse. Applying the linearity property and considering that the Fourier transform of a Gaussian pulse is again a Gaussian pulse with an inverse standard deviation, we obtain

$$\begin{aligned} S_0(f) = {} & I_0\sqrt{2\pi}\,\sigma_0\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_0 f)^2} \\ & + I_1\sqrt{2\pi}\,\sigma_1\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_1 f)^2}\cdot\mathrm{e}^{-j2\pi\delta f} \end{aligned} \tag{25}$$

$$\begin{aligned} S_1(f) = {} & I_1\sqrt{2\pi}\,\sigma_1\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_1 f)^2} \\ & + I_0\sqrt{2\pi}\,\sigma_0\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_0 f)^2}\cdot\mathrm{e}^{-j2\pi\delta f}. \end{aligned} \tag{26}$$

The difference $\Delta S(f)$ of the Fourier transforms of the two current traces is

$$\begin{aligned} \Delta S(f) &= S_1(f) - S_0(f) \\ &= I_1\sqrt{2\pi}\,\sigma_1\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_1 f)^2}\cdot(1-\mathrm{e}^{-j2\pi\delta f}) \\ &\quad - I_0\sqrt{2\pi}\,\sigma_0\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_0 f)^2}\cdot(1-\mathrm{e}^{-j2\pi\delta f}) \\ &= \sqrt{2\pi}\,(1-\mathrm{e}^{-j2\pi\delta f})\cdot(I_1\sigma_1\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_1 f)^2} \\ &\quad - I_0\sigma_0\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_0 f)^2}). \end{aligned} \tag{27}$$

Re-arranging this equation, we obtain

$$\begin{aligned} \Delta S(f) = {} & 2j\sqrt{2\pi}\,\cdot\mathrm{e}^{-j\pi\delta f}\cdot\mathrm{sen}(\pi\delta f)\cdot \\ & \cdot\left(I_1\sigma_1\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_1 f)^2} - I_0\sigma_0\,\mathrm{e}^{-(\pi\sqrt{2}\sigma_0 f)^2}\right). \end{aligned} \tag{28}$$

We point out that more accurate models of the current peaks in evaluation and postcharge would lead to similar results. For example, assuming that the peaks can be modeled as triangle waveforms, in Eq. 28 a term which takes into account all the lobes of a sinc function (i.e. the Fourier transform of a triangle) is also present.

Appendix C: Variability of δ in a TEL circuit

In this paragraph, a brief discussion about the variability of the parameter δ in TEL pipeline is provided. As discussed in the paper, the most interesting point of TEL circuits is in the fact that they allow to turn a security vulnerability into an implementation issue. Namely, once the TEL data encoding is generated at the beginning of a micropipeline, the only parameter which must be controlled is the fluctuation of δ along the propagation paths to meet the security requirements and at the same time guarantee functionality.

A possible circuit template for a TEL architecture is the *delay-based dual-rail precharge logic* (*DDPL*), presented in [19]. An improved version is proposed in [40] and adopted in this work, and a possible flip-flop implementation is presented in [42].

In [40], a set of optimized combinational gates is presented: any unpredictable variability of δ due to the timing mismatches of the logic gates is solved directly at gate level, by introducing some redundancy in the propagation paths of the cells. This way the delay at the output of a combinational circuit is always lower than the nominal value δ, chosen to address the security issues. Furthermore, the mismatch variations among adjacent transistors are expected to have a low impact on the overall impedance unbalance, where interconnect wire capacitances are dominant.

In [42], authors propose an efficient solution to generate the delay-based differential data encoding using a current starved inverter. This method is based on the presence of a delayed clock signal, which is generated by controlling the polarization of the starved inverter through a global static signal. In accordance to the discussion in [42], there are several possibilities to generate a fixed and stable delay δ along a circuit, so that process–voltage–temperature (PVT) variations may have a low impact on the variability of δ and then on the functionality of the circuit. For example, bandgap voltage references [57] may be inserted at the converter stages to guarantee that the polarization of the delay element is kept as stable as possible with PVT variations. A possible digital solution is adopting a voltage-controlled delay-locked loop (DLL), which has the advantage to generate a global fixed voltage to have a precise output delay.

Anyway the design and optimization of a robust and secure circuit implementation of TEL circuits are beyond the objective of this work, and represent a possible future improvement

to assess the security level and robustness of TEL also in a semi-invasive or active attack scenario, where an attacker can directly interact with the device (e.g. changing the operating working conditions, like temperature or power supply voltage).

References

1. Kocher, P.C.: Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems. In: Advances in Cryptology—CRYPTO'96, pp. 104–113. Springer, Berlin (1996)
2. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Advances in Cryptology—CRYPTO'99, pp. 388–397. Springer, Berlin (1999)
3. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Cryptographic Hardware and Embedded Systems—CHES 2004, pp. 16–29. Springer, Berlin (2004)
4. Sun, S., Yan, Z., Zambreno, J.: Experiments in attacking FPGA-based embedded systems using differential power analysis. In: IEEE International Conference on Electro/Information Technology, 2008, EIT 2008, pp. 7–12. IEEE, New York (2008)
5. Shamir, A.: Protecting smart cards from passive power analysis with detached power supplies. In: Cryptographic Hardware and Embedded Systems—CHES 2000, pp. 71–77. Springer, Berlin (2000)
6. Veyrat-Charvillon, N., Medwed, M., Kerckhof, S., Standaert, F.X.: Shuffling against side-channel attacks: a comprehensive study with cautionary note. In: Advances in Cryptology—ASIACRYPT 2012, pp. 740–757. Springer, Berlin (2012)
7. Plos, T., Hutter, M., Herbst, C.: Enhancing side-channel analysis with low-cost shielding techniques. In: Proceedings of Austrochip, pp. 90–95 (2008)
8. Akkar, M.L., Bevan, R., Dischamp, P., Moyart, D.: Power analysis, what is now possible. In: Advances in Cryptology—ASIACRYPT 2000, pp. 489–502. Springer, Berlin (2000)
9. Bucci, M., Luzzi, R., Guglielmo, M., Trifiletti, A.: A countermeasure against differential power analysis based on random delay insertion. In: IEEE International Symposium on Circuits and Systems, 2005, ISCAS 2005, pp. 3547–3550. IEEE, New York (2005)
10. May, D., Muller, H.L., Smart, N.P.: Non-deterministic processors. In: Information Security and Privacy, pp. 115–129. Springer, Berlin (2001)
11. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Investigations of power analysis attacks on smartcards. In: USENIX Workshop on Smartcard Technology, vol. 17, p. 17 (1999)
12. Danis, A.U., Ors, B.: Differential power analysis attack considering decoupling capacitance effect. In: European Conference on Circuit Theory and Design, 2009, ECCTD 2009, pp. 359–362. IEEE, New York (2009)
13. O'Flynn, C., Chen, Z.: A case study of side-channel analysis using decoupling capacitor power measurement with the OpenADC. In: Foundations and Practice of Security, pp. 341–356. Springer, Berlin (2013)
14. Rakers, P., Connell, L., Collins, T., Russell, D.: Secure contactless smartcard ASIC with DPA protection. IEEE J Solid-State Circuits **36**(3), 559–565 (2001)
15. Ratanpal, G.B., Williams, R.D., Blalock, T.N.: An on-chip signal suppression countermeasure to power analysis attacks. Trans. Dependable Secure Comput. **1**(3), 179–189 (2004)
16. Muresan, R., Gregori, S.: Protection circuit against differential power analysis attacks for smart cards. IEEE Trans. Comput. **57**(11), 1540–1549 (2008)
17. Tiri, K., Akmal, M., Verbauwhede, I.: A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. In: Proceedings of the 28th European Solid-State Circuits Conference, 2002, ESSCIRC 2002. pp. 403–406. IEEE, New York (2002)
18. Bucci, M., Giancane, L., Luzzi, R., Trifiletti, A.: Three-phase dual-rail pre-charge logic. In: Cryptographic Hardware and Embedded Systems-CHES 2006 (pp. 232–241). Springer, Berlin, Heidelberg (2006)
19. Bucci, M., Giancane, L., Luzzi, R., Scotti, G., Trifiletti, A.: Delay-based dual-rail precharge logic. Very Large Scale Integr. (VLSI) Syst. IEEE Trans. **19**(7), 1147–1153 (2011)
20. Hwang, D.D., Tiri, K., Hodjat, A., Lai, B.C., Yang, S., Schaumont, P., Verbauwhede, I.: AES-based security coprocessor IC in 0.18-CMOS with resistance to differential power analysis side-channel attacks. Solid-State Circuits IEEE J. **41**(4), 781–792 (2006)
21. Popp, T., Mangard, S.: Masked dual-rail pre-charge logic: DPA-resistance without routing constraints. In: CHES 2005, pp. 172–186. Springer, Berlin, Heidelberg (2005)
22. Tiri, K., Verbauwhede, I.: Place and route for secure standard cell design. In: Smart Card Research and Advanced Applications VI, pp. 143–158. Springer, US (2004)
23. Kulikowski, K.J., Karpovsky, M.G., Taubin, A.: Power attacks on secure hardware based on early propagation of data. In: IOLTS, vol. 6, pp. 131–138 (2006)
24. Suzuki, D., Saeki, M.: Security evaluation of DPA countermeasures using dual-rail pre-charge logic style. In: Cryptographic Hardware and Embedded Systems—CHES 2006, pp. 255–269. Springer, Berlin, Heidelberg (2006)
25. Gierlichs, B.: DPA-Resistance Without Routing Constraints?. Springer, Berlin, Heidelberg (2007)
26. Schaumont, P., Tiri, K.: Masking and dual-rail logic don't add up. Springer, Berlin, Heidelberg (2007)
27. Guilley, S., Hoogvorst, P., Mathieu, Y., Pacalet, R.: The "backend duplication" method. In: Cryptographic Hardware and Embedded Systems—CHES 2005, pp. 383–397. Springer, Berlin, Heidelberg (2005)
28. Tiri, K., Hwang, D., Hodjat, A., Lai, B.C., Yang, S., Schaumont, P., Verbauwhede, I.: Prototype IC with WDDL and differential routing-DPA resistance assessment. In: Cryptographic Hardware and Embedded Systems—CHES 2005, pp. 354–365. Springer, Berlin, Heidelberg (2005)
29. Giorgetti, J., Scotti, G., Simonetti, A., Trifiletti, A.: Analysis of data dependence of leakage current in CMOS cryptographic hardware. In: Proceedings of the 17th ACM Great Lakes symposium on VLSI, pp. 78–83. ACM (2007)
30. Lin, L., Burleson, W.: Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems. In: IEEE International Symposium on Circuits and Systems, 2008. ISCAS 2008, pp. 252–255. IEEE (2008)
31. Alioto, M., Giancane, L., Scotti, G., Trifiletti, A.: Leakage power analysis attacks: a novel class of attacks to nanometer cryptographic circuits. Circuits Syst. I: Reg. Papers IEEE Trans. **57**(2), 355–367 (2010)
32. Alioto, M., Bongiovanni, S., Djukanovic, M., Scotti, G., Trifiletti, A.: Effectiveness of leakage power analysis attacks on DPA-resistant logic styles under process variations. IEEE Trans Circuits Syst. I: Regul Pap **61**(2), 429–442 (2014)
33. Moradi, A.: Side-channel leakage through static power—should we care about in practice? IACR Cryptology ePrint Archive 25 (2014)
34. Kamel, D., Renauld, M., Flandre, D., Standaert, F.X.: Understanding the limitations and improving the relevance of SPICE simulations in side-channel security evaluations. J. Cryptogr. Eng. **4**(3), 1–9 (2014)

35. Barenghi, A., Pelosi, G., Regazzoni, F.: Simulation-time security margin assessment against power-based side channel attacks. IACR Cryptology ePrint Archive, online report number 307. https://eprint.iacr.org/2014/307/20140430:210914 (2014). Accessed 30 April 2014
36. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards, vol. 31. Springer, New York (2008)
37. Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In: Cryptographic Hardware and Embedded Systems—CHES 2002, pp. 13–28. Springer, Berlin, Heidelberg (2003)
38. Standaert, F.X., Malkin, T.G., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In: Advances in Cryptology—EUROCRYPT 2009, pp. 443–461. Springer, Berlin, Heidelberg (2009)
39. Renauld, M., Standaert, F.X., Veyrat-Charvillon, N., Kamel, D., Flandre, D.: A formal study of power variability issues and side-channel attacks for nanoscale devices. In: Advances in Cryptology—EUROCRYPT 2011, pp. 109–128. Springer, Berlin, Heidelberg (2011)
40. Bongiovanni, S., Scotti, G., Trifiletti, A.: Security evaluation and optimization of the delay-based dual-rail pre-charge logic in presence of early evaluation of data. In: Proceedings of SECRYPT, pp. 183–194 (2013)
41. Tiri, K., Verbauwhede, I.: A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In: Proceedings of the Conference on Design, Automation and Test in Europe, vol. 1, p. 10246. IEEE Computer Society (2004)
42. Bongiovanni, S., Olivieri, M., Scotti, G., Trifiletti, A.: A flip-flop implementation for the DPA-resistant delay-based dual-rail precharge logic family. In: Mixed Design of Integrated Circuits and Systems (MIXDES), 2013 Proc. of the 20th International Conference, pp. 163–168. IEEE (2013)
43. Gladman, B.R., Simpson, S.: Partially optimized Serpent Boxes boolean functions. Brian Gladman's Home Page. http://brgladman.org/oldsite/cryptography_technology/aesr1/f_box.h (1998). Accessed 17 Dec 1998
44. Shastry, P.V.S., Agnihotri, A., Kachhwaha, D., Singh, J., Sutaone, M.S.: A combinational logic implementation of S-box of AES. In: Circuits and Systems (MWSCAS), 2011 IEEE 54th International Midwest Symposium, pp. 1–4. IEEE (2011)
45. Guilley, S., Sauvage, L., Hoogvorst, P., Pacalet, R., Bertoni, G.M., Chaudhuri, S.: Security evaluation of WDDL and SecLib countermeasures against power attacks. Comput. IEEE Trans. **57**(11), 1482–1497 (2008)
46. Mateos, E., Gebotys, C.H.: A new correlation frequency analysis of the side channel. In: Proceedings of the 5th Workshop on Embedded Systems Security, p. 4. ACM (2010)
47. Schimmel, O., Duplys, P., Boehl, E., Hayek, J., Bosch, R., Rosenstiel, W.: Correlation power analysis in frequency domain. In: COSADE, 4–5 Feb 2010 (2010)
48. Tiran, S., Ordas, S., Teglia, Y., Agoyan, M., Maurine, P.: A model of the leakage in the frequency domain and its application to CPA and DPA. J. Cryptogr. Eng. **4**(3), 1–16 (2014)
49. Anderson, R., Biham, E., Knudsen, L.: Serpent: A Proposal for the Advanced Encryption Standard. NIST AES Proposal, p. 174 (1998)
50. Alioto, M., Bongiovanni, S., Scotti, G., Trifiletti, A.: Leakage power analysis attacks against a bit slice implementation of the Serpent block cipher. In: MIXDES, 19–21 June 2014 (2014)
51. Gilbert Goodwill, B.J., Jaffe, J., Rohatgi, P.: A testing methodology for side-channel resistance validation. In: NIST Non-Invasive Attack Testing Workshop (2011)
52. Durvaux, F., Standaert, F.X., Veyrat-Charvillon, N.: How to certify the leakage of a chip? In: Advances in Cryptology—EUROCRYPT 2014, pp. 459–476. Springer, Berlin, Heidelberg (2014)
53. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual information analysis. In: Cryptographic Hardware and Embedded Systems—CHES 2008, pp. 426–442. Springer, Berlin, Heidelberg (2008)
54. Macé, F., Standaert, F.X., Quisquater, J.J.: Information Theoretic Evaluation of Side-Channel Resistant Logic Styles. Springer, Berlin, Heidelberg (2007)
55. Agrawal, D., Archambeault, B., Rao, J.R., Rohatgi, P.: The EM side-channel (s). In: Cryptographic Hardware and Embedded Systems—CHES 2002, pp. 29–45. Springer, Berlin, Heidelberg (2003)
56. Meynard, O., Réal, D., Guilley, S., Flament, F., Danger, J.L., Valette, F.: Characterization of the electromagnetic side channel in frequency domain. In: Information Security and Cryptology, pp. 471–486. Springer, Berlin, Heidelberg (2011)
57. Chen, H.M., Huang, C.L., Chang, R.C.: A new temperature-compensated CMOS bandgap reference circuit for portable applications. In: Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium, p. 4. IEEE (2006)