Design and analysis of secure emerging crypto-hardware using HyperFET devices

Ignacio M. Delgado-Lozano, Erica Tena-Sánchez, Juan Núñez, and Antonio J. Acosta

Abstract—The emergence of new devices to be used in low-power applications are expected to reach impressive performance compared to those obtained by equivalent CMOS counterparts. However, when used in lightweight security applications, these emerging paradigms are required to be reliable and safe enough during the task of protecting important and valuable data. In this work, the usage of HyperFET devices for security applications has been analyzed and new paradigms for enhancing security against Power Analysis attacks have been developed for the first time. To perform this analysis, classical dual-precharge logic primitives implemented with 14nm FinFET have been upgraded to incorporate HyperFET devices. The proposed primitives incorporating HyperFETs, as well as a 4-bit Substitution box of PRIDE algorithm as demonstrative example, have been designed and simulated using predictive models. Simulation-based Differential Power Analysis attacks demonstrate high improvements in security levels in a x25 factor at least, with negligible degradation in performance. This first approach could be easily extensible to other ciphers or crypto-circuits, where the incorporation of HyperFET devices will enhance security for most future applications.

Index Terms—VLSI design of cryptographic circuits, side-channel attacks (SCAs), information security, low-power, dual precharge logic (DPL), substitution box (Sbox), sense amplifier based logic (SABL), emerging technologies, FinFET, HyperFET.

1 Introduction

NOWADAYS, with the dizzying advance of new technologies in different domains and the demand for increasingly compact and low-power devices for IoT, such as wearable or e-health devices, new paradigms are emerging that the scientific community must address. These devices not only have to comply with the hard power restrictions imposed on them, but they also need to keep the sensitive information they handle safe from possible attackers.

These crypto-hardware devices make use of mathematically secure algorithms to keep private information secure, but due to their physical implementation, these devices leak side-channel information that can be used by third-parties to reveal private data through Side-Channel Attacks (SCA) [1]–[4] that exploit leakage sources as power consumption [2], delay [1] or electromagnetic radiation [3]. Among the wide variety of SCAs, Differential Power Analysis (DPA) attacks are the most extended ones due to their simplicity, the minimal equipment required and the effectiveness, being based in the well known fact that the power consumption in a logic circuit is dependent on the data being processed.

In order to address the complexity of these designs covering both area/performance and security constraints, design and analysis methods must be adopted at different levels of abstraction. The countermeasures against DPA attacks can be applied going from the algorithm down to the physical level; following masking or hiding strategies depending on the used technique. Masking techniques [4]–[7] seek to break the relationship of power consumption with the processed data by masking critical operations of the algorithm using a secret random mask. In the case of hiding techniques [8]–[12], this dependence is broken by making the power consumption of the algorithm equal or random regardless of the data being processed.

The masking and hiding techniques applied at the algorithm level are not automatable since their dependence on the specific algorithm used, so when facing a new design, it would be necessary to redesign the algorithm and include the specific countermeasures at that level of abstraction. However, countermeasures applied at the gate level are independent of the algorithm used. Once the secure cell library is fully developed, following a correct place and route process we can obtain secure implementations following the same design methodology regardless of the algorithm used. In the case of gate-level hiding countermeasures, one of the most studied proposals use Dual-Precharge Logic (DPL) styles, designed to carry out one computation in each clock cycle regardless the input conditions and getting the same power consumption in every cycle.

Nevertheless, DPL styles have some associated penalties in terms of power consumption, delay and area due to the increase in the number of transistors used to construct logic gates. They need to implement the logic that alternates between pre-charge and evaluation phases, generates both the output and its complementary value, thus requiring differential internal branches to be symmetrical [8].

The scientific community is addressing different strategies aiming to avoid the existing bottlenecks associated with the scaling of CMOS technologies to deep nanometric dimensions, which is causing certain challenges that impact integrated circuit design. The increase in both static power consumption due to leakage currents and power density

• *I.M. Delgado-Lozano was with Universidad de Sevilla and the Instituto de Microelectrónica de Sevilla when this paper was first submitted and now is with Tampere University, Tampere, FINLAND, 33720. E. Tena-Sánchez, J. Núñez and A.J. Acosta are with the Universidad de Sevilla and the Instituto de Microelectrónica de Sevilla (CNM-CSIC), Seville, SPAIN, 41092.*
E-mail: ignacio.delgadolozano@tuni.fi, {erica, jnunez, acojim}@imse-cnm.csic.es

Manuscript received April 19, 2005; revised August 26, 2015.

per area are two of the main challenges to be faced in the short term, without forgetting other limitations such as the increase in interconnect capacitances, the impact of variability and modeling difficulties. In order to be able to tackle the demanding restrictions in terms of power consumption and performance of the new applications that dominate the market, three main strategies emerge.

First, the strategy known as "More Moore" pursues the dimensional and functional scaling of CMOS technologies beyond what Moore's Law allows. To achieve this, new materials and device concepts such as SOI (silicon on insulator) or strained silicon, must be used. Within this last category, the FinFETs stand out, indicated to reduce leakage currents and operate with lower polarization voltages than planar CMOS. Secondly, technologies known as "More than Moore (MtM)" have emerged in recent years as an alternative for developing novel non-conventional functionalities and, although they may be based on silicon technologies, they do not have to be scaled according to Moore's Law. Finally, different emerging device technologies, known as "Beyond CMOS" [13], are being explored for information processing and micro-architectures that implement existing or new functionalities, allowing the scaling of integrated circuits and the increase of their performance beyond what "More Moore" technologies achieve. The idea of using "beyond CMOS" devices drawn away from conventional technologies, and frequently from silicon is a challenge, not only for generic processing purposes, but for security applications. Therefore, it is necessary to assess the role of these new transistors, for instance steep-slope devices such as TFETs, that have already been analyzed for different applications, including secure cryptographic implementations [14], [15]. However, there are very few works focused on the study of other new steep slope devices as it is the case of HyperFET, and as far as we know, none dedicated to security applications.

The main contributions of the paper are:

- Analysis of suitability of HyperFET devices for secure applications.
- Design of logic primitives in a DPL-based DPA-resistant Sense-Amplifier Based Logic (SABL) style, using FinFET and HyperFET devices.
- Characterization of a PRIDE substitution box (Sbox-4) as a case study through electrical simulations on predictive models in both technologies.
- Evaluation of security via simulation-based DPA attacks, showing impressive security improvement for the HyperFET proposal.

The organization of this paper is as follows: In Section 2, it is presented the previous work concerning the logic styles against DPA attacks and emerging technologies for security applications. Section 3 presents the operation principle of emerging HyperFET devices, including the design of DPL-SABL logic primitives incorporating HyperFET devices. Section 4 shows the design of PRIDE Sbox-4 blocks as case study, and the detailed DPA attacks on the proposals, Section 5 includes the analysis of obtained results in terms of performance and security for the carried out implementations. To end, in Section 6 we summarize the conclusion of this work and establish the future lines of research.

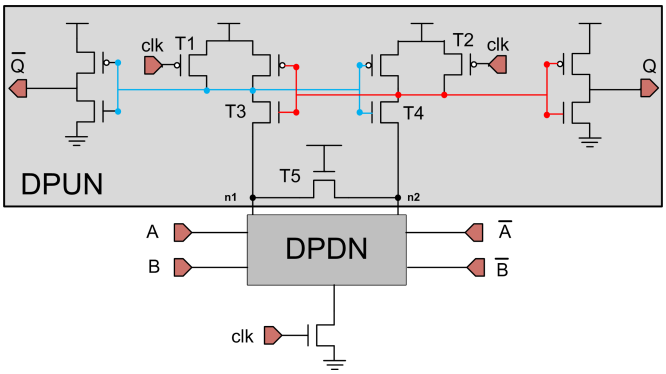


Fig. 1. Original SABL-DPL structure [10].

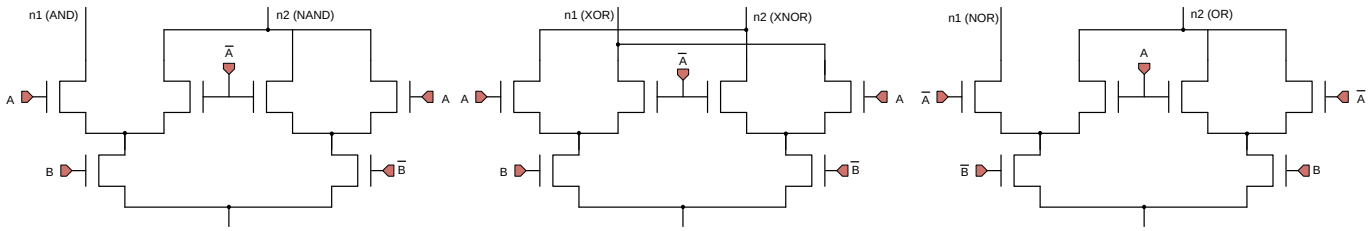
2 Previous Works

2.1 Logic Styles against DPA Attacks

Since Kocher et al. [2] demonstrated that DPA attacks are able to recover the secret key of a cryptosystem with a high rate of success, a lot of countermeasures have been proposed aiming to withstand this kind of attacks, keeping secure the system to be protected. From the very beginning, standard CMOS logic style showed a large dependence between power consumption and data being encrypted, making this logic style not suitable for security applications. Given this circumstance the scientific community developed new logic styles that allow a lower dependence between processed data and power consumption, leading to larger levels of robustness against DPA attacks.

One of these logic families, known as Dual Precharge-Logic (DPL), works with two operating phases in order to obtain the same power consumption in every clock cycle, working in each transition with the true and the complemented value. First, during the precharge phase, both, true and complemented outputs, are forced to the same value. During the evaluation, the logic computation is made depending on the inputs and the logic function implemented, leading to only one switch at the output. This leads to a constant number of switches per clock cycle, which facilitates that a cryptographic system obtains the same power consumption in every transition. Among the DPL styles, the best results in terms of security are obtained by full-custom solutions based on differential logic styles that exploit their symmetry to assure identical power consumptions, regardless the values at the output, since both the true and the complemented value are simultaneously generated. [10], [16]–[19]

The proposals that have shown more interesting properties are Dynamic Current Mode Logic (DyCML) [16], Low-Swing Current Mode Logic (LSCML) [17], Three-Phased Dual-Rail (TDPL) [18], Delay-Based Dual-Rail Precharge Logic (DDPL) [19] and Sense Amplifier Based Logic (SABL) [10], which will be used along this work due to its efectiveness when compared with the rest of DPL alternatives [8]. SABL logic style could be splitted into a differential pull-up network (DPUN) which establishes precharge and evaluation phases and a differential pull-down network (DPDN) which performs the needed logic operation. The DPUN-SABL structure, presented in Fig. 1 operates as follows: T1 and T2 transistors are ON in the precharge phase, when



(a) AND/NAND (b) XOR/XNOR (c) OR/NOR

Fig. 2. DPDN structures for a) AND/NAND, b) XOR/XNOR and c) OR/NOR gates.

clk=0. Then, nodes n1 and n2 will be set to 1, forcing the outputs $Q\bar{Q}$ = 00, due to output inverters. When clk is set to 1, the evaluation phase begins, and transistors T3 and T4 connected to nodes n1 and n2, are grounded through a discharge path in the DPDN block and T5 between n1 and n2, which is always ON, are able to yield the result based uniquely on the logic function generated by the DPDN block and the input values. Some of the key aspects to assure the design of safe DPL gates are the following: i) to use the same amount of charge in every transition; ii) a fully symmetrical DPDN block independent from the input values, i.e having all the paths from n1 and n2 to ground the same transistor count and equivalent RC values, leading to constant delay; and iii) all the internal nodes of DPDN block have to be connected to n1 or n2. The implementation of DPDN blocks, depending on the logic function implemented, is shown in Fig.2. The full symmetry in DPUN block and the fact that the outputs of DPDN are not directly connected to the output inverters in DPUN block make SABL logic style appropriated against DPA attacks, and superior to other alternatives [8].

2.2 Emerging Technologies for Security Applications

As a result of technology scaling, it has been shown that CMOS technologies present some weaknesses in terms of power density and energy resources given the unfeasibility to obtain reduced threshold voltages, without inducing important leakage currents. In a world where resource constraint applications are increasingly usual, as it is the case of portable and lightweight cryptography with low-power consumption implementations, emerging alternatives to CMOS are required to be implemented in the upcoming IoT systems [20], [21].

Recently, new transistor technologies have been developed easing the research on new low-power and safe lightweight implementations. Many of these new devices are able to work as Boolean switches within the framework of classical computing systems while some others propose new characteristics that are apt for disruptive computing applications as non-boolean logic or non-Von Neumann architectures. In this contexts, many tries have been dedicated to design secure circuits and architectures against DPA attacks using several emerging devices [14], [15], [22], [23].

Some authors have focused their efforts in the use of deep nanometric FinFET transistors, as substitute of bulk CMOS, having presented remarkable properties as impressive ON/OFF current ratio and diminished short channel effects. For instance, some proposals [22] have used a back-gate bias randomly adjusted to cause larges quantities of noise aiming to hide the information leakage during the encryption phase, reinforcing the DPA-resilience of the system. Other contributions [23] have consisted of adiabatics FinFET-based circuits that yield to low-power and secure cryptosystems that are able to improve their robutsness against SCAs, through a decreased operation frequency and having as result a reduced instantaneous power consumption. In [24] a comprehensive benchmark of several MOSFET and FinFET dual-rail precharge logic (DPL) cryptographic cell implementations was presented. The results obtained suggest that the use of FinFET-based implementations improves the performance figures given by their MOSFET-based counterparts, but achieving worst figures of security.

Tunnel FET devices [25], [26] present a symmetrical doping structure, similar to a gated p-i-n diode working under reverse bias polarization. These devices are able to reach steep slopes ($<$ 60mV/dec) working with lower supply voltages when compared with equivalent nanometric CMOS nodes. The distinctive features of steep-slope devices can be exploited efficiently in the hardware security domain to provide high-level circuit protection with extremely low power consumption. Although the design of lightweight cryptographic applications using steep-slope devices is not very extensive, TFET-based secure cells have been already reported. In this sense, several implementation of low-voltage current-mode logic (CML) circuits [15], [27]–[29] exhibit significant advantages in terms of power consumption, area and security metrics compared to their CMOS counterparts.

As an alternative to the development of new transistor concepts, HyperFETs have been recently proposed, in which a phase transition material (PTM), exhibiting insulator-metallic transitions, is connected to the source of a FET transistor. The abrupt phase transitions of the PTM are used as a mechanism to increase the ratio between the ON and the OFF current of the transistor, resulting in reduced steep slope. There are a very small number of papers dealing with the analysis of the operation characteristics and the design of circuits using HyperFET devices. For example, in [30] a first performance evaluation is carried out and compared with a transistor-only technology, reporting energy advantages associated with supply voltage reduction. On the other hand, in [31], [32], design considerations associated with deviations from ideal behavior appearing in the interconnection of HyperFET logic gates are highlighted. In addition to reducing power consumption in conventional

logic applications, these devices are considered potential candidates for implementing computing paradigms such as neuromorphic architectures and other non-Boolean processors [33].

However, to the best of author's knowledge, no HyperFET-based solution have been proposed as an emerging steep-slope solution to implement DPA-resilient crypto-circuits. In this paper, we will study the resistance against DPA attacks comparing a 14 nm FinFET technological node, which showed impressive performance figures of merit in [24], and its corresponding modification with HyperFET devices, equivalently in a 14 nm node. Moreover, we will try to establish a fair trade-off between the performance and security figures of merit obtained by each one of both technologies.

3 HyperFET Devices

3.1 Operation Principle

HyperFET devices consist of the connection of a PTM at the source terminal of a FET transistor (Fig 3.a). The boosting mechanism of the ratio between ON and OFF currents is based on the abrupt transitions between the insulating (high resistance) and metallic (low resistance) zones [34]. Several HyperFETs have been obtained experimentally, with steep slopes significantly below 60mV/dec [34]–[36]. In [37], authors have proposed a phase-change Tunnel FET with steep slope of 30mV/dec.

As illustrated in the I-V curve of Fig 3.b, when a voltage is applied between PTM terminals, the current circulating through it increases linearly, with a slope equivalent to the inverse of the resistance in the insulating state. When the current density exceeds a certain threshold value ($J_{C,IMT}$), there is a transition from the insulating to the metallic state (IMT), which leads to a significant reduction of the PTM resistance. Thereafter, when the applied voltage is reduced, the current decreases linearly (with a slope equal to the inverse of the resistance in the metallic state). When a sufficiently low current density (called $J_{C,MIT}$) is reached, the transition from metallic to insulating state (MIT) takes place.

The operation of the HyperFET is described as follows. Initially, when the intrinsic FET transistor is OFF, the negligible current flowing through the PTM causes it to be in an insulating state. Indeed, the high resistance connected to the transistor source reduces its effective voltages (VGS and VDS in Fig 3.a) and, consequently, also reduces the leakage current. When the gate-to-source voltage is increased and the transistor switches to the ON state, the current through HyperFET increases until the transition from insulating to metallic state occurs and it rises abruptly. In this scenario, the conduction current of HyperFET can be similar to that of the intrinsic transistor if the metallic state resistance is low enough.

The results shown in this study have been performed using an HyperFET composed of an intrinsic FinFET transistor (predictive model, corresponding to a 14nm LSTP node [38]) and a PTM inspired by the Verilog-A macro-model reported in [30]. Table 1 shows a summary of the physical and electrical parameters of this PTM. Also, since transitions are abrupt but not instantaneous, a transition time (TT) has been

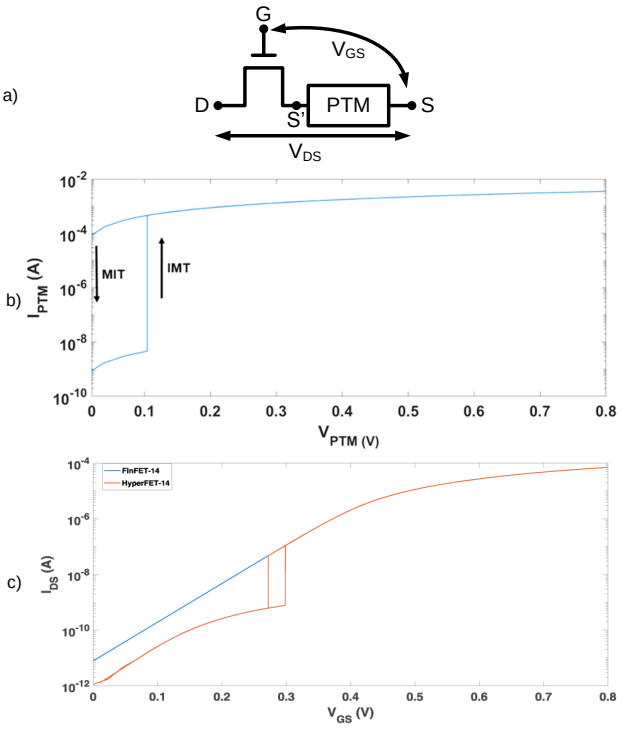


Fig. 3. (a) HyperFET device. (b) Current-voltage characteristic of a phase transition material (PTM) reported in [36] (PTM-Sim). (c) Current-voltage characteristic of the simulated FinFET and its iso-ION HyperFET counterpart.

TABLE 1
PTM parameters [30].

Physical		Electrical	
ρ_{INS}	$100\Omega \cdot cm$	R_{INS}	$45.2M\Omega$
ρ_{MET}	$0.001\Omega \cdot cm$	R_{MET}	452Ω
$J_{C,MIT}$	$8000A/cm^2$	V_{MIT}	$32\mu V$
$J_{C,IMT}$	$520A/cm^2$	V_{IMT}	$204mV$
L	$20nm$	C	$1fF$
A	$42{\cdot}21nm^2$	TT	$50ps$

taken into account. Fig 3.c shows the HyperFET I-V curve together with that of the intrinsic FinFET transistor (both transistors with L=18nm). The expected improvements in security are derived from the fast abrupt transition and its hysteresis characteristic.

3.2 HyperFET-based Proposal for Secure Cryptocircuits

For all the reasons stated above, we have considered HyperFETs as an emerging technology with appealing characteristics for security implementations. This led us to modify the SABL structure in order to introduce HyperFETs with the purpose of a security improvement. In a first approach, we have replaced the bottom clocked FinFET by an HyperFET that dominates the phase of evaluation, being the unique change carried out when compared with the FinFET-14 implementation (Fig. 4). Since the bottom transistor controls the transition from precharge to the evaluation phase, it is

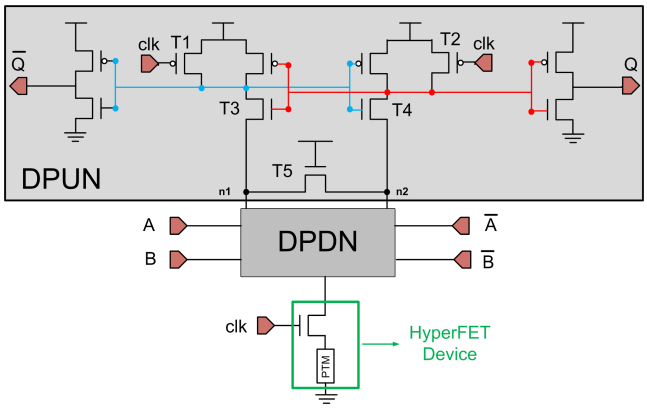


Fig. 4. SABL-DPL structure with HyperFET modification.

the best place to obtain abrupt transitions between these two phases by introducing the clocked pull-down HyperFET device. The selection of only one transistor is sufficient to obtain remarkable differences in the security figures, by exploiting the HyperFET properties, without implying any effect in the symmetry or variability in the predictive model in the logic gate, given the fact that this device is shared by every differential branch of DPDN blocks. Thus, no matter which DPDN branch is connected, the variability of this HyperFET does not affect negatively to the symmetry. For this reason, such proposal is clearly applicable to any DPL logic gate with clocked bottom transistor, expecting improvements in security in all cases. Other locations for HyperFET inside DPDN or DPUN blocks would affect symmetry and it would require precise HyperFET models, which will be considered in future work.

4 DPA Attacks on PRIDE Sbox-4

Following the procedure established by Mangard et al. [4], there exists a lot of models to set a correlation between power consumption and data being processed. Among them we can find different proposals as Hamming Weight, Hamming Distance at the input, Hamming Distance at the output or Zero-Value. It has been concluded from previous works [8] that the Hamming Distance at the output model offers the best results for DPL-based cryptocircuits. It consists of associate higher values of power consumption to a high number of bits changing at the output of a certain cryptographic device. Analogously, a minimum power consumption will be correlated with no changes of output bits. In this work, we focus on PRIDE, which is a 64x64-bit lightweight block cipher using a 128-bits key during the encryption, which is executed in 20 operation rounds. Concretely, we focus on the 4-bit Substitution Box (henceforth Sbox-4), the widely known as most vulnerable section in the algorithm [39]–[42], as demonstration vehicle to compare the robustness against DPA attacks of both implementations, with and without HyperFETs. The results are totally transferable to other algorithms, since the proposals are made at cell level. The Sbox-4 implemented within the PRIDE algorithm is a 4-input ($x_0 - x_3$), 4-output ($y_0 - y_3$) combinational block that follows the next equations (1):

$$\begin{aligned} y3 &= x1 \oplus x3 \cdot x2 \\ y2 &= x0 \oplus x2 \cdot x1 \\ y1 &= x3 \oplus y3 \cdot y2 \\ y0 &= x2 \oplus y2 \cdot y1 \end{aligned} \tag{1}$$

To implement the functionality given by these equations, we have used 4 2-input XOR/XNOR and 4 2-input AND/NAND logic gates designed in SABL logic style [10]. Each one of these gates uses 18 14-nm FinFETs in the original case, while for the HyperFET modification we mantain 17 of those devices and only change one of them for an HyperFET, following the schemes in Fig.1 and Fig.4 , leading to a total of 144 FinFETs for the Sbox-4 implementation, while we have 136 FinFETs and 8 HyperFETs when we introduce our new modifications.

DPDN blocks, which implement the logic functionality of the cell, have been designed using the minimum transistor width for the FinFET-14 nm model. While DPUNs have been designed adjusting the dimensions properly in order to assure a quick and efficient transition between the evaluation and the precharge phase. However, since no modification is introduced in this block, it will be completely similar in both implementations. HyperFET model has been introduced in each cell considering the parameters given in [36].

The first simulations have consisted of applying 2000 patterns to the PRIDE Sbox-4 implemented in Cadence with and without HyperFETs capturing the power supply current traces for every transition. For each implementation, 50 power supply current traces (Figs. 5 and 6) overlapped from random transitions, among the 2000 patterns applied. In those figures we can see, in both cases, that the shapes of power supply current traces are different among them, specially in the evaluation phase, leading to a possible dependence between the power supply current trace shape, and thus the power consumption in every point, and the data being processed. In a second experiment, we have selected specific transitions that are repeated along the simulation and aiming to observe visually if the same power supply current trace is obtained every time the same input patterns are feeded repeatedly. For instance, in the case represented in the Fig.7, we are overlapping the power supply current traces from the FinFET-14nm original implementation, having selected among the 2000 patterns applied the situations where an output transition $y_{n-1} = 0$ is followed by an output transition $y_n = 15_{10} = 1111_2$, observing that the power supply current trace is always exactly the same, when this situation is presented. This is completely transferable to any other values of y_{n-1} and y_n. However, when we repeat this experiment for the HyperFET modified implementation (Fig.8), we can observe that the power supply current trace is different even for the same case where $y_{n-1} = 0$ and $y_n = 15_{10} = 1111_2$, obtaining similar results for other selected transitions. This spreading of power supply current curves are caused by the hysteresis in the PTM section. This result means that the Hamming Distance model applied at the output is no longer valid to retrieve the key through a DPA attack, since the same sequence of transitions could lead to different power supply current trace shapes, this

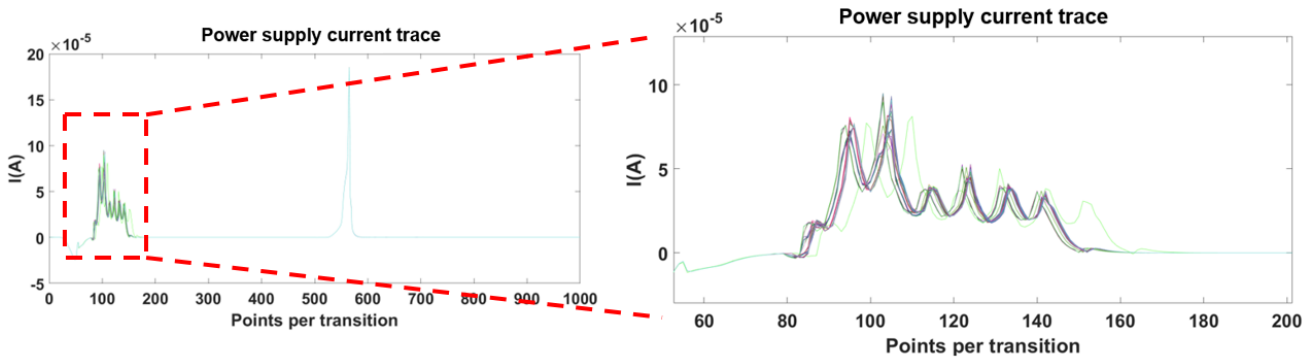


Fig. 5. Overlapped power supply current traces of original FinFET-14nm implementation for 50 random transitions.

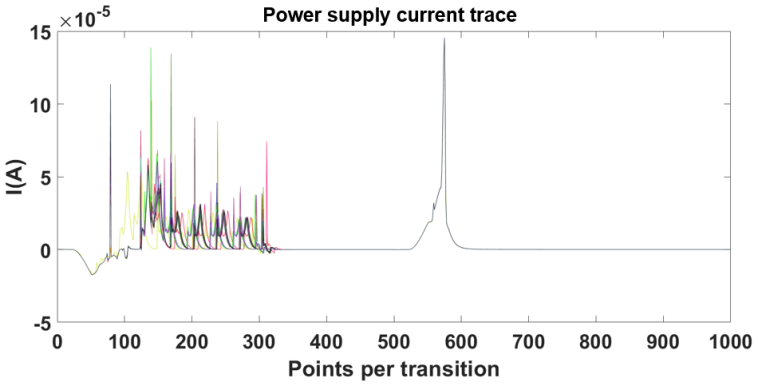


Fig. 6. Overlapped power supply current traces of HyperFET modified for 50 random transitions.

way, dependence between processed data and power consumption could be hidden. To demonstrate this statement, DPA attacks have been performed on both implementations, analyzing if our prediction about the "hiding" produced in the implementation with HyperFETs is ocurring or not. To achieve this purpose, we will measure the efectiveness of DPA attacks in each case, using classical security figures of merit, as the minimum required measurements to disclose (MTD) [8], [43], [44] the secret key.

5 Evaluation and Results

In order to evaluate the security level presented by both implementations, the DPA attack have been made from an "attacker friendly scenario" without any presence of noise, since these conditions will allow us to set the same attack conditions for both proposals, leading to security results that will only depend on the nature of the technologies being implemented and where other factors will not be taken into consideration.

5.1 Electrical Simulation Setup and Figures of Merit

Electrical simulations have been carried out through SPECTRE, applying 2000 randomly generated plaintext patterns at 500 MHz for all the 16 possibles keys, capturing data every 2 ps, and using nominal V_{dd} = 0.8 V with T = 27 ºC. The results from these electrical simulations have been used to perform security evaluations through DPA attacks and performance measurements, including power and timing figures. To establish security level comparisons, we will carry out first order DPA attacks and compute the MTD. However, we are not only interested in the security results since we are working with lightweight block ciphers and implementations where other figures of merit as area and power consumption must be taken into consideration. For this reason, we are going to utilize the Security Delay Power (SPD) figure of merit, presented in [45], that computes the trade-off between security, power consumption and timing performance, represented by the delay value, given by:

$$SPD = \frac{MTD}{Power \cdot Delay} \tag{2}$$

DPA attacks mission is to recover the secret key K from a cryptosystem, in which the input patterns D and the cryptographic algorithm are known. The procedure to encrypt data is the following (Fig. 9): D is a randomly generated 4-bit input pattern, K is the selected 4-bit key, which carries out a XOR operation with D, generating the output X, being this signal the Sbox-4 input data. Finally, Y is the Sbox-4 output data after all the process and $iVdd$ is the Sbox-4 supply current during encryption.

5.2 Results

The DPA attack has been performed on MATLAB by applying the method presented in [4], and totally analogous to the previously made in [8]. Table 2 presents the obtained results in terms of performance and security. As classical

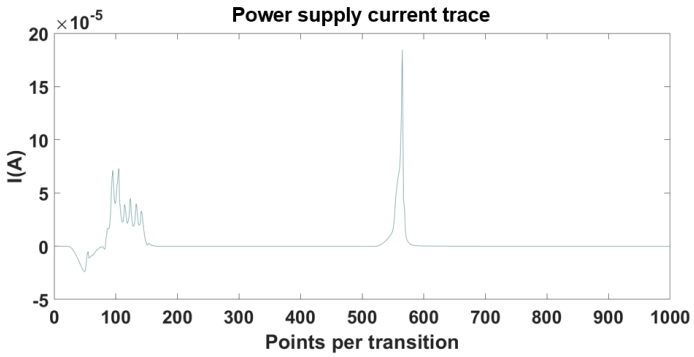


Fig. 7. Overlapped power current supply traces of original FinFET-14nm implementation for the situation $y_{n-1} = 0$, $y_n = 15_{10} = 1111_2$

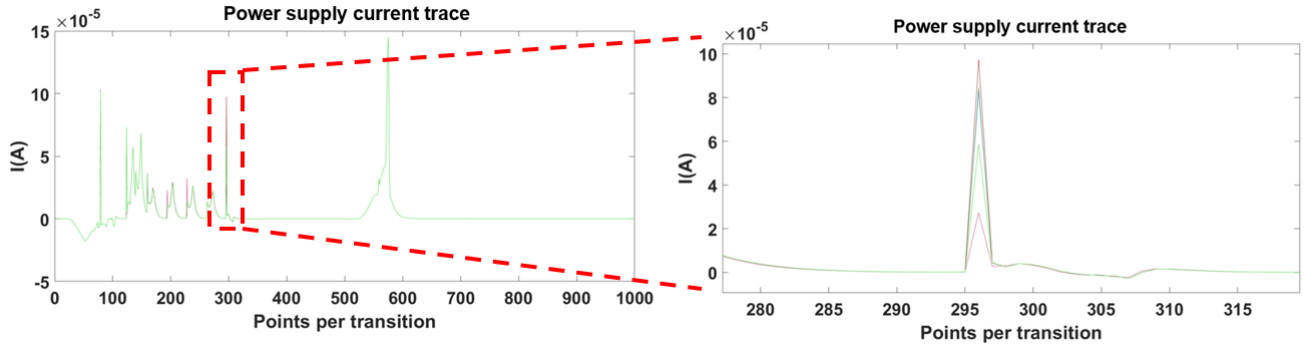


Fig. 8. Power current supply trace of HyperFET modified implementation for the situation $y_{n-1} = 0$, $y_n = 15_{10} = 1111_2$.

TABLE 2
Sbox-4 PRIDE implementation results.

Technology	Max. Power (μW)	Power Avg. (μW)	Max. Delay (ns)	PDP ($\mu W \cdot ns$)	Duty Cycle (%)	MTD			SPD (fJ^{-1})			Failed Attacks
						Min	Max	Avg	Min	Max	Avg	
FinFET - 14	148.13	5.04	0.18	0.89	42.40	12	224	76.06	13.54	252.75	85.83	0
HyperFET - 14	319.78	5.16	0.52	2.68	25.00	1147	>2000	1900.38	427.86	749.51	711.36	12

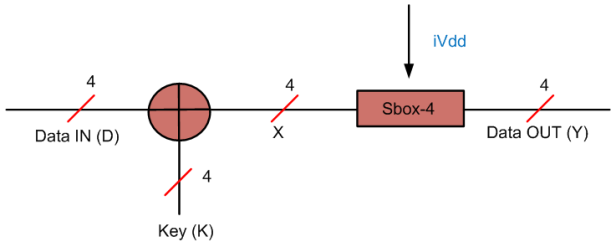
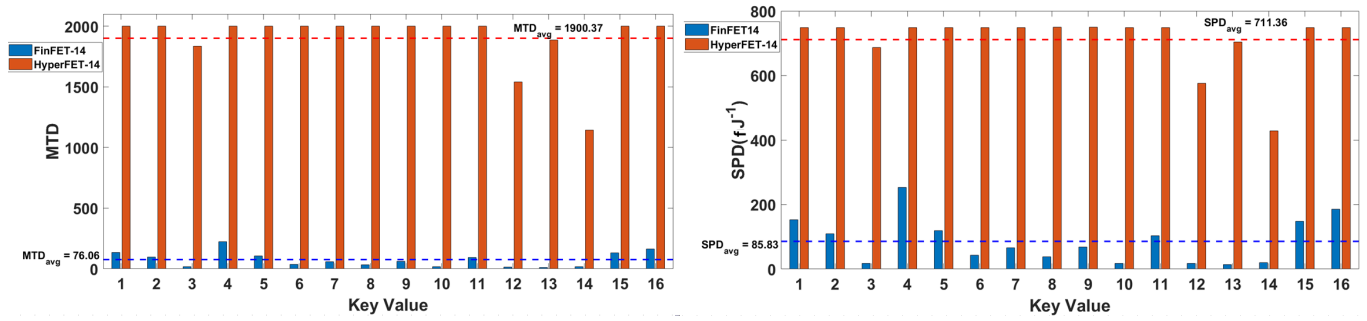


Fig. 9. Cryptographic device scheme.

figures of performance, we have computed maximum peak of power consumption, average power consumption, delay, power-delay product (PDP) and duty cycle. On the other hand, in terms of security, we have considered the minimum (Min.), maximum (Max.) and average (Avg.) MTD, taking into consideration every possible key, as the most proper figure to establish the level of robustness of a cryptographic device. To end, the minimum (Min.), maximum (Max.) and average (Avg.) SPD are selected to carry out a trade-off between performance and security. Additionally, to depict the MTD and SPD values obtained for each key we show two histograms, in Fig. 10 where direct comparisons can be made.

The most important results that we can comment from the table and histograms is the superiority of implementations incorporating HyperFETs over the traditional implementation with FinFETs. Only four attacks are successful when HyperFETs are introduced, leading to an average MTD at least x24.99 times better, taking into consideration that in the cases where the key is not retrieved we have considered as MTD = 2000, probably being considerably higher. In terms of timing performance, original FinFET implementations outperform the results obtained by those where HyperFETs are introduced. Concerning to power measurements, although the maximum peak of power consumption shows a vakue x2.43 superior for the implementation with HyperFETs, no significants changes in the average power consumption are observed. Nonetheless, the most important differences are given for the duty cycle, delay and PDP figures. In the worst case scenario, the difference between the obtained duty cycles is up to 17.4%, while the results in terms of delay are x2.89 times better for the original



(a) MTD (b) SPD

Fig. 10. Histograms with values of MTD and SPD for all the possible keys.

proposal. Finally, the figures of power and delay lead to a x3.01 worse result for the implementation with HyperFETs. Despite the fact that the original proposal outperforms the results obtained by the one presented in this paper with HyperFETs introduced, SPD figure shows that the HyperFET-modified proposal overcomes the results obtained by the original one in almost one order of magnitude, with more than x8.28 better result, being this implementation suitable for security applications, and being the benefits obtained in terms of security better than the disadvantages produced in terms of performance.

Additionally, another important result obtained from our studies is the place, inside the transition, where the correlation model is retrieving the key. As it is possible to observe in Fig.11, for the case of original FinFET-14nm proposal, the correlation is maximum for the correct key, which is outlined in green (denotes the correct key) and red (denotes the predicted key) against the rest of blue keys, around the 200th point, corresponding to the end of the evaluation phase and where, according to Figs. 7 and 5, different power consumptions are obtained for different data but with the same power consumption when same data are processed. However, when the HyperFET modified implementation case is studied Fig.12, the four attacks that succeed only are able to retrieve the secret key in the precharge phase, between point number 500 and 600, while the correlation is totally hidden in the first points of the transition where the evaluation of the logic operations are computed. Given this result, the prediction we previously made about the hiding produced in evaluation phases given the different comsuption is confirmed, since no key is retrieved in the evaluation phase once introduced the HyperFET modifications, being this region the main source of leaked information in the original proposal. As prospective work, it could be studied if the same effect occurs when we introduce PTMs to convert transistors T1 and T2, which control the clock signal that rules the precharge phase, from Fig.4 on HyperFETs aiming to obtain, as well, masking in the precharge phase.

6 Conclusions

The work presented in this paper is a first approach to assess the use of HyperFETs in security applications. The main goal was to analyze the DPA resilience of FinFET cryptocircuits using DPL-based logic gates incorporating PTMs to transform FinFETs in HyperFETs. Due to the extraordinary properties of HyperFETs as it is the case of its steep slope causing boosted I_{ON}/I_{OFF} ratio and hysteresis on transition, we have considered these devices suitable for cryptographic circuits given, also, its apparent non-dependence between power supply current traces and the data being computed derived from our first simulations (Fig.8). Since we find hard constraints in order to design circuits for wearable and IoT applications, where cryptographic blocks are included to protect valuable data, a trade-off between performance and security must be achieved. To allow this purpose, the classical DPDN structure of SABL logic style has been modified substituting by an HyperFET the bottom FinFET that controls the evaluation phase, leading to an effective hiding between power consumption and data being processed, and seeking this way improved figures of security.

A 4-bit substitution box (Sbox-4) of PRIDE algorithm has been designed using Cadence in FinFET 14 nm technology. A comparison was established between the implementation with HyperFETs and the original proposal, obtaining interesting results from the DPA attacks performed. As summary, the original FinFET proposal clearly shows superior classical performance figures of merit, as delay, duty cycle or PDP. In terms of power consumption, no high differences can be concluded. In terms of security, HyperFETs show their superiority with a security figure, MTD, above 25 times superior to the obtained by the original FinFET 14 nm, with only 4 out of 16 succesful attacks. The result obtained for SPD, including security, power and delay, shows that the HyperFET modified implementation achieves results one order of magnitude superior with respect to the original FinFET implementation. As future work, we will study the introduction of HyperFETs within the DPUN block, in order to control the leakage of information not only in the evaluation, but also in the precharge phase, aiming to hide the power trace of this region and to avoid attacks by blurring the dependence between data and power consumption. Ultimately, this will improve the security level.

Acknowledgments

This work was funded by the Spanish Government with support from FEDER under Projects TEC2016-80549-R and TEC2017-87052-P. This project has received funding from the European Research Council (ERC) under the European

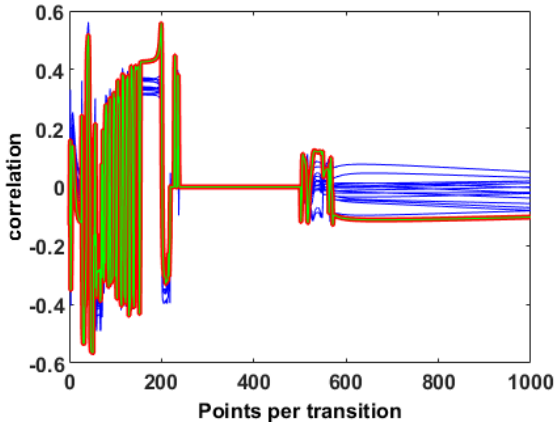


Fig. 11. Succesful attack for Key13. FinFET 14 nm original proposal.

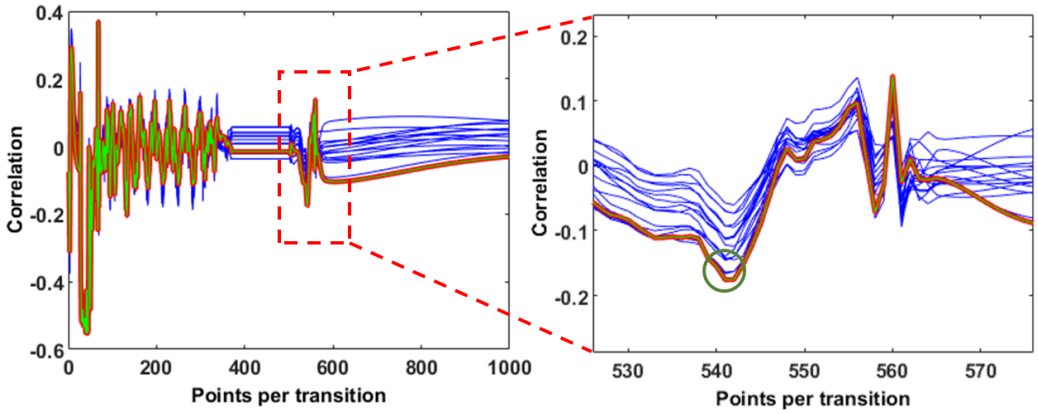


Fig. 12. Succesful attack for Key13. FinFET 14 nm with HyperFET modification.

Union's Horizon 2020 research and innovation programme (grant agreement No. 804476)

REFERENCES

[1] P. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, other systems," in *Proceedings of International Cryptology Conference (CRYPTO'96)*, 1996, pp. 104–113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of International Cryptology Conference (CRYPTO'99)*. Springer, Berlin, Heidelberg, 1999, pp. 388–397.

[3] Y.-I. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J.-L. Danger, "Analysis of electromagnetic information leakage from cryptographic devices with different physical structures," *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 571–580, Jun. 2013.

[4] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secret of smart cards*. Springer, 2007.

[5] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Private circuits securing hardware against probing attacks," in *Proceedings of International Cryptology Conference (CRYPTO'03)*. Springer, Berlin, Heidelberg, 2003, pp. 463–481.

[6] C. Gebotys, "A table masking countermeasure for low-energy secure embedded systems," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 14, no. 7, pp. 740–753, Jul. 2006.

[7] T. D. Cnudde and S. Nikova, "Securing the present block cipher against combined side-channel analysis and fault attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3291–3301, Dec. 2017.

[8] E. Tena-Sánchez, J. Castro, and A. J. Acosta, "A methodology for optimized design of secure differential logic gates for dpa resistant circuits," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 2, pp. 203–215, Jun. 2014.

[9] K. Tiri and I. Verbauwhede, "Design method for constant power consumption of differential logic circuits," in *Design, Automation and Test in Europe (DATE'05)*. IEEE, 2005, pp. 628–633.

[10] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards," in *European Solid-State Circuits Conference (ESSCIRC)*. IEEE, 2002, pp. 403–406.

[11] K. Tiri and I. Verbauwhede, "A logic level design methodlogy for a secure dpa resistant asic or fpga implementation," in *Design, Automation and Test in Europe (DATE'04)*. IEEE, 2004, pp. 246–251.

[12] H. Kim, V. Rozic, and I. Verbauwhede, "Three phase dynamic current mode logic: A more secure dycml to achieve a more balanced power consumption." Springer, Berlin, Heidelberg, 2012, pp. 68–81.

[13] IEEE, "Ieee international roadmap for devices and systems."

[14] S. Taheri and J.-S. Yuan, "Security analysis of tunnel field-effect transistor for low power hardware," *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 8, no. 2, pp. 271–275, 2017.

[15] Y. Bi, K. Shamsi, J.-S. Yuan, Y. Jin, M. Niemier, and X. S. Hu, "Tunnel fet current mode logic for dpa-resilient circuit designs," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 3, pp. 340–352, Jul. 2017.

[16] M. W. Allam and M. I. Elmasry, "Dynamic current mode logic (dycml): a new low-power high-performance logic style," *IEEE Journal of Solid-State circuits*, vol. 36, no. 3, pp. 550–558, mar 2001.

[17] I. Hassoune, F. Macé, D. Flandre, and J.-D. Legat, "Low-swing current mode logic (lscml): A new logic style for secure and robust smart cards against power analysis attacks," *Microelectronics Journal*, vol. 37, no. 9, pp. 997–1006, sep 2006.

[18] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *International Workshop on Cryptographic Hardware and Embedded Systems (CHES'06)*. Springer, Berlin, Heidelberg, oct 2006, pp. 232–241.

[19] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay-based dual-rail precharge logic," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 19, no. 7, pp. 1147–1153, jul 2011.

[20] R. Mahmoud, Y. Tasneem, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective measures," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, dec 2015, pp. 336–341.

[21] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of iot systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, nov 2014, pp. 417–423.

[22] M. Zhang and N. K. Jha, "Finfet-based power management for improved dpa resistance with low overhead," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 7, no. 3, pp. 1–16, Aug. 2011.

[23] S. D. Kumar, H. Thapliyal, and A. Mohammad, "Finsal: Finfet-based secure adiabatic logic for energy-efficient and dpa resistant iot devices," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 110–122, Jan. 2018.

[24] E. Tena-Sánchez, I. M. Delgado-Lozano, J. Núñez, and A. J. Acosta, "Benchmarking of nanometer technologies for dpa-resilient dpl-based cryptocircuits," in *2018 Conference on Design of Circuits and Integrated Systems (DCIS'18)*, nov 2018.

[25] S. Saurabh and M. Jagadesh, *Fundamentals of tunnel field effect transistors*. CRC Press, 2016.

[26] H. Lu and A. Seabaugh, "Tunnel field-effect transistors: State-of-the-art," *IEEE Journal of the Electron Devices Society*, vol. 2, no. 4, pp. 44–49, jul 2014.

[27] W.-Y. Tsai, H. Liu, X. Li, and V. Narayanan, "Low-power high-speed current mode logic using Tunnel-FETs," in *2014 22nd International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, oct 2014, pp. 1–6.

[28] Y. Bi, K. Shamsi, Y. Jiann-Shiun, F.-X. Standaert, and J. Yier, "Leverage emerging technologies for DPA-resilient block cipher design," in *Design, Automation & Test in Europe Conference & Exhibition, 2016 (DATE2016)*. Dresden, Germany: IEEE, 2016.

[29] Y. Bi, X. S. Hu, Y. Jin, M. Niemier, K. Shamsi, and X. Yin, "Enhancing Hardware Security with Emerging Transistor Technologies," in *Proceedings of the 26th edition on Great Lakes Symposium on VLSI - GLSVLSI '16*. New York, New York, USA: ACM Press, 2016, pp. 305–310.

[30] A. Aziz, N. Shukla, S. Datta, and S. K. Gupta, "Steep Switching Hybrid Phase Transition FETs (Hyper-FET) for Low Power Applications: A Device-Circuit Co-design Perspective–Part I," *IEEE Transactions on Electron Devices*, vol. 64, no. 3, pp. 1350–1357, mar 2017.

[31] M. J. Avedillo and J. Núñez, "Insights Into the Operation of Hyper-FET-Based Circuits," *IEEE Transactions on Electron Devices*, vol. 64, no. 9, pp. 3912–3918, sep 2017.

[32] J. Núñez and M. J. Avedillo, "Power and Speed Evaluation of Hyper-FET Circuits," *IEEE Access*, vol. 7, pp. 6724–6732, 2019.

[33] A. Aziz, N. Shukla, S. Datta, and S. K. Gupta, "Steep Switching Hybrid Phase Transition FETs (Hyper-FET) for Low Power Applications: A Device-Circuit Co-design Perspective—Part II," *IEEE Transactions on Electron Devices*, vol. 64, no. 3, pp. 1358–1365, mar 2017.

[34] N. Shukla, A. V. Thathachary, A. Agrawal, H. Paik, A. Aziz, D. G. Schlom, S. K. Gupta, R. Engel-Herbert, and S. Datta, "A steep-slope transistor based on abrupt electronic phase transition," *Nature Communications*, vol. 6, no. 1, p. 7812, nov 2015.

[35] J. Song, J. Woo, S. Lee, A. Prakash, J. Yoo, K. Moon, and H. Hwang, "Steep Slope Field-Effect Transistors With Ag/TiO2-Based Threshold Switching Device," *IEEE Electron Device Letters*, vol. 37, no. 7, pp. 932–934, jul 2016.

[36] A. Verma, B. Song, B. Downey, V. D. Wheeler, D. J. Meyer, H. G. Xing, and D. Jena, "Steep Sub-Boltzmann Switching in AlGaN/GaN Phase-FETs With ALD VO2," *IEEE Transactions on Electron Devices*, vol. 65, no. 3, pp. 945–949, mar 2018.

[37] W. A. Vitale, E. A. Casu, A. Biswas, T. Rosca, C. Alper, A. Krammer, G. V. Luong, Q.-T. Zhao, S. Mantl, A. Schüler, and A. M. Ionescu, "A Steep-Slope Transistor Combining Phase-Change and Band-to-Band-Tunneling to Achieve a sub-Unity Body Factor," *Scientific Reports*, vol. 7, no. 1, p. 355, dec 2017.

[38] A. S. University. Predictive technology model (ptm) website. [Online]. Available: http://ptm.asu.edu

[39] O. Lo, W. J. Buchanan, and D. Carson, "Power analysis attacks on the aes-128 s-box using differential power analysis (dpa) and correlation power analysis (cpa)," *Journal of Cyber Security Technology*, vol. 1, no. 2, pp. 88–107, apr 2017.

[40] S. Picek, K. Papagiannopoulos, B. Ege, L. Batina, and D. Jakobovic, "Confused by confusion: Systematic evaluation of dpa resistance of various s-boxes," in *15th International Conference on Cryptology in India (INDOCRYPT'14)*. New Delhi, India: Springer, dec 2014, pp. 374–390. [Online]. Available: http://link.springer.com/10.1007/978-3-319-13039-2_22

[41] K. H. Boey, M. O'Neill, and R. Woods, "How resistant are sboxes to power analysis attacks?" in *2011 4th IFIP International Conference on New Technologies, Mobility and Security*. IEEE, 2011, pp. 1–6.

[42] E. Prouff, "Dpa attacks and s-boxes," in *2005 12th Fast Software Encryption Workshop (FSE'05)*. Springer, Berlin, Heidelberg, 2005, pp. 424–441.

[43] K. Tiri and I. Verbauwhede, "A vlsi design flow for secure side-channel attack resistant ics," in *Design, Automation and Test in Europe (DATE'05)*. IEEE, aug 2005, pp. 58–63.

[44] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti, "Effectiveness of leakage power analysis attacks on dpa-resistant logic styles under process variations," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 2, pp. 429–442, feb 2014.

[45] E. Tena-Sánchez and A. J. Acosta, "Logic minimization and wide fan-in issues in dpl-based cryptocircuits against power analysis attacks," *International Journal of Circuit Theory and Applications*, vol. 47, no. 2, pp. 238–253, feb 2019.

Ignacio M. Delgado-Lozano received a B. Sc. 4-year degree in Physics in 2017, and a M.Sc. degree in Microelectronics in 2018, both from the University of Seville. From 2018 to 2019, he worked at the Instituto de Microelectrónica de Sevilla (IMSE-CNM-CSIC)/University of Seville. Since 2019 to present, he is a PhD student at Tampere University, Finland. His main research interests include the design of secure cryptographic hardware with emerging technologies.

Erica Tena-Sánchez received a B. Sc. degree in Telecomunications in 2010 from the University of Cantabria, Spain, and Electronics Engineering (with honors), M.Sc. degree in Microelectronics and Ph. D. degree from the University of Seville, Spain, in 2012, 2013 and 2019 respectively. Since 2011, she has been with the Instituto de Microelectrónica de Sevilla (IMSE-CNM-CSIC)/University of Seville. Her current research interests lies in the field of CMOS Digital Design of secure cryptographic circuits.

Juan Núñez received the Telecommunication Engineering degree in 2005. Since then, he has been with the Instituto de Microelectrónica de Sevilla (IMSE-CNM-CSIC)/University of Seville and the Department of Electronics and Electromagnetism at the University of Seville, where he is currently a researcher. In 2011, he obtained the Ph. D. degree from that University. His main research interests currently include the design and evaluation of logic circuits using deep-submicron and emerging technologies.

Antonio J. Acosta received a B.Sc. 5-year degree in Physics and a Ph.D. degree in Physics from the University of Seville, Spain, in 1989 and 1995, respectively. He is Full Professor at the University of Seville and Senior Researcher at the Instituto de Microelectrónica de Sevilla (IMSE-CNM-CSIC). His current research interests lie in the fields of low-power and low-noise CMOS Digital and mixed-signal high-performance VLSI Design, timing in VLSI digital system, and cryptographic circuits. He has co-authored more than one hundred international scientific publications and has led a number of different national and European R&D projects. Dr. Acosta has served as a member of editorial boards in international journals and on program committees in several prestigious conferences. He was General Chair of the 2002 PATMOS International Workshop.