Projection of dual-rail DPA countermeasures in future FinFET and emerging TFET technologies

I. M. DELGADO-LOZANO, Tampere University
E. TENA-SÁNCHEZ, J. NÚÑEZ, and A. J. ACOSTA, Instituto de Microelectrónica de Sevilla (IMSE-CNM), CSIC/Universidad de Sevilla

The design of near future cryptocircuits will require greater performance characteristics in order to be implemented in devices with very limited resources for secure applications. Considering the security against differential power side-channel attacks (DPA), explorations of different implementations of dual-precharge logic gates with advanced and emerging technologies, using nanometric FinFET and Tunnel FET transistors, are proposed aiming to maintain or even improve the security levels obtained by current MOSFET technologies and reducing the resources needed for the implementations. As case study, dual-precharge logic primitives have been designed and included in the 4-bit substitution box of PRIDE algorithm, measuring the performance and evaluating the security through simulation-based DPA attacks for each implementation. Extensive electrical simulations with predictive PTM model on scaled 16nm and 22nm MOSFET, 16nm and 20nm FinFET and 20nm TFET, demonstrate a clear evolution of security and performances with respect to current 90nm MOSFET implementations, providing FinFET as fastest solutions with a delay 3.7 times better than conventional proposals, but being TFET the best candidate for future cryptocircuits in terms of average power consumption (x0.02 times compared with conventional technologies) and security in some orders of magnitude.

CCS Concepts: • **Security and privacy → Side-channel analysis and countermeasures**; • **Hardware →** *Tunneling devices.*

Additional Key Words and Phrases: 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, TFET

ACM Reference Format:
I. M. Delgado-Lozano, E. Tena-Sánchez, J. Núñez, and A. J. Acosta. 2020. Projection of dual-rail DPA countermeasures in future FinFET and emerging TFET technologies. *ACM J. Emerg. Technol. Comput. Syst.* 1, 1, Article 1 (January 2020), 16 pages. https://doi.org/10.1145/3381857

1 INTRODUCTION

Nowadays, the electronic devices that are daily present in our lives work with secret information that must not be revealed to third parties, thus there is an increasing need of secure devices to prevent malicious attacks [8, 12, 13, 20]. In this context, secure devices make use of cryptographic algorithms that although are mathematically safe, can leak side-channel information when a Side-Channel Attack (SCA) is applied, being the main sources of leaked information: delay [12], power consumption [13] or electromagnetic radiation [8]. Among the wide variety of SCAs, Differential

Authors' addresses: I. M. Delgado-Lozano, ignacio@imse-cnm.csic.es, Tampere University; E. Tena-Sánchez, erica@imse-cnm.csic.es; J. Núñez, jnunez@imse-cnm.csic.es; A. J. Acosta, acojim@imse-cnm.csic.es, Instituto de Microelectrónica de Sevilla (IMSE-CNM), CSIC/Universidad de Sevilla, Américo Vespucio, 28, Seville, Spain, 41092.

1550-4832/2020/1-ART1 $15.00
https://doi.org/10.1145/3381857

Power Analysis (DPA) are extended due to their simplicity, effectiveness, and the minimal equipment required [20]. DPA attacks are based on the well known fact that dynamic power consumption in a logic circuit depends on the data being processed by the device. Thus, by correlating the encrypted data with the power consumption of a cryptographic device it is possible to retrieve the secret key through statistical analysis.

To make cryptocircuits more resistant to DPA attacks, some alternatives and countermeasures have been widely proposed at circuit level, standing out those based on masking [6, 7, 10, 20] and hiding [11, 15, 29, 31, 33, 34]. Although both masking and hiding techniques can be applied to different abstractions levels, ranging from algorithm to gate level, we are going to focus on gate level hiding. Algorithm-level countermeasures are very specific and difficult to automate, due to their heavy dependence on specific cryptographic algorithm. Concerning gate-level countermeasures, masking has shown to be either vulnerable or very complicated to implement due to the large number of masks needed to provide a secure solution [26]. For this reason, gate-level hiding techniques present better trade-off between performance and security as compared to gate-level masking. To enhance gate-level hiding strategies, Dual-Rail with Precharge-Logic (DPL) families have been designed to carry out one computation in each clock cycle regardless the input conditions and getting the same power consumption in every cycle, ideally. In the case of DPL gates, those based on current-mode logic gates present static power consumption, being not suitable for low-power applications. Among the different DPL logic styles, Sense-Amplifier Based Logic (SABL) [31] style has been extensively analyzed giving a good trade-off between performance and security [29], being widely accepted and thus, selected in this paper as our reference logic style.

DPL logic styles have some associated penalties in terms of area, delay and power consumption due to the higher number of transistors used to maintain the two-phases operation mode and the symmetry inside their constitutive blocks.

The scientific community is facing the diversion of strategies aiming to avoid the existing bottlenecks for current technologies as the limit of CMOS technology is approaching. The idea of using emerging devices “beyond CMOS" [9] drawn away from conventional technologies, and frequently from silicon, is a challenge. This is not only for generic processing purposes, but also for security applications. It is necessary to assess the role of these new devices, for instance the Tunnel FET (TFET) transistors, a promising alternative for SCA-resilient implementations [4, 28], in the near future security applications.The design of DPA resistant DPL-based circuits is addressed, considering conventional MOSFET transistors, in both current and scaled nanometric technology nodes, nanometric FinFET technologies, and emerging technologies as TFETs, allowing a fair comparison on demonstrative cryptocircuit implementations. The main contributions of the paper are:

i) Design of logic primitives in a DPL-based DPA-resistant SABL style, using MOSFET, FinFET and TFET technologies.

ii) SABL structure redesign for TFET technologies.

iii) Characterization of a PRIDE 4-bit substitution box (Sbox-4) as a case study through electrical simulations on predictive PTM models in seven selected current and emerging technologies.

iv) Evaluation of security via DPA attacks.

The organization of this paper is as follows: In Section 2, it is presented the previous work concerning emerging technologies for security applications. Section 3 presents the design of CMOS DPL-based secure logic gates against DPA attacks. Section 4 shows the modifications needed by the DPL logic gates to have a proper behavior in TFET technology. Section 5 includes the design of PRIDE Sbox-4 block as case study and the analyzed 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.

2 EMERGING TECHNOLOGIES FOR SECURITY APPLICATIONS

The use of scaled MOSFET technologies shows some deficiencies in terms of power density and energy efficiency due to the impossibility of reducing threshold voltages, without exponentially increasing the leakage currents. In a context of resource constrained applications, as it is the case of portable and lightweight cryptography, which demand circuits with ultra-low power consumption and high efficiency in terms of energy, emerging alternatives to CMOS-based approaches are required to the full deployment of secure IoT systems [19, 36].

The development of new transistor technologies, circuits and architectures, represents an opportunity to face these challenges, facilitating the implementation of low-power and secure lightweight design styles. Some of these new devices can operate as Boolean switches in conventional computing systems whereas others have new features that make them more suitable for other computing paradigms such as non-Boolean logic or non-Von Neumann architectures. In particular, great efforts have been devoted to the implementation of DPA-resilient circuits using a wide variety of emerging devices [4, 14, 28, 37].

Several works have been carried out using FinFET transistors for security applications, as an emerging substitute for bulk CMOS at deep nanometric nodes (22 nm and beyond) with outstanding properties as a high ON/OFF current ratio and reduced short channel effects. In [37], a low-power DPA countermeasure is proposed consisting of a back-gate bias randomly adjusted which generates a large amount of noise allowing to mask the differential signal at key moments during the encryption, enhancing the resistance of the system against DPA attacks. In [14], an adiabatic FinFET-based circuit is presented providing a low-power and secure system which increase its resistance against SCAs by decreasing the frequency and thus, the instantaneous power consumption.

TFETs [25], [18] are gated p-i-n diodes with symmetrical doping structure and operating under reverse bias condition. These devices can achieve steeper sub-threshold slopes (<60 mV/dec) and operate with reduced supply voltages compared to CMOS transistors without significantly increasing leakage currents. Although TFETs could offer superior performance against hardware-level attacks, as demonstrated in [4, 28], for Current Mode Logic (CML) implementations, further analysis should be performed over other more advanced DPL structures with no static power consumption, as SABL.

In this paper, we will study the design of DPL cryptocircuits against DPA attacks using FinFET, TFET and scaled MOSFET transistors [30]. Two different technological nodes (16 and 20 nm) will be used for predictive models of FinFET transistors [27], whereas 16 and 22 nm will be taken into consideration for MOSFET scaled technologies [38], and a 20 nm model [17] for TFET transistors. In addition, we will establish a comparison in terms of security with two 90 nm TSMC commercial technologies (standard and low-power), to have a global picture of next term DPL-based implementations.

3 DPL AS SECURE LOGIC APPROACH AGAINST DPA

In 1999, Kocher et al. [13] showed that DPA attacks could retrieve the secret key of a cryptographic device with a high level of effectiveness. Standard CMOS logic style shows a great dependence between processed data and power consumption, thus, it was discarded for cryptographic applications soon, leading to the search of alternative logic styles in which the dependence between data being encrypted and power consumption were much lower, providing greater levels of reliability and security to cryptocircuits.

DPL works with two alternating operation phases, precharge and evaluation, providing both the true and the complemented output with one transition per cycle and (almost) the same power consumption per processed data. DPL gates present a differential pull-down network (DPDN) which

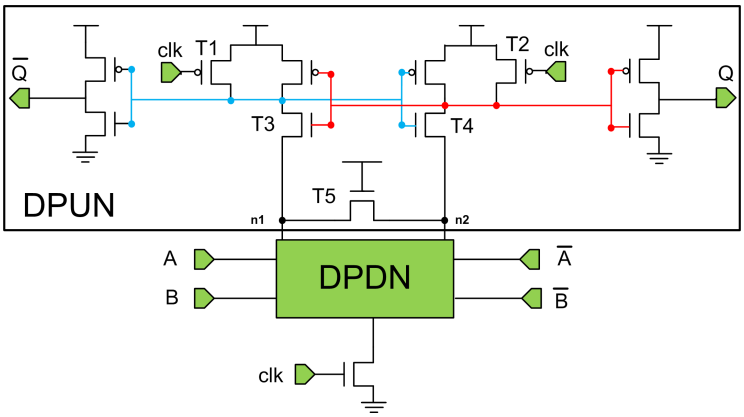


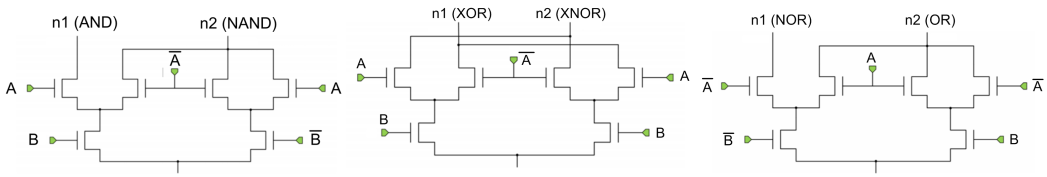
Fig. 1. SABL-DPL structure.

performs the logic function and a differential pull-up network (DPUN) which provides the gate outputs. The SABL proposal [31] is a DPL technique with superior effectiveness presented when compared with other DPL alternatives as it is stated from the results obtained in previous works [29]. The DPUN structure for SABL in Fig. 1 is implemented using clocked P-type transistors. The operation of this block is the following: T1 and T2 transistors are ON in the precharge phase, when clk = 0. So, nodes n1 and n2 will be set to 1, with values $Q\bar{Q}$ = 00 due to the output inverters. In the evaluation phase (clk = 1), one of the T3 and T4 transistors connected to nodes n1 and n2, is grounded through a discharge path in the DPDN, giving the result depending only on the logic function implemented by the DPDN block and the input values. Transistor T5, always in conduction, equalizes n1 and n2 to 0. The key aspects to ensure the design of secure DPL gates are: i) to use the same amount of charge in each transition, as mentioned previously; ii) a fully symmetrical DPDN block independent from the input values meaning that all the paths from n1 and n2 to GND must have the same transistor count and equivalent RC values leading, thus, to constant delay; and finally iii) all the internal nodes of DPDN block have to be connected to n1 or n2. The full symmetry in DPUN block and the fact that the outputs of DPDN are not directly connected to the gate of output inverters in the DPUN block makes SABL logic style indicated against DPA attacks, and superior to other symmetric and differential DPL alternatives [29].

The implementation of DPDN blocks for different logic functions are shown in Fig.2. These structures are also valid for FinFET transistors because of their similar operation mode to MOSFET. However, the specificities of TFETs with an asymmetric doping structure, and an operation mode based on the band-to-band tunneling (BTBT) principle make necessary the specific design of secure SABL gates against DPA implemented with TFET transistors.

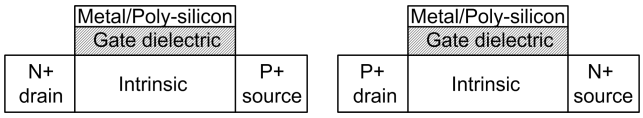
4 STRUCTURAL MODIFICATIONS FOR THE USE OF TFETS IN SABL

The current flow in a conventional MOSFET device is based on the carriers thermionic emission through a potential barrier. This implies a difficulty in order to maintain acceptable levels of power consumption in nanometric technological nodes. However, TFETs show some interesting electric properties and can represent a feasible alternative to conventional MOS transistors, due to the differences in the carrier transport mechanism [21]. The TFET device consists of a p-i-n structure, with an added gate in inverse polarization conditions (Fig. 3). Its most distinctive characteristic is the doping structure, where the source doping is the opposite from the drain one, whereas for MOSFETs transistors the doping is completely symmetric.



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

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



(a) N-TFET (b) P-TFET

Fig. 3. TFET structure scheme.

The operation principle of TFETs is mainly based on the BTBT principle that allows carriers to leave the valence band, go through the bandgap by tunnel effect, and pass to the conduction band or vice-versa in such a way that the entry of carriers in the channel is controlled by this mechanism. For a N-TFET transistor, when the gate voltage is low, the device is OFF. In this circumstance, the channel conduction band is far above the source valence band preventing the tunnel effect from a band to the other and leading to a negligible drain intensity. When the gate voltage is increasingly augmented, the density of carriers under the gate starts to be modulated and the conduction band begins to descend. Once the gate voltage is sufficiently high, the channel conduction band is so low that itself and the source valence band are totally aligned (Fig.4). Once the electrons have passed to the channel, they moved to the drain due to the positive voltage applied in this terminal [25]. The operation principle is completely analogous for type P-TFET transistors, taking into consideration the exchange of doping structure between drain and source terminals.

Since carrier transport from source to drain is made through BTBT, instead of thermionic emission, TFETs present a double advantage. The first one is the activation of carrier transport mechanism with a reduced supply voltage V_{dd} ($V_{dd} = 0.3V$ instead of voltages around $V_{dd} = 1V$ for MOSFET transistors with the same dimensions). On the other hand, BTBT reduces enormously the probabilities of tunnel effect when the transistor is OFF, minimizing the leakage currents. Additionally, the drain current in TFETs is highly sensitive to the gate voltage variation, so a slight diminution of this parameter could quickly take the device into the cutoff region. Nevertheless, TFETs present a difficulty with respect to the conventional MOSFETs, since due to its asymmetric p-i-n structure, the current flows only in one direction. For a given gate voltage, a N-TFET has an appreciable current only if the p-i-n structure is reverse biased or, equivalently, if V_{ds} is positive. In case of a negative V_{ds}, the p-i-n structure is forward biased and the device behaves as a forward polarized diode. Further considerations about TFET transistor characteristic curves are given at [25].

The unidirectional conduction leads to some limitations when designing logic gates [21]. Concerning SABL gates, it is not possible to replace directly MOSFET transistors by TFET ones, being necessary some modifications in the DPUN block. Firstly, the n-type transistor introduced between

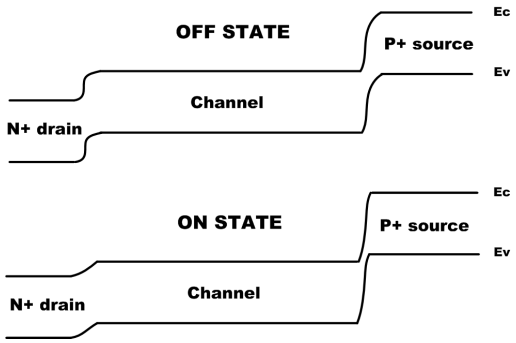


Fig. 4. Bands diagram for a n-TFET transistor.

n1 and n2 nodes that was always in ON state, now will only drive in one direction, depending on the drain and source terminals position, which are not interchangeable in TFET technology. To sort this problem out, we introduce a second transistor connecting n1 and n2 nodes applying an exchange in the terminals with respect to the first of them, in such a way that conduction is re-established in both directions between both nodes. In addition, in the output and input nodes of DPDN output inverter, it is produced the bootstrapping phenomenon, described in [21] and solved in [3]. This phenomenon consists of a capacitive coupling produced between two different nodes due to the unidirectional conduction and the impossibility of discharge (charge) a node once its voltage value is higher (lower) than V_{dd} (GND). For instance, if the output node Q in the Fig.1 is capacitively coupled with the input of the inverter, we could have a higher voltage than V_{dd} in Q. In case of a MOSFET-based implementation of this circuit, the symmetric transistor structure would allow a fast discharge from this node to the source terminal, thus, we would find a slight peak turning back to V_{dd} quickly. However, the asymmetric structure of TFET generates a low conduction state when V_{ds} is positive, so the p-type transistor cannot discharge Q, getting a superior voltage than V_{dd}. This explanation is analogous for voltages under GND value. To illustrate this effect (Fig. 5), we have simulated an AND/NAND gate in the original SABL style, where both the problem of unidirectionality and bootstraping lead to degraded waveforms. Although the bootstrapping effect would not produce a logic fault in DPL-SABL gates, strong delay problems appear, increasing this factor up to a 60%. Additionally, the signals degradation could be propagated through a series of logic gates leading to a tedious functionality check given that the circuit would not work between two well established voltage values (V_{dd} and GND) as it is typical in logic circuits.

The solution to the bootstraping phenomenon explained in [3] will be applied to this case. It tries to find an alternative way to charge/discharge the node affected by bootstrapping. Placing a P-TFET with its source connected to the bootstrapped node, its drain connected to V_{dd} and gate connected to GND, it is possible to discharge a node with undesired positive voltage. In the same way, this effect could lead to a negative voltage value below GND. In this case, introducing a N-TFET with its source connected to the bootstrapped node, its drain to GND, and its gate to V_{dd} would allow to charge the negative node, bringing it back to GND. Therefore, adding both transistors to the bootstrapped node, we could protect it from this phenomenon in both directions. Nodes potentially affected by bootstrapping phenomenon were the output ones (Q and $\bar{Q}$) and the input nodes to the DPUN output inverter. Adding the N-TFET that allowed the conduction between n1 and n2 nodes in both directions, the DPUN block used in order to build the logic gates for secure cryptographic applications is shown in Fig.6, while the waveforms once solved the bootstrapping and unidirectionality problems are shown in Fig.7.

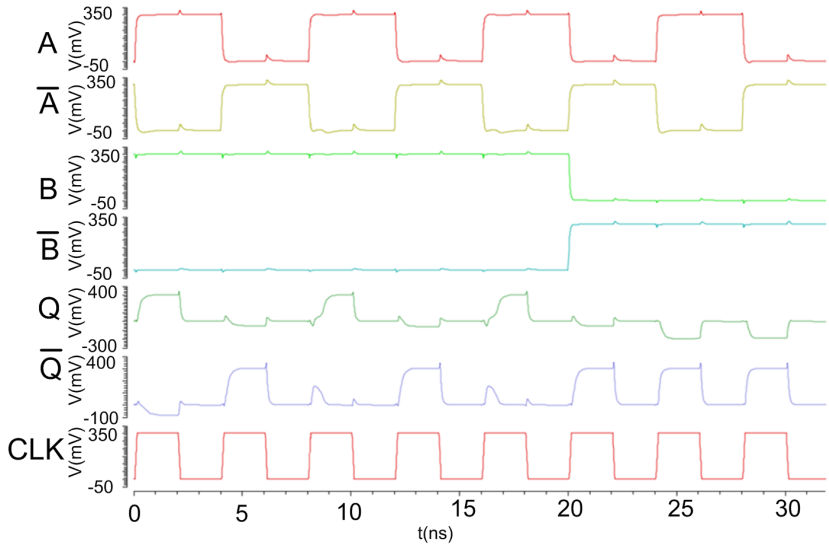


Fig. 5. Bootstrapped waveforms for TFET-based AND/NAND logic gates in original SABL style.

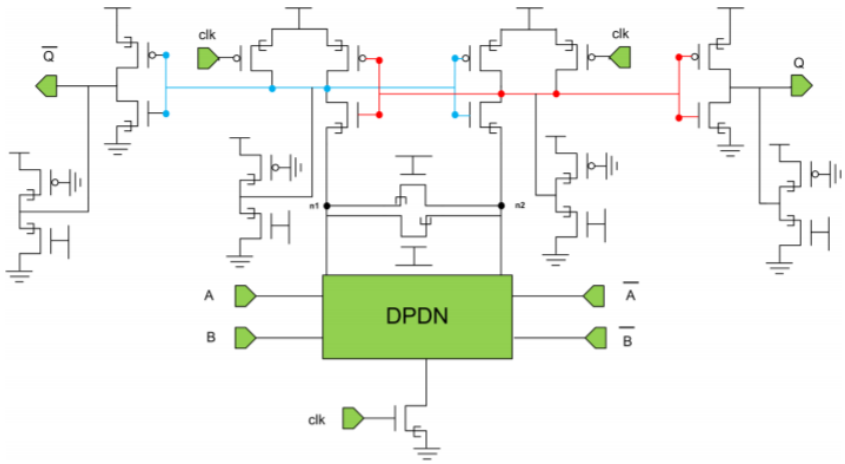


Fig. 6. DPUN block with modifications for TFET technology.

5 CASE STUDY AND RESULTS

The main goal of this work is to compare TFET implementations of cryptographic DPL primitives with conventional and emerging technologies (concretely, FinFET transistors) used in cryptographic applications to determine their vulnerability to DPA attacks.

TFET-based implementations are expected to have strong DPA resilience, due to the above mentioned carrier transport mechanism (BTBT) which reduces the probabilities of tunnel effect when the device is switched off, and hence it can operate at a very reduced supply voltage. This has two accumulative beneficial effects, reducing the power consumption figures, and making more

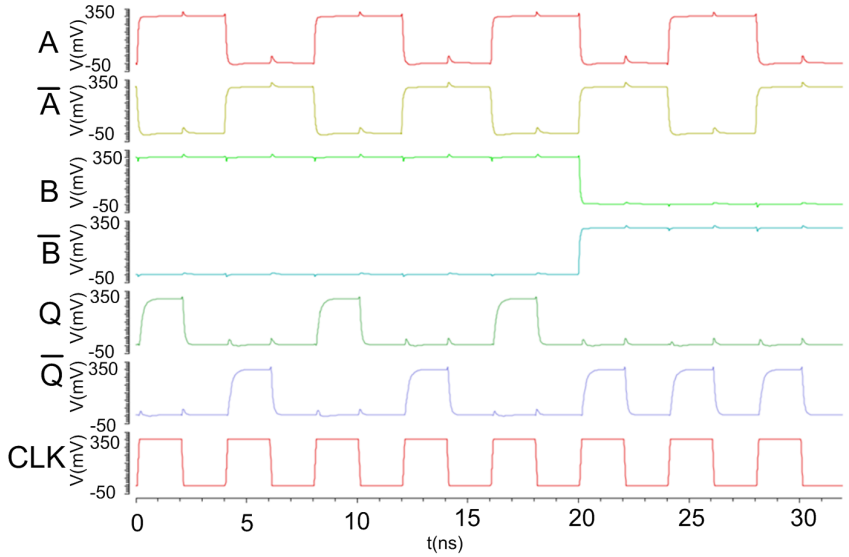


Fig. 7. Waveforms for TFET-based AND/NAND logic gates with solutions for bootstrapping.

difficult the guessing of data through power current traces. These two characteristics make TFET a promising device to implement low-power oriented secure cryptocircuits.

The current trend to reduce area and power consumption for portable security in the so-called lightweight cryptography is generating new families of low-resources algorithms [22]. In such context of lightweight cryptography, there exist several ciphers with excellent trade-off between hardware resources, security and power consumption. Since our study focuses on the applicability to security of new technologies and comparison with existing ones, the choice of a particular algorithm as case study is not critical. The selected cipher is PRIDE [1], a SPN (Substitution-Permutation Network) structure block cipher, with a 64-bit input plaintext and a 128-bit key during the encryption process executed in 20 operation rounds (being the first 19 rounds identical, and in the last round the linear layer is omitted). First, the 64-bit input is splitted into 16 4-bit nibbles which are XORed with the round key; then, the Sbox-4 is executed in parallel over the 16 nibbles and finally, permutated and processed by the linear layer. As stated in [1], PRIDE significantly outperforms all existing block ciphers of similar key-sizes, with the exception of SIMON and SPECK. Some preliminary work on Piccolo algorithm reveals that the results of the implementations presented in this paper are independent of the algorithm used as a case study.

As case study to evaluate the security level obtained by each proposed implementation, we will design, characterize and attack the PRIDE Sbox-4, which is the most vulnerable component in block ciphers. Most of the DPA attacks on block ciphers target this non-linear operation block (Sboxes), thus it is widely used as a vehicle to evaluate the security level reached by different countermeasure proposals against DPA attacks [5, 11, 16, 23, 24, 29, 31]. Since our purpose is to compare different technologies, we are going to analyze them from an attacker friendly scenario that allows us to set the same attack conditions. Therefore, an ideal environment without the presence of any noise will be useful to establish a comparison among technologies, where different factors apart from the technology ones are not taken into consideration. This Sbox-4 has been implemented in both CMOS, FinFET and TFET technologies, being the results completely transferable to other block ciphers. The Sbox-4 used by PRIDE is a 4-bit input ($x_0 - x_3$), 4-bit output ($y_0 - y_3$) combinational

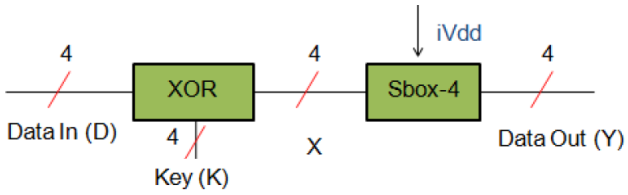


Fig. 8. Cryptographic device scheme.

block described by the equation (1):

$$\begin{aligned} y3 &= x1 \oplus x3x2 \\ y2 &= x0 \oplus x2x1 \\ y1 &= x3 \oplus y3y2 \\ y0 &= x2 \oplus y2y1 \end{aligned} \tag{1}$$

To build this Sbox-4, we have used 4 2-input XOR/XNOR and 4 2-input AND/NAND SABL gates. Each one of these gates uses 18 transistors for MOSFETs and FinFETs, following the scheme in Fig.1 and Fig2, and 27 transistors for TFETs, following the schemes in Fig.6 and Fig.2. These numbers lead to a total of 144 transistors for MOSFET and FinFET implementations of PRIDE Sbox-4, and 216 transistors when the implementation is TFET-based. These Sboxes have been designed under Cadence using the following technologies:

- TSMC: Standard 90-nm TSMC technology.
- TSMC-LP: Low-power 90-nm TSMC technology.
- MOSFET-PTM: Predictive technology models for 22 nm and 16 nm.
- FinFET-PTM: Predictive technology models for 20 nm and 16 nm.
- TFET: Technology model for 20 nm.

For a fair comparison, the DPDNs have been designed using the minimum transistor width in every technology, whereas DPUNs have been designed maintaining the same aspect ratio for all the implementations. Performance measurements (average power, worst-case delay, power-delay product (PDP), duty cycle) and security evaluations (DPA attacks) have been obtained through SPECTRE electrical simulations, integrated into the Cadence environment. Specifically, transient simulations for 2000 randomly generated plaintext patterns and a suitable simulation step of 5 ps have been carried out to capture with sufficient accuracy the power supply current waveforms with reasonable execution times for all the 16 possible keys. Nominal V_{dd} for each technology and T = 27 ºC have been used.

To measure the security level achieved by each implementation, simulation-based DPA attacks are carried out. The main objective of a DPA attacks is to recover the secret key K of a cryptographic device, in which the input or/and output patterns (D or/and Y) and the cryptographic algorithm are known. The implemented encryption process scheme is shown in Fig. 8 where D is the 4-bit input pattern randomly generated, K is the 4-bit key, X is the Sbox-4 input data get after the XOR operation between D and K, Y is a 4-bit output data and $iVdd$ is the measured supply current in the Sbox-4 during encryption.

The DPA attack has been carried out under MATLAB by following the procedure explained by Mangard et al. in [20] and it is completely analogous to the one done in [29] (Fig. 9). First, the power consumption ($iVdd_i$) of the implemented Sbox-4 is obtained, through electrical simulations under SPECTRE, during encryption for a huge number of input messages (D_i) with a fixed private key (K_{secret}). After that, the hypothetical power consumption values (H_{ij}) are mathematically calculated

Table 1. Performance and security data for the Sbox-4 PRIDE implementation in different technologies.

Technology	# Trans.	Vdd (V)	Avg.Power (μW)	Delay (ns)	PDP (fJ)	Duty Cycle (%)	MTD Key6	MTD Max	MTD Avg
TSMC-90	144	1.20	39.80	0.59	23.57	38.50	140	367	150.38
TSMC-90 LP	144	1.20	38.22	0.86	32.98	32.99	20	112	27.81
MOSFET-PTM 22 nm	144	0.95	2.21	1.00	2.21	26.67	112	465	221.94
MOSFET-PTM 16 nm	144	0.90	1.29	0.96	1.23	27.59	74	240	79.81
FinFET-PTM 20 nm	144	0.90	5.65	0.21	1.19	45.67	85	136	52.94
FinFET-PTM 16 nm	144	0.85	3.75	0.16	0.59	46.80	80	104	46.81
TFET 20 nm	216	0.30	0.86	1.02	0.87	28.46	>>2000	>>2000	>>2000

using the Hamming Distance power model [20], for all posible 16 keys (K_j). Then, the power supply current traces ($iVdd_i$) are correlated with the hypothetical power consumption values (H_{ij}). Finally, the correct key (K_{guess}) is the one with the maximum correlation value obtained in the previous step. To compare the robustness of the implemented Sboxes, the MTD (Measurements To Disclosure) [2, 32, 35] metric is used, being MTD the minimum number of power traces needed to retrieve the correct key. 2000 randomly generated patterns have been used processing the power traces and input patterns extracted from the SPECTRE simulation of the PRIDE Sbox-4 setup. Table 1 shows, for each implementation, the results in terms of performance and security. Supply voltage (Vdd), average power consumption, worst-case delay, PDP and duty cycle are given as classical performance figures of merit. In terms of security, we include Key6 (key attacked on the figures), maximum (Max.) and average (Avg.) MTD taking into consideration all the keys.

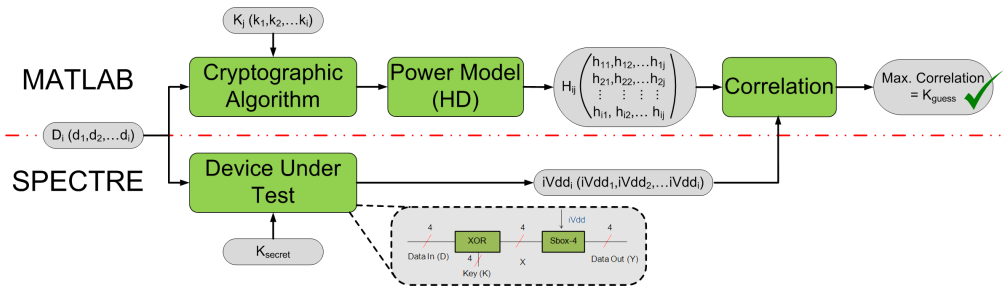


Fig. 9. DPA attack Flow.

As summary, the most impressive result that we can get from this table is that the key is not retrieved in any case for TFET technology since the MTD is higher than 2000 while for the rest of technologies, as an average, around 200 patterns are sufficient to retrieve the keys. Whereas there is not a highlighted key for the attack to the TFET-based implementation (Fig.10), Fig. 11 shows successful attacks for all the rest of technologies. In such figures, it is drawn the estimated correlation guessed in the DPA attack (Y-axis) versus the applied plaintexts (X-axis), for each one of the possible keys (each colour of the graph corresponds to one possible key). The MTD is evaluated when the correlation values becomes clearly different as the number of input plaintexts increase.

If we analyze these results in terms of performance, FinFET technologies obtain the best results taking into account delay and duty cycle. The figures of delay show an improvement of x5 for FinFET-PTM 20 nm compared to equivalent technological nodes (TFET 20 nm and MOSFET-PTM 22 nm) while the duty cycle is x1.60 and x1.71 better, respectively. Both nodes of FinFET technology

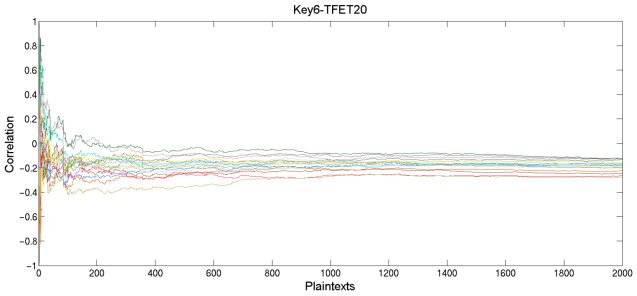
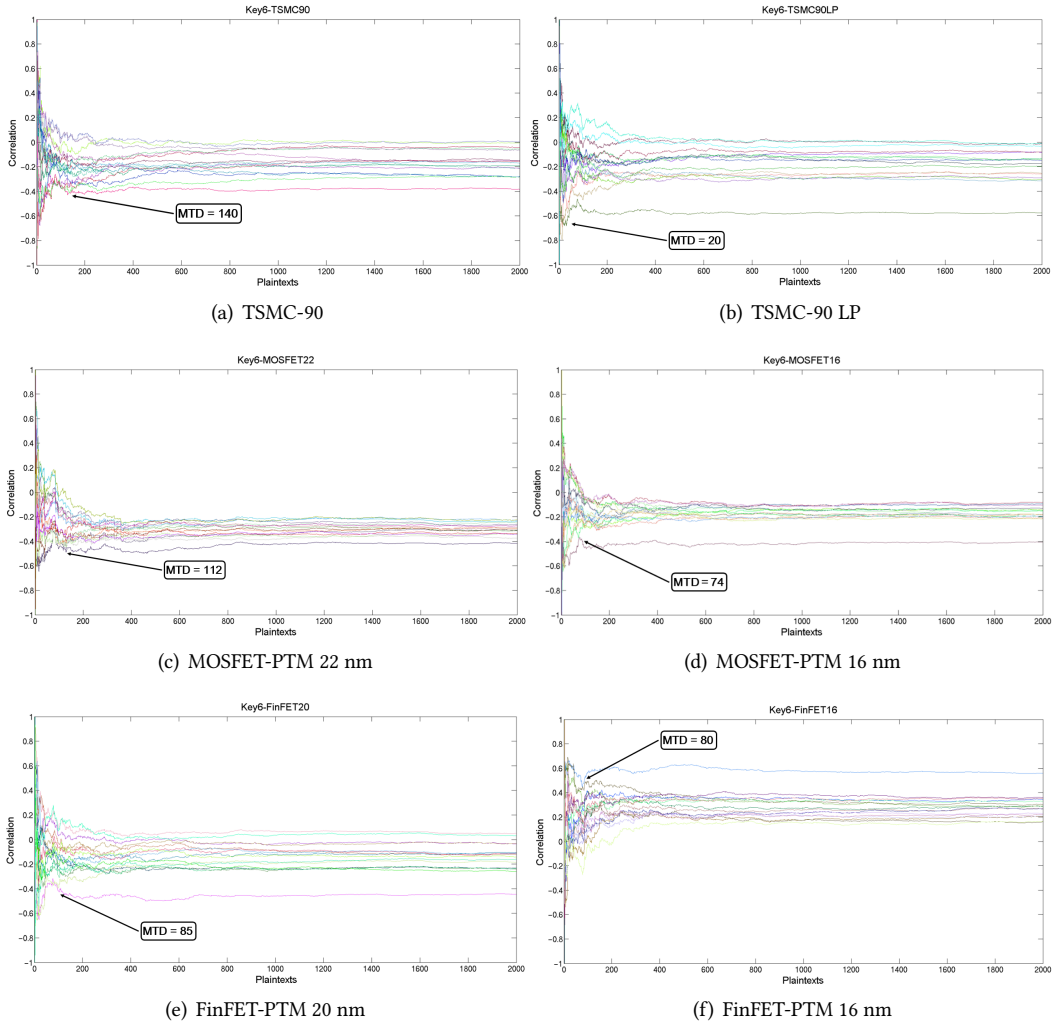


Fig. 10. Unsuccessful attack for TFET 20 nm technology. Correlation coefficients versus trace number (2000 input patterns for Key6)

show a much worse average MTD compared to TFET and MOSFET-PTM similar nodes. With a MTD figure around x3 worse than conventional technology TSMC-90, FinFET could represent a good alternative for applications where the relevance of speed on security is allowed for the cryptographic algorithm. Obviously, the best technology among all compared in terms of security is the TFET 20 nm one, since the secret key is not revealed in any case, when 2000 patterns are applied. Indeed, the Key6 = 0110 was randomly selected to perform an attack with a higher number of traces, in order to check if we are able to exactly determine how many traces are needed to retrieve the secret key for this implementation. Fig. 12 shows that an attack with 10000 traces is still unsuccessful in the mission of recovering the secret key. This enhances the idea of the TFET superior resistance against DPA attacks when compared with the rest of technologies considered in this work. Additionally, TFET obtains the best figures in terms of average power consumption, due to its low supply voltage, and the second one in terms of PDP, but with important drawbacks in terms of speed and duty cycle that could be prohibitive in specific applications. The area overhead is about 50%, but the gain in security is far above one order of magnitude.

A key point related to the effectiveness of a DPA attack is the power supply current trace shape. In this kind of attacks, we try to establish a correlation between the data being processed and the instantaneous power being consumed by the attacked blocks. There is a wide variety of models to guess which data consume a larger amount of power and which one less [20]. In this work, the model utilized has been the Hamming Distance applied to the output signal which implies that when a higher number of bits are changing at the output of the attacked block, we guess the power consumption is going to be higher. A clear and detailed explanation on how the attacks are performed can be found in [29]. The instantaneous power consumption of a certain block, in this case a Sbox, is given by $P_{inst} = V_{dd} \cdot I_{inst}$ being V_{dd} the supply voltage of the block and I_{inst} the instantaneous power supply current consumption. Since V_{dd} is constant, analyzing the instantaneous current point by point is equivalent to analyze instantaneous power consumption. Then, the power supply current trace is critical and important to correlate it with the data being processed, and try to recover the secret key. If we capture the power supply current trace during an encryption transition we find Fig.13: i) a peak of negative intensity corresponding to the clock rise in the change from precharge to evaluation phase; ii) a burst of positive intensity peaks corresponding to the different logic operations within the Sbox, six in our case; and iii) a last positive intensity peak in the evaluation-to-precharge transition.

It has been found an existing relationship between the power supply current peaks of ii) and the resistance to DPA attacks. Concretely, the narrower and higher the peaks, they are more distinguishable among them, hence, it is easier to establish a correlation between the power



(a) TSMC-90 (b) TSMC-90 LP

(c) MOSFET-PTM 22 nm (d) MOSFET-PTM 16 nm

(e) FinFET-PTM 20 nm (f) FinFET-PTM 16 nm

Fig. 11. Successful attacks for several technologies. Correlation coefficients versus trace number (2000 input patterns for Key6).

consumption and the operations carried out within the Sbox, so the DPA attack can reveal the correct key with a lower number of patterns. In Fig. 13, it is possible to observe the power supply current trace of 50 overlapped transitions for MOSFET-PTM 22nm, FinFET-PTM 20nm and TFET 20nm.

For the MOSFET case (a), peaks are not high but they are easy to differentiate due to its separation, facilitating to know the instants where logic operations are taking place. For the FinFET case (b), the technology is much faster than the rest and the peaks are closer among each others but they are very narrow, being easy to specify the phases of encryption during a transition. However, in the TFET case (c) the peaks are not narrow nor high. Thus it could be observed, a region of higher power consumption corresponding to evaluation but where the different logic operations are masked and not easy to distinguish by singular peaks. To conclude the analysis, Fig.14 shows a security vs

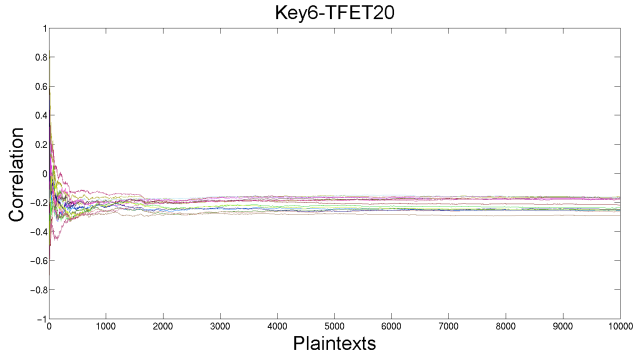
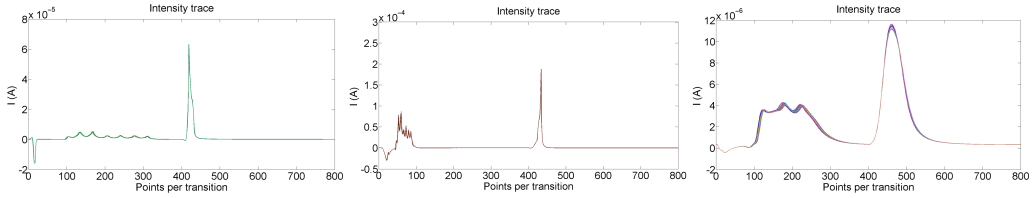


Fig. 12. Unsuccessful attack for TFET 20 nm technology. Correlation coefficients versus trace number (10000 input patterns for Key6).



(a) MOSFET-PTM 22 nm (b) FinFET-PTM 20 nm (c) TFET-PTM 20 nm

Fig. 13. Power supply current traces for scaled nodes of MOSFET, FinFET and TFET technologies.

performance design space map where the exceptional position of TFET Sbox-4 demonstrates the suitability of such emerging technology for DPL-based cryptographic primitives.

6 CONCLUSIONS AND FUTURE WORK

This work must be conceived as a first approach to measure the DPA resilience of circuits implemented with advanced and emerging technologies (specifically FinFET and TFET, respectively), using DPL-based logic gates to build hardware cryptographic algorithms. Due to the strict constraints required in order to design circuits for wearable and IoT applications, a trade-off between performance and security must be maximized. In this context, the possibility to use new devices is appealing due to the fact that MOSFET-based DPA resistant solutions present important drawbacks in terms of power, delay and area.

For these reasons, the use of FinFET and TFET transistors due to their extraordinary properties, as high ON/OFF ratio for both technologies, and low supply voltage in the case of TFETs, are considered for the design of DPL logic gates to be implemented in key cryptographic blocks, as it is the case of Sboxes. To allow this, we have modified the DPUN structure of SABL logic style in order to make it fully operative with TFET transistors, and to avoid some associated problems to this technology, as bootstrapping and unidirectional driving current. Sbox-4 of PRIDE algorithm has been implemented under CADENCE in TSMC 90 nm technology, TSMC low-power 90 nm technology, MOSFET predictive models for 22 nm and 16 nm, FinFET predictive models for 22 nm and 16 nm and a TFET model for 20 nm. DPA attacks were performed, obtaining interesting results.

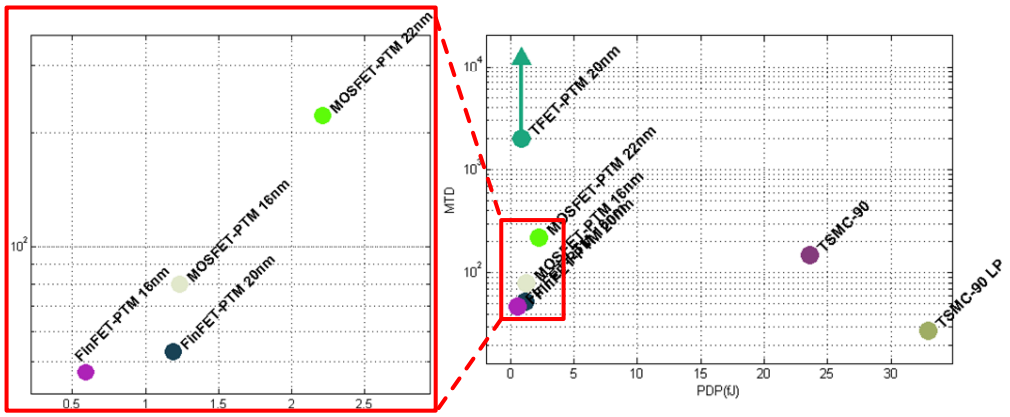


Fig. 14. Trade off: Security vs. PDP

Summarizing, it can be concluded that FinFET technology show clear improvements in terms of delay and duty cycle with important drawbacks in terms of security, where the behavior is inferior for both nodes compared to every other technology except TSMC-90 LP. Finally, TFET technology has proven its inherent resilience to DPA attacks since we have not been able to retrieve the correct key in any case applying 2000 patterns, and even 10000 patterns for a key randomly selected. Additionally, this technology, due to its low supply voltage presents the best values in terms of power consumption, although some trade-off considerations must be taken given its penalties in terms of delay and duty cycle.

As future work, specific and individual design for TFET DPL-based gates to be used in cryptographic applications will be considered in order to achieve an enhanced trade-off between security and performance, trying to reduce the delay and duty cycle penalties by increasing slightly the power consumption at the same time that security levels are improved.

ACKNOWLEDGMENTS

This work was partially supported by the Spanish Government by the Projects TEC2016-80549-R and TEC2017-87052-P with support from the European Regional Development Fund - FEDER.

REFERENCES

[1] Martin R. Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, and Tolga Yalçin. 2014. Block ciphers - Focus on the linear layer (feat. PRIDE). In *Lecture Notes in Computer Science*, 8616 LNCS (Ed.). Springer, 57–76. https://doi.org/10.1007/978-3-662-44371-2_4

[2] Massimo Alioto, Simone Bongiovanni, Milena Djukanovic, Giuseppe Scotti, and Alessandro Trifiletti. 2014. Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations. *IEEE Transactions on Circuits and Systems I: Regular Papers* 61, 2 (feb 2014), 429–442. https://doi.org/10.1109/TCSI.2013.2278350

[3] María José Avedillo and Juan Núñez. 2015. Improving speed of tunnel FETs logic circuits. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 51, 21 (oct 2015), 1702–1704. https://doi.org/10.1049/el.2015.2416

[4] Yu Bi, Kaveh Shamsi, Jiann-Shiun Yuan, Yier Jin, Michael Niemier, and Xiaobo Sharon Hu. 2017. Tunnel FET Current Mode Logic for DPA-Resilient Circuit Designs. *IEEE Transactions on Emerging Topics in Computing* 5, 3 (July 2017), 340–352. https://doi.org/10.1109/TETC.2016.2559159

[5] Kean Hong Boey, Maire O'Neill, and Roger Woods. 2011. How Resistant are Sboxes to Power Analysis Attacks?. In *2011 4th IFIP International Conference on New Technologies, Mobility and Security*. IEEE, 1–6. https://doi.org/10.1109/NTMS.2011.5720614

[6] Thomas De Cnudde and Svetla Nikova. 2017. Securing the PRESENT block cipher against combined side-channel analysis and fault attacks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 25, 12 (Dec. 2017), 3291–3301.

https://doi.org/10.1109/TVLSI.2017.2713483

[7] C.H. Gebotys. 2006. A table masking countermeasure for low-energy secure embedded systems. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 14, 7 (July 2006), 740–753. https://doi.org/10.1109/TVLSI.2006.878344

[8] Yu-Ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger. 2013. Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures. *IEEE Transactions on Electromagnetic Compatibility* 55, 3 (June 2013), 571–580. https://doi.org/10.1109/TEMC.2012.2227486

[9] IEEE. [n.d.]. IEEE International Roadmap for Devices and Systems. Retrieved April 8, 2019 from https://irds.ieee.org/

[10] Yuval Ishai, Amit Sahai, and David Wagner. 2003. Private Circuits: Private Circuits Securing Hardware against Probing Attacks. In *Proceedings of International Cryptology Conference (CRYPTO'03)*. Springer, Berlin, Heidelberg, 463–481.

[11] Hyunmin Kim, Vladimir Rozic, and Ingrid Verbauwhede. 2012. Three phase dynamic current mode logic: A more secure DyCML to achieve a more balanced power consumption. Springer, Berlin, Heidelberg, 68–81. https://doi.org/10.1007/978-3-642-35416-8_6

[12] Paul Kocher. 1996. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, Other Systems. In *Proceedings of International Cryptology Conference (CRYPTO'96)*. 104–113. https://doi.org/10.1007/3-540-68697-5_9

[13] Paul Kocher, Joshua Jaffe, and Benjamin Jun. 1999. Differential Power Analysis. In *Proceedings of International Cryptology Conference (CRYPTO'99)*. Springer, Berlin, Heidelberg, 388–397. https://doi.org/10.1007/3-540-48405-1_25

[14] S. Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. 2018. 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* 37, 1 (Jan. 2018), 110–122. https://doi.org/10.1109/TCAD.2017.2685588

[15] Itamar Levi, Alexander Fish, and Osnat Keren. 2017. CPA secured data-dependent delay-assignment methodology. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 25, 2 (Feb. 2017), 608–620. https://doi.org/10.1109/TVLSI.2016.2592967

[16] Owen Lo, William J. Buchanan, and Douglas Carson. 2017. Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). *Journal of Cyber Security Technology* 1, 2 (apr 2017), 88–107. https://doi.org/10.1080/23742917.2016.1231523

[17] Hao Lu, David Esseni, and Alan Seabaugh. 2015. Universal analytic model for tunnel FET circuit simulation. *Solid-State Electronics* 108 (jun 2015), 110–117. https://doi.org/10.1016/j.sse.2014.12.002

[18] Hao Lu and Alan Seabaugh. 2014. Tunnel field-effect transistors: State-of-the-art. *IEEE Journal of the Electron Devices Society* 2, 4 (jul 2014), 44–49. https://doi.org/10.1109/JEDS.2014.2326622

[19] Rwan Mahmoud, Yousuf Tasneem, Fadi Aloul, and Imran Zualkernan. 2015. Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 336–341. https://doi.org/10.1109/ICITST.2015.7412116

[20] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. 2007. *Power analysis attacks: Revealing the secret of smart cards*. Springer.

[21] Daniel H. Morris, Uygar E. Avci, Rafael Rios, and Ian A. Young. 2014. Design of Low Voltage Tunneling-FET Logic Circuits Considering Asymmetric Conduction Characteristics. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 4, 4 (dec 2014), 380–388. https://doi.org/10.1109/JETCAS.2014.2361054

[22] Matthew A. Morrison, Nagarajan Ranganathan, and Jay Ligatti. 2017. Design of Adiabatic Dynamic Differential Logic for DPA-Resistant Secure Integrated Circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 1, 2 (apr 2017), 88–107. https://doi.org/10.1109/TVLSI.2014.2342034

[23] Stjepan Picek, Kostas Papagiannopoulos, Barış Ege, Lejla Batina, and Domagoj Jakobovic. 2014. Confused by confusion: Systematic evaluation of DPA resistance of various S-boxes. In *15th International Conference on Cryptology in India (INDOCRYPT'14)*. Springer, New Delhi, India, 374–390. https://doi.org/10.1007/978-3-319-13039-2_22

[24] Emmanuel Prouff. 2005. DPA Attacks and S-Boxes. In *2005 12th Fast Software Encryption Workshop (FSE'05)*. Springer, Berlin, Heidelberg, 424–441. https://doi.org/10.1007/11502760_29

[25] Sneh Saurabh and Mamidala Jagadesh. 2016. *Fundamentals of tunnel field effect transistors*. CRC Press.

[26] Patrick Schaumont and Kris Tiri. 2007. Masking and dual-rail logic don't add up. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 95–106.

[27] Saurabh Sinha, Greg Yeric, Vikas Chandra, Brian Cline, and Yu Cao. 2012. Exploring sub-20nm FinFET design with predictive technology models. In *Proceedings of the 49th Annual Design Automation Conference - DAC '12*. ACM Press, New York, New York, USA. https://doi.org/10.1145/2228360.2228414

[28] Shayan Taheri and Jiann-Shiun Yuan. 2017. Security analysis of tunnel field-effect transistor for low power hardware. *International Journal of Computer Science and Information Technologies (IJCSIT)* 8, 2 (2017), 271–275. www.ijcsit.com

[29] Erica Tena-Sánchez, Javier Castro, and Antonio J. Acosta. 2014. 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* 4, 2 (June 2014), 203–215. https://doi.org/10.1109/JETCAS.2014.2315878

[30] Erica Tena-Sánchez, Ignacio M. Delgado-Lozano, Juan Núñez, and Antonio J. Acosta. 2018. Benchmarking of nanometer technologies for DPA-resilient DPL-based cryptocircuits. In *2018 Conference on Design of Circuits and Integrated Systems (DCIS'18)*.

[31] Kris Tiri, Moonmoon Akmal, and Ingrid Verbauwhede. 2002. 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, 403–406.

[32] Kris Tiri, David Hwang, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, and Ingrid Verbauwhede. 2005. Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment. In *International Workshop on Cryptographic Hardware and Embedded Systems (CHES'05)*. Springer, Berlin, Heidelberg, 354–365. https://doi.org/10.1007/11545262_26

[33] Kris Tiri and Ingrid Verbauwhede. 2004. A logic level design methodlogy for a secure DPA resistant ASIC or FPGA implementation. In *Design, Automation and Test in Europe (DATE'04)*. IEEE, 246–251. https://doi.org/10.1109/DATE.2004.1268856

[34] Kris Tiri and Ingrid Verbauwhede. 2005. Design method for constant power consumption of differential logic circuits. In *Design, Automation and Test in Europe (DATE'05)*. IEEE, 628–633. https://doi.org/10.1109/DATE.2005.113

[35] Kris Tiri and Ingrid Verbauwhede. 2005. A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs. In *Design, Automation and Test in Europe (DATE'05)*. IEEE, 58–63. https://doi.org/10.1109/DATE.2005.44

[36] Teng Xu, James B. Wendt, and Miodrag Potkonjak. 2014. Security of IoT systems: Design challenges and opportunities. In *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 417–423. https://doi.org/10.1109/ICCAD.2014.7001385

[37] Meng Zhang and Niraj K. Jha. 2011. FinFET-based power management for improved DPA resistance with low overhead. *ACM Journal on Emerging Technologies in Computing Systems* 7, 3 (Aug. 2011), 1–16. https://doi.org/10.1145/2000502.2000503

[38] Wei Zhao and Yu Cao. 2006. New generation of predictive technology model for sub-45nm design exploration. In *7th International Symposium on Quality Electronic Design (ISQED'06)*. IEEE. https://doi.org/10.1109/ISQED.2006.91