Gate-Level Design Methodology for Side-Channel Resistant Logic Styles Using TFETs

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

***Abstract*—The design of secure circuits in emerging technologies is an appealing area that requires new efforts and attention as an effective solution to secure applications with power constraints. The paper deals with the optimized design of DPA-resilient hiding-based techniques, using Tunnel Field-Effect Transistors (TFETs). Specifically, proposed TFET implementations of Dual-Precharge-Logic primitives optimizing their computation tree in three different ways, are applied to the design of PRIDE Sbox-4, the most vulnerable block of the PRIDE lightweight cipher. The performance of simulation-based DPA attacks on the proposals have shown spectacular results in security gain (34 out of 48 attacks fail for optimized computation trees in TFET technology) and power reduction (x25), compared to their CMOS-based counterparts in 65nm, which is a significant advance in the development of secure circuits with TFETs.**

***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, TFET**

I. Introduction

In recent years, the scaling of CMOS technologies has significantly reduced power consumption reaching a practical limit, since the scaling of the supply voltages in order to reduce the dynamic power consumption, while maintaining adequate speed, is counterbalanced by the exponential growth of the leakage currents. In order to address the demanding consumption and performance constraints in new applications, as it is the case of portable devices, wearables, etc., the dimensional and functional scaling of CMOS technologies must be pushed beyond what Moore's Law allows. In this sense, the advent of emerging devices ("beyond-CMOS") allows the scaling up of integrated circuits and the increase of their performance beyond what is established in Moore's Law. This, ultimately, leads them to complement or replace CMOS technologies. The so-called "steep-slope" devices, which are characterized by inverse sub-threshold (SS) slopes below 60mV/dec, the physical limit for CMOS technologies at room temperature, are now receiving a great deal of attention. The reduction of SS allows the threshold voltage to be reduced without increasing the leakage current excessively, obtaining high ratios between the ON current (ION) and the OFF current (IOFF), resulting in highly energy-efficient circuits with extremely low supply voltages and low power consumption. The Tunnel Field-Effect Transistors (TFET) are the most studied steep-slope devices [1], [2]. The particular characteristics of these devices are showing great advantages for secure low-power applications [3], [4].

It is important to notice that, although cryptocircuits implement mathematically secure algorithms, their physical implementation, regardless of the used technology, leaks side-channel information that could be used by third parties to reveal private data, through the well known side-channel attacks (SCAs) [5], [6]. Among SCAs, those exploiting power consumption (Differential Power Analysis, DPA attacks [5]) have been positioned as some of the most powerful attacks due to their effectiveness and low cost. The security of cryptographic circuits against DPA is determined by their resilience against attacks, where the main objective is to obtain the secret key or information processed by the device, using power consumption as an attack vector during encryption/decryption processes. To counteract DPAs, a wide range of countermeasures have been proposed. These countermeasures can be applied at different abstraction levels, going from algorithm (higher level of abstraction) to those applied at gate level (lower abstraction). The ones targeting directly the source of information leakage, this means to try to have the same power consumption during operation regardless of the data being processed, are the hiding countermeasures at gate level, applied to the lower level of abstraction. Among them, Dual Precharge Logic (DPL) styles have been posed as the ones with the best security metrics if properly implemented [7], [8]. The main objective of this paper is to propose and evaluate advanced DPL-based countermeasures to obtain the highest security levels using the advantages provided by emerging technologies, most specifically, with TFETs.

The organization of the paper is as follows. In Section II, the security proposal is presented. Section III exposes the security evaluation of the proposed countermeasures and attack results. Finally, the conclusions are depicted in Section IV.

II. Security Proposal

TFET stands out as the best positioned of a wide range of emerging devices [9]. The potential of these transistors to operate with a reduced supply voltage and, therefore, achieving significant power and energy compared to conventional MOSFETs or FinFETs in applications requiring moderate operating frequencies, has been shown in [10], [11]. On the other hand, speed advantages have also been demonstrated in applications with severe limitations on power dissipation or energy consumption [12], [13].

The use of TFETs has been shown to have a positive impact on hardware security, being able to provide superior security in integrated circuits. In [14] and [15], it is highlighted

Ignacio M. Delgado-Lozano is with the Network and Information Security Group (NISEC) of Tampere University, Tampere, FINLAND, 33720. E-mail:ignacio.delgadolozano@tuni.fi. He is financially supported in part by HPY Research Foundation.

Erica Tena-Sánchez, Juan Núñez and Antonio J. Acosta are with Instituto de Microelectrónica de Sevilla IMSE-CNM (Universidad de Sevilla CSIC), Seville, SPAIN, 41092. E-mail: {erica, jnunez, acojim}@imse-cnm.csic.es

that TFETs can help improve circuit design resilience against power analysis attacks while still preserving low power consumption compared to their CMOS counterparts. The impact that the specific characteristics of TFETs impose from a circuit design perspective has been explored in [16], [17], and involves modifications in the direct migration of CMOS circuit topologies to a TFET-based design style. Especially relevant to this work is the impact of circuit operation effects associated to the low conduction of the n-type (p-type) TFET transistors with negative (positive) drain to source voltage.

The use of DPL logic styles to achieve the same power consumption during operation has been demonstrated to be extremely secure if symmetrically placed and routed [7], [8], [18]. An extra security level can be added to these logic styles if some modifications are applied in the Differential Pull Down Network (DPDN) structure [8]. The optimization of the DPDN, and hence the overall security level of the gate, was improved by setting at the same voltage the internal nodes of the DPDN. Due to the voltage differences in the internal nodes of the DPDN branches (see nodes n1 and n2 in Figure 1), the evaluation of the next stage of both differential branches starts at different voltage values causing information leakage exploitable by DPA attacks [8]. Unfortunately, the migration from CMOS structures to TFET implementations is not straightforward, and a redesign process is needed to adequate the correct functionality of the TFET gates. As studied in [15], using as Differential Pull Up Network (DPUN) a modification of SABL logic style using TFET devices, achieves high security levels even with a great reduction in power consumption compared to their conventional CMOS counterparts. This security level in DPL-based CMOS circuits can be improved including some optimization in the DPDN structure [8]. The main goal of this paper is to adapt the methodology followed in [8] but using TFET devices, which is not straightforward due to the unidirectionality of TFETs.

The design methodology of the optimized DPDN structure using TFET devices adapts the two approaches presented in [8] for CMOS technologies: i) equalizing the voltage values after evaluation phase in the internal nodes $n1$ and $n2$ using the $single-switch$ (P) solution, and ii) setting the voltage value in $n1$ and $n2$ at the same V_{DD} value using the $double-switch$ (2P) solution [19]. In the adaptation to TFET technology, the $single-switch$ solution (P) requires two transistors because of the characteristic unidirectionality of TFETs. This way, the equalization of voltages in $n1$ and $n2$ is possible in both directions, while in a hypothetical solution that uses only one transistor, the conduction would be impossible in one of the two possible directions. In Figure 1, the DPDN optimization schematic using SABL logic style as DPUN is shown.

III. Evaluation and Results

In [15], [19], it was demonstrated that DPL-based DPA resistant gates are good candidates to replace CMOS counterparts for low-power secure systems against DPA attacks. This paper aims to demonstrate that additional countermeasures, as the ones presented in [8], [19] can also be implemented in TFET, with competitive security-cost trade-off. As a demonstrative vehicle we use the lightweight block cipher PRIDE [20], which uses a 64-bit input plaintext and a 128-bit key for the encryption in a total of 20 operation rounds. Concretely, our attack is focused on the 4-bit substitution box (Sbox-4) that this cipher implements. Many DPA attacks address their threats to this non-linear block to retrieve, in groups of bits, the secret key of block ciphers [6], [8]. The Sbox-4 included in the PRIDE block cipher is a 4-bit input ($x_0 - x_3$), 4-bit output ($y_0 - y_3$) combinational block described by the equation (1):

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

Thus, for the configuration of this Sbox-4 we need four 2-input XOR/XNOR and four 2-input AND/NAND SABL gates. To analyze and compare the suitability of the modifications proposed in section II for TFETs, we use four different configurations:

- Classic: Classic SABL [7] implementation for a 65nm commercial technology from UMC foundry (UMC65) and its adaptation for TFETs [15].
- P: P modification for both XOR/XNOR and AND/NAND gates in UMC65 [8], [19] and its adaptation for TFETs presented in this work.
- 2P: 2P modification for both XOR/XNOR and AND/NAND gates in UMC65 [8], [19] and its adaptation for TFETs presented in this work.
- P2P: P modification for AND/NAND gates and 2P modification for XOR/XNOR gates and its adaptation for TFETs, since in [8], [19], the authors demonstrated the better suitability of P modification for AND/NANDs and of 2P for XOR /XNORs.

In order to provide a fair comparison between these two very different technologies, we have designed the DPDN blocks using the minimum transistor width, while in the DPUN blocks we have maintained the same aspect ratio in both technologies, with the minimum transistor width that ensures the proper operation of the logic gates that constitute the Sbox-4. As benchmarking, we carried out transient simulations for 5000 randomly generated plaintext patterns for all the 16 possible keys for 4-bit Sbox. Nominal V_{dd} (V_{dd} = 1.2 V for UMC65 and V_{dd} = 0.3 V for TFETs) and T=27 ºC have been used to perform these experiments. In terms of performance measurements, we have captured the peak of maximum power consumption (Max. Power), the average power consumption (Avg. Power) in a clock cycle, the average delay (Avg. Delay) in the output, the power-delay product (PDP) and the duty cycle. These results have been captured using SPECTRE electrical simulations, as a part of the CADENCE environment. It is important to notice, that we do not aim to directly compare these two technologies, especially in terms of performance figures of merit. Our objective is, rather, to determine if our implementations with TFET technology and its corresponding modifications present an overwhelming better security level that justify the differences in terms of performance. This way, due to the the higher nominal V_{dd}, we expect that power figures are worse from the classical UMC65 compared to those

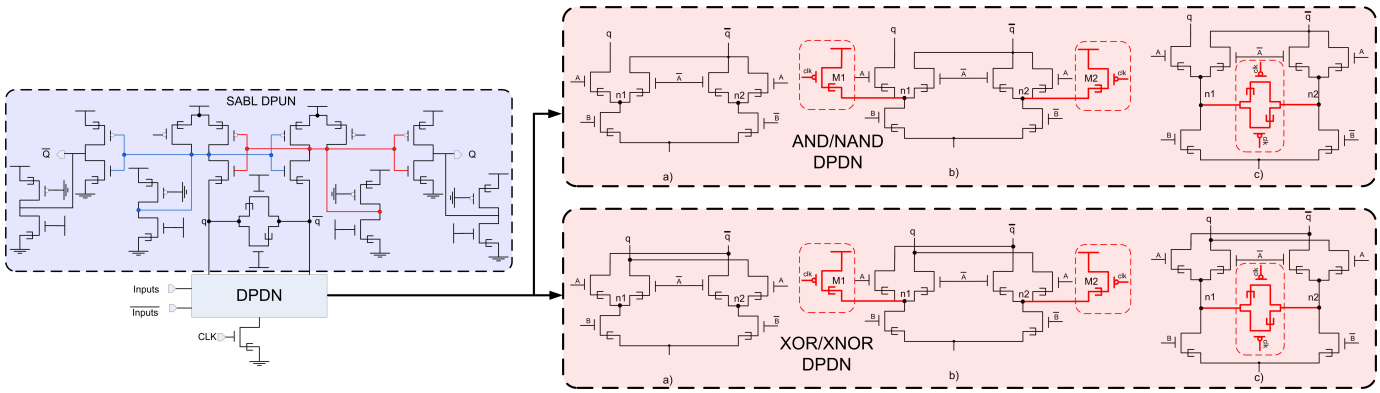

Fig. 1. TFET SABL structure schematic with DPDN 2P/P optimizations.

TABLE I
PERFORMANCE AND SECURITY RESULTS FROM ATTACKS OVER UMC65 AND TFET TECHNOLOGIES USING P, 2P, AND P2P MODIFICATIONS.

Tech.	Proposal	Max. Power(μW)	Avg. Power(μW)	Avg. Delay(ns)	PDP(fJ)	Duty Cycle(%)	Min. MTD	Avg. MTD	Failed Attacks
TFET	**Classic**	3.01	0.86	1.02	0.87	28.46	189	2175.56	5
	2P	3.98	1.04	1.23	1.29	23.01	491	4437.63	11
	P	2.96	0.89	1.04	0.92	28.94	4992	4999.50	15
	P2P	3.32	0.96	1.15	1.10	25.01	500	3014.33	8
UMC65	**Classic**	228.14	21.05	0.67	14.16	35.34	5	45.31	0
	2P	339.03	25.88	0.75	19.40	32.73	35	1531.25	3
	P	220.30	21.83	0.67	14.63	35.71	6	77.56	0
	P2P	253.23	23.50	0.72	16.85	33.55	64	1131.19	0

from emerging TFET technology. For the same reason, the performance figures presented (delay, duty cycle) should be better in the classical approach compared to the emerging one, since a higher V_{dd} allows a faster switching of transistors, which is especially important in the use of digital logic gates.

In terms of security, we have analyzed the different Sboxes composed of the logic gates that we have modified in both technologies from an attacker-friendly scenario. This means that we have set an ideal environment where we avoided the presence of any noise in order to establish a fair comparison where other factors apart from the technology and the modifications of each implementation do not interfere with the final security result. To carry out our DPA attacks, we have used a Hamming Distance power model running a MATLAB routine that follows the procedure presented by [6], [8], [15]. Although the use of dynamic logics presenting evaluation and precharge phases, could lead to think that a Hamming Weight model is more appropriate to find correlations between power and data, the memory effect present in n1 and n2 makes the Hamming Distance a more suitable model to retrieve the correct key, by performing such correlations. To compare the security level achieved by the several Sboxes implemented, among the widely used range of evaluation metrics available, we use the number of Measurements to Disclose (MTD) the correct key. Concretely, in Table I we include the average MTD over the 16 possible keys, as well as the minimum MTD to have an idea about the worst case attacks. Taking into account that our attack applies 5000 patterns to retrieve the correct key in each case, we have included a column that represents the number of attacks that are not able to disclose the correct key (failed attacks) out of the 16 possible keys from the 4-bit Sbox. In these cases, the MTD considered for these keys is MTD = 5000, although probably in some cases the result would have been MTD $>>$ 5000.

Table I shows the main results obtained for the different technologies and implementations. As summary, we can conclude that the modifications proposed for both technologies improve the security results. Concretely, the implementation that better works for the classic UMC65 technology is the one that incorporates 2P modification in both AND/NAND and XOR/XNOR gates, with an MTD x33.80 better compared to the classic proposal in this technology. A good result is obtained also by the P2P proposal with an MTD x24.97 better. However, the P implementation only outperforms the results obtained by the classical proposal on a factor of x1.71.

In the case of the emerging TFET technology, the best implementation in terms of security is the one that presents the P modification, which shows an Avg. MTD = 4999.50 (x2.29 compared to regular SABL), but with only one successful attack out of the different 16 keys. For this reason, the Avg. MTD can be misleading, since probably the real value is quite higher, but we decided to use MTD = 5000 when the attack is not successful as we are not able to ensure the exact number of patterns required to have a successful attack. Nonetheless, we can ensure that MTD $>>$ 5000. On other issues, P and P2P implementations also outperform the numbers achieved by the regular SABL proposal (x2.04, and x1.39). In terms of a security comparison between both technologies, we can conclude that TFET technology is more suitable for the use in this kind of security applications, not only because when comparing best cases from both technologies TFETs outperform the result obtained by UMC 65 in a factor x3.27,

but also because we are not able to retrieve the correct key in many cases (39 out of 64) with 5000 patterns, while for the UMC65 only 3 attacks out of the total 64 fail.

In terms of performance, for both technologies the 2P modification worsen the results obtained by the classic implementation in around a 21% in all performance and average power measurements for TFETs, showing a PDP value a 48% worse than in the classic implementation. For UMC65, the power consumption figure is a 23% worse, while the delay and the PDP values are a 12% and a 37% worse respectively. For the P implementation, the results are very similar to those obtained by the classical approach, it is possible to observe a slight improvement in the duty cycle value, while the delay, power (and obviously, PDP) are negligibly higher due to the inclusion of a higher number of transistors. This way, P proposal clearly outperforms classic SABL in terms of security, while having very similar performance figures for TFETs. In the middle, we can find P2P modifications that present worse statistics in a range of 6-11% concerning power, delay and duty cycle output, while the PDP is worse in a 19% in the case of UMC65, and a 26% for TFETs.

Finally, if we compare generally both technologies, we clearly observe much superior power figures of merit for the emerging technology TFET when compared to the classical UMC65, having roughly x25 times less power consumption. On the other hand, UMC65 outperforms TFET concerning figures as the delay or the duty cycle with factors near to x1.5 and x1.25, respectively. However, in the trade-off between power consumption and delay, the PDP figures show how clearly TFET surpass UMC65 with figures roughly x15 times superior. Although we have already commented that the comparison between both technologies would never be fair and direct because of the different characteristics as the supply voltage V_{dd}, these results where TFET clearly obtains better figures of merit in terms of security and power consumption state that TFET technology is a clear contender to take into consideration when designing lightweight security applications in the immediate future.

IV. Conclusions

The paper has addressed the use of TFETs in the optimized design of three different proposals for the DPDN block of DPL structures, of recognized strength against DPA attacks, consisting in the elimination of residual charge in internal nodes of the tree: proposals named as P, 2P and P2P. The low conduction effects of the (p)nTFET with (positive) negative voltage from the drain to the source have been taken into account for the adaptation of the reference SABL structure, in the realization of XOR/XNOR, AND/NAND and OR/NOR gates. The proposals have been applied in the design of the Sbox-4 block of the PRIDE cipher, that have been fully characterized. Simulation-based DPA attacks on different Sbox-4 have been performed, showing stunning gains in security and power reduction, compared to the counterparts realized in 65 nm CMOS technologies. Particularly, a x15 improvement in power-delay figures are found, with a variable gain in security figures ranging from a minimum of x2, with a big amount of failed attacks for TFET proposals. As future work, the corroboration of security via Mutual Information Analysis (MIA) or Test Vector Leakage Assessment (TVLA), will be performed. As main conclusion, there is room enough for new increments in security by using emerging technologies in low-power secure applications.

V. Acknowledgments

This work was partially funded by the Spanish Government with support from FEDER under Projects TEC2017-87052-P and PID2020-116664RB-I00, by Programa Operativo FEDER 2014-2020 and Consejería de Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía (Projects US-1380876 and US-1380823) and by the SPIRS and SCARE Projects with Grant Agreement No. 952622 and No. 804476, respectively, under the European Union's Horizon 2020 research and innovation programme.

References

[1] K. Swaminathan, H. Liu, X. Li, M.S. Kim, J. Sampson, V. Narayana, "Steep slope devices: Enabling new architectural paradigms", *51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2014.

[2] U. E. Avci, D.H. Morris and I.A. Young, "Tunnel Field-Effect Transistors: Prospect and Challenges", *IEEE Journal of the Electron Device Society*, vol. 3, no. 3, pp. 88-95, Jan. 2015.

[3] J. Yuan, J. Lin, Q. Alasad, S. Taheri, "Ultra-Low-Power Design and Hardware Security Using Emerging Technologies for Internet of Things", *Electronics*, vol. 6, pp. 67, Sep. 2017.

[4] S. Taheri, J. Yuan, "Security Analysis of Tunnel Field-Effect Transistor for Low Power Hardware", 2017.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", *Proc. of International Cryptology Conference (CRYPTO'99)*, pp. 388-397, 1999.

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

[7] K. Tiri, M. Akmal, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards", *in Proc. of the European Solid-State Circuits Conference (ESSCIRC'02)*, pp. 403-406, 2002.

[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] Nikonov, Dmitri E., and Ian A. Young. "Benchmarking of beyond-CMOS exploratory devices for logic integrated circuits", *IEEE Journal on Exploratory Solid-State Computational Devices and Circuits*, vol. 1 pp. 3-11, Dec. 2015.

[10] A.M. Ionescu, H. Riel: "Tunnel field-effect transistors as energy-efficient electronic switches", *Nature*, no. 479, pp. 329–337, 2011.

[11] K. Swaminathan et al., "Modeling Steep Slope Devices: From Circuits to Architectures", *Proc. of Design, Automation and Test in Europe Conference (DATE'14)*. Dresden, Mar. 2014.

[12] M. Alioto and D. Esseni, "Tunnel FETs for Ultra-Low Voltage Digital VLSI Circuits: Part II–Evaluation at Circuit Level and Design Perspectives", *IEEE Trans. on VLSI Systems*, vol. 22, no. 12, pp. 2499-2512, Dec. 2014.

[13] J. Núñez and M. J. Avedillo, "Comparative Analysis of Projected Tunnel and CMOS Transistors for Different Logic Application Areas," *IEEE Transactions on Electron Devices*, vol. 63, no. 12, pp. 5012-5020, 2016.

[14] Y. Bi, K. Shamsi, J. 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, 1 July-Sept. 2017.

[15] I.M. Delgado-Lozano, E.Tena-Sánchez, J.Núñez, and A.J.Acosta. "Projection of Dual-Rail DPA Countermeasures in Future FinFET and Emerging TFET Technologies". *ACM Journal on Emerging Technologies in Computing Systems*, vol. 16, no. 3, art. 30, May 2020.

[16] A. Pal et al., "Insights into the design and optimization of tunnel-FET devices and circuits", *IEEE Trans. on Electron Devices*, vol. 58, no. 4, pp. 1045-1053, April 2011.

[17] J. Núñez, M. J. Avedillo, "Reducing the Impact of Reverse Currents in Tunnel FET Rectifiers for Energy Harvesting Applications", *IEEE Journal of Electron Devices Society*, vol. 5, no. 6, pp. 530-534, Nov. 2017.

[18] K. Tiri, and I. Verbauwhede, "Place and Route for Secure Standard Cell Design", on Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS'04), pp. 143–158, 2004.

[19] E.Tena-Sánchez, J. Castro, and A. J. Acosta. "Low-Power Differential Logic Gates for DPA Resistant Circuits", *17th Euromicro Conference on Digital System Design (DSD)*, pp. 671-674, 2014.

[20] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar and T. Yalçin, "Block Ciphers- Focus on the Linear Layer (feat. PRIDE) Full Version". *Proc. of International Cryptology Conference (CRYPTO'14)*, pp. 57-76, 2014.