Low-Power Differential Logic Gates for DPA Resistant Circuits

Erica Tena-Sánchez
Instituto de Microelectrónica de Sevilla
Universidad de Sevilla/CNM-CSIC, Spain
Email: erica@imse-cnm.csic.es

Javier Castro
Anafocus Company
Seville, Spain
Email: jcastro@anafocus.com

Antonio J. Acosta
Instituto de Microelectrónica de Sevilla
Universidad de Sevilla/CNM-CSIC, Spain
Email: acojim@imse-cnm.csic.es

Abstract—**Information leakaged by cryptosistems can be used by third parties to reveal critical information using Side Channel Attacks (SCAs). Differential Power Analysis (DPA) is a SCA that uses the power consumption dependence on the processed data. Designers widely use differential logic styles with constant power consumption to protect devices against DPA. However, the right use of such circuits needs a fully symmetric structure and layout, and to remove any memory effect that could leak information. In this paper we propose improved low-power gates that provide excellent results against DPA attacks. Simulation-based DPA attacks on Sbox9 are used to validate the effectiveness of the proposals.**

I. Introduction

Nowadays the security of users private information is a major concern. Embedded electronic devices usually store private information, making use of cryptography to ensure data confidentiality. These cryptocircuits implement mathematically secure algorithms, but because of their physical implementation, they leak information (power, timing, EMI, etc) that could be used by third parties to reveal private data, through side-channel attacks (SCAs). Thus, cryptocircuits have to be designed carefully to avoid private information leakage.

Among known SCAs, DPA (Differential Power Analysis) [1], makes use of the dependence of power consumption in the processed data by the cryptographic device during encryption to reveal the secret key. Due to the effectiveness of these attacks, it has been largely studied the implementation of cryptographic circuits resistant to DPA attacks [2],[3].

Many countermeasures have been proposed to deal with DPA attacks, globally categorized as masking and hiding techniques. The best results are achieved with hiding techniques, based on the implementation of a logic circuit whose power consumption was independent of the processed data, as it is provided in [2],[3]. Among them, full-custom solutions based on differential structures are very well considered [3],[4].

DPL (Dual-Precharge Logic) styles comprise a differential pull-down network (DPDN) to perform the logic function and a differential pull-up network (DPUN) to provide the true and complemented outputs in precharge and evaluation phases. To be used in secure applications, besides fully symmetry, it should be ensured that a fixed amount of charge is used in every transition. Sense-Amplifier Based Logic (SABL [3]) is a differential logic style that brings into play exactly the same charge, if new optimization procedures are used [4].

This work faces the optimized design of both DPUN and DPDN blocks, necessary to fulfill demanding security requirements. It is shown how commonly used differential logic gates can be enhaced for cryptographic applications. To achieve this objective, two methodologies are used together: one to improve the security in the DPDN [4] and other to achieve a low-power solution for the DPUN [5]. Making use of both methodologies, the performance of the differential logic gate is enhaced, achieving greater security against DPA attacks and reducing the power consumption and delay of the cell. The main contributions of this paper are: i) the optimization of the DPDN [4] to remove stored charge in internal nodes, trying to avoid harmful memory effects, ii) the spreading of DPA resistant feature to simpler DPUN [5], and iii) simulation-based DPA attacks to Sboxes (Substitution boxes) implemented with different proposals of Xor/Xnor and And/Nand gates, to assess the improvement of our proposals.

The organization of the paper is as follows. Section II includes the previous work related to the used methodology. Section III presents the optimization procedures proposed in this work. Section IV includes simulation-DPA attack results to assess the proposals. Finally, in Section V the conclusions are given.

II. Previous Work

To be used in secure applications, DPUN in DPL cells uses a dual-rail (differential) logic style, dinamically alternating evaluation and precharge phases. Therefore, the gate switches once in every clock cycle, so the switching activity is always the same. Even using a suited logic style in the DPUN, the DPDN must be fully symmetrical, regardless of the input values. Here, symmetry means that all the paths from outputs to ground must have the same transistor count and the same equivalent resistance and capacitance in every node. Then the gate will operate with a constant delay (RC value), regardless of the specific input values. In the same way, for every input condition, the charge stored in the internal nodes should be the same. However, it does not happen in classical DPDN, where the difference on the power consumption due to previous computed values, can be used by attackers. This effect can be strongly reduced using the configuration proposed in [4], where two methods are presented to remove the memory-effect on the internal nodes: the double-switch solution and the single-switch solution. So, in this work we use the three different DPDN shown in [4]: the classic, double-switch and single-switch solutions.

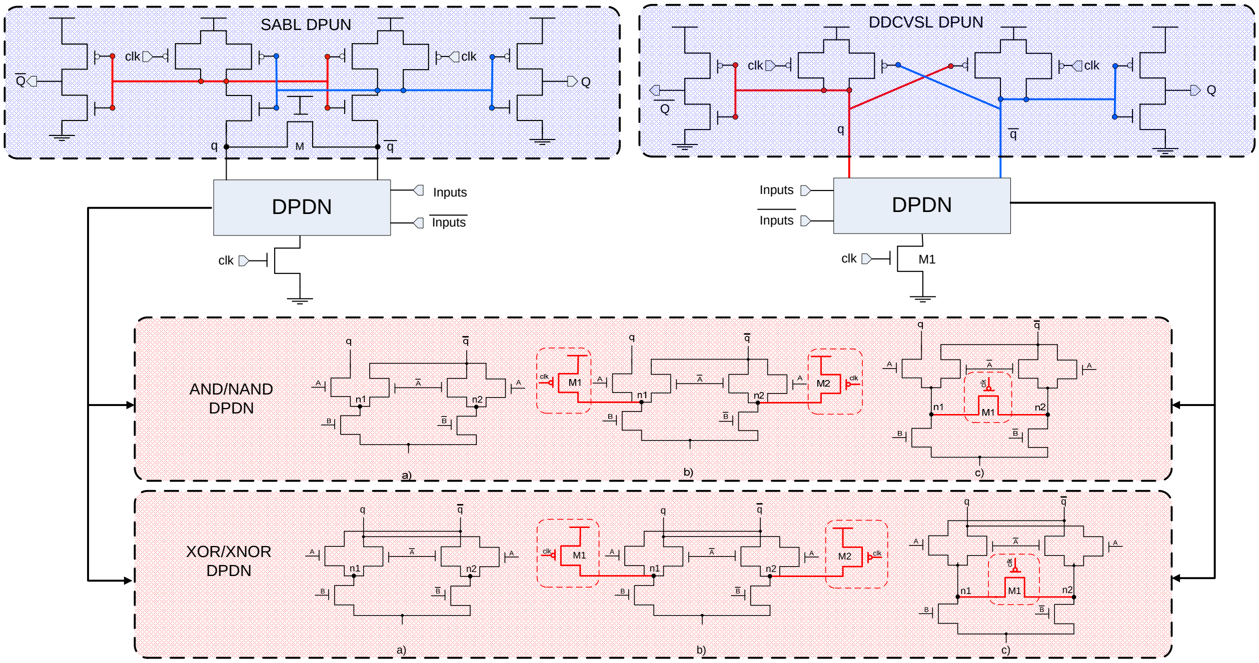

Fig. 1. DPUN and DPDN combinations: a) classic, b) double-switch solution, and c) single-switch solution.

As the gate needs fully balanced differential output nodes, the DPUN has to be also carefully designed. There exists several differential logic DPUN families in the literature, but only some of them are suited for DPA resistance. A DPUN technique that offers well-known high DPA-resistance is the SABL [3] gate. The specific features that make SABL resistant to DPA are i) the presence of the clocked bottom transistor, ii) full symmetry and iii) outputs of DPDN not connected to the gate of output inverters. For this work, SABL will be considered as the reference gate.

III. Proposed implementations

This section discusses the combination of optimized DPDN with simpler DPUN, as shown in Fig. 1, to get low-power and secure DPL implementations, in such a way the SABL solution could be overtaken either in performances or in security. For this purpose, after the characterization of several differential structures, we have selected the DPUN structure called *Dynamic Differential Cascode Voltage Switch Logic (DDCVSL)* [5], because of its relative simplicity.

The main *a priori* problem of DDCVSL for DPA-resistant applications, is the direct connection between the output capacitances in nodes connecting the DPDN and the DPDN branches making the structure poorly resistant to DPA. Fig. 2a) shows the simulated waveforms of a Xor/Xnor gate with classic DPDN using a DDCVSL DPUN in a 90 nm technology. As it can be seen, at t=60ns the internal nodes change in opposite way due to the change of the input B compared with its value in the previous evaluation. That will lead to a significant difference in power consumption. This memory effect can be skipped if we use the proposed DPDN with double-switch solution, then improving the security of the Xor/Xnor gate, as it is shown in Fig. 2b).

In order to assess the effectiveness of the proposed methodologies to improve the DPUN and DPDN, the following proposals are generated mixing both methodologies for And/Nand and Xor/Xnor gates: SABL Classic (DPUN SABL with classic DPDN), SABL_2P (SABL DPUN with the double-switch solution for DPDN), SABL_P (SABL DPUN with the single-switch solution for DPDN), DDCVSL Classic (DPUN DDCVSL with classic DPDN), DDCVSL_2P (DPUN DDCVSL with the double-switch solution for DPDN) and DDCVSL_P (DPUN DDCVSL with the single-switch solution for DPDN).

All the proposed gates have been implemented in CADENCE using a TSMC 90nm technology. They have been simulated with SPECTRE under nominal conditions. Inputs and outputs of the gate under test are coming/going from/to gates of the same style, being the clock frequency 100MHz. Input patterns are such that all possible combinations take place, then measuring the power consumption for all possible transitions.We measure the minimum energy value (Min), the maximum energy value (Max), the mean energy (μ) and the standard deviation (σ) for all the transitions, in order to quantify the DPA-resistance of the cell. The energy per cicle has been computed as shown in equation (1).

$$E = V_{DD} * T_{CLK} * \frac{1}{T_{CLK}} \int_{-T_{CLK}/2}^{T_{CLK}/2} \mathrm{i_{DD}}(\mathrm{t})\, \mathrm{d}t \qquad (1)$$

From these values, we obtain the Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD), according to eq. (2) and eq. (3), respectivelly, usually conceived as an indirect measurement of DPA resistance.

$$NED = (Max - Min)/Max \qquad (2)$$

$$NSD = \sigma/\mu \qquad (3)$$

TABLE I. SIMULATION RESULTS FOR THE DIFFERENT IMPLEMENTATIONS OF THE AND/NAND AND XOR/XNOR GATES.

		Evaluation			Precharge			Eavg_Total	Delay	Transistors
		NED	NSD	Eavg (fJ)	NED	NSD	Eavg (fJ)	(fJ)	(ps)	
And/Nand	SABL Classic [3]	4.25e-3	1.23e-3	8.44	5.86e-3	1.37e-3	12.24	20.68	208	18
	SABL (2P)	10.93e-3	2.62e-3	8.22	3.80e-3	1.00e-3	16.08	24.30	246	20
	SABL (P)	2.85e-3	6.64e-4	8.57	5.85e-3	1.52e-3	12.72	21.29	219	19
	DDCVSL Classic	168.61e-3	29.65e-3	4.78	223.06e-3	68.18e-3	7.84	12.62	89	15
	DDCVSL (2P)	287.24e-3	80.23e-3	4.38	241.02e-3	90.61e-3	11.39	15.77	154	17
	DDCVSL (P)	147.49e-3	25.23e-3	4.88	245.55e-3	77.81e-3	8.17	13.06	108	16
Xor/Xnor	SABL Classic [3]	3.47e-3	1.54e-3	12.00	2.14e-3	5.13e-4	21.72	33.72	173	18
	SABL (2P)	1.08e-4	2.36e-5	12.24	1.51e-3	3.88e-4	30.96	43.20	198	20
	SABL (P)	2.65e-3	1.20e-3	12.12	2.11e-3	6.32e-4	22.20	34.32	176	19
	DDCVSL Classic	210.13e-3	115.81e-3	7.72	8.05e-3	2.31e-3	14.28	22.00	125	15
	DDCVSL (2P)	1.41e-3	3.67e-4	6.13	4.54e-3	1.30e-3	19.92	26.05	142	17
	DDCVSL (P)	10.61e-3	1.94e-3	8.03	8.29e-3	2.61e-3	14.04	22.07	126	16

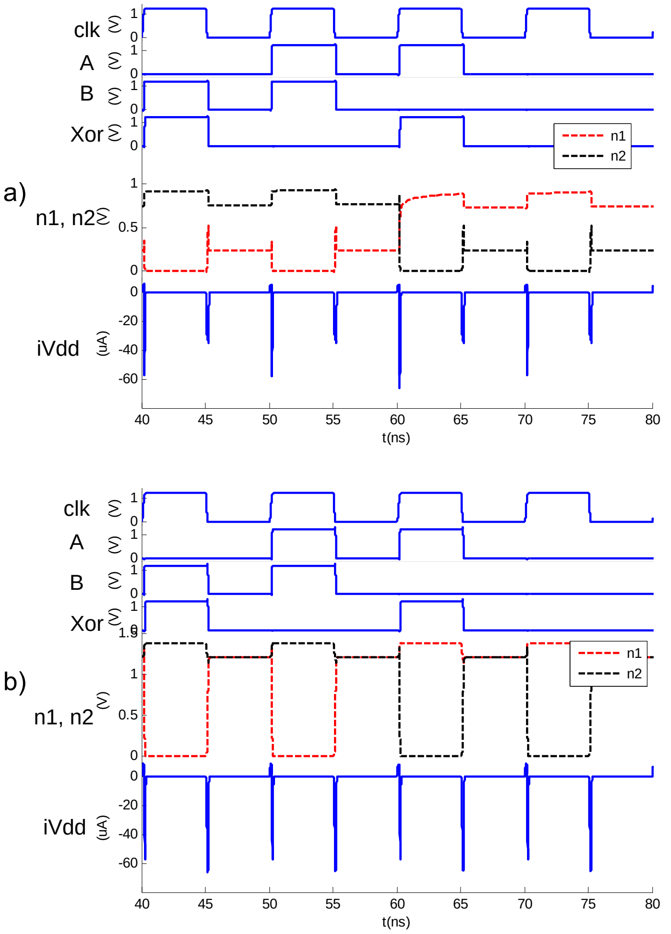

Fig. 2. Waveform displays and internal (n1 and n2) simulated for the DDCVSL Xor/Xnor gate: a) with the classic DPDN and b) with the double-switch solution DPDN.

In Table I, the NED, NSD, power consumption for both the precharge and evaluation phases, then the total power consumption, the delay and the number of transistors for each gate are included. In order to quantify the DPA-resistance of the cells, the values of NED and NSD of the evaluation phase are considered, since power consumption in the evaluation phase has a greater dependence on the processed data (in the precharge phase, nodes $n1$ and $n2$ are floating). In view of the results reported in Table I, we can conclude that the best choice for the And/Nand gate is the combination of the SABL DPUN with the single-switch modification in the DPDN, and in the case of the Xor/Xnor gate we can choose two different gates: the SABL_2P with the best security results, and the DDCVSL_2P low-power solution with enhanced security over the SABL classical one, and a great improvement in power consumption and delay over the SABL classic and the enhanced SABL_2P.

IV. SIMULATION-BASED DPA ATTACK

The values of NED and NSD are only an estimation of the robustness of the differential gates. A definitive way to measure the security of the gates is to develop a DPA attack on a cryptographic circuit incorporating both the referenced and proposed gates. The cryptocircuit selected for the attack is the 9-bit Substitution box, henceforth called Sbox9, of the Kasumi algorithm [6], implemented with 84 2-input And/Nand gates and 95 2-input Xor/Xnor gates. Four different designs of the Sbox9 are implemented: the Sbox9_CMOS with classic CMOS gates, the Sbox9_SABL Classic, the Sbox9_SABL proposal implemented with And/Nand_SABL_P and Xor/Xnor_SABL_2P, and the Sbox9_DDCVSL Proposal with And/Nand_SABL_P and Xor/Xnor_DDCVSL_2P. All the designs of Sbox9 have been implemented in CADENCE using a TSMC 90nm (Vdd=1.2V) technology. They have been simulated with SPECTRE under nominal conditions, being the clock frequency 500MHz and capturing data every 10ps.

The performed DPA attack is based in the steps proposed in [4]. To compare the robustness of the implemented Sboxes, the MTD (Measurements To Disclosure) metric is used, being MTD the minimum number of power traces needed to retrieve the correct key. In the first round applying the same 1250 input patterns, we obtain a successful attack for the Sbox9_CMOS and Sbox9_SABL Classic, being the MTD for the Sbox9_CMOS 145 and 344 for the Sbox9_SABL Classic, as shown in Fig. 3a) and 3b). In the case of the proposals the key is not recovered. Another attack is performed in the case of the Sbox9_SABL Proposal and Sbox9_DDCVSL Proposal with 10000 input patterns. Again, the attacks are unsuccessful, being the 10000 input patterns not enough to retrieve the key, as illustrsated in Fig. 4a) and 4b).

In view of the results, the proposed And/Nand and Xor/Xnor gates improve the robustness of the implemented

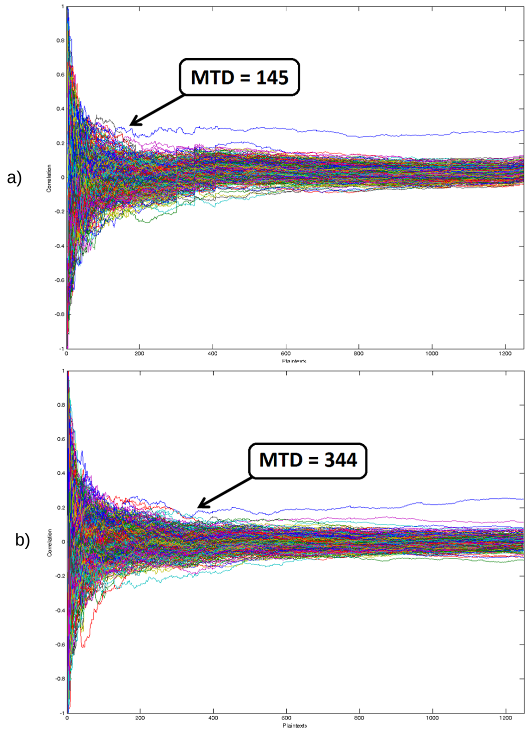

Fig. 3. Correlation coefficients vs trace number (1250 input patterns): a) Sbox9_CMOS and b) Sbox9_SABL Classic.

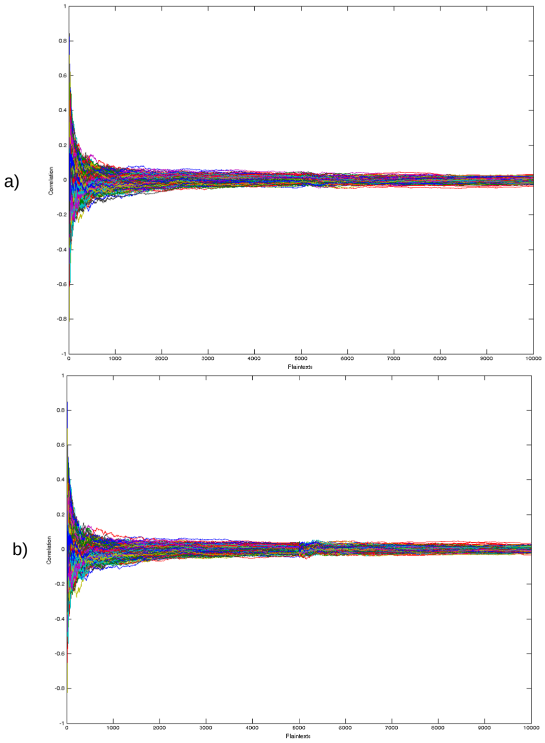

Fig. 4. Correlation coefficients vs trace number (10000 input patterns): a) Sbox9_SABL Proposal and b) Sbox9_DDCVSL Proposal.

gates. In both proposed Sbox9, the MTD is >>10000, improving at least x29.07 the robustness of the circuit. As both Sbox9 proposals use the same And/Nand gate, it can be said that improvement of both proposed Xor/Xnor gates is in the same order, thus, the best choice for the Xor/Xnor gate is the Xor/Xnor_DDCVSL_2P because of its improvement in security, power consumption and delay over the classic Xor/Xnor_SABL gate and the Xor/Xnor_SABL_2P.

V. Conclusion

This paper has presented the design of DPL gates for cryptographic applications using two combined optimized methodologies for DPDN and DPUN. The improvement factor of each proposed gate over the classical And/Nand_SABL Classic and Xor/Xnor_SABL Classic in every case is shown in Table II.

TABLE II. Simulation improvement factors of single gates over the reference ones.

		Evaluation		Eavg	Delay
		NED	NSD		
And/Nand	SABL (P)	x0.67	x0.54	x1.03	x1.05
Xor/Xnor	SABL (2P)	x0.03	x0.02	x1.28	x1.14
	DDCVSL (2P)	x0.41	x0.24	x0.77	x0.82

After selecting the best gates for power and security, simulation-based DPA attacks have been made to assess the security against DPA attacks. The DPA attack results show that the proposed Sbox9_SABL Proposal and the Sbox9_DDCVSL Proposal improve the robustness of the circuit in a factor at least of x29.07 after 10000 input patterns DPA attack over the reference circuit Sbox9_SABL Classic. Due to the fact that the improvement on security is comparable in both proposed Sbox9, it can be said that the Xor/Xnor_DDCVSL_2P is a better choice than the Xor/Xnor_SABL_2P, because for the same security level the Xor/Xnor_DDCVSL_2P has less power consumption (x0.60), delay (x0.72) and area (3 transistor less per gate).

Acknowledgment

This work was partially supported by CSIC under Project 201450E034 and by the Spanish Government under Projects TEC2010-16870, IPT2012-0695-390000 and TEC2013-45523-R.

References

[1] P. Kocher, J. Jaffe, and B. Jun, ”Differential Power Analysis”, *CRYPTO*, pp. 388-397, 1999.

[2] K. Tiri, I. Verbauwhede, ”A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation,” *DATE*, pp. 246-251, 2004.

[3] 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”, *ESSCIRC*, pp. 403-406, 2002.

[4] E. Tena-Sanchez, J. Castro, A.J. Acosta, ”A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits,” *IEEE JETCAS* vol. 4, no. 2, pp. 203-215, Jun. 2014.

[5] P. Ng, P.T. Balsara, D. Steiss, ”Performance of CMOS differential circuits,” *IEEE Journal of Solid-State Circuits*, vol. 31, no. 6, pp. 841-846, Jun. 1996.

[6] Third Generation Partnership Project, 3GPP TS 35.202 version 7.0.0 Release 6, Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification, ETSI/SAGE, 2007.