An Investigation of Security-aware Strategies against Differential Power Analysis

Vinícius Renato Rocha Geraldo, Mateus Brugnaroto, Vitor Lima, Rafael I. Soares
Technology Development Center - CDTec
Federal University of Pelotas – UFPel
Pelotas, Brazil
{vrrgeraldo, mbrugnaroto, vgdlima, rafael.soares}@inf.ufpel.edu.br

***Abstract*— This work investigates topologies of different logic styles that aim to obtain a power consumption homogeneous and independent of data to resist the Differential Power Analysis (DPA). An overview highlights the following logic styles: Secure Triple Track Logic (STTL), Pre-Charge Static Logic (PCSL), Differential Pass-Transistor Precharge Static Logic (DPPL) and Wave Dynamic Differential Logic (WDDL). They are implemented under some conditions in order to obtain a fair comparison of their strategies against DPA. This work highlights the main benefits and drawbacks of these topologies, comparing the energy consumption, propagation delay and DPA-resistance of the basic gates NAND2, NOR2, and XOR2. The results show that WDDL and STTL leak less information through this side channel.**

Keywords—Security; Side Channel Attacks; DPA; cryptography; circuit design.

I. INTRODUCTION

The security of encryption hardware – such as smart cards – is threatened by the Side Channel Attacks (SCA). This kind of attacks allows finding dependencies between physical quantities of the device and data processed. Thus, the attacker can disclosure a cryptographic key of a system through the exploitation of physical characteristics such as power consumption, electromagnetic radiation and timing processing of devices in CMOS technology.

Attacks based on power consumptions and timing attacks was firstly described by Kocher [1,2]. They are powerful methodologies that require specifics countermeasures to minimize the vulnerabilities. Differential Power Analysis (DPA) is an SCA that analyzes the circuit power consumption through a statistical correlation, where, is possible to establish a dependency relation between data and power consumption. Differential Electromagnetic Analysis (DEMA) exploits the same vulnerabilities, although it explores the electromagnetic radiation emitted by the circuit. DPA and DEMA are proven effective to disclosure a cryptographic key in circuits implemented in ASIC, FPGA, and microprocessors.

Kocher et al. [2] show that circuits implemented with CMOS technology have different power consumption to compute different data. i.e., output transitions ‘0’ to ‘1’ (TLH) and ‘1’ to ‘0’ (THL). It results in different consumptions which are explored by the DPA and DEMA attacks. In this context, countermeasures have been developed to avoid the information leakage in the design of crypto devices.

Dual Rail [5] (DR) is an encoding scheme where a bit of information is encoded in two wires. This kind of encoding is commonly used in asynchronous circuit design methodology where the circuits are clockless. Theoretically, DR gates are immune to DPA attacks because independently of the output result, the transitions TLH and THL always occur. However, it is necessary to ensure that the structure must be balanced, that is, TLH and THL must be equals and causing the same power consumption independently to inputs stimulus.

Dual-Rail Pre-Charge Logic (DPL) [3] is a DR topology that adds an extra phase in its computation. This phase is responsible for carrying all circuit to the same beginning statement, avoiding the electrical behaviors from the last computation.

This paper evaluates four significants topologies proposed to hide the leakage of information through the circuits with independent data consumption highlighting features such as energy consumption, gates delays, and estimating the vulnerabilities level. A comparison in Spice level between the topologies is presented in order to investigate pros and cons of the each one.

The paper is organized as follows: Section 2 presents a theoretical reference. Section 3 presents the details how the simulations have been performed. Section 4 presents the results through electrical simulations. Finally, Section 5 presents conclusions and directions for further work.

II. PRELIMINARIES

Power analysis consists of noninvasive attacks that can be performed with off-the-shelf equipment. Therefore, it poses a severe threat to the security of cryptographic devices like smart cards [4]. Figure 1 represents the NAND2 power consumptions obtained by SPICE simulations using @45nm CMOS technology. The dashed lines represent the power consumptions arches, i.e., sensitize the output when varying an input bit. the power consumptions variations are the electrical behaviors exploited by the DPA attackers. Therefore, Figure 1 presents the data dependence between the computations and power consumption.

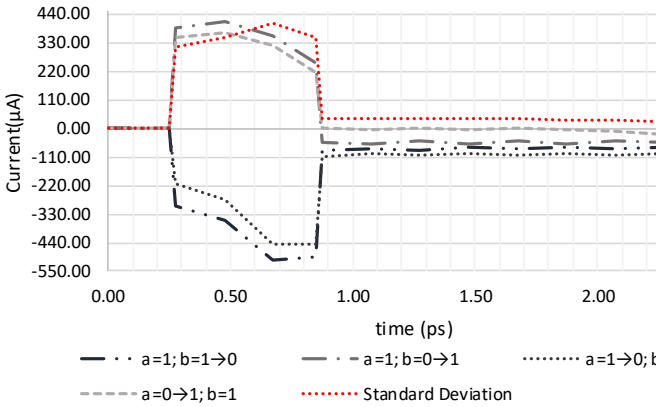

Figure 1 – Simulations of NAND2 current to various CMOS stimulus

A. *Differential Power Analysis (DPA)*

DPA is the most popular type of power analysis attacks, mainly because it does not require detailed knowledge about the attacked device. The goal of DPA is to reveal secret keys of cryptographic devices based on a large number of power traces that have been recorded while encrypting or decrypting different data blocks. Furthermore, they can reveal the secret key even if the recorded power traces are extremely noisy. The dependence comes from the characteristic of consumption of the CMOS technology, where, switching low-to-high (TLH) and high-to-low (THL) the traces have different consumptions [4].

B. *Countermeasures*

The countermeasures are strategies that aim to mitigate the leakage information from the side channels. One of the most popular strategies to minimize the leakages is developing a circuit that the power consumption is uniform and independent from the computations.

Dual-Rail Pre-Charge Logic (DPL) [3] works in 2 steps, precharge and evaluation phases. The precharge produces an unconditional output responsible for establishing an initial capacitance charge in the circuit, while the evaluation phase computes the input data according to the circuit logic.

The DPL is a robust strategy and widely used in the literature, although it has three critical drawbacks that increase the information leakage [7]. The drawbacks are: (1) propagation delays accumulated through the circuit, (2) allows early propagation effects (EPE), i.e., cases where a gate evaluates its output at different time instances depending on the value of its input, and (3) unbalanced transistor network to compose a gate.

In the literature are presented several proposals of logic styles to mitigate the information leakage. In this work four of the main proposals are reviewed as follows.

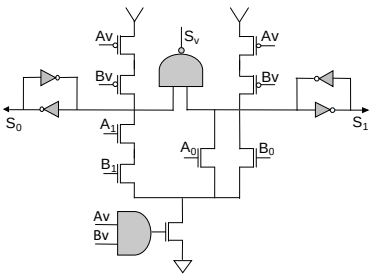

Figure 2 - NAND2/AND2 STTL

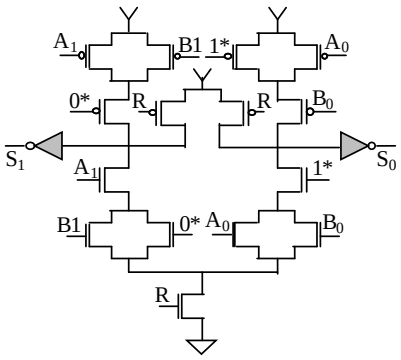

Figure 3 - NAND2/AND2 PCSL

1. *Secure Triple Track Logic (STTL)*

STTL is a topology that adds a validation track indicating when the logic rails are stable to be performed. Therefore, the STTL is theoretically able to eliminate the propagation delays and the EPE problems. Figure 2 exposes the AND2/NAND2 STTL gate, where, the latches are used to maintain the signal low and the gates with background in brown represent the traditional CMOS. Additionally, the S_x are the outputs and the A_x and B_x are the inputs stimulus, where *x* would be: (i) v, the validation signal, (ii) 1, the logic itself and (iii) 0, the complementary logic.

2. *Pre-Charge Static Logic (PCSL)*

PCSL is introduced in [9] and implements a topology that modifies the transistors arrangement seeking out to solve the drawback occasioned by the unbalancement of the DPL gates. The strategy adds dummy transistors to equilibrate the internal capacitances. Figure 3 represents the NAND2/AND2 the arrangement and its inputs, where the A_x , B_x and S_x express the same representation than STTL. Additionally, * indicates the dummies transistors, and the input R, determine the phase to compute. The PCSL has a symmetric arrangement.

3. *Differential Pass-transistor Pre-charge Logic (DPPL)*

DPPL is a logic defined by pass transistors and, such as STTL, is projected to eliminate the undesirable EPE. As the PCSL, the DPPL has a very balanced transistors arrangement. Figure 4 depicts the AND2/NAND2 with the same inputs and outputs labels as defined above.

4. *Wave Dynamic Differential Logic* (WDDL)

WDDL is a DR logic topology defined from a regular standard cell library CMOS. WDDL has the simplest project effort whereas it would be implemented by the gates available in the standard cells. Figure 5 shows the AND2/OR2 logic arrangement.

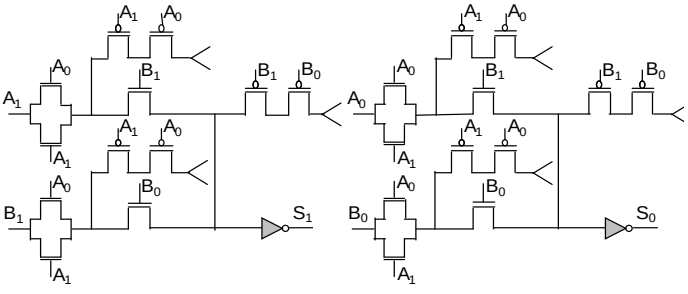

Figure 4 - NAND2/AND2 DPPL

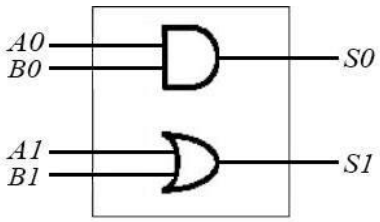

Figure 5 – AND2/OR2 WDDL

III.SIMULATION

This work proposes an electrical model according to each logic style reviewed in order to obtain the electrical behaviors through SPICE simulations. In order to produce a fair comparison between logical styles, some conditions are defined such as use the predictive 45-nanometer technology (Free PDK – 45 nm), a delay of fanout-of-4 inverters (FO4) and the inputs slopes equal to the rise time of 2 inverters serially arranged.

The Normalized Standard Deviation (NSD) and Normalized Energy Deviation (NED) metrics are widely used in the literature [6, 8, 10-13] to evaluate the power consumptions variations and estimate the leaked information in a desing. The calculus required to obtain the NSD and NED are described in the Equations (8) and (9) and are applied over a set of power traces. Equation (8) defines the *NED*, where the *max(E)* and *min(E)* represent respectively the maximum and minimum energy obtained from the traces. Equation (9) exposes the NSD, where, the $\overline{E}$ is the average energy consumption and the $\sigma(E)$ is the standard deviation of the Energy.

$$NED = \frac{max(E) - min(E)}{max(E)} \quad (8)$$

$$NSD = \frac{\sigma(E)}{\overline{E}} \quad (9)$$

STTL have an extra validation track, named Sv, indicates whenever the output data is stable and valid. These tracks signalize when the inputs are ready to compute. It means that the validation signal must be slower than the respective bit of information. It is an important countermeasure, although, it represents a restriction that must be considered at the moment to project the gates.

IV.RESULTS

This paper compares the topologies WDDL, PCSL, STTL, and DPPL according to the following features: NED, NSD, delay and power consumption. The comparisons are made using the logic gates AND/NAND, OR/NOR, and XOR/XNOR. The robustness against DPA is estimated through the metrics NED and NSD, which values closer to 0 means an ideal security. Figure 6 (a) shows the evaluation of the NED performed on the power consumption traces obtained from the topologies investigated. In the precharge phase, STTL is more stable than the others, reaching on average up to 322.9% more homogeneous than worst case. In the evaluation phase, WDDL topology shows up better, reaching an average gain of up to 206.03%. According to the metric NSD as shown in Figure 6 (b), the results confirm the same performance of the topologies. In precharge phase, STTL has gained up to 322.9%, while WDDL in the evaluation phase reaches gains in the average up to 210.41%.

Figure 6 (c) shows the energy consumed by the topologies. WDDL has the lowest consumption, reaching 5x less than STTL which showed the highest consumption in the precharge phase. The investigation of the delay of the topologies takes into account the sum of the precharge and evaluation phases. The investigation of the delay of the topologies takes into account the sum of the precharge and evaluation phases as exposed in Figure 6 (d). WDDL has best delays performance in the phases of precharge and evaluation, with gains in average by logic gates varying between 115.76% to 232.30% in the precharge phase compared to STTL and DPPL, and in the evaluation phase, presents gains varying between 120% to 315.73% compared to STTL and PCSL respectively.

V. Conclusions

This work investigates some topologies that aim the power consumption homogenization as a countermeasure against DPA. The evaluation is given considering the security-level, energy consumption and, delay. Electrical simulation results determine that WDDL is the best topology according to security in the evaluation phase, indicating that leaks less information than PCSL, STTL and the DPPL. However, in the precharge phase, STTL shows to be more secure according to the NED and NSD metrics. On the other hand, STTL has shown to be the most expensive in terms of energy consumption and delay. Unsatisfactory results for STTL in the evaluation phase may be justified because of its unbalanced transistors network. Ongoing works investigate a new strategy of balancing transistors aiming higher levels of security for these types of logical styles.

References

[1] P.C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and others Systems," in Proceedings of the 16th International Cryptology Conference, 1996, pp. 104-113.

[2] P.C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Proceedings of the 19th International Cryptology Conference, 1999, p. 388-397.

[3] J.L. Danger., S. Guilley, S. Bhasin, M. Nassar and L. Sauvage. "Overview of dual rail with precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors,", 2009.

[4] S. Mangard, E. Oswald, and T. Popp. "Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)". Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007, pp. 1-13.

[5] D. Sokolov, J. Murphy, A. Bystrov and A. Yakolev. "Design and Analysis of Dual-Rail Circuits for Security Applications". IEEE Tranl. on Computers april 2005, vol. 54(4): pp. 449-460.

[6] STINE, E. J., CHEN, J., CASTELLANO, I., SUNDARARANJAN, G., QAYAM, M., KUMAR, P., REMINGTON, J., SOHONI, S., FreePDK v2.0: "Transitioning VLSI Education Towards Nanometer Variation-Aware Designs". In: MSE International Conference on Microeletronic Systems Education, 2009.

[7] A. Razafindraibe, P. Maurine and M. Robert, "Evaluation of the robustness of dual rail logic against DPA," *2006 IEEE International Conference on IC Design and Technology*, Padova, 2006, pp. 1-4.

[8] M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti. "Three-Phase Dual-Rail Pre-charge Logic". In: Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg, 2006.

[9] Chong, K.-S., Ne, K.Z.L., Ho, W.-G., Liu, N., Akbar, B.H., Chang, S. "Counteracting Differential Power Analysis: Hiding Encrypted Data from Circuit Cells". Electron Devices and Solid-State Circuits (EDSSC), 2015.

[10] Biham, E., Shamir, A, Differential Cryptanalysis of the Data Encryption Standard, 1st ed., vol.1. Springer-Verlag: New York, 1993.

[11] P. Shinu, P. D. Kumar. "Design of Delay Based Dual Rail Precharge Logic to Reduce DPA Attacks". Computing, Electronic and Electrical Technologies (ICCEET), 2012. pp. 552-556.

[12] C. Monteiroa, Y. Takahashib, T. Sekineb. "Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level". Microelectronics Journal. V. 44 I. 6. pp 496-503, 2013.

[13] E. Tena-Sánchez, J. Castro, A. J. Acosta. "A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits". Journal on Emerging and Selected Topics in Circuits and Circuits. V. 4, I. 2, 2014.

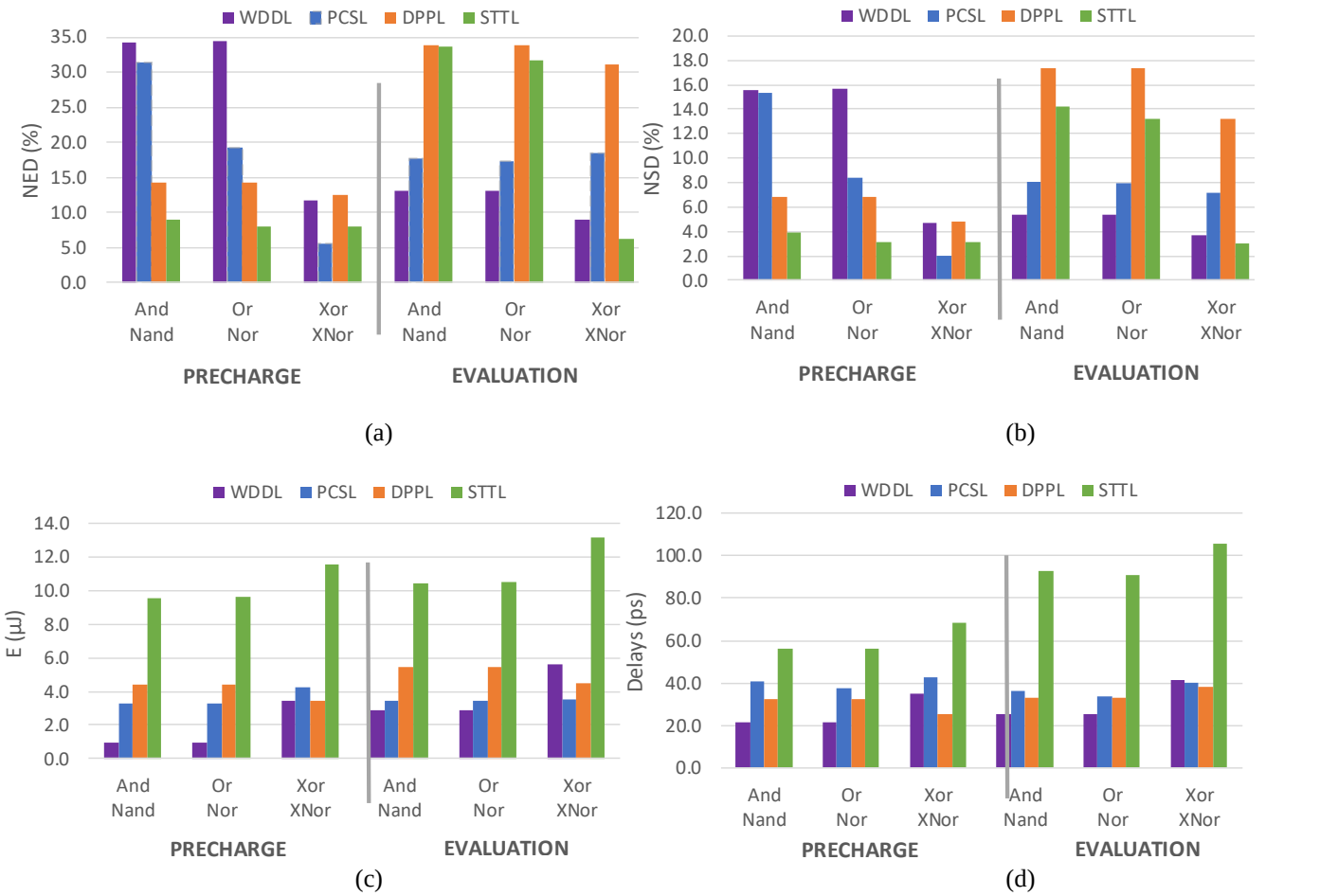

Figure 6 – Comparison of WDDL, PCSL, DPPL and STTL topologies, considering the basic gates in the precharge and evaluation phases. (a) NED metric. (b) NSD metric. (c) Average power consumption. (d) Critical propagations delays.