Review of Gate-Level Hardware Countermeasure Comparison Against Power Analysis Attacks

E. Tena-Sánchez
IMSE-CSIC/U. Sevilla
erica@imse-cnm.csic.es

F. E. Potestad-Ordóñez
IMSE-CSIC/U. Sevilla
potestad@imse-cnm.csic.es

V. Zuñiga-González
IMSE-CNM-CSIC
virginia@imse-cnm.csic.es

C. Fernández-García
IMSE-CNM-CSIC
carlos@imse-cnm.csic.es

J. M. Mora-Gutiérrez
IMSE-CNM-CSIC
jmiguel@imse-cnm.csic.es

C. J. Jiménez-Fernández
IMSE-CSIC/U. Sevilla
cjesus@imse-cnm.csic.es

A. J. Acosta-Jiménez
IMSE-CSIC/U. Sevilla
acojim@imse-cnm.csic.es

***Abstract*—In this paper, we present a review of the work [1]. The fast settlement of Privacy and Secure operations in the Internet of Things (IoT) is appealing the selection of mechanisms to achieve a higher level of security at the minimum cost and with reasonable performances. In recent years, dozens of proposals have been presented to design circuits resistant to Power Analysis attacks. In this paper a deep review of the state of the art of gate-level countermeasures against Power Analysis attacks has been done, performing a comparison between hiding approaches (the power consumption is intended to be the same for all the data processed) and the ones considering a masking procedure (the data are masked and behave as random). The most relevant proposals in the literature, 35 for hiding and 6 for masking, have been analyzed, not only by using data provided by proposers, but also those included in other references for comparison.**

***Index Terms*—hardware countermeasures; gate level; VLSI design of cryptographic circuits; side-channel attacks (SCAs); information security; logic design; Internet of things (IoT).**

Tipo de contribución: Investigación ya publicada.

I. Introduction

The high growth that the Internet of Things (IoT) is experiencing has brought with it an increase in the exchange of sensitive information from interconnected users. Traditionally, the mathematical algorithm and the length of the key defined the security of crypto-systems. However, the physical implementation of cryptographic algorithms leads to information leakages that can be exploited by third parties to reveal critical data [2], [3]. Among the different types of attacks, the so-called Side-Channel Attacks (SCAs) belong to the group of passive noninvasive attacks and are those where the cryptographic device is not manipulated, e.g. there is no trace that a malicious agent has had access to the device and there is no damage to the circuit [2], [3]. Among SCAs, those based on analysis of the power consumption (Power Analysis, PA) produced by the circuit have attracted significant attention from the research community [3].

Since the emergence of power analysis attacks in the late 1990s, numerous countermeasures have been proposed by the scientific community to search for alternatives to minimize the weak points of crypto-circuits [4], [5], [6]. There are several countermeasure strategies at the hardware level. These countermeasures range from the layout up to algorithm level and go from attack detection to adding redundant blocks to obfuscate possible information leakage. They can be classifyed depending on the technique used to break the data correlation with the power consumption: hiding (the power consumption is intended to be the same for all the data processed) or masking (the data are masked and behave as random). This review focus on gate-level hiding and masking countermeasures.

II. State of the art: Gate-level countermeasures against power analysis attacks

PA attacks exploit the correlation between power consumption and the data that are processed by the cryptographic device during encryption, following several strategies, to reveal the critical data. Hardware countermeasures are oriented towards breaking the relationship between data being processed and consumed power. To break this rate at the gate level, two different mechanisms are widely used: hiding and masking techniques. The hiding attempts to have the same power consumption at the gate, circuit, or algorithm level, independently of the data being processed. In masking, the critical data are masked with a random data sequence during encryption such that operations on the masked data are indistinguishable from random data.

A. Gate-level masking

Gate-level masking consists of computing both the inputs and the mask inside the gate itself. In these implementations, each masked signal a_m is propagated along with its mask m_a, being the unmasked signal $a = a_m \oplus m_a$. The simplest way to perform masking is through boolean masking, where an input word gets masked by being XOR-ed by a random value. Arithmetic masking involves more complex arithmetic operations within specific algorithms. Boolean masking is preferably used at the gate level, while at the algorithm or circuit level, the use of dedicated arithmetic masking techniques that best suit the algorithm are recommended.

B. Gate-level hiding

Hiding tries to achieve exactly the same power consumption in operations, regardless of the data being processed. Since the first PA attacks were presented, there have been numerous logic style proposals that seek to be resistant to these attacks by having data-independent power consumption. In a first approach, this identical consumption can be achieved using dual-rail signals and differential gates, where the true and

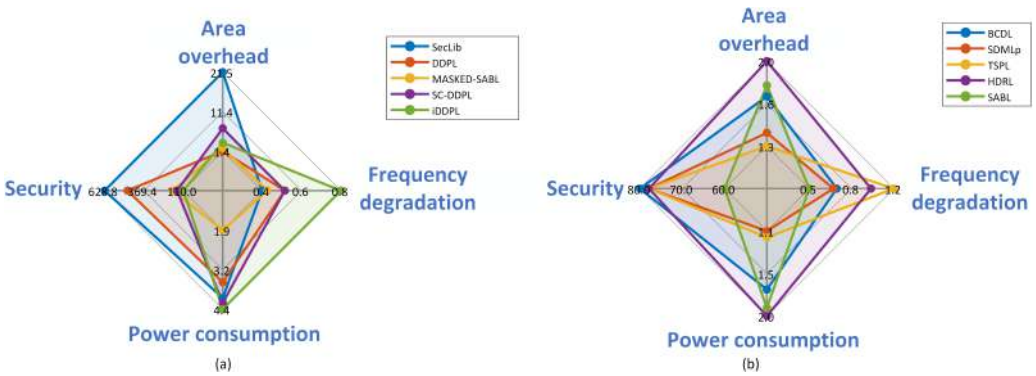

Fig. 1. Top 5 countermeasures in security levels (a) and top 5 countermeasures with best trade-off between performance and security levels (b).

complemented outputs are simultaneously generated: in every clock cycle, one of the differential branches performs the gate function and the other one its complement at the same time.

Since hiding means exact power consumption independently of the data processed, it implies full symmetry. However, most of these techniques suffer from the difficulty of tailoring the place and route operation so that the capacitive load of two wires is equal. This is particularly difficult in nanometric technologies, where the transistor sizes and wiring widths continuously shrink. Placing and routing a circuit manually, i.e. doing a full-custom (FC) design, significantly increases the design costs. An additional drawback is the so-called early evaluation, also called data-dependent time-of-evaluation, referring to the cases where a gate evaluates its output at different time instances depending on the value of its input. It becomes more problematic when several of such gates are cascaded to realize a combinational circuit, causing the power consumption pattern of the circuit to have a clear dependency on its input value.

III. Comparative analysis of gate-level countermeasures

The presented analysis considers the most relevant solutions in the literature, 35 hiding proposals, and 6 based on masking, not only by using the data provided by proposing authors, but also those included in the other references for comparison. For a complete analysis, please refer to [1]. Advantages and drawbacks of the proposals are analysed, showing quantified data for cost, performance (delay and power), and estimated security level, when available. The comparison between performances, features, and security levels of these proposals is not easy to carry out, given the variety of approaches and considered technologies. However, a summary of the comparative analysis is presented using the normalized values presented by the reference authors of each countermeasure.

Fig. 1-a provides a visual comparison of the top 5 countermeasures with the best security levels. Fig. 1-b depicts the top 5 countermeasures with the best trade-off between security values and area-delay-product performance and area overhead. From these figures, it can be seen that, typically and as expected, the higher the security the higher the cost. However, this is not always the case. For example, in Fig. 1-b it can be seen that the SABL approach has approximately the same power and area costs as BCDL but provides significantly less protection against PA. Nevertheless, in addition to performance degradation and security levels, it is also important to consider the inherent design difficulties of each proposal, as well as the feasibility of including the countermeasure in the design.

IV. Conclusions

In this paper a deep review of the state-of-the-art of gate-level countermeasures against power analysis attacks has been done. This work also visually depicts the performance, cost, and security level relation of the several solutions to better assist cryptodesigners in the selection of the best solution, style according to their constraints. Overall, these results suggest that RSL and DRSL solutions are the best approaches when considering masking, while BCDL, SDMLp, TSPL, HDRL and SABL are those with best security-performance figures. It can also be concluded that hiding proposals reach higher security levels, but with more difficult design constraints, which, if not met, can result in security weaknesses. Finally, this review also suggests that the combination of masking and hiding, as in Masked_SABL, can provide the most secure solution, but at the cost of more complexity.

Acknowledgments

This work has been funded by project SCAROT 1380823-US/JUNTA/FEDER, UE. Thanks to SPIRS Project with Grant Agreement No. 952622 under the European Union's Horizon 2020 programme and Grant PID2020-116664RB-I00 funded by MCIN/AEI/10.13039/501100011033.

References

[1] E. Tena-Sánchez, F. E. Potestad-Ordóñez, C. J. Jiménez-Fernández, A. J. Acosta and R. Chaves, "Gate-Level Hardware Countermeasure Comparison against Power Analysis Attacks," *Applied Sciences*, 12(5), 2390, 2022.

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

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

[4] 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 28th European Solid-State Circuits Conference (ESSCIRC'02)*, pp. 403-406, 2002.

[5] M. Nassar, S. Bhasin, J. Danger, G. Duc, S. Guilley, and A. E. P. Effect, "BCDL : A High Speed Balanced DPL for FPGA with Global Precharge and no Early Evaluation," *in Proc, of the Conference on Design, Automation and Test in Europe (DATE'10)*, pp. 849–854, 2010.

[6] B. Fadaeinia, M. T. Hasan Anik, N. Karimi and A. Moradi, "Masked SABL: A Long Lasting Side-Channel Protection Design Methodology," *in IEEE Access*, vol. 9, pp. 90455-90464, 2021.