

# Vulnerability Evaluation and Secure Design Methodology of Cryptohardware for ASIC-embedded Secure Applications to Prevent Side-Channel Attacks

E. Tena-Sánchez<sup>1</sup>, I. Durán, S. Canas and A. J. Acosta<sup>2</sup>

Instituto de Microelectrónica de Sevilla, IMSE, CNM (CSIC, Universidad de Sevilla)

Email: {erica<sup>1</sup>, acojim<sup>2</sup>}@imse-cnm.csic.es

This poster presents the state of the art in the research performed by our group in designing and testing cryptohardware for ASIC-embedded secure applications. Implementations of both block-ciphers (Kasumi-Sbox9, AES-128) and stream-ciphers (Trivium) are explored at a circuit and transistor level, to increase their security figures. Analysis of vulnerability is made via Correlation Power Analysis (CPA) attacks, by implementing Correlation Electromagnetic Analysis attacks (CEMA), and using t-test leakage detection analysis, which are made at simulation and experimental level.

Cryptocircuits can be attacked by third parties using side channel attacks (SCAs). To protect security devices against CPA/CEMA attacks, differential logic styles with (almost) constant power dissipation are widely used. The right use of such circuits needs not only a fully symmetric structure and layout, but removing any energy secure hole in security in the way of a memory effect that could leak information. New methodologies to improve pull-down logic configuration for secure differential gates by redistributing the charge stored in internal nodes, removing memory effects appearing as a significant hole in security is being studied [1]. The methodology has been applied to the design of AND/NAND and XOR/XNOR gates in a 90nm TSMC technology. Proposals optimize the SABL (Sense Amplifier Based Logic) gates, widely used in cryptocircuit implementations, by removing residual charge in the pull-down circuit and simplifying the pull-up, see Figure 1. Proposals improve SABL in terms of area, power consumption, propagation delay and security.

To demonstrate the gain in performances, both gates have been designed, physically implemented and experimentally characterized, in 90 nm TSMC technology. Experimental results show a reduction of 15% in area, 12% in power consumption and 40% in delay, having at least an improvement of a factor of x50 in security (MTD measurement) [2,3], see Table I.

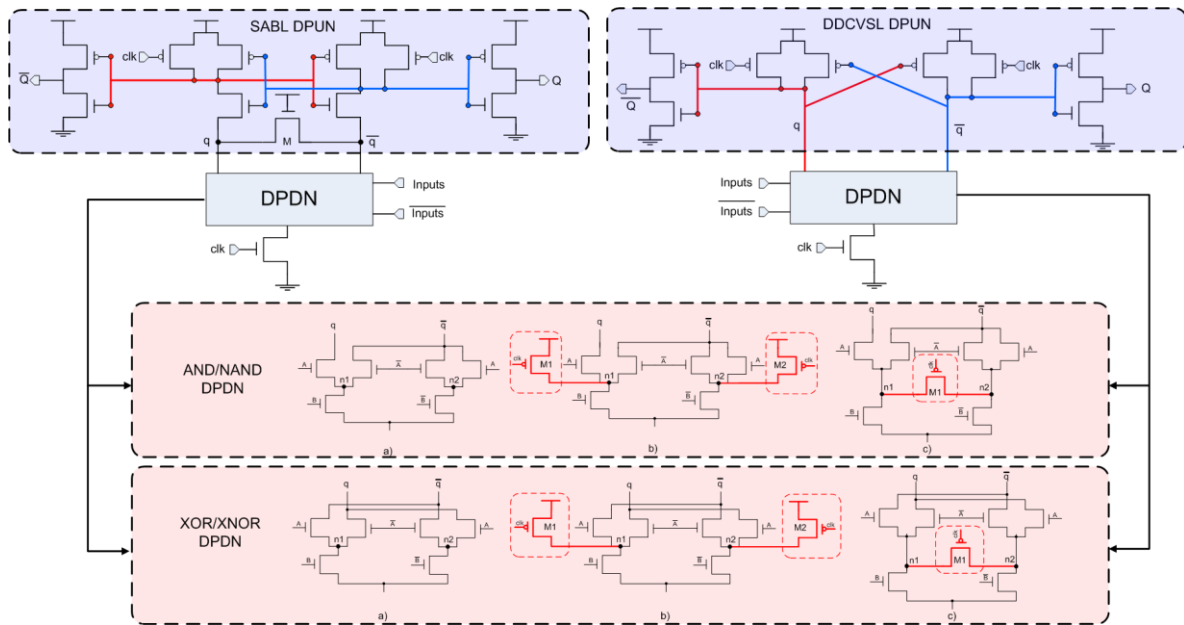


Figure 1. SABL and DDCVSL pull-up network with different combinations of differential pull-down networks.

		Evaluation			Precharge			Eavg_Total (fJ)	Delay (ps)	Transistors
		NED	NSD	Eavg (fJ)	NED	NSD	Eavg (fJ)			
XOR/XNOR	SABL [11]	3.47e-3	1.54e-3	12.00	2.14e-3	5.13e-4	21.72	33.72	173	18
	DDCVSL [15]	1.41e-3	3.67e-4	6.13	4.54e-3	1.30e-3	19.92	26.05	142	17

Table I. Simulation results for single gate measurements.

A double setup for simulation and experimental-based CPA/CEMA attacks have been developed. First, a simulation-based CPA attack on the Trivium stream cipher [4,5] (designed with insecure CMOS standard cells) and Sbox-9 of the Kasumi algorithm (implemented with standard CMOS gates and our gates [1]) has been done [1-3]. Experimental CPA/CEMA attacks and t-test on Trivium, AES and Sbox-9 implementations on FPGA and ASIC are being done to build a complete vulnerability analysis framework [6], see Figure 2. Work on this is in progress.

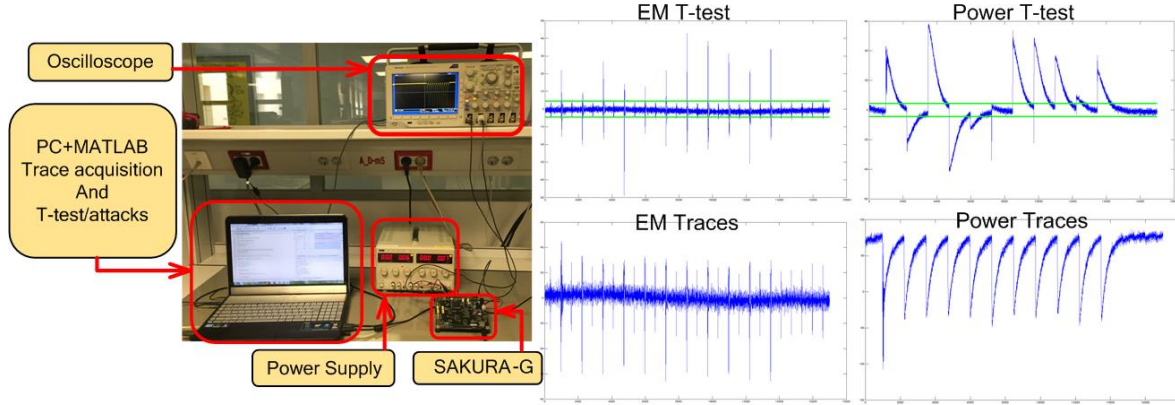


Figure 2. Experimental setup, power/EM traces and t-test results.

Finally, the effect of high-performance techniques for high speed designs in secure cryptographic implementations, using dual precharge logic styles with fine-grained pipelining with an overlapping three-phase clock scheme (see Figure 3), has been studied [7]. Simulation-based CPA attacks show how the proper synchronization of data signals gives better results in terms of power consumption and operating frequency, but affect negatively the security against side channel attacks, decreasing the number of input patterns needed to disclosure the secret key.

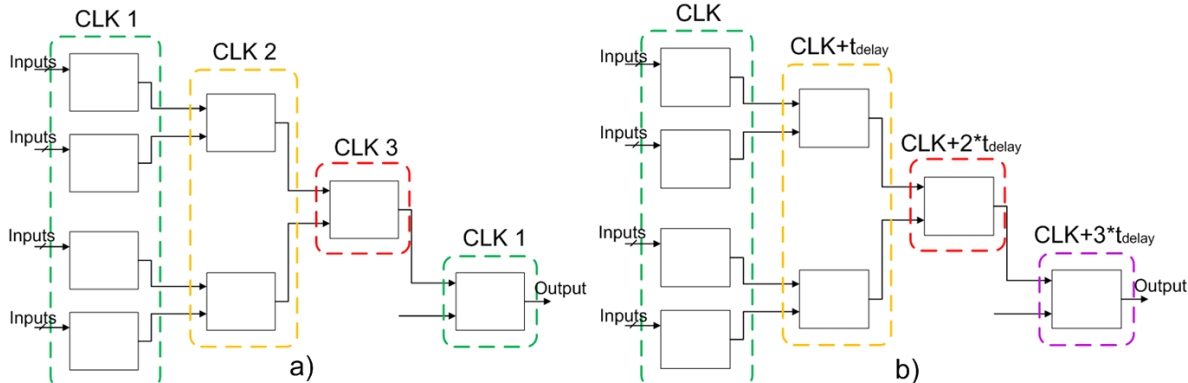


Figure 3. a) Combinational function scheme with 3 phases and b) combinational function scheme with local delay.

#### ACKNOWLEDGMENTS

This work was partially supported by CSIC (Projects 201450E034 and 201550E039) and by Spanish Government (Project TEC2013-45523-R), (with support from the European Regional Development Fund - FEDER).

#### REFERENCES

1. Tena-Sanchez, E.; Castro, J.; Acosta, A.J., "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, 2014.
2. Tena-Sanchez, E.; Castro, J.; Acosta, A.J., "Low-Power Differential Logic Gates for DPA Resistant Circuits," 17th Euromicro Conf. on Digital System Design (DSD'14), 2014.
3. Tena-Sánchez, E.; Castro, J.; Acosta, A.J., "Design and test of a low-power 90nm XOR/XNOR gate for cryptographic applications," Int. Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS'14), 2014.
4. Tena-Sánchez, E.; Acosta, A.J., "DPA vulnerability analysis on Trivium stream cipher using an optimized power model," Int. Symposium on Circuits and Systems (ISCAS'15), 2015.
5. Tena-Sánchez, E.; Acosta, A.J., "Optimized DPA attack on Trivium stream cipher using correlation shape distinguishers," Conf. on Design of Circuits and Integrated Systems (DCIS'15), 2015.
6. Canas S., Tena-Sánchez, E. and Acosta, A.J., "A low-cost FPGA-based platform to perform fast Power/Electromagnetic Attacks on cryptographic circuits", Conf. on Design of Circuits and Integrated Systems (DCIS'16), 2016.
7. Tena-Sánchez, E.; Acosta, A.J. and Nuñez J., "Secure Cryptographic Hardware Implementation Issues for High-Performance Applications", Int. Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS'16), 2016.