Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-43-46

ATTACKS ON SMART CARDS' HARDWARE AND THEIR UP-TO-DATE COUNTERMEASURES

Milena Djukanović
Faculty of Electrical Engineering, University of Montenegro

Abstract:
This paper presents up-to-date side-channel attacks and their countermeasures. A classification of side-channel attacks and countermeasures is done and how to design a model of side-channel attack is presented. A novel transistor-level countermeasure approach, three-phase dual-rail pre-charge logic (TDPL), against side-channel attacks based on analysis of crypto core's leakage currents is explained. Algorithms and models to predict the input vector for maximum and minimum leakage current in CMOS and TDPL gates are reviewed. Extensive transistor level simulations on basic gates implemented in 65 nm CMOS technology are presented and a methodology to analyze this data and compare CMOS vs. TDPL as a possible countermeasures. The results of this study show that leakage current can be easily exploited as a side channel by an attacker to extract information about the secret key in cryptographic hardware in CMOS crypto-design, while TDPL can be a reliable countermeasure to use in future design of smart cards.

Key words:
smart cards,
hardware,
side-channel attacks,
cmos,
tdpl.

INTRODUCTION

Smart cards are perhaps some of the most widely used electronic devices today, and in many cases these devices are in the front-line, defending citizens and systems against attacks on information security [1]. The most important characteristic of a smart card is security and there are four components that guarantee it: card body, chip hardware, operating system and application. There are few different approaches in systematic classification of attacks on smart cards: invasive, semi-invasive and non-invasive. However, the most efficient group of attacks are non-invasive attacks (also called passive or side-channel attacks), and they are based on weaknesses in implementation of software or hardware.

Side-channel attacks (SCA) benefit from side channel information, which is collected by measuring some physical quantity [2]: power consumption, electromagnetic radiation, execution time, computation faults (Fig. 1). Especially one of these side-channel attacks has attracted much attention since it has been announced and it is called Power Analysis Attack [3]. This attack exploits the dependence of the dynamic or static power consumption on the inputs of a cryptographic algorithm, i.e. the input ciphertext (plaintext) that is to be decrypted (encrypted) and the secret key. The general idea of a side-channel attack is that all available knowledge of a smart card's hardware has to be used in order to design a model of a side-channel attack which will help in finding a hidden key. That knowledge usually obtains information about implemented cryptographic algorithm and technology used for integrating cryptographic hardware.

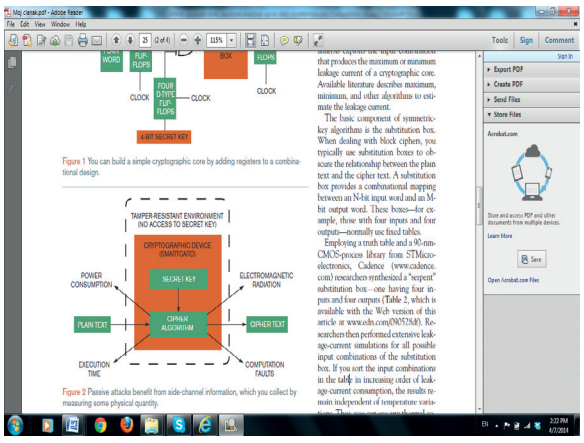

Fig. 1. Side-channel attack types [4].

The most important step in one side-channel attack is to make the best possible model of a side-channel attack (Fig. 2). As seen in this figure, the model of a side-channel does not have to bee highly sophisticated or complicated, it is rather simple. One of input parameters of the model has to be a key or a part of a key. The fact that the output of a side-channel model is dependent of the secret key

is it's most important characteristic. This model dependence has to be equal to the realistic dependence between the output and the secret key implemented in the cryptographic core.

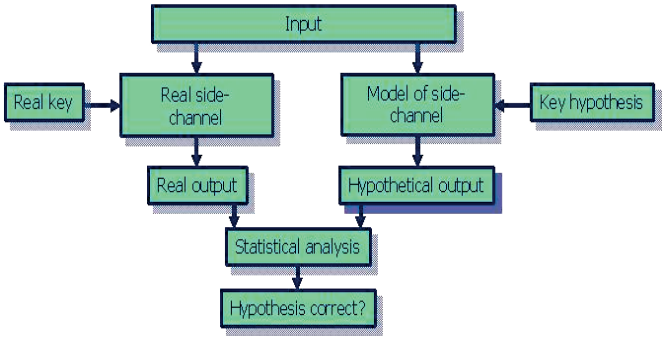

Fig. 2. Model of a side-channel attack.

In order to reveal the secret key in cryptographic core, the attacker makes the hypothetis of the key and finds out through side-channel model is it correct. This hypothesis is usually related to the Hamming weight of the key or some segment of the key. Main idea of this attack is based on measuring the real side-channel information and comparing it to hypothetical side-channel output. Different statistical methods used in side-channel attacks ask from attacker to measure the side-channel output more than once. The more of these measurements there are, the better are aproximated differences in attacker's model of a side-channel.

The succes of a side-channel attacks surely depends on the implemented technology. Nowadays, CMOS is by far the most commonly used in digital integrated circuits. However, in sub-100 nm technologies dynamic power is no longer the dominant contribution to the chip power budget because of the much faster increase of leakage (i.e., static) power at each technology generation [5]. That is the reason why dependence of leakage current on input and other data in CMOS logic and new countermeasure logic will be analyzed in this paper.

The remainder of this paper is organized as follows. Section II will examine all available countermeasure styles for side-channel attacks. In Section III leakage current and its data dependence has been studied on basic l-type gates [6] of CMOS and TDPL technology, using a 65-nm CMOS cell library from STMicroelectronics in the Cadence environment. Section IV shows the results of measured resistances of CMOS and TDPL technologies against side-channel attacks based on analysis of leakage current. Conclusions are reported in Section V.

COUNTERMEASURE STYLES

With new characteristics of leakage current in new technologies in the recent years, a wide extent of hardware countermeasures have been proposed in the technical literature. These countermeasures can be classified according to the involved abstraction level during the design flow: system-level, gate-level and transistor-level. System-level techniques include adding noise to the device power consumption [7], duplicating logics with complementary operations [8], active supply current filtering with power consumption compensation, passive filtering, battery on chip and detachable power supply, etc. Gate-level countermeasures include circuital techniques which can be implemented using logic gates available in a standard-cell library, e.g. random masking [9], random pre-charging, state transitions and Hamming weights balancing. Transistor-level techniques are created as a countermeasure for power analysis attacks and consist of the adoption of a logic family whose power consumption is independent of the processed data.

CMOS is the most popular transistor-level approach, also implemented in all software libraries of standard smart card cells, but not efficient as a countermeasure for PA attacks. Static Complementary CMOS logic only consumes energy from the power supply when its output has a 0-1 transition. In fact, during the 1-0 transition the energy previously stored in the output capacitance is dissipated and in the two events of a 0-0 or a 1-1 transition no power is used. This asymmetric power demand provides the information used in PA to find the secret key. A logic style with data-independent power consumption does not reveal this information. When logic values are measured by charging and discharging capacitances we need to use a fixed amount of energy for every transition. The most efficient logic styles that have these characteristics and combine dual-rail and precharge logic are SABL (Sense Amplifier Based Logic) [10], WDDL (Wave Dynamic Differential Logic) [11], 3sDL (3-state Dynamic Logic) [12] and one of recently proposed - TDPL (Three-Phase Dual-Rail Precharge Logic) [13], [14].

In a dual-rail pre-charge (DRP) logic style, signals are encoded as two complementary wires and power consumption is constant under the hypothesis that the outputs drive the same capacitive load. This fact means that if we have different values of capacitors, the power consumption in periods will not be constant. This is the reason for adding one more phase – discharge, so the power consumption can be independent on the values of capacitors. During the first phase (*precharge*), the output lines of a generic logic gate are both charged to VDD. In the second phase - *evaluation* phase, the output depends on the value of input. In the last phase – *discharge* phase, both outputs are discharged to VSS (Fig. 3, Fig. 4).

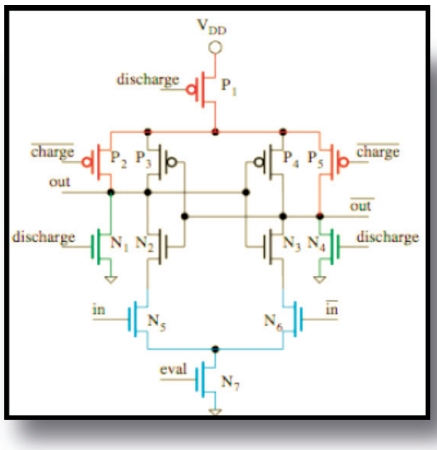

Fig. 3. An example of a TDPL circuit – TDPL inverter.

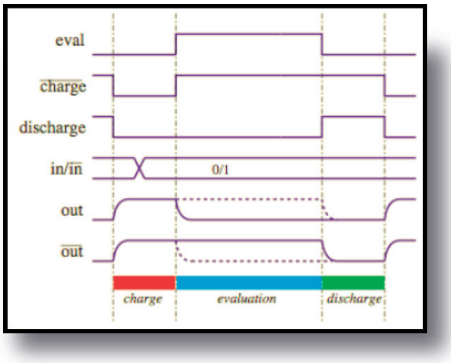

Fig. 4. Timing diagram of the TDPL inverter.

The proposed approach has already been tested by others, but mostly as a logic style against attacks based on analysis of crypto cores' dynamic currents. It has to be noted that leakage current can be measured in a similar way as the dynamic current is measured in traditional PA attacks and that leakage power measurements are in principle simpler to carry out [15], [16].

In this study, l-type model Mosfets both for CMOS and TDPL logic circuits are used, using a 65-nm CMOS cell library from STMicroelectronics in the Cadence environment.

LEAKAGE CURRENT AND ITS DATA DEPENDENCE

The results of the experiments carried out on basic l-type CMOS gates showing the sensitivity of the leakage current of these gates to input data variations are reported in Table I. It has to be noted that if we sort leakage currents associated to their logic levels in ascending order, the same order is preserved with temperature variations. It means, for example, that in a 2-input XOR gate, logic input *01* is able to generate the maximum leakage current for all temperature values.

TABLE I. LEAKAGE CURRENTS OF BASIC CMOS GATES

NOT Gate CMOS065						
A		**T=0°**	**T=25°**	**T=50°**	**T=75°**	**T=100°**
0		23.148n	37.561n	58.893n	88.319n	126.7n
1		40.99p	92.92n	183.933n	327.11n	533.9n
NAND Gate CMOS065						
A	**B**	**T=0°**	**T=25°**	**T=50°**	**T=75°**	**T=100°**
0	**0**	14.33n	16.47n	19.83n	24.99n	32.58n
0	**1**	23.13n	37.5n	58.75n	87.99n	126.03n
1	**0**	19.16n	30.86n	48.48n	73.16n	105.82n
1	**1**	81.96n	185.73n	367.42n	652.8n	1.06u
XOR Gate CMOS065						
A	**B**	**T=0°**	**T=25°**	**T=50°**	**T=75°**	**T=100°**
0	**0**	110.2n	210.49n	381.36n	647.34n	1.03u
0	**1**	164.66n	294.85n	501.27n	802.64n	1.21u
1	**0**	134.97n	245.56n	422.66n	684.02n	1.04u
1	**1**	140.62n	309.36n	608.78n	1.08n	1.76u

TABLE II. LEAKAGE CURRENTS OF BASIC TDPL GATES.

NOT Gate TDPL065						
A		**T=0°**	**T=25°**	**T=50°**	**T=75°**	**T=100°**
0		117.338n	235.887n	437.36n	745.162n	1.176u
1		117.338n	235.887n	437.36n	745.162n	1.176u
NAND Gate TDPL065						
A	**B**	**T=0°**	**T=25°**	**T=50°**	**T=75°**	**T=100°**
0	**0**	116.84n	234.77n	435.17n	741.38n	1.17u
0	**1**	117.33n	235.88n	437.35n	745.14n	1.176u
1	**0**	116.45n	234.36n	435.52n	743.2n	1.174u
1	**1**	118n	237.42n	440.4n	750.46n	1.184u
XOR Gate TDPL065						
A	**B**	**T=0°**	**T=25°**	**T=50°**	**T=75°**	**T=100°**
0	**0**	116.97n	236.74n	440.88n	752.81n	1.18u
0	**1**	116.97n	236.74n	440.88n	752.81n	1.18u
1	**0**	116.97n	236.74n	440.88n	752.81n	1.18u
1	**1**	116.97n	236.74n	440.88n	752.81n	1.18u

Table II reports leakage current simulations on standard TDPL gates. For NOT and XOR TDPL gates, whose structures are symmetric, leakage currents are independent on the input value. For NAND TDPL gate slight differences in leakage current values can be seen, but not enough evident to be precisely connected to the input data. With temperature rise, leakage current order is preserved for TDPL NAND gate, and leakage current values grow for the others. Both in Table I and II presented leakages are in Amperes and temperatures in Celsius degrees.

ANALYSED MEASURED RESISTANCES OF CMOS AND TDPL TECHNOLOGIES

In order to show the difference between use of CMOS and TDPL technology as a countermeasure against side-channel attacks based on analysis of leakage currents, a simple study is done. The obtained results for the three analyzed gates at the temperature 25° are summarized in Table III. Comparison of these technologies has been analyzed through two factors: NED (Normalized Energy Deviation) and NSD (Normalized Standard Deviation). The energy per cycle

$$E = V_{DD} \int_0^T I_D(t)dt \quad (1)$$

is adopted as figure of merit to measure the resistance against leakage current analysis attacks. NED is defined as

$$\frac{Max(energy/cycle) - Min(energy/cycle)}{Max(energy/cycle)} \quad (2)$$

while NSD is defined as

$$\frac{\sigma_D}{mean(energy/cycle)} \quad (3).$$

As expected, TDPL gates show extremely balanced energy consumption, and they are independent to input data values.

TABLE III. COMPARED NED AND NSD FACTORS FOR CMOS AND TDPL L-TYPE GATES.

	CMOS NOT	TDPL NOT	CMOS NAND	TDPL NAND	CMOS XOR	TDPL XOR
max$E$ nJ	111.5	283	222.8	284.9	371.2	284
min$E$ nJ	45.07	283	19.7	281.2	252.5	284
NED	59.5%	0%	91.1%	1.2%	31.9%	0%
$\overline{E}$ nJ	78.28	283	81.1	282.7	318.0	284
σ_E nJ	33.2	0	82.3	1.4	47.2	0
NSD	42.4%	0%	101%	0.5%	14.8%	0%

CONCLUSION

Since leakage current can become a problem to take into account during crypto-core design, especially for crypto-cores implemented in technologies with gate length under 0,1 μm which exhibit a high leakage power consumption, through a simple case study we have shown that TDPL 65nm technology is better as a countermeasure in comparison to CMOS 65nm technology.

REFERENCES

[1] Rankl, W. Effing, "Smart Card Handbook", John Wiley and Sons, third edition 2003.

[2] K. E. Mayes, K. Markantonakis, "Smart Cards, Tokens, Security and Applications", Springer, 2008.

[3] M. Aigner, E. Oswald, "Power Analysis Tutorial", available at http://www.iaik.tugraz.at.

[4] Milena Djukanovic, "Leakage-power analysis enables attacks on cryptographic devices," EDN Journal, Volume 54, Issue 10, pp. 23-26, May 2009

[5] International Technology Roadmap for Semiconductors, 2008. Update, available at http://www.public.itrs.net.

[6] K. Hoffman, "System Integration – from Transistor Design to Large Scale Integrated Circuits", John Wiley and Sons, England 2004.

[7] L. Benini, E. Omerbegovic, A. Macii, M. Poncino, E. Macii, F. Pro, "Energy-aware design techniques for differential power analysis protection", Proc. Design Automation Conf. (DAC '03), pp. 36-41, 2003.

[8] H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, W. Zhang, "Masking the energy behaviour of DES encryption", Proc. Design, Automation, and Test in Europe Conf. (DAT '03), pp. 84-89, 2003.

[9] J. Dj. Golic, R. Menicocci, "Universal masking on logic gate level", Electronics letters, vol. 40, no. 9, April 2004.

[10] K. Tiri, M. Akmal, I Verbauwhede, „A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards", Proc. IEEE 28th European Solid-State Circuit Conference (ESSCIRC'02), 2002.

[11] K. Tiri, I. Verbauwhede, „A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", Design, Automation and Test in Europe Conference and Exposition (DATE 2004), 16-20 February, 2004, Paris, France, volume 1, pp. 246-251, IEEE Computer Society, 2004.

[12] M. Aigner, S. Mangard, R. Menacocci, M. Olivieri, G. Scotti, A. Trifiletti, „A Novel CMOS Logic Style with Data Independent Power Consumption", in International Symposium on Circuits and Systems (ISCAS 2005), Kobe, Japan, May 2005, Proceedings, volume 2, pages 1066-1069, IEEE 2005.

[13] Marco Bucci, Luca Giancane, Raimondo Luzzi, Alessandro Trifiletti, "Three-phase Dual-rail Pre-charge Logic", Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2006.

[14] M. Jovanovic, Z. Mijanović, "Leakage Analysis Attacks for CMOS Cryptographic Hardware and TDPL Technology as Countermeasure," 13th YUINFO Conference, Kopaonik, Serbia, 2007

[15] M. Djukanovic, L. Giancane, G. Scotti, A. Trifiletti, "Impact of Process Variations on LPA Attacks Effectiveness", Proceedings of 2009 International Conference on Computer and Electrical Engineering (ICCEE09), Volume 1, Dec. 2009, pp.102-106

[16] Alioto, M., Bongiovanni, S., Djukanovic, M., Scotti, G., Trifiletti, A., "Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations," IEEE Transactions on Circuits and Systems I: Regular Papers, Issue 99, pp. 1-14, Aug. 2013.