Strategies against Side-Channel-Attack

Milena Stanojlović, Predrag Petković

Abstract – This contribution discusses cryptographic algorithm in hardware that protects the information leaks out of the device through so called „side channels“. This class of attacks is called side-channel attacks (SCA). Important information, such as secret keys, can be obtained by observing the power consumption, the electromagnetic radiation, the timing information etc. There are several types of protection and some will be discussed in this paper. Special attention is paid to Wave Dynamic Differential Logic (WDDL) that was evaluated in terms of load symmetry on an example.

Keywords – Side Channel Attack, Wave Dynamic Differential Logic.

I. INTRODUCTION

Data security becomes very important issue in everyday life. Starting from credit cards, coded alarm systems to all types of cipher-protected data transfer it is necessary to hide code keys from unauthorized misuse. The first defending line is using complex multi-bit ciphers. Crushing them by simple software tools based on proper combination search become very time-consuming. Longer password and more sophisticated coding algorithms result to the bigger number of combinations and therefore the better protection. One can say that the problem of data protection could be solved just increasing the number of combinations. However, the value of hidden data enormously increases. This inspires potential attackers to invest more money and brain in order to crack cipher. It has been shown in [1] that monitoring power helps a lot in finding cipher. Thereafter other methods emerged that makes cipher cracking easier, like Simple Power Analysis (SPA), Differential Power Analysis (DPA) and Electromagnetic Analysis (EMA) [2]. Common to all these methods is analysis of information that leaks from physically implemented hardware. They can be collected only if somebody intentionally uses sophisticated probes to attack crypto-processor. Therefore they are named side channel attack. There are different attack tactics like Fault induction attack, Timing attack, Probing attack [2].

The scientific community responses with new hardware and software based countermeasures.

The aim of this paper is to enlighten some strategies in fighting against SCA. Especially authors are interested in protecting data from power-meters during automatic meter reading [3]. It is expected that new solid-state power-meter designed as ASIC in Laboratory for Electronic Design Automation at University of Niš, comprise a communication block resistible to SCA. Therefore it is desirable to fight against SCA within standard CMOS technology and preferably using standard cell library. Therefore Waveform Dynamic Differential Logic (WDDL) is in scope of our interest and it will be discussed from implementation point of view. Our goal is to determine the permitted amount of load mismatch that still guarantees resistivity to DPA attack.

The paper is organized as follows. The subsequent section gives a brief survey of countermeasures. The third section presents basics of WDDL. Influence of unsymmetrical load of a WDDL cell to the SCA resistivity is described on example of AND gate in the fourth section together with simulation results.

II STRATEGIES AGAINST SCA

Although power analysis and EMA requires using different probes the source of data leakage is common in both cases. The leakage is the outcome of changes in IDD during logic state transitions. Each change 0-1 requires additional charge to be passed from bias to the output capacitance. In contrary change 1-0 discharges load and no current flows from VDD. This is sufficient to detect what is happening inside IC just by monitoring IDD.

All strategies in fighting against leaking data through power changes relay on hiding correlation between the logic state changes and the waveform of power. Depending on the level where performed they can be sorted as measures at architectural, algorithmic or gate level.

In scope of methodology they can be categorized as randomizing, masking and signal independent power change.

Randomization at algorithmic level relies on frequently change of secret key to avoid possibility of finding the correlation.

Masking methods require additional logic operations to cover real data. It is possible to perform them on algorithmic level and on the gate level, as well. However, higher order power analysis can crack masking.

There are several ways to make power consumption of a cell independent on data flow.

One is to keep constant power consumption all the time. This is possible by inserting analog modules. However the overall consumption of power is considerably high.

The other way is to force all digital cells to have the same power pattern for every logic change. This class of methods is known as *Dual-rail with Precharge Logic* (DPL). All signals are duplicated and have true and false representations. The cells operate in alternated *precharge*

Milena Stanojlović and Predrag Petković are with the Department of Electronics, Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia, E-mail: milenastanojlovic@yahoo.com; predrag@elfak.ni.ac.rs.

and *evaluation* phases to ensure exactly one switching event per cycle. *Wave Dynamic Differential Logic* (WDDL) [4] is good representative of DPL. It can be implemented with standard CMOS cells and therefore it is good candidate for implementation in standard ASIC technologies.

III WAVE DYNAMIC DIFFERENTIAL LOGIC

The main purpose of a WDDL cell is to provide uncorrelated power consumption to the operated data. Therefore it should have the same number of transitions for every combination of input signals. In case of inverter it means that every change on input must have the same contribution to IDD. This is possible if inverter is realized with two standard invertors (connected to the same VDD) as Fig. 1.a shows.

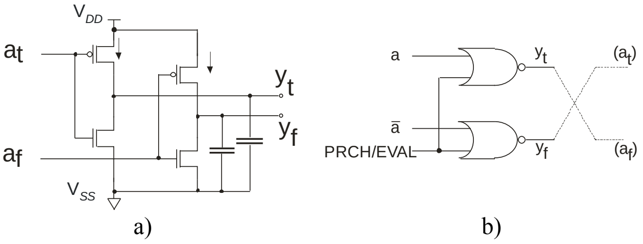


Fig. 1. WDDL inverter

Indexes *t* and *f* denotes true and fault signals, respectively. Knowing that $\mathbf{a_f}$=NOT($\mathbf{a_t}$) it is obvious that for same load any change on **a**=$\mathbf{a_t}$ will produce the same IDD.

However, for other types of cells it is not sufficient to have duplicated hardware. Each cell should have own dual cell. This means that for every $\mathbf{y_t}$=$\mathbf{a_t}$ ¤ $\mathbf{b_t}$ the complement output is needed such as $\mathbf{y_f}$=NOT($\mathbf{y_t}$)=NOT($\mathbf{a_t}$) * NOT($\mathbf{b_t}$). Note that ¤ and * denote different (complementary) operators. For AND operator OR is complementary and vice versa. Fig. 2 represents WDDL AND cell.

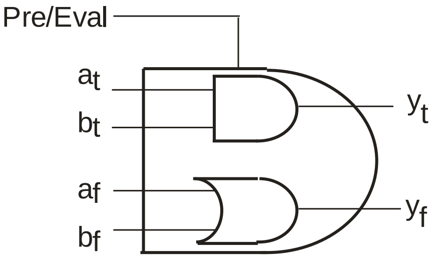


Fig. 2. WDDL AND cell

In order to provide the same IDD for every input change, combinational cells should work in two phases. During *precharge* phase all signals are forced to the low logic level. Thereafter, in *evaluating* phase outputs establish the proper values. Hence, the inverter cell is not realised as in Fig. 1.a but rather as shown in Fig 1.b. The same architecture is used as generator for waveforms of $\mathbf{a_t}$ and $\mathbf{a_f}$ from **a** and NOT(**a**) signals (dashed lines).

Figure 3 shows waveforms of controlling Precharge/Evaluation signal and all input and output signals for the case that corresponds to the single-rail AND cell stimulated with patterns **a**=1, **b**=0 and **a**=1, **b**=1.

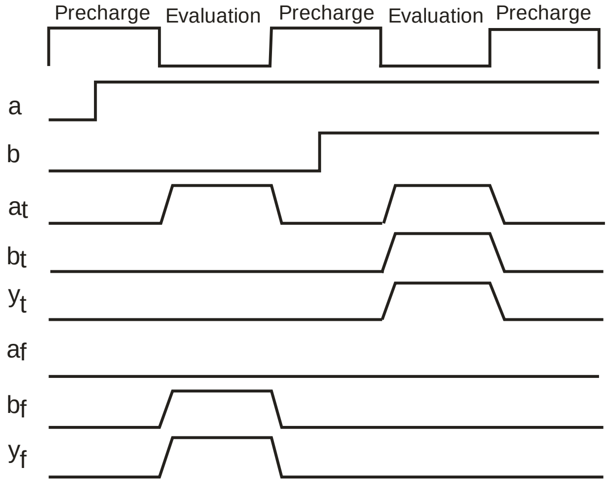


Fig. 3. Waveforms for WDDL AND cell

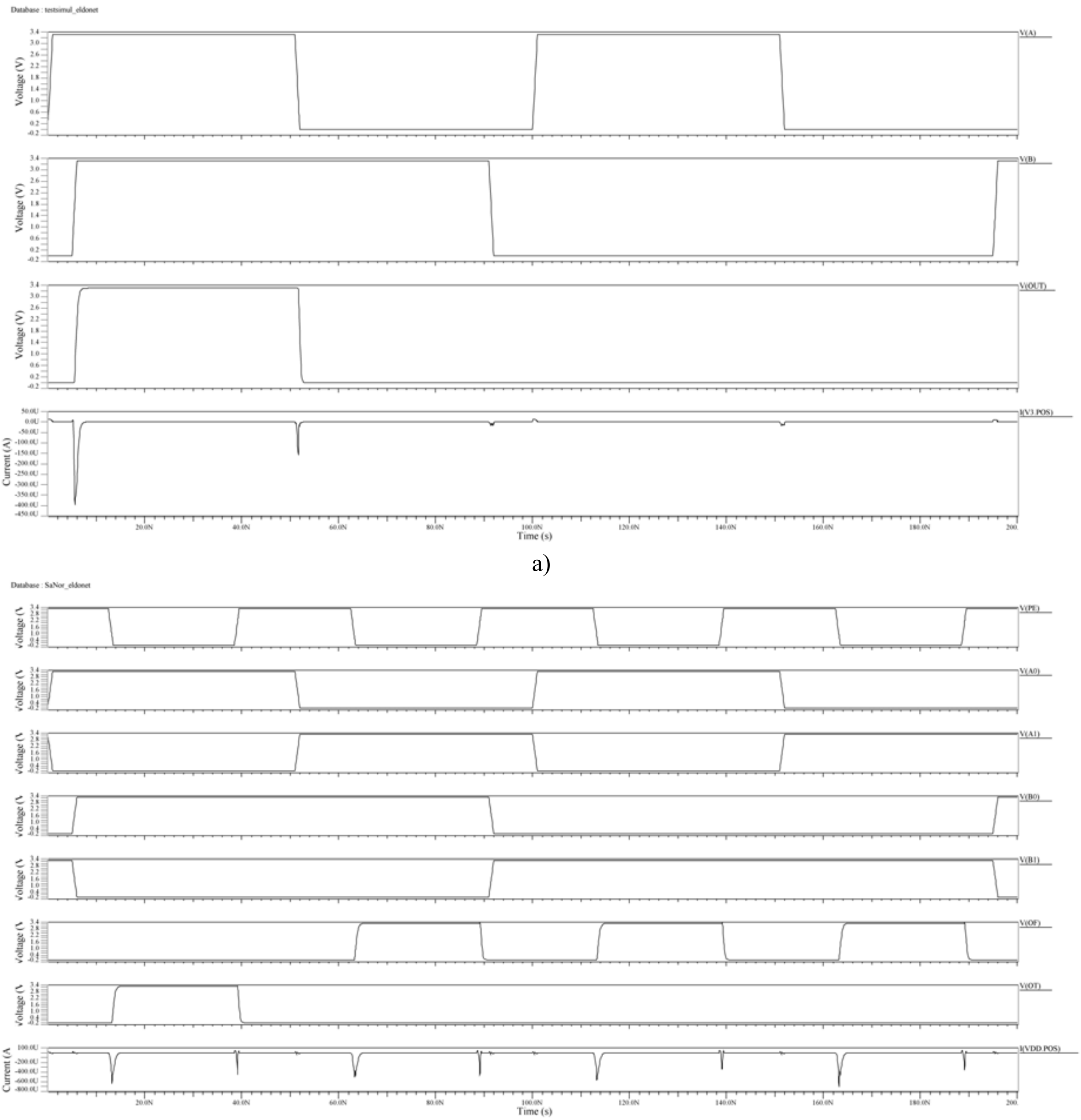
During precharge phase all signals are set to low level. During evaluating phase only exactly one of outputs goes to the high level. Therefore only one load capacitance will charge from VDD.

Obviously, if input signals come in slightly different moment WDDL architecture implemented for NAND cell will generate glitches observable to attacker. Simultaneously this will produce leakage and all design becomes vulnerable. This is reason why WDDL works only with “positive” gates (AND, OR) and not with negative gates (NAND, NOR). There is modification of WDDL that is capable to work with negative gates named Dual Spacer Dual Rail Logics [5].

So far it is clear that good SCA protection costs duplication in hardware. Unfortunately with sequential gates the price is even higher. To retain good DPA protection it is necessary to quadruple number of flip-flops [6]. In practical realizations in FPGA it is reported that hardware overhead is over five times and that operating frequency is lower for more than twice [6].

This price is acceptable having in mind the security aspect. However, WDDL is reliable only if loads of both “true” and “false” signals are balanced. When that is not case there is leakage due timing difference [7] that jeopardizes the overall concept.

Therefore several algorithms were developed to provide symmetrical routing. The main advantage of WDDL is that it can be implemented with standard cell libraries. Hence, standard routing tools can be utilized. Unfortunately they are not optimized for symmetry and tricky part is how to obtain symmetrical wires with minor intervention in standard routing algorithms



a)

b)

Fig. 4 Waveform of IDD for a) single-real AND gate; b) WDDL AND gate with balanced load

In the following section we will present the influence of mismatched load on power leakage.

IV WDDL RESISTIVITY TO UNBALANCED LOAD

As an example WDDL AND gate will be considered. It is designed in CMOS035 technology. The IDD waveform of a single-rail AND gate designed in the same technology will serve as a reference. Thereafter, an ideally balanced WDDL AND cell is simulated.

Figure 4 depicts waveforms of both gates. IDD waveform of single raid AND gate exploits very clear difference when output changes state from 0 to 1 and from 1 to 0, as Figure 4.a shows. Therefore, the whole information about state at the output is visible through IDD. In contrary, supply current of WDDL implemented AND gate have regular pattern independently on output logic states as the bottom diagram in Fig. 4.b presents. Consequently it is immune on side channel attack.

It is interested to evaluate what leakage should be expected under different amount of mismatched load. A set of several simulations were done for different rate of mismatch. As measure of mismatch the integral of IDD is used. Actually the integral corresponding to transition 0-1 is compared with that obtained for change 1-0. Obviously

WDDL cells have change on “false” output during neutral transitions (0-0 and 1-1), as well. In order to hide leaking information about output logic state the integrals of current corresponding to all changes should be the same. There are several methods for their comparison and, accordingly, for design apprising. One of them is to compare integrals of IDD during evaluation phase with each other. Particularly WDDL AND gate was analysed for load capacitances unjust of up to ±15%.

Table I summarizes results for different mismatch of load values. Assuming that mismatch of 10%.is sufficient to explore observable leakage, one can conclude that it can be reached for load mismatch up to 20%.

TABLE I
WDDL GATE MISMATCHED

Tran.	Single AND	WDDL Ct/Cf=1	WDDL ΔC=5%	WDDL ΔC=15%
0-0	-9.82837E-15 (A=(0->1), B=1)	-4.97E-13	-5.10E-13 -2.61%	-5.36E-13 -7.86%
0-1	-5.45165E-14 (A=(1->0), B=1)	-4.99E-13	-5.12E-13 -2.62%	-5.38E-13 -7.88%
1-0	1.01E-14 (A=1, B=(1->0))	-4.81E-13	-4.94E-13 -2.71%	-5.20E-13 -8.16%
1-1	-3.00538E-13 (A=1, B=(0->1))	-4.86E-13	-4.99E-13 -2.68%	-5.25E-13 -8.05%

V CONCLUSION

This paper presented some of countermeasures against SCA. WDDL was particularly examined in scope of unsymmetrical load. The results obtained for ideally matched outputs were compared to several mismatch levels for typical exploitation conditions. The obtained results will be analyzed in scope of technology and geometrical parameters. Actually for known tolerances of particular technology one can estimate appropriate wire width and/or metal level that should be used for best matching false and true signals.

Capacitance and resistance of a wire depend on technological and geometrical parameters.

Therefore, for known amount of the parameter mismatch it is possible to calculate physical dimensions of wires that could keep matching within acceptable limits. Besides layout designer could decide what shape and width of wires to use. It is known that it is easier to match larger patterns. Hence, wire dimensions could be customized for better matching. Tolerances of wire capacitance and resistance depend on metal layer. It is feasible to establish some kind of design rule that will limit wire length in respect of matching similar to the *antenna rule*.

When analyzing load mismatch it is important to be aware of different timing effects that should open up under different faulty circumstances. In order to get good insight into WDDL vulnerability one needs to perform thorough corner analysis for lower VDD, higher temperature, quicker/slower excitation.

The obtained results will help in making decision on what type of SCA protection should be most appropriate for implementation in integrated power meter.

ACKNOWLEDGMENT

This work was supported by The Serbian Ministry of science and technology development within the project TR 11007.

REFERENCES

[1] Kocher, P., Jaffe, J. and Jun, B., “Differential Power Analysis,” in Proceedings of CRYPTO’99, ser. LNCS, vol. 1666. Springer-Verlag, 1999, pp. 388–397.

[2] Quisquater, J.-J., “Side channel attacks State-of-the-Art”, Report, Oct. 2002. Avilable on: http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf [Accessed 15.12.2009.].

[3] Litovski, V., Petković, P., “Why The Power Grid Needs Cryptography?”, *Electronics*, Vol. 13, No. 1, YU ISSN 1450-5843, June, 2009, pp. 30-36

[4] Tiri, K., and Verbauwhede, I., “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” Proc. of DATE’04. IEEE Computer Society, February 2004, pp. 246–251, Paris, France.

[5] Sokolov, D., Murphy,, J., Bystrov, A., and Yakovlev, A., “Design and Analysis of Dual-Rail Circuits for Security Applications”. IEEE Transactions on Computers, Vol. 54, No. 4, 2005, pp. 449–460, ISSN 0018-9340.

[6] Selmane, N., Bhasin, S., Guilley, S., Graba, T., and Danger, J.-L., “WDDL is Protected Against Setup Time Violation Attacks”, HAL – CCSD, hal-00410135, version 1 – 17, Aug. 2009

[7] Guilley, S., et al., “Shall we trust WDDL? in Future of Trust in Computing”, In “Future of Trust in Computing”, Springer, 2009, pp. 208-215, ISBN: 978-3-8348-0794-6 (Print) 978-3-8348-9324-6 (Online).