Hardware Based Strategies Against Side-Channel-Attack Implemented in WDDL

Milena J. Stanojlović and Predrag M. Petković

***Abstract*—This contribution discusses cryptographic algorithm in hardware that protects the information leaks out of the device through so called „side channels". Attacks on crypto-processors are based on analyses of the leaked data are known as 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.**

***Index Terms*—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 by increasing the number of combinations. However, the value of encrypted data enormously increases. This inspires potential attackers to invest more money and brainstorm 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 make cipher cracking easier. Some of them are 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. With that aim *Wave Dynamic Differential Logic* (WDDL) [4] 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 and to observe effects of V_{DD} faults on vulnerability of WDDL.

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. The fifth section considers influence of faults made by attacker to the crypto-processor with WDDL cells.

II. Strategies against SCA

Although power analysis and EMA requires using different type of probes the source of data leakage is common in both cases. The leakage is the consequence of changes in I_{DD} 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 V_{DD}. The amount of the additional charge is proportional to the number of capacitors being charged. For one who has elementary knowledge of digital cell circuitry this is valuable information that helps him to get the figure about transitions inside IC. Therefore, digital signal tracking supported with monitoring I_{DD} becomes powerful tool for discovering digital circuit behavior.

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

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

M. J. Stanojlović is with the Department of Electronics, Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia (e-mail: milenastanojlovic@yahoo.com).

P. M. Petković is with the Department of Electronics, Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia (e-mail: predrag.petkovic@elfak.ni.ac.rs).

architectural, algorithmic or gate level.

In scope of methodology they can be categorized as *randomizing*, *masking* and *blinding*.

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

Masking techniques 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 analyses are able to crack masking.

Blinding makes power consumption of a cell independent on data flow. Basically there are two ways to make power consumption of a cell independent on data flow:

- to keep constant power consumption all the time (by inserting analog modules but the overall consumption of power is considerably high);
- to force all digital cells to have the same power pattern for every logic change.

The second class of methods is known as Dual-rail with Precharge Logic (DPL) [5]. All signals are duplicated and have true and false representations. The cells operate in alternated pre-charge 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 I_{DD}. This is possible if inverter is realized with two standard invertors (connected to the same V_{DD}) as Fig. 1a shows.

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 on outputs y_t and y_f, any change on $\mathbf{a}=\mathbf{a_t}$ will produce the same I_{DD}.

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 symbol and circuitry of WDDL AND cell.

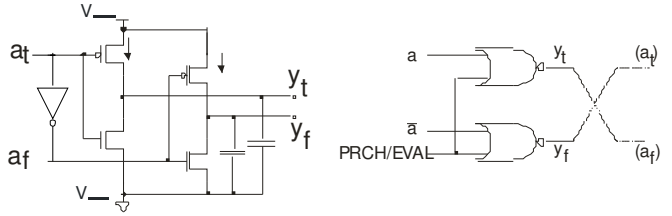
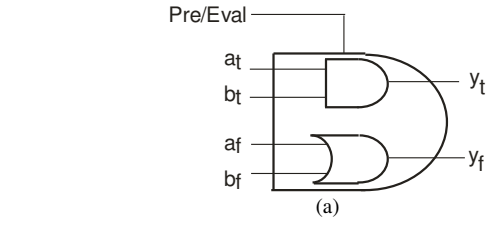


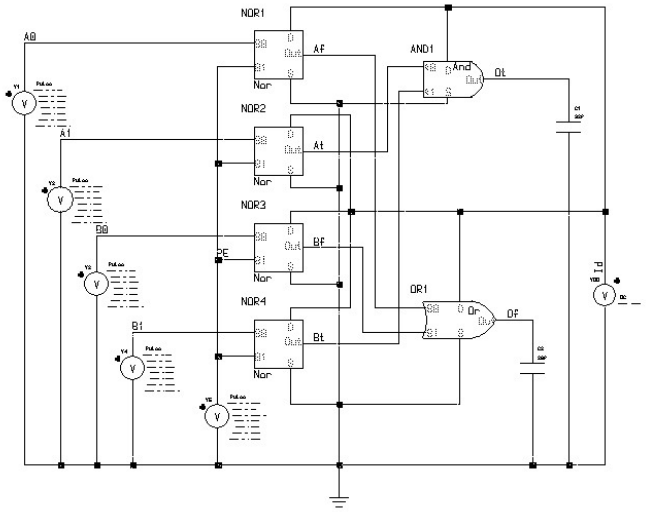
Fig. 1. WDDL inverter.

In order to provide the same I_{DD} for every input change, combinational cells should work in two phases. During *pre-charge* 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 realized as in Fig. 2a but rather as shown in Fig. 2b. The same architecture is used to generate waveforms of true and false signals that drive WDDL operators ($\mathbf{a_t}$ and $\mathbf{a_f}$ from **a** signal and $\mathbf{b_t}$ and $\mathbf{b_f}$ from **b** signal).

Fig. 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.



(a)



(b)

Fig. 2. WDDL AND cell (a) symbol, (b) circuitry.

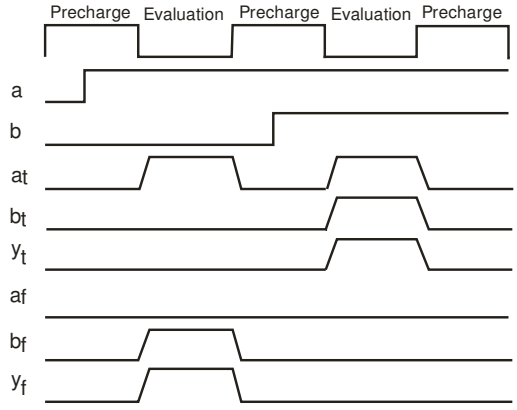


Fig. 3. Waveforms at ports of WDDL AND cell.

During pre-charge 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 V_{DD}.

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). The negative gates would require forcing gates to V_{DD} instead to zero during pre-charge. There is modification of WDDL that is capable to work with negative gates named Dual Spacer Dual Rail Logics [6].

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 [7]. 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 [7].

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 [8] that jeopardizes the overall concept.

The main advantage of WDDL is that it can be implemented with standard cell libraries. Hence, it is desirable to utilize standard routing tools, as well. Unfortunately they are not optimized for symmetry and tricky part is how to obtain symmetrical wires with minor intervention in standard routing algorithms. Therefore, several algorithms were developed to provide symmetrical routing [8].

The aim of this article is to determine amount of load misbalance allowable to protect design from SCA based on power analysis. In the following section we will present the influence of mismatched load on power leakage.

IV. WDDL RESISTIVITY TO UNBALANCED LOAD

As an example AND gate implemented in WDDL (WDDL AND) will be considered. It is designed in TSMC CMOS035 technology. The I_{DD} waveform of a single-rail AND (SR AND) gate designed in the same technology will serve as a reference. Thereafter, an ideally balanced WDDL AND cell is simulated.

Figs. 4a and 4b depicts waveforms of both gates. Fig. 4a shows that I_{DD} waveform (bottom, denoted as I(V3POS)) of single raid AND gate exploits very clear difference when output (VOUT, diagram above I_{DD} in Fig. 4a changes state from 0 to 1 and from 1 to 0. Moreover, these changes are significantly higher in comparison with those that characterize neutral events. Therefore, the whole information about state at the output is visible through I_{DD}.

In contrary, supply current of WDDL AND gate have regular pattern independently on output logic states as the bottom diagram in Fig. 4b presents. This is consequence of change on "false" output (the waveform just above I_{DD} in Fig. 4b whenever "true" output (the third waveform from bottom in Fig. 4b is still. Obviously false output changes during input combination that gives neutral transitions (0-0 and 1-1) for SR AND. If the I_{DD} waveform has the same pattern for every combination of input signals there will be no leak of information about output logic state. Integral of I_{DD} is suitable to be adopted for measure of leaking the data and accordingly, for design apprising. Practically the dynamic of power change is traced as the potential attacker would do implementing Power Analysis SCA.

For the case of SR AND cell it is reasonable to compare the integral corresponding to 0-1 output transition with that obtained for change 1-0. Their discrepancy represents so called *power signature*.

For WDDL cell we compare integrals of I_{DD} during evaluation phase with each other.

As noted in the previous section WDDL will work well only if loads of true and false outputs are in balance.

It is interesting to evaluate what leakage should be expected under different amount of mismatched load.

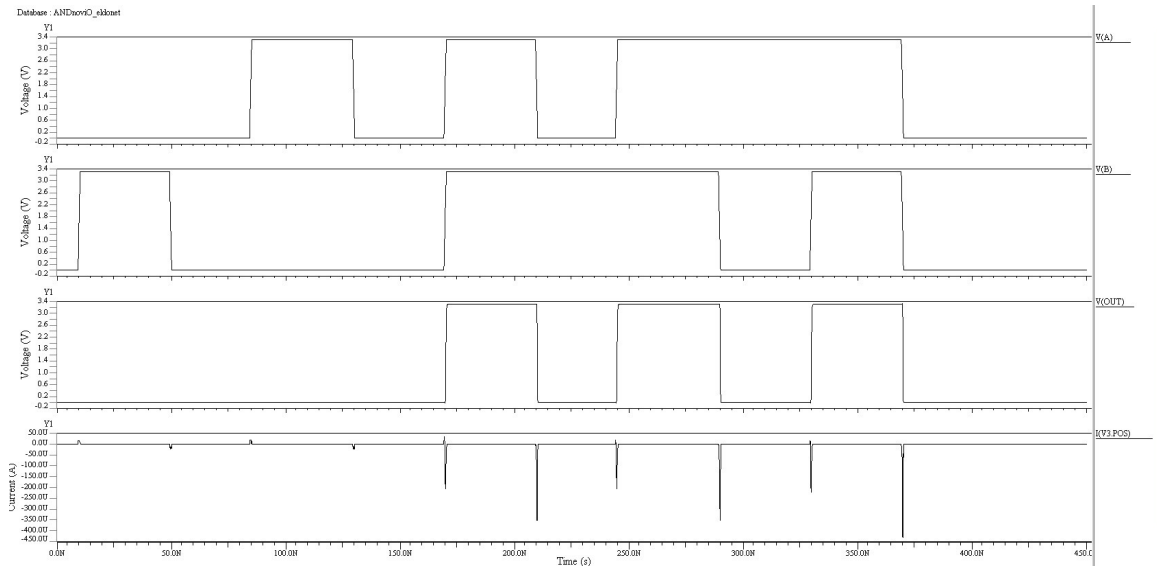
Therefore a set of several simulations were done for different rate of capacitive load mismatch. Particularly WDDL AND gate was analyzed for load capacitances unjust of up to ±15%.

Table I summarizes results for different mismatch of load values.

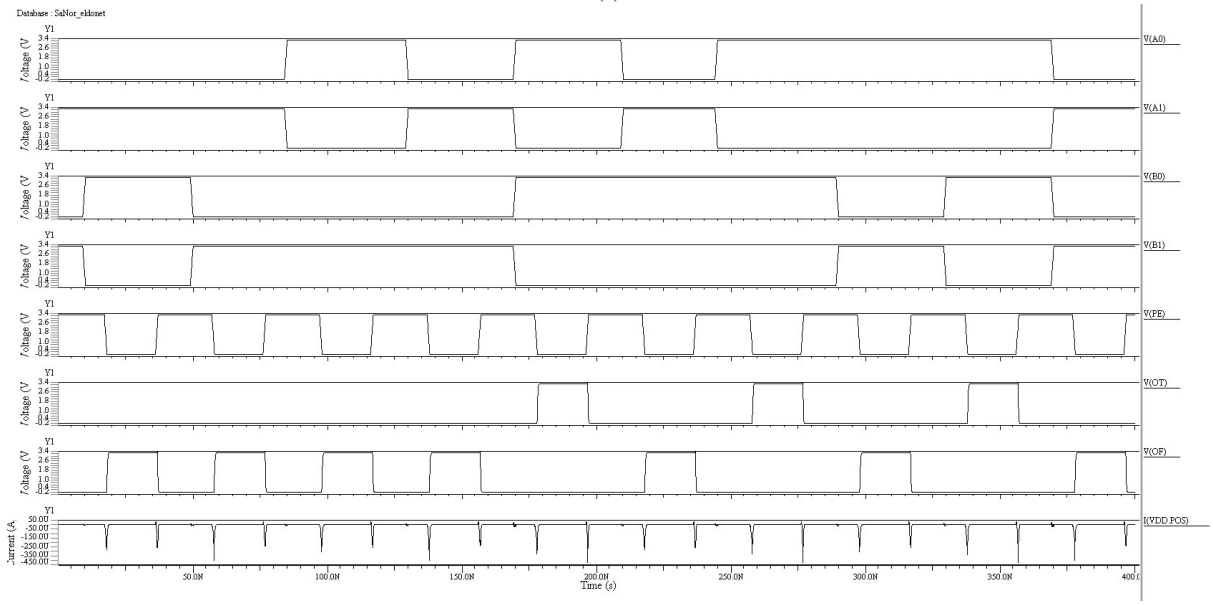
The first column shows actual input signal transitions. Second column gives energy, i.e. integral of power in time, during input signal change for SR AND cell.

TABLE I
WDDL GATE MISMATCHED

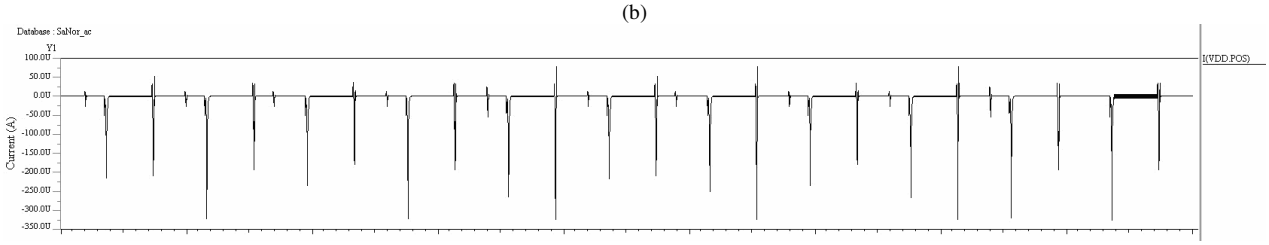
Tran A	Tran B	Single rail AND	WDDL Ct/Cf=1	WDDL ΔC=5%	WDDL ΔC=15%
0	0->1	4.60E-14	-1.0233E-12	1.81%	5.43%
0	1->0	-4.83E-14	-1.0108E-12	1.87%	5.60%
0->1	0	4.80E-14	-9.6789E-13	1.86%	5.58%
1->0	0	-5.38E-14	-1.0021E-12	1.88%	5.64%
0->1	0->1	-2.14E-13	-1.0772E-12	1.69%	4.88%
1->0	1	-4.50E-13	-1.0352E-12	1.78%	5.37%
0->1	1	-2.51E-13	-1.0613E-12	1.71%	5.07%
1	1->0	-4.94E-13	-9.7665E-13	1.85%	5.54%
1	0->1	-2.56E-13	-1.0693E-12	1.70%	4.91%
1->0	1->0	-5.16E-13	-1.0101E-12	1.83%	5.63%



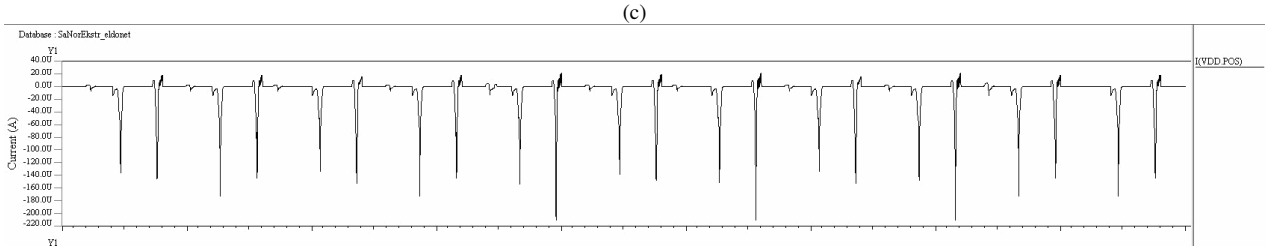
(a)



(b)



(c)



(d)

Fig. 4. Waveform of I_{DD} for (a) single-real AND gate; (b) WDDL AND gate with balanced load, (c) WDDL AND attacked with V_{DD}=2.4 V, (d) WDDL AND attacked with V_{DD}=4.2 V.

The subsequent column represents the energy used by WDDL AND cell. Obviously, the energy is increased especially (two orders of values) for combinations that produce neutral output change for simple AND cell. Even for cases when an event occur on SR AND, the WDDL AND cell needs ten times higher energy. This is an outcome of double transitions (to low-high and high-low).

Third column presents relative difference in required energy in respect to the nominal, balanced load for every input signal combination when mismatched load capacitances for 5%.

The last column shows case when imbalance was raised to 15%.

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%.

V. WDDL RESISTIVITY TO V_{DD} FAULTS

As another example we consider influences of faults entered by attacker to resistivity of WDDL AND gate. Actually, observing circuit behavior under intentionally caused faults can help attackers to discover the secret code. Potential attackers are able to increase or decrease V_{DD} over/under the standard limits. Such attacks are simulated in case when V_{DD} was decreased from nominal 3.3 V to 2.4 V. Thereafter the case when V_{DD} is increased to 4.2 V is simulated, as well.

The obtained waveforms of I_{DD} are presented in Fig. 4c and Fig. 4d respectively. Although I_{DD} for balanced load could not be presented in this paper in the same scale as these two, the differences are obvious.

In addition, results are summarized in Table II.

Similarly to Table I, the first column indicates input vector signal. Results obtained for WDDL AND cell with balanced load biased for nominal V_{DD}=3.3 V are shown in the second column. Thereafter results obtained for V_{DD-}=2.4 V and V_{DD+}=4.2 V are listed respectively in columns three and four.

Last three rows present average value of energy, maximum, minimum values and relative difference between extreme values. The last parameter illustrates observability of different input sequence through I_{DD}. Larger δ corresponds to higher correlation between circuit behavior and consumed power.

One may observe that ratio of average values of energy in columns 2 and 3 E_{WDDL24}/E_{WDDL33}= 0.37, are not proportional to ratio V_{DD-}/V_{DD} = 0.72 that could be expected. Therefore it is not caused only by lower voltage bat by decrease of I_{DD} and decreased time needed to accomplish transition from low to high level and reverse.

Similarly, for case when voltage was increased to 4.2 V (V_{DD+}/V_{DD} = 1.27) the energy was increased for factor 5.42 (E_{WDDL24}/E_{WDDL33}= 5.42). This is caused by increased current but also with increased time needed to charge/discharge load and parasitic capacitances.

Although differences in energy are more than five times greater, the waveform shape hides IDD changes much better. This confirms parameter d that is more than two times smaller.

TABLE II
WDDL GATE UNDER V_{DD} ATTACKS

Tran A	Tran B	E_{WDDL}[Ws] @ V_{DD}=3.3V	E_{WDDL}[Ws] @ V_{DD}=2.4V	E_{WDDL}[Ws] @ V_{DD}=4.2V
0	0->1	-1.0233E-12	-3.94E-13	-5.52E-12
0	1->0	-1.0108E-12	-3.81E-13	-5.50E-12
0->1	0	-9.6789E-13	-3.60E-13	-5.40E-12
1->0	0	-1.0021E-12	-3.77E-13	-5.49E-12
0->1	0->1	-1.0772E-12	-3.97E-13	-5.65E-12
1->0	1	-1.0352E-12	-3.96E-13	-5.54E-12
0->1	1	-1.0613E-12	-3.94E-13	-5.62E-12
1	1->0	-9.7665E-13	-3.67E-13	-5.45E-12
1	0->1	-1.0693E-12	-3.97E-13	-5.61E-12
1->0	1->0	-1.0101E-12	-3.79E-13	-5.50E-12
average		-1.02E-12	-3.84E-13	-5.53E-12
Max		-1.08E-12	-3.97E-13	-5.65E-12
Min		-9.68E-13	-3.60E-13	-5.40E-12
δ [%]		11.29	10.28	4.63

VI. CONCLUSION

This paper presented some of countermeasures against SCA. In particular WDDL topology was examined in scope of resistivity to power analysis based SCA.

The results obtained for ideally matched outputs were compared to two 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 the best complementary matching of power signature at 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 V_{DD}, higher temperature, quicker/slower excitation. As example, results obtained for extreme V_{DD} values were reported as well. They showed that timing effects related to faster or slower capacitor charging have remarkable effect on SCA possibilities.

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

[2] Jean-Jacques Quisquater, Side channel attacks State-of-the-Art, Report, Oct. 2002. [Online]. Available: 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, Banja Luka, June, 2009, pp. 30–36.

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

[5] Rajesh Velegalati, "Securing Light Weight Cryptographic Implementations on FPGAs Using Dual Rail with Pre-Charge Logic," PhD Thesis, George Mason University, Fairfax, VA, 2009. [Online]. Available: http://digilib.gmu.edu:8080/bitstream/1920/5623/1/Velegalati_Rajesh.pdf [Accessed on March 2010].

[6] Danil Sokolov, Julian Murphy, Alexander Bystrov, and Alex Yakovlev, "Design and Analysis of Dual-Rail Circuits for Security Applications," IEEE Transactions on Computers, 54(4):449–460, 2005. ISSN 0018-9340.

[7] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, Tarik Graba, Jean-Luc Danger, "WDDL is Protected Against Setup Time Violation Attacks," HAL–CCSD, hal-00410135, version 1–17, Aug. 2009.

[8] Sylvain Guilley, Sumanta Chaudhuri, Laurent Sauvage, Tarik Graba, Jean-Luc Danger, Philippe Hoogvorst, Vinh-Nga Vong, Maxime Nassar, Florent Flament, "Shall we trust WDDL?," in Future of Trust in Computing, Berlin, Germany (2008), pp. 1–8, DOI : 10.1007/978-3-8348-9324-6_22.