Evaluation on FPGA of Triple Rail Logic Robustness against DPA and DEMA

Victor Lomné, Philippe Maurine,
Lionel Torres, Michel Robert
LIRMM, UMR 5506,
University Montpellier 2, CNRS
161, rue Ada, 34392 Montpellier, France
Email: {firstname.lastname}@lirmm.fr

Rafael Soares, Ney Calazans
Pontifícia Universidade
Católica do Rio Grande do Sul
Faculdade de Informática, FACIN, PUCRS
Av. Ipiranga, 6681, 90619-900 Porto Allegre, Brazil
Email: {rsoares,calazans}@inf.pucrs.br

***Abstract*—Side channel attacks are known to be efficient techniques to retrieve secret data. In this context, this paper concerns the evaluation of the robustness of triple rail logic against power and electromagnetic analyses on FPGA devices. More precisely, it aims at demonstrating that the basic concepts behind triple rail logic are valid and may provide interesting design guidelines to get DPA resistant circuits which are also more robust against DEMA.**

***Index Terms*—DPA, CPA, DEMA Logic Style, DES, FPGA, Side-Channel Attacks.**

I. Introduction

In the last century, modern cryptology has mainly focused on defining cryptosystems resistant against logical attacks. But lately, with the increasing use of secure embedded systems, researchers focused on the correlation between data processed by cryptographic devices and their physical leakages. As a result, new, efficient side-channel attacks exploiting these physical leakages have appeared such as DPA [1] (Differential Power Analysis) and DEMA (Differential Electro-Magnetic Analysis).

Several countermeasures against power analyses have been proposed in former works [2][3][4][5][6][7]. Most of these aim at hiding or masking the correlation between processed data and physical leakages, by adding, for example, random power consumption.

In this context, self-timed circuits seem an interesting alternative, since it is more difficult to correlate the leaking syndromes to the data flowing in a secure design in the absence of a global synchronization signal [4][8].

Among all available asynchronous circuit families, QDI (Quasi-Delay Insensitive) circuits offer another main advantage, namely the return to zero dual rail encoding used to encode logic values [9][10]. Also, a single rising transition on one of the two wires generates an invalid code, which has no logical meaning. Consequently, the transmission of a valid logic one or zero always requires switching exactly one wire to VDD. The differential power signature of QDI circuits may therefore be strongly reduced, provided the use of perfectly balanced cells.

Several implantations of robust dual rail cells are available in the literature [5][6][7][10][11][12]. Most of these have been proposed to design robust ASIC, and a few works were dedicated to mapping of secure dual rail logic on FPGA [13].

Among all these works, an investigation of the effective robustness against DPA of dual rail logic has been introduced in [5][14][15]. These evaluations demonstrated that the load imbalances introduced during place and route steps significantly reduce the robustness against DPA of dual rail logic. More precisely, the authors of [5] identified the potential mismatches of data propagation delays through different data paths as the main remaining weakness of dual rail logic against DPA. As a result, they suggested in [5] the use of an additional third wire to simultaneously balance the power consumption and the timing, thus obtaining quasi-data independent power consumption and computation time logic.

The scope of this paper is to investigate the efficiency of triple rail logic against DPA and DEMA. To the authors knowledge, this is the first report on concrete results about the robustness of redundant logic against DEMA.

The experiments described here were achieved by implementing a sensitive block of the DES algorithm on FPGA using both dual rail and triple rail data encoding. Next, the robustness against power and electromagnetic analyses of the prototypes were computed.

The remainder of this paper is organized as follows. Section 2 presents secure triple rail logic and its concepts. Section 3 introduces the hard macros developed to efficiently map triple rail logic on FPGAs. Section 4 introduces the power and electromagnetic analysis platform used to evaluate the robustness of triple rail logic against DPA and DEMA. Experimental results are given section 5, and conclusions are drawn in Section 6.

II. Secure Triple Track Logic Concepts

Dual rail logic has been identified as an interesting countermeasure against DPA in several works [5][6][7][10][11][12][14] since its associated dual rail encoding theoretically allows reducing the correlation between the processed data and power consumption. However, this claim holds if and only if some conditions are fulfilled [5]. As highlighted in [5], these conditions are related to the impact of the place and route steps on both the switching currents and

978-3-9810801-5-5/DATE09 © 2009 EDAA

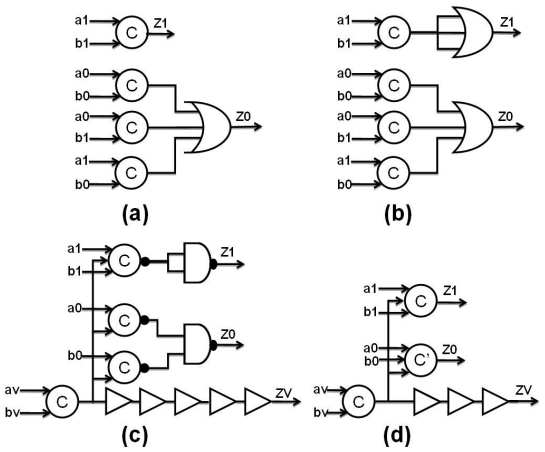

Fig. 1. And2 gate asynchronous implementations: (a) basic dual rail And2 (b) more secure dual rail And2 (c) triple rail And2 (d) compact triple rail And2. C stand for a C-element and C´ for a generalized C-element ($Z = (a+b).c + Z^{-1}.(a+b+c)$).

the timings of dual rail designs. Indeed, performing automatic place and route, either in ASIC or programmable logic devices, may result in undesirable routing capacitances unbalancing both the timing and the switching current profiles of dual rail gates and blocks. Place and route are thus extremely critical steps of the design flow of secure dual rail designs [14][15].

To eliminate this remaining dual rail weakness against DPA, authors in [5] suggested the use of an additional third wire indicating whenever the output data is stable (and thus valid) or not, as Figure 1 shows. Figure 1 displays gate level representations of a dual rail ((a) and (b)) and triple rail ((c) and (d)) And2 gate. In this Figure, implementations (b), (c) and (d) are power balanced. However, the third rail in (c) and (d) must fulfil a timing constraint, to effectively obtain a quasi data independent timing behaviour at block level.

The validity output pin ZV of triple rail gates is controlled by buffers, three in the case of Figure 1(d). These buffers ensure that the propagation delay Θv from the validity inputs (av, bv) to the output ZV remains greater than the delays Θd from ($a1$, $a0$, $b1$, $b0$) inputs to the data outputs ($Z0$, $Z1$). Note that the number of buffers must be defined by designers to guarantee that this timing characteristic is satisfied even in presence of output load mismatches introduced by the place and route step as described in [5][15]. With such design guidelines of triple rail gates, one may warrant with a high level of confidence, that the time at which a triple rail gate fires is independent of the specific data processed by its containing block.

Figure 2 illustrates this key characteristic of secure triple rail logic. After the firings of av, bv, cv and dv (assumed to occur at the same time without loss of generality), $e0$, $e1$, $f0$, $f1$ fire first. Then, the firing of ev and fv occur, which in turn triggers $g0$ or $g1$, followed by gv, since validity rails have a greater propagation delay. Thus the firing of triple rail gates is triggered by the validity rails characterized by a switching speed lower than that of data rails. In other words, the validity

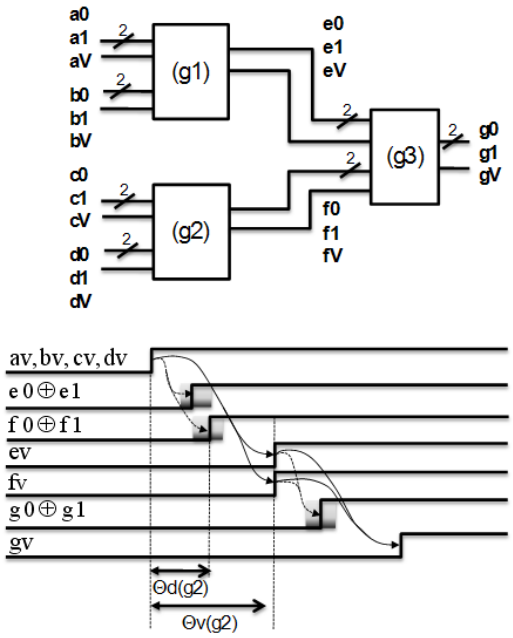

Fig. 2. The basic operation of secure triple rail logic.

rail array (arrows in Figure 2) operates as a backbone of the logical block, sequencing the events independently of the data processing (dashed arrows in Figure 2).

Note that during the firing sequence, the time at which $e0$ ($f0$, $g0$) and $e1$ ($f1$, $g1$) settle may be different, due to possible output load mismatches. This is represented by the greyed rectangles on Figure 2. However, these arrival time mismatches do not affect the firing of the following gates, which are triggered by the validity rails. This characteristic avoids the effect of load mismatches piling up on the timing along data paths. This warrants quasi data independent power consumption and computation time at the block level.

III. Implementation on FPGA

The first step to map secure triple rail logic to FPGAs is to design specific hard macros implementing basic triple rail gates such as the triple rail And2 gate represented in Figure 1. A possible solution to realize an And2 gate on FPGA is to integrate it in a hard macro with the functionality represented either in Figure 1(c) or Figure 1(d).

FPGA hard macros are hardware functions created from basic FPGA components (e.g. LUTs, wires and flip-flops) from a specific device of some FPGA family. In Xilinx FPGAs, these macros can be generated from scratch through the graphic layout editor of the FPGA editor environment. Once designed, hard macros can be instantiated in HDL source code as any other design component. The manual hard macro design process allows that specific wire delays be verified and/or changed, although this is done indirectly. In general, the instantiation of hard macros guarantees that all instances of a module present identical and predictable delay characteristics.

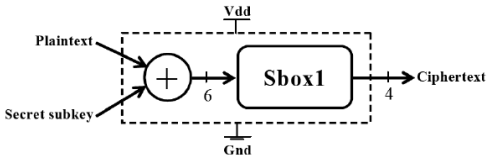

Fig. 3. Sub-module of DES Cipher function.

This allows implementing asynchronous circuits on FPGA as demonstrated for example by Pontes et al. in [16].

Triple rail gates are composed by C-Elements, and generalized C-elements (C´ in Figure 1(d)), to avoid propagating hazards to the outputs. Note that when realizing these macros the true and false data paths must be designed to have the same logical depth, to obtain a quasi independent power consumption and computation time at cell level. This explains the additional And2 (resp. Or3) gate on the true path in Figure 1(c) (resp. Figure 1(b)).

As Figure 1(c) and 1(d) show, the logic delivering the secure triple rail And2 validity signal ZV is implemented by an independent logic, characterized by a greater propagation delay. To realize it on an FPGA, we also implemented an independent logic. More precisely, the propagation of the validity signal is slowed down by forcing it to pass through three cascaded LUTs (in the case of Figure 1(d)). This allows implementing a quasi independent timing logic for the validity signal, having a constant and greater propagation delay than propagation delays of the true and false data paths, respectively.

Following these design guidelines, the mapping of a secure triple rail And2 can be realized with 11 LUTs (6 slices) using only basic C-elements as shown Figure 1(c), or realized with 6 LUTs using basic and generalized C-elements as in Figure 1(d). An exception to this is the Xor2 STTL gate, which does not allow improvement. This is implemented only as in Figure 1(c).

IV. Experimentation

In order to evaluate the robustness of secure triple rail logic against DPA, we implemented a sensitive sub-module of a cryptographic algorithm. The Data Encryption Standard was chosen because it is a well-known symmetric cryptosystem, and most of studies on side-channel attacks refer to it. Only a sub-module of the DES Cipher Function has been implemented for this study.

A. DES sub-module characteristics

This sub-module takes the first 6-bit block among 48 expansion function output bits, and idem with first round Key. Then, blocks are bit-by-bit added modulo 2, and the resulting 6-bit block is submitted to the Sbox1 module, which yields to a 4-bit block as output. A sketch of this architecture appears in Figure 3. This is sufficient to apply DPA attacks. The algorithm was implemented in single rail logic (SR), in dual rail logic (as shown Figure 1(a), (b)), and secure triple rail logic using C-elements only (Figure 1(c)) and generalized C-elements (Figure 1(d)). Note that the sub-module was implemented in single rail logic and basic dual rail logic (Figure 1(a)), to validate the power and electromagnetic analysis flow, but also to obtain trustable references while evaluating the robustness against power and electromagnetic analyses of secure triple rail logic.

TABLE I
Prototype characteristics

	single rail	dual rail Fig.1a	dual rail Fig.1b	triple rail Fig.1c	triple rail Fig.1d
Min (ns)	15.6	48.1	55.9	103	81.7
Max (ns)	26.6	58.5	61.7	103	81.7
Avg (ns)	22.2	53.5	58.9	103	81.7
Diff (ns)	10.9	10.4	5.8	0	0
Slices	175	490	490	966	501
Area (%)	9%	25%	25%	50%	26%

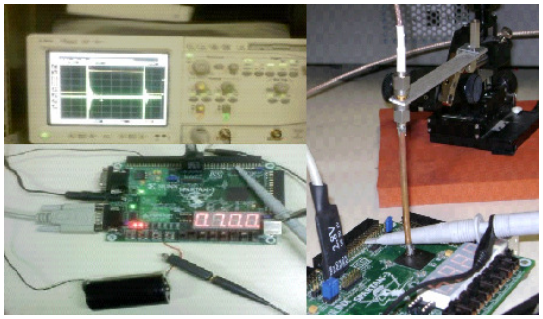

Fig. 4. STTL robustness measurement setup.

Table 1 gives the area required to implement SR, dual rail and secure triple rail sub-modules on FPGA. It also gives results of timing analysis considering all possible input transitions and all possible values of the sub-key.

These results demonstrate that the computation time of both secure triple rail sub-modules are, as expected, rigorously constant. Note however, that the computation time is roughly 3.8 to 5 times greater than the one obtained for the SR mapping. This is the price to pay for a quasi independent computation time. The independent validation logic implemented on FPGA explains this result. Note also that using generalized C-elements, the area required to map dual rail and triple rail is nearly the same.

B. Measurement setup

To validate the secure triple rail concepts, i.e. to evaluate the robustness against power and electromagnetic analyses of our prototypes, we used the measurement setup illustrated in Figure 4 which is composed by 6 elements:

- A Xilinx Spartan3 board, (the core voltage regulator has been disconnected to supply the core with a less noisy battery).
- A current probe with a bandwidth of 1GHz, to measure the instantaneous FPGA core switching current.

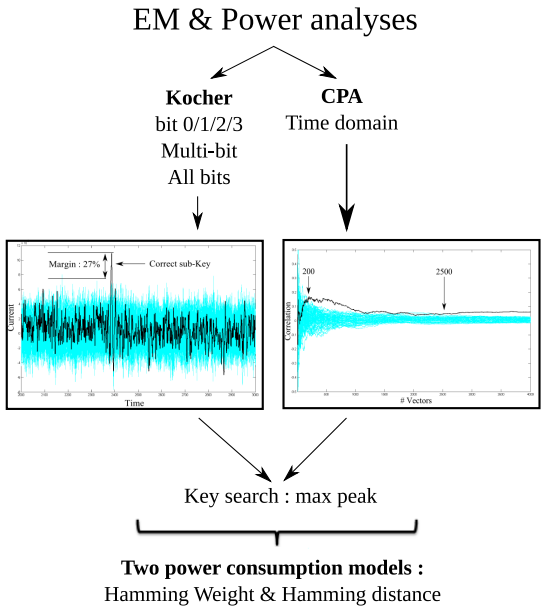

Fig. 5. Overview of the applied power and electromagnetic analysis flow.

- An 4GS/s oscilloscope, to sample the switching current.
- A PC to control the whole measurement setup, i.e. provide data to the sub-module through an on chip RS232 module and store the measured power traces.
- A hand-made 1mm passive magnetic probe.
- A low noise 63db amplifier.

C. Performed power and electromagnetic analyses

In order to perform power and electromagnetic analyses, we first collected power curves on the single rail, dual rail and secure triple rail mappings.

More precisely, we collected one power curve for all possible data transitions at the input of the sub-module. To reduce the noise and increase the Signal to Noise Ratio, each transition was applied 50 times to obtain, for each ciphering, an averaged power trace. The data collection step achieved, we ran several power and electromagnetic (EM) analyses based on two different power consumption and EM models: the Hamming-Weight and the Hamming-Distance models.

We first performed some differential power and EM analyses considering different selection functions. For these attacks, we used the selection function introduced by Kocher [1]. More precisely, we performed four different analyses targeting each one output bit of the Sbox1.

We then performed multi-bit differential analyses; i.e., we sorted the power traces according to the value of 2 output bits rather than 1. All power traces forcing respectively those two bits to the value 11 and 00 were gathered in the sets of power traces $V1$ and $V0$; all others power traces were discarded.

We then used two variants of the Kocher selection function. These variants consist in considering respectively the Hamming Weight (HW) or the Hamming Distance (HD) of the four output bits of the Sbox1. More precisely, we defined two sets of power traces according to the value of the HW or HD rather than to the value of one output bit.

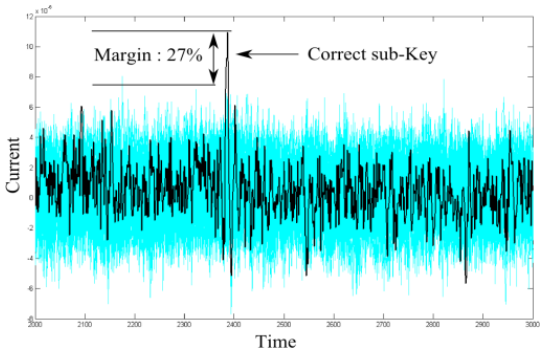

Fig. 6. Differential Power Analysis traces obtained for the SR DES sub-module (sub-key 10).

Finally, we performed Correlation Power and EM analyses based on the HW and on the HD respectively. These analyses were performed in the time domain, i.e. one correlation value (between the instantaneous value of the current and either the HD or HW) was computed for each sample of the power traces.

As illustrated Figs. 6 and 7 all the above power and EM analyses provided, in our case, 64 evolutions (one for each possible guess) of a quantity (a difference of current or magnetic field or correlation) versus time. Usually, the secret key corresponds (theoretically) to the guess resulting to the curve having the greatest amplitude.

V. Results and Analysis

Even if theoretically, the guess corresponding to the secret key is characterized by the highest amplitude, a margin should be considered in practice to warrant a high level of confidence when concluding about the successfulness of a power or EM analysis.

Note that we defined this margin as the minimal relative difference between the amplitude of the differential trace obtained for the right key, and the amplitude obtained for wrong guesses. We considered that an analysis was successful if the resulting margin was greater than 10%.

A. First experiment

All the power and EM analyses described in the preceding section were first applied on the single rail DES sub-module in order to validate our power and EM analysis flow. The analyses were done using an input sequence of 4033 different vectors. This sequence was defined in order to obtain the average power and EM traces for all possible 6-bit input transitions. For each considered sub-key value, most differential power and EM analyses were successful. Note however that the margin obtained for power analyses ranges between 10% and 30%, while for EM analyses it ranges between 16% and 52%.

Moreover, during the analyses, we observed that the Hamming distance model gives, as expected, higher margins than the Hamming Weight model.

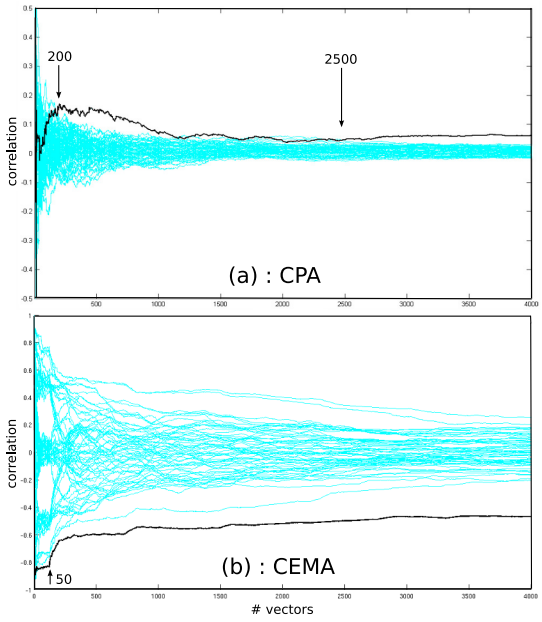

Fig. 7. CPA (a) and CEMA (b) traces obtained for the SR DES sub-module (sub-key 10).

TABLE II
PERCENTAGE OF CORRECT GUESSES OF THE SUB-KEY

Single Rail sub-module	70%
Dual Rail sub-module (Fig. 1a)	90%
Dual Rail sub-module (Fig. 1b)	3%
Triple Rail sub-module (Fig. 1c)	5%
Triple Rail sub-module (Fig. 1d)	1.5%

As an illustration, Figure 6 gives the differential power analysis traces obtained for the sub-key 10, while Figure 7 represents the evolution of the correlation coefficient with respect to the number of input vectors used to perform the CPA (a) and CEMA (b). Here, 200 and 50 inputs are sufficient to reveal the secret sub-key using respectively CPA and CEMA, even if the statistical convergence is not fully reached.

B. Second experiment

In a second experiment, we applied all power analyses described in Section 4 on the dual rail and triple rail DES sub-modules. This experiment was done to demonstrate the robustness of secure triple rail logic against DPA/CPA (secure triple rail logic has been introduced in [5] as a DPA countermeasure). More precisely, 17 different power analyses were performed for all possible values of the sub-key. Table 2 reports the percentage of right guesses, i.e. the number of sub-keys disclosed after performing the 17 power analyses on each power curve set.

Triple rail logic appears more robust against DPA/CPA than basic dual rail logic and single rail logic. Note, that several secure dual rail logic styles have been introduced in the literature [3][5][6][7][14][15]. Since it was impossible to evaluate all of them (12 minutes are necessary to collect the power curves for one sub-key value, and 15 minutes are necessary to perform the 17 power analyses), we evaluate the dual rail logic from Figures 1(a) and (b). Of course, other secure dual rail logics might be more robust than the considered dual rail logics. However, this increase in robustness is obtained at the cost of area overhead which can be important if specific routing is applied [14][17].

TABLE III
PERCENTAGE OF CORRECT GUESSES OF THE SUB-KEY

Single Rail sub-module	99%
Dual Rail sub-module (Fig. 1b)	31%
Triple Rail sub-module (Fig. 1d)	9%

As a conclusion, we may state that the triple rail prototypes are at least 14 and 18 times more robust than basic single rail and basic dual rail. One key point here is that this robustness is achieved without balancing the output loads on the true and false paths, thanks to the third rail that avoids the effects of routing capacitance mismatch pile up on both timing and power consumption. However, the price to be paid is a lower speed.

C. Third experiment

The third experiment performed aimed at evaluating the robustness of secure triple rail logic against electromagnetic analysis. During this experiment, the probe was placed, above the FPGA, at the place where the signal was found stronger. The EM curves of single rail, dual rail (Figure 1(b)) and triple rail (Figure 1(d)) prototypes were collected for different values of the sub-key using the EM platform described in Section 4.b. 17 different EM analyses were run for each considered value of the sub-key. The obtained results are given in Table 3.

From this it is possible to conclude that dual rail and triple rail logics seem more resistant to EM analyses than single rail logic. It also appears that triple rail logic is more resistant than dual rail logic. In the authors opinion, the quasi data independent timing behaviour of triple rail logic explains its increased resistance against EM. Indeed, simultaneously balancing the switching current and timing theoretically allows to balancing the magnetic field, which is proportional to di/dt, radiated by the whole chip.

However, this block level balancing act does not warrant that all points of the chip radiate the same magnetic field, since the cell placement and the power/ground routing is unconstrained. This explains the remaining weakness of dual rail and triple rail logic against DEMA and CEMA. Thus, effort must be done to properly place cells (i.e. distribute the activity) and route the supply and ground rails (which are the main source of magnetic emissions [17]) in order to reduce and balance the electromagnetic emissions.

VI. CONCLUSION

In this paper, an experimental evaluation of triple rail logic robustness against DPA and DEMA has been introduced. This evaluation has been done on FPGAs using hard macros and

standard place and route algorithms. The results obtained demonstrate: (a) that secure triple rail logic is definitively more robust against DPA/CPA than single rail logic and slightly more robust than dual rail logic, (b) that the mapping on FPGA of dual rail and triple rail logic occupies the same die area and (c) that triple rail logic, while more resistant than single rail and dual rail logic is not fully robust against DEMA/CEMA.

This latter result suggests that further effort must be done to spatially balance, in amplitude and time, the switching current flows within the die. However, one may wonder if such a task can be successfully achieved.

ACKNOWLEDGMENT

This work was partially supported by The ANR - ICTER Project (French National Research Agency), The International "Secure Communicating Solutions" Cluster, and the CAPES/COFECUB (French-Brazilian Cooperation), this last under grant no BEX1446/07-0.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proc. 19th International Conference on Cryptology (CRYPTO)*, 1999, pp. 388–397.

[2] Z. Chen and Y. Zhou, "Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage," in *Proc. 8th Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2006, pp. 242–254.

[3] A. Bystrov, A. Yakovlev, D. Sokolov, and J. Murphy, "Design and Analysis of Dual-Rail Circuits for Security Applications," *IEEE Transactions on Computers*, vol. 54, no. 4, pp. 449–460, 2005.

[4] J. J. A. Fournier, S. W. Moore, H. Li, R. D. Mullins, and G. S. Taylor, "Security Evaluation of Asynchronous Circuits," in *Proc. 5th Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2003, pp. 137–151.

[5] A. Razafindraibe, M. Robert, and P. Maurine, "Improvement of dual rail logic as a countermeasure against DPA," in *Proc. International Conference on Very Large Scale Integration (VLSI-SoC)*, 2007, pp. 270–275.

[6] S. Guilley, P. Hoogvorst, Y. Mathieu, R. Pacalet, and J. Provost, "CMOS Structures Suitable for Secure Hardware," in *Proc. Design, Automation and Test in Europe Conference and Exposition (DATE)*, 2004, pp. 1414–1415.

[7] F. Mace, F. Standaert, I. Hassoune, J.-D. Legat, and J.-J. Quisquater, "A Dynamic Current Mode Logic to Counteract Power Analysis Attacks," in *Proc. 19th International Conference on Design of Circuits and Integrated Systems (DCIS)*, 2004, pp. 186–191.

[8] Z. C. Yu, S. B. Furber, and L. A. Plana, "An Investigation into the Security of Self-Timed Circuits," in *Proc. 9th International Symposium on Asynchronous Circuits and Systems (ASYNC)*, 2003, pp. 206–215.

[9] G. F. Bouesse, M. Renaudin, S. Dumont, and F. Germain, "DPA on Quasi Delay Insensitive Asynchronous Circuits: Formalization and Improvement," in *Proc. Design, Automation and Test in Europe Conference and Exposition (DATE)*, 2005, pp. 424–429.

[10] A. Razafindraibe, P. Maurine, M. Robert, F. Bouesse, B. Folco, and M. Renaudin, "Secured Structures for Secured Asynchronous QDI Circuits," in *Proc. 19th International Conference on Design of Circuits and Integrated Systems (DCIS)*, 2004, pp. 20–26.

[11] K. Tiri and I. Verbauwhede, "Securing Encryption Algorithms against DPA at the Logic level: Next Generation Smart Cards Technology," in *Proc. 5th Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2003, pp. 125–136.

[12] K. J. Kulikowski, M. Su, A. B. Smirnov, A. Taubin, M. G. Karpovsky, and D. MacDonald, "Delay Insensitive Encoding and Power Analysis: A Balancing Act," in *Proc. 11th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC)*, 2005, pp. 116–125.

[13] F. X. Standaert, S. B. Ors, and B. Preneel, "Power Analysis of an FPGA Implementation of Rijndael: Is Pipelining a DPA Countermeasure?" in *Proc. 6th Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2004, pp. 30–44.

[14] K. Tiri and I. Verbauwhede, "A Digital Design Flow for Secure Integrated Circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, vol. 25, no. 7, pp. 1197–1208, 2006.

[15] K. Kulikowski, V. Venkataraman, Z. Wang, and A. Taubin, "Power Balanced Gates Insensitive to Routing Capacitance Mismatch," in *Proc. Design, Automation and Test in Europe Conference and Exposition (DATE)*, 2008, pp. 1280–1285.

[16] J. J. H. Pontes, R. Soares, E. Carvalho, F. Moraes, and N. Calazans, "SCAFFI: An intrachip FPGA asynchronous interface based on hard macros." in *ICCD*, 2007, pp. 541–546.

[17] T. Ordas, M. Lisart, E. Sicard, P. Maurine, and L. Torres, "Near-Field Mapping System to Scan in Time Domain the Magnetic Emissions of Integrated Circuits," in *Proc. 18th International Workshop on Power and Timing Modeling Optimization and Simulation (PATMOS)*, 2008.