Triple Rail Logic Robustness against DPA

Victor Lomné, Thomas Ordas, Philippe Maurine, Lionel Torres, Michel Robert, Rafael Soares, Ney Calazans

TRIPLE RAIL LOGIC ROBUSTNESS AGAINST DPA

Victor Lomné, Thomas Ordas, Philippe Maurine,
Lionel Torres, Michel Robert
LIRMM, UMR 5506, Univ Montpellier 2, CNRS
161, rue Ada, 34392 Montpellier, France

{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 Alegre - Brazil

{rsoares,calazans}@inf.pucrs.br

Abstract

Side channel attacks are known to be efficient techniques to retrieve secret data. Within this context, the scope of this paper is to evaluate, on and for FPGA, the robustness of triple rail logic against power analyses. More precisely, this paper aims at demonstrating that the basic concepts on which leans this logic are valid and may provide interesting design guidelines to obtain DPA (Differential Power Analysis) resistant circuits.

INTRODUCTION

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

Numerous countermeasures against power analyses have been proposed in former works [2-4, 10, 11, 14]. Most of these aim at hiding or masking the correlation between processed data and physical leakage. One approach is to add random power consumption to mask information leakage.

Within this context, self-timed circuits are 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 the asynchronous circuit families, QDI (Quasi-Delay Insensitive) circuits is advantageous due to the return to zero dual rail encoding used to present logic values [5, 12]. Indeed, some rising transition on each of the two wires indicate that a bit is set to an invalid value which has no logical meaning. Also, the transmission of a valid logic 'one' or 'zero' always requires switching a rail to V_{DD}. The differential power signature of QDI circuits may therefore be strongly reduced, provided the use of balanced standard cell implementations.

Several implementations of robust dual rail standard cells are available in the literature [10-15]. Most of these have been proposed to design robust ASICs, even if some of the works provide the mapping of secure dual rail logic on FPGA [7].

Among these works, an investigation of the effective robustness against DPA of dual rail logic has been introduced in [10, 16]. These demonstrated that the load mismatches introduced during place and route steps significantly reduce the robustness against DPA of dual rail logic. More precisely, the authors of [10] identified potential mismatches of data propagation delays through different datapaths as the main remaining weakness of dual rail logic against DPA. These authors suggested the use of an additional third wire to simultaneously balance the power consumption and the circuit timing, thus obtaining quasi-data independent power consumption and computation time logic. This approach is called Secure Triple Track Logic (STTL).

The scope of this paper is to investigate the efficiency of STTL against DPA. These evaluations have been achieved by implementing a sensitive block of the DES algorithm on FPGA, using dual rail and triple rail encoding of data. The robustness against power of the different prototypes has been evaluated. Implementations of these techniques on FPGA are new in the field of reconfigurable systems research.

The remainder of this paper is organized as follows. In Section 2, the secure triple rail logic and its main concepts are briefly presented. Section 3 introduces the required FPGA hard macros developed to map efficiently STTL on FPGAs. Section 4 introduces the power analysis platform used to evaluate the robustness of triple rail logic against DPA. Experimental results are explored in Section 5. Finally, conclusions are drawn in Section 6.

SECURE TRIPLE TRACK LOGIC AND ITS CONCEPTS

Dual rail logic has been identified as an interesting countermeasure against DPA in several works [10-15], since the 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 [10].

As highlighted in [10], these conditions are related to the impact of the place and route steps on both the switching current and the timing of dual rail designs. Indeed, placing and routing, either in ASIC or programmable logic devices result in introducing undesirable routing capacitances, which unbalance both the timing and switching current profiles of dual rail gates and blocks. Place and route are thus critical steps of the design flow of secure dual rail designs [9,16].

In order to eliminate this remaining dual rail weakness against DPA, [10] suggests to use an additional wire to indicate whenever the output data is stable and thus valid or not as shown Fig.1 that gives gate level (power balanced (b,c)) representations of a dual rail and triple rail And2 gate. However, this third rail must fulfill a timing constraint to effectively obtain a quasi-data independent timing behavior at block level.

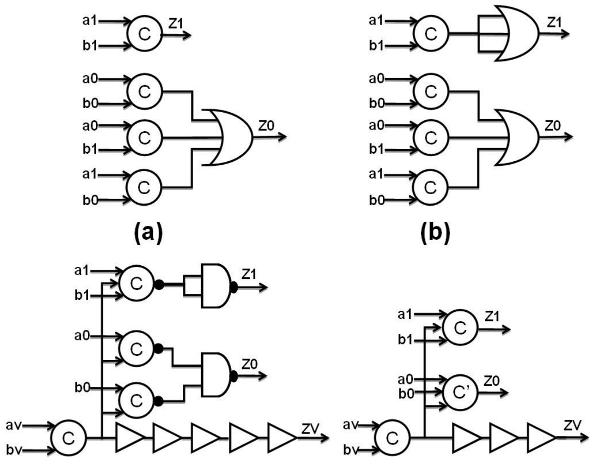

Fig. 1. Dual rail and STTL circuits: (a) basic dual rail And2; (b) more secure dual rail And2; (c) triple rail And2; (d) compact triple rail And2. Here, C stands for a C-element and C' for an asymmetrical C-element ($Z=(a+b)\cdot c + Z.(a+b+c)$).

As shown, the validity output pin *ZV* of triple rail gates is controlled by buffers, three in the case of Fig.1d. These buffers ensure that the propagation delay Θ v from the validity inputs (*av, bv*) to the output *ZV* remains greater than the delays Θ d from (*av, bv*) inputs to the data outputs (*Z0, Z1*) as shown Fig. 2. Note that the number of buffers must be defined by the 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 [10, 16]. With such design guidelines of triple rail gates, one may warrant that the time at which triple rail gate fires is independent of the data processed by the block with a high level of confidence.

Fig.2 illustrates this key characteristic of secure triple rail logic. As shown, after the firings of *av, bv, cv* and *dv* (assumed to occur at the same time without loss of generality), *e0, e1, f0 and f1* fire first. Then, the firings of *ev* and *fv* occur, which in turn triggers *g0* or *g1,* followed by *gv,* since validity rails have a larger propagation delay. Thus, the switching of triple rail gate is triggered by the validity rails, characterized by a switching speed lower than data rails. The validity rail array (arrows Fig.2) operates as a backbone of the logical block sequencing the events independently of the data processing (dashed arrows in Fig.2).

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

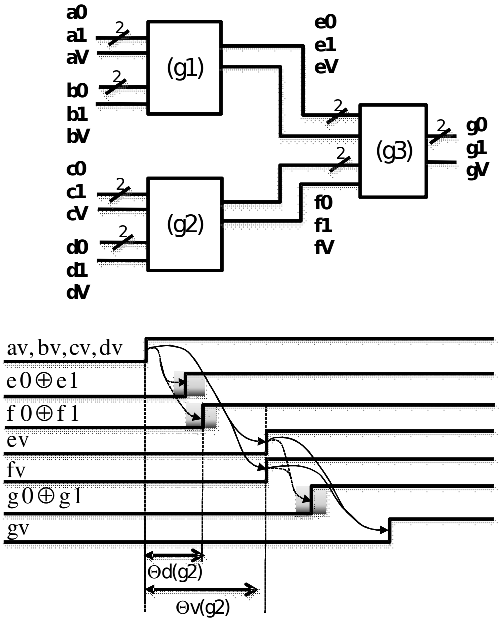

Fig. 2. Illustration of the basic operation of secure triple rail logic.

IMPLEMENTATIONS ON FPGA

The first step to map secure dual or triple rail logic concepts on FPGAs is to design hard macros implementing basic gates such as dual and triple rail And2 depicted on Fig.1. A possible solution to implement a triple rail And2 gate on FPGA is to integrate, as a hard macro, the functionality represented on Fig.1c and Fig.1d

These functionalities are composed by C-Elements (Muller gates [10]), and generalized C-elements (C' in Fig.1d), to avoid propagating hazards on the outputs. To realize these macros the true and false datapaths must be designed to have the same logical depth, in order to obtain a quasi-independent power consumption and computation time at cell level. This explains the additional or3 (nand2) gate on the true path Fig. 1b (Fig.1c).

As shown in Fig.1c and 1d, the logic delivering the secure triple rail And2 validity signal *ZV* is implemented by an independent logic characterized by a larger propagation delay. To design it for FPGAs, an independent logic has been implemented. More precisely, the propagation of the validity signal is slowed down by forcing it to pass through three cascaded Look-Up Tables (see Fig. 1d). This allows implementing a quasi-independent timing logic for the validity signal having a constant and larger propagation delay than the 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 Fig. 1c, or realized with 6 LUTs using basic and generalized C-elements as shown Fig. 1d.

EXPERIMENTATION

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

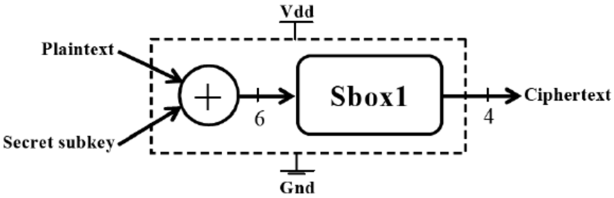

Fig.3. Sub-module of DES Cipher function.

4-a: DES sub-module characteristics

The selected sub-module takes the first 6-bits block among 48 expansion function output bits, and idem with the first round Key. Then, blocks are bit-by-bit added modulo 2, and the resulting 6-bits block is submitted to the Sbox1 which yields a 4-bit block ciphertext as output. A sketch of this calculation is given in Fig.3. This calculation is sufficient to apply DPA attacks.

This algorithm was implemented in single rail logic (SR), dual rail logic (as shown Fig. 1a, 1b), and in two versions of secure triple rail logic, using C-elements only (Fig. 1c) and generalized C-elements (Fig. 1d). Note that the sub-module was implemented in single rail logic and dual rail logic, to validate the power analysis flow, but also to obtain trustable references while evaluating the robustness against power analyses of the secure triple rail logic prototype. In none of the implementations appears any attempt to balance the false and true path loads using specific routing techniques [9].

Table 1 gives the FPGA area and timing analysis data for all implementations. Timing results in Table 1 consider all possible input transitions and all possible values of the sub-key.

Table 1: Prototype characteristics

	SR logic	Dual rail (Fig.1a)	Dual rail (Fig.1b)	Triple rail (Fig.1c)	Triple rail (Fig.1d)
Min (ns)	15.6	48.1	55.9	103.0	81.7
Max (ns)	26.6	58.5	61.7	103.0	81.7
Avg (ns)	22.2	53.5	58.9	103.0	81.7
Diff (ns)	10.9	10.4	5.8	0	0
Area (slices)	175	490	490	966	501
Area (%)	9%	25%	25%	50%	26%

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

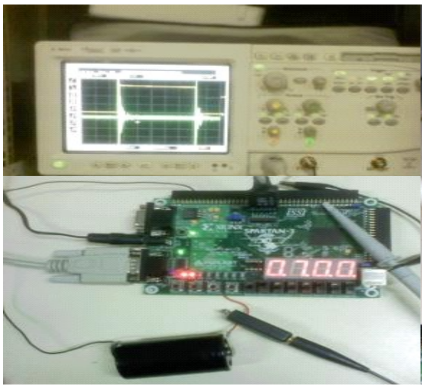

Fig.4. Measurement setup

4-b: Measurement setup

To validate the secure triple rail concepts, i.e. to evaluate the robustness against power analyses of our prototypes, we used the following measurement setup (Fig.4):

- A Xilinx Spartan3 board, where, the core voltage regulator has been disconnected to supply the core with less noisy battery.
- A differential current probe with a bandwidth of 1GHz, to measure the instantaneous switching current of the FPGA core.
- A 4GS/s oscilloscope measure the switching current.
- A PC to control the whole measurement setup, which provides data to the sub-module through an on chip RS232 module and stores the measured power traces.

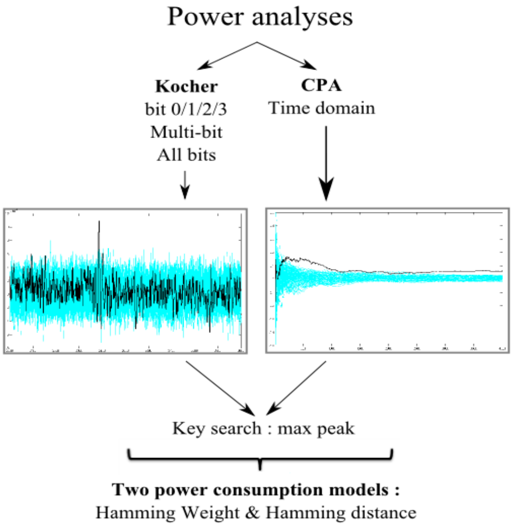

Fig.5. Overview of the applied power analysis flow.

4-c: Performed power analyses

In order to perform power analyses, we first collected power curves on the single rail, dual rail and secure triple rail mappings. More precisely we collected a power curve for each possible data transition at the input of the sub-module (64 for the dual rail and triple rail mapping and 4033 for the SR one).

To reduce the noise and increase the Signal to Noise Ratio, each transition was applied 50 times to obtain an averaged power trace for each ciphering. After completing the data collection step, we ran several analyses based on two different power consumption models: the Hamming-Weight (HW) and the Hamming-Distance (HD).

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

We then performed multi-bit differential analyses, i.e. we sorted the power traces according to the value of two (or three or four) output bits rather than 1. All power traces forcing those two (or three or four) bits respectively to the value ‘11’ and ‘00’ were thus gathered in the sets of power traces V1 and V0, all other power traces being discarded.

We then used two variants of the Kocher selection function. These variants consisted in considering respectively the Hamming Weight or the Hamming Distance 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.

Finally, we performed Correlation Power 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 analyses provide, in our case, 64 evolutions (one for each possible guess) of a quantity (a difference of current or correlation) versus time. Usually, the secret key corresponds (theoretically) to the guess resulting in the curve with the largest amplitude.

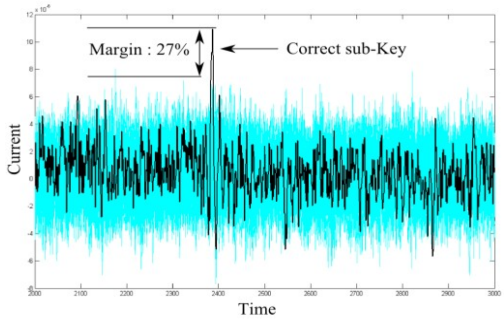

Fig.6. Differential Power Analysis traces obtained for the SR DES sub-module (sub-key 10).

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 while concluding about the successfulness of a power or EM analyses.

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%.

5-a: First experiment

All power analyses described in the previous 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 traces of all possible input transitions (6 bits). For each considered sub-key value, most differential power analyses were successful. Note that the margin obtained for power analyses were ranging between 10% and 30%.

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

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

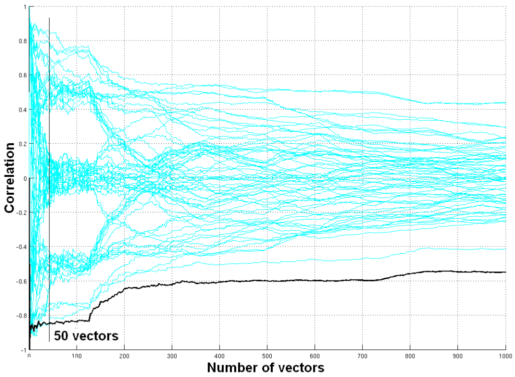

Fig.7. CPA traces obtained for the SR DES sub-module (sub-key 10)

5-b: Second experiment

In a second experiment, we applied all power analyses described Section 4, on the dual rail and triple rail DES sub-modules. This experiment was done in order to demonstrate the robustness of secure triple rail logic against DPA/CPA (secure triple rail logic has been introduced in [10] as a DPA countermeasure). More precisely, all 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 the power analyses.

Table 2: 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 shown, triple rail logic is more robust against DPA/CPA than dual rail logic and single rail logic. Note, that several secure dual rail logics have been introduced in the literature [3,9,10,11,14,16]. 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 all the power analyses), we evaluate the dual rail logic (Fig.1a,b) which are, to our knowledge, characterized by the lowest area overhead with respect to single rail logic. 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 an area overhead which can be important if special routing techniques are applied [6,9].

As a conclusion, we can state that the triple rail prototypes are clearly more robust than basic single rail and dual rail logic. 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 piling up the effects of routing capacitance mismatches on both timing and power consumption. However the price to be paid is a lower speed.

CONCLUSION

In this paper, an experimental evaluation of triple rail logic robustness against DPA & CPA has been introduced. This evaluation has been done on FPGA using hard macros and standard place and route algorithms. The results obtained demonstrate that: (a) secure triple rail logic is definitively more robust against DPA/CPA than single rail logic and slightly more robust than dual rail logic while offering an additional interesting characteristic: a constant computation time, (b) the mapping on FPGA of dual rail and triple rail logic occupies approximately the same die area that dual-rail implementations, and (c) triple rail logic is a suitable logic for secure applications.

REFERENCES

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

[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),* pp. 242-254, Oct. 2006.

[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, Apr. 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),* pp. 137-151, Sept. 2003.

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

[6] T. Ordas, M. Lisart, E. Sicard, P. Maurine, L. Torres, “Near-field Mapping System to Scan in Time Domain the Magnetic Emissions of Integrated Circuits” Proceedings of the 18th International Workshop on Power and Timing Modeling Optimization and Simulation, 2008

[7] 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),* pp. 30-44, Aug. 2004.

[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)*, pp. 206–215, May. 2003.

[9] Kris Tiri, and Ingrid 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, July 2006.

[10] A. Razafindraibe, M. Robert, P. Maurine “Improvement of dual rail logic as a countermeasure against DPA”, IFIP International Conference on Very Large Scale Integration, 2007. VLSI-SoC 2007, pp. 270-275, Oct. 2007.

[11] 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)*, pp. 1414–1415, Feb. 2004.

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

[13] 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)*, pp. 125–136, Sept. 2003.

[14] 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)*, Nov. 2004.

[15] 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)*, pp. 116–125, Mar. 2005.

[16] K.J. 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), pp.1280-1286*, Mar 2008.