Secure Triple Track Logic Robustness Against Differential Power and Electromagnetic Analyses

Victor Lomné, Amine Dehbaoui, Thomas Ordas, Philippe Maurine, Lionel Torres, Michel Robert, Rafael Soares, Ney Calazans, Fernando Gehm Moraes

Secure Triple Track Logic Robustness Against Differential Power and Electromagnetic Analyses

V. Lomné[1], A. Dehbaoui[1], T. Ordas[1], P. Maurine[1], L. Torres[1], M. Robert[1], R. Soares[2], N. Calazans[2], F. Moraes[2]

[1]LIRMM, UMR 5506 , University Montpellier 2 / CNRS, Montpellier, France
[2]Pontifica Universidade Católica do Rio Grande do Sul, Faculdade de Informática - FACIN - PUCRS, Porto Alegre, Brazil
e-mail: victor.lomne@lirmm.fr

ABSTRACT

Side channel attacks (SCA) are known to be efficient techniques to retrieve secret data. In this context, this paper concerns the evaluation of the robustness of secure triple track logic (STTL) against power and electromagnetic analyses on FPGA devices. More precisely, it aims at demonstrating that the basic concepts behind STTL are valid in general and particularly for FPGAs. Also, the paper shows that this new logic may provide interesting design guidelines to get circuits that are resistant to differential power analysis (DPA) attacks which and also more robust against differential electromagnetic attacks (DEMA).

Index Terms: Side Channel Attacks, logic style, DES, FPGA.

1. 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 Differential Power Analysis (DPA) [1] and Differential Electromagnetic Analysis (DEMA) [2].

Several countermeasures against power analysis have been proposed in former works [3-5, 6-8]. 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 [5, 9].

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 [10, 11]. The protocol of this logic consists of two phases: precharge and evaluation. The precharge phase allows starting a computation from a known electrical state, for example 00. The evaluation phase consists in a transition of exactly one wire such as from encoding 00 to encoding 10 or from 00 to 01. The differential power signature of QDI circuits may therefore be strongly reduced, provided the use of perfectly balanced cells.

Several implementations of robust dual rail cells are available in the literature [6-8, 11-13]. 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 [14].

Among all these works, an investigation of the effective robustness against DPA of dual rail logic has been introduced in [15, 16, 17-23]. Tiri and Verbauwhede [15] proposed a new design flow to implement circuits resistant against DPA. Kulikowski et al. [16] presented a general method and case studies to support their proposal of a directional discharge protocol, which ensures that dual rail circuits are always fully discharged and charged in each cycle. Tiri et al. [17] were the first to propose the use of dual rail logic with precharge (DPL). They also proposed [19] the wave dynamic differential logic style (WDDL) that uses a

standard cell flow. The differential logic is generated from single-ended gates, which reduces the design complexity. Di and Yang [21] presented the Dual Spacer Dual-Rail Delay Insensitive Logic (D^3L) that uses a dynamic random selection scheme to obtain a uniform power consumption and data independent timing performance. Bucci et al. [18] show that the balance of DPL gates can be improved by adding a third phase called *systematic discharge*, executed after the evaluation phase. Rammohan et al. [23] proposed a Reduced Complementary Dynamic and Differential Logic (RCDDL) that ensures a reduced number of gates in the *uncomplimentary logic* improves security and reduces power consumption and area. Regazzoni et al. [20] have started to explore the resistance of MOS Current Mode Logic (MCML) against DPA. Guilley et al. [22] conducted studies about imbalanced layout of DPLs on FPGAs. These Authors showed the impacts on the security of DPLs caused by different place and route constraints techniques using Xilinx and Altera tools.

The evolution of proposals for increasing resistance to SCA described in the last paragraph demonstrated that the load imbalance introduced during place and route steps significantly reduce the robustness against DPA of dual rail logic. Razafindraibe et al. [6] 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, these Authors suggested the use of an additional third wire, transforming dual rail circuits in triple rail circuits, to which [6] refers as *triple track logic*. The effect of this third wire is simultaneously obtaining quasi-data independent power consumption and computation time, enabling the building of more secure circuits. The acronym suggested in [6] and adopted here includes this notion of secure circuits, i.e. secure triple track logic or STTL.

A previous publication by the Authors [24] addressed the problem of resistance of STTL to DPA attacks in FPGAs comparing single rail and STTL cryptographic modules. Another recent publication [25] introduced an amelioration of the techniques to implement STTL gates to reduce area and improve robustness. That paper also compared STTL to single rail and dual rail implementations. The scope of the current paper is to capitalize on the results reported on the two previous papers and additionally investigate the efficiency of STTL against DPA and DEMA. This paper also offers more details about the efficient implementation of STTL gates in FPGAs. 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 (with STTL). 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 STTL basic concepts. Section 3 introduces the FPGA hard macros developed to efficiently map asynchronous triple track logic on programmable devices. Section 4 introduces the power and electromagnetic analysis platform used to evaluate the robustness of triple track logic against DPA and DEMA. Experimental results are given in Section 5, and a set of conclusions are drawn in Section 6.

2. STTL BASIC CONCEPTS

Dual rail logic and STTL are examples of asynchronous design styles. The well-known synchronous hypothesis is not valid for these styles. They imply several new design constraints and assumptions, including data encoding (e.g. bundle data, dual-rail, triple-rail, 1-of-n, etc.), environment assumptions (fundamental mode, IO mode, etc.), timing models, handshake protocols, basic logic components, etc. The discussion of these topics is outside the scope of this work. However, to help understanding the STTL concepts at least the basic logic elements of this design style need to be introduced. STTL as used in this paper needs only access to well-known basic logic gates (And, Or, Xor, etc.) and the Muller C-element (or just C-element), a component well-known in the asynchronous design community but which may be unfamiliar to most synchronous designers. A C-element can be regarded as a component able to synchronize events. C-elements are asynchronous sequential components implementable with basic logic gates and feedback wires. A basic 2-input C-element behavior appears in Table I. Simply stated, a transition can only be observed at the output of the C-element if one transition occurs at each of its input.

C-elements exist in several flavors besides the simple implementation just discussed. Each of these are useful to support specific asynchronous behavior: three-input C-elements, asymmetric C-elements, generalized C-elements, etc. The discussion of these specific devices is outside the scope of this work, and can be found in asynchronous textbooks like [26].

Given the behavior of the C-element and the fact that STTL employs triple rail encoding, it is possible then to describe the basic gates of this logic. First, note that dual rail logic encodes one bit of information using two wires. STTL adds a third wire for representing this one bit in the same way plus signaling the validity of this code. Figure 1 displays gate level representations of an AND gate with two inputs (And2) in both dual rail logic (1(a) and 1(b)) and STTL (1(c) and 1(d)). In this Figure, implementations (b), (c) and (d) are power balanced. However, the third rail in (c) and (d) must fulfill a timing con-

straint, to effectively obtain a quasi data independent timing behavior at block level.

The validity output pin ZV of triple track gates is controlled by buffers, three in the case of Figure 1(d). These buffers ensure that the propagation delay Qv from the validity inputs (av, bv) to the output ZV remains greater than the delays Qd 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 the required timing characteristic is satisfied even in presence of output load mismatches introduced by the place and route step as described in [6, 16]. With such design guidelines of triple track gates, one may warrant with a high level of confidence, that the time at which a triple track gate fires is independent of the specific data processed by its containing block.

Figure 2 illustrates this key characteristic of secure triple track 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 track gates is triggered by the validity rails characterized by a switching speed lower than that of data rails. In other words, the validity rail array (arrows in Figure 2) operates as a backbone of the logical block, sequencing the events independently of the data processing (dotted arrows in Figure 2).

Table I. Truth table for a basic 2-input C-Element.

C-Element		
InA	**InB**	**S^i**
0	0	0
0	1	S^{i-1}
1	0	S^{i-1}
1	1	1

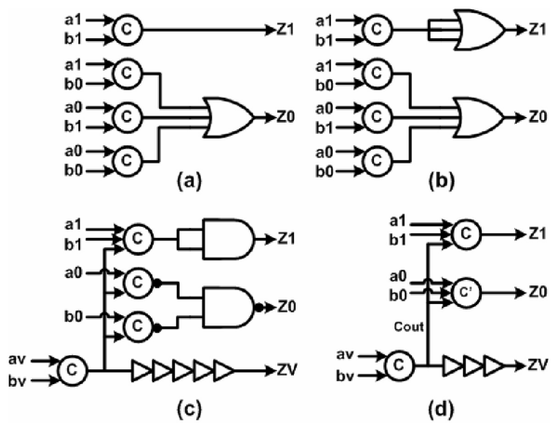

Figure 1. And2 gate asynchronous implementations:(a) basic dual rail And2 (b) more secure dual rail And2 (c) triple track And2 (d) compact triple track And2. C inside a circle represent a C-element and symbol containing a c' is a special kind of three-input C-element whose output behavior is expressed by the Boolean Equation Z0=Cout.Z0 + (Z0+Cout).(a0+b0).

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 grayed 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.

3. IMPLEMENTATION ON FPGA

The first step to map STTL to FPGAs is to design specific *hard macros* implementing basic triple track gates such as the triple track And2 gate represented in Figure 1.

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. Hard macros have previously been applied in other applications such as test for circuits [27] and reconfigurable systems [28].

Hard macros can be placed in one of several possible positions of an FPGA chip automatically by synthesis tools, or manually placed by the designer either using tools like the FPGA Editor, the Floorplanner or even a constraint text file. Once designed,

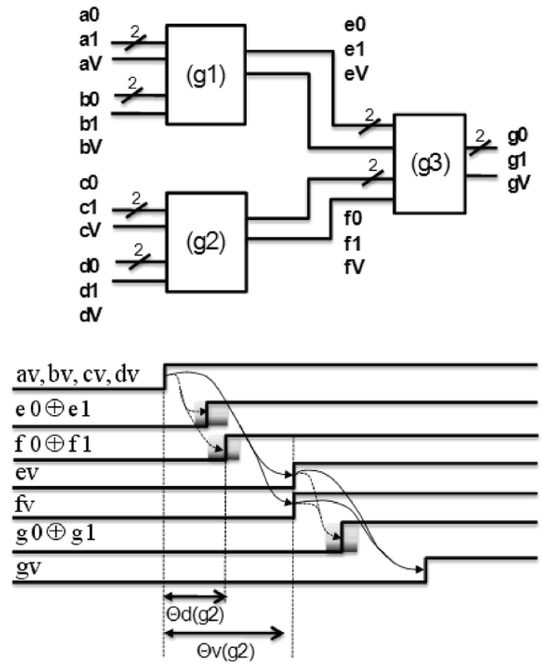

Figure 2. The basic operation of STTL gates.

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. This allows implementing asynchronous circuits on FPGA as demonstrated for example by Pontes et al. in [29]. A possible solution to realize an And2 gate on FPGA is to integrate it in a hard macro with the functionality shown in either Figure 1(c) or Figure 1(d).

Figure 3 shows an example of hard macro that implements the And2 gate represented in (Figure 1 (d)).

As Figure 1(c) and 1(d) show, the logic delivering the secure triple track And2 validity signal ZV is implemented by an independent logic, characterized by a propagation delay greater than the rest of the gate. 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 track And2 can be realized with 11 LUTs (6 slices) using the implementation of Figure 1(c), or realized with only 6 LUTs using the implementation of Figure 1(d). The scheme of Figure 1(d) can be used to implement any STTL logic gate except for the Xor2 STTL gate, which does not allow this kind of improvement and is implemented using the scheme of Figure 1(c).

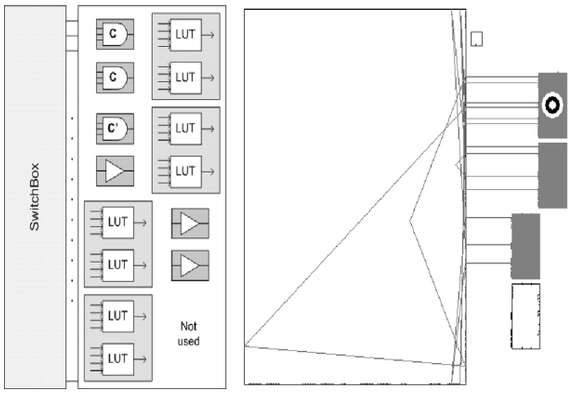

Figure 3. (a) Xilinx CLB abstract drawing composed by 4 slices and one switch box. Each slice contains 2 LUTs that implement the logic. (b) hard macro that implements an And2 gate (Figure 1 (d)). The grayed boxes represent the employed slices.

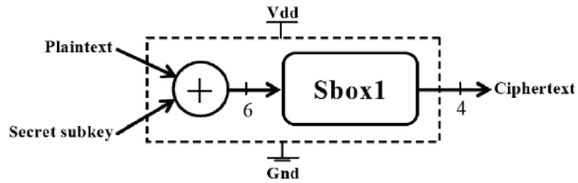

Figure 4. Sub-module of DES cipher.

4. EXPERIMENTATION

In order to evaluate the robustness of STTL against DPA, a sensitive sub-module of a cryptographic algorithm has been implemented. The Data Encryption Standard (DES) was chosen because 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 has been implemented for this study.

A. DES sub-module characteristics

A sketch of the architecture for the implemented sub-module appears in Figure 4. This sub-module takes the first 6-bit block from the 48 output bits of the DES expansion function, and the corresponding part of the first round Key. Then, blocks are bit-by-bit added modulo 2 (Xor function), and the resulting 6-bit block is submitted to the Sbox1 module, which yields a 4-bit block as output. This is sufficient to apply DPA attacks. The algorithm was implemented in five versions: single rail (SR), two dual rail versions (according to Figure 1(a), (b)), and two STTL versions (according to Figure 1(c) and Figure 1(d)). The single rail and basic dual rail (Figure 1(a)) versions validate the power and electromagnetic analysis flow. They also allow obtaining reliable references while evaluating the robustness against power and electromagnetic analyses of STTL.

Table II gives the area required to implement SR, dual rail and STTL sub-modules on FPGA. It also gives results of timing analysis, considering all possible

Table II. Prototype characteristics.

	SR logic	Dual rail Fig.1(a)	Dual rail Fig.1(b)	Triple track fig.1(c)	Triple track fig.1(d)
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
Area (slices)	175	490	490	966	501
Occupied die area	9%	25%	25%	50%	26%

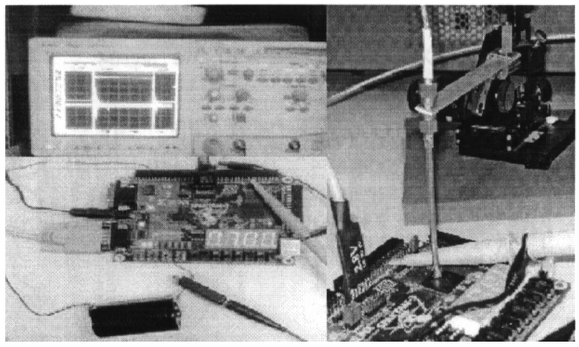

Figure 5. STTL robustness measurement setup.

input transitions and all possible values of the sub-key. The results demonstrate that the computation time of both STTL 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 on FPGA 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 track is nearly the same.

B. Measurement setup

To validate the secure triple track concepts, i.e. to evaluate the robustness against power and electromagnetic analyses of our prototypes, we used the measurement setup illustrated in Figure 5 which is composed by 6 elements:

1. A Xilinx Spartan3 board. The core voltage regulator has been disconnected to supply the core with a less noisy battery;
2. A current probe with a bandwidth of 1GHz, to measure the instantaneous FPGA core switching current;
3. An 4GS/s oscilloscope, to sample the switching current;
4. A PC to control the whole measurement setup, i.e. to provide data to the sub-module through an on chip RS232 module and store the measured power traces;
5. A hand-made 1mm passive magnetic probe;
6. A low noise 63db amplifier.

C. Performed power and electromagnetic analyses

In order to perform DPA and DEMA, we first collected power curves on the single rail, dual rail and secure triple track 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. Once finished the data collection step, we ran several power and electromagnetic (EM) analyses based on two different power consumption and EM models: the Hamming-Weight (HW) and the Hamming-Distance (HD) models. Figure 6 illustrates the employed power and electromagnetic analysis flow.

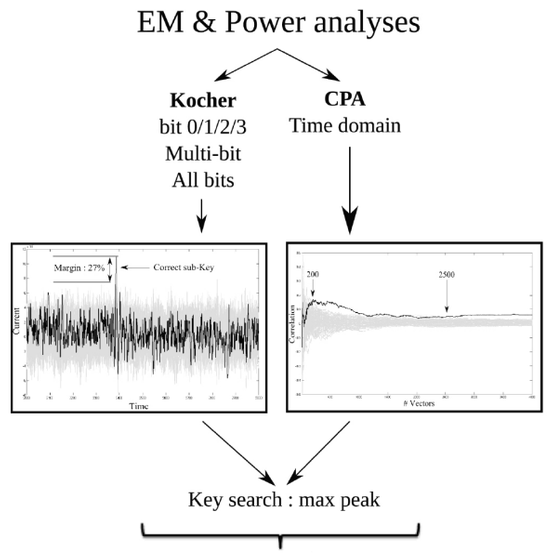

Figure 6. Overview of the applied power and EM analysis flow.

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 HW or the HD model on the four output bits of the Sbox1. Specifically, 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 Analysis (CPA) [30] and Electromagnetic Analysis (CEMA) based on HW and on HD, respectively. These analyses were performed in the time domain, i.e. one correlation value was computed for each sample of the power traces, between the instantaneous values of the current and either the HD or HW.

As illustrated in Figures 7 and 8, in our case all the above power and EM analyses provided 64 evolutions of a quantity versus time. These evolutions were one for each possible guess, and comprise a difference

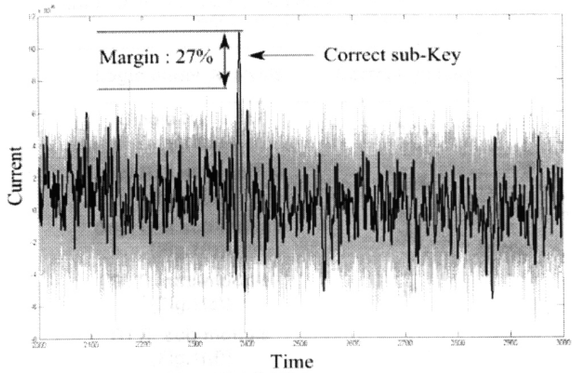

Figure 7. Differential Power Analysis traces obtained for the SR DES sub-module (sub-key 10).

of either a current value, a magnetic field value or a correlation measure. Usually, the secret key corresponds (theoretically) to the guess resulting in the curve with the greatest amplitude. 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 correct key, and the amplitude obtained for wrong guesses. We considered that an analysis was successful if the resulting margin was greater than 10%.

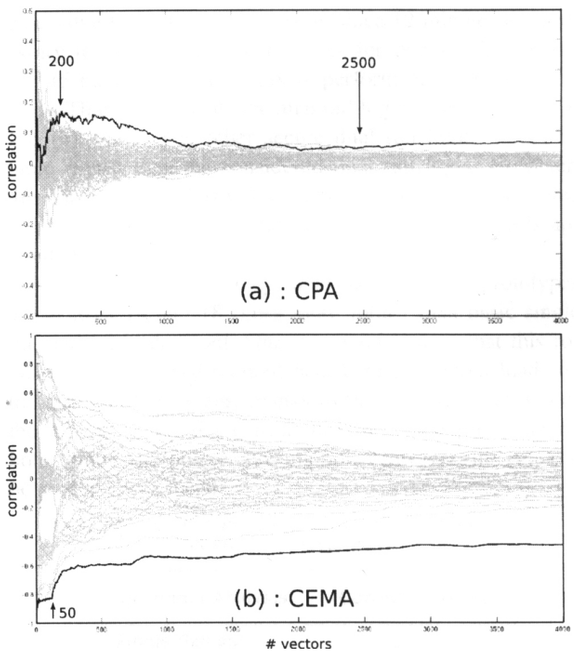

Figure 8. CPA (a) and CEMA (b) traces obtained for the SR DES sub-module (sub-key 10).

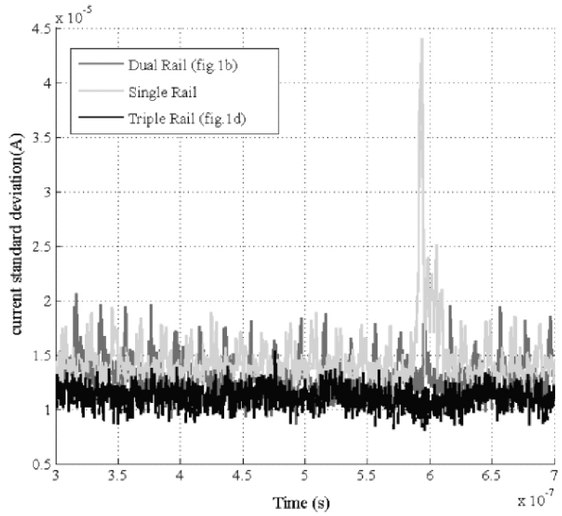

Figure 9. Measured standard deviation of the current consumed during the computation of the Sbox1.

5. RESULTS AND ANALYSIS

A. Power consumption traces

As a first evaluation of the robustness of triple track logic against simple and differential power analyses, we measured the standard deviation of the consumed current during the whole computation of the Sbox1 implemented in traditional single rail logic, dual rail logic (Fig. 1(b)) and STTL (Fig. 1(d)). Figure 9 gives the obtained results. On this Figure, one may observe that the standard deviation of both balanced dual rail logic and triple track logic is roughly 3 times lower than that of single rail logic validating the effectiveness of both dual rail and triple track logic from a current amplitude point of view.

B. First experiment

All the DPA and DEMA described in the preceding section were first applied on the single rail DES sub-module, 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 varies between 10% and 30%, while for EM analyses it varies between 16% and 52%. Moreover, during the analyses, we observed that the HD model gives, as expected, higher margins than the HW model.

As an illustration, Figure 7 gives the differential power analysis traces obtained for the sub-key 10, while Figure 8 represents the evolution of the correla-

Table III. Percentage of sub-key correct guesses on the conducted experiments.

Logic under Analysis	Correct guesses
Single Rail sub-module	70%
Dual Rail sub-module (Fig.1(a))	90%
Dual Rail sub-module (Fig.1(b))	3%
STTL sub-module (Fig.1(c))	5%
STTL sub-module (Fig.1(d))	1.5%

tion coefficient with respect to the number of input vectors used to perform the CPA [30] and CEMA. Here, 200 and 50 inputs are respectively sufficient to reveal the secret sub-key using CPA and CEMA, even if the statistical convergence is not fully reached.

C. Second experiment

In a second experiment, we applied all power analyses described in Section 4 on the dual rail and triple track DES sub-modules. This experiment demonstrates the robustness of STTL against DPA/CPA. Indeed, 17 different power analyses were performed for all possible values of the sub-key. Table III reports the percentage of right guesses, i.e. the percentage of sub-keys disclosed after performing all 17 power analyses on each curve set.

From the results, STTL appears to be 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 [4, 6-8, 15, 16]. In practice, it is unfeasible to evaluate all of them, since 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. Thus, 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 logic. However, this increase in robustness is obtained at the cost of area overhead which can be important if specific routing is applied [15, 31].

As a conclusion, we may state that the STTL 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 piling up on both timing and power consumption. However, the price to be paid is lower speed.

Table IV. Percentage of sub-key correct guesses on the conducted experiments.

Logic under Analysis	Correct guesses
Single Rail sub-module	99%
Dual Rail sub-module (Fig.1(b))	31%
STTL sub-module (Fig.1(d))	1.5%

D. Third experiment

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

From this it is possible to conclude that dual rail logic and triple track logic seem more resistant to EM analyses than single rail logic. It also appears that triple track logic is more resistant than dual rail logic.

The Authors consider that the quasi data independent timing behavior of triple track 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 guarantee that all points of the chip radiate the same magnetic field, since the cell placement and the power/ground routing are unconstrained. This explains the remaining weakness of dual rail and STTL 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 [31], in order to reduce and balance the EM emissions.

6. CONCLUSION

In this paper, an experimental evaluation of STTL robustness against DPA and DEMA has been introduced. This evaluation has been done on FPGAs using hard macros and standard place and route algorithms, which is an original approach in both FPGA applications as well as on cryptographic countermeasures. The results obtained demonstrate: (a) that STTL 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 STTL occupies the same die area; (c) that STTL, while more resistant than single rail and dual rail logic is not fully robust against DEMA/CEMA.

The later results suggest 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.

ACKNOWLEDGEMENTS

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. CNPq /PNM. The Brazilian Authors were also partially supported by the CNPq under the grants 140044/2008-6 (PNM), 309255/2008-2 and 300774/2006-0.

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] K. Gandolfi, C. Mourtel, F. Oliver, "Electromagnetic Analysis: Concrete Results," in *Proc. 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 255-265, May. 2001.

[3] 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.

[4] Bystrov, A. Yakovlev, D. Sokolov and J. Murphy, "Design and Analysis of Dual Rail Circuits for security Applications," *IEEE Transactions on Computers*, 54(4), pp. 449-460, Apr. 2005.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] K. 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.

[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.1280-1285, Mar. 2008.

[17] K. Tiri, M. Akmal, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards," *in Proc. European Solid-State Circuits Conference (ESSCIRC)*, pp. 403-406, Sept. 2002.

[18] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Pre-Charge Logic," *in Proc. 8th International Workshop Cryptographic Hardware and Embedded Systems (CHES)*, pp. 232-241, Aug. 2006.

[19] K. Tiri, and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," *in Proc. Design, Automation, and Test in Europe Conference (DATE)*, pp. 246-251, Feb. 2004.

[20] F. Regazzoni, S. Badel, T. Eisenbarth, J. Grobschadl, A. Poschmann, Z. TopraK, M. Macchetti, L. Pozzi, C. Paar, Y. Leblebici and P. Ienne, "A Simulation –Based Methodology for Evaluating DPA-Resistance of Cryptographic Functional Units with Application to CMOS and MCML Technologies," *in Proc. International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (IC-SAMOS)*, pp. 209-214, Jul. 2007.

[21] J. Di, and F. Yang, "D3L - A Framework on Fighting against Non-Invasive Attacks to Integrated Circuits for Security Applications", *in Proc. 3rd IASTED International Conference on Circuits, Signals, and Systems (ICCS)*, pp. 73-78, Oct. 2005.

[22] S. Guilley, S. Chaudhuri, L. Sauvage, T. Graba, J.-L. Danger, P. Hoogvorst, V. Vinh-Nga, and M. Nassar, "Place-and-Route Impact on the Security of DPL Designs in FPGAs," *in Proc. IEEE International Workshop on Hardware-Oriented Security and Trust (HOST)*, pp. 26-32, Jun. 2008.

[23] S. Rammohan, V. Sundaresan, R. Vemuri, "Reduced Complementary Dynamic and Differential Logic: A CMOS Logic Style for DPA-resistant Secure IC Design," *in Proc. 21st International Conference on VLSI Design (VLSI Design)*, pp. 699-705, Jan. 2008.

[24] R. Soares, N. Calazans, V. Lomné, P. Maurine, L. Torres and M. Robert. "Evaluating the Robustness of Secure Triple Track Logic through Prototyping," in Proc. *21st Symposium on Integrated Circuits and Systems Design (SBCCI)*, pp. 193-198, Sep. 2008.

[25] V. Lomné, T. Ordas, P. Maurine, L. Torres, M. Robert, R. Soares and N. Calazans,. "Triple Rail Logic Robustness against DPA," in Proc. *2008 International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, pp. 415-420, Dec. 2008.

[26] C. J. Myers. "Asynchronous Circuit Design," *Wiley-IEEE*, 2003, 404 p.

[27] Z. Zhang, Z. Wen, L. Chen, F. Zang, T. Zhou, "A Novel BIST Approach for Testing Logic Resources Using Hard Macro," *in Proc. International Conference on Neural Network and Digital Signal Processing*, pp. 379-381, Jun. 2008.

[28] M. Huebner, T. Becker, J. Becker, "Real-Time LUT-Based Network Topologies for Dynamic and Partial FPGA Self-Reconfiguration," *in Proc. 17th Symposium on Integrated Circuits and Systems Design (SBCCI)*, pp. 28-32, Sept. 2004.

[29] J. Pontes, R. Soares, E. Carvalho, F. Moraes, N. Calazans, "SCAFFI: An Intrachip FPGA Asynchronous Interface based on Hard Macros," *in Proc. 25th International Conference on Computer Design (ICCD)*, pp. 541-546, Oct. 2007.

[30] E. Brier, C. Clavier, F. Olivier, "Correlation Power Analysis with

a Leakage Model," *in Proc. 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 16-29, Aug. 2004.

[31] 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," *in Proc. 18th International Workshop on Power and Timing Modeling Optimization and Simulation (PATMOS)*, Sept. 2008.