Analysis and Improvement of Dual Rail Logic as a Countermeasure Against DPA

Alin Razafindraibe, Michel Robert, Philippe Maurine

Analysis and Improvement of Dual Rail Logic as a Countermeasure Against DPA

A. Razafindraibe, M. Robert, and P. Maurine

University of Montpellier / LIRMM
II, 161 rue Ada, 34392 Montpellier, France

Abstract. Dual rail logic is considered as a relevant hardware countermeasure against Differential Power Analysis (DPA) by making power consumption data independent. In this paper, we deduce from a thorough analysis of the robustness of dual rail logic against DPA the design range in which it can be considered as effectively robust. Surprisingly this secure design range is quite narrow. We therefore propose the use of an improved logic, called Secure Triple Track Logic, as an alternative to more conventional dual rail logics. To validate the claimed benefits of the logic introduced herein, we have implemented a sensitive block of the Data Encryption Standard algorithm (DES) and carried out by simulation DPA attacks.

1 Introduction

It is now well recognized that the Achilles' heel of secure applications lies in their physical implementation. Among all the potential techniques to retrieve the secret key, one can mention side channel attacks . If there are many side channel attacks, DPA attack [1], is considered as one of the most efficient since it requires only less skills and materials, than others attacks such electromagnetic attacks, to be successfully implemented. Because of it dangerousness, many countermeasures have been proposed in former works [2, 3]. Recently, synchronous [4] or asynchronous dual rail logic [5, 6] has been identified as a promising solution to increase the robustness of secure applications. However some experiments have shown that the use of basic dual rail structures is not sufficient to warrant a high level of robustness against DPA. To overcome this problem, specific dual rail cells [4,7,8] and ad hoc place and route methods [9] have been developed. Goals of these countermeasures are to make the power consumption of logic gates independent of the manipulated data and to balance the wire capacitance of each differential pair during place & route steps.

Within this context, the first contribution of this paper is to analyze thoroughly the robustness of dual rail logic against DPA and to identify the secure design range. From the latter, we will identify the most sensitive parameters in secure dual rail design and will propose adequate countermeasures while staying as close to classical design flow as possible.

By looking closely this secure design range, it appears that it is too narrow. To address this problem, we propose the STTL (Secure Triple Track Logic) secure logic to implement key modules of ciphering algorithms. This is the second contribution of the paper.

N. Azemard and L. Svensson (Eds.): PATMOS 2007, LNCS 4644, pp. 340–351, 2007.

The remainder of the paper is organized as follows: First, the basics of DPA are briefly summed up and the claimed benefits of DRL are reviewed. Then, the masked assumptions supporting these claims are identified and their validity range evaluated by simulation on a 130nm process. After a discussion about this secure design range, the STTL is introduced as an adequate hardware countermeasure against DPA. The design features of this logic are also detailed. Before concluding, validations of the robustness of the proposed logic are presented.

2 Differential Power Analysis

DPA, first introduced in [1], succeeds in retrieving the secret key by exploiting the fact that the power consumption of cryptosystems is data dependent. Generally, DPA attack is executed in three phases: data collection, data sorting and data analysis.

Data collection consists in running a large number of cryptographic operations and recording the sampled corresponding power traces.

Data sorting consists in extracting, for all possible sub-secret keys, two sets of power traces from the whole power trace collection. These sets of power trace, $S_{‘0’}$ and $S_{‘1’}$, are built considering the expected value of the bit under attack according to both the guessed value of the sub-key and to the input data.

Data analysis consists in computing, for each possible guess of the secret key, the average power traces of $S_{‘0’}$ and $S_{‘1’}$ and in performing the difference between the averages. Finally, the secret key is usually disclosed by identifying the guess leading to the difference with the higher amplitude.

If this protocol is quite simple, one can wonder about the syndrome which is really captured by the DPA while applied on a dual rail circuit. In order to identify it, let us consider that a DPA is performed, with v vectors ($\in$ V), on the output bit z of a logic block made of P gates. Among the v vectors applied to the cryptosystems, $t \in$ T of them forced z to the logic value ‘1’, while the $f = v - t$ forced z to ‘0’ ($f \in$ F). With such definitions, the syndrome, S_{DPA}, captured by the DPA is:

$$S_{DPA}(Z) = \frac{1}{t} \cdot \sum_{u=1}^{t} I_u(t) - \frac{1}{f} \cdot \sum_{w=1}^{f} I_w(t) \tag{1}$$

In the above expression, $I_u(t)$ and $I_w(t)$ are the current profiles of the whole block under attack while vectors $u \in$ V and w$\in$W are applied on its inputs. These current profiles can be defined as the current consumes by all the gates of which is made up the block:

$$I_v(t) = \sum_{p=1}^{P} i_p(t) \qquad I_w(t) = \sum_{p=1}^{P} i_p(t) \tag{2}$$

Considering the definitions above and defining r_p^T, f_p^T (r_p^F et f_p^F) as the numbers of vectors of T (F) forcing the output of gate p to the a logic ‘1’ and ‘0’ respectively, it is then possible to deduce from (1) the following DPA signature expression :

$$S_{DPA}(Z) = \sum_{p=1}^{P-1} \left(\frac{f_p^F}{f} - \frac{f_p^T}{t} \right) \cdot \Delta i_p(t) + \Delta i_Z(t) \tag{3}$$

where $\Delta i_{p}(t)$ is the differential current profile of gate p, and $\Delta i_z(t)$ is the differential current profile of the gate driving the bit under attack. Here, we denote by differential switching current the waveform obtained by performing the difference between the currents provided by V_{DD} to the considered gate to settle respectively a logic '1' and a logic '0' on its output.

Note, that if f_p^T/t and f_p^F/f are close one from the other, the expression (3) resumes to the differential current profile of the gate driving *z*, within its operating context. This highlights the great sensitivity of DPA.

3 Dual Rail Logic: A Countermeasure Against DPA

To secure cryptosystem against such an attack, the first action to be made is to break its assumptions in making power consumption independent of the manipulated data. Countermeasures have been proposed in [2] at all level of abstraction. Most of them aim at reducing the correlation between the data and leaking syndromes. Dual rail logic is one of these countermeasures.

The main advantage of dual rail Logic lies in the associated encoding used to present logic values. Indeed, for such an encoding, a rising transition on one of the two wires indicates that a bit is set to a valid logic '1' or '0', while a falling edge indicates that the bit returns to the invalid state which has no logical meaning. Consequently, the transmission of a valid logic '1' or '0' always requires switching a rail to V_{DD}. Therefore the differential current profiles of dual rail cells, and thus circuits, should be significantly lower than the ones of single ended gate. However, this claim holds if and only if the power consumption and the propagation delay of dual rail cells is data independent i.e. if the current waveform related to the settlement of logic '1' and '0' are rigorously the same.

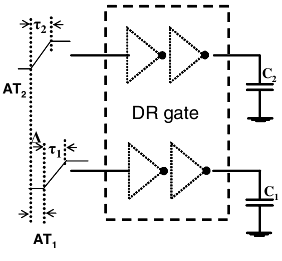

Fig. 1. A Dual rail cell within its context

Since conventional dual rail cells, such as DCVSL or asynchronous DIMS logic [12] do not have perfectly balanced power consumption a lot of effort have been devoted in [4,7,8] to define secure dual rail cells. In its seminal paper [7], K. Tiri has introduced the Sense Amplifier Based Logic as logic with constant power consumption. Dynamic Current Mode Logic has also been identified in [10] as an alternative to SABL while secure Dual Rail CMOS schematics are given in [4, 7].

Even if all these formerly proposed solutions appear efficient, at cell level, to counteract the DPA, they are all based on three crude assumptions. Indeed, in all these works, it is assumed that after place & route steps:

- Assumption n°1: each wire of each differential output is loaded by an identical capacitance value (C_2=C_1).
- Assumption n°2: all the inputs of the gate under consideration are controlled by identical drivers, i.e. that the transition times (labeled by τ in the remainder of the paper) of all the input signals have the same value (τ_T=τ_F),
- Assumption n°3: the switching process of the gate under consideration starts always at the same time (AT_T=AT_F).

Considering that both the power consumption and the timings of Dual Rail CMOS gates strongly depend on the transition time of the signals triggering the gate switching, and on the output capacitance switched, one can wonder about the validity domain of the three aforementioned assumptions.

4 Secure Design Range

To evaluate this validity domain, the modeling of the switching current waveform of CMOS dual rail gate is of prime importance. Considering that any single rail gate can be reduced to an equivalent inverter [11,14] or buffer (fig.1), we did model, at first order, the maximum amplitude Δi_{MAX} of the differential switching current profile of a dual rail gate loaded by unmatched capacitances, controlled by imbalanced transition time and finally triggered by imbalanced arrival time signals [21].

Considering I_{TH} as the smaller current imbalance that can be monitored with a given number N of current profiles measures according to the SNR definition:

$$SNR = \frac{I_{TH}}{\sigma} \cdot \sqrt{N} \tag{4}$$

we did deduce from the modelling of Δi_{MAX} [21], three criteria allowing to quickly estimate the robustness against DPA of a Dual Rail cell within its context. These criteria are the following:

$$\left.\frac{C_2}{C_1}\right|_{Crit} = max\left\{ \frac{1}{R_i} \cdot \frac{\frac{V_{DD}}{V_{DSAT}} - 1}{(1-\beta)} + 1 ; \left(\frac{V_{DSAT}}{\beta \cdot V_{DD}} \left(1 - \frac{1}{R_i} \right) \right)^{-1} \right\} \tag{5}$$

$$\left.\frac{\tau_1}{\tau_2}\right|_{Crit} = 1 - \frac{(V_{DD} - V_T)}{V_{DD}} \cdot \frac{1}{R_i} \quad if \quad I_{MAX} > I_{TH} \tag{6}$$

$$\left|\frac{\Delta}{\tau}\right|_{Crit} = \frac{(V_{DD} - V_T)}{V_{DD}} \cdot \frac{1}{R_i} \quad if \quad I_{MAX} > I_{TH} \tag{7}$$

$$R_i = \frac{I_{MAX}}{I_{TH}} \tag{8}$$

In the above expressions, V_{DD}, V_T and V_{DSAT} are the supply, threshold and saturation voltages of the considered transistor, β is the ratio of current provided by a transistor while its drain source voltage is respectively equal to V_{DSAT} and V_{DD}.

As shown, the first criterion allows evaluating the robustness of a dual rail cell in presence of unmatched loads. More precisely, for a given threshold of current I_{TH}, expression (5) provides the imbalance that can be tolerated between the outputs. In the same way, the second and third criteria allow evaluating the robustness of a Dual Rail cell in presence of imbalanced input transition and arrival times respectively.

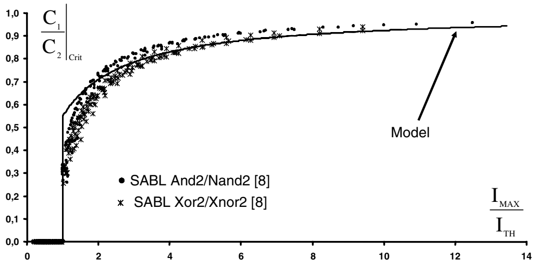

Fig. 2. Simulated and calculated values of $C_1/C_2|_{Crit}$ vs. $Ri=I_{MAX}/I_{TH}$ for two different SABL gates

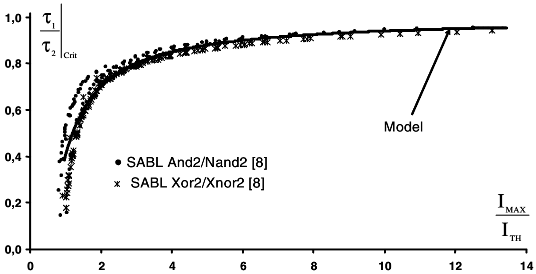

Fig. 3. Simulated and calculated values of $\tau_1/\tau_2|_{Crit}$ vs $Ri=I_{MAX}/I_{TH}$ for two different SABL gate

One property of these criteria is that they do depend only on process parameters. This implies that, for a given cell topology, it is possible to obtained, by electrical simulation [19], characteristic curves of its robustness against DPA in presence of load, transition and arrival times imbalances. This provides a really interesting way to compare the robustness of different cell topologies regardless of their sizing provided to apply a unique gate sizing policy for all drives.

To demonstrate the validity of these first order criteria, we simulated and computed the critical load, transition and arrival time imbalance curves of SABL and2/nand2 and xor2/xnor2 gates. Fig 2, 3 and 4 report the results obtained.

As shown, the accuracy of the proposed robustness criteria is satisfactory. However, a detailed interpretation of these characteristics provides more interesting results.

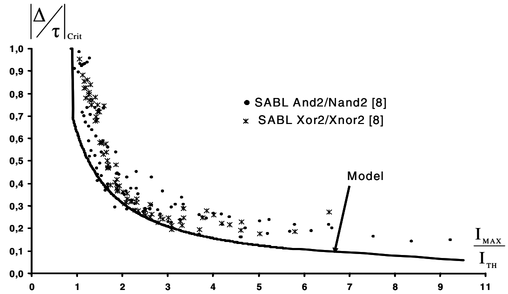

Fig. 4. Simulated and calculated values of $|\Delta/\tau|_{\text{Crit}}$ vs $\text{Ri}=I_{\text{MAX}}/I_{\text{TH}}$ for two different SABL gates [8]

Let us consider that $R_i=I_{MAX}/I_{TH}$ is equal to 2 (100µA / 50µA). For such a R_i value, we may conclude that the two considered SABL gates remains robust against DPA if:

- the load imbalance C_l/C_2 is smaller than 0.7 ($C_l>C_2$), i.e. if C_2 remains smaller than 1.4 times C_l
- the transition time imbalance τ_l/τ_2 is smaller than 0.7,
- and the arrival time imbalance $|\Delta/\tau|$ is smaller than 0.2 ($\tau_l=\tau_2=\tau$), i.e. if all the signals triggering the gate arrive within a time window of width equal to 0.2 time the smaller input transition time τ. This is quite small considering that typical transition time values range between 20ps and 300ps for the 130nm process under consideration.

This demonstrates that dual rail logic may be considered as robust against DPA in presence of significant load and transition time imbalances but does not suffer any significant arrival time imbalances. This is all the more true since arrival time imbalances may grow with the logic depth of the data paths.

From the preceding expressions and results, it appears that there is effectively a design range in which dual rail logic can be considered as robust against DPA. However this secure design space is quite narrow since the tolerable arrival time imbalances are quite small.

Based on the previous expressions, we have to make Ri (i.e. I_{MAX}) as small as possible to enlarge this secure design range. With this intention, naturally, one possible solution is to work with reduced V_{DD} values. However this imposes to manage properly the power versus timing trade off. Considering once again the narrowness of the secure design range, it appears that another alternative lies in the progressive development of dedicated CAD tools and/or design solutions to balance not only the parasitic capacitances introduced during the place & route as proposed in [9], but also the transition and arrival times. Within this context, expressions (5-8) constitute clever design criteria to evaluate the dangerousness of elementary cells within a secure dual rail circuit. However, as CAD tools will not be available in a near future, we therefore concentrate our effort on design solutions and more precisely on the structures of dual rail cells used to implement secure design.

5 Secure Triple Track Logic

If the results obtained above demonstrate that the main benefit of the Dual Rail countermeasure lies in its ability in reducing the differential current profiles and thus the correlations between data and the power consumption, they also point out its main weakness: dual rail logic does not sufficiently reduce the correlation between data and computation times to constitute an extremely robust countermeasure. To eliminate this remaining weakness, we have developed a CMOS logic with data independent timing and power consumption called Secure Triple Track Logic (STTL in the rest of the paper). In fact, it is a variant of the dual rail logic.

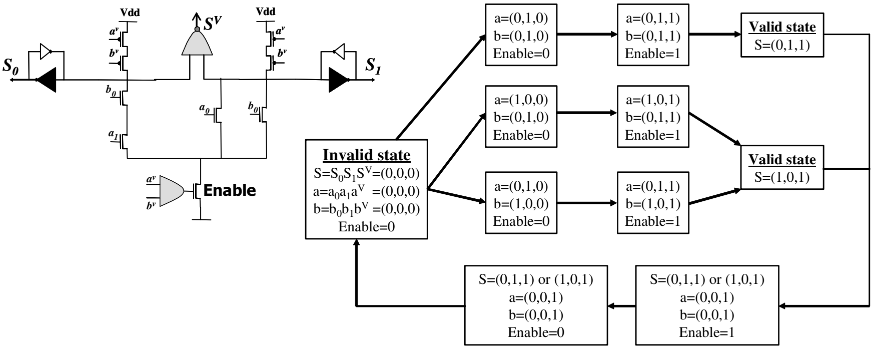

Fig. 5. STTL and2/nand2 gate

To introduce the main characteristics of this logic style, an STTL and2 /nand2 gate is represented in Fig.5 as well as a graph illustrating its operation. As shown, instead of using two output wires to convey one logical value, STTL uses three. Indeed an additional output wire S^V is used to indicate whenever the output data S is valid or not. Similarly, two additional input wires a^v and b^v, indicating the validity of the incoming signals a and b are used. STTL operates thus according a kind of triple rail encoding of data (fig.6). Note that this is not the first time that the use of an additional wire to encode the validity of a signal is proposed. Indeed, in [20] an additional wire is used to obtain "efficient hardware implementations" but not to obtain secure designs or a data independent logic.

As illustrated by Fig.6, the encoding of data is not a true triple rail encoding since the additional code value is redundant and does not convey any information about the bit value itself. This additional code value (and thus the power consumption of greyed

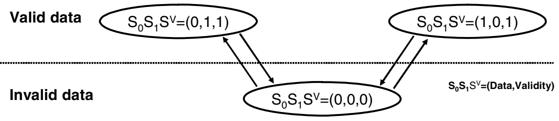

Fig. 6. Data encoding used by STTL

gates on Fig. 5) is therefore uncorrelated with the value of input data. This property is extremely important. Indeed, one key design characteristic of STTL gate is that all validity signals such (a^v, b^v and S^V) are delivered by low switching current gate (greyed gates on fig.5), i.e. gates having a greater delays than high switching current gates (blackened gates on fig.5) in order to ensure that all input validity signals (a^v, b^v) settle after the data signals (a_0, a_1, b_0, b_1). This can be obtained easily by sizing transistors of greyed cells smaller than those of blackened cells.

With such a Return to Zero encoding of data and specific gate design rules, the and2/ nand2 represented in Fig.5 operates as follows. Starting from the invalid state, data (a_0,a_1,b_0,b_1) settle first. In a second step, validity signals (a^v,b^v) rise forcing 'Enable' to '1' which allows in a fourth step the computation of the outputs. The return to the invalid state is performed in a similar way. First data (a_0,a_1,b_0,b_1) returns to '0'. Then the validity signals (a^v,b^v) are also forced to '0' by the environment to '0' allowing the gate to return to the invalid state.

If the use of an additional wire implies, at cell level, a data independent power overhead, estimated roughly to be within 10% to 30% compared to Dual Rail cells introduced in [12] depending on the complexity of the gate, it allows designing STTL gates having four interesting properties from security and design points of view:

First: avoid any internal cell activity while the data signals (a_0,a_1,b_0,b_1) are settling since no currents may flow if validity signals (a^v, b^v) are not true

Second: a quasi data independent power consumption as most of the proposed secure dual rail gates [4,7,8,10,12,17],

Third: a quasi data independent propagation delays, at block level, since the firing of gates will always be triggered by a data independent signals (Enable) computed from validity signals (a^v, b^v and S^V) which are also data independent.

Fourth: STTL gates are quite compact compared to other dual rail cells. As an illustration, Table 1 gives the number of transistors required to realize different basic functions in STTL and in others design styles.

Table 1. Transistor count comparison

Gates	STTL	[16]	[4]	[8]
Nand2/Nor2And2/Or2	27	64	112	14
Nand3/Nor3And3/Or3	29	128	224	28
Xor2/Xnor2	29	68	80	18
Xor3/Xnor3	35	136	160	36
AO21/ AOI21	39	128	224	28
AO22/ AOI22	42	192	336	42

The third property aforementioned counterbalances the identified weakness (relative to the arrival time imbalances) of basic or secure dual rail gates introduced in former works. Indeed, the gate firings are independent of the data processed if the incertitude on the arrival time of all input signals, introduced by the place and route steps, is smaller than the time window Q that separates the settlements of the data (E_0, E_1) and the validity signal E^V (see Fig.7).

An important point here is that this time window Q can be tuned by sizing adequately the low switching current gates. In other words, the robustness of a STTL circuit can easily be managed by enlarging or reducing the width of this time window.

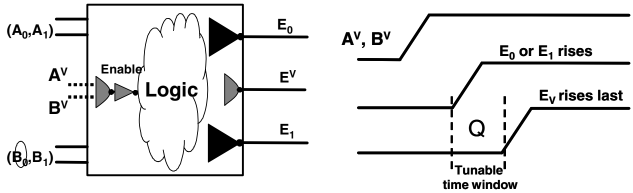

Fig. 7. Timing behaviour of an STTL gate

In order to evaluate the effectiveness of STTL, we have implemented a sensitive sub-module of DES algorithm [18] namely the sbox1 which is driven by XORs gates. With this intention, we make use of our STTL library but also formerly introduced dual rail logics in order to perform comparison. Among these others dual rail libraries, we may distinguish the ones including secure Dual Rail gates [4, 12] but also the SABL gate [8] and finally AO222 based logic [13;16]. With such a simulation setup, the expected properties of the STTL were analysed and verified.

In a first validation step, we have realized by simulation DPA attacks on the four output bits of the Sbox1 in order to identify precisely the impact of the routing on the robustness of the STTL. More precisely, to obtain a thorough evaluation of the robustness against DPA of the considered logic styles, all the simulations were first based on an ideal netlists (without parasitic capacitances) and subsequently on a back-annotated netlists. Note that to be fair, we have adopted the same sizing policy for all the Dual Rail cells but also the same parameters for the place & route steps done with Soc Encounter tool [15].

Fig.8 gives, for the 64 possible guesses of the secret key, the DPA signatures obtained during the attack of the third output (S_3) bit of the Sbox1 implemented with STTL gates. From this figure two conclusions may be drawn. First, performing DPA attacks on S_3, as for the three others, does not provide any information about the value of the secret key since its DPA curve is not distinguishable from the 63 others DPA signatures. Therefore STTL counteracts in this case the attack. Finally, the most important result that can be drawn considering Fig.8 is that STTL is, as expected, quasi insensitive to the load imbalances introduced by the place and route steps since the DPA signatures obtained with the ideal or back-annotated netlists are quasi identical.

In a second validation step, we wanted to demonstrate that STTL effectively leads to quasi-data independent propagation delay values at block level. We therefore extracted from electrical simulations of back-annotated netlists, the time spent by the signals to propagate from the inputs to the outputs. This was done for all possible input vectors considering STTL as well as the other logic styles introduced in [4, 8, 12]. Note that all input signals were assumed to be stable at t=0.

On Fig.9, we plotted the time spent by the signals to propagate from the inputs to the output S_3. More precisely, this figure gives the propagation delay distributions while S_3 settles logic '1' and '0' respectively for different Dual Rail Logic. Note, that we have also reported the average propagation delay values $<T_1>$ and $<T_0>$ spent by the circuit to settle a '1' and a '0' on output S_3. The obtained representation is interesting to evaluate the robustness of a logic block against DPA. Indeed, the more symmetrical are the distributions, the more data independent is the considered logic and thus the more robust the physical implementation is.

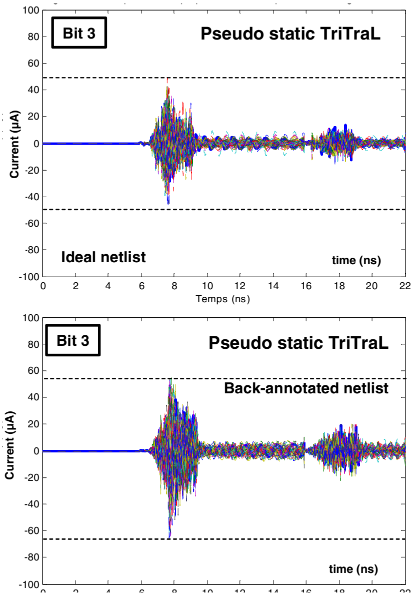

Fig. 8. DPA signatures obtained considering and without considering routing capacitances

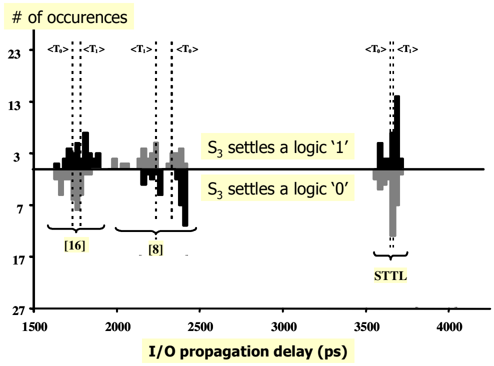

Fig. 9. Some Timing data

As shown, depending on the logic, the gap (<T_1> - <T_0>) between the average times spent to settle logic '1' and '0' can be quite small (few ps) or significant (several tenths of ps). Obviously, STTL exhibits a quasi data independent timing behaviour, while the ones introduced in [8, 12] do not. However the price to be paid is longer I/O propagation delays due to the use of low switching current gates to control the validity signals.

In a final step, we compared the robustness against DPA of all the considered logic styles. We thus performed by simulation DPA attacks on all the outputs of the structure represented on Sbox1. The netlists considered during these simulations were back-annotated ones Fig. 10 reports some relevant results we have obtained. These results may be summarized as follows. First, for all the attacked output bits, DPA was

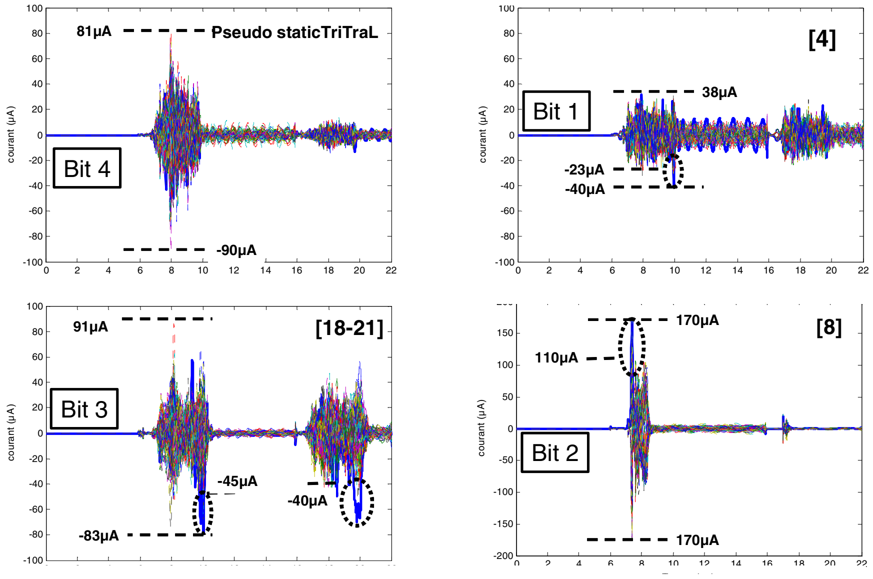

Fig. 10. Simulated DPA signature of the Sbox1outputs with back-annotated netlist (X-axis unit is ns)

unsuccessful while done on the STTL implementation. Second, these attacks may be considered as successful while done on SABL [8], and on circuits implemented with gates introduced in [4, 13, 16]. However as shown on Fig.9, for [4], the revealed syndrome is quite small.

6 Conclusion

A thorough evaluation of the robustness of Dual Rail Logic has been carried out in this paper. This analysis has pointed out that Dual Rail Logic does not sufficiently reduce correlation between data and computation times to be a fully robust countermeasure against DPA. This observation has led to the proposal of an improved logic called STTL. The main characteristics of this logic that made of it a robust countermeasure against DPA are: quasi data independent power consumption and timing behaviour. The latter characteristic ensures that STTL is particularly robust to load, and arrival time imbalances introduced by the place and route steps while the resulting cells remain quite compact with respect to formerly introduced logic styles.

References

[1] Kocher, P., et al.: Differential power analysis. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)

[2] Suzuki, et al.: Random Switching Logic: A Countermeasure against DPA based on Transition Probability, Cryptology ePrint Archive, report 2004/346

[3] Bystrov, A., Yakovlev, A., Sokolov, D., Murphy, J.: Design and Analysis of Dual-Rail Circuits for Security Applications. IEEE Trans. on Computers 54(4), 449–460 (2005)

[4] Guilley, S., et al.: CMOS Structures Suitable for Secure Hardware. In: 2004 Design, Automation and Test in Europe Conf. and Exposition (DATE 2004),February 2004, France, 16-20 (2004)

[5] Fournier, J.J.A., et al.: Security Evaluation of Asynchronous Circuits. In: D.Walter, C., Koç, Ç.K., Paar, C. (eds.) CHES 2003. LNCS, vol. 2779, pp. 137–151. Springer, Heidelberg (2003)

[6] Bouesse, G.F., et al.: DPA on Quasi Delay Insensitive Asynchronous Circuits: Formalization and Improvement. In: 2005 Design, Automation and Test in Europe Conference and Exposition (DATE 2005), 7-11 March, 2005, Munich, Germany (2005)

[7] Razafindraibe, A., et al.: Secure structures for secure asynchronous QDI circuits. In: DCIS'04: 19th International Conference on Design of Circuits and Integrated Systems (DCIS'04), November 24-26, 2004, Bordeaux, France (2004)

[8] Tiri, K., et al.: Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology. In: D.Walter, C., Koç, Ç.K., Paar, C. (eds.) CHES 2003. LNCS, vol. 2779, pp. 125–136. Springer, Heidelberg (2003)

[9] Tiri, K., et al.: A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs. In: 2005 Design, Automation and Test in Europe Conference and Exposition (DATE 2005), 7-11 March, 2005, Munich, Germany (2005)

[10] Mace, F., et al.: A dynamic current mode logic to counteract power analysis attacks. In: DCIS'04: 19th International Conference on Design of Circuits and Integrated Systems (DCIS'04), November 24-26, 2004, Bordeaux, France (2004)

[11] Maurine, P., et al.: Transition time modeling in deep submicron CMOS. IEEE Trans. on Computer Aided Design 21, 1352–1363 (2002)

[12] Razafindraibe, A., et al.: Asynchronous Dual rail Cells to Secure Cryptosystem against Side Channel Attacks (SAME'2005), October 5-6, 2005, Sophia Antipolis, France (2005)

[13] Maurine, P., et al.: Static Implementation of QDI Asynchronous Primitives. In: Chico, J.J., Macii, E. (eds.) PATMOS 2003. LNCS, vol. 2799, pp. 181–191. Springer, Heidelberg (2003)

[14] Chaterzigeorgiou, A., et al.: Collapsing the Transistor Chain to an Effective Single Equivalent Transistor. In: 1998 Design Automation and Test in Europe (DATE '98), February 23-26, 1998, Le Palais des Congres de Paris, Paris, France (1998)

[15] http://www.cadence.com/products/digital_ic/soc_encounter/index.aspx

[16] Piguet, C., et al.: Electrical Design of Dynamic and Static Speed Independent CMOS Circuits from Signal Transistion Graphs. In: 8th International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS '98), Technical University of Denmark, October 7-9, 1998, pp. 357–366 (1998)

[17] Kulikowski, K.J., et al.: Delay Insensitive Encoding and Power Analysis: A Balancing Act. In: 11th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC 2005), New York City, USA, March 13-16, 2005, pp. 116–125 (2005)

[18] [18] National Bureau of Standards: Data Encryption Standard, Federal Information Processing Standards Publication, vol. 46 (January 1977)

[19] Eldo User's Manual, Mentor Graphic's Corp (1998)

[20] Meng, T.H.-Y., et al.: Automatic Synthesis of Asynchronous Circuits from High-Level Specifications. IEEE Trans. On Computer Aided Design 8(11) (November 1989)

[21] Razafindraibe, A., Robert, M., Renaudin, M., Maurine, P.: Evaluation of the robustness of dual rail logic against DPA. In: IEEE International Conference on Integrated Circuit Design and Technology (24-26 May, 2006)