

Security Evaluation of Dual Rail Logic Against DPA Attacks

Hanitriniaina Razafindraibe, Philippe Maurine, Michel Robert, Marc Renaudin

▶ **To cite this version:**

Hanitriniaina Razafindraibe, Philippe Maurine, Michel Robert, Marc Renaudin. Security Evaluation of Dual Rail Logic Against DPA Attacks. VLSI-SoC 2006 - 14th IFIP International Conference on Very Large Scale Integration, Oct 2006, Nice, France. pp.181-186, 10.1109/VLSISOC.2006.313230 . lirmm-00109692

HAL Id: lirmm-00109692

https://hal-lirmm.ccsd.cnrs.fr/lirmm-00109692

Submitted on 25 Oct 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Security evaluation of dual rail logic against DPA attacks

A. Razafindraibe[1], P. Maurine[1], M. Robert[1], M.Renaudin[2]
LIRMM, Microelectronic Department, 161 rue Ada, 34392 Montpellier, France[1]
TIMA Laboratory,. 46 avenue Félix Viallet, 38000 Grenoble France[2]
razafind@lirmm.fr

***Abstract*—Based on a first order model of the switching current flowing in CMOS cell, an investigation of the robustness against DPA attacks of dual rail logic is carried out. The result of this investigation, performed on 130nm process, is the formal identification of the design range in which dual rail logic can be considered as robust.**

I. INTRODUCTION

It is now well recognized that the Achilles' heel of secure ciphering algorithms, such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard), lies in their physical implementation. Among all the potential techniques to obtain the secret key, side-channel attacks are the most efficient. If there are a lot of different side-channel attacks, DPA (Differential Power Analysis), introduced in [1] is nowadays considered as one of the most dangerous since it requires only few skills and materials to be successfully implemented.

Because of its dangerousness, many countermeasures against DPA attacks have been proposed in former works [2, 3]. Recently, synchronous [4] or asynchronous [5, 6] dual rail logic 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 attacks. To overcome this problem, specific dual rail cells [4, 7, 8] and ad hoc place and route methods [9] have been developed. Nevertheless, none formal evaluation of the intrinsic robustness of dual rail logic has been proposed. In this context, this paper aims at introducing an analytical evaluation of the robustness of dual rail logic against DPA attacks.

The remainder of this paper is organized as follows. In section II, the basics of DPA attacks are briefly summed up and the claimed benefits of dual rail logic are reviewed. The identification of the masked assumptions supporting these claims is also done in this section. In section III, an analytical model of the switching current waveform of CMOS cells is developed and validated on a 130nm process. This model is then used, in section IV and V, to identify the design range on which the dual rail logic can be considered as robust against DPA attacks. The latter is done through the development of design criteria (section V) that can be used to increase the robustness against DPA attacks of dual rail circuits. Finally, a discussion about the use of dual rail logic against DPA attacks is proposed and a conclusion is drawn in section VI.

II. DPA AND THE DUAL RAIL COUNTERMEASURE

Differential Power Analysis attacks lies on the fact that the power consumption of basic CMOS cells, and therefore of CMOS circuits, is data dependent. Considering this, it is possible to retrieve the secret key of a secure application by measuring the statistical correlation between the power consumption and the data according to some assumptions made on the secret key: the higher is the correlation value the closer the guess key is from the correct secret key.

Consequently, to secure a circuit against such attacks, the first to be made is to break DPA attacks assumption in making power consumption independent of the manipulated data. With this intention, countermeasures have been proposed [1] 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 this special logic style lies in the associated encoding used to present logic values. Fig.1 gives the return to zero (RTZ) encoding considered in the rest of this paper. As shown in Fig.1, a rising transition on one of the two wires indicates that a bit is set to a valid logic 'one' or 'zero', while a falling transition indicates that the bit is set to an invalid value which has no logical meaning. Consequently, the transmission of a valid logic 'one' or 'zero' always requires switching a rail to V_{DD}. Therefore the differential power signature of dual rail circuits should be significantly lower than the one of single rail circuit.

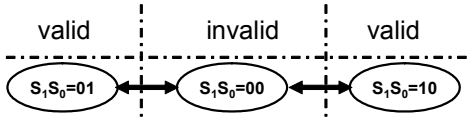


Figure 1. Dual rail encoding

However, this claim is valid if and only if both the power consumption and the propagation delay of dual rail cells are data independent. Since usual dual rail cells, such as DCVSL or asynchronous DIMS logic [15] do not have balanced power consumption nor data independent propagation delays, a lot of effort [4, 7, 8] have been devoted to define fully (power and delay) balanced dual rail structures. For example, in its seminal paper [7], K. Tiri has introduced the Sense Amplifier Based Logic (SABL) as logic with constant power consumption. Afterwards, dynamic current mode logic has also been identified in [10] as an alternative to SABL while secured dual rail CMOS schematics are given in [7] and [4].

Even if all these formerly proposed solutions appear efficient to counteract the DPA attacks, they are all based on three crude assumptions. More precisely, in all the above mentioned works it is assumed that:

- **Assumption n°1:** all the inputs of the gate under consideration are controlled by identical drivers, i.e. that the transition times of all the input signals have the same value.
- **Assumption n°2:** the switching process of the gate under consideration starts always at the same time.
- **Assumption n°3:** the differential output nodes are loaded by capacitance of identical value (C_1=C_2).

Considering that both the power consumption and the propagation delay of CMOS gates strongly depend on the transition time of the signal triggering the gate switching, and on the output capacitance switched, one can wonder what the validity domain of the three above mentioned assumptions.

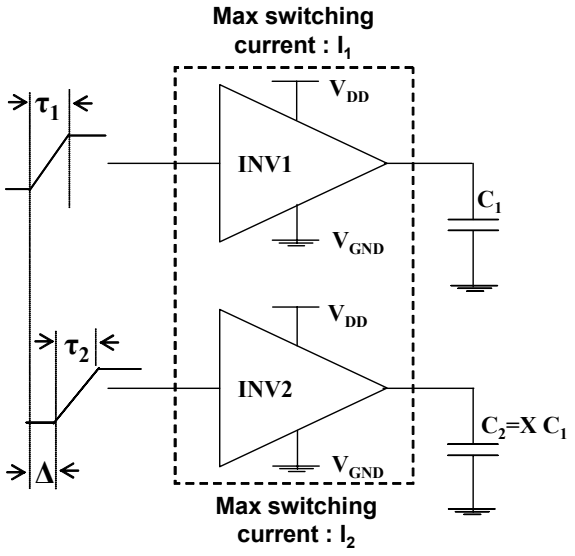


Figure 2. Reduced equivalent model of a dual rail cell

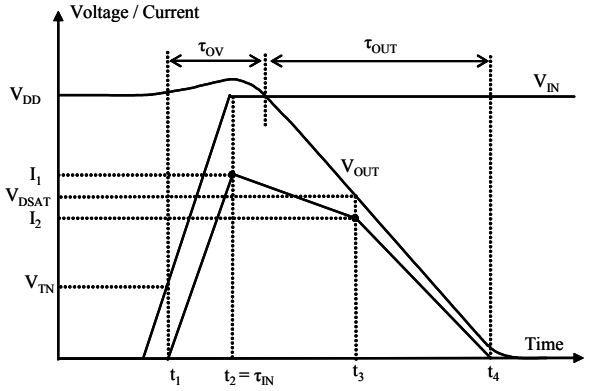


Figure 3. Typical waveforms observed during the switching of a cell

III. SWITCHING CURRENT WAVEFORM MODEL

To evaluate this validity domain, the modelling 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], let us model any dual rail cell by two inverters as illustrated by Fig.2. With such a reduction procedure, the modelling of the switching current waveform of dual rail gates comes down to the modelling of the switching current waveform of basic cmos inverters. A great effort has been dedicated to the modelling of the inverter switching process [11, 12]. For typical loading and controlling conditions (Fast input ramps [11]), the switching current waveform of a CMOS gate can be modelled by a piece wise linear function as illustrated by Fig.3.

In Fig. 3, I1, I2 and t1, t2, t3 and t4 are the characteristic points to be modelled. I1 and I2 are respectively the maximum current values that can deliver the considered inverter (V_{GS}=V_{DD}) while its drain to source voltage is equal to V_{DD} and V_{DSAT} respectively. This leads, considering short channel devices [13, 14], to the following expressions of I1 and I2:

$$I_1 = {}^{K}\!/_{DW} \cdot W \cdot (V_{DD} - V_T) \cdot (1 + \lambda \cdot V_{DD}) \qquad (1)$$

$$I_2 = {}^{K}\!/_{DW} \cdot W \cdot (V_{DD} - V_T) \cdot (1 + \lambda \cdot V_{DSAT}) \qquad (2)$$

where K, W, V_{DD}, V_T, λ and DW are respectively the transistor conduction factor, the transistor width, the supply and threshold voltages, the channel length modulation factor and finally the logical weight (DW=1 for inverters). The latter takes into account the reduction of the gate to an equivalent inverter.

Considering the characteristic points t_i, t_1 and t_2 are defined as the times at which the input signal reaches respectively the voltage values V_T and V_{DD}. These definitions lead to:

$$t_1 = \frac{V_{TN}}{V_{DD}} \cdot \tau_{IN} \qquad (3) \qquad\qquad t_2 = \tau_{IN} \qquad (4)$$

The characteristic time t_3 corresponds to the time at which the output voltage crosses the values V_{DSAT} while t_4 is the

time at which the switching process ends. Times t_3 and t_4 can thus be expressed by:

$$t_3 = \tau_{ov} + \frac{V_{DSAT}}{V_{DD}} \cdot \tau_{OUT} \quad (5) \quad t_4 = \tau_{OV} + \tau_{OUT} \quad (6)$$

where τ_{ov} is the time at which the overshooting ends [12] and τ_{out} is the output transition time measured between 80% and 20% of V_{DD} and extrapolated on the full voltage swing. For a fast input rising edge, an expression (7) can be found in [11] while the expression (8) of the τ_{ov} can easily be obtained by solving the differential equation governing the behaviour of the inverter.

$$\tau_{OUT} = \frac{DW \cdot C_L \cdot V_{DD}}{K \cdot W \cdot (V_{DD} - V_{TN})} \quad (7) \quad \tau_{OV} = \tau_{IN} + \frac{C_M}{I_1} \cdot V_{DD} \quad (8)$$

In the above expressions C_L and C_M stands respectively for the total output load capacitance and the I/O coupling capacitance.

In order to validate the first order model of the switching current waveform of CMOS gate, we did compare for various cells, calculated current waveforms to that obtained with Eldo (a spice level tool). Fig.4 gives an illustration of the results obtained. It represents the switching current waveforms of an inverter (130nm) loaded by C_L= 4fF for different controlling conditions (τ_{IN} ranging from 20ps to 100ps).

As shown, the calculated current waveforms are similar to that obtained with Eldo simulation tool. The proposed model (implemented in matlab tool) can thus

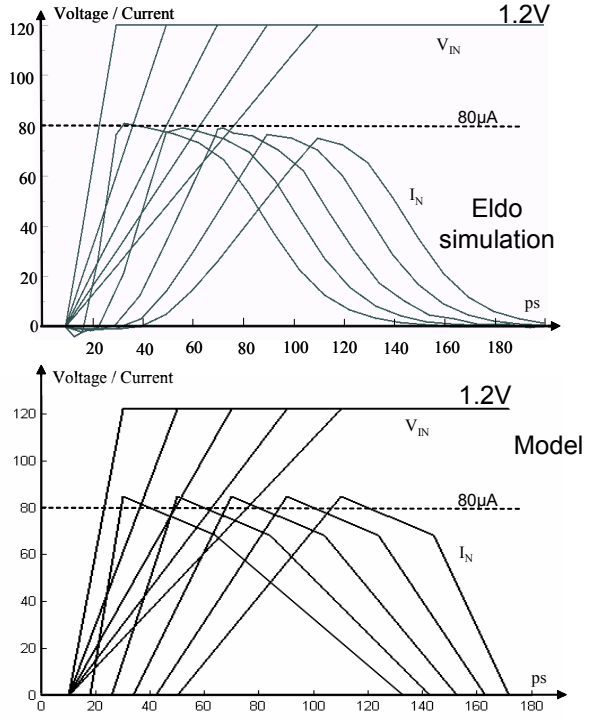


Figure 4. Simulated and calculated I,V waveforms of an inverter.

be exploited to evaluate the contribution of any CMOS cell to the DPA signature of any dual rail circuit.

IV. SWITCHING CURRENT IMBALANCE MODEL

The DPA signature of a dual rail circuit or logic block is, as established in [6], the sum of all the contributions of the standard cells constituting it. The key question is then what is the contribution of a single cell to the global signature of a circuit.

Neglecting the structural correlations introduced by the schematic of the logic block under consideration, the contribution of a cell is just the difference between the current profiles obtained when the gate settles respectively a valid '1' and a valid '0' on its differential output. In order to determine in paragraph V the validity domain of the three assumptions supporting the claim that the dual rail logic is intrinsically robust to DPA attacks, let us model the maximum amplitude of this difference (I^S_{MAX}) for different loading and controlling conditions.

A. Unbalanced output loads (Assumption n°3)

Considering for simplicity the reduced dual rail cell representation of Fig.2, first we have evaluated the effects of having unbalanced capacitance (C_1 and C_2) values on each wire of one differential output. More precisely, we have evaluated the maximum amplitude I^S_{MAX} of the difference between the current profiles associated to the settling of logic '1' and '0' respectively. Based to expressions (1-8) and with respect to the C_2/C_1 ratio, we have deduced two different expressions for I^S_{MAX}:

$$I^S_{MAX} = \frac{I_1(1-\beta)}{\left(\frac{V_{DD}}{V_{DSAT}} - 1\right)} \cdot \left(\frac{C_2}{C_1} - 1\right) \quad \text{if} \quad 1 < \frac{C_2}{C_1} < \frac{V_{DD}}{V_{DSAT}} \quad (9)$$

$$I^S_{MAX} = I_1 \cdot \left(1 - \frac{\beta . V_{dd}}{V_{dsat}} \cdot \frac{C_1}{C_2}\right) \quad \text{if} \quad \frac{C_2}{C_1} > \frac{V_{DD}}{V_{DSAT}} \quad (10)$$

Where β is the ratio between I_1 (1) and I_2 (2). Note that all other parameters have already been previously defined.

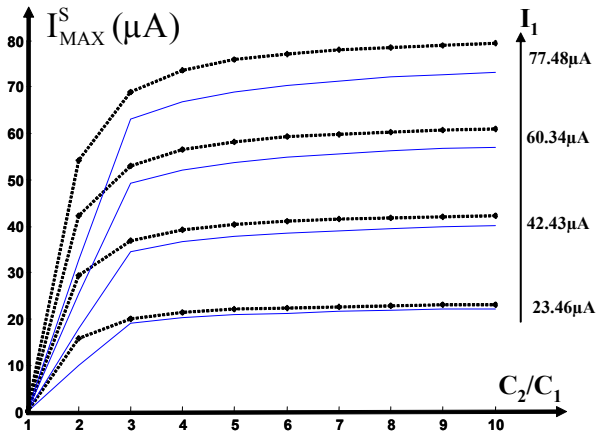


Figure 5. Simulated and calculated values of I^S_{MAX} vs C_2/C_1

Fig.5 shows the simulated and calculated evolutions of I^S_{MAX} with respect to C_2/C_1 (C_1=4fF). The considered transition time value of the input signal triggering the switching was 50ps. Considering Fig.5, one can conclude that the accuracy of expressions (9) and (10) is satisfactory.

B. Unbalanced input transition times (Assumption n°1)

In a second step, we did investigate the effect of unbalanced input transition times, i.e. on unbalanced values of τ_1 and τ_2 (Fig.2). Following the same reasoning than in the previous paragraph, we have obtained the expression of I^S_{MAX}:

$$I^S_{MAX} = \min\left\{K \cdot \frac{W}{DW} \cdot V_{DD} \cdot \left(1 - \frac{\tau_1}{\tau_2}\right); I_1\right\} \quad (11)$$

where τ_1 and τ_2 are the transition time values of the signals driving respectively INV1 and INV2. To illustrate the validity of expression (11), we have plotted on Fig.6 the simulated and calculated evolutions of I^S_{MAX} with respect to τ_2/τ_1 values for cmos inverters designed in a 130nm process (τ_1=50ps, C_1=C_2=4fF). As shown the accuracy of expression (11) is satisfactory.

C. Unbalanced arrival times (Assumption n°2)

In a last step, we did investigate the effect of unbalanced input signal arrival times (input transition times and output loads being perfectly balanced: τ_1=τ_2=τ and C_1=C_2). As in the two preceding paragraphs, we have deduced from the modelling of the switching current waveform the expression of I^S_{MAX}:

$$I^S_{MAX} = \min\left\{K \cdot \frac{W}{DW} \cdot \left(\frac{V_{DD} \cdot \Delta}{\tau}\right); I_1\right\} \quad (12)$$

where Δ is the difference between the arrival time values of the input signals controlling respectively INV1 and INV2. The other parameters have already been defined in previous paragraph.

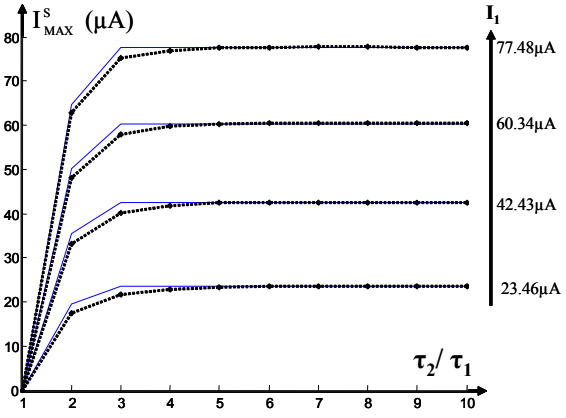


Figure 6. Simulated and calculated values of I^S_{MAX} vs τ_2/τ_1

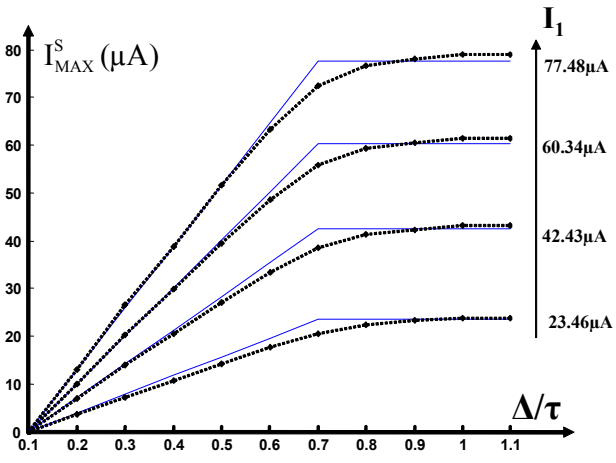


Figure 7. Simulated and calculated values of I^S_{MAX} vs Δ/τ

To validate the expression (12), we have plotted in Fig.7 the simulated and calculated evolutions of I^S_{MAX} with respect to the Δ/τ ratio and for different values of I_1. As shown, the difference between the simulated and calculated values is very small, so one can conclude that the precision of expression (12) is satisfactory.

V. DESIGN CRITERIA AND DISCUSSION

Up to this point, we have developed a first order model of the switching current waveform. Then, we have deduced expressions of the maximum amplitude of the difference I^S_{MAX} between the current profiles associated to the settling of logic '1' and '0' respectively. In this section, we're going to exploit these expressions to determine (quantify) the validity domain of assumptions 1 trough 3. Defining I_{TH} as the smallest current imbalance that can be monitored with a given amount of current profiles measures, it is now possible to quantify the imbalances that can be tolerated at both the input **(assumption 1 and 2)** and the output **(assumption 3)** of a dual rail gate.

A. Unbalanced output loads (Assumption n°3)

Equating expressions (9) and (10) to I_{TH}, it is possible to define the critical ratio value $(C_1/C_2)_{Crit}$ below which the induced current imbalance can be successfully captured by a differential power analysis (if I_1>I_{TH}):

$$\left.\frac{C_1}{C2}\right|_{Crit} = \min\left\{\left(\frac{I_{TH}}{I_1} \cdot \frac{\frac{V_{DD}}{V_{DSAT}} - 1}{(1-\beta)} + 1\right)^{-1}; \frac{V_{DSAT}}{\beta \cdot V_{DD}}\left(1 - \frac{I_{TH}}{I_1}\right)\right\} \quad (13)$$

Fig.8 illustrates the calculated and simulated evolutions of $(C_1/C_2|_{Crit})$ with respect to I_1 for different I_{TH} values. The simulated values have been obtained for inverters, nand2 gates and latches. As shown the accuracy of expression (13) is satisfactory. Note that the grey area of the figure is a direct illustration of the benefit of dual rail logic over single rail one (for I_{TH}=20µA).

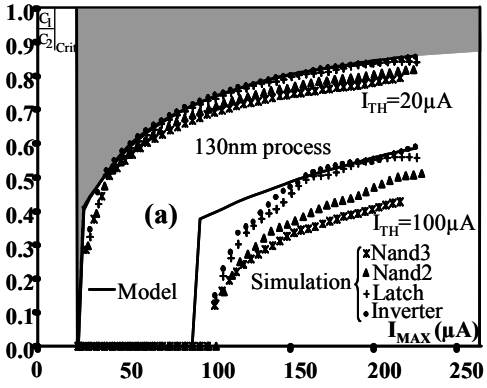


Figure 8. $C_1/C_2\,|_{Crit}$ vs $I_1=I_{MAX}$ for two different I_{TH} values

Considering the validity of **assumption n°3**, one can conclude that there is no absolute value of C_1/C_2 ratio above which all dual rail gates can be considered as robust. However according to (13) one can note that the more current (I_1) one gate can deliver, the closer from one is $(C_1/C_2)_{Crit}$, i.e. the less robust to DPA the gate is.

B. Unbalanced input transition times (Assumption n°1)

Following the same reasoning than in the preceding paragraph, we have obtained the transition time imbalance that can be tolerated at the gate inputs:

$$\left.\frac{\tau_1}{\tau_2}\right|_{Crit} = 1 - \frac{I_{TH}\cdot(V_{DD}-V_T)}{I_1\cdot V_{DD}} \text{ if } I_1 > I_{TH} \qquad (14)$$

Fig.9 shows the calculated and simulated evolutions of $(\tau_1/\tau_2)_{Crit}$ with I_1 for different I_{TH} values. The simulated values have been obtained for inverters, 2-inputs nand gates and latches. As illustrated by Fig. 9, the accuracy of expression (14) is satisfactory. With other respects, expression (14) allows to conclude that the more current (I_1) a gate can deliver, the less robust to DPA attacks the dual rail gate is. Note that the hachured area corresponds to the secure design space for I_{TH}=20µA.

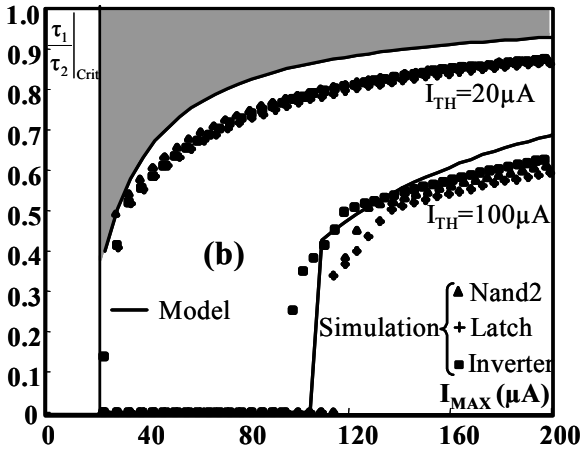


Figure 9. $\tau_1/\tau_2\,|_{Crit}$ vs $I_1=I_{MAX}$ for two different I_{TH} values

C. Unbalanced arrival times (Assumption n°2)

The arrival time imbalance that can be tolerated at the input of a dual rail cell has been obtained following the same reasoning than in the two preceding paragraphs:

$$\left|\frac{\Delta}{\tau}\right|_{Crit} = \frac{I_{TH}\cdot(V_{DD}-V_T)}{I_1\cdot V_{DD}} \text{ if } I_1 > I_{TH} \qquad (15)$$

where $\tau=\tau_1=\tau_2$ is the input transition time value of all the incoming signals (see Fig. 2). Note that in this expression Δ may have value ranging from [$-\tau$ to $+\tau$].

Fig.10 represents the calculated and simulated evolutions of $(\Delta/\tau)_{Crit}$ with I_1 for different I_{TH} values. As shown the accuracy of expression (15) is satisfactory.

Considering expression (15), it appears that **assumption n°2** is really a crude assumption. Let us consider a dual nand2 gate characterized by a value of I_1 equal to 80µA. Assuming that the outputs loads (C_1 and C_2) are identical, we may conclude, accordingly to (15), that the arrival time imbalance must not be greater than 0.8 times the transition time value of the incoming signal (I_{TH}=100µA). This is quite small considering that typical τ values are ranging from 20ps to 200ps.

D. Discussion

From the preceding expressions and results, it appears that there is effectively a design range within which dual rail logic can be considered as robust to DPA attacks. However, this design space appears for the 130nm process under consideration quite narrow since the tolerable load, input transition and arrival time imbalances are quite small especially for the arrival time imbalance.

In the previous paragraphs we have often concluded that the smaller is the current value (I_1), the more robust is the dual rail cell against DPA attacks. Consequently, one possible solution to enlarge this secure design range seems to work with reduced supply voltage values since it induces smaller current values (I_1). However, such an approach imposes to manage properly the power (security) versus timing trade off (speed).

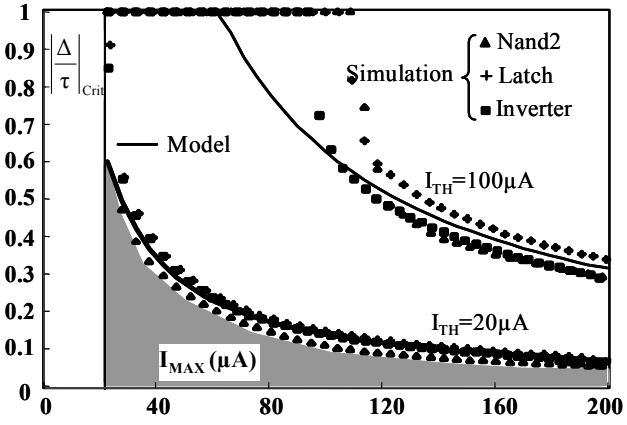


Figure 10. $|\Delta/\tau|_{Crit}$ vs $I_1=I_{MAX}$ for two different I_{TH} values

Considering once again the narrowness of the secure design range, it appears mandatory to develop dedicated tool and/or design solutions to properly balance not only the parasitic capacitances introduced during the place and route as proposed [9], but also tools and/or design solutions to properly balance the transition and arrival time values. Within this context expressions (13) trough (15) constitute clever design criteria to evaluate the dangerousness of a dual rail cell within a dual rail circuit.

VI. CONCLUSION

In this paper a first order switching current model has been introduced. Based on this analytical model, an investigation of the dual rail logic robustness against DPA attacks has been carried out. It has allowed identifying the design range in which dual rail logic can be considered as robust. For the 130nm process under consideration, the identified secure design range appears to be quite narrow for the nominal supply voltage value. However the results obtained suggest that it is possible to significantly enlarge it by using reduced supply voltage values.

REFERENCES

[1] P. Kocher and al. “Differential power analysis”. CRYPTO'99, Lecture Notes in Comp. Science, vol. 1666, pp. 388-397.

[2] D. Suzuki and al. ”Random Switching Logic: A Countermeasure against DPA based on Transition Probability”, Cryptology ePrint Archive, 2004/346, http://eprint.iacr.org/complete/

[3] D. Sokolov and al. "Design and Analysis of Dual-Rail Circuits for Security Applications," IEEE Trans. on Computers, vol. 54, no. 4, pp. 449-460, April, 2005.

[4] S. Guilley and al. ”CMOS structures suitable for secured hardware”. Design, Automation and Test in Europe Conference and Exposition.

[5] J. Fournier and al. “Security Evaluation of Asynchronous Circuits”, Workshop on Cryptographic Hardware and Embedded Systems, 2003.

[6] G. F. Bouesse and al. "DPA on Quasi Delay Insensitive Asynchronous Circuits: Formalization and Improvement," Design, Automation and Test in Europe, pp. 424-429, Vol. 1, 2005.

[7] A. Razafindraibe and al. “Secured structures for secured asynchronous QDI circuits” in XIX Conference on Design of Circuits and Integrated Systems (DCIS’04), Nov. 24-26, 2004

[8] K. Tiri and al. “Securing encryption algorithms against DPA at the logic level: next generation smart card technology”, Cryptographic Hardware and Embedded Systems Workshop, September 8-10, 2003

[9] K. Tiri and al. "A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs," date, pp. 58-63, Design, Automation and Test in Europe (DATE'05) Volume 3, 2005.

[10] F. Mace and al. “A dynamic current mode logic to counteract power analysis attacks”, DCIS 2004.

[11] P. Maurine and al, "Transition time modeling in deep submicron CMOS" IEEE Trans. on CAD, vol.21, n11, pp.1352-1363, 2002.

[12] K.O. Jeppson. “Modeling the Influence of the Transistor Gain Ratio and the Input-to-Output Coupling Capacitance on the CMOS Inverter Delay”, IEEE JSSC, Vol. 29, pp. 646-654, 1994.

[13] T. Tsividis. “Operation and Modeling of the Mos Transistor”, Oxford University Press, 1999.

[14] T. Sakurai and al. "Alpha-power law MOSFET model and its applications to CMOS inverter delay and other formulas", IEEE J. Solid-State Circuits, vol. 25, pp. 584-594, April 1990.

[15] Jens Sparso and al. “Principles of Asynchronous Circuit Design: A Systems Perspective”, Kluwer Academic Publishers.