A Model of DPA Syndrome and Its Application to the Identification of Leaking Gates

Alin Razafindraibe, Philippe Maurine

▶ **To cite this version:**

Alin Razafindraibe, Philippe Maurine. A Model of DPA Syndrome and Its Application to the Identification of Leaking Gates. PATMOS: Power And Timing Modeling, Optimization and Simulation, Sep 2007, Gothenburg, Sweden. pp.394-403, ⟨10.1007/978-3-540-74442-9_38⟩. ⟨lirmm-00175108⟩

HAL Id: lirmm-00175108

https://hal-lirmm.ccsd.cnrs.fr/lirmm-00175108v1

Submitted on 14 Sep 2019

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.

HAL Authorization

A Model of DPA Syndrome and Its Application to the Identification of Leaking Gates

A. Razafindraibe and P. Maurine

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

Abstract. Within the context of secure applications, side channel attacks are a major threat. The main characteristic of these attacks is that they exploit physical syndromes, such as power consumption rather than Boolean data. Among all the known side channel attacks the differential power analysis appears as one of the most efficient. This attack constitutes the main topic of this paper. More precisely, a design oriented modelling of the syndrome (signature) obtained while performing Differential Power Analysis of Kocher is introduced. As a validation of this model, it is shown how it allows identifying the leaking nets and gates during the logical synthesis step. The technology considered herein is a 130nm process.

1 Introduction

If there are many side channel attacks, the differential power analysis [1] appears as a major threat since it requires less material than others attacks, such as fault injection, to be successfully implemented. Due to its dangerousness, many countermeasures have been proposed in former works. Among those countermeasures, one can find techniques aiming at reducing the correlation between the power consumption and the data processed, by appending randomness within the circuit. Time randomization of the computations [2], random permutation of datapaths [3], random data insertion [4] are some examples of countermeasures adopting this approach.

There is a second approach. It aims also at reducing or masking all the potential sources of correlation rather than appending randomness in the circuit. Smoothing the variations of the current flowing through the supply rails using ad-hoc on chip circuits is one possible countermeasure [5], whereas using redundant logic, such as dual rail logic, is another technique adopting this second approach [6].

If many works have proposed countermeasures against differential power analysis, no effort has been devoted to the development of a physical oriented modelling of the DPA syndrome. More precisely, only little physical information related to what is the DPA syndrome is available in the literature to our knowledge. This lack of design oriented information is prejudicial, since designers may only rely on their own experience to evaluate, before fabrication, the robustness of their design against DPA.

In this paper, a design oriented modelling of the DPA syndrome is introduced. This is the main contribution of the paper. To validate the aforementioned modelling, the

N. Azemard and L. Svensson (Eds.): PATMOS 2007, LNCS 4644, pp. 394–403, 2007.
© Springer-Verlag Berlin Heidelberg 2007

latter is applied to identify, during the logical synthesis step, the critical gates in term of DPA, i.e. the gates that contribute the more to the DPA syndrome. This application will lead us to define the concept of critical gate. This is the second contribution of this work.

The remainder of this paper is organized as follows. A brief review of the different differential power analysis available in the literature is given in section 2. The design oriented modelling of the DPA syndrome is then introduced in section 3. Finally the latter is applied in section 4 to the identification of critical gates, and a conclusion drawn in section 5.

2 Different Differential Power Analyses

There is not only one differential power analysis but several. In this section we briefly sum up the basics of two of them. The first one is the differential power analysis introduced by P. Kocher in its seminal paper [1]. It will be denoted by DPA of Kocher in the remainder of the paper. The second one [2] is a generalisation to a larger target of the attack introduced in [1]. It will be denoted by multi-bits DPA subsequently. These two attacks constitute the historical approach of the power consumption analysis. A second approach has been suggested in various papers [2,10,11]. The latter proposed to use the correlation factor between the power samples and either the Hamming weight or the Hamming distance of the manipulated data to retrieve the secret key. Attacks falling within this second approach are not considered in the remainder of this paper.

2.1 Differential Power Analysis of Kocher

The differential power analysis introduced by P. Kocher in [1] is based on the fact that the power consumed by a ciphering circuit depends strongly on the manipulated data. This attack is usually performed in three steps: *data collection, data sorting and data analysis.*

Data collection consists in sampling and recording the current flowing through the ground or supply pad of the circuit under attack. This is done for a large number of cryptographic operations leading to an important collection of current or power traces.

Data sorting consist in extracting, for all possible guesses of key k_g, two sets of power traces. This tow sets $S_{\cdot 0,}^{kg}$ and $S_{\cdot 1,}^{kg}$ are defined considering the expected value of the bit under attack. Let us assume that the bit z is the target of differential power analysis of Kocher. In this case, $S_{\cdot 1,}^{kg}$ ($S_{\cdot 0,}^{kg}$) contains all the power samples corresponding to input plain texts expected to force z to '1' ('0') according to the guess of the key k_g.

Data analysis consist in computing in a first step, for all possible values of k_g, the average power samples $<S_{\cdot 0,}^{kg}>$ and $<S_{\cdot 1,}^{kg}>$ of sets $S_{\cdot 0,}^{kg}$ and $S_{\cdot 1,}^{kg}$. In a second step, differences $<S_{\cdot 0,}^{kg}> - <S_{\cdot 1,}^{kg}>$ are evaluated for all kg values resulting in a collection of kg differential power traces. Among these kg differential traces, one corresponds to the correct secret key k_r. The latter is usually, but not necessarily disclosed, by identifying the guess k_g leading to the curve with the highest amplitude.

The above protocol allowing performing a DPA of Kocher may be formalized in order to obtain a mathematical expression of the DPA syndrome, S_{DPA}. Let us consider that an attack is performed on the bit z of a ciphering block. Let $V \in \mathcal{V}$ be the number of plain texts (input vectors) applied on the inputs of the block. Let $T_{kg} \in \mathcal{T}_{kg}$ be the number of vectors of $\mathcal{V}$ expected to force z to the logic value '1' according to the guess value kg of the key. Let $F_{kg} \in \mathcal{F}_{kg}$ ($F_k = V - T_k$) be the number of plain text (input vectors) expected to forced z to the logic value '0'. Finally, let $I_v(t)$ be the courant waveform observed either on the ground or supply rail while the vector $v \in \mathcal{V}$ is applied on the block inputs. With such definitions, one can demonstrated that the syndrome DPA associated to the guess k_g is

$$S_{DPA}(z, k_g) = \frac{1}{T_{k_g}} \cdot \sum_{t \in T_{k_g}} I_t(t) - \frac{1}{F_{k_g}} \cdot \sum_{f \in F_{k_g}}^{f} I_f(t) \tag{1}$$

This expression is valid for all possible values of the key and therefore for the correct key k_r. We therefore may conclude that the DPA of Kocher will disclose the secret key if $S_{DPA}(z,k_r)$ has a greater amplitude than $S_{DPA}(z,k_g)$ for all other possible values of the key. Although this formalism allows understanding quickly what a DPA of Kocher is, it does not provide any physical information about what to do or not to increase the robustness of a circuit during the design.

2.2 Multi-bit DPA

As aforementioned, the Multi-bit DPA is a generalisation of the DPA of Kocher. Indeed, the main difference between the two attacks lies in their respective target. Thus a multi-bit DPA is roughly performed as a DPA of Kocher, i.e. following the same three steps: *data collection, data sorting and data analysis.*

However, the data sorting step is slightly different. Indeed, sorting the power samples is done according to the expected values of *m* target bits rather than the value of a single bit. As an example, let us consider that a multi-bit DPA targets two bits namely x and z. In this case, the sorting consists in defining two sets of power traces $S_{'00'}^{kg}$ and $S_{'11'}^{kg}$ accordingly to the guessed value kg of the key. $S_{'00'}^{kg}$ ($S_{'11'}^{kg}$) contains all the power traces corresponding to input vectors expected to force x and z to the logic value '0' ('1'). Note that this sorting leads to not exploit all the data collected during the data collection step unlike in the case of a DPA of Kocher.

The protocol allowing performing a multi-bit DPA may also be formalized to obtain a mathematical expression of the multi-bit DPA syndrome. In the case of an attack targeting two bits namely x and z, the formalization leads to:

$$S_{DPA}(x, z, k_g) = \frac{1}{T'_{k_g}} \cdot \sum_{t \in T'_{k_g}} I_t(t) - \frac{1}{F'_{k_g}} \cdot \sum_{f \in F'_{k_g}} I_f(t) \tag{2}$$

where $T'_k < T_k$ and $F'_k < F_k$ are respectively the numbers of vectors of V forcing (x,z) to the value '11' et '00'.

3 Design Oriented Modelling of DPA Syndrome

In the preceding section, the basic protocols to perform a differential power analysis of Kocher or a multi-bit one have been summarized. These protocols have been formalized to obtain a mathematical expression of the DPA syndrome. However the expression obtained does not give circuit designers insight into what should be done or not to obtain a robust circuit. This explains why a first order physical model of the DPA syndrome is introduced in this section.

Whatever differential power analysis we did consider (DPA of Kocher or multi-bit DPA), we did obtain, in section 2, a generic expression of the DPA syndrome for all possible guessed value of the key. For the correct secret key, this expression may be re-written:

$$S_{DPA}(C,k_r) = \frac{1}{T_{k_r}} \cdot \sum_{t \in T_{k_r}} I_t(t) - \frac{1}{F_{k_r}} \cdot \sum_{f \in F_{k_r}} I_f(t) \tag{3}$$

where C denotes the target of the attack, i.e. a single bit or *m* different bits. Considering that the power trace $I_t(t)$ (or $I_f(t)$) is the sum of the currents provided to, or drained from, the supply (or ground) rail when the vector *t (f)* of $\mathcal{T}_{k_r}$ ($\mathcal{F}_{k_r}$) is applied on the inputs of the ciphering block, expression (3) may be rewritten:

$$S_{DPA}(C,k_r) = \frac{1}{T_{k_r}} \sum_{t \in T_{k_r}} \sum_{p \in P} i_p^t(t) - \frac{1}{F_{k_r}} \sum_{f \in F_{k_r}} \sum_{p \in P} i_p^f(t) \tag{4}$$

where *p* denotes the gate *p* among the P gates constituting the block under attack and $i_p^t(t)$ ($i_p^f(t)$) is the current drained from the supply (or ground) rail while the vector *t (f)* of $\mathcal{T}_{k_r}$ ($\mathcal{F}_{k_r}$) is applied on its inputs. Applying the vector *t (f)* on the inputs of the block may produce three different events at the output s_p of the gate *p*, that is to say: s_p remains stable, s_p switches from the logic value '0' to the logic value '1' and s_p switches from the logic value '1' to the logic value '0'. This leads to define six different numbers that characterize the behaviour of the gate *p* during the differential power analysis: f_p^0, f_p^1, f_p^S, t_p^0, t_p^1 and t_p^S. These numbers are defined as follows:

- f_p^0, f_p^1 are the numbers of vectors of $\mathcal{F}_{k_r}$ inducing a falling and rising transitions of s_p *respectively,*
- in the same way, t_p^0, t_p^1 are the numbers of vectors of $\mathcal{T}_{k_r}$, inducing a falling and rising transitions of the s_p *respectively*
- and finally f_p^S *and* t_p^S are respectively the numbers of vectors of $\mathcal{F}_{k_r}$ and $\mathcal{T}_{k_r}$ that let the output s_p of gate *p* unchanged.

Considering these definitions, we did obtain the following expression of DPA syndrome, with equivalent expressions for wrong guess of the key:

$$S_{DPA}(C,k_r) = \sum_{p \in P} \left\{ \begin{array}{l} \left(\frac{t_p^1}{T_{k_r}} - \frac{f_p^1}{F_{k_r}} \right) \cdot i_p^1(t) + \left(\frac{t_p^0}{T_{k_r}} - \frac{f_p^0}{F_{k_r}} \right) \cdot i_p^0(t) \\ + \left(\frac{t_p^S}{T_{k_r}} - \frac{f_p^S}{F_{k_r}} \right) \cdot i_p^S(t) \end{array} \right\} \tag{5}$$

where $i_p^0(t)$, $i_p^1(t)$ and $i_p^S(t)$, are the currents provided to or drained from the supply (or ground) rail while the output s_p of gate p switches from '1' to '0', '0' to '1' or remains stable, respectively. Assuming that the switching current $i_p^S(t)$ of the gate p is negligible if its output remains stable, (5) can be simplified:

$$S_{DPA}(C,k_r) = \sum_{p\in P}\left\{\begin{array}{l}\left(\frac{t_p^1}{T_{k_r}} - \frac{f_p^1}{F_{k_r}}\right)\cdot \Delta i_p^{V_{DD}}(t) \\ -\left(\frac{t_p^1 - t_p^0}{T_{k_r}} + \frac{f_p^1 - f_p^0}{F_{k_r}}\right)\cdot i_p^0(t)\end{array}\right\} \\ = \sum_{p\in P}\left\{\begin{array}{l}\left(\frac{f_p^1}{F_{k_r}} - \frac{t_p^1}{T_{k_r}}\right)\cdot \Delta i_p^{Gnd}(t) \\ -\left(\frac{t_p^0 - t_p^1}{T_{k_r}} + \frac{f_p^0 - f_p^1}{F_{k_r}}\right)\cdot i_p^1(t)\end{array}\right\} \quad (6)$$

where $\Delta i_p^{VDD}(t)$ and $\Delta i_p^{Gnd}(t)$ are called the differential switching currents and are:

$$\Delta i_p^{V_{DD}}(t) = i_p^1(t) - i_p^0(t) \quad \Delta i_p^{Gnd}(t) = i_p^0(t) - i_p^1(t) \quad (7\text{-}8).$$

At this point, it is important to decide if the power traces are obtained by probing the supply rail V_{DD} or the ground rail Gnd. Let us consider that the measures are done on the V_{DD} rail. In this case, $i_p^0(t)$ can be considered as small compared to $\Delta i_p^{VDD}(t)$ since only the short circuit current is drained from the supply rail. Simplifying expression (6), we finally obtain the DPA syndrome associated with a DPA performed on the supply rail V_{DD}.

$$S_{DPA}^{V_{DD}}(C,k_r) = \sum_{p\in P}\left\{\left(\frac{t_p^1}{T_{k_r}} - \frac{f_p^1}{F_{k_r}}\right)\cdot \Delta i_p^{V_{DD}}(t)\right\} = \sum_{p\in P}\left\{\varepsilon_p^{VDD}\cdot \Delta i_p^{V_{DD}}(t)\right\} \quad (9)$$

In the same way, one can show that the DPA syndrome associated to a DPA performed on the ground rail can be expressed as:

$$S_{DPA}^{Gnd}(C,k_r) = \sum_{p\in P}\left\{\left(\frac{t_p^0}{T_{k_r}} - \frac{f_p^0}{F_{k_r}}\right)\cdot \Delta i_p^{Gnd}(t)\right\} = \sum_{p\in P}\left\{\varepsilon_p^{GND}\cdot \Delta i_p^{Gnd}(t)\right\} \quad (10)$$

Considering (9) and (10), one may conclude that the DPA syndrome, associated to the DPA of Kocher or to the multi-bit PA, are linear combinations of the differential switching currents of all gates. One important point here is to note that the multiplicative coefficients ε_p^{VDD} and ε_p^{Gnd} are independent of the physical implementation of the block since they are only function of the numbers of rising and falling transitions. Therefore they only depend on the logical structure of the block and can thus be evaluated during the logic synthesis step. Note also that the coefficients of the gates controlling the m bits targeted by the attack are necessarily equal to one if the guessed value of the key is the right one.

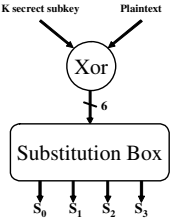

Fig. 1. Structure considered during the validation step

In a similar way, the differential switching currents do depend only on the physical synthesis (place and route …) of the circuits. Indeed, $\Delta i_p^{VDD}(t)$ depends strongly on various physical design parameters such as: the load driven by p, the transition times of the signals driving p, the sizing of gate p.

From the preceding remarks, we may conclude that the proposed model establishes a link between the DPA syndrome and both the logic and physical synthesis. In order to demonstrate the interest of such a link, we show, in the next section, how to apply this model to identify the leaking gates, i.e. the gates that contribute the more to the DPA syndrome.

4 Leaking Gates Identification

In order to validate the proposed modelling of the DPA syndrome and to demonstrate its usefulness, we apply it, in this section, to identify just after the logic synthesis the critical gates and nets of a verilog netlist. At this point, a critical gate is a gate that contributes more than the others to the DPA syndrome. The application example considered in this section is the well known substitution box of the DES algorithm [13] represented in Fig.1.

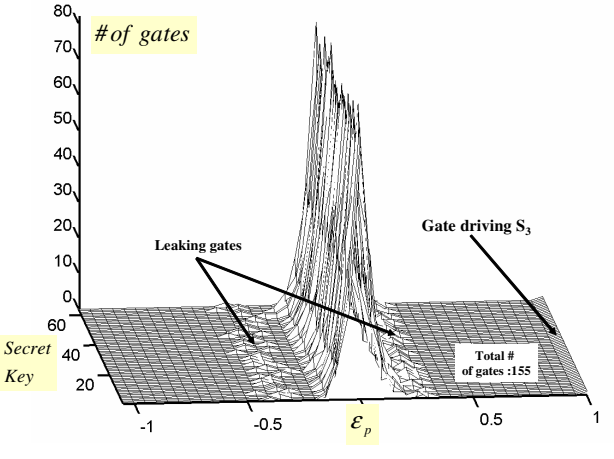

Fig. 2. Distribution of ε_p^{VDD} values with respect for all possible keys

4.1 ε_p^{VDD} Distribution Analysis

The logical synthesis of the structure represented Fig.1 has been performed with RTL encounter from Cadence [8]. It has been done with a reduced 130nm standard cell library containing only simple gates such as inverters, (n)and2, (n)and3, (n)and4, (n)or2, (n)or3 and finally (n)or4.

The verilog file [12] obtained after synthesis has been simulated with the hdl code simulator NCsim [8]. More precisely, a unique sequence of five thousands vectors (plain texts) has been applied to the structure represented Fig.1 for all possible values of the sub-key K. These simulations have provided the five thousands final logical values of all nets. These values have been stored in .csv files that are readable by Matlab [9]. Matlab scripts have been developed in order to be able to quickly compute the values of the coefficients ε_p^{VDD}.

Fig.2 gives the histogram of the ε_p^{VDD} for all the gates and all the possible correct keys while a DPA of Kocher targeting the output bit S_3 (see Fig.1) is performed. As shown, the coefficient of the gate driving S_3 is equal to 1. Beside this expected result, one can note that most (>95%) have a coefficient value ranging from -0.2 to 0.2 while two gates have an absolute coefficient value $|\varepsilon_p|$ greater than 0.2 and this for all possible value of the correct key. These gates (denoted by cg1 and cg2) have been identified. Their main characteristic is to be located (in term of logical depth) close to the gate driving the output net S_3. More precisely, the logic depth separating the inputs of these gates and the net S_3 was found smaller or equal to 2. These two gates are indicated as leaking gates on Fig.2 since they may contribute more than others gates to the DPA signature, according to the model introduced in section 3.

4.2 DPA Syndrome Analysis

The analysis of the ε_p^{VDD} histogram has indicated that gates cg1 and cg2 are critical or leaking gates, according to the DPA syndrome modelling. In order to validate the model, we have verified the validity of this result at the electrical level. We therefore generated from the verilog description three different spice netlists of the structure represented Fig.1.

The first generated netlist was a direct transcription of the verilog file description into a spice netlist. The resulting netlist is denoted by '*n_ref*' afterward.

The second and third netlists are modifications of the reference netlist *'n_ref'*. More precisely, *'n_ref'* has been first modified in order to multiply by three the current drained from the V_{DD} rail by the critical gates cg1 and cg2. The resulting netlist is called *'n_crit'* afterward. Finally *'n_ref'* has been modified in order to multiply by three the current drained from the V_{DD} rail by two gates having a ε_p^{VDD} close to zero, i.e. uncritical gates. The resulting netlist is called *'n_not_crit'*.

The multiplication of the current drained by these critical and uncritical gates was not done by sizing three times bigger the P transistors. We rather used courant controlled current source (CCCS in spice format) as shown Fig.3. This solution was chosen since it warrants to no change at all the behaviour of the rest of the circuit. Therefore any change of the DPA syndrome will only be due to the multiplication by three of the current drained from V_{DD} by the modified gates.

These modifications done, we simulated the three netlists. More precisely, a given sequence of two thousand vectors has been applied to these three structures for all possible values of the correct key. As a result, 64*2000 power traces have been collected. These traces have been used to perform, by simulation, a DPA of Kocher targeting the bit S_3. The DPA syndromes obtained with the three different netlists were compared. More precisely, we compared the DPA syndromes obtained with critical and uncritical netlists *('n_crit'* and *'n_not_crit'*) to the DPA syndrome obtained with the reference netlist *'n_ref'*. Fig.4 gives the differences obtained for 32 different values of the correct key.

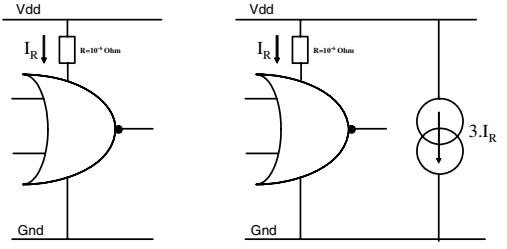

Fig. 3. Modifications done on two critical an uncritical gates

As expected, the multiplication by three of the current consumed by the critical or leaking gates induces a significant modification of the DPA syndrome. As shown on Fig.4 (left), the difference may reach 80µA. This represents 100% of the maximum amplitude of the DPA syndrome obtained with the reference netlist. Conversely, the multiplication by three, of the current drained from V_{DD} by the two less critical gates, induces only small modifications of the DPA syndrome. Indeed the difference remains smaller than 15µA. Note also that the observed differences (Fig.4, right) are either positive or negative.

This means that the amplitude of the DPA syndrome could either be reduced or increased.

Beside the validation of the DPA syndrome modelling introduced in section 3, these results leads to define the criticality of gates and nets with respect to the DPA, at the logical level: ***the greater $|\varepsilon_p|$ value is, the most critical the gate p is.***

4.3 Critical and Uncritical Gates and Nets

Beside this definition, one can wonder how many gates are extremely critical in a design and how many gates are uncritical. To provide beginnings of answers to these questions we did compute, from data obtained with NCsim, the coefficients for differential power analyses of Kocher targeting all the outputs bits of the structure represented on Fig.1. As an illustration, Fig.5 gives the coefficient values of all nets (and thus all gates driving these nets) in the case of a DPA of Kocher targeting S_3. For this attack, nets n_156, n_153, n_141 and n_160 have been find the most critical.

Processing as described above for the three others output bits, we successively identified all the critical nets in case of DPA of Kocher targeting one of the four Sbox output bits. We did find only 18 (11%) extremely critical gates for a total number of

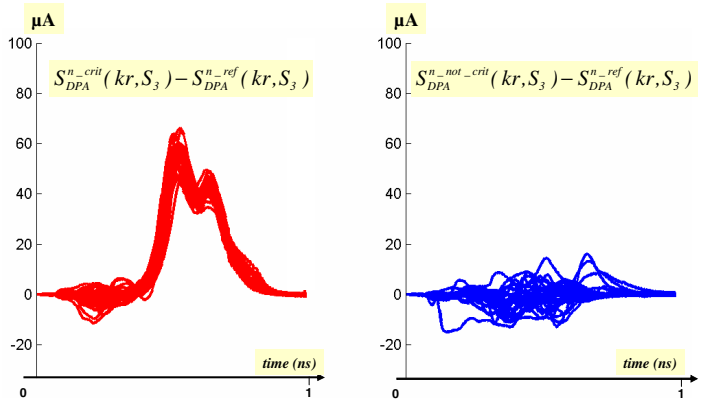

Fig. 4. Differences between the DPA syndromes obtained with the reference netlist and the critical (left) and uncritical (right)

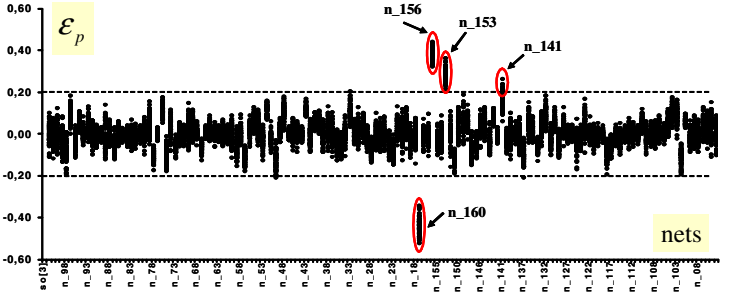

Fig. 5. ε_p values wrt net names for a DPA of Kocher targeting S_3

gates of 155. Conversely, we did find only 2 gates having an absolute coefficient value $|\varepsilon_p^{VDD}|$ smaller than 0.04. In others words, only 2 cells among 155 contribute twenty time less, to the DPA syndrome, than the cell driving the attacked bits. From these results, we may conclude that the number of extremely leaking or uncritical gates in a Sbox is small.

Since the number of critical nets and gates is small, it appears possible to constraint the place and route steps and the timing optimization in order to reduce to increase the robustness against DPA of a circuit. As an example a critical gate should be placed as close as possible from its drivers and from its loading gates. This allows reducing the time spent by the critical gate to switch by controlling both the transition times of the signal applied on its inputs and its output load. Moreover this avoids the insertion of buffers on critical nets during the timing optimization. This is extremely important since introducing a buffer on a critical net is equivalent to introduce an additional critical gate, i.e. is equivalent to increase the DPA syndrome associated to the correct secret key.

5 Conclusion

A design oriented modelling of the DPA syndrome has been introduced and validated in this paper. The definition of this modelling has lead to the definition of critical gates (and nets) with respect to DPA. Based on this definition, this model allows identifying during the logic synthesis step the gates that will contribute the more to the DPA syndrome. This advantage has been demonstrated in this paper on a well kwon example: the Sbox of a DES. The results obtained suggest that the number of leaking gates is small, at least for the considered example.

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] Daemen, J., Rijmen, V.: Resistance against implementation attacks: a comparative study of the AES proposal. In: Proceedings of the Second Advanced Encryption Standard Candidate Conference (1999)
[3] Goubin, L., Patarin, J.: DES and Differential Power Analysis, the duplication method. In: Koç, Ç.K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 3–15. Springer, Heidelberg (1999)
[4] Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Investigations of power analysis attacks on smartcards. In: USENIX workshop on Smartcard Technology (1999)
[5] Shamir, A.: Protecting Smart Card from passive power analysis with detached power supplies. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 71–77. Springer, Heidelberg (2003)
[6] Tiri, K., verbauwhede, I.: Securing encryption algorithms against DPA at the logic level: next generation smart card technology. In: ESSCIRC 2000 (2000)
[7] Messerges, T.S., et al.: Examining Smart Card Security under the Threat of Power Analysis Attack. IEEE trans. On Computer 51, 541–552 (2002)
[8] http://www.cadence.com/products/digital_ic/rtl_compiler
[9] http://www.mathworks.com/
[10] Coron, J.S., Kocher, P., Naccache, D.: Statistics and Secret Leakage. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 157–173. Springer, Heidelberg (2000)
[11] Mayer-Sommer, R.: Smartly Analysing the Simplicity and the Power of Simple Power Analysis on Smartcards. In: Paar, C., Koç, Ç.K. (eds.) CHES 2000. LNCS, vol. 1965, p. 231. Springer, Heidelberg (2000)
[12] Thomas, D., Moorby, P.: Verilog Hardware description language. Kluwer Academic Publishers, Dordrecht, http://www.whap.com
[13] DES: Data Encryption Standard, FIPS 46-2, www.itl.nist.gov/fipspub/fip46-2.htm