DIFFERENTIAL POWER ANALYSIS MODEL AND SOME RESULTS

Sylvain Guilley*, Philippe Hoogvorst* and Renaud Pacalet[†]
GET/Télécom Paris, CNRS LTCI
Département communication et électronique

** 46 rue Barrault, 75634 Paris Cedex 13, France.*

[†] *Institut Eurecom BP 193, 2229 route des Crêtes, 06904 Sophia-Antipolis Cedex, France.*
{sylvain.guilley, philippe.hoogvorst, renaud.pacalet}@enst.fr

Abstract CMOS gates consume different amounts of power whether their output has a falling or a rising edge. Therefore the overall power consumption of a CMOS circuit leaks information about the activity of every single gate. This explains why, using differential power analysis (DPA), one can infer the value of specific nodes within a chip by monitoring its global power consumption only.

We model the information leakage in the framework used by conventional cryptanalysis. The information an attacker can gain is derived as the autocorrelation of the Hamming weight of the guessed value for the key. This model is validated by an exhaustive electrical simulation.

Our model proves that the DPA signal-to-noise ratio increases when the resistance of the substitution box against linear cryptanalysis increases.

This result shows that the better shielded against linear cryptanalysis a block cipher is, the more vulnerable it is to side-channel attacks such as DPA.

Keywords: Differential power analysis (DPA), DPA model, DPA electrical simulation, substitution box (S-Box), DPA signal-to-noise ratio, cryptanalysis.

Introduction

Power attacks are side-channel attacks on cryptosystems implementing public or private key algorithms. They were first published by Kocher in 1998 [8]. Public key algorithms, like RSA, are vulnerable to simple power analysis (SPA), but can be efficiently secured by algorithmic counter-measures [11], like key and/or data blinding. Secret key algorithms, such as DES or AES, consist in the repetition of several rounds, and are thus threatened by the differential power analysis (DPA).

DPA can attack on either the first or the last round of an algorithm and requires the knowledge of either the cleartext or the ciphertext. The side-channel

exploited is the difference between the power consumed by a single gate when its output rises or falls.

Similar attacks take advantage of other types of leakage that disclose information about the internal computation. For instance, CPA [4] monitors the activity of a register: the attack exploits the fact that in CMOS logic, a gate only dissipates energy when it changes states. CPA, unlike DPA, can be modeled with the assumption that the energy dissipation is independent on the gate (either rising or falling) edge. Those attacks can also be conducted by recording a different physical quantity than the power consumption, like the electromagnetic field [6].

The rest of the article is organized as follows: Sec. 1 explains the principle of the DPA attack. In Sec. 2, we present a theoretical model for the DPA. The model is validated against exhaustive electrical simulations in Sec. 3. In Sec. 4, some results prove that the better shielded against linear cryptanalysis a block cipher is, the more vulnerable it is to side-channel attacks such as DPA.

1. Differential Power Analysis

Measuring the Consumption Bias of a CMOS Inverter

The schematic depicted on Fig. 1(*a*) has been implemented using discrete transistors to measure the instantaneous current drawn from the power source VDD and sent back to the ground VSS. Fig. 2 shows that the current I(VDD)

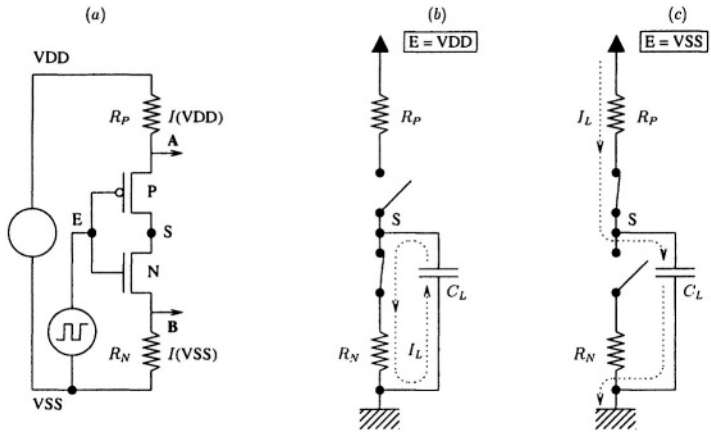

Figure 1. *(a)* Experimental setup used to measure the currents I(VDD) and I(VSS) when the output S of a CMOS inverter switches. The currents flows are illustrated in (*b*) and *(c)*.

flowing throught resistor R_P is the sum of:

- a short-circuit current, I_{short}, whose intensity is independent of the edge of the output S of the inverter and of
- a current I_L, loading a charging capacitance C_L and observed only when S rises from VSS to VDD (Fig. 1 (c)), because, otherwise, C_L discharges through R_N only (Fig. 1(b)). The capacitance C_L models both the gate output capacitance, linked to the gate fanout and to the routing wires, as well as the parasitic capacitances.

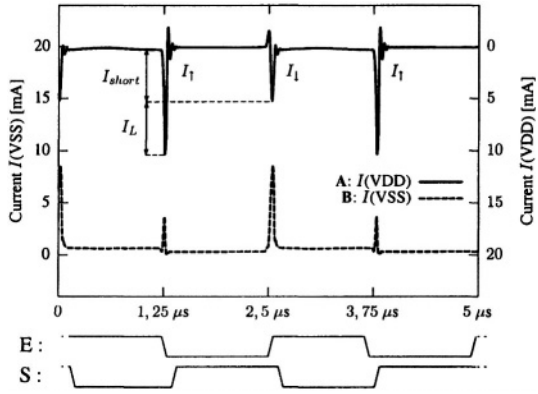

Figure 2. Measures of *I*(VDD) et *I*(VSS) of the inverter of Fig. 1 acquired by an oscilloscope.

The current *I*(VDD) depends on the edge (rising or falling) of S. We denote:

- $I_\downarrow = I_{short}$ the current observed upon a **VDD → VSS** edge and
- $I_\uparrow = I_{short} + I_L$ the one observed upon a **VSS → VDD** edge.

Principle of the DPA Attack

The analysis of the instantaneous power consumption can leak the type of operations being performed. Fig. 3 shows that the power consumption of a DES operator indicates the beginning of every encipherment.

Moreover, a more precise analysis can insulate the activity of a single gate, because:

- the instantaneous consumption of the circuit is the sum of all individual consumptions,
- each gate draws a different intensity ($I_\uparrow$ or $I_\downarrow$) according to its output edge, as shown in the previous example of the CMOS inverter.

The DPA attacks proceed in two phases. First, a large number of power consumption traces for different plaintexts[1] are recorded. Those traces contain the information about the type of edge (via a $I_\uparrow$ or $I_\downarrow$ contribution) of each gate in the design.

The second step consists in extracting this information from the traces $T_x(t)$. In the historical DPA [8], Kocher suggests to partition the traces according to the value of a particular bit i of the algorithm, which (hopefully) corresponds to a particular node in the netlist. One partition, S_0, gathers the traces $T_x(t)$, where $i = 1$, expected to contain an $I_\uparrow$ contribution, whereas the other, S_1, gathers the traces where $i = 0$. Thus the "differential trace", computed as:

$$\frac{1}{\#S_0}\sum_{T_x\in P_0} T_x(t) \; - \; \frac{1}{\#S_1}\sum_{T_x\in P_1} T_x(t)$$

reveals the $I_\uparrow - I_\downarrow$ power consumptions of the target gate i. This *modus operandi* can be used as an oracle to validate or invalidate an assumption. The DPA attack consists in testing whether the differential trace feature a singularity (peak) when analyzing the consumption of a gate i whose unknown state is guessed by making an hypothesis on a secret (typically a part of a round key). When the hypothesis on the key is correct, the differential trace is expected to feature a peak, resulting from the accumulation in a coherent manner of the $I_\uparrow - I_\downarrow$ information extracted from the power traces. More precisely, the peak is expected around the date t_S when the gate switches.

Refinements on this attack have been put forward [10]. The idea is to take into account that, in CMOS technologies, a gate only dissipates power when its output switches. The traces are thus partitioned into three sets. In addition to Kocher S_0 and S_1 sets, the S_2 set contains the traces with no or little dissipated power. Only traces from the sets S_0 and S_1 are used to compute the differential traces. For the sake of clarity, and to prepare for the presentation of our DPA model, we prefer not to present DPA in terms of traces partitioning but rather in terms of traces weighting. This allows us to reformulate the definition of the differential traces as an weighted accumulation of power traces, the weights being +1, –1 and 0 for traces traces belonging to sets S_0, S_1 and S_2.

Ghost peaks in differential traces

It has been reported [4] that "ghost" peaks also appear in differential traces computed with a wrong assumption of the key. We explain in the next section that those secondary peaks can be as high as the peak for the correct key and we provide a theoretical way to compute their relative amplitude.

[1] The plaintexts need not be known: the DPA is a ciphertext-only attack.

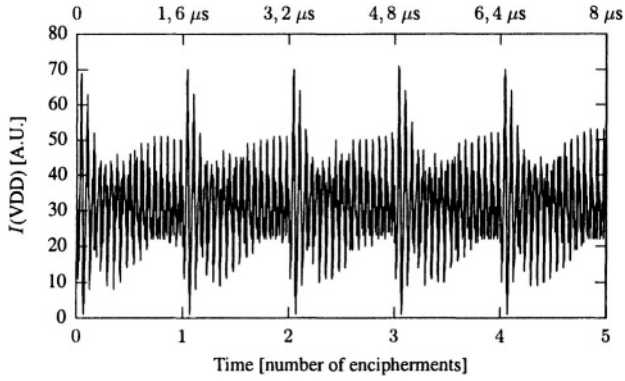

Figure 3. Power consumed by five DES encipherments (programmed in an FPGA).

2. DPA Model

Framework for DPA

Model general setup The DPA model we describe is applicable to hardware implementations of private key product ciphers. The algorithm consists in the repetition of some rounds, the first or the last one being attackable by DPA. Without any loss of generality, we focus on an attack on the last round. Fig. 4 shows the typical dataflow of one round: the "plaintext" corresponds to the intermediate message produced by the penultimate round which is mixed in the last round with the "key" to produce the "ciphertext". The last round features one non-linear function (called S-Box) and one linear function (in our case a bit-to-bit XOR-ing) with some bits of the round key k. Given a known value x and an unknown but constant key k, the value y of all the target bits $i \in [0, q[$ under investigation is derived as:

$$y = F(x \oplus k)\,. \tag{1}$$

In the original DPA [8], the value of each bit i of y is used to partition the traces so as to build differential traces. In other words, the "selection function" D introduced by Kocher is the projection of Eqn. 1 on i. In our model, the whole value of y is used to weight the traces in a view to obtain one differential trace.

As explained below, the function of Eqn. 1 applies to both AES and DES.

AES The schematic of Fig. 4 comes in a direct line from the structure of the last round of AES, with $F = S^{-1} =$ `InvSubBytes` and $p = q = 8$.

DES Fig. 5 represents a simplified dataflow of the last round of DES: the permutations and the expansion are left apart since the attacker can work around

them. The guess on the bit i (belonging to the right part of the round 15 output) comes down to a guess on a bit of the output y of the S-Box, since C_L is known to the attacker. DPA on DES is therefore a particular case of Fig. 4, where $F = S$ is the direct S-Box: $K^p \rightarrow K^q$ with $p = 6$ and $q = 4$ (we denote $K = (\{0,1\}, \oplus, \cdot)$ the field with two elements).

Fig. 5 schematic actually also applies to any Feistel cipher with constant S-Boxes, in which the attacked bit belongs to the right part of the penultimate round.

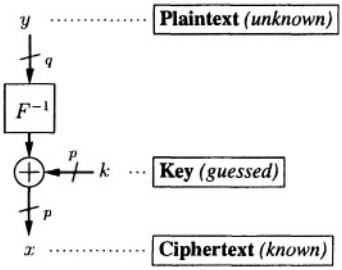

Figure 4. Schematic DPA setup.

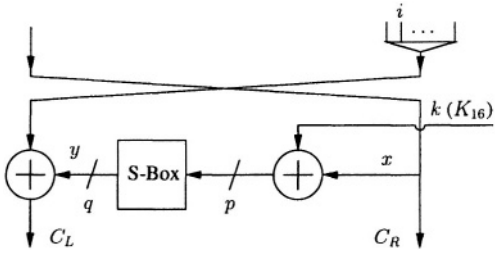

Figure 5. Simplified DES cipher flow showing a single S-Box out of 8.

Noise Sources Occurring during DPA

There are various sources of noise when doing a DPA:

N1. The activity of the rest of the circuit. This noise can be lowered by the accumulation of many independent traces. Noise spectral power vanishes as the inverse square root of the number of traces recorded.

N2. The jitter on the attacked gate. Depending on the delays in the lines and the type of edges, the switching of a gate output can happen at different dates, which leads to a loss of coherence of the trace accumulation. This is negligible for gates directly fed by registers, as their inputs are perfectly synchronized.

N3. S-Boxes themselves introduce their own bias. Measured traces slightly match the activity deduced from the computation of one plaintext bit $y_i = F_i(k \oplus \cdot)$, as described by Eqn. 1, even if the assumption on k turns out to be wrong. Although substitution box bits are designed to be independent from one another so as to block linear cryptanalysis, DPA *modus operandi* artificially introduces an inter-bit correlation. The plaintext bits y are computed all together which introduces an artificial correlation between them. This notion of S-Box "intrinsic noise" is in-

vestigated in the next section. It is also called "ghost peaks" in [4] and "algorithmic noise" in [10].

DPA Intrinsic Noise

The "DPA signal": a model for the differential traces peak amplitude. In this section we assume that the noise sources N1 and N2 are low enough. Under this condition, the DPA makes it possible to insulate the power consumption ($I_\uparrow$ or $I_\downarrow$) resulting from the activity of one single bit i: this manifests as a peak in the differential trace.

We propose to model the amplitude of the peak observed in the differential trace as a "DPA signal" that is built by an accumulation of scores. Given one ciphertext x, this score is:

+1 if the value $F_i(k \oplus x)$ inferred for the bit i by the selection function (Eqn. 1) is the same as the actual $F_i(k_0 \oplus x)$ for the correct key k_0,

-1 otherwise. As the recomputed bit value is false, the trace is considered to provide a $I_\uparrow$ power consumption contribution whereas the actual contribution is $I_\downarrow$, or vice-versa. Thus, instead of accumulating coherently $I_\uparrow - I_\downarrow$ to the differential traces, the opposite $I_\downarrow - I_\uparrow$ will be added, thus reducing the score coherence.

The scores are accumulated over many encipherments. Asymptotically, the accumulation is done for all the ciphertexts x.

As already mentioned when discussing the noise source N3, all the q bits of $y = F(k \oplus x)$ are guessed at the same time. As they take their values simultaneously, it is impossible to test the $y_i = F_i(k \oplus x)$ independently.

The "DPA signal" is thus the accumulation over all the ciphertexts x of the score obtained by a bit i of the plaintext against the q bits of actual plaintext. As a result, the DPA signal is built from the correlation of plaintext bit i for the trial key k with plaintext bit j for the actual key k_0:

$$\mathbf{Corr}(k_0, k; \mathbb{1}_i, \mathbb{1}_j), \qquad \text{where: } \forall k_0,\ k \in K^p,\ \forall a, b \in K^q, \tag{2}$$

$$\mathbf{Corr}(k_0, k; a, b) \stackrel{\text{def}}{=} \frac{1}{2^p} \sum_x (-1)^{\langle a | F(x \oplus k) \rangle \oplus \langle b | F(x \oplus k_0) \rangle}$$

as [11]:

$$\mathbf{DPA}(k_0, k; \mathbb{1}_i) = \sum_{j=0}^{q-1} \mathbf{Corr}(k_0, k; \mathbb{1}_i, \mathbb{1}_j). \tag{3}$$

Moreover, as it is easy to prove that:

$$\mathbf{Corr}(k_0, k; a, b) = \mathbf{Corr}(k_0 \oplus k, 0; a, b),$$

the correlation is independent of the actual key k_0. The relevant parameter is the difference $k_0 \oplus k$ between the actual key and the trial key. We simply denote this difference k, as if the actual key was 0. The correlation (Eqn. 2) is rewritten $\mathbf{Corr}(k; \mathbb{1}_i, \mathbb{1}_j)$. The "DPA signal" is rewritten accordingly: $\mathbf{DPA}(k_0, k; \mathbb{1}_i) = \mathbf{DPA}(k; \mathbb{1}_i)$. The correlation takes its values in [–1, +1] and equals +1 if the guess on the key is correct (*i.e.* $k = 0$) and $i = j$.

The "ghost peaks". When recomputing one bit of the plaintext from the ciphertext and a guessed key, the value can, by chance, match the actual value. If it happens often, the guessed key might be hard to distinguish from the actual key.

For instance, in the case of DES S-Box #3, there exists one wrong key that leads to a "DPA signal" as high as the one for the correct key: it occurs when the bits 0 or 3 of the S-Box output are guessed.

Those secondary peaks make it difficult to interpret the differential traces: they make up an artificial noise that was reported as "ghost peaks" [4].

DPA *modus operandi* justification In this section we assume that the S-Box F is balanced and that the attacker found the correct key (*i.e.* $k = 0$). If the partitioning test is done according to the value of $\langle a|F(x)\rangle$, where a belongs to K^q, (*e.g.* if $a = \mathbb{1}_i$, the sole bit i is used to partition the traces), the attacker computes the following DPA signal:

$$\begin{aligned}
\mathbf{DPA}(0; a) &= \sum_{j=0}^{q-1} \frac{1}{2^p} \sum_x (-1)^{\langle \mathbb{1}_j | F(x)\rangle \oplus \langle a | F(x)\rangle} = \frac{1}{2^p} \sum_{j=0}^{q-1} \sum_x (-1)^{\langle \mathbb{1}_j \oplus a | F(x)\rangle} \\
&= \frac{1}{2^p} \sum_{j=0}^{q-1} 2^p \, \delta(\mathbb{1}_j \oplus a) \qquad \text{(because } F \text{ is balanced)} \\
&= \begin{cases} 1 & \text{if there exists one } i \in [0, q[\text{ such as } a = \mathbb{1}_i, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

It shows that DPA exhibits a non-zero signal iff the partition is made on one of the q plaintext bits. In this case, the DPA signal is maximum (+1).

A new *modus operandi* for DPA. The traditional *modus operandi* for the DPA is to compute the differential traces for testing the value of the q bits of F output. However, the q differential traces are not independent, because the each predicted bit i is matched against all the actual plaintext $F(k_0 \oplus \cdot)$. For this reason we consider the sum of the q differential traces. The DPA signal

associated is:

$$\mathbf{DPA}(k) \stackrel{\text{def}}{=} \sum_{i=0}^{q-1} \mathbf{DPA}(k; \mathbb{1}_i) = \frac{1}{2^p} \left(\sum_{i=0}^{q-1} (-1)^{F_i} \otimes \sum_{j=0}^{q-1} (-1)^{F_j} \right) (k). \quad (4)$$

As an auto-correlation, the signal $\mathbf{DPA}(k)$ is maximum in absolute value in $k = 0$, *i.e.* when the attacker guess on the key is correct.

The method to compute the differential trace can be reformulated. Let k be the key being evaluated. For every ciphertext x, the power trace is weighted by $W(x, k)$, the centered Hamming weight of the recomputed plaintext (Eqn. 1):

$$W(x, k) \stackrel{\text{def}}{=} \sum_{i=0}^{q-1} F_i(x \oplus k) - q/2. \quad (5)$$

The weighted power traces are accumulated to yield the differential trace.

3. Electrical Simulation of the DPA

The DPA attack is simulated at the electrical level in order to validate our DPA signal model (Eqn. 4).

We find that, given the long time required by electrical simulations, a 6×4 S-Box like one S-Box of DES cannot be simulated for all the plaintext transitions. Instead of limiting ourselves to a subset of the possible messages, like in [13], we choose to simulate a simpler cryptographic operator. The cipher used is the one shown in Fig. 4, with Serpent [2] S-Box #0 $(p = q = 4)$.

The cipher is synthesized using various synthesis constraints into a 130 nm technology. The various logical netlists are translated into SPICE netlists using extracted standard cells in BSIM3V3 model.

The cipher is fed with all the transitions of plaintexts and the currents I(VDD) and I(VSS) are extracted during the simulation.

The exhaustive stimuli space exploration (2^{2q} traces) as well as the accuracy provided by the electrical simulation ensure that the traces we measure and the differential traces we compute emulate a perfectly noise-free DPA attack.

For the cipher described above, the theoretical model (Eqn. 4) predicts a DPA signal whose amplitude is given as an histogram in Fig. 6.

The differential traces depicted on Fig. 7 are computed from the traces acquired during the electrical simulation with the method explained above. The differential traces amplitude for the correct key can reach about 10 mA, which is also more or less the peak amplitude of a typical trace. The differential traces show that the amplitudes of secondary peaks are those predicted by the histogram of Fig. 6 for both side-channel I(VDD) and I(VSS). This conclusion is the same for all the netlists we simulate, which tends to show that DPA does not depend on the implementation.

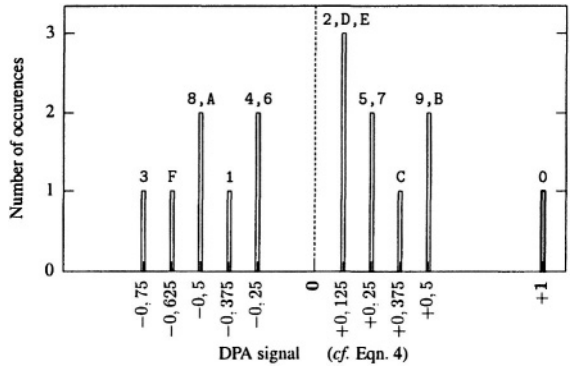

Figure 6. Theoretical histogram for the DPA signal (Eqn. 4). The hexadecimal values `0`, ..., `F` on top of the bars are those of $k_0 \oplus k$ (written on $p = 4$ bits). The thick peak for $k_0 \oplus k = 0$ is the DPA peak that betrays the secret key k_0, whereas the others are the "ghost peaks".

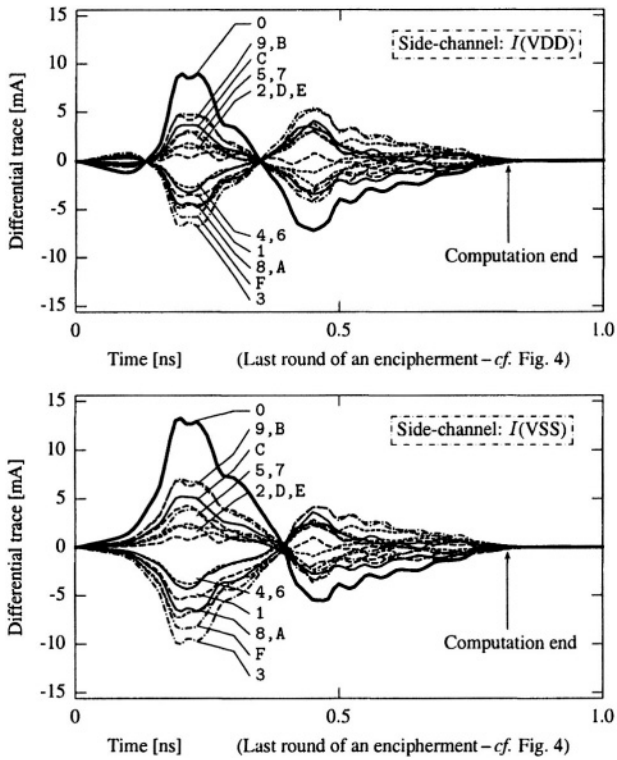

Figure 7. Electrical simulation of a DPA, using either I(VDD) or I(VSS) as the side-channel. The bold curve is the one computed when the hypothesis on the key is correct ($k_0 \oplus k = 0$).

The DPA signals obtained by simulation match the theory, which justifies the DPA model of Sec. 2 and proves that the difference $I_\uparrow - I_\downarrow$ of power consumption of a single gate can be extracted from the overall power consumed by a cryptographic operator. In addition, the model remains valid during much of the cipher computation time.

4. Connexions between DPA and Conventional Cryptanalysis

DPA Signal-to-Noise Ratio

DPA work factor is related to actual experiments, where the performance is assessed by a signal-to-noise ratio (SNR). As already mentioned, even if the DPA is not noisy, it does not allow to directly spot the right peak ($k = 0$) because there exists secondary peaks even for wrong keys ($k \neq 0$). Secondary peaks are modeled as noise. DPA quality is thus assessed by the following notion of SNR.

DEFINITION 1 *Signal* **Sig** *SNR.*

$$\mathbf{SNR(Sig)} \stackrel{def}{=} \frac{\mathbf{Sig}(k=0) - \overline{\mathbf{Sig}}}{\left(\frac{1}{\#k}\sum_k \left(\mathbf{Sig}(k) - \overline{\mathbf{Sig}}\right)^2\right)^{1/2}}, \textit{where } \overline{\mathbf{Sig}} \textit{ is the signal mean.}$$

As far as the DPA signal (Eqn. 4) is concerned, a balanced S-Box F satisfies:

$$\begin{cases} \mathbf{DPA}(0) &= \sum_{i,j} 2^{-p} \sum_x (-1)^{\langle \mathbb{1}_i \oplus \mathbb{1}_j | F(x) \rangle} \\ &= \sum_{i,j} \delta(\mathbb{1}_i \oplus \mathbb{1}_j) = q\,, \\ \overline{\mathbf{DPA}} &= 2^{-2p} \sum_{i,j} \sum_x (-1)^{F(x)_i} \left(\sum_k (-1)^{F(x \oplus k)_j}\right) \\ &= 0 \qquad \textbf{(because } F \textbf{ is balanced)}\,. \end{cases} \tag{6}$$

As a result, DPA SNR is:

$$\mathbf{SNR(DPA)}(F) = q\,2^{2p} \left(\sum_k \left(\sum_{i=0}^{p-1} \widehat{(-1)^{F_i}}(k) \right)^4 \right)^{-1/2}, \tag{7}$$

where $\hat{f}(k) = \sum_x (-1)^{\langle x|k \rangle} f(x)$ is the Hadamard-Walsh transform of the boolean function f.

The DPA SNR expression of Eqn. 7, proper to each S-Box F, fully characterize the DPA discrimination power.

It happens that the value of **SNR**(**DPA**)(F) (Eqn. 7) is significantly lower than $\mathbf{SNR}\left(\sum_{i=0}^{q-1} \mathbf{Corr}(k; \mathbb{1}_i, \mathbb{1}_i)\right)$ (refer to Eqn 2); for instance, those SNR are respectively 9.6 and 15.1 for AES. This proves that it is not realistic

to neglect the inter-bit correlations (N3) when doing DPA. The available information in the traces is the sum of the consumptions of the q output bits of the function F and the DPA indeed only reveals the correlation of one bit of the predicted plaintext with the Hamming weight of the full plaintext.

SNR for some typical S-Boxes. A relevant reference for the SNR is the experimental setup where there is no S-Box. Analysis is thus performed behind a set of $q = p$ independent XOR gates. In this case, $\mathbf{DPA}(k) = \sum_i (-1)^{k_i}$ (see Eqn. (8), with $F = I$, the identity matrix) and the SNR is $\sqrt{q}$.

The SNR of the DPA signal is computed using Eqn. 7 for balanced S-Boxes and an *ad hoc* calculus for the bent S-Box. Results are reported in Table 1.

Table 1. Signal-to-noise ratio of DPA signal on some typical S-Boxes.

S-Box	No S-Box ($F=I$)	Linear S-Box	DES S-Box 1	AES	Bent S-Box
p	8	8	6	8	8
q	8	8	4	8	4
DPA SNR	$\sqrt{8} = 2.8$	2.8	3.6	9.6	9.8

DPA SNR for an Affine Balanced S-Box. Let F be an affine balanced S-Box: $F(x) = M \times x \oplus D$.

LEMMA 2

$$\mathbf{Corr}(k;\, \mathbb{1}_i,\, \mathbb{1}_j) = (-1)^{\langle \mathbb{1}_j | M \times k \rangle} \delta_{i,j}\,, \tag{8}$$

thus: $\mathbf{SNR}(\mathbf{DPA})(F) = q^{\frac{1}{2}}$.

DPA SNR for a Bent S-Box. As far as (unbalanced) bent S-Boxes are concerned, DPA expression (Eqn. 4) yields high SNR (cf. Table 1). However, we have not investigated other expressions that could take advantage of the unbalancedness.

Results of Eqn.6 do not apply to an unbalanced S-Box. Instead, if F is bent,

$$\begin{cases} \mathbf{DPA}(0) &= q + \frac{1}{2^p} \sum_{i \neq j} \widehat{(-1)^{\langle \mathbb{1}_i \oplus \mathbb{1}_j | F \rangle}}(0)\,, & \text{hence:} \\ |\mathbf{DPA}(0) - q| &\leq q\,(q-1) 2^{-p/2} \ll q & \text{and} \\ \overline{\mathbf{DPA}} &= q\,2^{-p} \ll \mathbf{DPA}(0) & \text{if } p, q \to \infty \text{ and } p \geq 2q \text{ [5]}\,. \end{cases}$$

Therefore, at first order in $2^{-p/2}$, the expression of Eqn.7 for DPA SNR still holds. It allows for the derivation of a minoration of $\mathbf{SNR}(\mathbf{DPA})(F)$:

$$\mathbf{SNR}(\mathbf{DPA})(F) \gtrsim q\,2^{2p} \left(\sum_k \left(\sum_{i=0}^{q-1} 2^{\frac{p}{2}} \right)^4 \right)^{-1/2} = 2^{\frac{p}{2}}/q\,.$$

DPA SNR Bounds. Let us denote $Y_k = \left(\sum_{i=0}^{q-1} \widehat{(-1)^{F_i}}(k) \right)^2$.

SNR(DPA)(F) is thus rewritten as $q\,2^{2p} \left(\sum_k {Y_k}^2 \right)^{-1/2}$. The maximum and the minimum of the SNR correspond to the minimum and the maximum of $\sum_k {Y_k}^2$. Moreover,

LEMMA 3

- *If F is balanced:* $\sum_k Y_k = q\,2^{2p}$,
- *otherwise:* $\sum_k Y_k \in [0,\ q^2\,2^{2p}]$.

DPA SNR maximum bound. The application $C : (x_0, x_1, \cdots, x_{2^p-1}) \in (\mathbb{R}^+)^{2^p} \rightarrow \sum_{k=0}^{2^p-1} {x_k}^2 \in \mathbb{R}^+$ is convex. Its minimum is thus reached when C gradient is null, *i.e.* when all the x_k, $k \in [0,\ 2^p[$, are equal. Given Lem. 3, this value is $q\,2^p$ if F is balanced and can be as low as 0 otherwise.

Therefore, the maximum SNR of the DPA signal in a balanced S-Box is $2^{p/2}$. We ignore whether there exists S-Boxes that reach this bound. We also ignore whether DPA SNR is maximum bounded if the analyzed S-Box is unbalanced.

DPA SNR minimum bound. As $\sum_k {Y_k}^2 = \left(\sum_k Y_k\right)^2 - \sum_{k',k''} Y_{k'} Y_{k''}$, DPA SNR is minimum when the sum of positive terms $\sum_{k',k''} Y_{k'} Y_{k''}$ is minimum. It is null (and thus minimum) iff there exists an index k_0 such as all the Y_k, $k \neq k_0$, are null. If F is balanced, $\forall k,\ Y_k = q\,2^{2p}\,\delta(k \oplus k_0)$. This lower bound can only be reached provided $q\,2^{2p}$ (hence q) is a perfect square. If F is unbalanced, Y_k can reach $q^2\,2^p$. As for all $i \in [0,\ q[$ and $k \in K^p$, $\widehat{(-1)^{F_i}}(k) \leq 2^p$, Y_k reaches $q^2\,2^p$ iff for all i and k, $\widehat{(-1)^{F_i}}(k) = 2^p\,\delta(k \oplus k_0)$. S-Boxes satisfying this constraint are affine S-Boxes whose linear part rank is 1. Their corresponding SNR is $1/q$.

Summary of DPA Range and Typical Values. The results on the SNR of the DPA measured signal obtained in the Sec. 4 are summarized in Tab. 2.

Table 2. DPA signal-to-noise ratio bounds and typical values for different S-Boxes F.

SNR	Bound or typical value / S-Box type
$1/q$	Lower bound for unbalanced S-Boxes, reached only by rank 1 affine S-Boxes
1	Lower bound for balanced S-Boxes. Can only be reached if q is a perfect square
$q^{1/2}$	SNR of rank q affine S-Boxes
$2^{p/2}/q$	Approximative (at first order in $2^{-p/2}$) lower bound for bent S-Boxes
$2^{p/2}$	Upper bound for balanced S-Boxes

Conventional Cryptanalysis evaluators

Algorithmic attacks, like linear [9] or differential [3] cryptanalysis, are measured by a maximum singularity in distributions. For example [5],

$$\begin{cases} \Lambda_S \stackrel{\text{def}}{=} \sup_{a\neq 0,\,k} \left| \#\{x \,/\, \langle a|x\rangle \oplus \langle k|S(x)\rangle = 0\} - \frac{2^p}{2} \right| = \sup_{a\neq 0,\,k} \frac{1}{2}\hat{\theta}_S(k,\,a), \\ \Delta_S \stackrel{\text{def}}{=} \sup_{k\neq 0,\,a} \#\{x \,/\, S(x)\oplus S(x\oplus k) = a\} = \sup_{k\neq 0,\,a} (\theta_S \otimes \theta_S)\,(k,\,a), \end{cases}$$

are two parameters that characterize the resistances of an S-Box S against linear and differential cryptanalysis respectively. The lower they are, the more difficult the corresponding attack. We recall that in Eqn. 1, $F = S^{-1}$ for AES and $F = S$ for DES.

Comparing DPA and Conventional Cryptanalysis

The results of the previous section tend to show that the less linear a S-Box (and thus the higher its cryptographic quality), the higher the DPA SNR. The histograms of the occurrences of the SNR signal amplitudes are shown for some S-Boxes in appendix.

On the other hand, linear S-Boxes, the poorest protection against cryptanalysis, are the most difficult to attack by DPA.

DPA SNR Connexion with Conventional Cryptanalysis. The SNR of the DPA signal (Eqn. 7) is related to the two quantities Λ_S and Δ_S that characterize linear and differential cryptanalysis on S-Box F by:

$$\mathbf{SNR(DPA)}(F) \geq \frac{2^{\frac{3p}{2}-2}}{q\,\Lambda_S^2} = \mathcal{O}\left(\frac{1}{\Lambda_S^2}\right), \tag{9}$$

$$\mathbf{SNR(DPA)}(F) \geq \frac{2^p}{\Delta_S} = \mathcal{O}\left(\frac{1}{\Delta_S}\right). \tag{10}$$

The best shielded against linear or differential cryptanalysis (Λ_S or Δ_S low), the more vulnerable to DPA attack (**SNR**(**DPA**)(S) high).

5. Conclusion

The overall power consumption of a circuit leaks the activity of every single gate. The DPA attack exploits this side-channel to retrieve one secret kept within the circuit. The signal that an attacker computes to perform a DPA can be modeled as the auto-correlation of the Hamming weight of a given temporary variable used in the cryptographic algorithm. This auto-correlation function is maximum when the attacker key guess is correct. We validate this model against an electrical simulation of a block cipher. The SNR of the DPA signal increases when the resistance against linear or differential cryptanalysis

increases. The SNR is bounded, the lower bound being reached by the poorest cryptographic S-Boxes, namely affine S-Boxes. High quality cryptographic S-Boxes (AES, bent S-Boxes) feature high SNR, close to the maximum bound. As a consequence, DPA is fostered on devices implementing a high cryptographic quality private key algorithm.

Special care is thus needed while designing cryptoprocessors. As no trade-off is possible as for resistance against cryptanalysis, specific counter-measures must be devised. A possible counter-measure is to use secured logic gates [13]. However, those gates leak information because of parasitic effects: algorithmic counter-measures can thus be an adequate solution. For instance, the combination of a high SNR followed by a low SNR (in terms of *DPA* SNR) cipher on the same chip could provide a protection against both DPA and conventional cryptanalysis. Masking [1] and duplication [7] method are other counter-measures that require to re-design the ciphers.

References

[1] M. Akkar and C. Giraud. An Implementation of DES and AES secure against Some Attacks. *Proc. of CHES'01,* (2162):309–318, 2001.

[2] Ross J. Anderson. Serpent website (former candidate to the AES), 1999. `http://www.cl.cam.ac.uk/~rja14/serpent.html`.

[3] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology,* 4(1):3–72, 1991.

[4] Eric Brier, Christophe Clavier, and Francis Olivier. Optimal statistical power analysis. 2003. `http://eprint.iacr.org/`.

[5] Florent Chabaud and Serge Vaudenay. Links between Differential and Linear Cryptanalysis. *Proc. of Eurocrypt'94,* 950:356–365, 1995.

[6] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic Analysis: Concrete Results. *Proc. of CHES'01,* 2162:251–261, 2001.

[7] L. Goubin and J. Patarin. DES and Differential Power Analysis: The Duplication Method. *Proc. of CHES'99,* (1717):158–172, 1999.

[8] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis: Leaking Secrets. *Proc. of CRYPTO'99,* 1666:388–397, 1999.

[9] M. Matsui. Linear cryptanalysis method for DES cipher. *Proc. of Eurocrypt'93,* (765):386–397, 1994.

[10] Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan. Investigations of Power Analysis Attacks on Smartcards. *USENIX Workshop on Smartcard Technology,* pages 151–162, May 1999.

[11] Elisabeth Oswald. *On Side-Channel Attacks and the Application of Algorithmic Countermeasures.* PhD thesis, may 2003. `http://www.iaik.tu-graz.ac.at/aboutus/people/oswald/papers/PhD.pdf`.

[12] Takashi Satoh, Tetsu Iwata, and Kaoru Kurosawa. On Cryptographically Secure Vectorial Boolean Functions. *Proc. of Asiacrypt'99,* 1716:20–28, 1999.

[13] K. Tiri and I. Verbauwhede. Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology. *Proc. of CHES'03,*2779:126–136,2003.

Appendix: Illustration of DPA Signal-to-Noise Ratio on Histograms

The figures of this appendix show the histograms of occurrence of a given DPA signal amplitude. The actual signal is the peak of amplitude q (4 or 8), whereas the other peaks make up the S-Box intrinsic noise. It clearly appears in Fig. A.1(a) that a linear S-Box has a weak SNR (namely $\sqrt{q}$). Usual cryptosystems DES (Fig. A. 1(b)) and AES (Fig. A. 1(c)) have a better SNR. The SNR is still better for a bent S-Box of Maionara-McFarland type [12] (Fig. A. 1(d)).

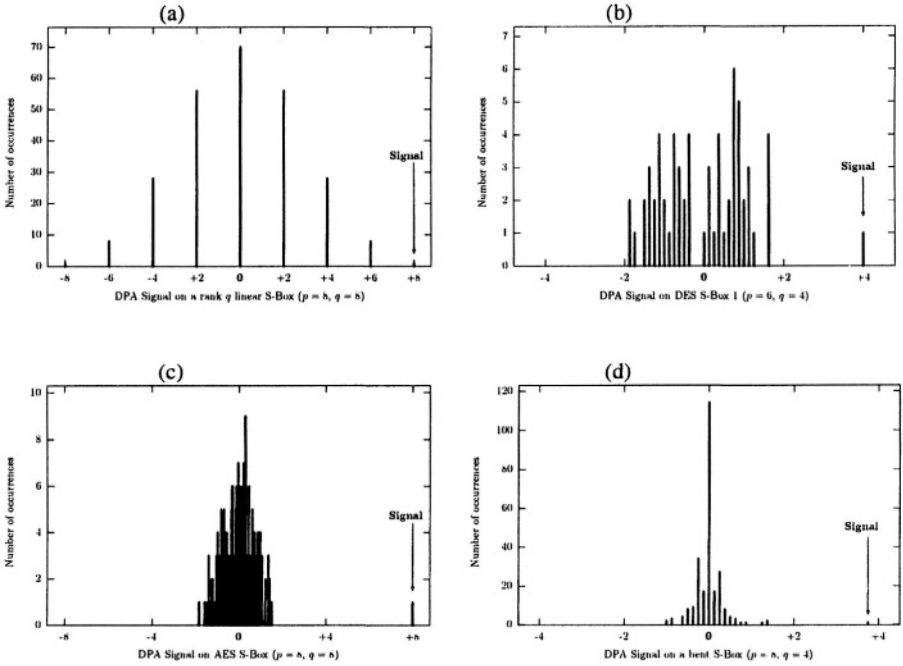

Figure A.1. Histogram of occurrences of the DPA signal measured on:

(a) a linear S-Box. $\mathbf{SNR}(\mathbf{DPA})(F) = \sqrt{8} \sim 2.8$ (Eqn. 7),

(b) DES S-Box 1. $\mathbf{SNR}(\mathbf{DPA})(F) = 3.6$,

(c) AES. $\mathbf{SNR}(\mathbf{DPA})(F) = 9.6$,

(d) a bent S-Box. $\mathbf{SNR}(\mathbf{DPA})(F) = 9.8$.