Available online at www.sciencedirect.com
ScienceDirect
INTEGRATION, the VLSI journal 40 (2007) 52–60
INTEGRATION theVLSI journal
www.elsevier.com/locate/vlsi

Power and electromagnetic analysis: Improved model, consequences and comparisons

Eric Peeters*, François-Xavier Standaert, Jean-Jacques Quisquater

UCL Crypto Group, Place du Levant, 3, B-1348 Louvain-La-Neuve, Belgium

Abstract

Since their publication in 1998 and 2001, respectively, Power and Electromagnetic Analysis (SPA, DPA, EMA) have been successfully used to retrieve secret information stored in cryptographic devices. Both attacks usually model the side-channel leakages using the so-called "Hamming weight" and "Hamming distance" models, i.e. they only consider the number of bit transitions in a device as an image of its leakage. In these models, the main difference between power and electromagnetic analysis is assumed to be the fact that the latter allows space localization (i.e. to observe the leakage of only a part of the cryptographic device). In this paper, we make use of a more accurate leakage model for CMOS devices and investigate its consequences. In particular, we show that it is practically feasible to distinguish between $0 \rightarrow 1$ and $1 \rightarrow 0$ bit transitions in certain implementations and that electromagnetic analysis is particularly efficient in this respect. We denote this model as the "switching distance" leakage model and show how it may be very helpful to defeat some commonly used countermeasures (e.g. data buses precharged with random values). Then, we compare the different models and stress their respective constraints/advantages regarding practical attacks.

Keywords: Cryptographic hardware; Side-channel attacks; Leakage models

1. Introduction

Since their public appearance in the mid-90s, side-channel attacks have attracted a significant attention within the cryptographic community. Power Analysis and Electromagnetic Analysis are typical examples of successful attacks against trusted cryptographic devices such as smart cards. They have been investigated by numerous research groups and have given rise to various publications. However, among these practical important results, only a few models for the leakages have been proposed and used.

First, in 1998, Kocher et al. [1] suggested to take advantage of the power consumed by a microchip in order to get information about what the device actually processes. They used a somewhat specific power consumption model based on the Hamming weight of the data handled in the chip. This typically corresponds to smart card implementations where data buses are precharged with constant values. The model was similarly used in [2–5]. A few years later, the model was extended in order to better integrate the behavior of CMOS circuits, where the power consumption generally relates to the number of bit transitions in a target device. The resulting "Hamming distance" power consumption model was applied to ASIC and FPGA implementations of cryptographic algorithms and demonstrated that any kind of implementation could potentially be the target in a side-channel attack [6–9].

In parallel, [10–12] suggested using the electromagnetic emanations of microelectronic circuits as an alternative, and potentially more powerful, source of side-channel leakage. The approach was shown to provide significant advantages, both from the theoretical and practical point of view. For example, Agrawal et al. [10] explained that electromagnetic emanations may be modulated by an inner loop structure and detailed that an adequate AM demodulator can be used to perform efficient attacks even a few meters away from the chip. It was also demonstrated

*Corresponding author.
E-mail addresses: peeters@dice.ucl.ac.be (E. Peeters), standaert@dice.ucl.ac.be (F.-X. Standaert), quisquater@dice.ucl.ac.be (J.-J. Quisquater).

0167-9260/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.vlsi.2005.12.013

that, in a semi-invasive context, electromagnetic analysis allows the observation of only parts of the devices under attack, therefore offering much more accurate information. However, regarding the leakage models, these references usually base their investigations on the same assumptions as in power analysis attacks (i.e. Hamming weight or distance leakage models).

In this paper, we intend to use a more complete description of the CMOS technology, allowing us to consider better power consumption and emanation models. In practice, we show that $0 \rightarrow 1$ and $1 \rightarrow 0$ bit transitions can be distinguished in certain implementations. Although this problem was already previously examined, e.g. in [13], we additionally demonstrate that electromagnetic analysis is particularly efficient in this respect. We therefore suggest a new way to use the localized electromagnetic emanation of a microprocessor. This model is denoted as the "switching distance" leakage model. We note that *we do not claim having discovered a new side-channel effect* as, theoretically, the ability to distinguish between the charge and the discharge of a load capacitance in a CMOS device is a well known fact. Rather, we propose a systematic investigation of this potential leakage and show that it may lead to practical improvements of previous attacks. Also, we show that this switching distance model is observable in real-world implementations and may allow an attacker to bypass some commonly used countermeasures (e.g. data buses precharged with random values). We finally propose a comparison of two correlation attacks against such a countermeasure, with power and electromagnetic measurements, respectively.

The rest of the paper is structured as follows. Section 2 describes the origin of the power and electromagnetic leakages in CMOS devices. Section 3 briefly presents our measurement tools. The different leakage models are presented in Section 4 and their practical consequences are discussed in Section 5. A synthetic comparison of the models is given in Section 6.

2. Side-channel sources

The CMOS technology is certainly the most widely used in current digital design applications. We start our study with a simple gate, namely the inverter which is the nucleus of all CMOS ICs. It is depicted in Fig. 1.

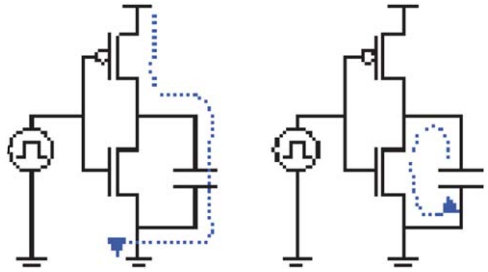

Fig. 1. The static CMOS inverter.

2.1. Power consumption in CMOS devices

Static CMOS gates have three distinct dissipation sources [14]. The first one is due to the leakage currents in transistors. Its contribution to the overall dissipation is in general very small. The second one is due to the so-called "direct path current": there exists a short period during the switching of a gate while NMOS and PMOS are conducting simultaneously. Finally, the most important dissipation (and most relevant from a side-channel point of view) is due to the charge and discharge of the load capacitance C_L represented by the dotted paths in Fig. 1 (right and left part, respectively). This capacitance is composed from the different parasitic capacitances (junctions, gates, ...) and the wiring capacitance (interconnections). The expression of the dynamic power consumption of the inverter is given by

$$P_{dyn} = C_L V_{DD}^2 P_{0\rightarrow 1} f, \quad (1)$$

where $P_{0\rightarrow 1} f$ is called the *switching activity* ($P_{0\rightarrow 1}$ is the probability of a $0 \rightarrow 1$ transition and f is the work frequency of the device), and V_{DD} is the voltage of the power supply.

In CMOS devices, when measuring the power consumption (either at the ground pin or at the power pin), the highest peak will therefore appear during the charge of this capacitance. During the discharge, the only current we can measure is the direct path current. We simulated and measured a simple CMOS gate to support this assumption. Fig. 2 shows SPICE simulations of a single inverter fed with a clock signal. The left figure illustrates the current which is going through the NMOS (thicker line) and the current in the capacitance (thinner line). The right figure illustrates the current probed at the VDD or at the GND pin and exactly corresponds to the sum of the two currents displayed on the left. We then confirmed these simulations with real measurements, taken at the ground pin of a 74HC04 CMOS inverter. It is illustrated in Fig. 3, where the charges/discharges of the load capacitance are clearly observable.

2.2. EM emanations in CMOS devices

Current ICs are constituted of millions of transistors and interconnections in which data-dependent current flows. In electromagnetic analysis attacks, these small moving charges are assumed to produce a variable magnetic field, which itself produces a variable electric field. Therefore, monitoring this data-dependent radiation allows us to obtain information about the data handled by the device. This effect has been successfully used to attack cryptographic implementations in [10–12,15].

Different methods can be considered to measure the electromagnetic radiations of microprocessors. In this paper, we focus on the use of a small magnetic loop probe (suggested in EMC measurement methods [16]) instead of larger probe [10,11]. One reason for this choice is that such probes allow us to take advantage of localization effects, due to their small size. For example, we noted that the

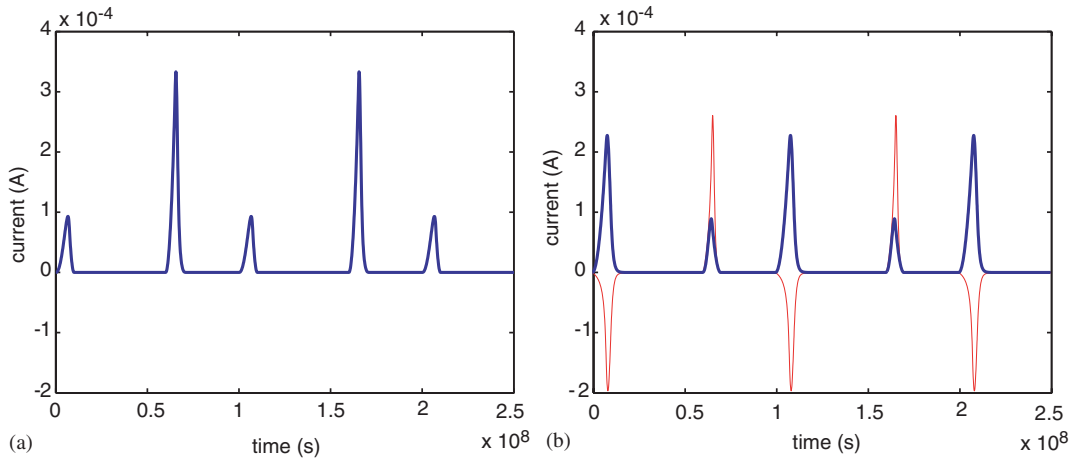

Fig. 2. PSPICE simulation: (a) current in the NMOS and C_L; (b) current in the PMOS.

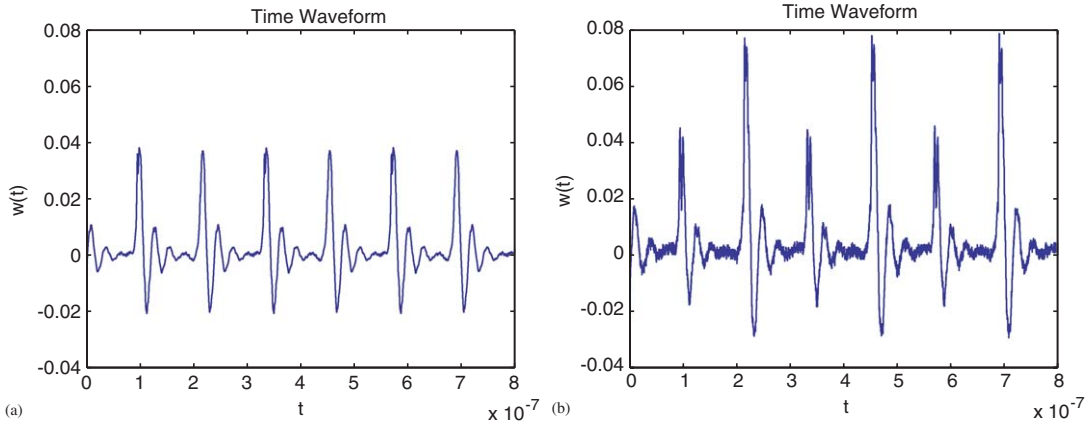

Fig. 3. Experimental results on 74HC04 inverter: (a) CMOS inverter without C_L; (b) CMOS inverter with $C_L = 10\,pF$.

emanations measured with the loop probe at more than one centimeter away from the chip are similar to the power consumption measured at the ground pin. The reason is simply that the portion of the magnetic field due to the power supply bond wires and lead frames is the most important in this region. However, when we placed the probe near the surface of the chip, we observed more localized emanations (e.g. bus, decoder, ...).

From a theoretical point of view, these electromagnetic leakages are generally explained as follows. First, the region located less than one wavelength away from the source is called the *near-field* zone. Our measurements typically take place in this region where the signals may be considered as quasi-static. This allows us to use the Biot–Savart law to describe the magnetic field $\vec{B}$

$$\mathrm{d}\vec{B} = \frac{\mu I \vec{\mathrm{d}l} \times \hat{r}}{4\pi |\vec{r}|^2}, \tag{2}$$

where I is the current carried on a conductor of infinitesimal length $\vec{\mathrm{d}l}$, μ is the magnetic permeability and $\vec{r}$ is a vector specifying the distance between the current and the field point ($\hat{r} = \vec{r}/|\vec{r}|$).

Secondly, Faraday's law expresses that any change in the environment of the loop probe will cause a voltage (*emf*) to be induced in the coil:

$$emf = -N\frac{\mathrm{d}\Phi}{\mathrm{d}t}, \tag{3}$$

$$\mathrm{d}\Phi = \int_{surface} \vec{B} \cdot \vec{\mathrm{d}S}, \tag{4}$$

where N is the number of turns in the coil and Φ the magnetic flux. We represent a bus wire above a dielectric substrate on Fig. 4. If we consider that the bus may behave as a infinite wire, we may reduce the above cited Biot–Savart equation to the following expression:

$$\vec{B} = \frac{\mu I}{2\pi \mathrm{d}}\hat{a}_\varphi, \tag{5}$$

where d is the distance to the wire and $\hat{a}_\varphi$ is a unit vector azimuthally oriented with respect to the wire. This

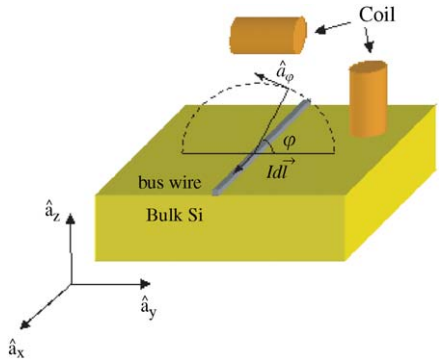

Fig. 4. Geometry of a bus wire.

equation clearly expresses that the closer we place the probe to the target circuit, the bigger the measured magnetic field is (what was observed in practice).

Although these simple equations do not describe the exact behavior of the magnetic field, they emphasize two important points: (1) The field is data-dependent (suggested by the dependence of the current intensity I). (2) The orientation of the field directly depends on the orientation of the current (as $\hat{a}_\varphi = \overrightarrow{dl} \times \hat{r}/|\overrightarrow{dl} \times \hat{r}|$).

A straightforward consequence of these remarks is that we may position the probe in the $\hat{a}_y$-direction (i.e. the axis of the probe is parallel to the $\hat{a}_y$-direction) as well as in the $\hat{a}_z$-direction (as suggested in Fig. 4). In practice, we measured the field strength in the three axis directions with the same probe (tiny coil). We observed a voltage magnitude of around 150 mV (after amplification, this becomes around 10 mV without amplification) for 8 bits toggling simultaneously with the probe oriented following the $\hat{a}_y$ or the $\hat{a}_z$ axis while only 60 mV were observed when orienting the probe in the $\hat{a}_x$ axis.

As a further research, a more accurate field model will be implemented. It is based on the Green's function associated with the two-layer media (air and dielectric) backed by a ground plane, which has been often considered for the analysis of microstrip patch antennas [17].

3. Practical measurements

The building of a good measurement setup is an important step in side-channel attacks, as it will influence the relevance of the observed data. In accordance with the previous section, it is crucial to avoid noise additions as much as possible. For this purpose, a first guideline is to isolate the target component from all other possible electronic devices on the board, e.g. memories, capacitances, ... Although the technical description of a good measurement setup for side-channel attacks is out of the scope of this paper, this section intends to provide some practical details about our experiments. It should allow an interested reader to reproduce our results.

We carried out all our experiments on a PIC 16F877 8-bit RISC-based microprocessor. We clocked this microchip at a frequency around 4 MHz. This microprocessor requires four clock cycles to process an instruction. Each instruction is divided into four steps: fetch (update of the address bus), decode and operands fetch (driven by the bus), execute and write back [18].

We monitored the power consumption of a device by inserting a small resistor at its ground pin or power pin. We chose a value of the resistor so that it disrupts the voltage supply by at most 5% from its reference (as advised in [19]). We used the 1-Ohm method [19] when attacking the device at the ground pin and used a differential probe in the case of targeting the power pin.

We note that monitoring electromagnetic emanation requires more care than power consumption measurements. Noisy environments are a big concern in this respect and we recommend the use of a Faraday cage to obtain better results. However, we carried out all our experiments without using such protection and the obtained observations were sufficiently accurate (even without any averaging process) to properly correlate with our model. In practice, we used the small hand-made loop probe (0.7 mm diameter) of Fig. 5 that we soldered on a semi-rigid coax mounted on an SMA connector (note that appropriate soldering iron and optical microscope were used).

Moreover, we amplified the signal with an appropriate large band and low noise preamplifier. Finally, we used a 1 GHz bandwidth oscilloscope to obtain enough precision in the measured signal. Note also that we correlated our leakage predictions and real measurements using exactly the same methods as previously used in, e.g. [6,8,9].

4. Leakage models

All three models presented in this section allow describing the power consumption of a microchip as well as its electromagnetic behavior. First, we give a short description of the Hamming weight and distance models. Then we present the switching distance model and provide experimental evidence that it allows more accurate predictions than former models (Fig. 6).

4.1. Hamming distance model

As explained in Section 2.1, the power consumption in CMOS devices is mainly due to its switching activity. That is, let x and x' be two consecutive intermediate values of a running algorithm in a target implementation, let t be the time at which x switches into x', then the power consumption of the device at this time is proportional to $D_H(x, x') = W_H(x \oplus x')$, where W_H denote the Hamming weight. This leakage model is usually denoted as the *Hamming distance model*. It was successfully used to attack ASIC and FPGA implementations of CMOS devices [6–9].

4.2. Hamming weight model

In certain contexts, this model can be simplified by the knowledge of implementation details. For example, in case

Fig. 5. Our loop probe.

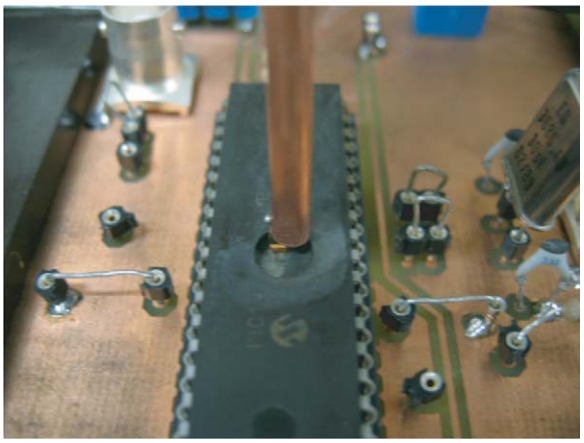

Fig. 6. Measurement setup with a PIC16F877 and a small loop probe.

of microprocessors with precharged buses, the power consumption may depend on the Hamming weight of the data on the bus. This is typically the case if the precharged value is "*all zeroes*" which yields the power consumption to depend on $W_H(0\ldots0 \oplus m) = W_H(m)$. It yields the *Hamming weight model*. It was used in Kocher's original DPA [1] and carefully investigated in [6], where precharged values different from "*all zeroes*" are considered.

4.3. Switching distance model

4.3.1. Using power measurements

Section 2.1 suggests that a CMOS gate consumes differently when charging or discharging the load capacitance. It should therefore be possible to observe these differences and obtain a more accurate leakage model. For this purpose, we define the normalized difference of the transition leakages as $\delta = P_{0\to1} - P_{1\to0}/P_{0\to1}$. It directly yields the improved power consumption model in Table 1.

To confirm this model, we carried out some experiments on the 8-bit PIC microprocessor. We used a loop of consecutive 'MOVLW' instructions with known random values and measured the resulting power consumption. Then we compared these measurements with predictions using both the Hamming distance and the improved models. The comparisons are in Figs. 7(a) and (b), where predictions are the darker line while the measured values are reported with the lighter line (Note that the measurements were scaled). Obviously, our predictions with the improved model are more accurate[1].

4.3.2. Using EM measurements.

It is suggested in Section 2.2 that electromagnetic measurements may allow us to obtain localized information, depending on the ability to manipulate the probe accurately. Moreover, we gave precise equations of the radiated field and showed that a variation in this field induced a small voltage in the small coil. An interesting point to note is that the value of this measured voltage directly depends on the direction of the current. Electromagnetic measurements therefore allow differentiating a charge/discharge of the bus by simply observing the sign of the peaks on the monitored traces.

Again, we confirmed these assumptions with practical experiments. Fig. 8 illustrates the difference between power and electromagnetic traces of three consecutive 'MOVLW' instructions where the samples corresponding to the update of the bus are circled. We clearly observe that the peak sign information is only distinguishable in the EM trace.

As a matter of fact, the sign information is only accessible if the probe can be localized accurately, which involves a precise knowledge of the chip under attack. It requires a somewhat different context (i.e. semi-invasive) which may be a drawback of the technique, but with appropriate support it is easily handled [20]. Our method was to observe the depackaged integrated circuit with a microscope to identify its different blocks (Flash EEPROM, RAM, bus, CPU blocks,...). Fig. 9 depicts a picture taken with an optical microscope. Magnifying these pictures, we were able to observe the region where the data bus (circled) connecting the memory blocks to the CPU blocks is located.

However, a simple scan of the surface with the probe easily revealed the best location to eavesdrop the bus as well.

4.3.3. Ideal model

According to the previous experiments, it is possible to build a new idealized emanation model, that we denote as the *signed distance model*. That is, we assume that charging

[1]The correlation values obtained for both models were, respectively 0.975 and 0.985.

(*resp*. discharging) the capacitance involves a leakage of +1 (*resp*. −1). Inverting the loop orientation obviously inverts the signs. It yields the leakage of a n-bit data x switching into x' to be proportional to: $S_D(x, x') = \sum_{i=0}^{n-1} x'(i) - x(i)$, where S_D denotes the signed distance and $x(i)$ is the ith bit of x. Basically, the signed distance model is a particular case of the switching distance model with $\delta = 2$.

We finally repeated our experiment of Section 4.3.1 with this new model. It is represented in Fig. 10. We obtained a correlation between predictions and measurements of 0.95, exhibiting that our model pretty well matches the real behavior of the emanation above the bus.

Table 1
Improved power consumption model

Transitions	Power
$0 \to 0$	0
$0 \to 1$	1
$1 \to 0$	$1 - \delta$
$1 \to 1$	0

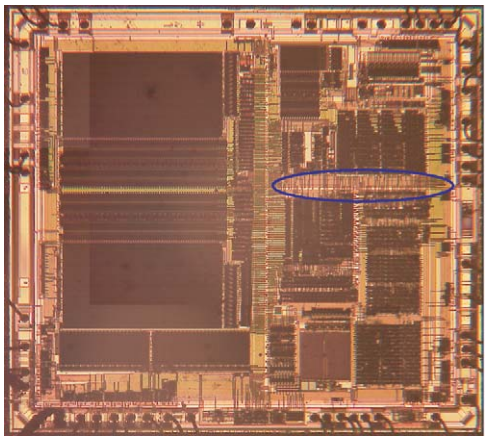

Fig. 9. Microscopic view of the targeted PIC.

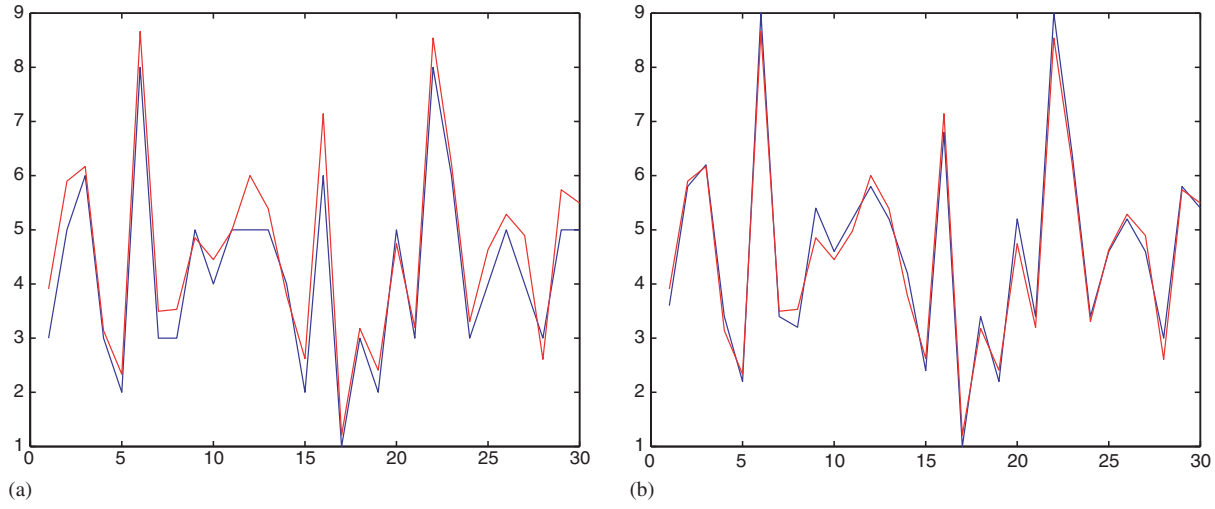

Fig. 7. Switching distance model with power consumption: comparisons: (a) model with $\delta = 0$; (b) model with $\delta = 0.17$.

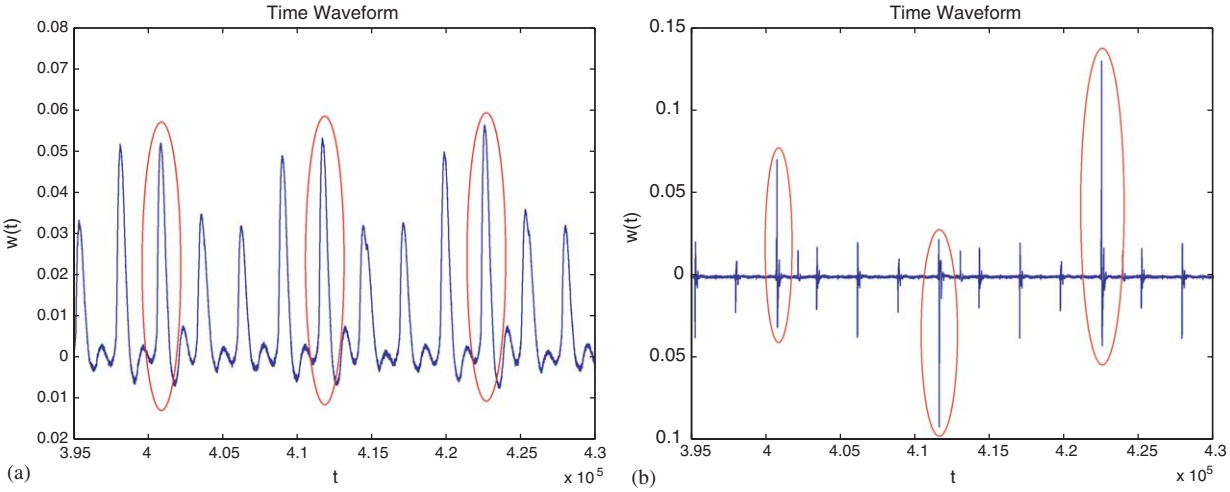

Fig. 8. Switching distance model comparison: power vs. EM traces: (a) power trace of a PIC; (b) EM trace of a PIC.

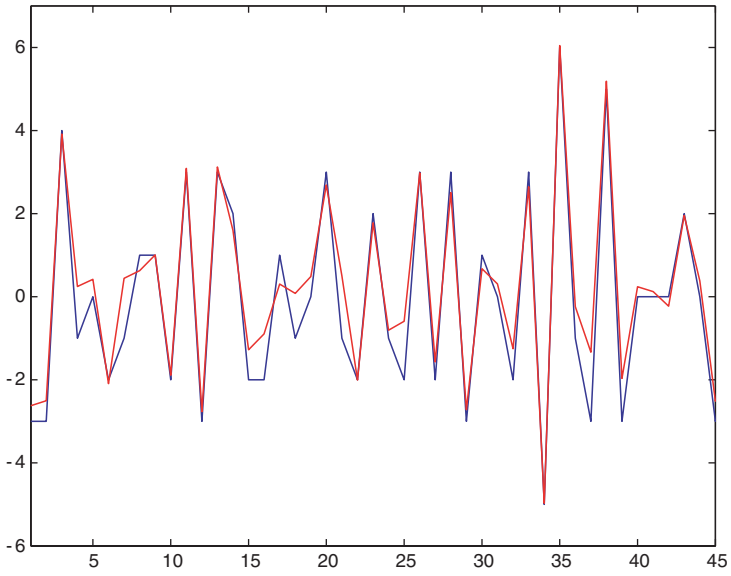

Fig. 10. Signed distance model with electromagnetic emanations.

A straightforward consequence of such a model is that the power consumption as well as the electromagnetic emission are spread over a larger set of discrete values (compared to the Hamming Weight and Hamming Distance models). From an information theoretic point of view, it suggests that the switching distance model will allow the improvement of side-channel attacks. It is investigated in the next section, where we show that the switching distance allows bypassing certain countermeasures (that the previous models cannot).

5. Consequences

A common countermeasure used in the smart card industry to counteract side-channel analysis is to precharge the buses with random values. As the Hamming distance model presented in Section 4.1 cannot be used to predict the leakages if one of the two values x or x' is unknown, side-channel opponents cannot target such buses with the former models. The switching distance model provides a straightforward tool to bypass such a countermeasure. We demonstrate it within the framework of the correlation analysis attacks [6,9], that usually holds in three steps.

First, the attacker *predicts* the leakage of the running device, at one specific instant, as a function of certain secret key bits. A typical target for such a prediction is the output of a substitution box $S(x \oplus k)$ in a block cipher, where x is a known input and k the secret key. Say we are using the Hamming distance leakage model, then the prediction phase only requires the attacker to predict the switching activity at the S-box output. If the S-box is s-bit large, it yields 2^s possible predictions, stored in a *prediction matrix*.

Secondly, the attacker *measures* the real leakage of the running device, at the specific time where it processes the same input texts as during the prediction phase. The result of this measurement is stored in the *consumption vector*.

Finally, the attacker *compares* the different predictions with the real, measured power consumption, using the correlation coefficient.[2] That is, he computes the correlation between the consumption vector and all the columns of the prediction matrix (corresponding to all the 2^s key guesses). If only one value leads to a high correlation coefficient, corresponding to the correct key guess, the attack is therefore declared to be *successful*.

Coming back to randomly precharged buses, let us say we observe a random value r switching into a predictable value $S(x \oplus k)$: $r \to S(x \oplus k)$. It is clear that the resulting leakage cannot be predicted using the Hamming distance model since an attacker does not know the random value r. However, considering the improved model of Table 1, the average leakage when a bit of $S(x \oplus k)$ equals zero is $(1-\delta)/2$ while the average leakage when such a bit equals one is $1/2$. As a consequence, predicting the leakage using the Hamming weight of $S(x \oplus k)$ (without taking care of r) will allow mounting a correlation attack. Note that the switching distance model is not used explicitly in the prediction (since we actually use the Hamming weight model). However, it is because the switching distance model holds that such a prediction is relevant. Note also that an attack against precharged buses will be significantly more efficient if the δ value increases.

[2] Let $M(i)$ denote the ith measurement data (i.e. the ith trace) and M the set of traces. Let $P(i)$ denote the prediction of the model for the ith trace and P the set of such predictions. Then we calculate

$$C(M,P) = \frac{\mu(M \times P) - \mu(M) \times \mu(P)}{\sqrt{\sigma^2(M) \times \sigma^2(P)}}, \quad (6)$$

where $\mu(M)$ denotes the mean of the set of traces M and $\sigma^2(M)$ its variance.

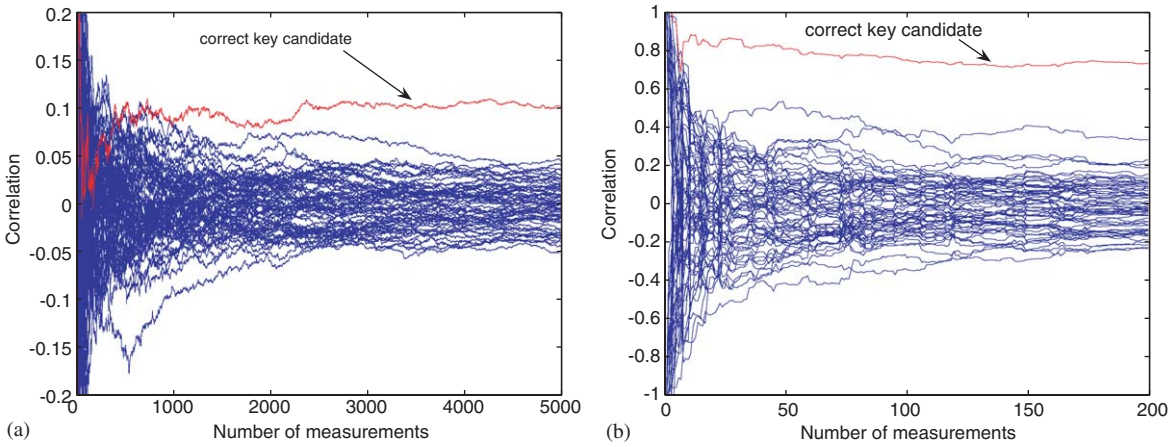

Fig. 11. Simulated correlation attacks against 8-bit S-boxes implemented in a processor with randomly precharged buses using the switching distance model: (a) power based model ($\delta = 0.17$); (b) emanation based model ($\delta = 2$).

To confirm these assumptions, we simulated attacks against a processor using precharged buses as follows: (1) We generated a number of values r_i and x_i, the key k being fixed. (2) We predicted the leakages using the Hamming weight of $S(x_i \oplus k)$, for the 2^s possible key candidates (in practice, we used $s = 8$). (3) We generated simulated measurements, using the switching distance model. For comparison purposes, we considered measurements based on power leakages ($\delta = 0.17$) and EM leakages ($\delta = 2$). (4) We performed the correlation phase. The results of the simulated attacks are in Fig. 11, where it is clearly observed that the correct key candidate can be recovered and that the EM measurements are significantly more efficient (see the scale difference).

In accordance with the comparisons we made in the previous sections between predictions and measurements, one can say that the reported simulated attacks (Fig. 11) should correspond quite well to real attacks on a 8-bit PIC16F877 microprocessor (0.9 μm technology). The main reason is the weak noise that is present on measurements.

6. Conclusions

Most published power and electromagnetic analysis attacks were based on the so-called ''Hamming distance'' or ''Hamming weight'' leakage models. These models only provide the attacker with information about the activity (or lack thereof) of certain target bits in a running implementation. While this information was sufficient to mount practical attacks against a variety of devices, it clearly does not take advantage of all the available leakage. Namely, such models do not distinguish the different possible activities of the target bits.

In this paper, we analyze the switching distance model, that permits distinguishing $0 \to 1$ from $1 \to 0$ bit transitions in CMOS circuits. We demonstrate that these different transitions can be observed both with power consumption and electromagnetic measurements. We also stress that, in a semi-invasive context, the latter are particularly efficient, when placing the small magnetic probe very close to the source (e.g. the data bus). We confirmed these claims with experiments carried out on a 8-bit microprocessor, but the model may be used in other hardware contexts.

The new model has important practical consequences as it allows defeating a popular countermeasure against power analysis attacks, namely precharging the buses with random values. We show that while the Hamming distance model cannot target such implementations, distinguishing the charges and discharges of CMOS load capacitances offers a straightforward way to bypass the random precharge.

Also, the model has potentially interesting theoretical consequences. Indeed, from an information theoretic point of view, the switching distance delivers substantially more leakage than former models. However, we observed that certain usual statistical tools used in side-channel attacks (e.g. difference of means [13,1] and correlation coefficient [6,9]) do not allow taking advantage of this additional leakage.[3] For example, the number of measurements required in a correlation power analysis will be the same, regardless of the model used to predict the power consumption. This suggests that these side-channel attacks do not use the optimal statistical tool to recover the secret. The investigation of better statistical tools (e.g. Maximum Likelihood [21], Hidden Markov Models [22],...) within the new model is a scope for further research.

Acknowledgements

The authors would like to thank Christophe Craeye and Philippe Manet for their comments on this work. We also

[3]This refers to scenarios where we use the model explicitly for predicting the leakage (i.e. knowing the values before and after the transition), contrary to Section 5 where one of these values is random and unknown.

thank Sébastien Speckens and Alexandre Vion for their helpful master thesis on this topic. François-Xavier Standaert is a post doctoral researcher funded by the FNRS (Funds for National Scientific Research, Belgium).

References

[1] P.C. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: M. Wiener (Ed.), Advances in Cryptology—CRYPTO'99, Lecture Notes in Computer Science, vol. 1666, Springer, Berlin, 1999, pp. 388–397.

[2] C. Clavier, J.-S. Coron, N. Dabbous, Differential power analysis in the presence of hardware countermeasures, in: Ç.K. Koç, C. Paar (Eds.), Cryptographic Hardware Embedded System—CHES 2000, Lecture Notes in Computer Science, vol. 1965, Springer, Berlin, 2000, pp. 252–263.

[3] J.-S. Coron, P.C. Kocher, D. Naccache, Statistics and secret leakage, in: Y. Frankel (Ed.), Financial Cryptography—FC2000, Lecture Notes in Computer Science, vol. 1962, Springer, Berlin, 2001, pp. 157–173.

[4] T.S. Messerges, Using second-order power analysis to attack DPA resistant software, in: Ç.K. Koç, C. Paar (Eds.), Cryptographic Hardware Embedded System—CHES 2000, USA, Lecture Notes in Computer Science, vol. 1965, Springer, Berlin, 2000, pp. 71–77.

[5] J. Waddle, D. Wagner, Towards efficient second-order power analysis, in: M. Joye, J.J. Quisquater (Eds.), Cryptographic Hardware Embedded System—CHES 2004, Lecture Notes in Computer Science, vol. 3156, Springer, Berlin, 2004, pp. 1–15.

[6] E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, in: M. Joye, J.J. Quisquater (Eds.), Cryptographic Hardware Embedded System—CHES 2004, Lecture Notes in Computer Science, vol. 3156, Springer, Berlin, 2004, pp. 16–29.

[7] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552.

[8] S.B. Ors, F. Gurkaynak, E. Oswald, B. Preneel, Power-analysis attack on an ASIC AES implementation, in: Proceedings of ITCC 2004, Las Vegas, April 5–7, 2004.

[9] F.-X. Standaert, S.B. Ors, B. Preneel, Power analysis of an FPGA implementation of Rijndael: is pipelining a DPA countermeasure? in: M. Joye, J.J. Quisquater (Eds.), Cryptographic Hardware Embedded System—CHES 2004, USA, Lecture Notes in Computer Science, vol. 3156, Springer, Berlin, 2004, pp. 30–44.

[10] D. Agrawal, B. Archambeault, J.R. Rao, P. Rohatgi, The EM side-channel(s), in: B.S. Kaliski Jr., Ç.K. Koç (Eds.), Cryptographic Hardware and Embedded Systems (CHES 2002), Lecture Notes in Computer Science, vol. 2523, Springer, Berlin, 2002, pp. 29–45.

[11] K. Gandolfi, C. Mourtel, F. Olivier, Electromagnetic analysis: concrete results, in: Ç.K. Koç, D. Naccache, C. Paar (Eds.), Cryptographic Hardware and Embedded Systems (CHES 2001), Lecture Notes in Computer Science, vol. 2162, Springer, Berlin, 2001, pp. 251–261.

[12] J.-J. Quisquater, D. Samyde, Electromagnetic analysis (EMA): measures and counter-measures for smart cards, in: I. Attali, T.P. Jensen (Eds.), Smart Card Programming and Security (E-smart 2001), Lecture Notes in Computer Science, vol. 2140, Springer, Berlin, 2001, pp. 200–210.

[13] S. Guilley, P. Hoogvorst, R. Pacalet, Differential power analysis model and some results, in: J.-J. Quisquater, P. Paradinas, Y. Deswarte, A.A. El Kalam (Eds.), Smart Card Research and Advanced Applications VI, IFIP 18th World Computer Congress, TC8/WG8.8 & TC11/WG11.2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS), 22–27 August 2004, Toulouse, France, Kluwer, Dordrecht, 2004, pp. 127–142.

[14] J.M. Rabaey, Digital Integrated Circuits, Prentice-Hall International, Englewood Cliffs, NJ, 1996.

[15] V. Carlier, H. Chabanne, E. Dottax, H. Pelletier, Electromagnetic side channels of an FPGA implementation of AES, IACR eprint archive, ⟨http://eprint.iacr.org/2004/145.pdf⟩.

[16] IEC 61967-3: Integrated circuits—measurement of electromagnetic emissions, 150 kHz to 1 GHz, Part 3: measurement of radiated emissions, surface scan method (10 kHz to 3 GHz), 47A/620/NP, New Work Item Proposal, Date of proposal: July 2001.

[17] D.M. Pozar, Input impedance and mutual coupling of rectangular microstrip antennas, IEEE Trans. Antennas Propag. 30 (1982) 1191–1196.

[18] PIC16F877 datasheet, Microchip, ⟨http://ww1.microchip.com/downloads/en/DeviceDoc/30292c.pdf⟩.

[19] IEC 61967-4: Integrated circuits—measurement of electromagnetic emissions, 150 kHz to 1 GHz—Part 4: measurement of conducted emissions—1 Ω/150 Ω, Direct coupling method, 47A/636/FDIS, Final Draft International Standard, Distributed on 2002-01-18.

[20] R.J. Anderson, M.G. Kuhn, Tamper resistance—a cautionary note, in: The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, CA, 18–21 November 1996, pp. 1–11.

[21] D. Agrawal, J.R. Rao, P. Rohatgi, Multi-channel attacks, in: C.D. Walter, Ç.K. Koç, C. Paar (Eds.), Cryptographic Hardware Embedded System—CHES 2003, Cologne, Lecture Notes in Computer Science, vol. 2779, Springer, Berlin, 2003, pp. 2–16.

[22] C. Karlof, D. Wagner, Hidden Markov model cryptanalysis, in: C.D. Walter, Ç.K. Koç, C. Paar (Eds.), Cryptographic Hardware Embedded System—CHES 2003, Cologne, Lecture Notes in Computer Science, vol. 2779, Springer, Berlin, 2003, pp. 17–34.

Eric Peeters was born in Brussels, Belgium, in 1979. He received the Electromechanical Engineering degree from the Université Catholique de Louvain in June 2002. He is currently a Ph.D. student of the UCL Crypto Group, under supervision of Pr. Jean-Jacques Quisquater. His research interests include digital design and FPGAs, design and hardware implementation of asymmetric ciphers and side-channel analysis.

François-Xavier Standaert was born in Brussels, Belgium in 1978. He received the Electrical Engineering degree and Ph.D. degree from the Université Catholique de Louvain, respectively in June 2001 and June 2004. In 2005, he was a Fulbright visiting researcher at Columbia University (Networks Security Laboratory) and MIT Medialab. He is now a post-doctoral researcher funded by the FNRS (Funds for National Scientific Research, Belgium), at the UCL Crypto Group. His research interests include digital design and FPGA's, cryptographic hardware, design of cryptographic primitives and side-channel analysis.

Jean-Jacques Quisquater is professor of cryptography and multimedia security at the Department of Electrical Engineering, Université Catholique de Louvain, Louvain-la-Neuve, Belgium. He is responsible, at least at the scientific level, of many projects related to smart cards (protocols, implementations, side-channels), secure protocols for communications, digital signatures, payTV, protection of copyrights and security tools for electronic commerce. He was the main designer of several coprocessors for powerful smart cards: CORSAIR (Philips) and FAME (Philips). He holds 17 patents in the field of smart cards. He is co-inventor of the so-called GQ cryptographic identification scheme.