10

# Characterization of the Information Leakage of Cryptographic Devices by Using EM Analysis

Olivier Meynard[1], Sylvain Guilley[1], Jean-Luc Danger[1],
Yu-Ichi Hayashi[2] and Naofumi Homma[2]
[1]*Telecom ParisTech*
[2]*Tohoku University*
[1]*France*
[1]*Japan*

## 1. Introduction

Cryptographic modules (software or hardware implementations of cryptographic algorithms) are widely used in our daily life in different applications in order to secure digital transactions and exchanges. In particular, cryptographic hardware is essential in smartcards, identification systems, mobile phones, pay television set-top boxes, transportation services and so on. This hardware component embeds cryptographic algorithms that are deemed safer and unbreakable from a mathematical point of view, and thus increases the confidence and robustness of cryptographic functions. However, the hardware implementation is still vulnerable to physical attacks. Side Channel Analysis (SCA) is a major threat for crypto-systems as they disclose some information about the internal process and the sensitive data. An electronic circuit needs some time to produce its results (such as a ciphertext in the case of encryption) and an amount of energy to switch states at each clock period. The operating times, the power dissipation, or the electromagnetic radiations are directly modulated by the data that are processed. Consequently the cryptographic device leaks some clues about the inner secrets and an attacker can retrieve secrets computed by the cryptographic device, just by analysing these externally measurable quantities without touching the component. Thus, those unintentional physical emanations can be analysed in a view to derive some sensitive information from them. Such analyses are altogether referred to as Side-Channel Attacks.

Since the mid-90s, side channel attacks have attracted a significant attention within the cryptographic community. In 1999, Kocher *et al.* described a side channel attack suitable for smart-cards: the power line, supplied from the card reader, is spied. This kind of attack is named Simple or Differential Power Analysis (SPA or DPA). With this cryptanalysis method an attacker can successfully reconstruct the secure data (Kocher et al., 1999a), either with one single measurement (SPA) or with many of them (DPA), using a statistical analysis. Two years later, Gandolfi *et al.* introduced the principles of the EMA, *i.e.* the ElectroMagnetic Analysis (Gandolfi et al., 2001). In fact Gandolfi applied the method of the DPA to electromagnetic emanations. EMA exploits correlation between secret data and variations in the emitted electromagnetic radiation. The EM radiation becomes an important

source of leakage because it can be conducted without tampering with the power supplies when the circuit under analysis is soldered on a printed circuit board (PCB). Such EM radiation has been studied as noise in the field of EMC (Electromagnetic Compatibility). Many studies on noise suppression or reduction have been conducted because noise interference can cause damage to other electronic devices in the vicinity. Some EMC-related committees have summarized the aforementioned knowledge and experiences, and have established guidelines on standardized acceptable values of EM radiation during device operations. Current electronic devices are usually designed so as to satisfy these EMC standards. However, these standards mainly aim to suppress and reduce EM radiation that disturbs other devices, but not necessarily the radiation that leaks secret information. Even if the EM radiation (*i.e.*, common-mode current) is below the value specified in the guidelines, extraction of secret key information from the radiation would remain a possibility. In fact, some previous studies (Kuhn, 2005) have demonstrated EM information leakage from electronic devices that are in compliance with the guidelines.

Addressing the above mentioned problem, this chapter investigates the possibility of EM information leakage at a distance from cryptographic devices. We first describe conventional side-channels, namely voltage drop and electromagnetic field, and then discuss how the common-mode current happens, contains the secret information and has a possibility of information leakage outside of cryptographic hardware. After briefly explaining the test device and the conventional SCA techniques, we present some measurement methods of common-mode current including those at a distance from the test device and their experimental results. Then we propose a method to investigate and characterize the EM radiation in frequency domain. With this characterization based on information theory we are in position to say which frequencies are carrying information. That helps us evaluate the possibility of EM analysis at a distance from cryptographic devices.

## 2. Side-channels

In this section, conventional and possible side-channels are described. As conventional side-channels, (i) voltage drop at an inserted resistor and (ii) electromagnetic fields close to the module are described. A mechanism behind EM propagation and radiation by ground bounce is also explained as a possible side-channel.

### 2.1 Conventional side-channels

Fig. 1 shows an overview of the conventional power-measurement method using a resistor (Kocher et al., 1999b). In this measurement, the transient current $I$ released from the power pins of the LSI is assumed to contain information leakage. The mechanism behind the leakage based on the switching behavior of CMOS gates is discussed in (Mangard et al., 2007). The current $I$ must be transformed into voltage units as general instruments (*e.g.*, digital oscilloscopes) which accept voltage signals. For this purpose, a small resistor is inserted in series between the pin and the PCB. The voltage observed at the resistor $R$ is $V = RI$ according to the Ohm's law. Then the attacker can measure the voltage $V$ which is proportional to the current $I$. Many studies have been using the above method due to its simplicity and reproducibility. When we consider the availability of measurement, however, the method involves manipulation (*i.e.*, insertion of a resistor) of the PCB and requires a contact to the PCB.

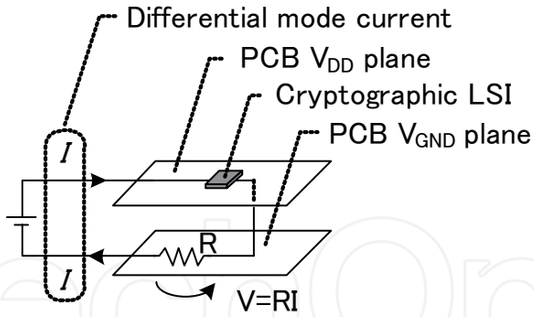



Fig. 1. Conventional side-channel: voltage drop.

The measurement method of EM field for SCAs is proposed in (Gandolfi et al., 2001), (Quisquater & Samyde, 2001) and is also being widely used. For the measurement, a magnetic field probe is placed very close to the chip. The probe transforms the magnetic field (or magnetic flux) into a voltage output based on the Electromagnetic Induction. Here, the output voltage $V$ is

$$V = -N\frac{\mathrm{d}\Phi}{\mathrm{d}t}, \tag{1}$$

where $\Phi$ represents the magnetic flux within the closed loop comprising the probe and $N$ is the number of the loops. Since $\Phi \propto I$, it follows that $V \propto \mathrm{d}I/\mathrm{d}t$. A magnetic probe directly outputs $V$, while a current probe outputs the value proportional to $I$ because of its loop integration. Although the output of the magnetic field probe is proportional to $\mathrm{d}I/\mathrm{d}t$ but not to $I$, a number of experiments have shown that the attack using the magnetic probe is feasible and efficient (Peeters et al., 2007). This method also requires close access to the PCB since the electromagnetic near field decreases in amplitude in proportion to $1/r^3$, where $r$ is the distance between the target and the probe. Therefore, signals measured from a distance suffer from the effects of external noise, resulting in a low S/N ratio.

### 2.2 Common-mode current

The above information leakage can be leaked via a different side-channel, which has a possibility that cryptographic modules can be attacked at distance. In the classical circuit theory, the level of the ground plane is assumed to be constantly zero. However, in reality, the ground level can change. Such transient voltage fluctuation in the ground plane is referred to as ground bounce. A transient current released from a digital circuit is a major source of ground bounce. Here, the released transient current $I$ is transformed into a voltage fluctuation $\Delta V$ through inductance.

Fig. 2 shows an image of ground bounce. The above inductance is distributed over the PCB since conductors with finite length (*e.g.*, pins and lead lines) have parasitic inductance. When a transient current $I$ is fed into such inductance, an electromotive force occurs due to electromagnetic induction (Sudo et al., 2004), which results in generating a voltage fluctuation $\Delta V$ in the ground plane. The fluctuation is expressed as the following equation (Sudo et al., 2004):

$$\Delta V = L_{eff} M \frac{\mathrm{d}I}{\mathrm{d}t}, \tag{2}$$

where $L_{eff}$ is the effective parasitic inductance, $M$ is the number of simultaneous switching outputs, and $\mathrm{d}I/\mathrm{d}t$ is the rate of the current change. The amount of $L_{eff}$ depends not only on

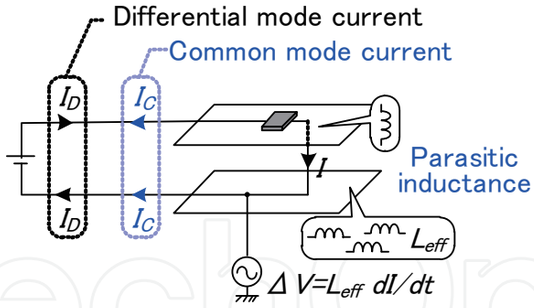



Fig. 2. Image of common-mode current.

the self-inductance within the cryptographic chip but also on the mutual inductance between the chip and the PCB. The voltage fluctuation caused by ground bounce can be modeled as an alternate voltage source as shown in Fig. 2. The model suggests that the voltage fluctuation can propagate to peripheral circuits through a common ground. Consequently, peripheral circuits, such as attached cables, are driven as antennas, which causes unintentional radiation via them (Hockanson et al., 1996).

Such radiation based on ground bounce is even more important since it generates common-mode current (Paul, 2006). If there is only differential-mode current as shown in Fig. 1, the electromagnetic fields radiated from the current pair (current with forward and reverse directions) are ideally canceled out since they are equal in amplitude and inverse in direction. The resulting radiation would be limited. In the case of common-mode current, on the other hand, the electromagnetic fields from the current pair are not cancelled out since their directions are the same. As a consequence, the common-mode current can cause strong radiation even if it is weak in amplitude. Assuming a transient current $I$ released from a cryptographic module causes a voltage fluctuation $\Delta V$. $\Delta V$ contains information leakage due to $\Delta V \propto \mathrm{d}I/\mathrm{d}t$. As a result, EMA would be possible by measuring the radiation driven by ground bounce. The mechanism also suggests that peripheral circuits interconnected to a cryptographic module can be an antenna responsible for information leakage.

## 3. Cryptographic devices

For the following experiments we employ a Side-channel Standard Evaluation Board (SASEBO-G) which is widely used as a uniform testing environment for evaluating the performance and security of cryptographic modules. Until now, various experiments associated with side-channel attacks are being conducted on the SASEBO boards, and many useful results are being expected to support the international standards work[1]. Fig. 3 shows the SASEBO-G used in these experiments, which employs two Xilinx FPGAs ; one FPGA is used to implement a cryptographic module in hardware or software and the other FPGA is dedicated to communicate with a host computer through either RS-232 or USB cables.

Two kinds of major cryptographic algorithms are implemented in one FPGA for the experiments: RSA crypto-system and AES (Advanced Encryption Standard) block encryption.

[1] http://www.rcis.aist.go.jp/special/SASEBO/index-en.html

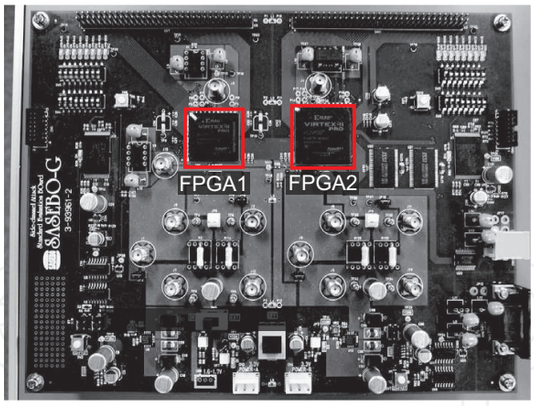



Fig. 3. Overview of SASEBO-G.

### 3.1 RSA crypto-system and SPA/SEMA

The RSA crypto-system, proposed by Rivest, Shamir, and Adleman in 1977, is one of the most popular public-key ciphers. The encryption and decryption operations are given by simple modular exponentiation:

$$C = P^E \bmod N, \tag{3}$$

$$P = C^D \bmod N, \tag{4}$$

where $P$ is the plaintext, $C$ is the ciphertext, $E$ and $N$ are the public keys, and $D$ is the secret key. Modular exponentiation is also used in other public-key ciphers such as ECC (Elliptic Curves Cryptography), and thus the following analysis technique can be widely applied to other public-key ciphers. The binary method (*aka* the square-and-multiply method) is known to be the most efficient exponentiation algorithm and is frequently used for actual applications, such as smartcards and embedded devices, because of its simplicity and low resource consumption. This algorithm performs multiplication and squaring sequentially according to the bit pattern of one exponent ($E$ or $D$). There are two variations of the algorithm. The left-to-right binary method starts at the exponent's MSB and works downward. The right-to-left binary method, on the other hand, starts at the exponent's LSB and works upward. **ALGORITHM I** shows a left-to-right binary method for scanning the bits of the exponent from MSB to LSB. Each multiplication (or squaring) operation requires a large number of clock cycles due to the large length of the operand. This algorithm always performs a squaring at Line 3 regardless of the scanned bit value, but the multiplication at Line 5 is executed only if the scanned bit is equal to 1.

The basic sequence in the binary method is not changed even when major acceleration techniques such as Montgomery multiplication (Montgomery, 1985) and the Chinese Remainder Theorem (CRT) (Menezes et al., 1996) are applied to the exponentiation computation.

With this algorithm for the next experiment, we perform SPA/SEMA (SEMA is the electromagnetic counterpart to SPA) in order to distinguish between multiplication and squaring in the power/EM waveform. Fig. 4 shows an image of the SEMA on an RSA module using the left-to-right binary method. When the difference between multiplication

**ALGORITHM I**

MODULAR EXPONENTIATION (LEFT-TO-RIGHT BINARY METHOD) FOR A SECRET KEY OF BIT LENGTH $k$.

| | |
|---|---|
| Input: | $X$, $N$, $E = (e_{k-1}, ..., e_1, e_0)_2$ |
| Output: | $Z = X^E \bmod N$ |

```
1 : Z := 1;
2 : for i = k − 1 downto 0
3 :     Z := Z * Z mod N;        – squaring
4 :     if (e_i = 1) then
5 :         Z := Z * X mod N;    – multiplication
6 :     end if
7 : end for
```

and squaring appears as shown in this figure, the key bit pattern '10100' can be derived from the knowledge of the algorithm.

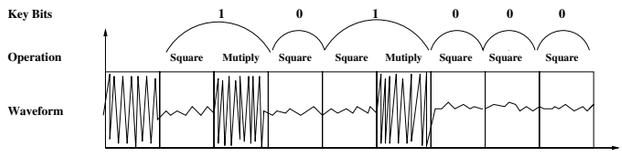



Fig. 4. Image of Simple Electromagnetic Analysis (SEMA) on RSA module.

If RSA is simply implemented with binary methods, definite vulnerabilities could exist. For example, differences between a conditional branch or an instruction sequence could be observed in the power/EM waveforms, giving strong clues about the value of the secret exponent. Even if the squaring and multiplication are performed using the same processing unit controlled by the same sequencer logic, chosen-message approaches that use specific data (Novak, 2002)–(Fouque & Valette, 2003)(Schramm et al., 2004)(Homma et al., 2008) can further enhance these differences.

One simple idea is to choose a message that has a large number of 1s (or 0s) in the bit sequence Miyamoto et al. (2008). For example, an input value of $2^{-k} \mod N$ or $R^{-1}$ (with $R = 2^k \mod N$) may produce large differences between the multiplication and the squaring operations for implementations using Montgomery multiplication because $R^{-1}$ is converted into the Montgomery domain in $Y = R^{-1}R = 1 \bmod N$ and an input of 1 is always multiplied in the modular multiplication operations. The power consumed by the multiplier for modular multiplication should be much lower than that for modular squaring that does not have an input of 1.

### 3.2 AES crypto-system and differential analysis

The AES is a symmetric encryption algorithm based on a SPN (Substitution Permutation Network) structure, which has a fixed block size of 128-bits and a key size of 128-bit, 192-bit, or 256-bit, that determines the number of encryption rounds (to respectively 10, 12 or 14). For our experiments, we consider the 128-bit block version that consists in 10 rounds encryption. It operates on a $4 \times 4$ array of Bytes termed the state. The AES cipher is specified as a certain number of operations per round that convert the input plain-text into cipher-text. One round of encryption consists of four operations: SubBytes, ShiftRows, MixColumns and AddRoundKey. The encryption period starts with a single AddRoundKey

operation followed by nine identical encryption rounds. The final encryption round operates without any MixColumns operation. These adaptations removes cryptographically ineffective operations and allows for a decryption process that is very close to the encryption process. Simultaneously the key schedule is computed: it derives enough keys to provide for each round a different subkey.

An attacker uses an hypothetical model of the device under attack to predict its electromagnetic radiation. These predictions are correlated with the measured samples. The DPA was proposed by P. Kocher in (Kocher et al., 1999b) and is based on Hamming Weight model. For our attacks, we have chosen to use the CPA (Correlation Power Analysis). This approach is based on the Hamming distance model proposed by É. Brier *et al.* in (Brier et al., 2004) for the first time. For this CPA, the outputs of S-Box are targeted on the last round of the AES to reveal one Byte of the secret key. Given the cipher and the results of the tenth round, the attacker can predict the leakage by computing the Hamming distance model between two states of the register. An hypothesis can be made for eight bits of the key that corresponds to output of the S-Box. To perform this attack some measures of electromagnetic emanation of the device are collected. For one hypothesis of 8 bits of the subkey the attacker has to calculate $256(=2^8)$ differential traces for all the subkey candidates. After that, the attacker has to predict the electromagnetic radiation when the bits of the register toggle. Let $X_i$ and $X_{i+1}$ be two consecutive values inside a register. An estimation of the radiated emanation at the time of the transition could be provide by the computation of the selected function $HD = HW(X_i \oplus X_{i+1})$ where $HD$ is the Hamming Distance and $HW$ the Hamming Weight. After that the attacker estimates the maximum likelihood between the theoretical predictions and the measurements by the Pearson correlation factor $\rho(W, HD)$ between the Hamming distance model and the measured power. It is defined as:

$$\rho(W, HD) \doteq \frac{\text{cov}(W, HD)}{\sigma(W) \cdot \sigma(HD)},$$

where $W$ represents the measurement and $HD$ the Hamming distance. We notice that $\rho(W, HD)$ follows the Cauchy-Schwarz inequality: $-1 \leq \rho(W, HD) \leq +1$. The correct key is obtained when the right key hypothesis provides the largest or smallest values of $\rho(W, HD)$. In other words, a spike is observed in the differential curve when the correct partial subkey bits have been used and where the selection function is correlated to the value of the bit being manipulated. The success of this attack depends on the number of the measured traces. Obviously this number will be changed with the distance between the component and the probe, with the selected element of the hardware implementation (S-Box) and with the leakage model used in selected function.

## 4. First experiments

### 4.1 Electromagnetic analysis based on common-mode current

Fig. 5 and Fig. 6 show a block diagram and overview of the measurement setup, respectively. The measurement system consists of the SASEBO, a digital oscilloscope, and a personal computer (PC). The SASEBO is equipped with two FPGAs, namely *FPGA1* and *FPGA2*. These two FPGAs work by using power supplied from on-board regulators and clock signal provided by an external function generator. Experiments are conducted by implementing cryptographic cores (circuits) on *FPGA1*.

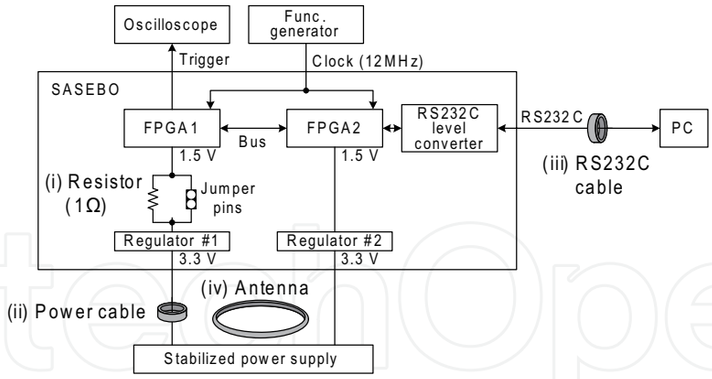



Fig. 5. Block diagram of measurement setup.

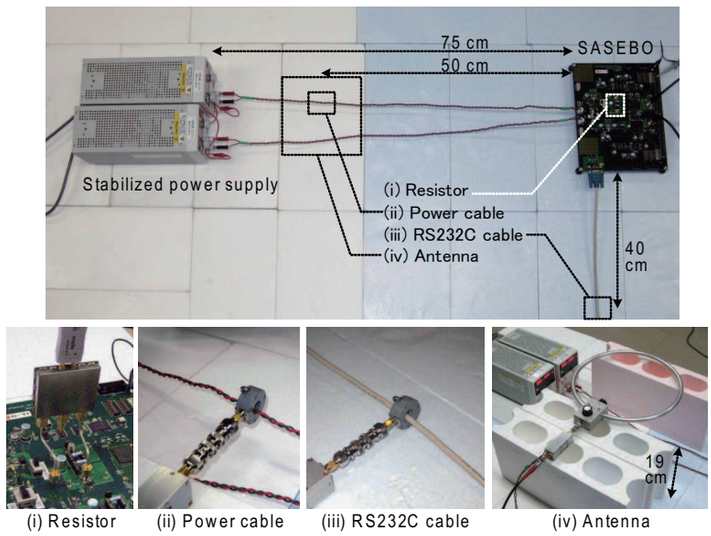



Fig. 6. Overview of four measurement methods.

Four types of measurements are conducted: (i) the voltage drop across a resistor, the current flowing in (ii) the attached power cable and (iii) the communication cable (RS232C cable), and (iv) the magnetic field around the power cable. Hereafter, these are referred to as (i) *Resistor*, (ii) *Power cable*, (iii) *RS232C cable*, and (iv) *Antenna*. It is important to emphasize that the measuring points (ii) and (iii) are not directly connected to *FPGA1*; there are circuit components (*e.g.*, voltage regulators and an RS232C level converter) between the measurement points and *FPGA1*. In addition, the locations of the measurements are about 50 cm away from the board.

Measurement instruments are summarized in Table 1. The details of the measurement methods are as follows. In measurement (i), the voltage drop across a 1-Ohm resistor inserted between the ground pin of *FPGA1* and the ground plane of the PCB is measured using a differential voltage probe. Note that the 1-Ohm resistor is short-circuited during the measurements (ii)-(iv) by using jumper pins.

In the measurements (ii) and (iii), the current flowing in cables is measured by the current probe clamping the cables as shown in Figs. 6(ii) and (iii). The measured voltage is proportional to the flowing current as described above. In measurement (ii), both lines (for

| | |
|---|---|
| Oscilloscope | Agilent MSO6104A<br>(with 25 MHz low-pass filter) |
| Voltage probe for (i) | Agilent 1130A differential (voltage) probe with<br>SMA probe head |
| Current probe for (ii) and (iii) | Fischer F-2000 current probe<br>(10 MHz – 3 GHz) |
| Current probe for (ii) and (iii) | AOR LA380 Wideband Active Loop Antenna<br>(10 kHz – 500 MHz) |
| Pre amplifier for (ii)-(iv) | MITEQ AM-1594-9907 (+51 dB, 300 kHz – 3.0 GHz) |

Table 1. Measurement instruments

$V = DD$:3.3 V and $GND$: 0 V) of a twisted pair cable are clamped, while the whole body of RS232C cable is clamped for measurement (iii). Since both of the current pairs are clamped, radiation due to differential-mode current is cancelled out within the probe, and thus the contribution only by the common-mode element is measured.

In the measurement (iv), a magnetic field around the power cable is measured using an antenna. We used an off-the-shelf indoor loop antenna which is used for amateur radio. We placed the antenna over the power cable at the height of about 20 cm and tuned it to maximize the measured amplitude in the range of 3–40 MHz.

In each measurement, the frequency bands of measured signals are limited up to 25 MHz by a low-pass filter equipped with an oscilloscope. This is because the measured raw traces were highly contaminated by high-frequency noise that interfered with the measurements. In addition, a trigger signal generated by the *FPGA1* is used in order to align the measured traces in time. As a probe for the trigger signal has a physical contact to the board, the measurements are not exactly contactless. However, the setup is enough to examine information leakages from the measuring points (i)–(iv). In practical scenario, an attacker would have difficulty in taking a trigger without any contact to the target, yet it is still possible. One practical way is to observe communication cables and then obtain a trigger from a specific binary sequence on them. In addition, the attacker can consult signal processing techniques to achieve precise waveform alignment (Homma et al., 2006).

#### 4.1.1 SEMA on RSA implementation

A 1,024-bit RSA circuit using a left-to-right binary method is implemented on *FPGA1*. Modular multiplication and squaring are performed by high-radix Montgomery multiplication algorithm using a 32-bit multiplier (Cryptographic Hardware Project, n.d.). In this implementation, one Montgomery multiplication requires 4,386 cycles, and the total number of cycles for the modular exponentiation (1,024-bit RSA operation) is approximately 7 million cycles. The parameters (*i.e.*, the key and the plaintext) are embedded into the *FPGA1* in order to allow *FPGA1* to operate as a standalone module. The goal of the attack is to distinguish between multiplication and squaring in the measured trace. Since we are interested in the difference between the measurements (i)–(iv), a chosen input message of $2^{1024}$ is used to enhance the difference between the multiplication and squaring.

Fig. 7 shows the results of the SEMA. The traces are measured at a sampling frequency of 400 MSa/s. Each of the traces is aligned in time, in which the modular exponentiation

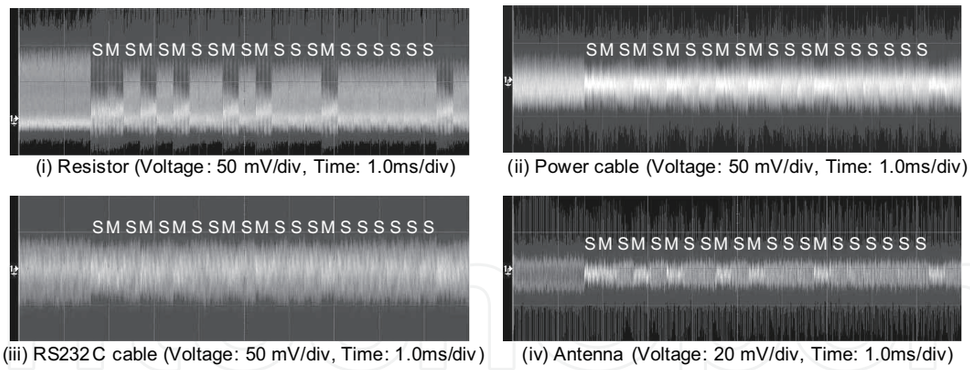



Fig. 7. Results of SEMAs on RSA.

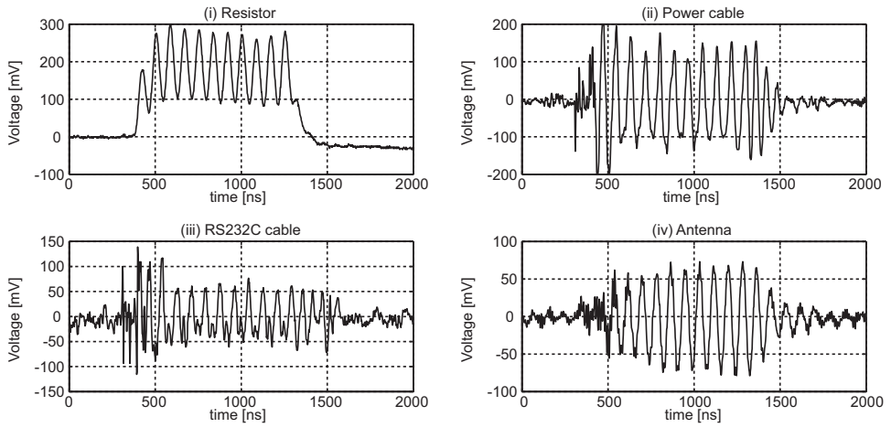



Fig. 8. Examples of measured waveforms.

starts at around 1.5 ms. Sequences of symbols 'S' and 'M' shown in the figure represent the corresponding squaring and multiplication operations, respectively.

The result of measurement (i) shows large difference between multiplication and squaring with multiplication having lower spikes compared to squaring. Although the differences are smaller than (i), they are still visible in results (ii)–(iv). The results indicate that it is possible to reveal a secret key by using any of the measurements (i)–(iv).

#### 4.1.2 DEMA on AES implementation

In the experiments, an AES circuit, retrieved from the reference (Cryptographic Hardware Project, n.d.), supporting a 128-bit key is implemented on *FPGA1*. The circuit uses a loop architecture, where one round operation is performed every clock cycle. As a result, one encryption takes 10 clock cycles for round operations and an additional clock cycle for data I/O. *FPGA2* is configured as the control and communication circuits, and plaintexts are fed from the PC into *FPGA1* via *FPGA2*. During the encryption, the corresponding traces are captured from the four measurement points at a sampling frequency of 500 MSa/s. The measurements are repeated for 30,000 different plaintexts, and the corresponding 30,000 traces are stored for each measuring points. Examples of the measured traces are shown in Fig. 8, where the encryption process starts at around 400 ns and finishes after 11 clock cycles or 916 ns (=11$\times$ 1/12 MHz).

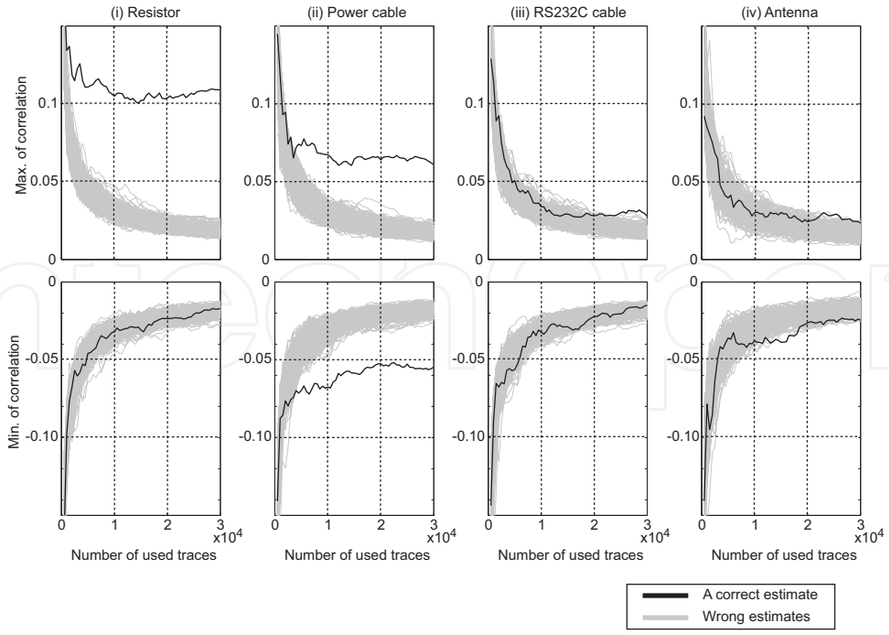



Fig. 9. Measures to disclosure in DEMA on AES.

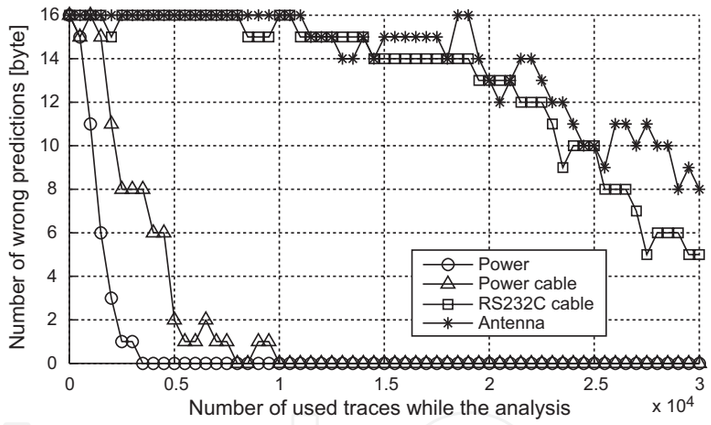



Fig. 10. Results of DEMAs on AES.

CPA (or CEMA) is applied to these traces. The 128-bit (16-Byte) register containing intermediate data is chosen as a target. The power (or EM radiation) estimates are calculated by counting changed bits of the target register in the final round of AES encryption. Here, Hamming distance model (Brier et al., 2004) is used as power model. Key candidates are searched by Byte. In other words, we generated a total of 16 power estimates corresponding to 16 Bytes of the round key. In the analysis phase, the linearity is evaluated by using Pearson's correlation coefficient.

The results are shown as error rates in Fig. 9 and Fig. 10. Fig. 9 shows the Measurement to disclosure (MTD) graph of each result. On the other hand, Fig. 10 shows error rates where the vertical axis represents the number of incorrectly predicted round-key Bytes and the horizontal axis shows the number of traces. Since the length of the secret key is 16 Bytes

(= 128 bits), the vertical value ranges between 0 and 16, where 0 indicates the successful extraction of the whole key (*i.e.*, completion of the attack).

In the analysis with the measurement (i), the key prediction is successful when the correlation with the correct key is the highest among $2^8$ candidates. On the other hand, in (ii)–(iv), the difference between maximum and minimum coefficients is used instead of the maximum coefficient since the results of (ii)–(iv) show correlation in both the positive and negative directions as shown in Fig. 8.

As shown in Fig. 10, the result for (i) goes to zero (*i.e.*, extract the whole key) fastest by 3,000 traces. In addition, the attack using the power cable (ii) also shows fast extraction. On the other hand, the attacks using the RS232C cable and the antenna require much larger number of traces. However, the error rate decreased gradually as the number of used traces increased. Therefore, we can say that all the EMAs can successfully reveal the secret keys.

#### 4.1.3 Discussion

As shown above, the contactless SEMAs and DEMAs worked well, but the traces from (ii)–(iv) contained smaller amount of information leakage or larger noise in comparison to that from (i). Various disturbing factors between the FPGA and the measuring points have effects on the results. Such factors include the filtering effect of parasitic circuit, the compensation effect of regulators, and external noise, and so on.

For example, there is an on-board regulator between the chip's power supply pins and the power cable. Since regulators are designed to stabilize their output voltage, they feature buffering and feedback control in order to suppress voltage fluctuation. The results of (ii) indicate that the voltage fluctuation containing information leakage was able to overcome the effects of the regulator.

Measurement (iii) is also affected by such disturbing factors. In the experimental setup, the RS232C cable is connected to *FPGA1* via an RS232 level converter and *FPGA2*. First, the RS232 level converter has the same effect as the voltage regulator. In addition, *FPGA1*, *FPGA2*, and the RS232C level converter have their own separated ground planes and they are connected via noise filters (inductors). This feature is used in SASEBO in order to measure side-channel information only from *FPGA1* without those from other components. The noise filters act as low-pass filters for current through them. However, the success of measurement (iii) indicates that the voltage fluctuation from *FPGA1* can propagate to the other part of the board even if such high-frequency current is filtered out. The results suggest that the propagation of the voltage fluctuation is rather robust and should be prevented by countermeasures.

### 4.2 Attack at distance

Now we demonstrate that Correlation-based on ElectroMagnetic Analysis (CEMA) on a hardware-based high-performance AES module is possible from a distance as far as 50 cm (Meynard et al., 2010). The aim of this experiment is to mount a successful Correlation Power Analysis (CPA (Brier et al., 2004)) and retrieve cryptographic elements, without any additional device, such as a demodulator or a TEMPEST receiver. The device whose EM emanations are studied is cadenced by a clock running at 24 MHz. For these low frequencies, the usage of a Faraday cage is not needed as it would induce some EM reflections and could alter the measurements. Furthermore, the size of the absorber would be too large for this range

of frequencies. Therefore, the material is placed on a plastic table that limits the reflection of EM radiation and avoids the conducted radiation. A plastic rod is placed perpendicularly to the board and is considered as a vertical axis to move the antenna by steps of 5 cm, as shown in the figure 11.

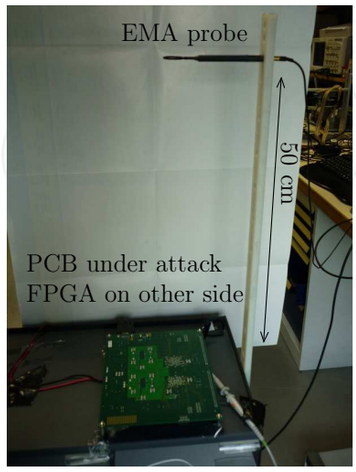



Fig. 11. EM measurement test bench with its antenna on a plastic rod.

We take care of keeping far away the power supply from the chip board, in order to avoid any coupling between the radiated waves and the power supply. We record the emanations on the side with the decoupling capacitors, because the signal on this part of the board has the best quality.

Firstly we check that for different distances, the curves for the same plaintext are scaled down, according to an inverse power law. as illustrated in figure 12.

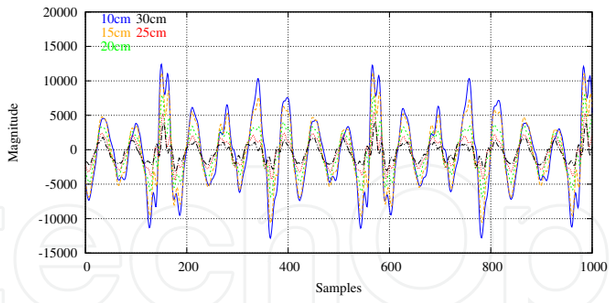



Fig. 12. Quasi-homothetic downscale of the raw curves at different distances.

In practice, the signal was amplified of 60 dB and averaged by a factor of 4096. The attack needs 51,519 measurements to break the Sbox #1, whereas only 1,000 are required at $d = 0$ cm. The correlation curve is represented in figure. 13. The correlation does not clearly stand out. We assume that the attack requires so many traces to fully disclose the key because the Hamming model is not holding anymore at this large distance. Then we propose to study the distortion of the leakage model with the distance.

It has already been noticed in the literature that the Hamming distance is not the best model in the case of very near-field analyses. For example, authors in Peeters et al. (2007) proves that under some circumstances, an ASIC can have a transition-dependent leakage. In this section,

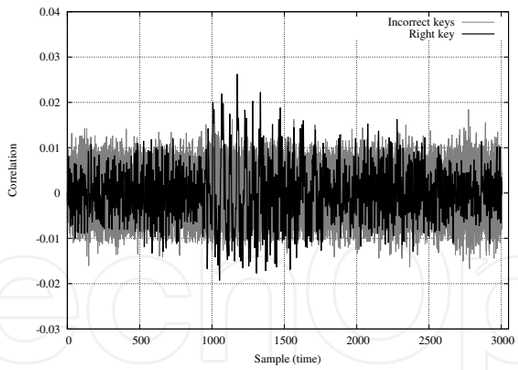



Fig. 13. CEMA on Sbox #1 at a distance $d = 50$ cm.

we show that the Hamming distance model is adequate for intermediate distance fields EM analyses, but that it distorts seriously in far-field analyses.

In near-field the leakage obeys a Hamming distance model: it is an affine function of the number of bit transitions between two consecutive states. On one hand, the Hamming distance is confirmed at $d = 0$ cm, as attested by figure. 14, at 15 cm, the model is chaotic and not consistent with an identical amount of dissipation per bit making up the analyzed Byte.

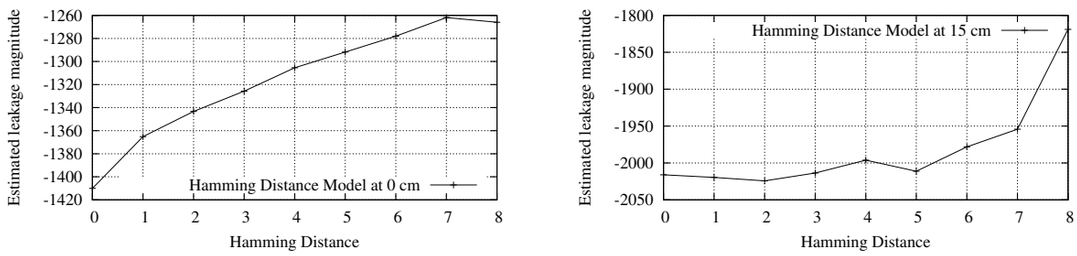



Fig. 14. Hamming distance at 0 cm and at 15 cm.

We target the Sbox #1, which exercises all the 256 transitions and propose to characterize the leakage to disclose the Sbox #1 on the tenth subkey of the AES. First we search the index $t_c$ of the maximal correlation, that corresponds to the moment when the data are stored in the register on the last round. Then we compute for this index the average and the variance for the 256 possible Hamming distances, the key and the message being known. The figure 15 depicted the leakage model at 50 cm.

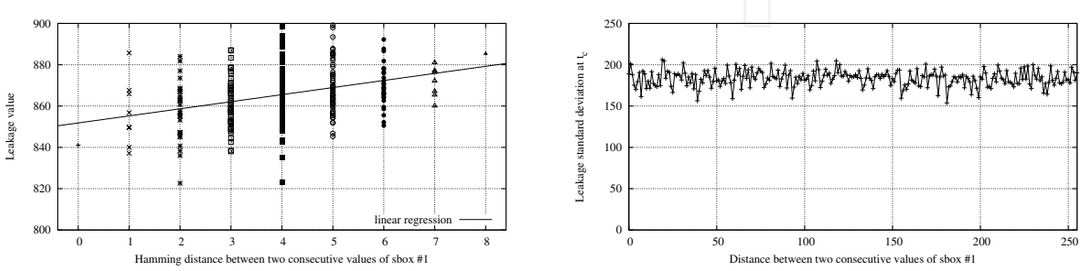



Fig. 15. Model at 50 cm for the Sbox #1.

We can observe that the standard deviation is almost independent of the Byte distances. Therefore, most of the model information is contained in the mean leakage value.

We notice that the leakage model distorts more and more with the distance. Therefore, we show that the leakage model change according to thresholds. Three regions can be identified: in near-field, the switching distance is the most suited, as initially observed in the article (Peeters et al., 2007); in medium-distance ($d \in [0,5]$ cm), the Hamming model is adequate; in long-distance ($d > 5$ cm), the model becomes less relevant.

We target in this topic situations where the difference of nature is not artificially due to a countermeasure, but naturally by the distortion into the communication channel between the leaking device and the side-channel sensor.

## 5. Characterization of the frequencies

EM radiations arise as a consequence of current flowing through diverse parts of the device. Each component affects the other components' emanations due to coupling. This coupling highly depends on the device geometry. Now we describe a measurement of EM radiation from a cryptographic device, whose intensity is a major suppression target in the EMC research field. We first generate an EM-field map on the entire surface of the device, and then pinpoint the points being high in EM-field intensity. Fig. 16 shows an overview of the EM measurement system in this experiment. The experimental scanner (WM7400) employs a micro EM probe whose bandwidth ranges from 1 MHz to 3 GHz, and scans the surface of the SASEBO. The probe head is arranged precisely at 2-cm distance from a target device within a tolerance of one micrometer. The system can measure the distance by the equipped laser geodesy.

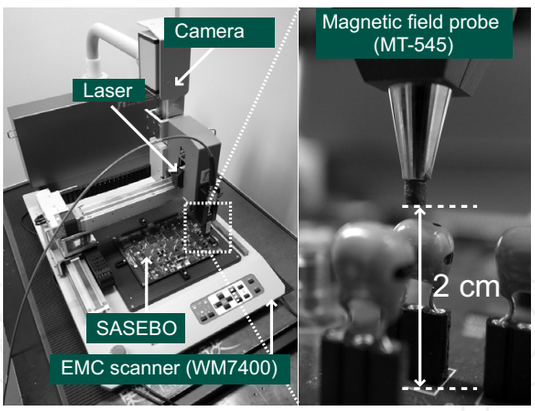
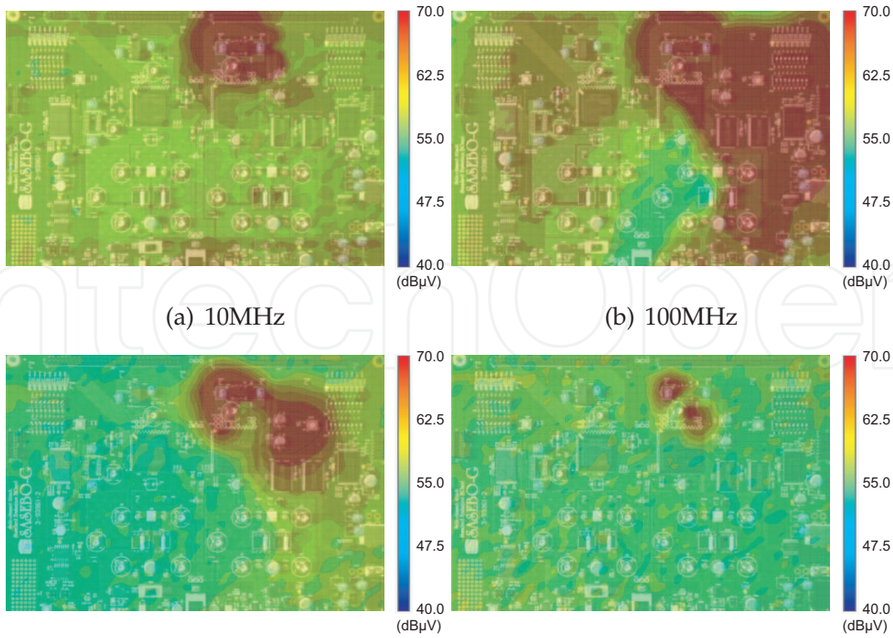



Fig. 16. EM measurement system.

Fig. 17 shows EM field maps on the entire surface of the SASEBO corresponding to the frequency bands ranging between (a) 10-100 MHz, (b) 100-200 MHz, (c) 200-300 MHz, and (d) 300-400 MHz, where the red and blue areas indicate higher and lower intensities, respectively.

The result shows that specific areas around *FPGA2* and a crystal oscillator, which is located at the upper side of *FPGA2* in Fig. 3, have higher EM-field intensities than other areas. This is because only the two components are active components on the board. We confirmed from the result that the EM-field intensity at the clock frequency is relatively higher than those of other frequencies. The phenomena of compromising signal has different origins such as




(a) 10MHz (b) 100MHz

(c) 200MHz (d) 300MHz

Fig. 17. Subfigure with four images

radiation emitted by the clock, crosstalk or coupling. Traditionally, we differentiate the direct emanations and the indirect or unintentional emanations. The first ones can be considered at a very short distance and requires the use of special filters to minimize interference with baseband noise. The direct emanations come from short bursts of current and are observable over a wide frequency band. On contrary, indirect emanations are present in high frequencies. According to Agrawal (Agrawal et al., 2002) these emanations are caused by electromagnetic and electrical coupling between components in close proximity. Often ignored by circuits designers, these emanations are produced by a modulation. The source of the modulation carrier can be the clock signal or other sources, including communication related signals. Li *et al.* provide in (Li et al., 2005) a model to explain such kind of modulation.

Therefore it is sometimes easier to extract information from signals unintentionally modulated at high frequencies, which are not necessarily related to the clock frequency, than baseband signals also referred to as direct emanations. The characterization of the frequencies that modulate the leakage is a scientific challenge, since as of today no relevant tool allows to distinguish which frequencies actually contain the sensitive information. For this reason, we propose a methodology in the following based on information theory.

### 5.1 Characterization of the EM channel in frequency domain

For the same bit sequence as in Figure 4, we obtained the EM trace illustrated on Figure 18. No difference appears between a square and multiply, even when messages are chosen to improve the result. We have even tried to improve the analysis using pattern matching techniques but without any satisfactory results in terms of contrast. First of all, the noise effect is decreased if the frequency band is reduced. Secondly, the leaked information is properly digitized whereas the strong carrier without relevant information is removed. Therefore it appears

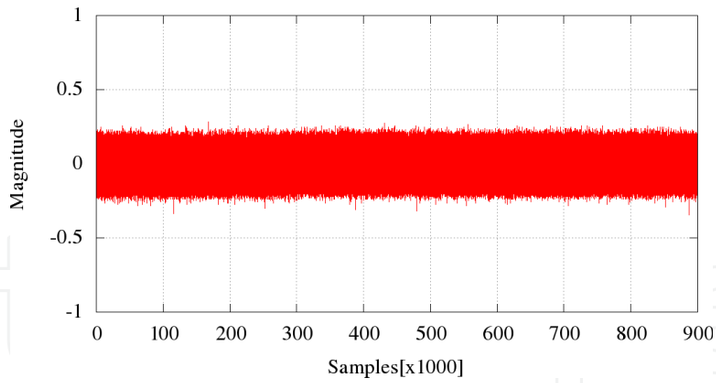



Fig. 18. Direct EM radiations emitted during an RSA computation.

strategic to find right modulated carrier. A straightforward technique consists in using a spectral analysis in order to detect the strong carrier frequencies. Another possible technique consists in scanning the frequency range of the wide-band receiver, but such demodulation process is time-consuming and one may omit some significant compromising signal. Another technique based on the STFT (Short Time Fourier Transform) has been proposed in (Vuagnoux & Pasini, 2009), but it consumes a huge amount of time as well as memory resources. We propose therefore a method based on information theory to characterize the leakage. After this characterization we are able to select the frequencies and their associated optimal bandwidth. The useful information is contained in these ranges of frequencies. Therefore, with a receiver tuned on the right frequency, we can retrieve the compromising signal. To provide this characterization, we propose an approach based on information theory. This method can be managed as follows: First we gather a large number of measurements, by knowing the key *i.e.* the operations that are computed by the chip. These EM measurements from the antenna are noisy, distorted and the operations are not distinguishable. For this step, we chose a time window where only one operation of square and one operation of multiply are performed as shown on Fig. 19. After the measurements are cut according to the operation performed. The number of samples is equal in each part of the signal, Each section of the signal is equal in term of number of samples, we get as much parts of EM signal for the multiplication as for the squaring, and we obtain two sets of measurements with the same number of traces.

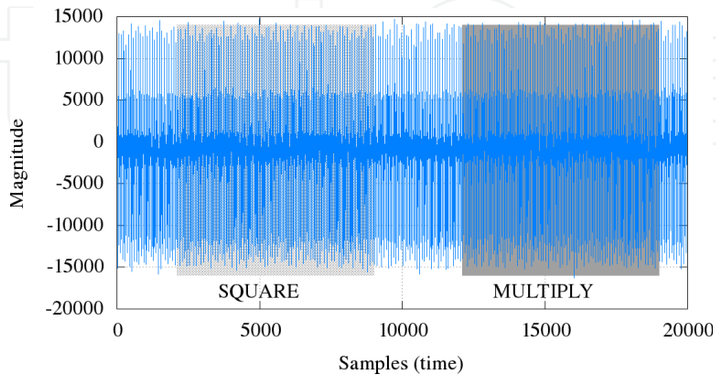



Fig. 19. EM measurement split into Square and Multiply parts.

Then, for each set, we compute: the FFT (*Fast Fourier Transform*) of every observation $O_f$; the mean spectrum related to each operation; and the mean of all the observations. Therefore

we obtain a specific spectral signature for each operation of the modular exponentiation algorithm. Finally we compute the Mutual Information value for each frequency. Thus we attribute a specific spectral signature to each operation of the modular exponentiation algorithm. In few words, we follow the processing shown in ALGORITHM 3.

**ALGORITHM 3**

| | |
|---|---|
| Input: | $O = (O_0, ..., O_{n-1}, O_n)$ Observation in time domain, |
| | $S = (S_0, ..., S_{n-1}, S_n)$ Secret (Operation) |
| Output: | Result of Mutual Information in frequency domain |
| 1 : | **for** $i = 0$ **to** $n$ |
| 2 : | Sort $O_i$ Observation according to the Secret $S_i$; |
| 3 : | Compute the FFT of each Observation $O_i$; |
| 4 : | **endfor** |
| 5 : | Compute the mean $(\mu_{Square}, \mu_{Multiply})$ and the variance $(\sigma_{Square}, \sigma_{Multiply})$ |
| 6 : | Compute the Mutual Information in frequency domain. |

As a distinguisher we take for instance an information theory viewpoint to retrieve the relevant frequencies and to bring a mathematical proof that the information is not necessarily carried by the clock frequency. In 2008, Gierlichs introduced in (Gierlichs et al., 2008) the Mutual Information Analysis. This tool is traditionally used to evaluate the dependencies between a leakage model and observations (*or Measurements*). We use MIA like in previous chapter but in this case we compute for each frequency the Mutual Information (MI) $\mathrm{I}(O_f; Operation)$ between Observations $O_f$ and $Operation$ that corresponds to the operations performed by the device (Meynard et al., 2011). Thereby, if $\mathrm{I}(O_f; Operation)$ is close to zero for one frequency $f$, we can say that this frequency does not carry significant information. On the contrary, if $\mathrm{I}(O_f; Operation)$ is high, the computed operation and the frequency are bound. As a consequence if we filter the EM signal around this frequency, we can retrieve the operations and the secret key using the SEMA.

The MI is computed as:

$$\mathrm{I}(O_f; Operation) = \mathrm{H}(O_f) - \mathrm{H}(O_f|Operation), \tag{5}$$

where $\mathrm{H}(O_f)$ and $\mathrm{H}(O_f|Operation)$ are respectively the entropies of all the observations in the frequency domain and of the observations knowing the operations. Both these entropies can be obtained according to:

$$\mathrm{H}(O_f) = -\int_{-\infty}^{+\infty} \Pr(O_f) \log_2 \Pr(O_f),$$

$$\mathrm{H}(O_f|Operation) = \sum_{j \in \{Multiply, Square\}} \Pr(j)\mathrm{H}((O_f|j)).$$

$$\text{with } \mathrm{H}(O_f|j) = -\int_{-\infty}^{+\infty} \Pr(O_f|j) \log_2 \Pr(O_f|j),$$

where $\Pr(O_f)$ denotes the probability law of observations at frequency $f$. Moreover we consider that the computed operations are equi-probable events, for our time windowing therefore $\forall j \in Operation, \Pr(j) = \frac{1}{2}$. And the distribution is assumed to be normal $\sim N(\mu, \sigma^2)$

of mean $\mu$ and variance $\sigma^2$, given by:

$$\Pr(O_f) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(O_f-\mu)^2}{2\sigma^2}\right).$$

We call it a parametric model. We approximate this model by a parametric estimation, and we use the differential entropy defined like a 1-dimensional normal random variable $O_f$ of mean $\mu$ and standard deviation $\sigma$ as the analytical expression: $H(O_f) = \log_2(\sigma\sqrt{2\pi e})$. From this value, the Mutual Information defined in Eqn. (5) can be derived, by computing for each operation the differential entropy:

$$\begin{aligned} \mathrm{I}(O_f; Operation) = \mathrm{H}(O_f) \\ - \frac{1}{2}(\mathrm{H}(f|Multiply) + \mathrm{H}(f|Square)), \end{aligned}$$

that can be simplified as:

$$\mathrm{I}(O_f; Operation) = \frac{1}{2}\log_2 \frac{\sigma^2_{O_f}}{\sigma_{O_f,Multiply}\sigma_{O_f,Square}}. \quad (6)$$

The figure 20 represents the result of Eqn. (6). From this graph, we notice that the information might be contained in a range of frequency between 5.0 and 60.0 MHz with the presence of a large lobe spread over these frequencies.

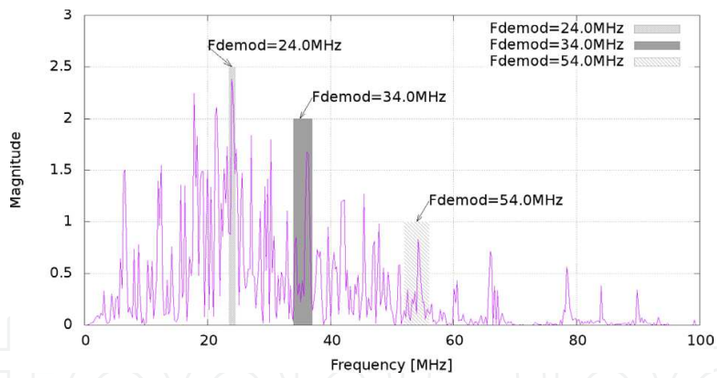



Fig. 20. Result of MIA in frequency domain.

This method provides a result with a quantity expressed in bit, that allows us to interpret easily the leakage frequencies regarding the level of compromising signal. Consequently, we are now able to fairly compare the level of compromising signal carried by different frequencies. Such Mutual Information metric allows to quantify the level of protection against SEMA attacks. Moreover it is worthwhile to underline that Mutual Information considers the non-linear dependencies that occur during the computation, such as cross-talk that occurs during the computation. The maximum in Magnitude is obtained for the frequencies around 24.0 MHz, that corresponds to the clock frequency of the component. We decide to pick up three ranges of frequencies corresponding to three peaks in Fig. 20:

- around 24.0 MHz,

- around 34.0 MHz,
- around 54.0 MHz.

and study the results of the demodulation at these frequencies to prove the efficiency of our approach.

In (Agrawal et al., 2002) Agrawal used a demodulator to measure EM emanation from an SSL accelerator. We apply a similar technique to the FPGA implementation which consumes far less power than the SSL accelerator. The EM radiation is expected to be much weaker than the previous one. We focus on a range of frequencies between 0.0 and 100.0 MHz and demodulate at the frequencies exhibited by the previous methods at 24.0 MHz, 34.0 MHz and 54.0 MHz. We employ the demodulation technique to investigate unintentional (or indirect)emanation. Each time, the demodulated signal shows a peculiarity that allows to distinguish clearly the two distinct operations.

The unintentional emanation described by Agrawal is the result of modulation or intermodulation between a carrier signal and the sensitive signal. In particular, the ubiquitous clock signal can be one of the most important sources of carrier signals. This assumption is confirmed by our results on figure 20. We tune the receiver to the clock frequency (*i.e.*, 24MHz) with a resolution bandwidth of 1MHz. Figure 21 shows one single demodulated EM waveform at 24 MHz. Indeed, the receiver improves the differences between the two operations dramatically as shown in Fig. 21.

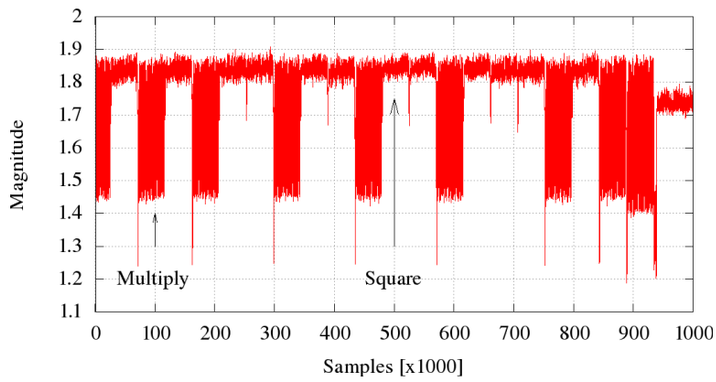
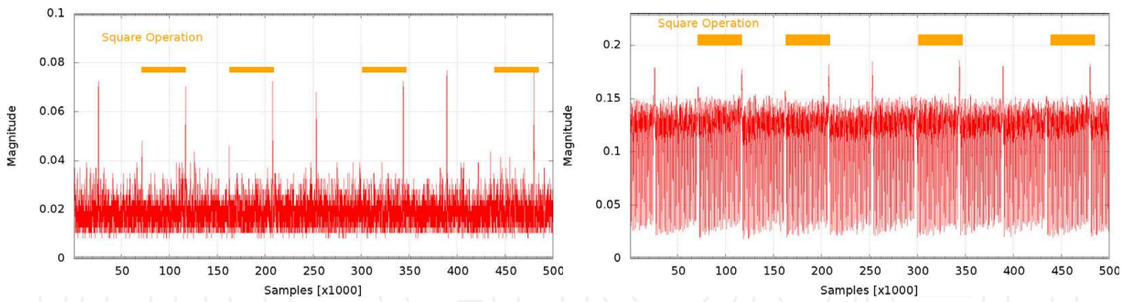



Fig. 21. One Single Demodulated EM waveform at 24 MHz.

We can obtain similar results by tuning the frequency of the receiver to the harmonics of the clock frequency. Moreover we can enlarge the distance between the FPGA and the probe despite a significant lose of S/N ratio. In order to obtain more powerful signals, we used an increased resolution bandwidth and then performed the same SEMA attacks successfully at least 5cm and more distance.

With the method developed previously we can focus on different frequencies that are not necessarily related to the clock harmonics. To measure such emanation, the probe must be placed close to the FPGA. Then an eavesdropper has to tune the receiver at every frequency of the spectrum. Interestingly, we found that the best results were not always obtained by demodulating the raw signal at the harmonics of the clock frequency.

Figures 22 and 22 show the single demodulated EM waveform at 34 and 54 MHz, which have been identified by the peaks obtained on our MI analysis on figure 20. The same sequence is replayed by changing only the demodulation frequency.




(a) 34MHz (b) 54MHz

Fig. 22. One single Demodulated EM waveform at 34 MHz and at 54 MHz.

If we compare the figures 21 and 22 we notice that sharp peaks appear at the beginning of every square operation. These peaks are not present before a multiply operation and thus we can easily distinguish the square from the multiply operations. We obtained the same phenomena for the demodulation at 54 MHz on figure 22. Moreover it is important to notice that the magnitude of the compromising signal decreases when the frequency of demodulation increases. The magnitude of the compromising signal follows the trend obtained in the previous section. These results confirm the results obtained during the characterization as shown on the table 2.

| Frequency | MI [bit] | Magnitude |
|---|---|---|
| 24.0 MHz | 2.5 | 0.5 |
| 34.0 MHz | 1.7 | 0.03 |
| 54.0 MHz | 1.0 | 0.02 |

Table 2. Comparison between the results.

## 6. Conclusions

In this chapter, we present firstly leakage mechanism behind Electromagnetic Analysis at near and far distances with contactless probe on FPGA implementations of cryptographic algorithms. The measurements are conducted with different techniques, the probe are attached to a power cable or on communication link, free space around the power cable and at distance from the electronic board. We show that an attacker from these measurements and by computing SEMA and DEMA is in position to retrieve the secret key. Different types of leakage radiation have been highlighted, such as Indirect and Direct emanation. Then we investigate a relationship between the intensity of EM radiation and the geometry of the board. In order to evaluate EM information leakage, we performed simple electromagnetic analysis (SEMA) experiments on a cryptographic device with an RSA module. We first measured EM radiations over the entire surface of a device including over the module, and then evaluated which spots and frequencies are available for EM information leakage. On the studied implementation the raw EM measurements show no obvious leakage. The result suggested that the signal (information)-to-noise ratio should be suppressed for achieving circuit and system security assuming that EM radiation can be interpreted as a signal encoding secret information.

In order to distinguish square and multiply operations in the SEMAs, we introduce a method to detect and characterize a crypto-system in frequency domain, *i.e* a distinguisher of frequencies that are carrying information. In addition we show that our method provides exploitable results and allows us to retrieve the leakages frequencies for unintentional emanations. The method proposed based on the mutual information analysis in frequency domain allows to extract the leakage frequencies of the signal related to the square and multiply operations. By following this method we are able to pinpoint the frequencies that are leaking more information and their bandwidth. Thanks to this tool we demonstrate that we are in position to give a quick diagnostic about the EM leakage of a device. Therefore an attacker is able to perform SEMAs. The method of choosing a right demodulation frequency is crucial; and thanks to our characterization based on the MI, information leaked through indirect EM emanations can be detected and observed with one single demodulated EM waveform.

## 7. Acknowledgment

This research was supported by the Strategic International Cooperative Program SPACES (Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems), funded by the ANR (french national research agency) and the JST (Japan Science and Technology agency).

## 8. References

Agrawal, D., Archambeault, B., Rao, J. R. & Rohatgi, P. (2002). The EM Side–Channel(s), *in* B. S. Kaliski Jr., C. K. Koç & C. Paar (eds), *CHES*, Vol. 2523 of *LNCS*, Springer, pp. 29–45.

Brier, É., Clavier, C. & Olivier, F. (2004). Correlation Power Analysis with a Leakage Model, *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, Vol. 3156 of *Lecture Notes in Computer Science*, Springer, pp. 16–29.

Cryptographic Hardware Project, T. U. (n.d.).
URL: *Website:* `http://www.aoki.ecei.tohoku.ac.jp/crypto/`

Fouque, P.-A. & Valette, F. (2003). The doubling attack - *hy upwards is better than downwards*, *CHES*, pp. 269–280.

Gandolfi, K., Mourtel, C. & Olivier, F. (2001). Electromagnetic Analysis: Concrete Results, *in* Ç. K. Koç, D. Naccache & C. Paar (eds), *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, Vol. 2162 of *Lecture Notes in Computer Science*, Springer, pp. 251–261.
URL: *http://link.springer.de/link/service/series/0558/bibs/2162/21620251.htm*

Gierlichs, B., Batina, L., Tuyls, P. & Preneel, B. (2008). Mutual information analysis, *CHES*, pp. 426–442.

Hockanson, D. M., Drewniak, J. L., Hubing, T. H., Doren, T. P. V. & Wilhelm, M. J. (1996). Investigation of fundamental EMI source mechanisms driving common-mode radiation from printed circuit boards with attached cables, *IEEE Transactions on Electromagnetic Compatibility* 38(4): 557–566.

Homma, N., Miyamoto, A., Aoki, T., Satoh, A. & Shamir, A. (2008). Collision-based power analysis of modular exponentiation using chosen-message pairs, *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington,*

*D.C., USA, August 10-13, 2008. Proceedings*, Vol. 5154 of *Lecture Notes in Computer Science*, Springer, pp. 15–29.

Homma, N., Nagashima, S., Imai, Y., Aoki, T. & Satoh, A. (2006). High-resolution side-channel attack using phase-based waveform matching, *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, Vol. 4249 of *Lecture Notes in Computer Science*, Springer, pp. 187–200.

Kocher, P. C., Jaffe, J. & Jun, B. (1999a). Differential Power Analysis, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, Vol. 1666 of *Lecture Notes in Computer Science*, Springer, pp. 388–397.
URL: *http://www.cryptography.com/resources/whitepapers/DPA.pdf*

Kocher, P. C., Jaffe, J. & Jun, B. (1999b). Differential Power Analysis, *in* M. Wiener (ed.), *Advances in Cryptology – Crypto '99*, Vol. 1666 of *LNCS*, Springer-Verlag, pp. 388 – 397.

Kuhn, M. G. (2005). Security Limits for Compromising Emanations, *in* J. R. Rao & B. Sunar (eds), *Cryptographic Hardware and Embedded Systems – CHES 2005*, Vol. 3659 of *LNCS*, Springer, pp. 265–279.

Li, H., Markettos, A. T. & Moore, S. (2005). Security evaluation against electromagnetic analysis at design time, *in* J. R. Rao & B. Sunar (eds), *Cryptographic Hardware and Embedded Systems – CHES 2005*, Vol. 3659 of *LNCS*, Springer, pp. 280–292.

Mangard, S., Oswald, M. E. & Popp, T. (2007). *Power Analysis Attacks - Revealing the Secrets of Smart Cards*, Springer-Verlag New York, Inc.

Menezes, A., van Oorschot, P. C. & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*, CRC Press.

Meynard, O., Guilley, S., Danger, J.-L. & Sauvage, L. (2010). Far Correlation-based EMA with a precharacterized leakage model, *DATE'10*, IEEE Computer Society, pp. 977–980. Dresden, Germany.

Meynard, O., Réal, D., Guilley, S., Danger, J.-L. & Homma, N. (2011). Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques, *DATE*, IEEE Computer Society. Grenoble, France.

Miyamoto, A., Homma, N., Aoki, T. & Satoh, A. (2008). Chosen-message spa attacks against fpga-based rsa hardware implementations, *FPL*, pp. 35–40.

Montgomery, P. L. (1985). Modular multiplication without trial division, *Math. Comp.*, vol. 44, no. 170, pp. 519–521, 1985.

Novak, R. (2002). Spa-based adaptive chosen-ciphertext attack on rsa implementation, *Public Key Cryptography*, pp. 252–262.

Paul, C. R. (2006). *Introduction to Electromagnetic Compatibility*, Wiley Interscience. ISBN-10: 0471549274.

Peeters, E., Standaert, F.-X. & Quisquater, J.-J. (2007). Power and electromagnetic analysis: Improved model, consequences and comparisons, *Integration, The VLSI Journal, special issue on* "Embedded Cryptographic Hardware" 40(1): 52–60.
URL: *http://dx.doi.org/10.1016/j.vlsi.2005.12.013*

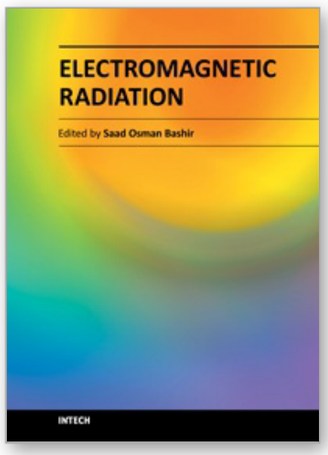
Quisquater, J.-J. & Samyde, D. (2001). Electromagnetic analysis (EMA): Measures and counter-measures for smart cards, *in* I. Attali & T. P. Jensen (eds), *Smart Card Programming and Security, International Conference on Research in Smart Cards, E-smart 2001, Cannes, France, September 19-21, 2001, Proceedings*, Vol. 2140 of *Lecture Notes in*

*Computer Science*, Springer, pp. 200–210.
URL: *http://link.springer.de/link/service/series/0558/bibs/2140/21400200.htm*

Schramm, K., Leander, G., Felke, P. & Paar, C. (2004). A collision-attack on aes: Combining side channel- and differential-attack, *CHES*, pp. 163–175.

Sudo, T., Sasaki, H., Masuda, N. & Drewniak, J. L. (2004). Electromagnetic Interference (EMI) of system-on-package (SOP), *IEEE Transactions on Advanced Packaging* 27(2): 304–314.

Vuagnoux, M. & Pasini, S. (2009). Compromising Electromagnetic Emanations of Wired and Wireless Keyboards, *Proceedings of the 18th USENIX Security Symposium*, USENIX Association.
URL: *http://www.usenix.org/events/sec09/*




**Electromagnetic Radiation**

Edited by Prof. S. O. Bashir

ISBN 978-953-51-0639-5

Hard cover, 288 pages

**Publisher** InTech

**Published online** 05, June, 2012

**Published in print edition** June, 2012

The application of electromagnetic radiation in modern life is one of the most developing technologies. In this timely book, the authors comprehensively treat two integrated aspects of electromagnetic radiation, theory and application. It covers a wide scope of practical topics, including medical treatment, telecommunication systems, and radiation effects. The book sections have clear presentation, some state of the art examples, which makes this book an indispensable reference book for electromagnetic radiation applications.

**How to reference**

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Olivier Meynard, Sylvain Guilley, Jean-Luc Danger, Yu-Ichi Hayashi and Naofumi Homma (2012). Characterization of the Information Leakage of Cryptographic Devices by Using EM Anal, Electromagnetic Radiation, Prof. S. O. Bashir (Ed.), ISBN: 978-953-51-0639-5, InTech, Available from: http://www.intechopen.com/books/electromagnetic-radiation/characterization-of-the-information-leakage-of-cryptographic-devices-by-using-em-analysis

INTECH
open science | open minds

**InTech Europe**
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

**InTech China**
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen