# Identification of information leakage spots on a cryptographic device with an RSA processor

Olivier Meynard [#1#3] Yu-ichi Hayashi [#2] Naofumi Homma [#2] Sylvain Guilley [#1] Jean-Luc Danger [#1]

[#1] Telecom ParisTech, 46 rue Barrault, 75634 Paris Cedex 13, France
meynard@enst.fr, guilley@enst.fr, danger@enst.fr
[#2] Tohoku University, 6-6-05 Aramaki Aza, Sendai, Miyagi 980-8579, Japan
yu-ichi@m.tains.tohoku.ac.jp, homma@aoki.ecei.tohoku.ac.jp
[#3] DGA-MI, La roche Marguerite, Bruz 35174, France

## Abstract

*This paper investigates a relationship between the intensity of EM radiation and that of EM information leakage on a cryptographic device. For this purpose, we first observe an EM-field map on a cryptographic device by an EM scanning system, and then perform simple electromagnetic analysis (SEMA) experiments at some distinct points on the device including over the module. The target device considered here is a Side-channel Attack Standard Evaluation Board (SASEBO) with an RSA hardware implemented in an FPGA. Through the experiment, we demonstrate which points are effective for EM information leakage. The result suggests that the position of greatest EM intensity is not always the most effective point in EM information leakage.*

## I. Introduction

Cryptographic modules (software or hardware implementations of cryptographic algorithms) are now indispensable for many electronic devices. Such modules are commonly used for secure communications and transactions to protect privacy and valuable data. On the other hand, the side-channel attack based on side-channel information is a major concern for designers of such modules. When a cryptographic module performs encryption or decryption, information on secret parameters that correlate to the intermediate data being processed can be leaked as side-channel information, via operation timing, voltage/current fluctuation, or electromagnetic (EM) radiation. Side-channel attacks have attracted widespread attention because they can be performed by using off-the-shelf equipment without leaving any evidence of an attack.

Power analysis attacks, such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA), are known as basic side-channel attacks [1], and many related attacks and countermeasures have been reported [2]. EM analysis (EMA) measuring the electromagnetic field generated by a cryptographic module has also been presented as an extension of the power analysis [3]–[6]. In particular, successful EMA of an SSL accelerator was carried out in [4] by measuring the accelerator's radiation at a distance. The previous work suggests that a side-channel attack is feasible even when obtaining close access to the module is difficult. In [5], it was reported that side-channel information can be acquired from power lines or I/O [20] lines. EMA at a distance from a cryptographic module is an emerging issue for designers and users of cryptographic modules.

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 [7]. 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. Devices in conformity with the standards work normally. However, these standards mainly aim to suppress and reduce EM radiation that disturbs other devices, but not the radiation that leaks secret information. Even if the EM radiation (i.e.,

**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
```

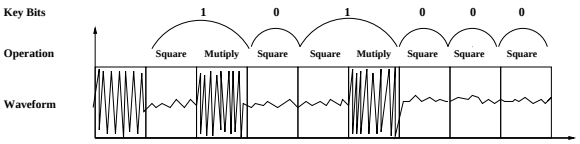



**Figure 1. Image of Simple Electromagnetic Analysis (SEMA) on RSA module.**

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 [8][9] have demonstrated EM information leakage from electronic devices that are in compliance with the guidelines.

Addressing the above problem, this paper investigates a relationship between the intensity of EM radiation and that of EM information leakage on a cryptographic device. For this purpose, we focus on a comparison of the two intensities observed at some distinct points on the surface of a PCB board. To the best of authors' knowledge, there is no experimental study addressing such information leakage at a board level. In order to evaluate EM information leakage, we perform simple electromagnetic analysis (SEMA) experiments on a cryptographic device with an RSA module. We first measure EM radiations over the entire surface of a device including over the module, and then evaluate which points and frequencies are effective for EM information leakage. The result suggests 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 noise concealing a signal encoding a secret information.

## II. Simple electromagnetic analysis on RSA

Simple Power Analysis (SPA)[1] is one of the major side-channel attacks, and many reports of SPAs and countermeasures have been published [2]. This type of attack exploits one or a few power traces obtained by a measurement device, such as an oscilloscope, and discover the secret information directly. This often requires detailed knowledge about the implementation of the cryptographic algorithm that is executed by the module. If some traces are available for the attacker, more powerful analyses such as chosen-message SPA attacks can be applied to the modules[10]–[13]. Simple Electromagnetic Analysis (SEMA) [14], which exploits EM information leakage, is an extension of SPA. The major features of SEMA are that EM waveforms are obtained by non contact probing and that the leakage of only a part of the cryptographic module/device is observed.

In general, SPA and SEMA are suitable for public-key ciphers which require a large amount of computations for each encryption/decryption operation. 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:

$$C = P^E \bmod N, \tag{1}$$

$$P = C^D \bmod N, \tag{2}$$

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, and thus the following analysis technique can be widely applied to other public-key ciphers.

The binary method (or 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 long 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 1. The basic sequence in the binary method is not changed even when major acceleration techniques such as Montgomery multiplication [15] and the Chinese Remainder Theorem (CRT) [16] are applied to the exponentiation computation.

The rationale of the SPA/SEMA of the RSA cryptosystem is to distinguish between multiplication and squaring in the power/EM waveform. Fig. 1 shows an image of the SEMA on an RSA module using the left-to-right binary method. When the difference between multiplication and

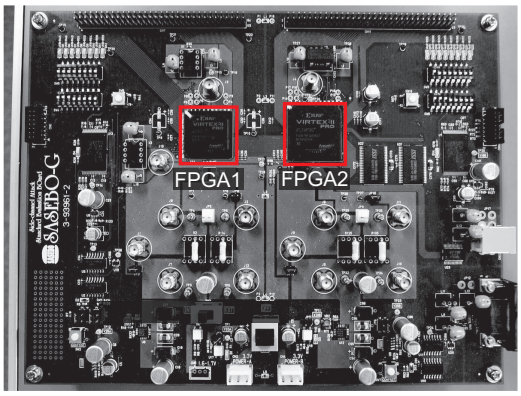



**Figure 2. Overview of SASEBO-G.**

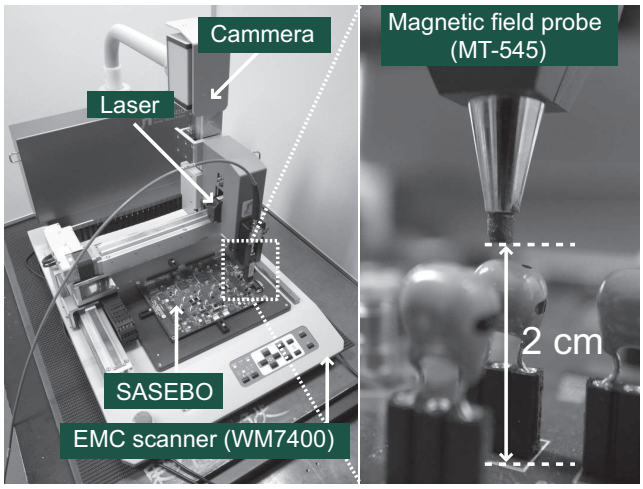



**Figure 3. EM measurement system.**

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

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 to 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 [10]–[13] can enhance these differences.

One simple idea is to choose a message that has a large number of 1s (or 0s) in the bit sequence [17]. 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 $Y = R^{-1}R = 1 \bmod N$ 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.

## III. Measurement of EM radiation on cryptographic device

This section describes 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.

For this purpose, 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 [18]. Fig. 2 shows the SASEBO-G used in this experiment, which employs two Xilinx FPGAs; one FPGA is used to implement a cryptographic module in hardware or software and the other FPGA is used to communicate with a host computer through RS-232 or USB cables.

We implemented an RSA processor based on a conventional left-to-right binary method and Montgomery multiplication [19] in FPGA2 shown in Fig. 2. The processor handles key of length 1,024-bit key length based on 32-bit word length for radix, and is predominantly-comprised of one 32-bit multiplier. On the other hand, we did not use FPGA1 in order to simplify the intensity of EM radiation from the SASEBO. The RSA operation was performed at a clock frequency of 24 MHz. The input value is $R^{-1}$ (=$2^{-k} \bmod N$ in order to produce large differences between the multiplication and squaring operations.

**Table I. Measurement conditions**

| | |
|---|---|
| CRYPTOGRAPHIC DEVICE (SASEBO-G) | |
| Target FPGA | Xilinx Virtex-II Pro |
| Clock frequency (crystal oscillator) | 24 MHz |
| Power supply voltage | 3.3 V |
| EMC SCANNER (WM7400) SETTING | |
| EM probe | MT-545 |
| Distance from SASEBO surface | 20 mm |
| Distance from FPGA surface | 5 mm |
| Pitch for SASEBO surface | 5 mm |
| Pitch for FPGA surface | 1 mm |

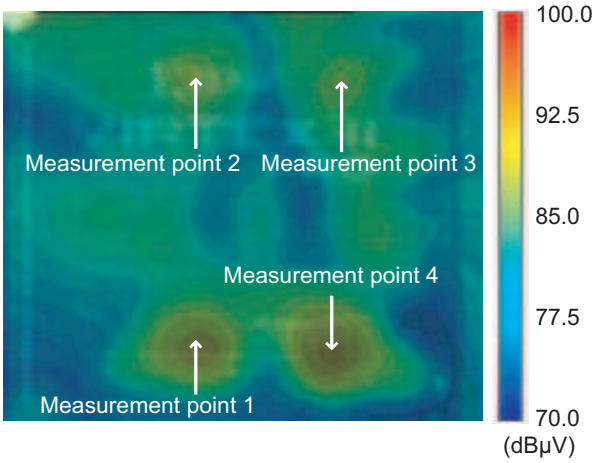



**Figure 4. EM-field map over FPGA2.**

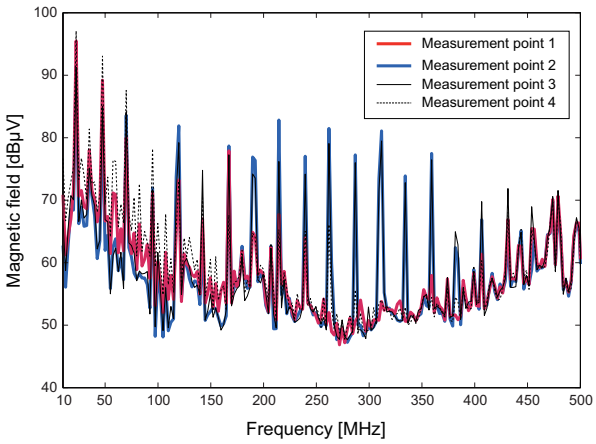



**Figure 5. Frequency characteristics of EM radiation over four points over FPGA2.**

Fig. 3 shows an overview of the EM measurement system in this experiment. The above SASEBO was set on the scanning table. 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. 3 also shows an image of the EM probing. The measurement condition are summarised in Table I.

In order to identify the source of EM radiation, we first examine the surface of FPGA2 performing an RSA operation inside. Fig. 4 shows an EM-field map over FPGA2, whose frequency band ranges from 10 to 500 MHz. The map indicates that there are four effective points which have higher intensities than other points. Therefore, we selected the four points as representatives

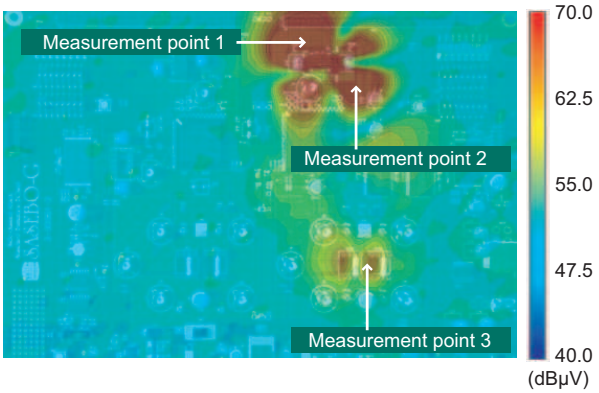



**Figure 7. EM-field map at 24 MHz.**

in the following experiment. Fig. 5 shows the frequency characteristics of EM radiation for the four points over the FPGA2. We can confirm here that EM radiation at the clock frequency (24 MHz) and its harmonic frequencies are much higher than other frequencies. In particular, the EM radiation at the clock frequency has the highest intensity among them.

Fig. 6 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. 2, 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.

## IV. Evaluation of EM information leakage

In order to evaluate EM information leakage, we performed simple electromagnetic analysis (SEMA) experiments on the above SASEBO-G. In this experiment, we focus on the EM radiation of 24 MHz as a primary frequency. Fig. 7 shows an EM-field map on the entire surface of the SASEBO at 24 MHz. We selected three specific points as regions of interest according to the result, where Point 1 is over the crystal oscillator, Point 2 is over the cryptographic module, and Point 3 is over the resistor between the FPGA ground pin and the ground plane. Highest EM radiations were observed at Points 1 and 2, and a relatively-high EM radiation was observed at Point 3 even though it is a bit away from the cryptographic module.

Fig. 8 shows the EM traces of the three points, where

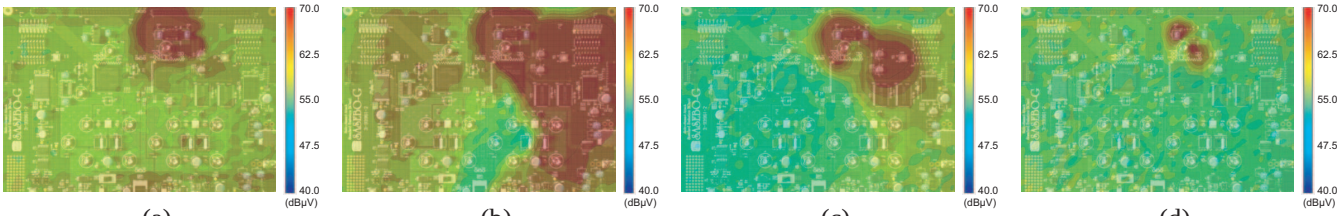



**Figure 6. EM-field maps: (a) 10-100 MHz, (b) 100-200 MHz, (c) 200-300 MHz, and (d) 300-400 MHz.**

the horizontal and vertical axes indicate time and voltage, respectively. The conventional SEMA is performed using the waveforms, but no relationship between the waveform patterns and the operations was observed. In this experiment, therefore, a demodulation technique is applied for the waveforms in order to emphasize the differences, and the waveforms as shown in Fig. 9 are obtained using a demodulation at 24 MHz. As a result, multiplication and squaring can easily be distinguished in Fig. 9 (c).

We consider the Amplitude Modulation technique, and we perform by the help of the hardware receiver a demodulation at 24 MHz. We need a dedicated apparatus for the study of the frequency: a spectrum analyser that can be set in demodulator/ Receiver. Different types of hardware receivers exist. For our experiment we propose to use a common device in academic research: *Rohde&Schwarz FSQ8*, for which some details are available in [21]. This device offers a maximal bandwidth of 50 MHz, and it can be tuned continuously between 100 Hz and 1 GHz. These devices are usually used to receive an Amplitude Modulated narrow-band signal.

$$Ms(t) = A \cdot \cos(2\pi f_c t) \cdot [1 + m \cdot v(t)],$$

where $f_c$ is the carrier frequency, $v(t)$ is the broadcast signal, $A$ is the carrier's amplitude and $m$ is the modulator's amplitude.

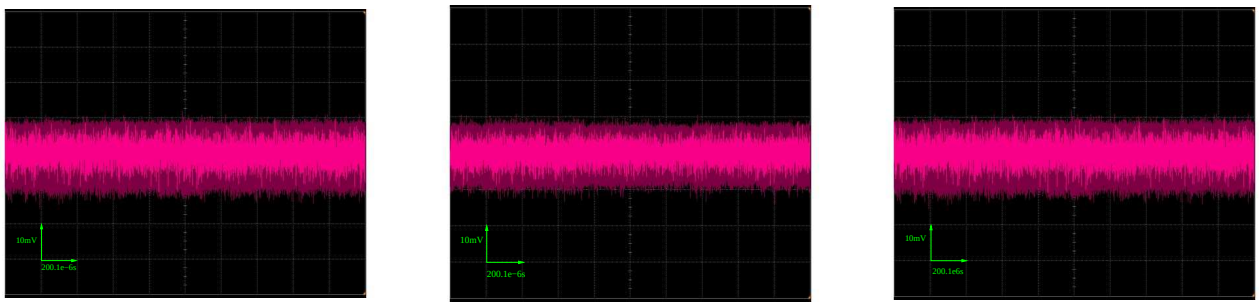
For this experiment, we use the same setup (RSA implementation on a SASEBO-G and antenna) as in the previous section, but the output of the probe is connected to a receiver/demodulator. In this experiment, we employ the demodulation technique to investigate unintentional (or indirect) emanation. The unintentional emanation described by Agrawal is the result of modulation or intermodulation between a carrier signal and the sensitive signal. We tune the receiver to the clock frequency (*i.e.*, 24MHz) with a resolution bandwidth of 1MHz. In Fig. 9 (a), we catch one measurement by demodulation at 24 MHz, over the crystal oscillator position 1, and this measurement is not carrying information. This part of the PCB supplies and gives the clock frequency to the RSA module on the FPGA. His radiation is therefore constant and doesn't carry any information. In Fig. 9 (b), the measurement is done at 2 cm from the FPGA. The radiation from the FPGA are weak at this distance. Finally we observe only at Position 3 in Fig. 9 (c), over the resistor between the FPGA ground pin and the ground plane, a difference between the operation square and multiply. This figure shows one single demodulated EM waveform at 24 MHz. Indeed, the receiver improves the differences between the two operations dramatically. It is important to notice that this position is a bit far away from the cryptographic module but his radiations are carrying information. This observation confirms the assumption of Agrawal. The unintentional emanation such as the ubiquitous clock signal can be one of the most important sources of signal and the information is carried a bit far away from the cryptographic module.

## V. Conclusion

This paper investigated a relationship between the intensity of EM radiation and that of EM information leakage on a cryptographic device. For this purpose, we focused on a comparison of the two intensities observed at some points on the surface of a PCB 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. 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.

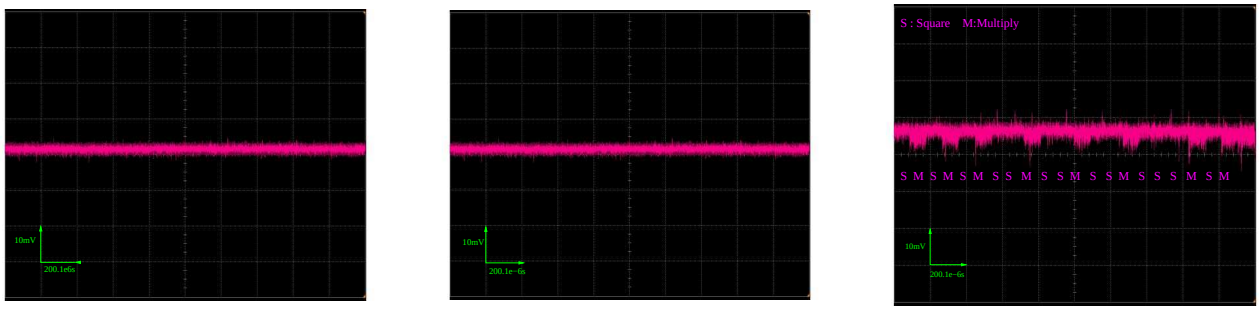
### Acknowledgements

This research was supported by Strategic International Cooperative Program called SPACES (Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems) supported by ANR and JST.



(a) (b) (c)

**Figure 8. EM waveforms of: (a) point 1, (b) point 2, and (c) point 3.**




(a) (b) (c)

**Figure 9. Demodulated EM waveforms of: (a) point 1, (b) point 2, and (c) point 3.**

## References


[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *CRYPTO 1999, Lecture Notes in Computer Science*, vol. 1666, pp. 388–397, Aug. 1999.

[2] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks - Revealing the Secrets of Smart Cards*. Springer, 2007.

[3] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," *CHES 2001, Lecture Notes in Computer Science*, vol. 2162, pp. 251–261, May 2001.

[4] D. Agrawal, , B. Archambeault, R. Rao, and P. Rohatgi, "The EM Side-Channel(s)," *CHES 2002, Lecture Notes in Computer Science*, vol. 2523, pp. 29–45, Aug. 2002.

[5] T. Sugawara, Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, and A. Satoh, "Mechanism behind information leakage in electromagnetic analysis of cryptographic modules," *WISA 2009, Lecture Notes in Computer Science*, vol. 5932, pp. 66–78, Aug. 2009.

[6] T. Plos, M. Hutter, and M. Feldhofer, "On comparing side-channel preprocessing techniques for attacking rfid devices," *WISA 2009, Lecture Notes in Computer Science*, vol. 5932, pp. 163–177, Aug. 2009.

[7] R. C. Paul, "Introduction to electromagnetic compatibility," 2006.

[8] G. M. Kuhn, "Security limits for compromising emanations," *CHES 2005, Lecture Notes in Computer Science*, vol. 3659, pp. 265–279, Aug. 2005.

[9] H. Sekiguchi and S. Seto, "Measurement of radiated computer RGB signals," *Progress In Electromagnetics Research C*, vol. 7, pp. 1–12, 2009.

[10] R. Novak, "SPA-based adaptive chosen-ciphertext attack on RSA implementation," *PKC 2002, Lecture Notes in Computer Science*, vol. 2274, pp. 252–262, Feb. 2002.

[11] P A. Fouque and F. Valette, "The doubling attack -why upwards is better than downwards," *CHES 2003, Lecture Notes in Computer Science*, vol. 2779, pp. 269–280, Sep. 2003.

[12] K. Schramm, G. Leander, P. Felke, and C. Paar, "A collision-attack on AES combining side channel- and differential-attack," *CHES 2004, Lecture Notes in Computer Science*, no. 3156, pp. 163–175, Aug. 2004.

[13] N. Homma, A. Miyamoto, T. Aoki, A. Satoh, and A. Shamir, "Collision-based power analysis of modular exponentiation using chosen-message pairs," *CHES 2008, Lecture Notes in Computer Science*, vol. 5154, pp. 15–29, Aug. 2008.

[14] J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," *E-Smart 2001, Lecture Notes in Computer Science*, no. 2140, pp. 200–210, Sep. 2001.

[15] P. L. Montgomery, "Modular multiplication without trial division," *Math. Comp.*, vol. 44, no. 170, pp. 519–521, 1985.

[16] J. A. Menezes, C. P. Oorschot, and A. S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997.

[17] A. Miyamoto, N. Homma, T. Aoki, and A. Satoh, "Chosen-message SPA attacks against FPGA-based RSA hardware implementations," *Proc. 2008 Int. Conf. on Field Programmable Logic and Applications*, pp. 35–40, Sep. 2008.

[18] Side-channel Attack Standard Evaluation Board, http://www.rcis.aist.go.jp/special/SASEBO/.

[19] A. Miyamoto, N. Homma, T. Aoki, and A. Satoh, "Systematic design of high-radix montgomery multipliers for rsa processors," *Proc. 26th IEEE Int. Conf. Computer Design*, pp. 416–422, Oct. 2008.

[20] Schmidt, Jörn-Marc and Plos, Thomas and Kirschbaum, Mario and Hutter, Michael and Medwed, Marcel and Herbst, Christoph, "Side-Channel Leakage across Borders,"*CARDIS 2010, Lecture Notes in Computer Science*, vol. 6035, pp. 36–48,2010.

[21] http://www2.rohde-schwarz.com/product/FSQ.html