# Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques

Olivier Meynard[1,2], Denis Réal[2],Florent Flament[1],
Sylvain Guilley[1], Naofumi Homma[3], Jean-Luc Danger[1].

[1]Département COMELEC, Institut TELECOM,
TELECOM ParisTech,CNRS LTCI, PARIS, FRANCE
*firstname.lastname@telecom-paristech.fr*

[2]DGA Information Superiority, Bruz, France.
*firstname.lastname@dga.defense.gouv.fr*

[3]Graduate School of Information Sciences, Tohoku University, Japan.
*lastname@aoki.ecei.tohoku.ac.jp*

## Abstract

*SPA/SEMA (Simple Power/Electro-magnetic Analysis) attacks performed on public-key cryptographic modules implemented on FPGA platforms are well known from the theoretical point of view. However, the practical aspect is not often developed in the literature. But researchers know that these attacks do not always work, like in the case of an RSA accelerator. Indeed, SEMA on RSA needs to make a difference between square and multiply which use the same logic; this contrast with SEMA on ECC, which is easier since doubling and add that are two different operations from the hardware point of view. In this paper, we wonder what to do if a SEMA fails to succeed on a device.Does it mean that no attack is possible? We show that hardware demodulation techniques allow the recording of a signal with more information on the leakage than a raw recording. Then, we propose a generic and fast method enabling to find out demodulation frequencies. The effectiveness of our methods is demonstrated through actual experiments using an RSA processor on the SASEBO FPGA board. We show cases where only demodulated signals permit to defeat RSA.*

**Keywords:** Demodulation, Simple Electro-Magnetic Analysis, Mutual Information, Modular Exponentiation.

## I. Introduction

978-3-9810801-7-9/DATE11/ © 2011 EDAA

Cryptographic algorithms are built to be secure against logical analysis. However, whatever be its implementation, it may let some prints of its activity filter through so-called side channels. A lot of such side channels have been investigated in the last years: execution time, power consumption, radiated emanations... The community's favorite one seems to be electro-magnetic (EM) radiations introduced first by Gandolfi *et al.* [1]. They analyzed EM radiations emitted by a DES and an RSA module, and showed the greater effectiveness of EM techniques over the corresponding power analysis. Simple Electro-Magnetic Analysis (*SEMA*) was firstly investigated by Quisquater and Samyde [2].According to Agrawal *et al.* [3], EM emanations can be classified into direct and unintentional emanations. On the one hand, direct emanations result from intentional current flows. Near-field techniques combined with tiny contactless probes may be required for eavesdropping on them. On the other hand, unintentional emanations are due to modulation of ubiquitous carrier signals such as the clock signal or the power supply signal. For instance, an EM probe can capture Amplitude Modulated (*AM*) signals from a Secure Socket Layer accelerator (*SSL*) performing exponentiation operations. Then an attacker can retrieve the secret using AM demodulations of the carrier signals [3]. Mangard also showed in [4] that EM near field attacks can be conducted with a simple handmade coil, and that measuring the far field emissions of a smart card connected to a power supply unit enables to

**ALGORITHM 1**
MODULAR EXPONENTIATION (L-TO-R BINARY METHOD)

| | |
|---|---|
| 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: $Z := Z * Z \bmod N$; – squaring
4: **if** $(e_i = 1)$ **then**
5: $Z := Z * X \bmod N$; – multiplication
6: **end if**
7: **end for**

determine the secret key used in the smart card. But even if EM techniques are attractive for side channel analysis, they can fail. We experimented eavesdropping on emanations involved in RSA computation. We observed that the raw recorded leakage does not enable to mount an attack. However, a demodulation permits to erase energetic signals not carrying information, thus the ratio between the leakage and the noise increases significantly. Furthermore, EM leakage is then properly digitalized. In order to validate this result, we studied EM emanations of a specific RSA processor in a SASEBO FPGA, which is smaller than those of the SSL accelerator used in [3].

This paper is organized as follows. In Section II, we reintroduce the Simple Electro-Magnetic Analysis on RSA and show that it does not function on the SASEBO. In Section III, we present a generic method enabling to choose proper demodulation frequencies. Then in Section IV, we perform a SEMA on a demodulated signal and confirm the efficiency of our approach compared to classical SEMA. Finally conclusions and perspectives are presented in Section V.

## II. SEMA on a RSA implementation

The RSA cryptosystem is a *de facto* standard public-key cryptosystem PKCS #1, which is based on encryption and decryption, as shown below:

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

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

where $P$ is the plaintext, $C$ is the ciphertext and $(E, N)$ is the public key. Usually, the size of $P$, $C$, $D$ and $N$ is greater than $1,024$ bits for security reasons. ALGORITHM 1 shows a classical way for computing a modular exponentiation called the left-to-right binary method. Multiplications and squaring operations are done sequentially according to the bit pattern of the exponent $D$. This algorithm always performs a squaring at Line 3 regardless of the scanned bit value, but the multiply operation at Line 5 is only executed if the scanned bit is 1. Let's note that

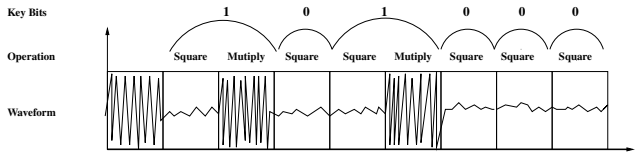


**Figure 1. SEMA principle on RSA.**

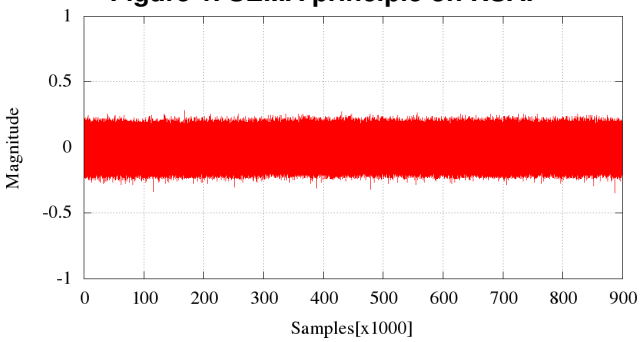


**Figure 2. Direct EM radiations emitted during an RSA computation.**

multiplication and squaring are done using the same module of the SASEBO. This module employs the high-radix Montgomery's modular multiplication ALGORITHM 2.

However, a multiplication loads two operands while the square only loads one. Furthermore, a conditional branch in the algorithm (between square or multiply) may introduce a bias in energy consumption or delay. Therefore, if an attacker is able to make a difference between a multiplication and squaring operation, he can recover the whole secret with only one trace. This is the original idea of the Simple Power Analysis (*SPA*)/ Simple electro magnetic Analysis (*SEMA*) against the RSA cryptosystem. Figure 1 illustrates the dependency.

Our first experiment was to test the SEMA on the SASEBO-RSA with near-field EM techniques. An RSA processor based on ALGORITHM 1 was implemented in an FPGA (XILINX VIRTEX II) on the SASEBO-G board (see the reference [5]). For all this experiments we have used a loop-type EM probe [6] and the signals have been amplified by 60 dB. We notify that we have done these experiments in favourable conditions: the signal that corresponds to the operation was routed on the FPGA, the architecture of the RSA is without any countermeasure and is not timing attack resistant. Moreover, we outputted a signal to synchronize our measurements. For the same bit sequence as in Figure 1, we obtained the EM trace illustrated on Figure 2.

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

**ALGORITHM 2**
HIGH-RADIX MONTGOMERY MULTIPLICATION (*MontMult*)

| | |
|---|---|
| Input: | $X = (x_{m-1}, ..., x_1, x_0)_{2^r}$, $Y = (y_{m-1}, ..., y_1, y_0)_{2^r}$, $N = (n_{m-1}, ..., n_1, n_0)_{2^r}$, $W = -N^{-1} \bmod 2^r$ |
| Output: | $Z = XY2^{-r \cdot m} \bmod N$ |

1: $Z := 0$;
2: **for** $i = 0$ **to** $m - 1$
3: $C := 0$;
4: $t_i := (z_0 + x_i y_0) W \bmod 2^r$;
5: **for** $j = 0$ **to** $m - 1$
6: $Q := z_j + x_i y_j + t_i n_j + C$;
7: **if** $(j \neq 0)$ **then** $z_{j-1} := Q \bmod 2^r$;
8: $C := Q/2^r$;
9: **end for**
10: $z_{m-1} := C$;
11: **end for**
12: **if** $(Z > N)$ **then** $Z := Z - N$;

in terms of contrast. However, we guessed that demodulation techniques should enable to improve this result for two reasons. 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. In Section III, the methods aiming at finding out demodulation frequencies are developed.

## III. Characterization of the EM Channel in Frequency Domain

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 [7], but it consumes a huge amount of time as well as memory resources. In this section we propose a method 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.

### A. Windowing and Sample Preparation

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

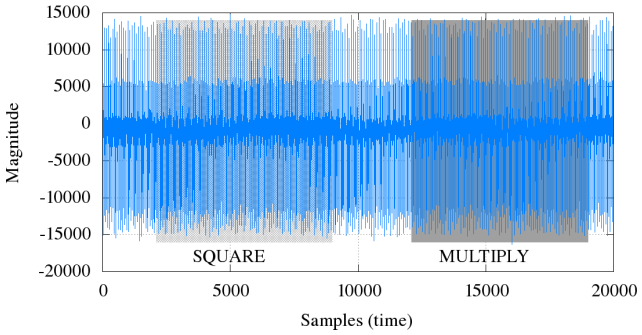


**Figure 3. EM measurement split into Square and Multiply parts.**

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. 3. After the measurements are cut according to the operation performed. The number of samples is equal in each part of the signal, and we obtain two sets of measurements with the same number of traces.

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. 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.

We introduce some details about the information theory in section III-B.

### B. An Information Theory Viewpoint.

It is interesting to adopt 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 [8] the Mutual Information Analysis. This tool is

traditionally used to evaluate the dependencies between a leakage model and observations (*or Measurements*). In our case, we use it as a metric that gives an indicator on the information contained at different frequencies. To do so, 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. 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:

$$\mathrm{I}(O_f; Operation) = \mathrm{H}(O_f) - \mathrm{H}(O_f|Operation), \quad (3)$$

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:

$$\begin{aligned} \mathrm{H}(O_f) &= -\int_{-\infty}^{+\infty} \Pr(O_f) \log_2 \Pr(O_f), \\ \mathrm{H}(O_f|Operation) &= \sum_{j \in \{Multiply, Square\}} \Pr(j) \mathrm{H}((O_f|j)). \end{aligned}$$

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

where $\Pr(O_f)$ denotes the probability law of observations at frequency $f$. Moreover we consider that the computed operations are equi-probable events, 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 for 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. (3) 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:

$$\mathrm{I}(O_f; Operation) = \frac{1}{2} \log_2 \frac{\sigma_{O_f}^2}{\sigma_{O_f, Multiply} \sigma_{O_f, Square}}. \quad (4)$$

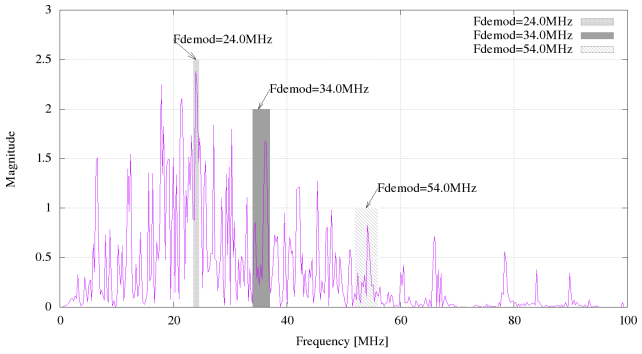


**Figure 4. Result of MIA in frequency domain.**

The figure 4 represents the result of Eqn. (4). 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. This method provides a result with a quantity expressed in bit, the leakage frequencies are also easy to interpret. 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 TEMPEST attacks. Moreover it is worthwhile to underline that Mutual Information considers the non-linear dependencies that occur 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. 4:

- around 24.0 MHz,
- around 34.0 MHz,
- around 54.0 MHz.

In Section IV, we study the results of the demodulation at these frequencies. Then we show the efficiency of our approach.

## IV. Demodulation technique

In this section we use the results obtained previously. We need a dedicated apparatus for the study of the frequency: a spectrum analyser that can be set in demodulator/ Receiver.

### A. Confirmation of the results with a Hardware Receiver

Different types of hardware receivers exist. We can cite receivers such as described by Agrawal in [3] or Kuhn in [9]. Typically, Kuhn presents in his PhD thesis the R-1250 model produced by *Dynamics Sciences*. Those receivers are super-heterodyne and wide-band. They

provide a large panel of configurations. For example, 21 intermediate frequency bandwidths from 50 Hz to 200 MHz are available. They switch automatically between different pre selection filters and mixers depending on the selected tuning frequency. Therefore those devices are quite expensive and uncommon. These devices are usually used to receive an Amplitude Modulated narrow-band signal.

For this experiment, we use the same setup (RSA implementation on a SASEBO-G and loop antenna) as in the previous section, but the output of the probe is connected to a receiver/demodulator and we perform the measurements directly on the FPGA. In [3] 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. Each time, the demodulated signal shows a peculiarity that allows to distinguish clearly the two distinct operations. In this experiment, we employ the demodulation technique to investigate two types of EM emanations: unintentional (or indirect) emanation and direct emanation.

## B. Unintentional emanations

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 4. We tune the receiver to the clock frequency (*i.e.*, 24MHz) with a resolution bandwidth of 1MHz. Figure 5 shows one single demodulated EM waveform at 24 MHz. Indeed, the receiver improves the differences between the two operations dramatically as shown in Fig. 5. We can obtain similar results by tuning the frequency of the receiver to the harmonics of the clock frequency.

## C. Direct emanation

As explained in [3] and [10], direct emanation is produced directly by tiny current flows of rising/falling edges of an internal signal. To measure such direct 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.

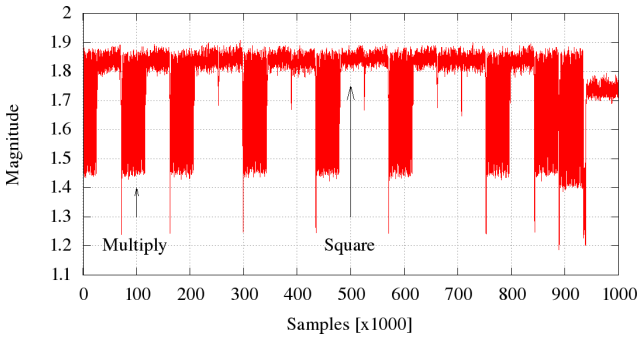


**Figure 5. One Single Demodulated EM waveform at 24 MHz.**

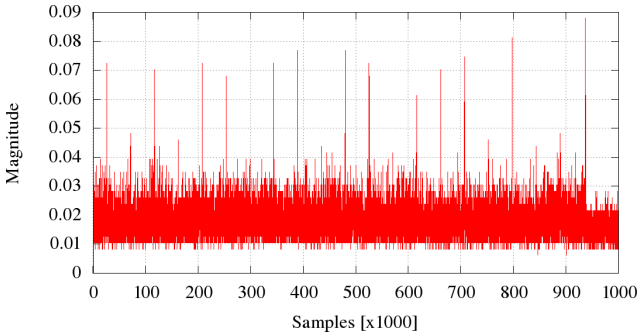


**Figure 6. One single Demodulated EM waveform at 34 MHz.**

Figures 6 and 7 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 4. The same sequence is replayed by changing only the demodulation frequency. If we compare the figures 5 and 6 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 7. 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 I.

| 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 I. Comparison between the results.**

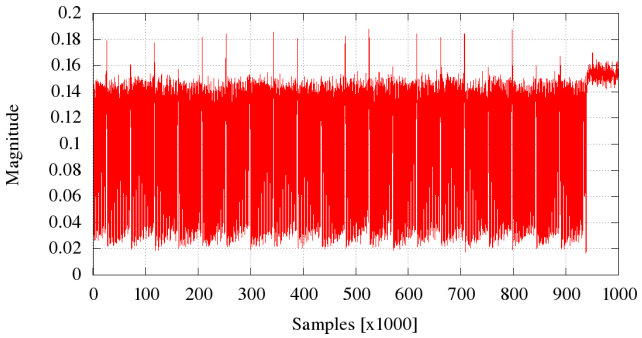


**Figure 7. One Single Demodulated EM waveform at 54 MHz.**

## V. Conclusions and future Works

This article presents possible SEMA attacks performed with a contactless probe on an FPGA implementation of RSA. On the studied implementation the raw EM measurements show no obvious leakage. In order to distinguish square and multiply operations in the SEMAs, we introduce a method to detect and characterize a cryptosystem 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 two types of emanations: unintentional and intentional emanations. The method proposed in this article is based on the mutual information analysis in frequency domain. It 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. As a comparison the TEMPEST methodology requires to scan exhaustively all the frequencies to discover those that leak. The demodulation allows to detect some biases that can be exploitable, for instance:

- conditional branch and control command,
- difference of operands,
- difference in computation of the High Radix Multiplier.

Therefore an attacker is able to perform SEMAs. Direct emanations were detected by our method and exploited by demodulation in this experiment. Although these emanations can be detectable only at small distance, they allow to highlight control instructions performed before each square/multiply operation. The method of choosing a right demodulation frequency is crucial; and thanks to our characterization based on the MI, information leaked through direct and indirect EM emanations can be detected and observed with one single demodulated EM waveform. Indeed our method allows a thorough characterization of leaking frequencies. This powerful tool enhances dramatically the SEMA approach. In our future work, our methods will be used to evaluate more advanced cryptographic implementations with countermeasures, such as dummy multiplications [11] and Montgomery powering ladder [12]. The detection of the control commands would be relevant and very useful in these cases.

## References

[1] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," in *Cryptographic Hardware and Embedded Systems - CHES 2001*, ser. LNCS, Çetin Kaya Koç, D. Naccache, and C. Paar, Eds., vol. 2162. Springer, 2001, pp. 251–261.

[2] J.-J. Quisquater and D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smard Cards," in *Smart Card Programming and Security (E-smart 2001)*, ser. LNCS, I. Attali and T. P. Jensen, Eds., vol. 2140. Springer-Verlag, September 2001, pp. 200–210, nice, France. ISSN 0302-9743.

[3] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM Side–Channel(s)," in *CHES*, ser. LNCS, B. S. Kaliski Jr., C. K. Koç, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 29–45.

[4] S. Mangard, "Exploiting Radiated Emissions – EM Attacks on Cryptographic ICs," in *Proceedings of Austrochip 2003*, L. Ostermann, Ed., 2003, pp. 13 – 16.

[5] Japanese RCIS-AIST: http://www.rcis.aist.go.jp/special/SASEBO/index-en.html.

[6] HZ-15 Probe Set, website: http://www2.rohde-schwarz.com/product/HZ15.html.

[7] M. Vuagnoux and S. Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," in *Proceedings of the 18th USENIX Security Symposium*. USENIX Association, 2009. [Online]. Available: http://www.usenix.org/events/sec09/

[8] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual Information Analysis," in *Cryptographic Hardware and Embedded Systems – CHES 2008*, ser. LNCS, E. Oswald and P. Rohatgi, Eds., vol. 5154. Springer, 2008, pp. 426–442.

[9] M. G. Kuhn, "Compromising Emanations: Eavesdropping risks of computer Displays," in *Technical Report UCAM-CL-TR-577*, December 2003.

[10] H. Li, A. T. Markettos, and S. Moore, "Security evaluation against electromagnetic analysis at design time," in *Cryptographic Hardware and Embedded Systems – CHES 2005*, ser. LNCS, J. R. Rao and B. Sunar, Eds., vol. 3659. Springer, 2005, pp. 280–292.

[11] N. Homma, A. Miyamoto, T. Aoki, A. Satoh, and A. Shamir, "Collision-based power analysis of modular exponentiation using chosen-message pairs," in *Cryptographic Hardware and Embedded Systems – CHES 2008*, ser. LNCS, E. Oswald and P. Rohatgi, Eds., vol. 5154. Springer, 2008, pp. 15–29.

[12] M. Joye and S.-M. Yen, "The Montgomery Powering Ladder," in *CHES*, ser. Lecture Notes in Computer Science, vol. 2523. Springer, 2002, pp. 291–302.