Characterization of the Electromagnetic Side Channel in Frequency Domain

Olivier Meynard[1,2], Denis Réal[2,4], Sylvain Guilley[1,3],
Florent Flament[1], Jean-Luc Danger[1,3], Frédéric Valette[2].

[1] Institut TELECOM / TELECOM ParisTech, CNRS LTCI (UMR 5141)
Département COMELEC, 46 rue Barrault, 75 634 Paris Cedex 13, FRANCE.
{meynard,guilley,fflament,danger}@TELECOM-ParisTech.fr
[2] DGA/MI (CELAR), La Roche Marguerite, 35 174 Bruz, FRANCE.
{denis.real,frederic.valette}@dga.defense.gouv.fr
[3] Secure-IC S.A.S., 37/39 rue Dareau, 75 014 Paris, FRANCE.
[4] INSA/IETR, Rue des buttes de Coesmes, 35, Rennes, France.

Abstract. In this article, we propose a new approach to characterize the EM leakage of electronic devices by identifying and focusing on the signals' frequencies leaking the most information. We introduce a set of tests based on cryptanalysis methods that will help vendors and users of sensitive devices to estimate the security risks due to leakage through electromagnetic emanations. We propose two approaches: an empirical one and another based on information theory. Both provide a characterization of the leakage *i.e.* the frequencies and the bandwidths where information is contained. These techniques are low cost, automatic, and fast as they can be performed with an oscilloscope and some softwares for the characterization. Such evaluation could also be carried out with TEMPEST. But TEMPEST evaluations require dedicated apparatus and time consuming step work that consists in scanning all the spectrum frequencies. Our approach does not substitute to regulatory TEMPEST evaluation, but nonetheless can identify the leakage with high confidence. To illustrate the relevance of our approach, we show that an online software filtering at some identified frequencies allows us to recover a key stroked in one measurement at the distance of 5 meters from the keyboard.

Keywords: Side Channel Analysis (SCA), TEMPEST, Mutual Information Analysis (MIA), Correlation Power Analysis (CPA), Principal Component Analysis (PCA), software demodulation, hardware demodulation, Differential Frequency Analysis (DFA).

1 Introduction

Electronic devices radiate an electromagnetic (EM) field that can compromise sensitive information handled internally. For instance, since the 60's, TEMPEST (Telecommunications Electronic Material Protected from Emanating Spurious Transmissions) tests are used by government agencies in order to measure the

amount of compromising EM signals. With the declassification in the 90's of a portion of the US TEMPEST standards, the civilian and academic researchers began to explore this topic. Van Eck published in [5] the first unclassified technical analysis of the security risks of emanations from computer monitors. Later Kuhn brought new elements into this area in [13], with eavesdropping experiments on CRT screens. In [12], he shows how to create a covert channel conveyed by a crafted TV program. Academic research teams have applied those methods to intercept keystroke signals [20]. They are able to reconstruct the signal data at a distance up to 20 meters even through walls. Concretely they find out the password that has been entered on a PS/2 keyboard with a bi-conical antenna, by tunning the receiver at the frequency carrying the most information. Because of the complexity of EM compromising signals, their evaluation requires expensive test equipments, advanced skills and time.

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. 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 frequency actually contains the sensitive information. For this reason, we propose a methodology based on an empirical approach, that we contrast with another one based on information theory. Our methodology enable attacks that can be lead without an expensive TEMPEST receiver. Electronic device constructors are legally required to conduct genuine TEMPEST evaluations. For them, our evaluation can give a first idea of the robustness of their devices. Also it can be seen as a preliminary to a TEMPEST evaluation, which is time consuming and expensive.

The rest of the paper is organised as follows: in section 2 we start by describing our test bench and the signal leaking on the EM channel. In section 3 we propose three distinguisher derived from state of the art side channel analysis, that allow to identify leaking frequencies. These methods are based on the CPA [3], the mutual information [8], and the principal components analysis [2]. Then, in section 4, we validate each of the three techniques by checking the demodulated signals at the predicted frequencies with a TEMPEST receiver. In the same section we devise a band-pass filtering method that is able to recover the shape of the compromising signal, using a single EM interception. The conclusion is in section 5.

2 Experimental Setup

To illustrate our experiments we consider a keyboard operating the PS/2 protocol.

2.1 The PS/2 Protocol

The PS/2 protocol is a bidirectional serial communication based on four wires (data, clock, ground, power supply). The data and clock lines are open-collectors and have two possible states: low and high states. If no data are transmitted the data and clock lines are in the high state. We say the bus is "Idle"; the keyboard is allowed to begin transmitting data. The PS/2 protocol transmits data in a frame, consisting of 11 bits. These bits are

- 1 start bit, always at 0,
- 8 data bits, least significant bit first, (d_i, $i \in [0, 7]$),
- 1 optional parity bit (odd parity, equal to $\bigoplus_{i=0}^{7} d_i$),
- 1 stop bit, always at 1.

Data sent from the keyboard to the computer is read on the falling edge of the clock signal as shown in Fig. 1. When a frame is sent, the clock is activated at a frequency specific to each keyboard, typically between 10 kHz and 16.7 kHz. The

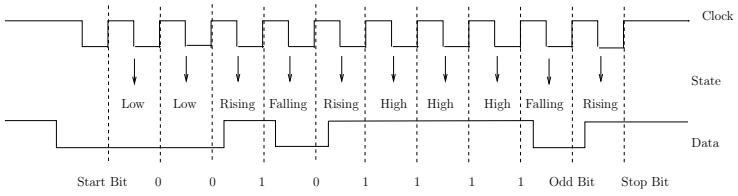

Fig. 1. PS/2 protocol, involved in the keyboard to computer communication.

state of sensitive data can be reconstructed thanks to the falling edge of both clock and data. Indeed because these signals are open-collectors, their low state consumes much more power than their high state. This property has already been noticed by Kuhn in [6]. The combination of the falling edge of the clock and the falling edge of the data helps the attacker in guessing the data. In fact a falling edge of the clock is always synchronized with the data start bit, contrarily to the data's falling edges whose positions depend of the keystroke. The eavesdropper can first of all build a dictionary with the positions of data's falling edges as a function of the key stroked.

2.2 Test Bench

Usually in a TEMPEST secure system the "Red/Black" separation principle must be followed, as explained by Kuhn in [13]. The "Red" equipment, which handles sensitive data, has to be isolated from the "Black" equipment that transmits ciphered data. For a TEMPEST protected equipment, the black signal shall not reveal any sensitive information. However in our case we use a commercial

keyboard without any countermeasure. As shown in Fig 2 we place a bi-conical antenna at 10 meters from a keyboard connected to a laptop by a PS/2 cable as in [20]. In our case, we name the data signal the red signal and the signal intercepted from the antenna, the black signal. To be sure that the radiated emission are produced only by the keyboard, the experimental test bench is placed in Faraday cage. The attack consists in recovering the red signal from one intercep-

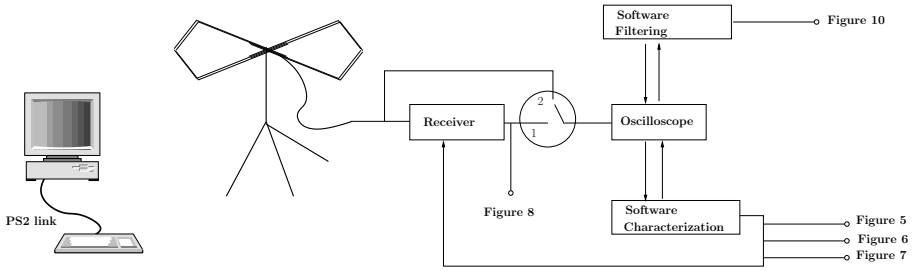

Fig. 2. Setup used for the keyboard eavesdropping.

tion of the black signal. Ideally an efficient attack can be led if the eavesdropper is able to use an antenna adapted to the frequency of the signal on which the receiver is set.

2.3 Hardware vs. Software Setup

To speed up the attack, the attacker needs an essential information concerning the signal: the carrier frequency and the bandwidth of the signal. The carrier frequency is introduced as the crosstalk effect is equivalent to a modulation with close or strong signals like the clock. Indeed this phenomenon introduces a few carrier frequencies as modeled by Li *et al* in [15].

To provide these elements, we propose two possibilities.

On the one hand we can implement the state of the art methodology as used in [1]. It is based on the use of the spectrum analyser/TEMPEST receiver like during a TEMPEST evaluation. Hardware frequency scanning takes advantage of the receiver's dynamic which is often far better than the Analog to Digital converter involved in an oscilloscope. Moreover these receivers offer a large panel of configurations. For example the range of frequencies is $[0, 20]$ GHz and the maximum bandwidth can reach 500 MHz. They are equipped with pre-amplifiers that enhance the dynamic range with a low noise figure. To conduct a TEMPEST evaluation, the evaluator must scan the whole range of frequencies with a spectrum analyser and meanwhile check visually the demodulated signal in order to find sensitive information. The TEMPEST receiver can be tunned continuously between 100 Hz and 10 GHz, with a variable bandwidth. This work is time consuming and irksome, and depends on the evaluator's acuity and background.

On the other hand, we propose to use exclusively a digital oscilloscope, instead of a TEMPEST receiver or more largely a receiver/spectral analyser. By accumulating measurements, we improve the traces accuracy. This helps to achieve an accuracy comparable to that of the receiver. A large number of traces of the signal radiated from the PS/2 cable are recorded. This black signal is divided into parts corresponding to the state level of the red signal. Those parts are Fourier transformed. They highlight consequently different frequency ranges where the compromising signal is potentially present. This methodology can produce the first coarse elements of a TEMPEST evaluation, and allows to avoid the time consuming phase of scanning the whole range of frequencies. We introduce software methods to analyse and characterize the compromising signal. For this paper we used a digital oscilloscope sampling at 1 GigaSample per second. A receiver as in [13] can be used to check our results.

3 Frequency Distinguisher

The phenomena of compromising signal has different origins such as 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 [1] 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* provides in [15] a model to explain such kind of modulation.

In [20], authors use standard techniques, such as Short Time Fourier Transform (STFT) and compute spectrum to detect compromising emanations. The STFT provides a 3D signal with time frequency and amplitude. Another approach is traditionally done by using a spectral analyser to detect signal carriers. Thus the whole frequency range of the receiver is scanned and at each potential frequency of interest the signal is demodulated by the evaluator and manually checked for a presence of red signal.

We lack a lot of information about the TEMPEST tests, which remain classified. Nevertheless, Fig. 3 lets us think that the tools employed for this kind of evaluation are not only based on the spectrum analysers commonly used in standard electromagnetic compatibility (EMC) and radio frequency interference (RFI) testing. As shown in figure 3, the signal in the frequency domain becomes exploitable beyond 15.0 MHz, which is coherent with our equipements' specifications. The bi-conical antenna is amplified with low-noise amplifier of 60.0 dB and has an approximative bandwidth of 30.0 MHz to 300.0 MHz. Consequently we cannot observe the low frequencies of the signal data, but we observe a high peak at 28.0 MHz. This peak could correspond to some odd harmonic of the internal

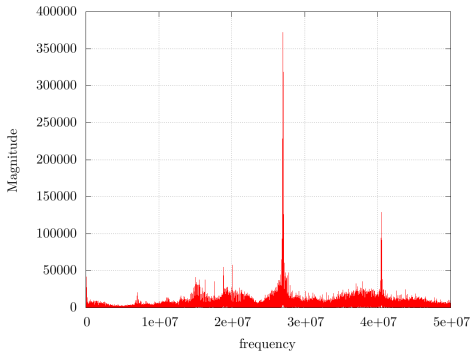

Fig. 3. Spectrum of the black signal.

keyboard microcontroller, for instance the seventh (7.0×4.0 MHz) for a microcontroller inside the keyboard running at a frequency of 4.0 MHz, depending on the device constructor, as described in [9, 10].

Hence the indirect emanations are also caused in our case by the cross-talk and the coupling among the internal frequency clock of the keyboard's microcontroller, the data and the clock frequency signal of the PS/2 line. Besides the FFT applied on the whole black signal does not provide us every leaking frequencies.

Therefore we propose in the sequel an approach based on the correlation between the red signal measured directly from the target system and the black signal, noisy and distorted, received from antenna proposed. We can distinguish the keystroke by the position of the falling edges of the data signal. We propose to gather a large number of measurements with the same keystroke. Each pair is composed of a red signal related to the data and a black signal from the antenna as shown in Fig. 4. Then after acquisition the black signal is cut according to the data, represented by the red signal.

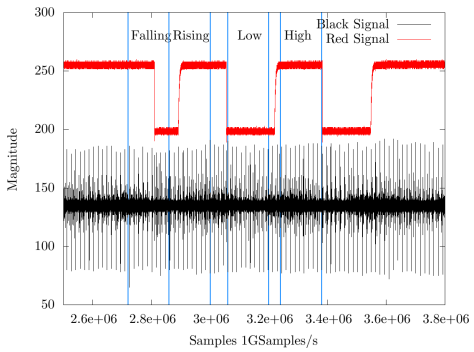

Fig. 4. Red/Black signals.

The parts of the black signal correspond respectively to the low state, high state, falling edge and rising edge of the red signal, and an additional part corresponding to the ambient noise. When no data are transmitted by the PS/2 link, the bus line is in the "Idle" state (*see Section 2.1*). This technique is also used in [17]. After this windowing phase we perform a FFT for each part of the measure. Each section of the signal is equal in term of number of samples. Then we calculate an average spectrum and the variance for each part of the signal. It is noticeable that the results do not change with the size of the window. Firstly we introduce a technique inspired from the Correlation Power Analysis.

An approach based on the correlation between the red signal measured directly from the target system and the black signal, noisy and distorted, received from antenna is appropriate. As we will see in the next section, we can attribute to each part of the signal a specific spectral signature. We propose in Section 3.1 an empirical approach.

3.1 First Approach Based on the CPA

We use an approach derived from CPA, introduced in [3]. However we process the signal in frequency domain, as already shown in these papers [7, 17]. They introduced the DFA, *i.e.* the Differential Fourier Analysis. In this technique, the FFT (*Fast Fourier Transform*) is used to avoid synchronization problems. In [16], the FFT is used to mitigate randomization countermeasures like shuffling. Here the FFT is used in order to select the frequencies which are carrying sensitive information and their bandwidth for characterizing the EM side channel. It is a profiling stage in the frequency domain that allows to learn details about the frequencies that depend of the red signal state. Therefore we compute the difference between

- the mean of the spectrum related to a specific state and
- the mean of the noise spectrum (*i.e.* when nothing occurs on the PS/2 link).

Then we divide this difference by the variance of the noise. It is suggested in [14] that in some cases the normalization factor induces a high noise level in CPA signal; to avoid this artifact, it is recommended to add a small positive constant ϵ to the denominator.

Thus we obtained four vectors in frequency domain by computing:

$$\rho(f, State) = \frac{E(f, State) - E(f, N)}{\sigma(f, N) + \epsilon},$$

where $E(f, State)$ and $E(f, N)$ represent the averaged spectrum curve obtained respectively for one state and for the noise. $\sigma(f, N)$ stands for the variance of the noise for every frequency f. State is a state from the StateSet set, defined as the set containing all the possible configurations of the red signal: $StateSet = \{High, Low, Falling, Rising\}$. The four frequency vectors corresponding to each state are plotted in Fig. 5. From these curves, we can deduce the range of frequencies that characterize each state.

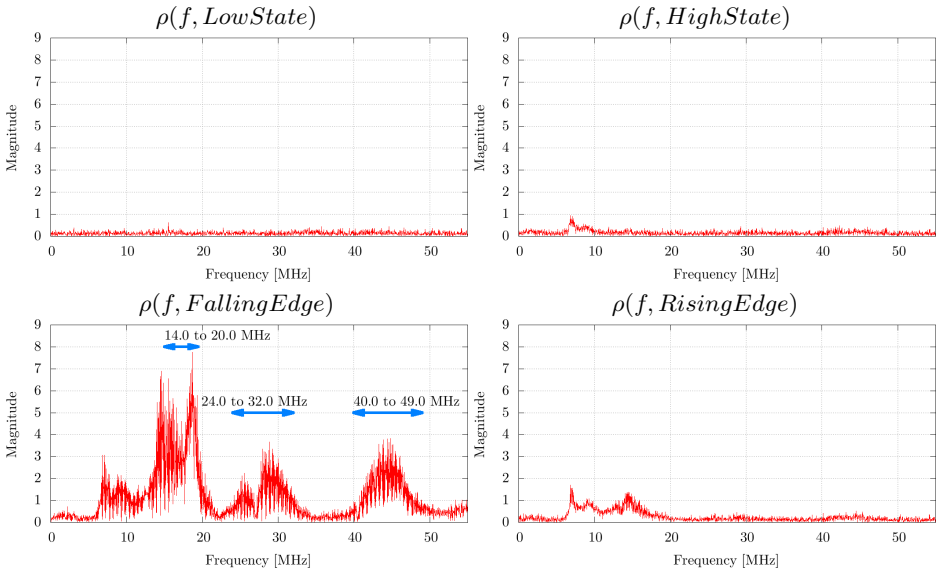

Fig. 5. Results of the Correlation for every state.

The "correlation" level in $\rho(f, Falling)$ is higher and contains a lot of frequency peaks compared to the other frequency domains traces. We notice three ranges of relevant frequencies:

- between 14.0 and 20.0 MHz,
- between 24.0 and 32.0 MHz,
- between 40.0 and 49.0 MHz.

3.2 Approach based on Mutual Information Analysis.

In Sec. 3.1, we highlighted a range of frequencies that can possibly carry information about the red signal. Now we adopt an information theory viewpoint. In previous work [19], Tanaka used the calculation of the channel capacity (using information theory) for evaluating the success rate of spied images reconstruction. The author calculates the amount of information per pixel in the reconstructed image and estimates a threshold from which it is effective. In our case, it is also interesting to adopt a method based on the information theory, in order to retrieve the relevant frequencies and to bring evidence that the information is not necessarily carried by the clock frequency and its harmonics such as specified by Carlier *et al.* in [4].

In 2008, Gierlichs introduced in [8] the Mutual Information Analysis. This tool is traditionally used to predict the dependence between a leakage model and observations (*or Measurements*). Therefore we can use it as a metric that gives an indicator on carriers frequencies. To do so, we compute for each frequency

the Mutual Information (MI) $\mathrm{I}(O_f; State)$ between Observations O_f and $State$ that corresponds to the state of the red signal. Thereby, if $\mathrm{I}(O_f; State)$ is close to zero for one frequency, we can say that this frequency does not carry significant information. On the contrary, if $\mathrm{I}(O_f; State)$ is high, the sensitive data and the frequency are bound. If we filter the black signal around this frequency, we can retrieve a significant part of the red signal. The MI is computed as:

$$\mathrm{I}(O_f; State) = \mathrm{H}(O_f) - \mathrm{H}(O_f|State), \tag{1}$$

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

$$\mathrm{H}(O_f) = -\int_{-\infty}^{+\infty} \Pr(O_f)(x) \log_2 \Pr(O_f)(x)\, \mathrm{d}x,$$
$$\mathrm{H}(O_f|State) = \sum_{s \in State} \Pr(s)\mathrm{H}(O_f|s).$$

with

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

where $\Pr(O_f)$ denotes the probability law of observations at frequency f. The random variable O_f takes its values x on $\mathbb{R}$, and $\Pr(O_f)(x)\,\mathrm{d}x$ is the probability that O_f belongs to $[x, x + \mathrm{d}x]$. Besides we consider that the states configuration are equi-probable events therefore $\forall s \in State$, $\Pr(s) = \frac{1}{4}$. And the distribution is assumed to be normal $\sim N(\mu, \sigma^2)$ of mean μ and variance σ^2, given by:

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

we call 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 μ and standard deviation σ as the analytical expression: $H(O_f) = \log_2(\sigma\sqrt{2\pi e})$. From this value, the Mutual Information defined in Eqn. (1) can be derived, by combining for each state the differential entropy:

$$\mathrm{I}(O_f; State) = \mathrm{H}(O_f) - \frac{1}{4}(\mathrm{H}(f|High) + \mathrm{H}(f|Low) + \mathrm{H}(f|Rising) + \mathrm{H}(f|Falling)),$$

that can be simplified as:

$$\mathrm{I}(O_f; State) = \frac{1}{4} \log_2 \frac{\sigma_{O_f}^4}{\sigma_{O_f,High}\sigma_{O_f,Low}\sigma_{O_f,Rising}\sigma_{O_f,Falling}}. \tag{2}$$

The figure 6 represents the result of Eqn. (2).

The result of the MIA are similar to that of $\rho(f, FallingEdge)$: we obtain the same ranges of relevant frequencies. In this respect, we confirm that some

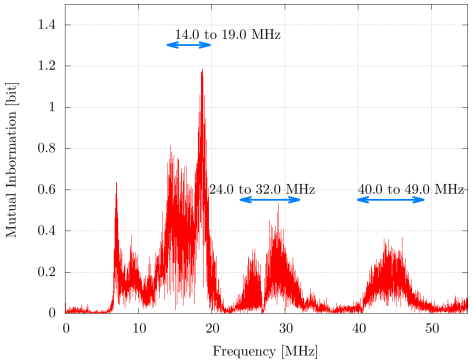

Fig. 6. Result of Mutual Information Metric I(f; $State$).

frequencies radiate more information than the others. As this method provides a result with a quantity expressed in bit, the leakage frequencies are easy to interpret. Consequently we are now able to fairly compare the level of compromising signal emanated by different keyboards or electronic devices. Such MI metric also allow to quantify the level of protection against TEMPEST attacks. In addition to the CPA approach, it is worthwhile to underline that MI considers the non linear dependencies; this metric is able to capture any coupling, such as cross-talk, that occurs when keys are pressed on a PS/2 keyboard.

3.3 Frequency Distinguisher in Principal Subspaces

The identification of relevant frequencies can also benefit from the PCA (Principal Component Analysis). The PCA has been applied to side-channel analysis by Archambeau *et al.* in [2] and Standaert *et al.* in [18] in the case of template attacks. In order to investigate the benefit of PCA, we have adapted it to our topic. In this approach, we use the same partitioning as defined previously in section 3. The observations of black signal in frequency domain are classified according to the state of the data signal, in order to build the covariance matrix. We denote by $\mu_j(f)$ the average of the observations corresponding to a state j, and by $\mu(f)$ the average of all the observations: $\mu(f) = \sum_{j \in StateSet} \mu_j(f)$. The attacker also computes the covariance matrix Σ_o, as:

$$\Sigma_o = \frac{1}{4} \sum_{j \in StateSet} (\mu_j(f) - \mu(f))(\mu_j(f) - \mu(f))^\mathsf{T} . \tag{3}$$

The PCA gives us four main components, which are linear combinations of the four per state black signals averages in frequency domain. These components form a basis, which characterizes four modalities of compromise. The main leakage modality is given by PCA as the eigenvector corresponding to the largest eigenvalue. The four eigenvectors are plotted in Fig. 7.

On the first eigenvector, the three frequencies ranges identified by CPA and MI are visible. Nonetheless, the ranges [24.0, 32.0] MHz and [40.0, 49.0] MHz

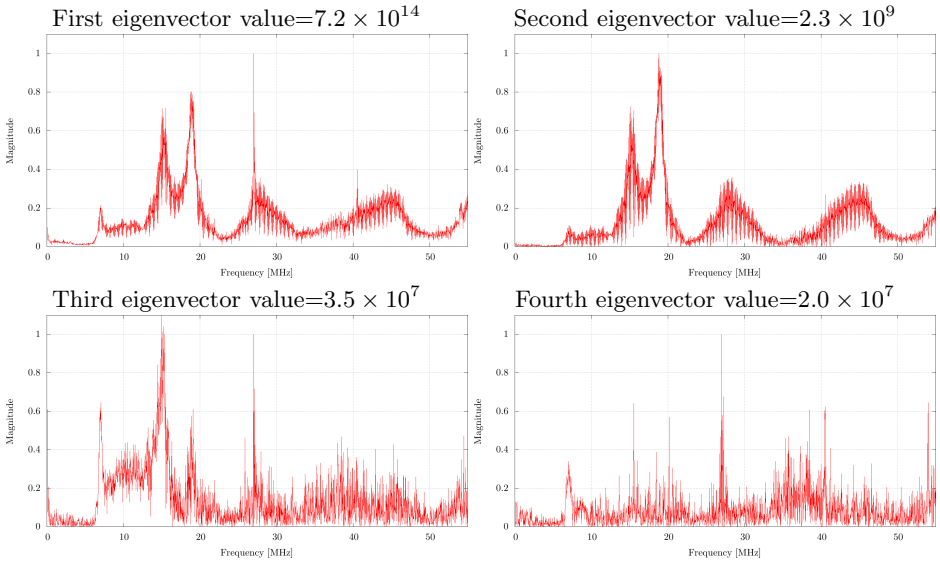

Fig. 7. The four eigenvectors obtained by PCA.

have a small amplitude and are noisy. Additionally, one narrow peak appears at $f = 27$ MHz, that can be bound to the frequency of the keyboards' microcontroller. The second eigenvector is very similar to the first one. Anyway the ratio between the largest eigenvalue and the second one is greater than five orders of magnitude. This means that the first direction contains an overwhelming quantity of information. The fourth eigenvalue is theoritically null, but because the covariance matrix is badly conditioned the numerical computation yields value2×10^7 this indicates that the eigenvector corresponding to small eigenvalue are very approximative, thus untrustworthy. Therefore the two last ones carry mostly noise information. However the PCA does not consider the nonlinear dependencies.

To summarize, in Tab. 1 we establish a comparison between the different methods.

To check the results obtained with the three previous methods, two ways can be followed. The first one consists in using a hardware receiver, as described by Agrawal in [1] and Kuhn in [6]. The second one consists in software demodulation thanks to an appropriate filtering.

4 Extraction of the Compromising Signal.

4.1 Confirmation of the Results with a Hardware Receiver.

Different types of hardware receivers exist. We can cite receivers such as described by Agrawal in [1] or Kuhn in [6]. Typically, Kuhn presents in his PhD

Distinguisher	Advantages	Drawbacks
CPA	⋆ Easiest method	⋆ Empirical methods. ⋆ Four curves results. ⋆ Hard to compare two implementations. ⋆ Only linear dependencies considered.
MIA	⋆ Based on information theory. ⋆ Single curve result. ⋆ Commensurable results (Mutual Information values are expressed in bits). ⋆ Non-linear dependencies considered.	
PCA		⋆ Hard to compare two implementations. ⋆ Results are not only on first eigenvector. ⋆ Spurious peaks appear. ⋆ Only linear dependencies considered.

Table 1. Drawbacks and Advantages of the three analyzed distinguishers.

thesis the R-1250 produced by *Dynamics Sciences*. Those receivers are superheterodyne and wide-band. They offer a large panel of configurations. For example, they can be tuned continuously between 100 Hz and 1 GHz and they offers the selection of 21 intermediate frequency bandwidths from 50 Hz to 200 MHz. 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:

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

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.

With such a device, we successfully demodulate the black signal at various frequencies, as shown in Fig. 8. We focus on a range of frequencies between 0.0 and 50.0 MHz, and demodulate at the frequencies exhibited by the previous methods (PCA, MIA and PCA), at 17.0 MHz, 27.0 MHz and 41.0 MHz with a bandwidth of 1 MHz. Each time, the demodulated signal shows a peculiarity that allows to distinguish clearly the state of the red signal. More precisely, the falling edge of the red signal is indicated by a clear peak. This concurs with the observation about the "falling edge transition technique" explained by Vuagnoux in [20]. Also, it is consistent with observations from Section 2.1.

Moreover the data are read on the falling edge of the clock. Consequently the falling edge of the clock occurs just after the falling edge of the data, as already shown in Fig. 1. We see on the demodulated signal that the energy at dates corresponding to the clock falling edges is not constant. Empirically, clock peaks have more energy when the state of data signal is high, and are doubled by falling transitions of the signal data. This is another leakage that can be used to recover the red signal.

During these experiments we noticed an other kind of compromising signal not based on the "Falling edge Transition Technique". As shown in Fig. 8, at the frequency 36.0 MHz, only the signal related to data (falling edge) appears, whereas the peaks bound to the clock completely disappear. This compromising signal is not very obvious to characterize, and requires some care to find the adequate frequency of demodulation. In this case, the TEMPEST receiver definitely provides us the setup to pinpoint this compromising frequency.

4.2 Software Filtering

To estimate the part of the sensitive signal contained in our measurements, and also to find the compromising signal, we devise a software band-pass filter by using MATLAB. We perform bandpass filtering within the range frequencies identified during the leaking frequencies characterization stage.

We propose to realize a filter based on the zero padding technique in frequency domain: its frequency response is sketched in Fig. 9. The complete software demodulation consists of:

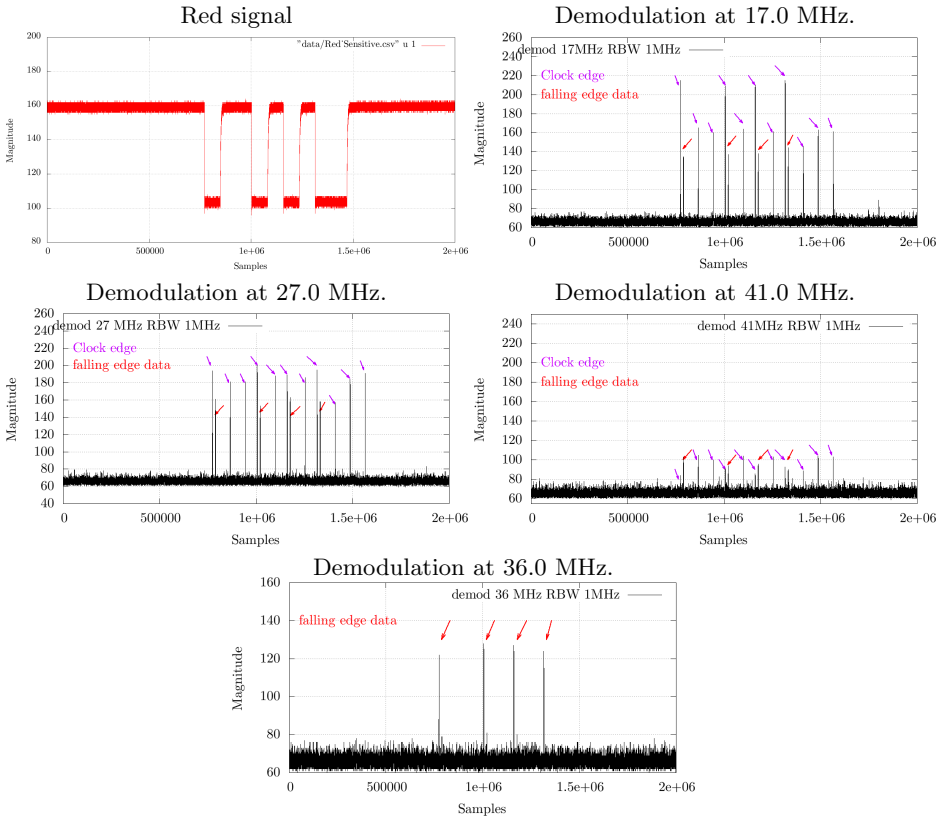

Fig. 8. Results of demodulation (red signal, and black signal demodulated at 17.0 MHz, 27.0 MHz,41.0 MHz and 36.0 MHz).

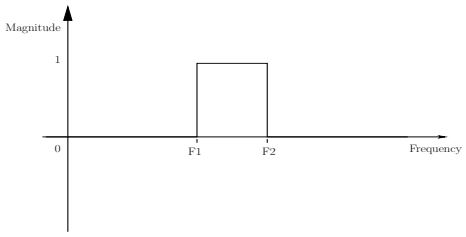

Fig. 9. Design of bandpass filter.

– converting the black signal from the time to the frequency domain thanks to an FFT,
– multiplying this signal with our pass-band filter,
– converting back the signal from the frequency to the time domain thanks to an IFFT.

This process allows to obtain the approximative shape of the demodulated signal, from which we are hopefully able to extract the key that was pressed.

The figure 10 shows the result of a single black curve demodulated by this software approach. We can distinguish the compromising signal, *i.e.* the falling edge of the data line. Furthermore, the levels of the compromising signal related to PS/2 clock do not have the same amplitude: it is directly linked to that of the red signal's state.

Those observations do match those obtained with the hardware demodulator. Thus the software filtering process offers the possibility to have a coarse idea of the compromising signal shape.

Nevertheless with this tool we do not have the advantage of hardware demodulation:

– the bandwidth of the software filter is larger: it cannot be set that narrow as the 1 MHz of the hardware receivers;
– the compromising signal at 36 MHz spotted by the hardware receiver is not visible with the software filtering: no compromising signal is visible.

5 Conclusion

We introduce a new set of techniques to extract the leakage frequencies of the black signal providing information about the red signal. They have successfully been tested on the electromagnetic emissions of a PS/2 keyboard intercepted at a distance of 5 meters. By the help of side channel analysis methods applied in frequency domain, we are able to distinguish the frequencies that are more leaking sensitive information and their bandwidth. Thanks to these tools (inspired from CPA, MIA and PCA), we demonstrate that we are in position to give quick diagnostics about EM leakage.

Our experiments show that the leakage is carried by some frequencies that are not necessarily the harmonics of the clock frequency. This confirms the observations previously done in the work of M. Hutter *et al.* [11]. We also notice that our three methods retrieve the same compromising spectrum shape, and consequently the same leakage frequencies. CPA and MIA yield clearly the most accurate results. Some frequencies that leak more sensitive information than others might result from intermodulation. We show that the red signal can be recovered from the demodulation of the black signal, either with a hardware receiver or by a software band-pass filtering technique, which consists merely in selecting frequencies of interest from the FFT of the black signal. Despite its simplicity, this filter enables an identification of the leakage in time domain.

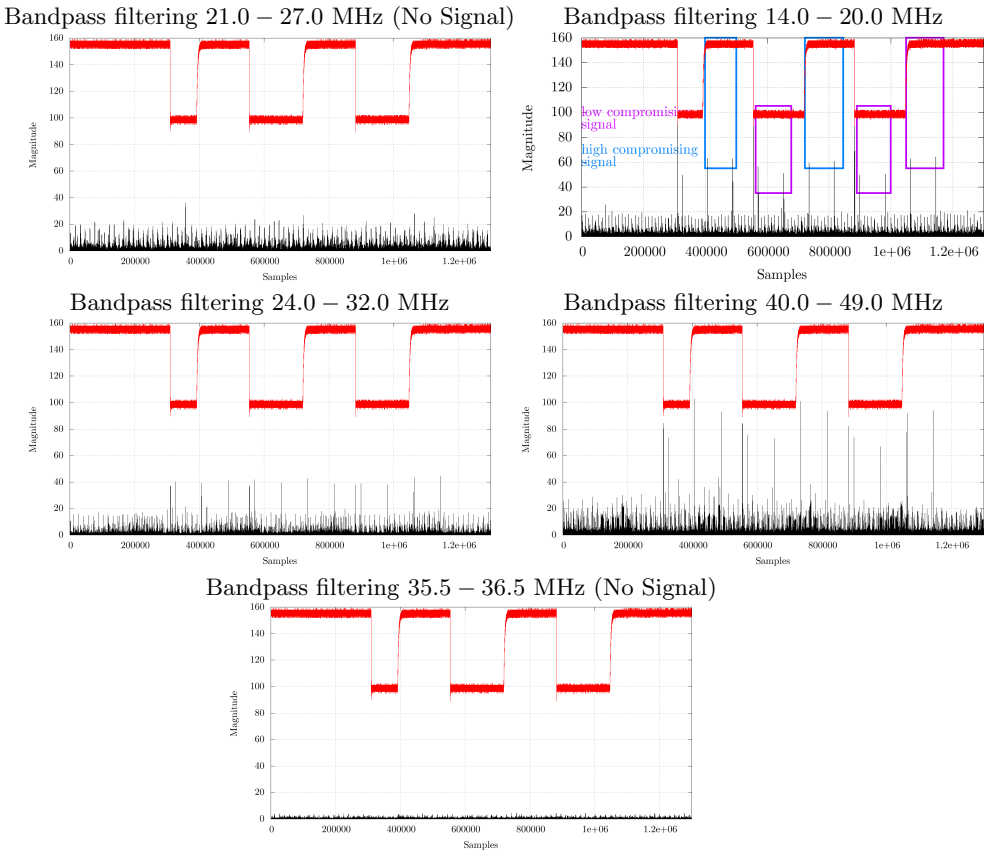

Fig. 10. Results of software demodulation.

We could successfully characterize the leaking frequencies from our black signal using our methods. This allows us to recover the secret information which is the red signal in this case. However, these generic methods could also be applied in different contexts, for instance RSA recovering key problematics. Indeed in asymmetric cryptography, the sequence of operations are secret dependant. Someone able to find out square and multiply operation sequences occurring during an RSA encryption is able to recover the private exponent. A possible extension to this work could consist in applying our methodology to a confidential sequence of operations.

References

1. Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The em side–channel(s). In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002*, volume 2523 of *LNCS*, pages 29–45. Springer, 2003.
2. Cédric Archambeau, Éric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater. Template Attacks in Principal Subspaces. In *CHES*, volume 4249 of *LNCS*, pages 1–14. Springer, October 10-13 2006. Yokohama, Japan.
3. Éric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In *CHES*, volume 3156 of *LNCS*, pages 16–29. Springer, August 11–13 2004. Cambridge, MA, USA.
4. Vincent Carlier, Herve Chabanne, Emmanuelle Dottax, and Herve Pelletier. Electromagnetic side channels of an fpga implementation of aes, 2004.
5. Wim Van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? In *Computers Secutity*, 1985.
6. KUHN M. G. Compromising emanations: Eavesdropping risks of computer displays. In *Technical Report UCAM-CL-TR-577*.
7. Catherine H. Gebotys, Simon Ho, and C.C. Tiu. Em analysis of rijndael and ecc on a wireless java-based pda. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2005*, volume 3659 of *LNCS*, pages 250–264. Springer, 2005.
8. Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual information analysis. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *LNCS*, pages 426–442. Springer, 2008.
9. `http://www.beyondlogic.org/keyboard/keybrd.htm`.
10. `http://www.computer-engineering.org/ps2keyboard/`.
11. Michael Hutter, Stefan Mangard, and Martin Feldhofer. Power and em attacks on passive \$13.56 MHz\$ rfid devices. In *CHES '07: Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems*, pages 320–333, Berlin, Heidelberg, 2007. Springer-Verlag.
12. Markus G. Kuhn. Security limits for compromising emanations. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2005*, volume 3659 of *LNCS*, pages 265–279. Springer, 2005.
13. Markus G. Kuhn and Ross J. Anderson. Soft tempest: Hidden data transmission using electromagnetic emanations. In *Information Hiding*, pages 124–142, 1998.

14. Thanh-Ha Le, Jessy Clédière, Cécile Canovas, Bruno Robisson, Christine Servière, and Jean-Louis Lacoume. A Proposition for Correlation Power Analysis Enhancement. In *CHES*, volume 4249 of *LNCS*, pages 174–186. Springer, 2006. Yokohama, Japan.
15. Huiyun Li, A. Theodore Markettos, and Simon Moore. Security evaluation against electromagnetic analysis at design time. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2005*, volume 3659 of *LNCS*, pages 280–292. Springer, 2005.
16. Thomas Plos, Michael Hutter, and Martin Feldhofer. Evaluation of side-channel preprocessing techniques on cryptographic-enabled hf and uhf rfid-tag prototypes. In Sandra Dominikus, editor, *Workshop on RFID Security 2008, Budapest, Hungary, July 9-11, 2008*, pages 114 – 127, 2008.
17. Oliver Schimmel, Paul Duplys, Eberhard Boehl, Jan Hayek, and Wolfgang Rosenstiel. Correlation power analysis in frequency domain. In *COSADE*, pages 1–3, February 4-5 2010.
18. François-Xavier Standaert and Cedric Archambeau. Using subspace-based template attacks to compare and combine power and electromagnetic information leakages. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *LNCS*, pages 411–425. Springer, 2008.
19. Hidema Tanaka. Information Leakage Via Electromagnetic Emanations and Evaluation of Tempest Countermeasures. In *ICISS*, pages 167–179, 2007.
20. Martin Vuagnoux and Sylvain Pasini. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. In *Proceedings of the 18th USENIX Security Symposium*. USENIX Association, 2009.