Practical Electro-Magnetic Analysis

Non-Invasive Attack Testing Workshop NIAT-2011

Fred de Beer, Marc Witteman, Bartek Gedrojc and Yijun Sheng

Riscure, The Netherlands

{debeer, witteman, gedrojc, sheng}@riscure.com

Abstract: Electro-Magnetic Analysis is a technique that can be used to test leakage of secret information from cryptographic devices through radiation. Development of this technique requires advanced knowledge of physics and signal processing, but the resulting tools can be applied straightforward with little training.

Attacking unprotected devices with EMA is relatively easy, and these devices may be broken in less than an hour with EMA.

EMA is attractive if components on chip filter leakage or add noise to the power signal or if a power tap is hard to install. In other cases, power analysis usually requires less effort to break an unprotected product.

Keywords: Electro-Magnetic Analysis, Non-Invasive, Side Channel Attacks, Embedded Systems

1 Introduction

Embedded systems with cryptographic functionality often operate in hostile environments and need protection against side channel attacks. Power analysis attacks have grown popular although EMA (Electro-Magnetic Analysis) offers significant benefits when analyzing devices with non-standard interfaces, when a power tap is hard to configure or when power analysis countermeasures are implemented [1], [2].

In this article we show the benefits of EMA and its practical use. We discuss application scenarios, probe design, spatial exploration and post processing techniques. Finally, we explain the steps in a practical, completely non-invasive attack, and compare the EMA outcome of two different probes with the results of power analysis for two different target devices.

2 Application scenarios

We discuss two reasons why EMA would be applied for testing side channel resistance of embedded systems or smart cards.

2.1 Hard to install power tap

For cryptographic processors on large embedded chips, installing a power tap may be difficult for various reasons:

- The power line may run though one of the inner layers of the printed circuit board,
- The power pin that feeds the process of interest (e.g. the encryption running on a separate cryptographic processor) may be difficult to select out of the many power pins,
- The insertion of a measurement resistor or current probe between a stabilizing capacitor 2, see figure 1, and the power pin needs space which is not always available. Extending the connection between capacitor and embedded processer with a wire introduces additional wire inductance. This wire inductance together with the impedance of the measurement resistor or current probe may result in a supply voltage fluctuation causing an unreliable operation of the processor. Another option is to insert a measurement resistor or current probe between stabilizing capacitors 1 and 2, however this will reduce the measurement quality significantly.

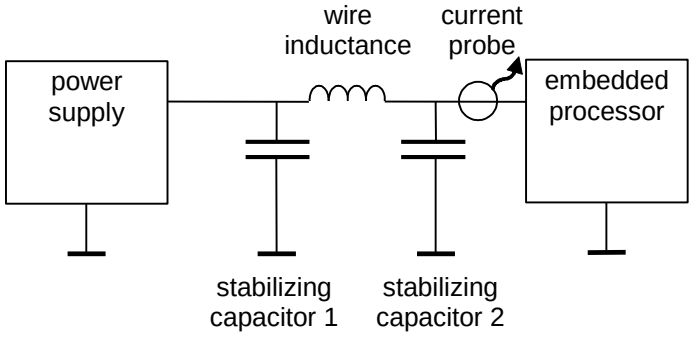


Fig. 1 Simplified connection scheme between power supply and embedded processor.

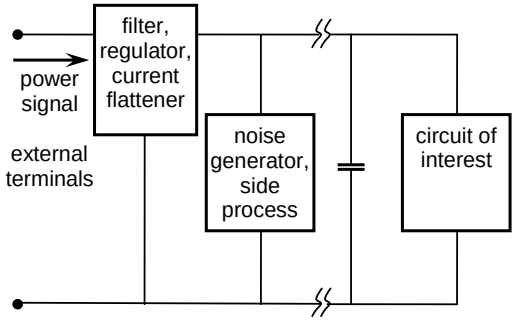


Fig. 2 Simplified chip circuit diagram, showing connections between terminals, filter, noise generator and circuit of interest.

2.2 Noisy power signal

The power consumption of the chips may be noisier or show less data leakage compared to the power consumption of the circuit of interest for various reasons:

- The circuit of interest is usually not directly connected to the power pin, see figure 2. Power regulation and stabilization components act as a low pass filter for the power signal. Additional filter components may be added as countermeasure against power analysis. An effective circuit against power analysis is a current flattening circuit. The current flattener regulates the input current to a fixed level, reducing information leakage by the circuit of interest. An example is shown if figure 3, showing first the clear and detailed power consumption signal of a chip without current flattening activated, and then the power signal from the same chip with current flattening activated.
- The power pin is usually also connected to other actives areas on the chip beside the circuit of interest. The power consumption of the other areas adds noise to the power signal from the circuit of interest. Additional power fluctuations may also be added as countermeasures against power analysis

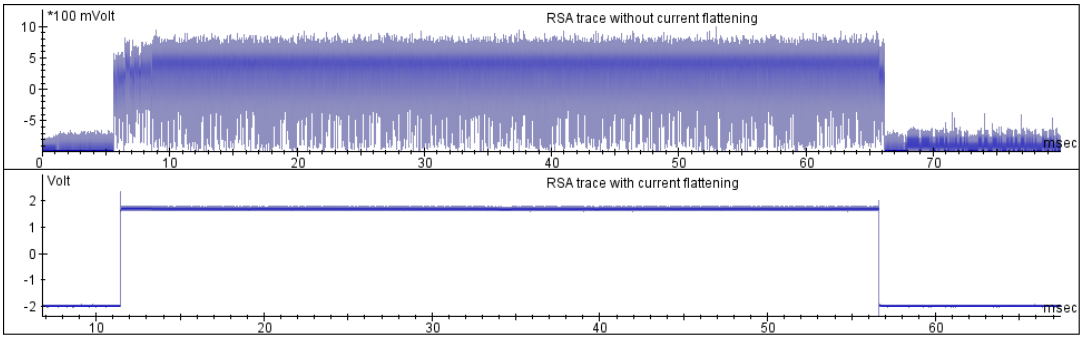


Fig. 3 Power signal without and with current flattening

For both situations, the EM probe is capable of measuring the signals inside the chips without, or with less, influence of side processes or countermeasures.

3 EM probe design

The selection of a suitable EM probe is a first step that strongly influences the EMA results. EM probes differ in measured quantity (magnetic H- and B-field), sensitivity, spatial resolution and frequency band width. We will explain the trade-off between these characteristics and propose a practical optimum.

3.1 Probe requirements

The probe is a combination of sensor and amplifier. The following EM probe requirements are defined:

- The probe orientation must match the direction of the emanated EM field, see figure 4. The EM field is generated by an electrical current that flows through a loop within the die plane. If loop size is equal or smaller than the EM probe resolution, then the average EM emanation over the loop is pointing out of the die plane. An inductive sensor is sensitive to this field when the coil axis is directed perpendicular to this plane.

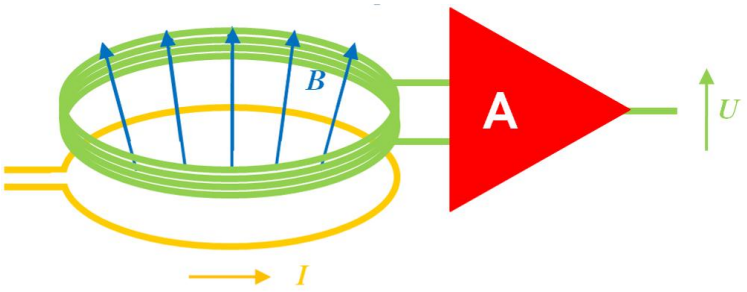


Fig. 4 Orientation of current loop (yellow) and sensor coil (green)

The spatial resolution of the probe should be equal to the die area that is involved in the process under investigation, e.g. the size of the crypto processor. Probes with a lower resolution will also include EM emanation of processes that run in adjacent die areas, resulting in a lower signal to noise ratio. Probes with a higher resolution will only measure part of the process under investigations (e.g. only part of all involved S-boxes). To capture the full process measurements at several die locations are required. The resolvable detail size of a near field sensor is usually approximately equal to the probe size, provided that the distance between sensor and die is smaller than the sensor size. For a non-invasive measurement this minimum distance is usually limited to thickness of the die cover (~ 1 mm). Usually the resolution is limited by the minimum distance between die and sensor.

- The EM probe (combination of sensor and amplifier) sensitivity must be sufficient to use the full input range of the oscilloscope for a typical EM field strength. Typical field strength of smart cards was found to be in the order of magnitude of 1 µT in the frequency range between 1 and 50 MHz. A minimum full input range of 100 mV is selected, which is usually available on mid and high end oscilloscopes. The EM probe sensitivity requirement is in the order of magnitude of 100mV/µT for the frequency

range of 1 – 50 MHz. Since embedded processors usually operate at higher power consumption than smart cards, their EM emanation is usually stronger, up to approximately 10 times. The sensitivity does not need to be constant over the frequency range, a low noise signal is more important.

- The transistor switching time is shorter than the clock cycle. To capture these transients, we set the requirement of the probe bandwidth to at least 5 times the clock frequency. For smart cards, a bandwidth of 250 MHz is usually sufficient, for embedded processors with higher clock frequencies a larger bandwidth is required.

These requirements may be used for probe selection.

3.2 Probe variants

There is a large range of EM probes. The probes with a coil as sensor are the most widely used. These probes may be divided into B-field and H-field probes based on their design and characteristics as will be explained below.

3.2.1 B-field probes

B-field probes usually have a coil with multiple windings providing a strong output signal. The probe amplifier is a voltage amplifier with high input impedance and an output signal $u_o(t)$ proportional to the time derivation of the B-field $B(t)$ and the generating current $i(t)$:

$$u_o(t) = C_2 \, dB(t)/dt = \mu C_2 C_1 \, di(t)/dt$$

with:
C_2 = constant depending on probe sensor parameters and amplifier gain
μ = the magnetic permeability
C_1 = constant depending on the parameters of the current loop on chip

Figure 5 illustrates the relation between simultaneously measured EM probe signal $u_o(t)$, the current signal $i(t)$ and the power signal $p(t)$. The current signal $i(t)$ on the die is calculated by integration of the EM probe signal. The high frequency components in the measured power signal $p(t)$ are usually reduced compared to the current signal on the die.

These characteristics give the B-field probe its high and increasing sensitivity for high frequencies. The bandwidth is usually limited by the amplifier, especially the limited input impedance for high frequencies.

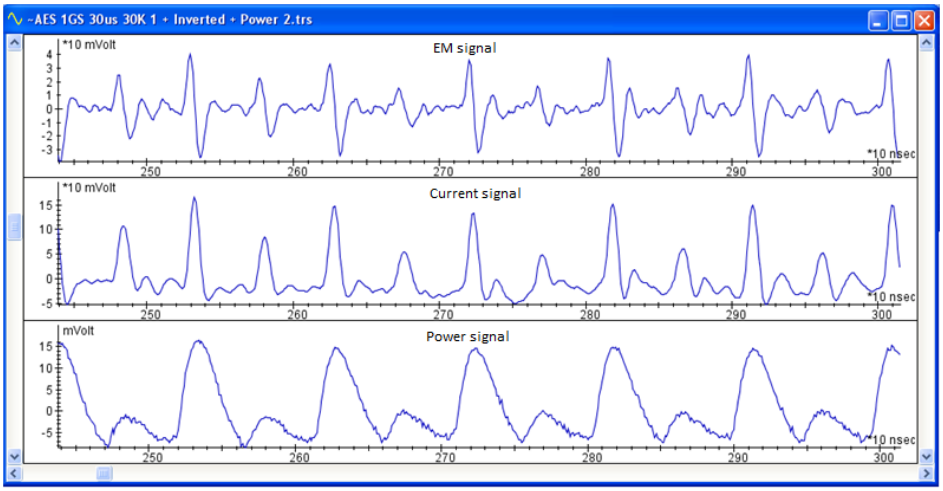


Fig. 5 From top to bottom the EM probe signal, the current signal and the simultaneously measured power consumption

3.2.2 H-field probes

H-field probes usually have an electrically shielded coil with a single winding. The probe amplifier is a current amplifier with a low input impedance and an output signal $u_o(t)$ proportional to the H-field $H(t)$:

$$u_o(t) = C_3\, H(t) = C_3 C_1\, i(t).$$

with:
C_3 = constant depending on probe sensor parameters and amplifier gain

These characteristics give the H-field probe a flat frequency characteristic which is usually limited by the amplifier. This makes the H-probe suitable for EMI measurements.

The H-probe is preferable if a flat frequency range and a linear relationship between current and output signal is required. The B-probe is required if a large sensor signal – resulting is a low noise measurement – is required. The experiments which are described in this paper will illustrate the best choice for EMA.

3.3 Reduction of induced noise

Shielding is often required to reduce electrically and magnetically induced noise. Since the noise source can be close to the target object (e.g. both on the same printed circuit board)

the shielding needs to be close the probe sensor. We distinguish electrically and magnetically induced noise.

3.3.1 Electrically induced noise

There are two options to reduce electrically induced noise:

- A metal shielding covering the coil, see figure 6. The metal ring should be open to avoid full magnetic shielding of the EM emanations from the die. Metal shielding is usually applied to H-field probes with a single winding coil. An electrical shield for B-field probes with multiple winding coils would require too much space.

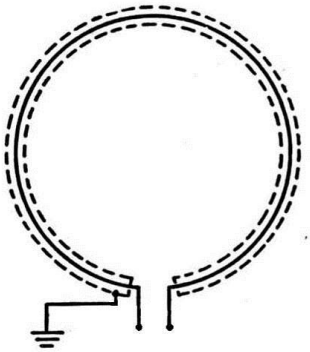


Fig. 6 Electrical shield of single winding coil.

- A symmetric coil with differential amplifier, see figure 7. Electrical induced noise will appear as common mode noise at the two inputs of the differential amplifier while the magnetically induced signal has opposite polarity on the two inputs. The differential amplifier reduces the common mode signal.

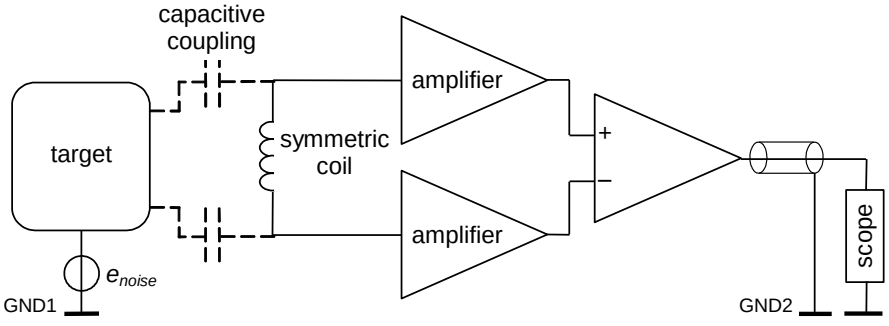


Fig. 7 Differential amplifier with symmetric coil.

3.3.2 Magnetically induced noise

To reduce the magnetically induced environment noise and keep the magnetically induced signal from the chip, we separate signal and noise based on the source location:

- The magnetic signal is coming from a source (the die) which is located underneath the sensor at close distance.
- The magnetic noise is coming from a source (environment) which located next to the sensor and not at close distance.

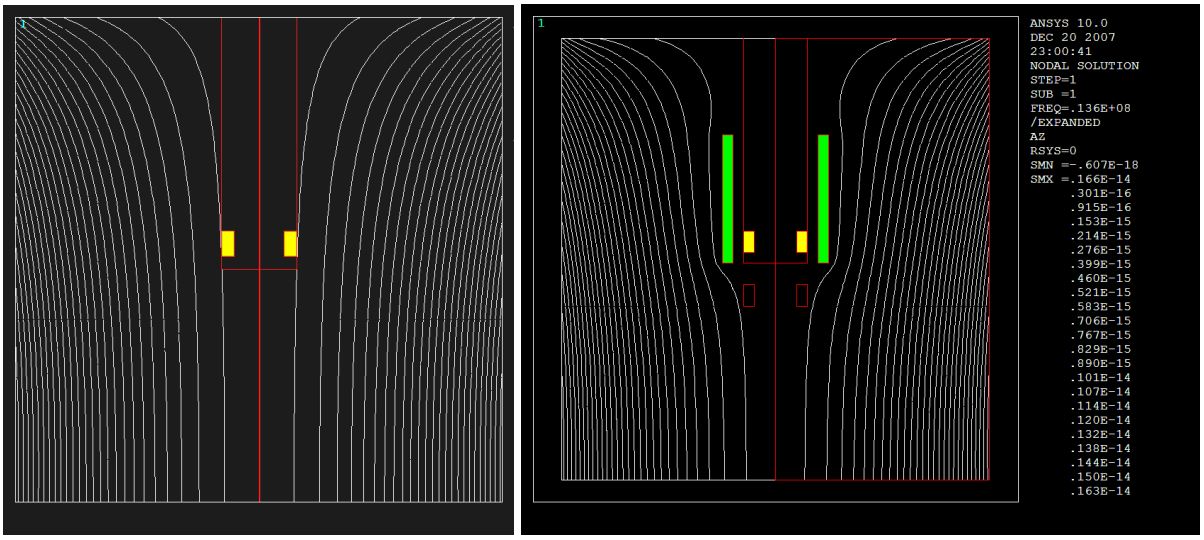


Fig. 8 Effect at sensor (yellow) of magnetic shield (green) on field by noise source at large distance (outside figure)

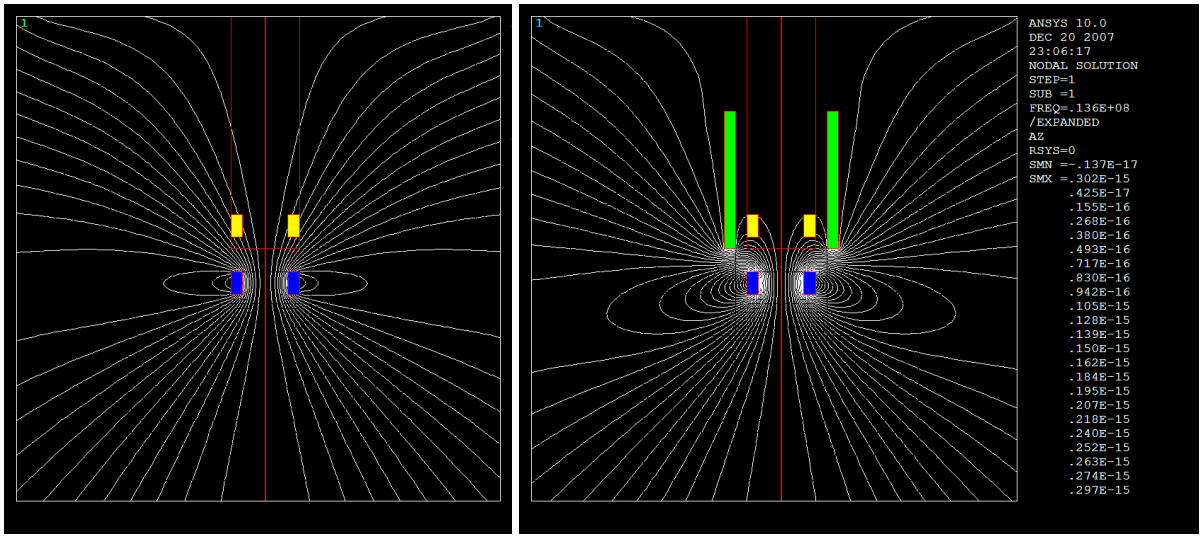


Fig. 9 Effect at sensor (yellow) of magnetic shield (green) on field by noise source (blue) close to shield aperture

This difference in source location is used in a magnetic shield which has an aperture between sensor and die. Figure 8 shows that the magnetic shield *fully* deflects the parallel flux lines for sources at large distance. Figure 9 shows a *partial* deflection for curved flux lines of nearby sources.

4 Analysis methodology

The methodology of Electro-Magnetic analysis differs from power analysis on four points: aliasing, probe positioning, alignment and resampling.

4.1 Avoid aliasing

Aliasing occurs if the analog signal contains components at frequencies above half the sample frequency. Due to aliasing, the signal reconstructed from the sample differs from the original analog signal, see figure 10. For high frequencies, the power signal is usually weak while the EM signal remains strong. Aliasing is therefore more relevant for EM signals. To avoid aliasing a low pass filter should be inserted between the EM probe and the oscilloscope input. Due to the limited decline of the frequency characteristic of the low pass filter, the cut-off frequency is usually not selected at half the sample frequency but lower, e.g. at approximately 1/5 of the sample frequency.

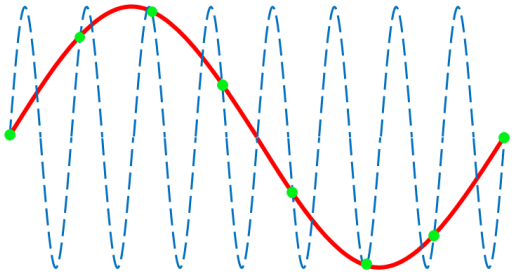


Fig. 10 Illustration of aliasing: the reconstructed signal trough the sample point of the analog input signal (dashed line)

4.2 Probe positioning

An EM probe with high spatial resolution can focus on part of the chip. As a consequence, proper positioning of the EM probe above the chip surface is of importance. A software controlled XY stage scans the chips surface while the process of interest (e.g. cryptographic operation) runs. When several processes with different clock frequencies run simultaneously, the EM signal should be filtered to reduce the frequency components that

relate to uninteresting processes. Figure 11 shows an illustration of a 2x2 mm scan over a smart card surface. The main processor of the smart card runs at the external clock frequency, while the crypto-processor runs at an internal clock. The height corresponds with the signal strength at that each location.

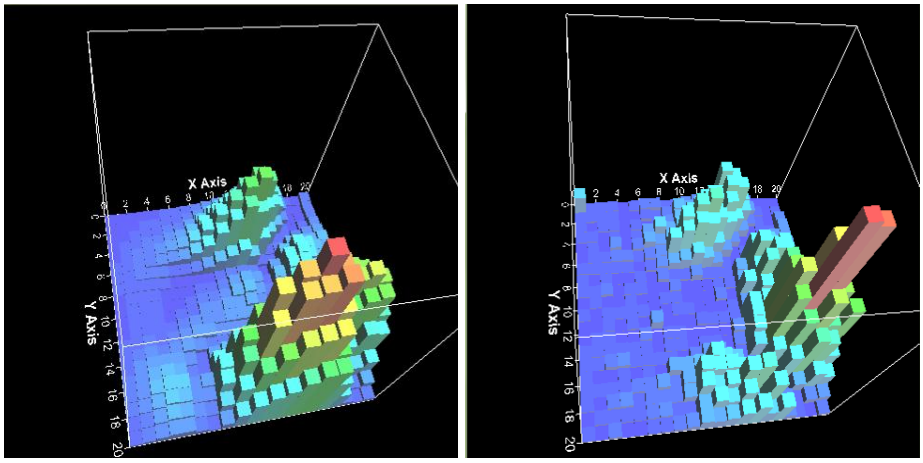


Fig. 11 Illustration of 2x2 mm XY scan over smart card surface: left for external clock frequency, right for internal clock frequency.

We apply two criteria for selection of the best probe position:

- Strong signal in at the clock frequency for the process of interest.
- Out of the locations with a strong signal we select the position that shows a pattern in the EM signal that can be related to the process of interest.

4.3 Alignment

Alignment of noisy traces is usually performed on low frequency patterns. EM signals contain less low frequency components compared to power measurements due to the frequency characteristic of the EM probe. A robust and fast method is to use the low frequency pattern of the envelope of the EM signal. An envelope can be obtained by calculation the absolute value of each sample, followed by a digital low pass filter. Figures 12 to 14 show two EM traces, the absolute value of these traces and the filtered traces. The filtered traces in figure 14 are suitable for alignment. The alignment process determines the number of samples to shift the second traces for proper alignment with the first. To avoid signal loss due to the rectification and filtering process, the determined shift should be applied to the original trace and not the rectified and filtered trace.

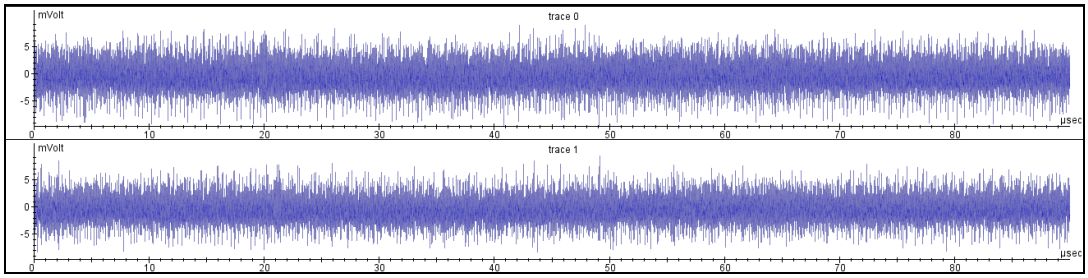


Fig. 12 Two unprocessed EM signal traces

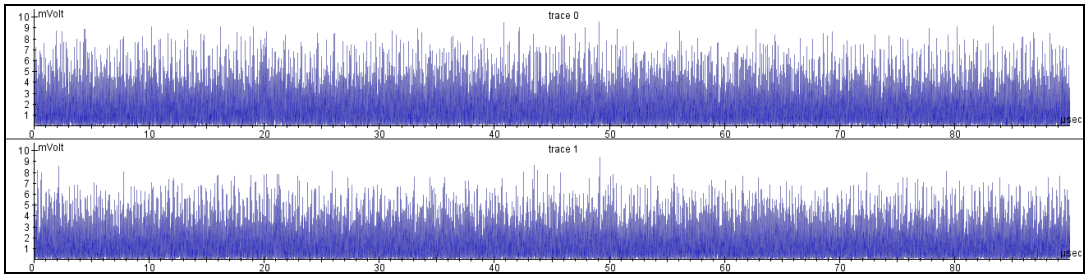


Fig. 13 The absolute value of two EM traces

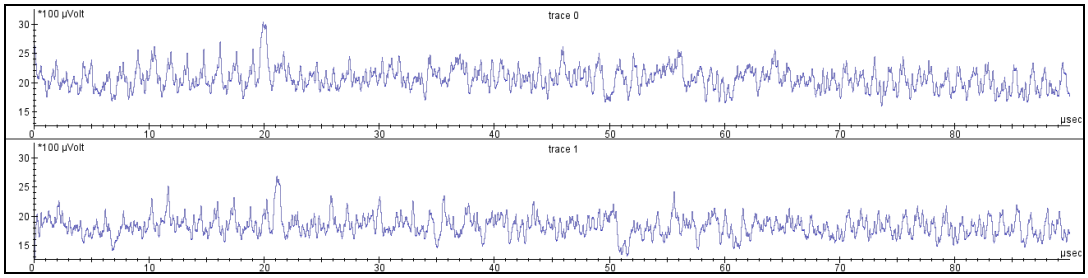


Fig. 14 Traces obtained by filtering the absolute value of the EM signal

4.4 Resampling

Resampling of EM or power signal traces compresses data and increases the speed of the analysis process. A robust and fast method to resample power signals is to average all measured sample within one clock cycle of the process of interest. This method should not be applied directly to EM signals because these signals contain approximately equal positive and negative peaks within one clock cycle, resulting to a low average. This characteristic is a result of the absence of low frequency components in the EM signal. However, by calculating the absolute value of the sample data both peaks will be positive and similar resampling techniques can be used as for power analysis. Figures 15 to 17 show two EM

traces, the absolute value of these traces and the resampled traces. The resamples traces in figure 17 are suitable to determine correlation between measured data and crypto data.

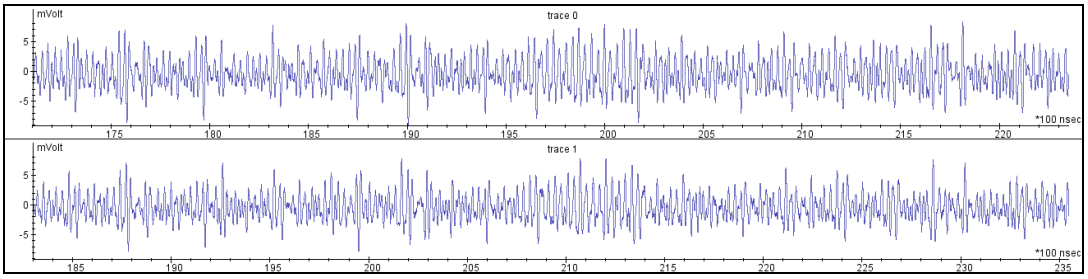


Fig. 15 Two unprocessed aligned EM signal traces

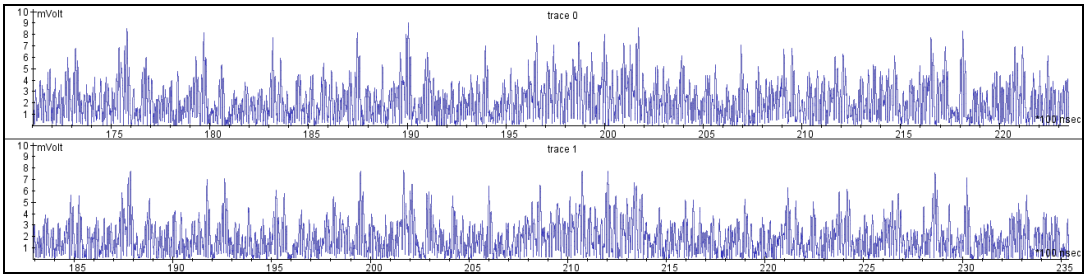


Fig. 16 Absolute value of aligned EM signal traces

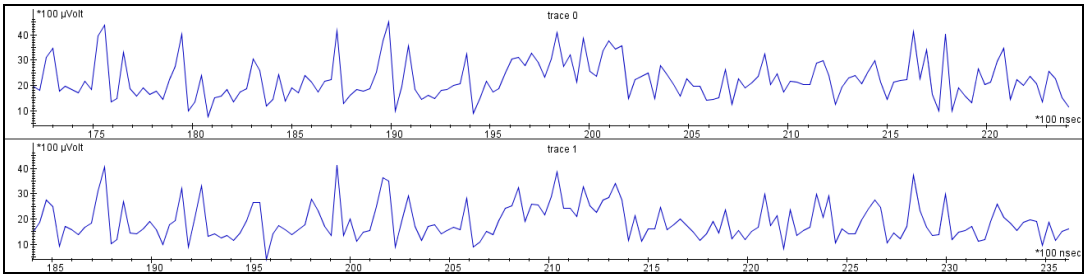


Fig. 17 Absolute value of EM signal traces resampled

5 Experiments

The above described analysis method is applied to the signals obtained from two targets using two types of probes. We selected two targets that also allow power analysis, because it is relatively simple to tap the power and there are no countermeasures against power analysis implemented on these targets. Please note that for these types of targets power analysis is usually selected instead of EMA. However, we made this target selection to be able to make a comparison between power analysis and EMA analysis. Both targets implement the DES algorithm in hardware and allow a fast repetition of the cryptographic

process. The amount of traces needed for these experiments could easily be acquired within one hour, using a side channel test tool and a standard oscilloscope.

5.1 Target of evaluation

The mini board EVAL-USB-64 C from Bostonandroid [6] is used as a first target see figure 18. The board is powered by 3V battery (2 x AAA). The microcontroller ATXmega64A3 on the board includes DES Crypto Engine running on a 32MHz clock.

Fig. 18 Mini board EVAL-USB-64 C from Bostonandroid.

We used the smart card BasicCard ZC6.5 [7] as a second target.

5.2 Probes

We use three probes for the experiments:

- Our B-field probe [5] with symmetrical coil, differential amplifier and magnetic shield

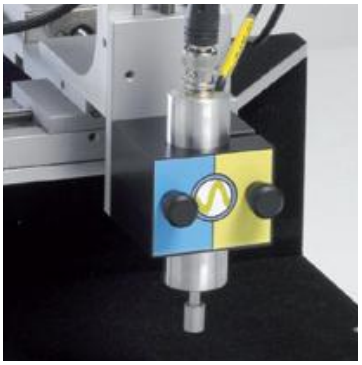


Fig. 19 Riscure HS probe with XYZ stage and magnetic shield.

- H-field probe [3] which was recommended to us with HD24248 amplifier [4]

Fig. 20 Morita Tech MT-545 probe (without amplifier).

- Current probe [5] to measure the current flowing into the power pin. The current probe uses a transformer as sensor. The chip current flows through the primary windings. The voltage from the secondary windings is amplified.

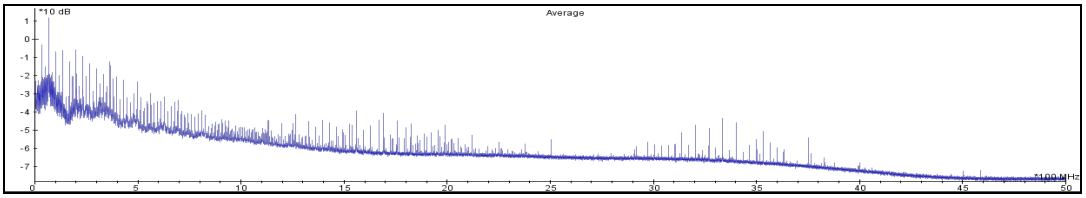
Fig. 21 Current probe

5.3 Measurement results

5.3.1 Embedded processor

Figure 22 shows the frequency spectra measured by the B-, H- and current probe. The spectrum of the current probe shows that the power signal does mainly contain low frequency components. The spectrum of the H-probe is almost flat compared to the B-probe but much weaker.

Figure 23 shows the detailed time signal measured by the B-, H- and current probe. The time signal of the H-field probe is weaker.



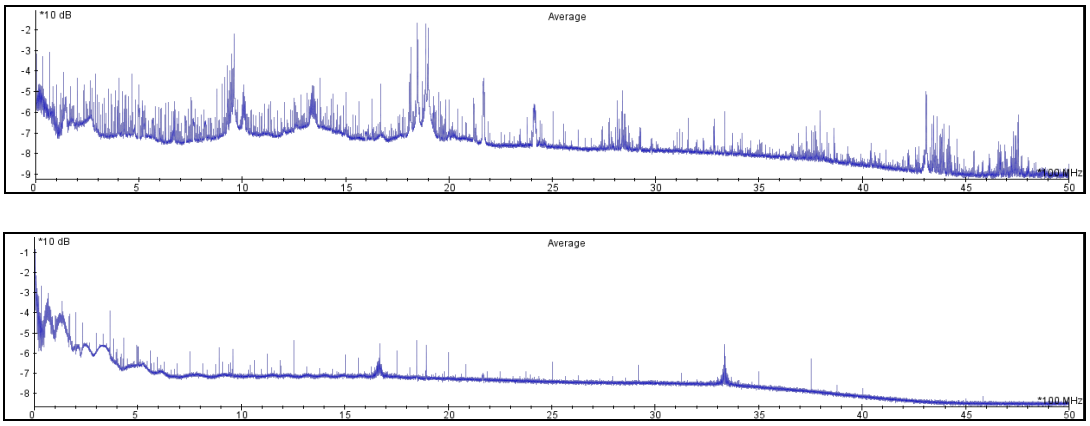


Fig. 22 From top to bottom: spectra of B-probe, H-probe and current probe

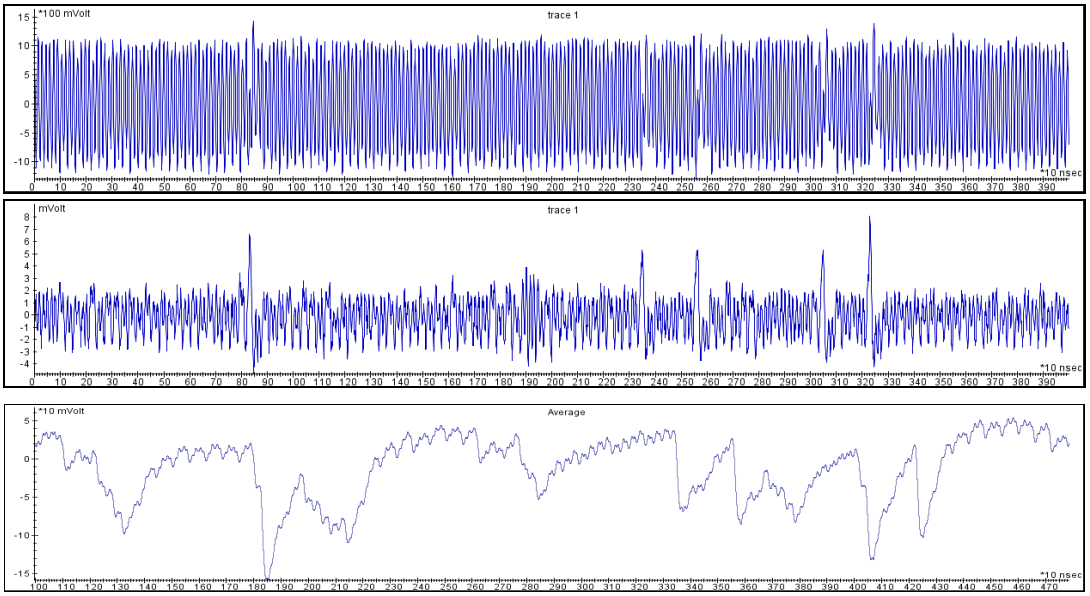


Fig. 23 From top to bottom: signal from B-, H- and current probe with 90 MHz low pass filter

5.3.2 Smart card

Similar analysis as for the embedded processor is performed for the smart card with similar results, see figures 24 and 25, and Table 1.

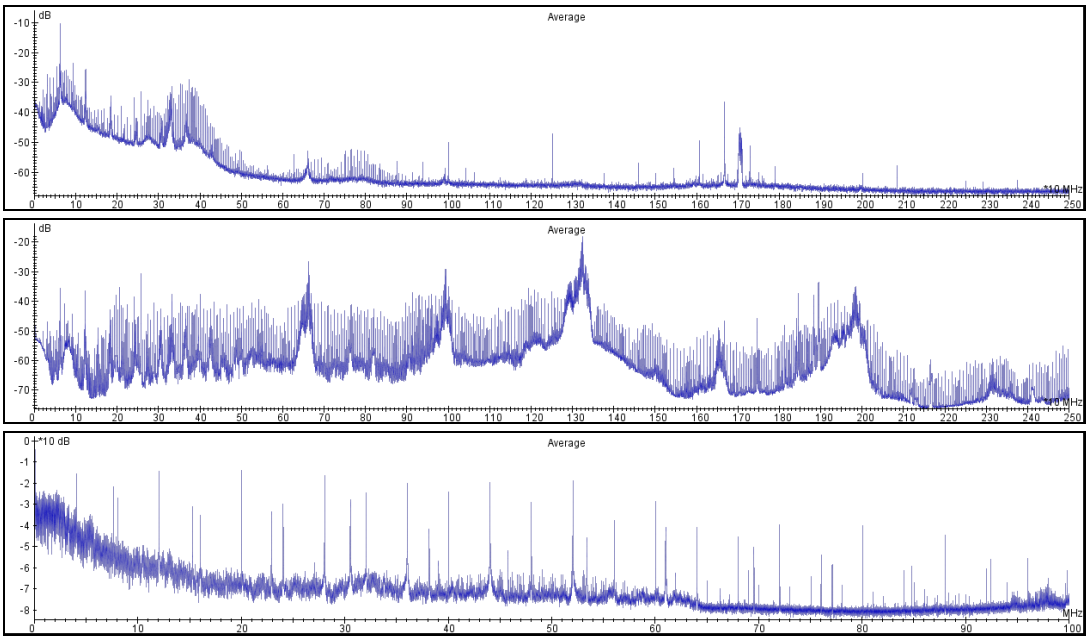


Fig. 24 From top to bottom: spectra of B-probe, H-probe and current probe (different frequency scale)

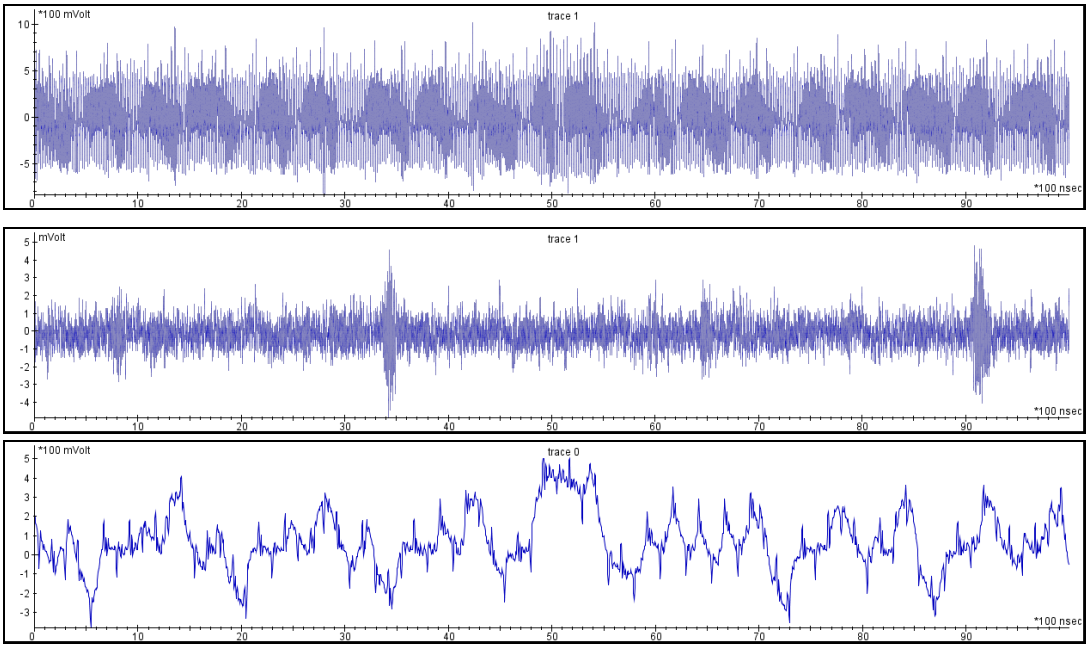


Fig. 25 From top to bottom: signal from B-, H- and current probe with 90 MHz low pass filter

5.3.3 Number of measurements for key retrieval

Table 1 gives the average required number of traces to retrieve the DES round key. Power analysis with the current probe reveals the key first, followed by the B-probe and H-probe. This is explained by a smaller relative contribution of the amplifier noise because the transformer signal of the current probes exceeds the sensor signal from the B-field probe which exceeds the H-field probe.

Table 1. Required number of traces to retrieve DES round key from embedded processor

Target	Current probe	B-probe	H-probe
Embedded board	1200	6675	10000
Smart card	3333	11350	> 50000

6 Conclusions

We studied the application of EMA for testing the resistance of embedded systems and smart cards against side channel analysis, and found that this may be beneficial when the power signal is hard to tap, when the target device implements countermeasures against power analysis or when other processes on the chip add noise to the power signal. In other cases, power analysis may have preference because it needs fewer measurements.

We investigated two basic designs of EM probe: B- and H-probes. The H-probe provides a flat frequency range and a linear relationship between current and output signal. The B-probe generates a large sensor signal, resulting in a higher signal to noise ratio. The experiments indicate the B-probe as best choice for EMA because the generated EM emanation is usually weak.

EM analysis methods differ from power analysis in the way signals are filtered and aligned, but these methods are not much harder to implement.

We conclude that attacking unprotected devices with EMA is straightforward, and that these can be broken in less than an hour with EMA.

7 References

[1] 'Matching shielded loops for cryptographic analysis' W. Aerts, E. De Mulder, B. Preneel, G.A.E. Vandenbosch, and I. Verbauwhede, Proceedings 'EuCAP 2006', Nice, France, 6–10 November 2006

[2] 'Electromagnetic Analysis: Concrete Results' Karine Gandol, Christophe Mourtel, and Francis Olivier, CHES 2001, vol. 2162 of Lecture Notes in Computer Science, pp. 251 Springer-Verlag, 2001.

[3] http://www.morita-tech.co.jp/catalogs/MW7400+MT545%20TD.pdf

[4] http://www.rfcomp.com/download/product_specs/low_noise/HD24248specs.pdf

[5] www.riscure.com

[6] http://www.bostonandroid.com/EVAL-USB-Lite.html.

[7] http://www.basiccard.com/