Horizontal DEMA Attack as the Criterion to Select the Best Suitable EM Probe

Christian Wittke[1], Ievgen Kabin[1], Dan Klann[1], Zoya Dyka[1], Anton Datsuk[1]
and Peter Langendoerfer[1]

[1] IHP – Leibniz-Institut für innovative Mikroelektronik, Germany.

{wittke, kabin, klann, dyka, datsuk, langendoerfer}@ihp-
microelectronics.com

Abstract. Implementing cryptographic algorithms in a tamper resistant way is an extremely complex task as the algorithm used and the target platform have a significant impact on the potential leakage of the implementation. In addition the quality of the tools used for the attacks is of importance. In order to evaluate the resistance of a certain design against electromagnetic emanation attacks – as a highly relevant type of attacks – we discuss the quality of different electromagnetic (EM) probes as attack tools. In this paper we propose to use the results of horizontal attacks for comparison of measurement setup and for determining the best suitable instruments for measurements. We performed horizontal differential electromagnetic analysis (DEMA) attacks against our ECC design that is an implementation of the Montgomery *kP* algorithm for the NIST elliptic curve *B-233*. We experimented with 7 different EM probes under same conditions: attacked FPGA, design, inputs, measurement point and measurement equipment were the same, excepting EM probes. The used EM probe influences the success rate of performed attack significantly. We used this fact for the comparison of probes and for determining the best suitable one.

Keywords: Side channel analysis, horizontal differential electromagnetic analysis attack (DEMA), electromagnetic (EM) probe, difference of the mean test.

1 Introduction

Side channel analysis (SCA) attacks are a serious threat for implementations of cryptographic algorithms. In order to prevent potential attacks from being successful designers need to aim at zero information leakage. Whether or not this aim was achieved needs to be investigated before such an implementation is released. This means that the cryptographic implementations need to be analysed by running suitable attacks. In order to ensure the validity of the result these attacks need to be as sophisticated as possible while using the best attack tools such as measurement equipment. As there is a plethora of attacks the designer needs to focus on some attacks as a starting point. Power and

electromagnetic measurements are used most often to attack cryptographic implementations. This is due to the fact that power analysis (PA) and electromagnetic analysis (EMA) attacks are non-destructive, pretty well understood and in most cases sufficient to extract the keys successfully. This is also the reason why we focus on EMA attack in this paper.

A reasonable means to determine the most powerful attacks (idea, equipment, etc.) is to investigate current publications. But in these papers the focus is normally on the description of the main idea and showing that at least a part of the key was extracted successfully. In more clear words the impact of proper equipment and measurement point are ignored or may be not discussed due to page limitations. The EM probes used for measurements in Heyszl et al. [1], Sauvage et al. [2], Peeters et al. [3] and de Beer et al. [4], are either industrial or self-made but no details are given. But the EM probes have different parameters such as diameter, number of coils, amplifiers, etc. that influence the measurement results and by that also the success rate of an attack significantly. Selecting the measurement equipment, for example "the best suitable" EM probe, is one of the most important preparation steps of EMA attacks.

In this paper we propose to use horizontal DEMA attacks as a fast and low-cost method for selecting the best suitable EM probe. We measured EM traces for the analysis with 7 different EM probes. All other conditions were the same: the rest of measurement equipment, the attacked design, the data processed while EM traces were captured, etc. So, on the one hand it provides a solid basis for selecting an EM probe based on the results discussed here and on the other hand it provides kind of a blueprint how to compare EM probes before selecting one as attack tool in the design phase. To the best of our knowledge this paper is the first comprehensive comparison of probes that enables selecting the best suitable probe.

The rest of the paper is organized as follows. Section 2 summarizes the fundamentals of electromagnetic radiation in terms of side channel analysis. Section 3 presents the device under attack, the measurement setup, including all investigated probes. Section 4 describes the details of the investigated ECC design followed by the description of our performed horizontal DEMA attack in section 5. Section 6 shows the comparison results of all 7 EM probes using horizontal DEMA. The paper finishes with short conclusions and future work.

2   Measuring electromagnetic radiation

The basic assumption of side channel analysis attacks is that the current through a cryptographic chip depends on the processed inputs and on the used private key. Thus, the current through a cryptographic device can be analyzed to extract the key (Power Analysis attacks). Because the changes of the current through a wire cause the changes of its magnetic field, the magnetic field of the current depends also on the processed inputs and private key and can therefore be analyzed to extract the key (Electromagnetic Analysis attacks). Important is, that in this case not the magnetic field but the rate of its changes will be measured using coils. Nevertheless, the result of the measurements depends extremely on the size, position and orientation of the coil. In this section we

explain how the placement and orientation of electromagnetic (EM) probes influence the measurement results. We explain it on an example of the EM field of a single wire with current. We made our measurements on a single wire on the PCB (see section 3) to experimentally illustrate the theoretical knowledge given in this section and to compare the influence of EM probes on the measurement results.

Let us assume, there is a long, thin and straight wire with direct current I in vacuum (or in air). Then the current I causes a magnetic field that can be characterized using the magnetic induction. The magnetic induction (or flux density) $\vec{B}$ is a vector. The magnitude of the magnetic induction at the distance l from the wire can be calculated using the formula:

$$B = \frac{\mu_0 I}{2\pi l} \tag{1}$$

Where μ_0 is a coefficient called permeability of the vacuum. The direction of the vector $\vec{B}$ can be defined with the right-hand rule. The flux of the magnetic field through a surface depends on its area and orientation to the vector $\vec{B}$. Magnetic flux through a surface with the area S is the sum of the normal component of all vectors $\vec{B}$ through this surface:

$$\Phi = \int_S B_{norm} \, dS \tag{2}$$

If the current through the wire is alternating, its magnetic field varies over time. In a coil with area S a voltage will be induced (Faraday's law)[1]:

$$u(t) = -\frac{d\Phi}{dt} = \frac{d(\int_S B_{norm}(t) \, dS)}{dt} \tag{3}$$

If the coil has n turns, the induced voltage is:

$$u(t) = \sum_{i=1}^{n} u_i(t) \tag{4}$$

Accordingly to formulae (3) and (4) coils with different diameter and number of turns can be used to measure the changes of the magnetic field of a wire with a current: the faster the current changes and the closer the coil is to the wire, the higher the measured voltage is. In addition the orientation of the coil influences the measurement significantly.

Fig. 1 shows some coils at different positions. Coils at positions a) and b) are placed horizontally. Coils at positions c) and d) are placed vertically. The positions and orientation of the probe shown in Fig. 1 b) and d) are not suitable for electromagnetic measurements. The most successful positions and orientations of the coil for measurements are the positions a) and c).

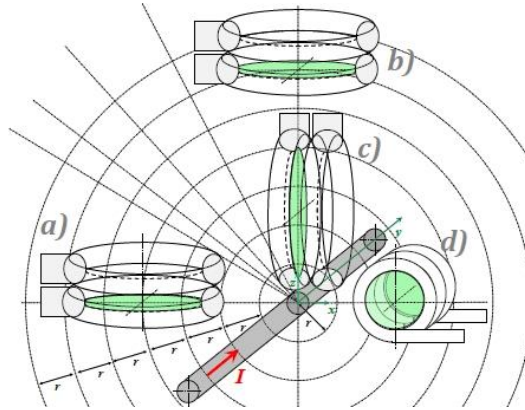[1] Static magnetic fields cannot be detected in this way.

Fig. 1. The magnetic flux through a surface (coil) depends on the distance and on its orientation to the wire

3 Measurement setup

3.1 Device under Attack

The device under attack (DUA) is a Xilinx Spartan-6 FPGA. The board with the Spartan-6 was designed at IHP and is shown in Fig. 2. The FPGA is placed on the front side of the board (Fig. 2 on the left) and most components are placed on the backside (Fig. 2 on the right). This design improves the measurements and ensures that all EM probes can reach any measurement point on the FPGA board, without being harmed.
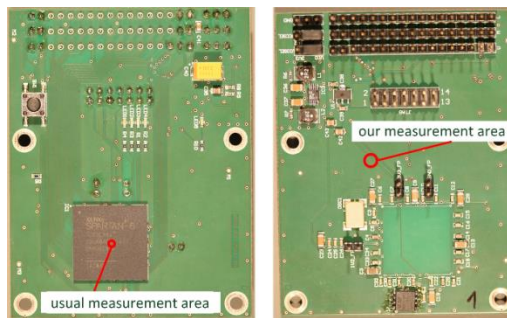

Fig. 2. Front and back side of the attacked Spartan-6 FPGA Board

Fig. 2 shows two measurement areas. The first one on the left in Fig. 2 is over the die. This is the usual area for measuring the EM field. The second measurement area in Fig. 2 on the right is over a long power supply interconnect on the PCB. The board has

several GPIOs to control the FPGA, e. g. start elliptic curve point multiplication and provide input data.

We decided to do the measurement on the PCB wire due to the following reasons: the electromagnetic field that influences the probe should be the same for all probes, i.e. the source radiation of the EM field should be the same and there should be only one possible EM source, e.g. a single wire as described in the theory part in section 2. Measurements over the integrated circuit are influenced significantly by different parts of the circuit, due to various probe dimensions.

The horizontal and vertical probes in our experiments were placed in their optimal orientation and at the most suitable position to the interconnect as described in section 2. The horizontal probes were placed at the edge of the interconnect, i.e. similar to the position *a*) in Fig. 1. The vertical probes were placed above the middle of the interconnect, i.e. similar to the position *c*) in Fig. 1.

3.2 Measurement equipment

We captured the traces using a LeCroy Waverunner 610 Zi oscilloscope with a sampling rate of 2.5 GS/s. This results in 625 measurement points per clock cycle at 4 MHz clock frequency. The distance between the EM probe and the surface of the DUA is as small as possible for the commercial probes, but selected with caution to avoid contact to the PCB surface and damaging the probe. The whole measurement setup is shown in Fig. 3.
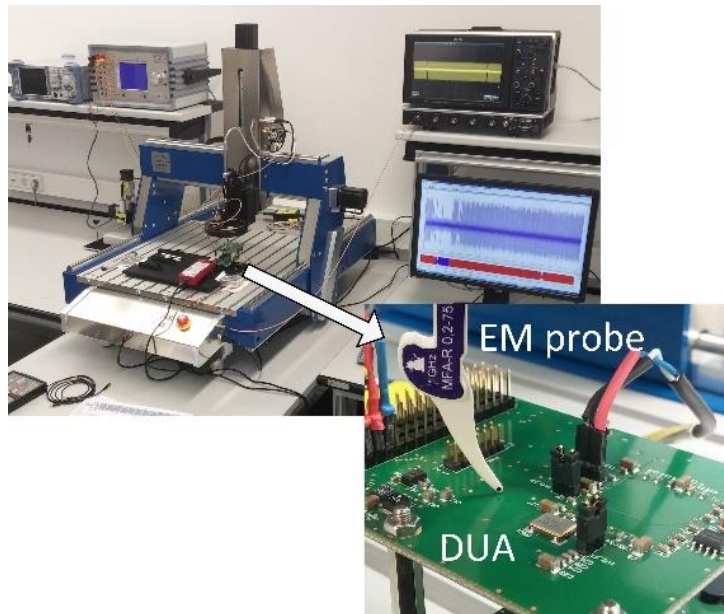

Fig. 3. Measurement setup: DUA, EM probe, oscilloscope, power supply

3.3 Used EM probes

In this section different EM probes from various manufacturers and also our self-made probe were examined. The commercial probes are from Riscure [5] and Langer [6]. The seven examined probes have different geometries and characteristics. The two Langer ICR probes and the Langer MFA-R-75 probe have an internal preamplifier. The two Riscure probes work using their built-in amplifier. We decided to use also the passive Langer LF-B3 probe and our self-made probe with an extra amplifier from Riscure [8]. All the probes and their specifications are listed in Table 1. The table summarizes all available specifications clearly and allows comparing the probes. The specifications were gathered from the manufacturers and data sheets. In addition to the technical data there are photos and zoomed in pictures given for the Langer ICR probes.

Table 1. Overview of used EM probes.

Probe	Picture	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Riscure low sensitivity [5]		Cu[b]	1.128 mm[c] 1.596 mm[d]	13[b]	-	-	h	yes	yes
Riscure high sensitivity [5]		Cu[b]	1.128 mm[c] 1.596 mm[d]	13[b]	-	-	h	yes	yes
self-made		Cu	2 mm	9	-	-	h/v	no	no
Langer ICR HH 150-27 [9]		Cu	150 µm	-	1.5 MHz - 6 GHz	100 µm	h	yes	yes
Langer ICR HV 150-27 [9]		Cu	150 µm	-	1.5 MHz - 6 GHz	80 µm	v	yes	yes
Langer LF-B3 [10]		Cu	1.5 mm	-	100 kHz - 50 MHz	2 mm	h	no	no
Langer MFA-R-75 [11]		Cu	150 µm	-	1 MHz - 1 GHz	300 µm	v/h[e]	no	yes

The header spans: **Specification[a]** over columns (1)–(8).

"-" not specified
[a](1) material, (2) diameter, (3) number of turns, (4) frequency range, (5) resolution, (6) orientation: horizontal (h), vertical (v) or both (h/v), (7) shielding, (8) integrated amplifier
[b] by visual inspection
[c] inner diameter calculated from the inner area of the coil, given in data sheet
[d] outer diameter calculated from the outer area of the coil, given in data sheet
[e] under certain circumstances, i.e. layout of the DUA

4 Implementation details of investigated ECC designs

The most time and energy consuming part of the cryptographic operations using EC is the scalar point multiplication, denoted as *kP*. In the *kP* operation $P=(x,y)$ is a point of the EC with affine coordinates *x*, *y* and *k* is a large binary number. The encryption algorithm contains two *kP* operations and only one *kP* operation should be calculated for the decryption of the obtained message. The calculation of *kP* takes more than 99% of the time and energy needed for a decryption.

If the chip performs decryption of received messages, *k* is the private key of the owner of the chip. If the attacker has physical access to the working chip, the power consumption and electromagnetic radiation of the *kP* operation can be measured, saved and analysed in order to extract the private key.

For our experiments reported here we used an hardware accelerator for the *kP* operation for EC *B-233* [7]. The *kP* design was implemented based on the Montgomery *kP* algorithm in projective Lopez-Dahab coordinates [12]. The *kP* operation is realized as a sequence of only three field operations: addition, squaring and multiplication of long binary numbers that represent the elements of an extended binary Galois field $GF(2^l)$, in our case $GF(2^{233})$ with the irreducible polynomial $f(t)=t^{233}+t^{74}+1$ [7]. 6 multiplications, 5 squarings and 3 additions of elements of $GF(2^{233})$ are needed to process a single bit of the key *k*. The ECC design consists of a controller, registers, an arithmetic-logic unit that performs additions and squarings and a multiplier that calculates the field product. Our field multiplier takes 9 clock cycles for calculating a field product of 233 bit long operands. All register operations and field additions and squarings are performed in parallel to the field multiplication which increases the inherent resistance of our ECC design against SCA attacks. The controller manages the sequence of field operations and registers operations.

The processing of each key bit takes 54 clock cycles. The sequence of the performed operations doesn`t depend on the processed key bit value. The shape of the power profile that corresponds to processing of a single key bit looks similar for each processed key bit value. Due to this fact, the investigated design is resistant against SPA and SEMA attacks i.e. it is not possible to reveal the key just by visual inspection. This can be seen in Fig. 4 displaying beginning of a power trace (PT) and in Fig. 5 showing the beginning of the corresponding electromagnetic trace (EMT).

The PT and EMT were captured in parallel during an execution of a decryption, i.e. of a *kP* operation. The PT was measured using the Riscure Current probe [8] and the EMT was measured using a Riscure high sensitivity which was placed over the middle of the FPGA, marked in Fig. 2 as "*usual measurement area*". The key cannot be revealed by visual inspection of the traces, neither of the PT nor of the EMT. Even the processing of each single key bit is hard to distinguish.
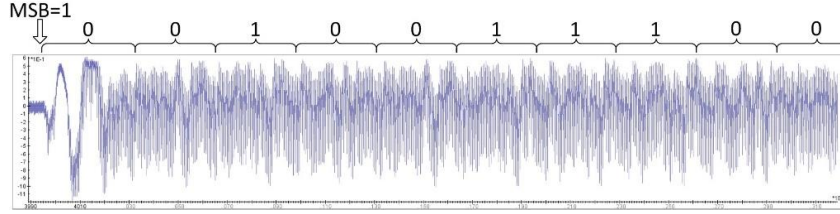
MSB=1   0   0   1   0   0   1   1   1   0   0

Fig. 4. Power trace of our SPA and SEMA resistant implementation of the Montgomery *kP* algorithm measured on Spartan-6 FPGA. The PT was measured using the Riscure current probe [8] and the measurement equipment as described in section 3.2.
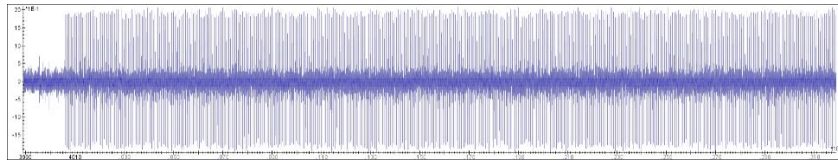

Fig. 5. Electromagnetic trace of our ECC design measured with the Riscure high sensitivity probe which was placed over the middle of the chip. The measurement equipment was used as described in section 3.2.

5   Description of performed DEMA attacks

In our experiments we performed the *kP* operation with the following operands:

- the scalar *k* in hexadecimal:

k=93919255FD4359F4C2B67DEA456EF70A545A9C44D46F7F409F96CB52CC

- the affine coordinates of the EC point *P=(x,y)*:

x=181856ADC1E7DF1378491FA736F2D02E8ACF1B9425EB2B061FF0E9E8246
y=9FED47B796480499CBAA86D8EB39457C49D5BF345A0757E46E2582DE6

5.1   Preparation of the EMT for the horizontal attack

To perform our horizontal DEMA attack we prepared the measured electromagnetic traces in two steps as described in this section.

Step 1: Selecting the part of traces to be analysed.

The part of the trace to be analysed corresponds to the processing of the data in the main loop of the *kP* algorithm. In our experiments the scalar $k=k_{231}...k_0$ is 232 bit long. In the main loop of our implementation of the Montgomery *kP* algorithm the *230* key bits $k_{229}, ... , k_0$ are processed. Thus, the analysed part of EM traces consists of 230 time slots. Each time slot corresponds to the processing of a key bit k_j with $0 \leq j \leq 229$. The processing of a key bit in the main loop takes 54 clock cycles each.

Step 2: Compression of traces

We represented each clock cycle using only one value instead of 625 measured values. We calculated this value as the difference of the maximal and the minimal values measured within the clock cycle.

After the preparation of the EMT described above we have a long part of the trace for analysis. The prepared trace consists of 230 time slots. Each slot consists of only 54 values (one value per clock cycle). Thus, each value of the analysed part of the compressed trace can be represented as v_j^i, where j is the number of the time slot ($0 \leq j \leq 229$) and i is the number of the clock cycle ($1 \leq i \leq 54$) within the time slot.

5.2 Attack details

We performed our horizontal DEMA attack using the *difference of the mean* test applied to the compressed traces as follows:

- Using the 230 time slots we calculated the arithmetical mean of all values with the same number i and different number j:

$$\overline{v^i} = \frac{1}{230} \sum_{j=0}^{229} v_j^i \tag{5}$$

  Thus, the 54 average values $\overline{v^i}$ define the *mean* electromagnetic profile of the slot.

- For each i we obtained one key candidate $k_{candidate}^{\ i}$ using the following assumption: the jth bit of the key candidate is 1 if in the slot with number j the value with number i – i.e. the value v_j^i – is smaller than or equal to the average value $\overline{v^i}$. Else the jth bit of the ith key candidate is 0:

$$k_{candidate\,j}^{\quad i} = \begin{cases} 1, if\ v_j^i \leq \overline{v^i} \\ 0, if\ v_j^i > \overline{v^i} \end{cases} \tag{6}$$

5.3 Evaluation of the success of the attack

To evaluate the success of the attack we compared all extracted key candidates with the scalar k that was really processed. For each key candidate we calculated its relative correctness as follows:

$$\delta = \frac{\#correct\_extracted\_bits\ (k_{candidate\,j}^{\quad i})}{230} \cdot 100\% \tag{7}$$

Our assumption (6) can be false and in that case the opposite assumption would be true. Thus, bitwise inverting key candidates with a correctness of less than 50% will result in in a relative correctness of those key candidates of more than 50%.

6 Comparison of different probes based on attack results

For the comparison of the different 7 EM probes we measured 8 EM traces under same conditions (DUA, design, inputs, measurement point and measurement equipment): two traces for the self-made EM probe and one EMT for all other probes. We performed the horizontal DEMA attack as described in section 5 for each trace and evaluated the success of the attack using the relative correctness of the key extraction corresponding to formula (8).

The relative correctness of the extracted keys can be represented graphically to visualize the success of the attack and to compare the attack results. We use the success of the attack as the criterion for the EM probe comparison. Fig. 6 - Fig. 9 show the results of the attacks for the different EM probes used in our experiments.

The first probes we experimented with are the Riscure low and high sensitivity probes. Both probes have an integrated amplifier a horizontal coil and were placed in the *xy*-plane (see Fig. 1 position *a*) for the measurements. The difference in the probes is only their amplifier (see Table 1). The black graph in Fig. 6 shows the key correctness of all key candidates for the horizontal Riscure low sensitivity probe. 18 key candidates show around 70 - 80% correctness, except the 1st and 53rd candidates that have a correctness of 85%. The attack using EMT measured with the Riscure high sensitivity probe was less successful (see yellow graph in Fig. 6). The peaks of key correctness appear for the same key candidates (index numbers j), but with lower correctness.
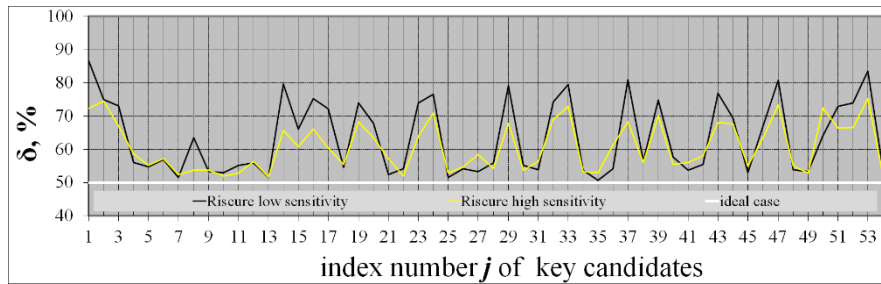

Fig. 6. Results of horizontal DEMA attack using EMTs measured with the Riscure low sensitivity (black graph) and the Riscure high sensitivity probe (yellow graph). Both probes are horizontal probes and are identical with the exception of the integrated amplifier.
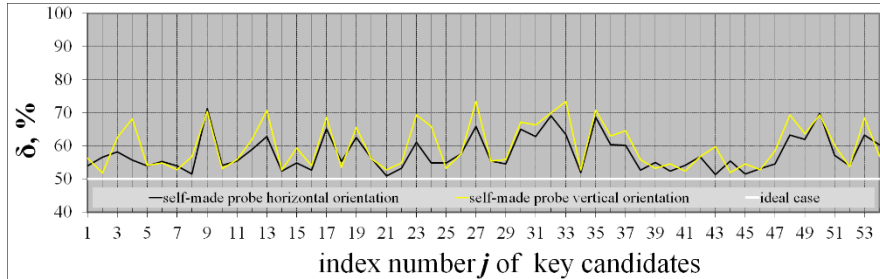
Fig. 7. Results of horizontal DEMA attack using EMTs measured with our self-made probe in horizontal orientation (black graph) and vertical orientation (yellow graph). The probe was used with a Riscure amplifier.

The next EM probe experimented with is our self-made probe with an amplifier from Riscure. We used the probe in horizontal and vertical orientation, according to position *a*) and position *c*) (see Fig. 1), i.e. we measured two EMTs using the self-made probe. Fig. 7 shows the results of our horizontal DEMA attack for both traces. The maximal correctness is about 70 % for both probes. The attack using the measurements done in vertical orientation shows better results in the sense that more key candidates reach a correctness of 70% (see yellow graph).

Fig. 8 shows the results of the attack for the Langer horizontal micro-probe ICR HH 150-27 and for the Langer vertical micro-probe ICR HV 150-27. The correctness of most of the key candidates is between 50 and 60% that is close to the ideal case of 50%. This is not due to the design, but due to the probes.
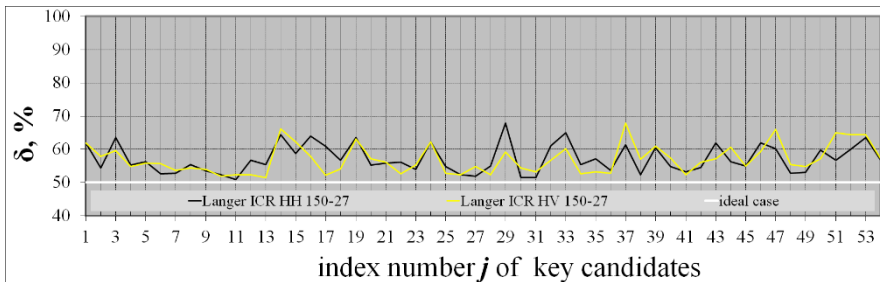

Fig. 8. Results of our horizontal DEMA attack using EMTs measured with the Langer horizontal probe ICR HH 150-27 (black graph) and the Langer vertical probe ICR HV 150-27 (yellow graph) with the same integrated amplifier. Probes differ in the orientation of the coil only.

The next examined probe is the LF-B3 probe from Langer. This is a probe without amplifier and we used it with the amplifier from Riscure. The probe was used in the measurement as shown in Fig. 1 position *a*), i.e. horizontally oriented. The black graph in Fig. 9 shows 5 key candidates with a correctness of more than 90%.
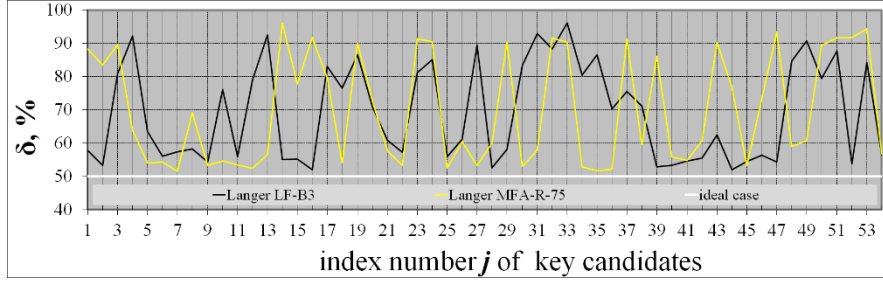
Fig. 9. Results of horizontal DEMA attack using EMTs measured with the Langer MFA-R-75 vertical probe (yellow graph) and with Langer LF-B3 probe (black graph).

The results of the attack using the EMT measured with the Langer MFA-R-75 probe are also shown in Fig. 9. The probe has an internal pre-amplifier and is a vertical probe, i.e. the probe was used according to position *c*) in Fig. 1. The measurements recorded with this probe lead to the best attack results under the given measurement conditions, Fig. 9 shows 16 peaks with a correctness of more than 90%.

Table 2 summarizes the attack results for all probes. The number of key candidates revealed with a correctness of 70..80%, 80..90% or 90..100% is shown for each evaluated EM probe.

Table 2. Number of key candidates revealed with the correctness of 70..80%, 80..90% or 90..100% per investigated EM probe.

Probe	# key candidates with 100%> $\delta{\geq}90\%$	#key candidates with 90%> $\delta{\geq}80\%$	# key candidates with 80%> $\delta{\geq}70\%$
Langer MFA-R-75	14	4	2
Langer LF-B3	5	13	6
Riscure low sensitivity	-	4	15
Riscure high sensitivity	-	-	7
Self-made vertical	-	-	6
Self-made horizontal	-	-	1
Langer ICR HH 150-27	-	-	-
Langer ICR HV 150-27	-	-	-

Selecting the best suitable probe for EM attacks using Table 2 is quite simple. The probes are ordered from best to worst top down, easily being verified by the number of key candidates revealed with highest level of correctness.

7   Conclusion

In this paper introduced the concept of a horizontal differential electromagnetic attack as a powerful means to extract keys from cryptographic devices executing asymmetric

cryptographic operations. Note that our focus here was not on introducing just a new attack but at providing a means to evaluate and compare the suitability of different electromagnetic probes when used for assessing the resistance of cryptographic implementations against side channel attacks. Our focus on electromagnetic emanation analysis attacks was motivated by the following facts. EMA attacks are used quite often and do not require modifications of the device under attack. So, this type of attacks needs to be taken serious.

In order to illustrate and to highlight the effect of the EM probe on the result of the assessment of a certain implementation, we run the same horizontal DEMA attack against traces recorded from the same operation on the same FPGA but with seven different probes. In order to be able to compare the EM probes we did an assessment on the key extraction quality. To do so we compared the key candidates we extracted using the difference of the mean test from the measurements with the actually processed key. The percentage of correctly revealed key bits gives a very good indication about the probe best suited for an EMA attack. In addition the number of key candidates that was revealed with a certain correctness can be used for the assessment of the probes.

The best suited probe allowed to reveal 14 key candidates with a correctness of more than 90 per cent whereas the least suited probe did not allow to get a single key candidate with a correctness of more than 70 per cent. So, our experiments clearly show that selecting the wrong probe for tests may lead to a wrong impression of good resistance.

References

1. J. Heyszl et al., "Localized Electromagnetic Analysis of Cryptographic Implementations", in Topics in Cryptology CT-RSA, pp 231–244, 2012.
2. L. Sauvage et al., "Practical results of EM cartography on a FPGA-based RSA hardware implementation", in IEEE International Symposium on Electromagnetic Compatibility, pp 768–772, 2011.
3. E. Peeters et al., "Practical Electro-Magnetic Analysis", in Integration, the VLSI Journal - Special issue: Embedded cryptographic hardware, pp 52–60, 2007.
4. F. de Beer et al., "Power and electromagnetic analysis: improved model, consequences and comparisons", in Non-Invasive Attack Testing Workshop NIAT, 2011.
5. Riscure Inspector, "EM Probe Station", 2015, https://www.riscure.com/ security-tools/hardware/em-probe-station
6. LANGER EMV-Technik GmbH, "ICR Nahfeldmikrosonden", 2015, http://www.langer-emv.de/produkt/e/icr-nahfeldmikrosonden/
7. NIST, "Digital Signature Standard (DSS)", FIPS PUB 186-4, 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
8. Riscure Inspector, "Current Probe", Datasheet, 2011, https://www.riscure.com/benzine/documents/CurrentProbe.pdf
9. LANGER EMV-Technik GmbH, "Technical parameters", http: //www.langer-emv.com/produkte/ic-messtechnik/feldmessung-ueber-ic/ icr-nahfeldmikrosonden-kopie-1/technische-parameter/
10. LANGER EMV-Technik GmbH, "LF, 100 kHz - 50 MHz", http://www. langer-emv.de/produkt/e/lf-100-khz-50-mhz/
11. LANGER EMV-Technik GmbH, "MFA02 micro probe set", http://www. langer-emv.com/produkte/stoeraussendung/nahfeldsonden/set-mfa02/

12. D. Hankerson, J. Lopez, and A. Menezes: *Software implementation of elliptic curve cryptography over binary fields.* Proc. of CHES 2000, LNCS Vol. 1965, Springer, 2000.