Electromagnetic Analysis Attack on a FPGA Implementation of an Elliptic Curve Cryptosystem

Abstract— **This paper presents simple (SEMA) and differential (DEMA) electromagnetic analysis attacks on an FPGA implementation of an elliptic curve processor. Elliptic curve cryptography is a public key cryptosystem that is becoming increasingly popular. Implementations of cryptographic algorithms should not only be fast, compact and power efficient, but they should also resist side channel attacks. One of the side channels is the electromagnetic radiation out of an integrated circuit. Hence it is very important to assess the vulnerability of implementations of cryptosystems against these attacks. A SEMA attack on an unprotected implementation can find all the key bits with only one measurement. We also describe a DEMA attack on the improved implementation and demonstrate that a correlation analysis requires 8000 measurements to find the key bits.**

Index Terms— **Elliptic Curve Cryptosystems, side channel attacks, SEMA, DEMA**

I. INTRODUCTION

Keeping information secret and authentic is a very old concern, but the exponential growth of technology exacerbates the need for secure communication. The ubiquitous use of computers and other electronic communication systems increases the need for securing the information kept in this devices or sent between them. Cryptographic algorithms and protocols are essential in protecting the confidentiality and authentication of data; they replace the problem of protecting information by protecting short cryptographic keys.

Ironically, the very same technology which forms the basis for the higher demand in security has a few annoying side effects. Kocher introduced the use of side channels to break a cryptosystem [1], [2]. He suggested to derive information on secret keys by measuring the execution time and the power consumption of implementations of cryptosystems. With this idea, cryptanalysis no longer focuses exclusively on the mathematical aspects but also evaluates weaknesses of implementations. Electronic circuits need some time to produce the result and need a certain amount of energy to switch states. The three main physical properties of cryptographic modules can be exploited in side channel attacks: power consumption, timing and electromagnetic radiation. Others such as sound and heat are currently being explored but seem less promising.

Elliptic Curve Cryptography (ECC) was proposed independently by Miller [3] and Koblitz [4] in the 1980s. Since then a considerable amount of research has been performed on secure and efficient ECC implementations.

This article reports on the first implementation of an electromagnetic analysis (EMA) attack on a hardware implementation of an elliptic curve (EC) processor with a key length of 160 bits [5]. Earlier work (discussed in Section II) is either theoretical or presents attacks on software implementations for 8-bit smart cards. The main difference between our implementation of an EC processor and these software implementations is that in our hardware all operations are done in parallel. Hence the number of bit transitions during every clock cycle can be up to 160, compared to 8 for a smart card. This implies that predictions of the transitions are much harder. In order to detect the effect of any bit changes we have to increase the number of measurements by a factor of 20 or more.

This paper is organized as follows: In Section II we discuss the previous work on EMA attacks, section III summarizes the mathematical background needed to understand the proposed work, in Section IV we describe our measurement setup, finally in Section V and VI we present the SEMA and DEMA attacks results on the EC processor. We conclude the paper and discuss further work in Sect. VII.

II. PREVIOUS WORK

It is well known that the US government has been aware of electromagnetic leakage since the 1950s. The resulting standards are called TEMPEST; partially declassified documents can be found in [11]. The first published papers are work of Quisquater and Samyde [12] and the Gemplus team [13]. Quisquater and Samyde showed that it is possible to measure the electromagnetic radiation from a smart card. Their measurement setup consisted of a sensor which was a simple flat coil, a spectrum analyzer or an oscilloscope and a Faraday cage. Quisquater also introduced the terms Simple EMA (SEMA) and Differential EMA (DEMA). The work of Gemplus deals with experiments on three algorithms: DES, RSA and COMP-128. They observed the feasibility of EMA attacks and compared them with power analysis attacks in favor of the first. Namely, EM radiation can also exploit local information and, although more noisy, the measurements can be performed from a distance. This fact broadens the range of targets to which side channel attacks can be applied. Of concern are not only smart cards and similar tokens but also SSL accelerators and many other cryptographic devices.

According to Agrawal *et al.* there are two types of radiations: intentional and unintentional [14], [15]. The first type results from direct current flows. The second type is caused by various couplings, modulations (AM and FM), etc. The two papers mentioned above deal exclusively with intentional radiations. To the contrary, the real advantage over other side channel attacks lies in exploring unintentional radiations [14], [15]. More precisely, EM leakage consists of multiple channels. Therefore, compromising information can be available even for DPA resistant devices which can be detached from the measurement equipment.

More theoretical considerations related to all side channel attacks, but mainly induced by work on EMA, are also given by Chari *et al.* in [16]. They discussed so-called template attacks in which the attacker uses a device that is identical to the target device. The only difference is that this replica is programmable which makes it possible to handle the noise in each measurement sample. Unlike previous considerations, which all try to eliminate noise, this approach attempts to model the noise in order to extract more useful information. As an example, they detailed the template attack on RC4 using only one single measurement sample. Other case studies listed include DES and RSA exponentiation. At that moment, template attacks were envisioned as the strongest possible side channel attacks from an information theoretical point of view, but the authors themselves came up with an even stronger approach afterwards. Namely, besides carefully exploring all available EM radiations an attacker can also focus on a combination of two or more side channels. Agrawal *et al.* defined these so-called multi-channel attacks in which the side channels are not necessarily of a different kind [17]. For example, they discussed combined power and EM analysis but also multi-channel DPA attacks. The former uses a CMOS leakage model and the maximum-likelihood principle for performing and analyzing. Agrawal *et al.* showed that it is even more effective than template attacks. Another example of a multi-channel attack is introduced by Walter and Thompson in [18]. They were the first to combine power and timing analysis.

Mangard also showed that near-field EM attacks can be conducted with a simple hand-made coil in [19]. He also demonstrated that measuring the far-field emissions of a smart card connected to a power supply unit also suffices to determine the secret key used in the smart card.

Carlier *et al.* showed that EM side channels from an FPGA implementation of AES can be effectively used by an attacker to retrieve some secret information in [20]. They worked close to the FPGA, which allowed them to get rid of the effects of other computations made at the same time. During DEMA, they measured the effect of one particular byte we want to exploit. They also introduced a new Square EM Attack.

Up to now, most papers on EMA applied similar techniques as PA while apparently much more information is available to be explored. It is likely that future work will also deal with combinations of EMA with other side channel attacks.

III. Mathematical Background

A. Elliptic curves over $GF(p)$

The public key cryptosystem implemented on the FPGA is the elliptic curve cryptosystem. An elliptic curve E is expressed in terms of the Weierstrass equation:

$$y^2 = x^3 + ax + b, \tag{1}$$

where $a, b \in GF(p)$ with $4a^3 + 27b^2 \neq 0 \pmod p$. The inverse of the point $P = (x_1, y_1)$ is $-P = (x_1, -y_1)$. The sum $P + Q$ of the points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ (assume that $P, Q \neq \mathcal{O}$, and $P \neq \pm Q$) is the point $R = (x_3, y_3)$ where:

$$x_3 = \lambda^2 - x_1 - x_2,\ y_3 = (x_1 - x_3)\lambda - y_1,\ \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \tag{2}$$

For $P = Q$, the "doubling" formulae are:

$$x_3 = \lambda^2 - 2x_1,\ \ y_3 = (x_1 - x_3)\lambda - y_1,\ \ \lambda = \frac{3x_1^2 + a}{2y_1}. \tag{3}$$

The point at infinity $\mathcal{O}$ plays a role analogous to that of the number 0 in ordinary addition. Thus, $P + \mathcal{O} = P$ and $P + (-P) = \mathcal{O}$ for all points P. The points on an elliptic curve together with the operation of "addition" form an Abelian group. Then it is straightforward to introduce the point or scalar multiplication as main operation for ECC. This operation can be calculated by using double-and-add algorithm as shown in Algorithm 1. For details see [3], [4], [6].

Algorithm 1. Elliptic Curve Point Multiplication

Require: EC point $P = (x, y)$, integer k, $0 < k < M$, $k = (k_{l-1}, k_{l-2}, \cdots, k_0)_2$, $k_{l-1} = 1$ and M
Ensure: $Q = (x', y') = [k]P$

```
Q ← P
for i from l − 2 downto 0 do
    Q ← 2Q
    if k_i = 1 then
        Q ← Q + P
    end if
end for
```

The goal is to guess the key bits k_i because by finding them, the algorithm is broken.

B. Electromagnetic Analysis Attack

Nowadays, CMOS is by far the most commonly used technology to implement digital integrated circuits. A CMOS-gate consists of a pull-up network with p-MOS transistors and a pull-down network with n-MOS transistors. Those networks are complementary: when the input is stable, only one of the two networks conducts [7]. The most simple logic gate is an inverter; its power consumption is representative for all logic ports and gives a general image of the power consumption in a CMOS circuit. During the functioning of the inverter, 3 types of power consumption can be distinguished. The leakage current, the current that flows from the power source to the ground during the switching from 0 to 1 (short-circuit current) and the current used to charge and discharge the different capacitors in a digital network (dynamic power consumption). The last one causes the biggest power consumption in present designs. Important to note is that these capacitors are necessary to maintain the two different logic levels. In addition, all capacitors for each gate differ, which results in a different power consumption of the different gates according to the data being processed. The sudden current pulse that occurs during the transition of the output of a CMOS gate causes a variation of the electromagnetic field surrounding the chip; this can be monitored for example by inductive probes which are particularly sensitive to the related impulsion. When using a loop antenna, the voltage induced by the current equals:

$$V = -\frac{\mathrm{d}\phi}{\mathrm{d}t} \ \text{ and } \ \phi = \iint \vec{B} \cdot d\vec{A}, \tag{4}$$

where V is the probe's output voltage, ϕ the magnetic flux sensed by probe, t is the time, $\vec{B}$ is the magnetic field and $\vec{A}$ is the area that it penetrates.

Two types of electromagnetic analysis attacks are distinguished. In a *simple electromagnetic analysis* (SEMA) attack, an attacker uses the information from one electromagnetic radiation measurement directly to determine (parts of) the secret key. In a *differential electromagnetic analysis* (DEMA) attack, many measurements are used in order to filter out noise and the key is derived using a statistical analysis. While SEMA exploits the relationship between the executed operations and the electromagnetic radiation, DEMA exploits the relationship between the processed data and the electromagnetic radiation. A SEMA attack is typically used when there is a conditional branch in the algorithm, which results in a different radiation pattern whenever the branch is taken. A DEMA attack uses the property that processing different data needs a distinct amount of power and radiates a different field.

C. Discrete Fourier Transform

We use the discrete Fourier transform (DFT) in order to find the clock frequency in Section VI. Let x be a complex series with N samples of the form $x = x_0, x_1, \ldots, x_{N-1}$ where x_i is a complex number. The series outside the range 0, $N-1$ is extended N-periodic, that is, $x_i = x_{i+N}$ for all i.

The discrete Fourier transform (DFT) of x is denoted as X; it also has N samples. The forward transform is defined as

$$X_n = \frac{1}{N}\sum_{i=0}^{N-1} x_i e^{-jk2\pi n/N} \quad for\, n = 0 \cdots N-1. \tag{5}$$

D. Correlation Analysis

In DEMA, an attacker uses a hypothetical model of the attacked device. The quality of this model is dependent on the knowledge of the attacker. The model is used to predict several values for the electromagnetic radiation of a device.

These predictions are compared to the real, measured electromagnetic radiation of the device. Comparisons are performed by applying statistical methods on the data. Among others, the most popular are the *distance-of-mean test* and the *correlation analysis*. We decided to use the correlation analysis in our attack. For the correlation analysis, the model predicts the amount of side channel leakage for a certain moment of time in the execution. These predictions are correlated to the real electromagnetic radiation. The correlation can be measured using the Pearson correlation coefficient [10]. Let t_i denote the ith measurement data (i.e. the ith trace) and T the set of traces. Let p_i denote the prediction of the model for the ith trace and P the set of such predictions. Then we calculate

$$C(T,P) = \frac{E(T\cdot P) - E(T)\cdot E(P)}{\sqrt{Var(T)\cdot Var(P)}} \quad -1 \le C(T,P) \le 1. \tag{6}$$

In Eq.(6), $E(T)$ denotes the expectation (average) trace of the set of traces T and $Var(T)$ denotes the variance of a set of traces T. T and P are said to be uncorrelated, if $C(T,P)$ equals zero. Otherwise, they are said to be correlated. If their correlation is high, *i.e.* if $C(T,P)$ is close to $+1$ or -1, it is usually assumed that the prediction of the model, and thus the key hypothesis, is correct.

IV. Measurement Setup

Figure 1 shows the most important part of our measurement setup: the VIRTEX FPGA which is under attack. Because the field surrounding the chip is mainly a magnetic field in the near field, a loop antenna is used to pick up the variations of the field.

Our setup consists of essentially two boards [21]. The main board is responsible for interfacing to the PC via the parallel port. It is connected with the XILINX parallel cable in order to program the VIRTEX FPGA and it provides some LEDs, switches and buttons for testing purposes. The daughter board itself just carries the VIRTEX FPGA, it allows to access some pins for triggering and to measure the power consumption of the VIRTEX FPGA in a convenient way.

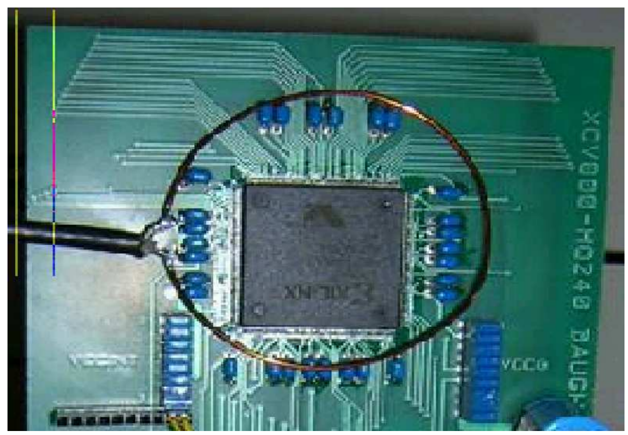

Fig. 1. The measurement setup. The loop antenna is placed parallel with the FPGA.

V. SEMA Attack on an FPGA Implementation of an EC Processor

The EM radiation trace of a 160-bit EC point multiplication is shown in Fig 2 [22]. The SEMA attack is implemented on the EC processor published in [5], [23] which uses Algorithm 1 for EC point multiplication. It can be derived from Fig. 2 that the key used during this measurement is 11001100, because there is difference between the EM radiation traces of the EC point addition and doubling. The SEMA attack was successful because of the conditional branch in Step 4 of Algorithm 1.

As a countermeasure to this attack we implemented the EC point multiplication by using the always double and add algorithm from [24]. Algorithm 2 shows that the EC point addition is executed independently from the value of the key bits. One EM radiation measurement of this architecture is shown in Fig. 3.

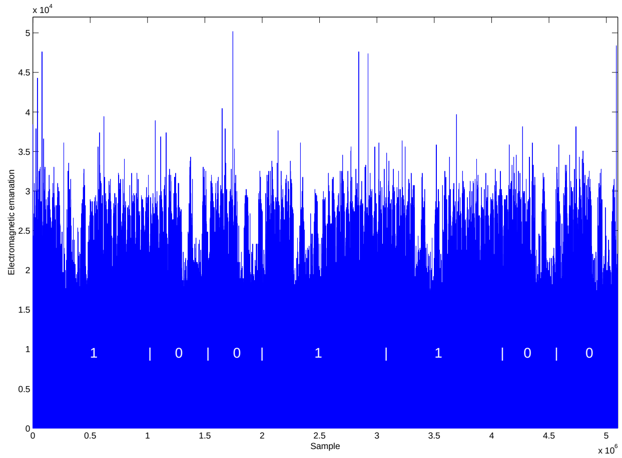

Fig. 2. Electromagnetic radiation trace of a 160-bit EC point multiplication with double-and-add algorithm.

Algorithm 2. Elliptic Curve Point Multiplication, always double and add

Require: EC point $P = (x, y)$, integer k, $0 < k < M$, $k = (k_{l-1}, k_{l-2}, \cdots, k_0)_2$, $k_{l-1} = 1$ and M

Ensure: $Q = (x', y') = [k]P$

1: $Q \leftarrow P$
2: **for** i from $l-2$ downto 0 **do**
3:     $Q_1 \leftarrow 2Q$
4:     $Q_2 \leftarrow Q_1 + P$
5:     **if** $k_i = 1$ **then**
6:         $Q \leftarrow Q_2$
7:     **else**
8:         $Q \leftarrow Q_1$
9:     **end if**
10: **end for**

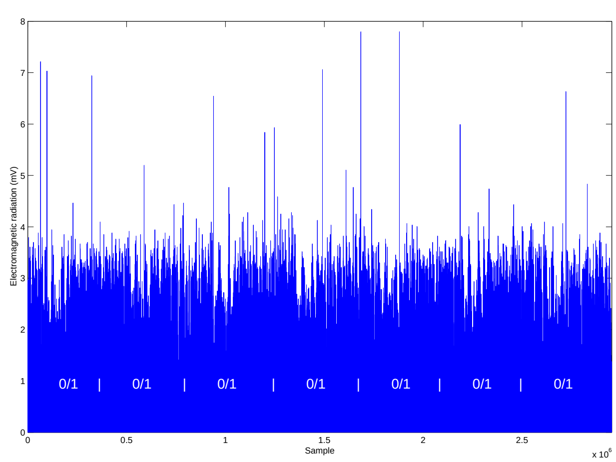

Fig. 3. Electromagnetic radiation trace of a 160-bit EC point multiplication with always double and add algorithm.

VI. DEMA Attack on an FPGA Implementation of an EC Processor

The target for our DEMA attack is the second most significant bit (MSB) of the key, k_{l-2}, in Algorithm 2. If $k_{l-2} = 0$, then Q will be updated by $2P$, otherwise by $3P$ at step 5 in Algorithm 2.

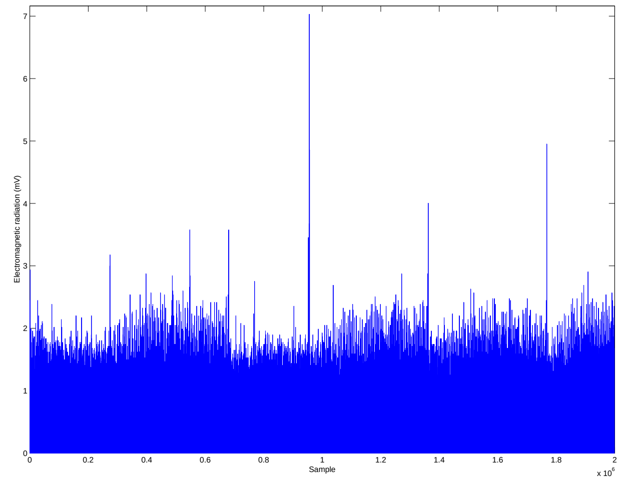

Fig. 4. The EM trace of the $1st$ measurement

In the first step of our attack, we have produced a so-called EM radiation file. For this purpose, we have chosen N random points on the EC and one fixed, but random key. We have let the FPGA execute N point multiplications of N EC points, P_i, $i = 1, \cdots, N$ with the same key, k as $Q_i = [k]P_i$. We will attack the circuit at the time the coordinates of Q_1 is updated for the second time at step 3 of Algorithm 2. Hence, we have measured the EM radiation of the FPGA during 2400 clock cycles around this event. The clock frequency applied to the chip was around 300 kHz and the sampling frequency of the oscilloscope was 250 MHz. With these measurements, we have produced a $N \times 2\,000\,000$ matrix, M_1. The electromagnetic radiation trace of one of these measurements, is shown in Fig. 4.

We have applied a pre-processing technique to reduce the amount of measurement data in every clock cycle. We have found the maximum value of the measurement data in each clock cycle as follows:

$$M_2(i,j) = max(M_1(i, D_i \cdot (j-1) + 1 : D_i \cdot j))\,, \qquad (7)$$

where $i = 1, \ldots, N$, $j = 1, \ldots, 2400$. $M_2(i,j)$ is the element of the matrix M_2 at the ith row and the jth column. D_i is the number of samples per clock cycle during ith measurement, $M_1(i, D_i \cdot (j-1)+1 : D_i \cdot j)$ is the row vector $[M_1(i, D_i \cdot (j-1)+1)\; M_1(i, D_i \cdot (j-1)+2) \cdots M_1(i, D_i \cdot j)]$.

Because the clock frequency of the function generator we have used for our experiments was slightly differing during the measurements we have to find D_i. In order to compute D_i we have to know the exact clock frequency. We have calculated the DFT of each measurement. The clock frequency can be between 250 kHz and 375 kHz. So we have looked between these frequencies for the maximum value in the DFT trace. The result for the 1-st measurement is shown in Fig. 5. According to this figure the clock frequency during the first measurement was *302.8 kHz*. Hence, $D_1 = 250 \cdot 10^6 / 302.8 \cdot 10^3 = 825.63$. From the DFT it is also visible that there is amplitude

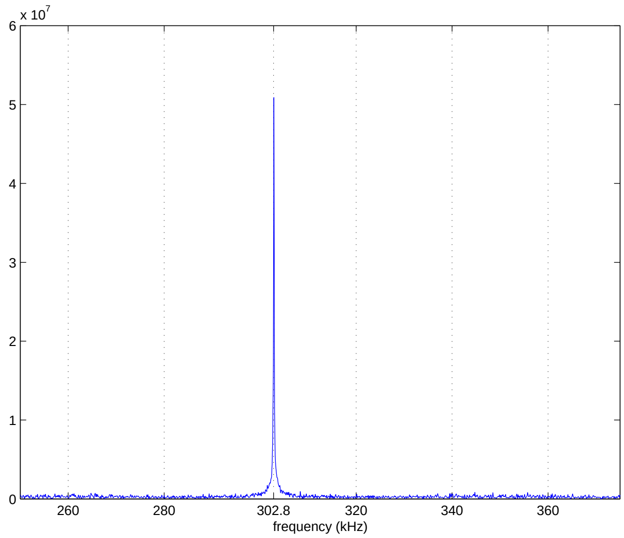

Fig. 5. The DFT of the EM trace of the 1-st measurement between 250 kHz and 375 kHz

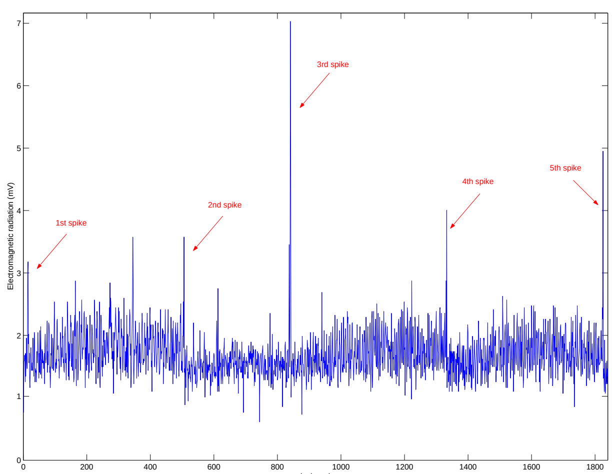

Fig. 6. The EM trace of the 1-st measurement after taking the maximum value in every clock cycle

modulation (AM) at the clock frequency [9]. Figure 6 shows the first measurement after taking the maximum value in every clock cycle.

We have implemented the EC point multiplication with Algorithm 2 in the C programming language. The C program computes N EC point multiplications with N EC points and the key. The EC points and the key are the same as the ones given to the FPGA during the measurements. During the execution of the EC point multiplications, C program computes the number of bits that change from 0 to 1 and from 1 to 0 in some registers at the corresponding steps to the five spikes shown in Fig. 6. The number of transitions is used as the EM radiation prediction.

We have predicted the EM radiation of the events which corresponds to the five spikes shown in Fig. 6 for $k_{l-2} = 0$ and $k_{l-2} = 1$ for each measurement. We wrote the prediction

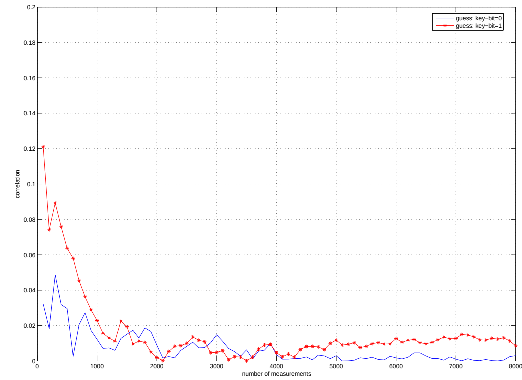

Fig. 7. The change in correlation for the third spike according to the number of measurements for each guess.

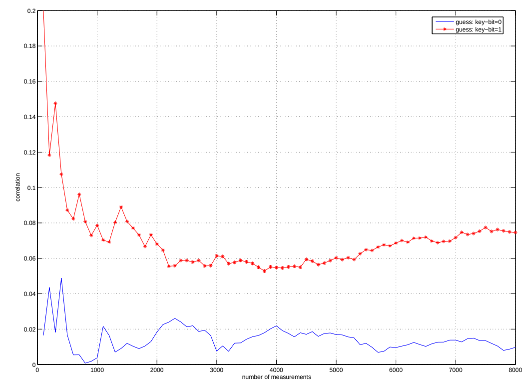

Fig. 8. The change in correlation for the fourth spike according to the number of measurements for each guess.

for spike p, guess g and measurement i in $M_3(p, g, i)$. Now we can learn the right value of k_{l-2} by finding the correlations between M_3 and M_2. There will be two values for each spike, one for the guess that the key-bit is 0, one for the guess that the key-bit is 1. The first aim was to find the correlation for the third spike, because that is the highest one. Figure 7 shows the correlation for the third spike for each guess according to the number of measurements. As it can be seen, the difference between both guesses is not very convincing.

So, we checked the other spikes. The correlations for spike 4 and 5 give us the correct key-bit by using only 1000 measurements. The correlation for the guess that the key-bit is 1 is much higher than the correlation for the other guess as shown in Fig. 8 and Fig. 9.

After 1000 measurements, the correlation for the $k_{l-2} = 1$ guess starts to differ from the correlation for the $k_{l-2} = 0$ guess. The correlation for the $k_{l-2} = 1$ guess starts to rise, for the $k_{l-2} = 0$ guess the correlation stays around 0.

VII. Conclusions and Further Work

In this paper we have presented a simple (SEMA) and differential (DEMA) electromagnetic analysis attacks on an FPGA implementation of an elliptic curve processor. As a

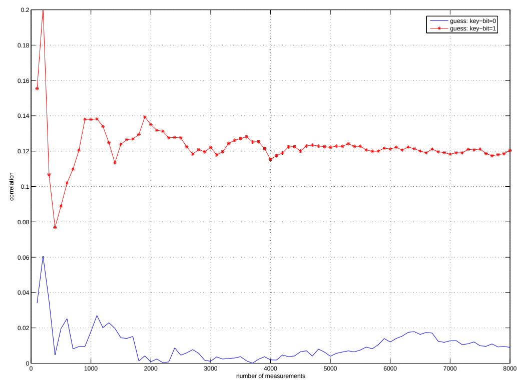

Fig. 9. The change in correlation for the fifth spike according to the number of measurements for each guess.

result of SEMA attack on an unprotected implementation we can find all the key bits using just one measurement. Then we have conducted DEMA attack on the improved implementation and have shown that it is possible to find the key bits by making more measurements and using correlation analysis. Our attacks show that electromagnetic attacks form a realistic threat for a broad range of cryptographic hardware implementations. Further work is necessary to optimize these attacks using more sophisticated antennas and signal processing techniques. On the other hand, system designers and cryptographers should jointly develop, implement and evaluate additional countermeasures against side channel attacks; these can consist of frequent key updates, and various masking and de-correlation approaches.

References

[1] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems," in *Advances in Cryptology: Proceedings of CRYPTO'96*, N. Koblitz, Ed., 1996, vol. 1109 of *LNCS*, pp. 104–113, Springer-Verlag.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology: Proceedings of CRYPTO'99*, M. Wiener, Ed., 1999, vol. 1666 of *LNCS*, pp. 388–397, Springer-Verlag.

[3] V. Miller, "Uses of elliptic curves in cryptography," in *Advances in Cryptology: Proceedings of CRYPTO'85*, H. C. Williams, Ed., 1985, vol. 218 of *LNCS*, pp. 417–426, Springer-Verlag.

[4] N. Koblitz, "Elliptic curve cryptosystem," *Math. Comp.*, vol. 48, pp. 203–209, 1987.

[5] S. B. Örs, L. Batina, B. Preneel, and J. Vandewalle, "Hardware implementation of an elliptic curve processor over $GF(p)$," in *IEEE 14th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, 2003, pp. 433–443.

[6] I. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.

[7] S.-M. Kang and Y. Leblebici, *CMOS Digital Integrated Circuits: Analysis and Design*, McGraw Hill, 2002.

[8] R. A. Serway, *Physics for scientists and engineers*, Saunders Golden sunburst series. Saunders college publishing, 1996.

[9] L. W. Couch, *Digital and Analog Communication Systems*, Prentice Hall, 1997.

[10] G. M. Clarke and D. Cooke, *A basic course in statistics*, Arnold London, 4th edition, 1998.

[11] NSA, "NSA TEMPEST Documents," `http://www.cryptome.org/nsa- tempest.htm`.

[12] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): Measures and counter-measures for smard cards," in *Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security (E-smart)*, I. Attali and T. Jensen, Eds., 2001, vol. 2140 of *LNCS*, pp. 200–210, Springer-Verlag.

[13] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Proceedings of 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Ç. K. Koç, D. Naccache, and C. Paar, Eds., 2001, vol. 2162 of *LNCS*, pp. 255–265, Springer-Verlag.

[14] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s): Attacks and assessment methodologies," in *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, Eds., 2002, vol. 2523 of *LNCS*, pp. 29–45, Springer-Verlag.

[15] D. Agrawal, B. Archambeault, S. Chari, J. R. Rao, and P. Rohatgi, "Advances in side-channel cryptanalysis," *RSA Laboratories Cryptobytes*, vol. 6, no. 1, pp. 20–32, Spring 2003.

[16] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, Eds., 2002, vol. 2523 of *LNCS*, pp. 172–186, Springer-Verlag.

[17] D. Agrawal, J. R. Rao, and P. Rohatgi, "Multi-channel attacks," in *Proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, C. Walter, Ç. K. Koç, and C. Paar, Eds., 2003, vol. 2779 of *LNCS*, pp. 2–16, Springer-Verlag.

[18] C. D. Walter and S. Thompson, "Distinguishing exponent digits by observing modular subtractions," in *Proceedings of Topics in Cryptology - CT-RSA*, D. Naccache, Ed., 2001, vol. 2020 of *LNCS*, pp. 192–207, Springer-Verlag.

[19] S. Mangard, "Exploiting radiated emissions - EM attacks on cryptographic ICs," in *Proceedings of Austrochip*, 2003.

[20] V. Carlier, H. Chabanne, E. Dottax, and H. Pelletier, "Electromagnetic side channels of an FPGA implementation of AES," Cryptology ePrint Archive-2004/145, 2004, `http://eprint.iacr.org/`.

[21] S. B. Örs, E. Oswald, and B. Preneel, "Power-analysis attacks on an FPGA – first experimental results," in *Proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, C. Walter, Ç. K. Koç, and C. Paar, Eds., 2003, vol. 2779 of *LNCS*, pp. 35–50, Springer-Verlag.

[22] P. Buysschaert and E. De Mulder, "Elektromagnetische analyse (EMA) van een FPGA implementatie van een elliptische krommen cryptosysteem," M.S. thesis, K.U.Leuven, Departement Elektrotechniek - ESAT, Kasteelpark Arenberg 10, B 3001 Heverlee, Belgium, May 2004.

[23] S. B. Örs, L. Batina, B. Preneel, and J. Vandewalle, "Hardware implementation of an elliptic curve processor over $GF(p)$ with montgomery modular multiplier," *International Journal of Embedded Systems*, February 2005.

[24] J.-S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," in *Proceedings of the 1st International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Ç. K. Koç and C. Paar, Eds., 1999, vol. 1717 of *LNCS*, pp. 292–302, Springer-Verlag.