Simple Electromagnetic Analysis in Cryptography

Zdenek Martinasek, Vaclav Zeman, Krisztina Trasy

***Abstract*—The article describes the main principle and methods of simple electromagnetic analysis and thus provides an overview of simple electromagnetic analysis. The introductory chapters describe specific SPA attack used visual inspection of EM traces, template based attack and collision attack. After reading the article, the reader is sufficiently informed of any context of SEMA. Another aim of the article is the practical realization of SEMA which is focused on AES implementation. The visual inspection of EM trace of AES is performed step by step and the result is the determination of secret key Hamming weight. On the resulting EM trace, the Hamming weight of the secret key 1 to 8 was clearly visible. This method allows reduction from the number of possible keys for following brute force attack.**

***Keywords*—elektromagnetic analysis, simple analysis, EMA, side channels.**

I. Introduction

Since their public appearance in the mid-90s [1], side-channel attacks have attracted a significant attention within the cryptographic community. The power analysis (PA) and the electromagnetic analysis (EMA) are typical examples of successful attacks against trusted cryptographic devices. Scientist van Eck [2] had merit in the advancement of electromagnetic attacks in the public sector, Eck proved that it is possible to capture and measure the size of the electromagnetic field of computer monitors and it is possible to obtain the original image from measured waveforms. Scientists Kuhn and Anderson [3] invented countermeasurement against the attack and it was a special shielding film, which reduce the electromagnetic radiation of the monitor.

The first published articles focused on the EMA of integrated circuits and computing units performing the cryptographic operations were [4] by Gandolfi in 2001 and [5] by Quisquater and Samyde. The attacks were realized by using several antennas located near the integrated circuit of smart card. These attacks were invasive, which means that it was necessary to destroy of smart card cover to give the antenna as close as possible to the chip. Agrawal [6] build on this work and used the declassified materials from the project TEMPEST and showed that EM side channel attacks on cryptographic devices are practically realizable and also some information that leaked through EM channel are more significant than information that leaked through the power side channel. Articles [7], [8], [9] are focused on systematic study of EM leakage information from computing equipment such as smart cards, computer processors and cryptographic accelerators.

Zdenek Martinasek is with Brno University of Technology, Brno, Czech Republic. He is now with the Department of Telecommunications, Purkynova 118, 612 00 Brno, (martinasek@feec.vutbr.cz).

Vaclav Zeman is with Brno University of Technology, Brno, Czech Republic. He is now with the Department of Telecommunications, Purkynova 118, 612 00 Brno (zeman@feec.vutbr.cz).

Krisztina Trasy is with Department of Garden and Open Space Design, Faculty of Landscape Architecture, Corvinus University of Budapest, Fovam ter 8, Budapest, Hungary (krisztina.trasy@stud.uni-corvinus.hu).

Manuscript received September 3, 2012; revised January 11, 2007.

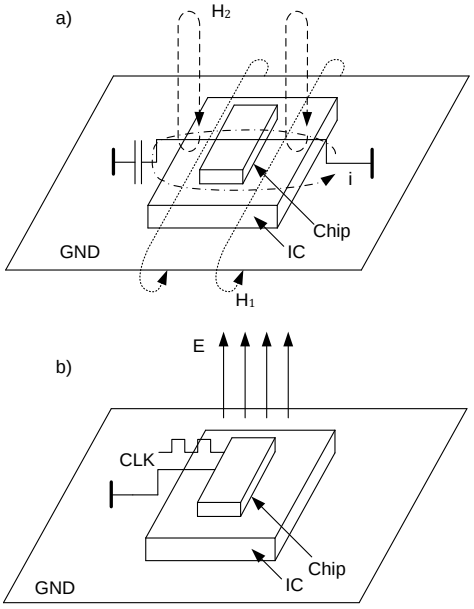

Fig. 1. The principle of direct emissions of the magnetic field of IC

As well as in classical power analysis, the attacker is measuring dynamic electromagnetic field of cryptographic device depending on input data. The plain text is encrypted by using a secret key and measured waveforms are recorded within a measuring device for encrypting each plaintext. The attacker can deduct sensitive information directly (SEMA, Simple Electromagnetic Analysis) or can use mathematical approach (DEMA, Different Electromagnetic Analysis). In SEMA, the attacker tries to determine the key more or less directly from one measured trace. In other words SPA attacks are useful in practice if only one or very few traces are available. DEMA and DPA attacks are the most popular because the attacker does not need any detailed knowledge about the attacked device. In contrast to SA, the DA attacks require a large number of power traces measurements. DPA attack uses mathematical approach to determine the sensitive information.

The goal of the article is to describe the main principle and the methods of simple electromagnetic analysis. In the other words, the article create an overview of simple electromagnetic analysis. Another aim of the article is the practical realization of SEMA which is focused on AES implementation with a description of the experimental testbed. The SEMA of AES is performed step by step and the result is the determination of secret key Hamming weight. After reading the article, the

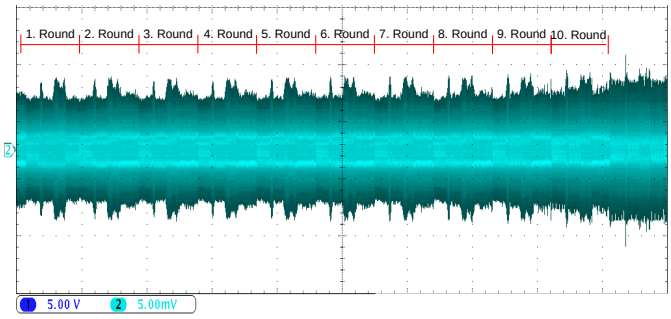

Fig. 2. EM trace of AES

reader is sufficiently informed of any context of SEMA.

The article is divided as follows: the following section describes SEMA attacks and the following three subsections discuss specific attack types used visual inspection of EM traces, template based attack and collision attack. The last chapter illustrates a specific example of SEMA attack, which was realized on the encryption algorithm AES. Visual analysis of electromagnetic traces was aimed at operation `AddRoundKey`.

II. Side channel sources

The most modern cryptographic equipments are based on CMOS technology. The basic element of this logic is the inverter [10]. The inverter contains two field-effect transistors with the opposite type of conductivity PMOS (P-channel) and NMOS (N-channel) and works as follows:

- when the voltage of input is high the PMOS transistor is off and the NMOS transistor is on and the output of inverter is low,
- on the other hand, when the voltage of the input is low NMOS transistor is off and the PMOS is on, so the output voltage is high.

The power consumption is minimal for both these stable states. Power peak occurs during the transition between these states when both transistors are open in a short time and power supply is shorted to the ground. The size of current peaks is directly proportional to the number of transistors which have been switched in the whole integrated circuit. The main source of power change is charging and discharging a parasitic capacity by a current [11]. This parasitic capacity represents the capacity of control electrodes following transistors in the integrated circuit. The dynamic power consumption of the inverter can be expressed by the formula [11]:

$$P_{\text{dyn}} = C \cdot V_{\text{CC}}^2 \cdot P_{0\to1} \cdot f, \tag{1}$$

where C is the parasitic capacity, $P_{0\to1}$ is the probability of transition between states $0 \to 1$, f is a switching frequency and V_{CC} is the supply voltage. If the power consumption is measured (to ground or power junction of the inverter) will be the highest peak while charging the parasitic capacity [11].

The result of charging and discharging of parasitic capacitance is the step change of circuit current which affects emit electromagnetic fields in the vicinity of the inverter. Modern

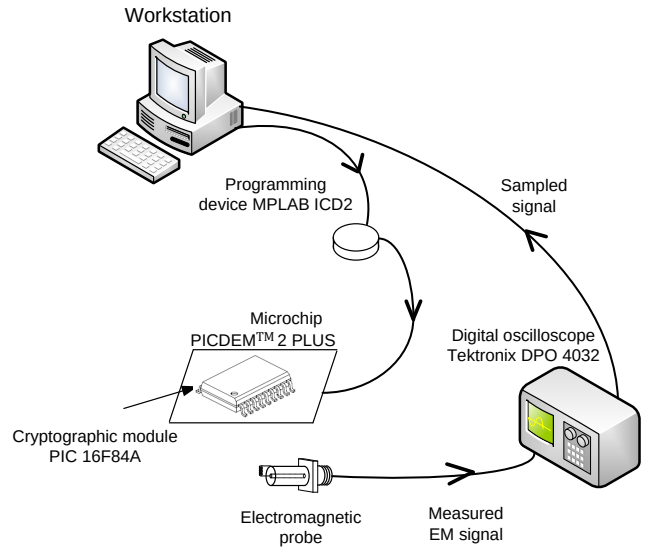

Fig. 3. Diagram of the testbed.

integrated circuits are composed of millions of transistors and connections, in which the changing currents are dependent on the transmitted data. These currents generate a variable electromagnetic field that can be measured by the probes. The ways of EM radiation emitted by integrated circuits (IC) are the following:

- conductive emission - is reflected in the integrated circuit pins, respectively, in routes which are connected on pins. These routes may behave as antennas emitting radiation during a step change in current.
- Electric and magnetic near-field emissions - EM field is generated due to current loops in IC. The magnetic field component can be divided into two parts H1 and H2 as it is shown in figure 1 a). The field H1 is closed around the ground contact of printed circuit boards and H2 is generated by currents in the internal capacitors and closes in the area above the surface of the IC in the range of approximately 10 mm. The magnetic field H2 is significantly larger than the field H1.

The electric field is located in the vicinity of parts under power supply. The main source of the electric field are internal a conductive connection in the IC. Figure 1 b) shows the emission of the electric field caused by the clock signal. Most of the flow is concluded to the ground, but part of the flow is radiated into the environment.

Based on the assumption that the IC generates an electromagnetic field, it is possible to characterize the electromagnetic emission by measuring. These measurements are realized by electric and magnetic probes. Measurement with small magnetic probes are used to determine the size of near magnetic field. The advantage of these probes is that they can be placed as close as possible to the source of radiation and increase the measurement accuracy. If the probe is placed further away it is possible to detect the microprocessor clock signal. Useful EM signals, which are dependent on the processed data, can be captured in the areas of the processor and

```
1.R = m
2.for i = 0:(b - 1) {
3.         R = (R*R)mod(n)
4.         if (d(i)==1) {
5.              R=(R*m)mod(n)   }
6. }
7. return R
```

Fig. 4. Algoritmus square and multiply

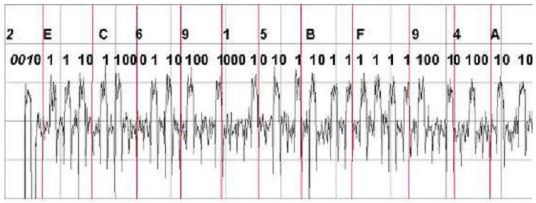

Fig. 5. Current consumption of square and multiply [13]

the memory of cryptosystem [11], [12].

Our measurements typically take place in this region where the signals may be considered as quasi-static. This allows to use the Biot-Savart law to describe the magnetic field $\vec{B}$:

$$d\vec{B} = \frac{\mu I \vec{dl} \times \hat{r}}{4\pi |\vec{r}|^2} \tag{2}$$

where I is the current carried on the conductor of infinitesimal length $\vec{dl}$, μ is the magnetic permeability and $\vec{r}$ is a vector specifying the distance between the current and the field point ($\hat{r} = \vec{r} / |\vec{r}|$).

Faraday's law can be used to express the voltage that will induce in the probe:

$$V_{emf} = -N\frac{d\phi}{dt} \tag{3}$$

$$d\phi = \int_{surface} \vec{B} \cdot d\vec{S} \tag{4}$$

where N is the number of turns in the coil and ϕ the magnetic flux. This equation clearly expresses that the closer we place the probe to the chip, the bigger the measured magnetic field is. These simple equations do not describe the exact behavior of the magnetic field because the field is data-dependent (that means dependent of the current intensity) and the orientation of the field directly depends on the orientation of the current. The processor will still process the same data (in a program loop) and we calculate the mean values of EM field to reduce this dependency (electronic noise).

If we assume that the bus may behave as an infinite wire, we can reduce the above cited Biot-Savart equation to the following expression:

$$\vec{B} = \frac{\mu I}{2\pi R}\hat{a_\varphi} \tag{5}$$

where R is the distance to the wire and $\hat{a_\varphi}$ is a unit vector azimuthally oriented with respect to the wire. It follows from these assumptions that the size of the induced voltage will be affected of probe position (angle) and microchip.

III. Simple Electromagnetic Analysis

This chapter will explain the principle of simple elektromagnetic analysis and will describe the various types. A simple power analysis (same like EM analysis II) was defined by Kocher [1] as follows: SPA is a technique that involves directly a interpreting power consumption measurements collected during cryptographic operations. In other words, the attacker tries to determine the secret key directly from the measured EM traces. This could make the simple analysis attack for potential attackers quite attractive technology, but they usually need detailed knowledge about the implemented algorithm and cryptographic device (module). In the extreme case, the attacker attempts to reveal the secret key based on one single measured EM trace. We can distinguish between single shot SPA attacks and multiple shot. From the name, it is clear that the attacker records only one EM trace in a single shot of SPA attacks and more EM traces in multiple shot. If there is only one measured waveform, it is necessary to use statistical methods to extract the useful signal. The advantage is the possibility to reduce the noise in measured traces when the attacker has more traces available. For both types of SPA attacks it is unconditionally necessary existence significant (direct or indirect) dependence of a secret key and EM trace.

A. Visual Inspections of EM Trace

Direct observation of traces is based on the following facts. All algorithms that run on cryptographic devices are performed successively in a defined sequence. Cryptographic algorithm consists of several functions (operations), which are translated into instructions supported by cryptographic module (microprocessor). For example, the core of AES algorithm is composed of these functions: key expansion, adding keys, nonlinear byte substitution rotation rows and matrix multiplication. These operations can be implemented in the microprocessor and in this case, the functions are implemented using a microprocessor supported instruction.

In most cases, the microprocessors have the instruction set, which includes arithmetic instructions (addition), logical instruction (XOR), instructions work with data (store, move), program branch instruction (jump or condition). Each instruction is working with a different number of bits or bytes and uses the different parts of the circuit such as an arithmetic logic unit, the internal or external memory (RAM or ROM) or input and output ports. These microprocessor components are physically separated and are different from functions and realization. For this reason, every instruction has typical EM trace which leads to the creation of characteristic EM pattern (fingerprint). The ability to distinguish between individual instruction in EM trace brings serious security threat when a sequence of instructions depends directly on a secret key. If specific instruction is processing during algorithm, when the key bit is 1 and different instruction is processed and if a key bit is 0, then it is possible to determine the secret key directly from the measured EM trace looking at the sequence

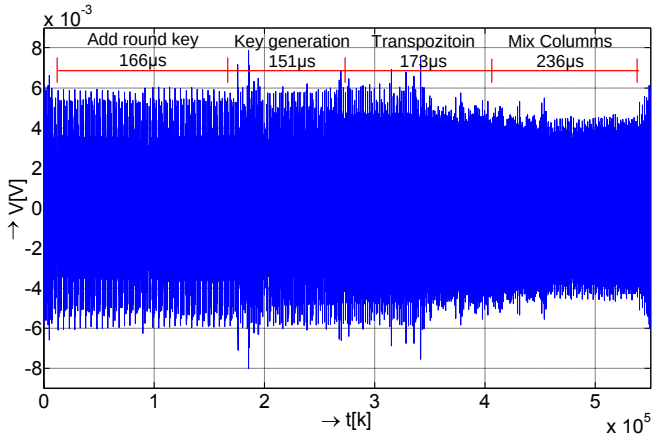

Fig. 6. EM trace of the first round.

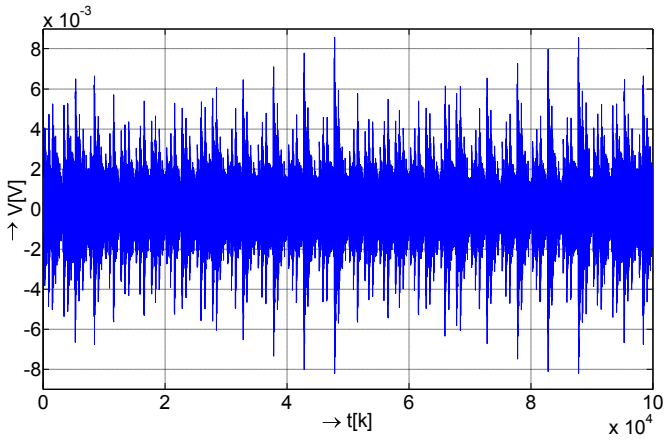

Fig. 7. EM trace of `Add Round Key`.

of performed instructions. A typical example of this SPA is attack to the implementation of an asymmetric algorithm RSA. Asymmetric RSA algorithm is based on a mathematical operation modular exponentiation. For the calculation of modular exponentiation there are more methods, but square and multiply algorithm are often used for the implementation in to the cryptographic modules. In this algorithm, each key bit (d) is processed sequentially (left-to-right) and is processed with a modular square operation followed by a conditional modular multiplication. The multiplication is only executed when the associated key bit is equal to one. Schema of algorithm is shown in figure 4. The attacker can easily determine from the EM trace (sequence of instructions) in which step was performed row 3 and in which 5 of algorithm. An example of current consumption square and multiply algorithm is shown in Figure 5. The attacker then easily determines the value of the secret key.

B. Template Based Attacks

Template based attacks use the fact that EM consumption is dependent on the currently processed data. Electromagnetic traces are characterized multidimensional normal distribution, which is fully defined by the vector of mean values and covariance matrix $(\mathbf{m}, \mathbf{C})$. This pair $(\mathbf{m}, \mathbf{C})$, is denoted as a template. The attacker assumes that he can characterize the device with the help of templates for certain sequences of instructions. For example, the attacker has full control over the same device on which he wants to perform attack. On this device, he starts a sequence of instructions for different input data d_i and a different key k_j and records the EM waveforms. Subsequently, the attacker groups corresponding sequences (d_i, k_j) and calculate the vector of mean values and covariance matrix of multivariate normal distribution. The result is obtained templates for all pairs data and keys $(d_i, k_j) : h_{d_i,k_j} = (\mathbf{m}, \mathbf{C})$. During the attack, the attacker uses these templates and just measured power consumption to determine the secret key of device as follows. At first, he measures the EM trace of device and the second step is the calculation of the probability density function of multivariate normal distribution $(\mathbf{m}, \mathbf{C})_{d_i,k_j}$ and the measured trace. In other words, he calculates the probabilities for the measured EM trace for all templates according to the following equation:

$$p(t; (\mathbf{m}, \mathbf{C})_{d_i,k_j}) = \frac{exp(-\frac{1}{2} \cdot (\mathbf{t} - \mathbf{m})' \cdot \mathbf{C}^{-1} \cdot (\mathbf{t} - \mathbf{m}))}{\sqrt{(2 \cdot \pi)^T \cdot det(\mathbf{C})}}. \quad (6)$$

Probabilities indicate how good the templates match measured trace. Fully intuitively, the maximum probability should correspond to the correct template. Each template is associated with a secret key therefore the attacker can determine the secret key. This method is based on the theory which is described in [14].

C. Collision Attacks

Collision Attacks are based on the fact that the attacker is able to observe the EM consumption for two encryption runs with two different inputs d_i and d_i and the unknown key k_j . In a collision, the attacker exploits the fact that in two encryption runs a specific intermediate value v_i, j can be equal:$v_j = f(d_i, k_j) = f(d_i^*, k_j)$. Intermedia1e value collides if an intrermedia1e value in one encryption run is equal to the intrermedia1e value the other encryption run. The most important knowledge is that for two inputs d_i and d_i^* a collision cannot occur for all key values but only for a certain subset of keys. Each collision allows to reduce the search space for the key. If several collisions can be realized, the key can be identified.

IV. Experimental measurements

The testbed focused on the measuring direct emissions was built to realize SEMA using Visual Inspections of EM Trace (section III-A). Diagram of the testbed is shown in figure 3 and was designed from the following devices:

- cryptographic module PIC16F84 microcontroller,
- workstation with installed software MPLAB,
- electromagnetic probe for sensing near EM field,
- ICD2 programing device,
- development board PICDEM 2 PLUS,
- oscilloscope Tektronix DPO-4032 with a maximum sampling frequency of 2.5GSa/s.

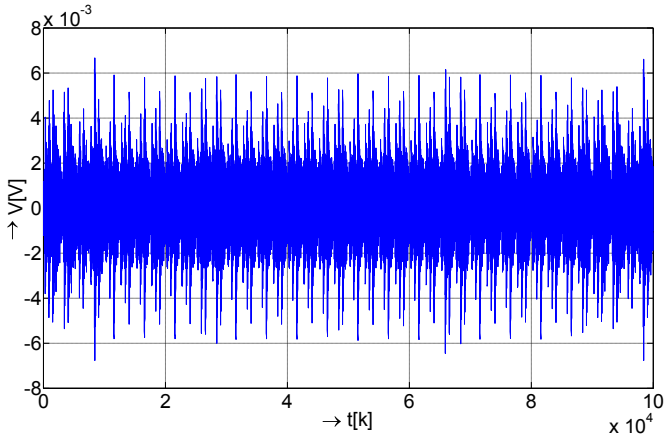

Fig. 8. The reference EM trace T_{ref}

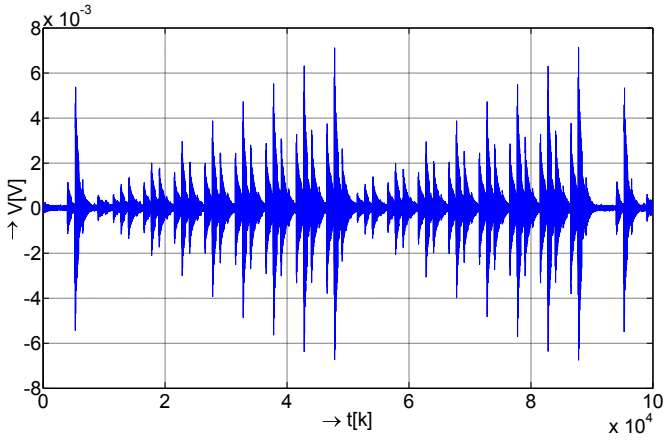

Fig. 9. The differential EM trace.

Encryption algorithm AES was implemented to the cryptographic module PIC16f84A. The algorithm was created by Edim Permadim [15] but it was necessary to take a few adjustments for measurement. For example the synchronization signal was inserted to simplify synchronization with oscilloscope. Figure 2 shows the total EM trace of AES algorithm stored by oscilloscope. Ten rounds of AES are clearly visible and the attacker can concentrate only the interesting parts on.

We analyzed EM trace of the whole AES algorithm and we focused only analyzing operations `Add Round Key`, because in initializing phase this operation works with original secret key. This operation performs the logical operation XOR with the block of plaintext **A** and the block of secret key $\mathbf{K_{sec}}$ and saves the result to the block **S**. In the original form, the AES algorithm works with the length of data blocks of 128 bits (4×4 matrix). Operations `Add Round Key` can be written as follows:

$$\mathbf{S} = \mathbf{A} \otimes \mathbf{K_{sec}}. \tag{7}$$

Figure 6 shows the EM trace of the AES first rounds. The raw contour of the individual phases are visible but more precise identification should be done at the level of individual instructions. The algorithm begins with an initialization phase `Add Round Key` and this operation takes 166 microseconds. The following operation is `Sub keys Generation`, which is executed every each cycle because insufficiency of storage space is available on a microprocessor. This operation takes 151 microseconds. The next operations are byte substitution and rotation and take 151 microseconds. The final operation is the `Mix Column`, which is quite demanding and takes 236 microseconds. The total duration of one round implemented AES algorithm is 726 microseconds.

Suppose the secret key is byte expressed $K = \{n, n, n, n, n, n, n, n\}$ for $0 \leq n \geq 256$. From the mathematical perspective each byte is a group of eight elements containing two groups of elements (specific number of 1 and 0). The number of all secret keys i of possible combinations

TABLE I
PERMUTATION OF SECRET KEY DEPENDING ON THE HAMMING WEIGHT

Hamming weight w of secret key (max 8)	Permutation i of secret key (theoretical max 256)
1	8
2	28
3	56
4	70
5	64
6	28
7	8
8	1

is given by the permutation with repetition:

$$i_{m_1,m_2,\ldots,m_k} = \frac{m!}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!}. \tag{8}$$

The number of non-zero bits in the key can be described with Hamming weight w $0 \leq w \geq 8$. If the attacker knows the secret key Hamming weight, the number of all possible variants can be reduced according to (8). Table I shows the number of key combinations according to the (8) depending on the Hamming weight. The table shows that the knowledge of key Hamming weight will significantly reduce the number of possible secret key. In the worst case ($w = 4$) it would be chosen from 70 possible values from theoretical 256. This number corresponds to 30% of total number secret key.

Secret key $\mathbf{K_{sec}}$ was filled with various data manually in our experiment and the data was set randomly. Data had value from 01h to FFh, where Hamming weight w of the next element is always greater one compared to the previous element. For example the value of the first secret key word $k_{0,0}$ was 01h (B'00000001') then $w(k_{0,0}) = 1$. The following element in the matrix has a value 03h (B'00000011') than Hamming weight of the last element of $w(k_{0,1}) = 2$ and the last element $k_{3,3}$ takes the value FFh (B'11111111'), were $w(k_{1,3}) = 8$. The matrix of secret key $\mathbf{K_{sec}}$ look as follows (hexadecimal notation):

$$\mathbf{K_{sec}} = \begin{pmatrix} 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \\ 01 & 03 & 07 & 0F \\ 1F & 3F & 7F & FF \end{pmatrix}.$$

Hamming weight of the secret key can be determined by realization of two measurement of EM traces. The authors follow the own work focused on power side channel [16], [17], [18], [19], [20]. The method is following: the attacker measures the reference EM trace T_{ref}, which corresponds to the operation `Add Round Key` where the values of key and state are zero. It is necessary for the attacker to have full control over the same device on which he wants to perform attack. Measured reference EM trace T_{ref} is displayed in figure 8. No significant peaks are visible on trace because the cryptographic module works with no data. After that, the attacker measures EM traces of cryptographic module corresponding to the `Add Round Key`. This trace is shown in the figure 7. During the second measurement, the microprocessor works with data according to the rules described above therefore peaks were observed on trace. The peaks corresponding to data processing are very evident but Hamming weight is not entirely clear for lower values. The best way to improve readability is to calculate differential signal as a simple subtraction of trace in this two measurements, i.e. trace of T_{ref} and measured EM trace. The result of this simple operation is the waveform shown in figure 9. The figure shows peaks corresponding to work with data. Very important is that the increasing of the Hamming weight of the secret key 1 to 8 is clearly visible. In this case, the Hamming weight of secret key equals 72.

The numerical evaluation of measured data could be summarized again with table I, because the HW is successively equal to values $1, 2, 3, 4, 5, 6, 7, 8$. It is obvious that table contains results only for the first half of the key because the second half is the same. From the table it is evident that the knowledge of key Hamming weight reduced the number of possible keys. We do not assume determination of the whole secret key (in our key 128 bits length) in one time moment but we assume determination of secret key successively by bytes like in SEMA and DEMA. In this case this method allow reduction from the number of possible keys from 2048 to 263 and in the worst case for $w = 4$ it corresponds to 56. If it is not possible to determinate the secret key by bytes, this method allows to reduce the number of possible key for brute force attack from $3.40 \cdot 10^3 8$ to $1.58 \cdot 10^2 0$ for 128 bits length key. In the worst case for Hamming weight $w = 4$ and it corresponds to $3.32 \cdot 10^2 9$.

V. Conclusion

The article describes the main principle and methods of simple electromagnetic analysis. The introductory chapters describe specific SPA attack used visual inspection of EM traces, template based attack and collision attack. Another aim of the article was the practical realization of SEMA which is focused on AES implementation. The visual inspection of EM trace of AES is performed step by step and the result is the determination of secret key Hamming weight.

We analyzed the EM trace of the operations `Add Round Key` in initializing phase because in this time the algorithm works with original secret key. Hamming weight of secret key was determined by realization of two measurements of EM traces and then subtracting waveforms. The first trace corresponds to the operation `Add Round Key` where the values of key and state are zero and the second corresponds to the operation `Add Round Key` where the values of key equal secret key and state are random. During the second measurement, the microprocessor performs the date with operation XOR, therefore peaks were observed on trace. The Hamming weight of the secret key 1 to 8 was clearly visible and in this case, the Hamming weight of secret key equaled 72. In this case this method allows reduction from the number of possible keys and it depended on the fact if the attacker is able to test thee key by bytes or whole.

Acknowledgment

Research was sponsored by the Technology Agency of the Czech Republic project TA02011260 and the Ministry of Industry and Trade of the Czech Republic project FR-TI4/647.

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 1999, pp. 388–397.

[2] W. V. Eck and N. Laborato, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, pp. 269–286, 1985.

[3] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," in *Proc. 2nd Workshop on Information Hiding*. Springer-Verlag, 1998, pp. 124–142.

[4] K. Gandolfi, D. Naccache, C. Paar, K. G, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," 2001.

[5] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *Smart Card Programming and Security*, ser. Lecture Notes in Computer Science, I. Attali and T. Jensen, Eds. Springer Berlin / Heidelberg, 2001, vol. 2140, pp. 200–210, 10.1007/3-540-45418-7_17. [Online]. Available: http://dx.doi.org/10.1007/3-540-45418-7_17

[6] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi, "The EM Side Channel(s)," 2003, pp. 29–45. [Online]. Available: http://dx.doi.org/10.1007/3-540-36400-5_4

[7] Çetin Kaya Koç, P. Rothatgi, W. Schindler, and C. D. Walter, Eds., *Cryptographic Engineering*, 2009.

[8] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *CHES '01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*. London, UK: Springer-Verlag, 2001, pp. 251–261.

[9] B. Struif, "Use of biometrics for user verification in electronic signature smartcards," in *Smart Card Programming and Security*, I. Attali and T. Jensen, Eds., no. 2140, Berlin, 2001. [Online]. Available: 2140/21400220.htm

[10] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 57, no. 2, pp. 355 –367, feb. 2010.

[11] E. Peeters, F.-X. Standaert, and J.-J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integration, the VLSI Journal*, vol. 40, no. 1, pp. 52 – 60, 2007, embedded Cryptographic Hardware. [Online]. Available: http://www.sciencedirect.com/science/article/B6V1M-4J3NWY2-1/2/0197aa6143d75a8303ace31403077841

[12] T. Ostermann, W. Gut, C. Bacher, and B. Deutschmann, "Measures to reduce the electromagnetic emission of a soc," in *VLSI-SOC*, 2003, pp. 31–.

[13] M. Joye and F. Olivier, "Side-channel analysis," in *Encyclopedia of Cryptography and Security (2nd Ed.)*, 2011, pp. 1198–1204.

[14] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory (v. 1)*, 1st ed. Prentice Hall, Apr. 1993. [Online]. Available: http://www.worldcat.org/isbn/0133457117

[15] E. Permadim. (2010, Dec.) Pic microcontoller math library methods. [Online]. Available: http://www.piclist.com/techref/microchip/math/index.htm

[16] Z. Martinasek, T. Macha, and P. Stancikk, "Power side channel information measurement," in *Research in telecommunication technologies RTT2010*, September 2010.
[17] Z. Martinasek, T. Petrik, and P. Stancik, "Conditions affecting the measurement of power analysis," in *Research in telecommunication technologies RTT2011*, September 2011.
[18] Z. Martinasek and P. Machu, "New side channel in cryptography," in *Proceedings of the 17th Conference Student EEICT 2011*, April 2011.
[19] Z. Martinasek, T. Macha, and V. Zeman, "Classifier of power side channel," in *Proceedings of NIMT2010*, September 2010.
[20] Z. Martinasek, T. Macha, O. Raso, J. Martinasek, and P. Silhavy, "Optimization of differential power analysis," *PRZEGLAD ELEKTROTECHNICZNY*, vol. 87, no. 12, pp. 140 – 144, 2011. [Online]. Available: http://pe.org.pl/articles/2011/12a/28.pdf

Zdenek Martinasek received BSc at the Department of Telecommunications at the Faculty of Electrical Engineering and Communication at Brno University of Technology in 2006. He received Ing. (MSc) at the same department in 2008. Now he is a PhD student at the same faculty. He also helps to cover pedagogically Master's program course. The area of his professional interests is cryptography,side channel analysis, sensors and modern data communication.

Vaclav Zeman received MSc. (Ing) at Faculty of Electrical Engineering and Communication at Brno University of Technology in 1991. He received Ph.D. at the Department of Telecommunications the at same Faculty in 2003. Now is the Associate Professor (doc. 2005) Faculty of Electrical Engineering and Communication at Brno University of Technology. He publishes in the cryptology area and communication systems area. Now, he is a lecturer and he deals with cryptology and information system security.

Krisztina Trasy was born in 1988 and she is last year MSc student of Department of Garden and Open Space Design, Faculty of Landscape Architecture, Corvinus University of Budapest.