Zdenek Martinasek[1], Vaclav Zeman[1], Petr Sysel[1], Krisztina Trasy[2]

Brno University of Technology(1),Corvinus University of Budapest(2)

Near electromagnetic field measurement of microprocessor

Abstract. *The article describe systematically the electromagnetic (EM) side channels sources and electromagnetic field of the microprocessor and is focused on the best way how to measure the near electromagnetic field of microprocessor. It was suggested and realized several electromagnetic probes and it was performed the measurement regarded to the theoretical background on the testbed with cryptographic module (microprocessor) performed the Advanced Encryption Standard (AES). On the measured waveforms of the electromagnetic emission was studied the influence of probe construction namely two parameters wire diameter and number of turns. In following measurement was studied how induced voltage depending on the distance of measuring coil to microprocessor and the last measurement dealt with position of probe and microchip.*

Streszczenie. *W artykule przedstawiono zagadnienie emisji pola elektromagnetycznego przez mikroprocesor i zawartych w nim informacji o stanie układu. Korzystając z platformy mikroprocesorowej, zaimplementowano AES i dokonano pomiarów sondami cewkowymi, badając zależność indukowanego napięcia od parametrów sondy (grubość drutu, ilość zwojów). (**Pomiary pola elektromagnetycznego mikroprocesora w bliskiej odległości**)*

Keywords: elektromagnetic analysis, EMA, side channel, electromagnetic field of microprocessor.
Słowa kluczowe: analiza elektromagnetyczna, EMA, kanał boczny, pole elektromagnetyczne procesora.

Introduction

The power analysis (PA) and the electromagnetic analysis (EMA) are typical examples of successful attacks against trusted cryptographic devices. Netherlandish scientist van Eck [4] 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. The work [7] invented countermeasuremnt 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 [6] and [12]. The attacks were realized by using several antennas located near the integrated circuit of smart card. These attacks were invasive thus it was necessary to intrusion of smart card cover to give the antenna as close as possible to the chip. Agrawal [1] 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 leaked through EM channel are more significant than information leaked through the power side channel. The new possibilities of EM side channel attacks are also given in this article where indirect EM radiation occurs by relationships between different parts of the cryptographic system. Articles [3, 5, 13] are focused on systematic study of EM leakage information from computing equipment such as smart cards and computer processors.

In this paper, we intend to use a more complete description of the electromagnetic side channels sources and electromagnetic field of the microprocessor. The paper is focused on the best way how to measure the near electromagnetic field of microprocessor. We suggest and realized several electromagnetic probes (handmade intended only for near-field measurements) and we performed the measurement in the created testbed regarded to the theoretical background. At first, we analyzed whole EM trace of whole algorithm AES and subsequently, we focused our measurement on operation `AddRoundKey`. First of all, we studied the effect of processed data on the resulting EM signal. We performed a thorough analysis of measured EM signal and we analyzed every performing instruction of microprocessor in EM signal. For sure we measured current consumption of the same microprocessor which performed identical data and we compared the traces each other. After this deep analysis, we

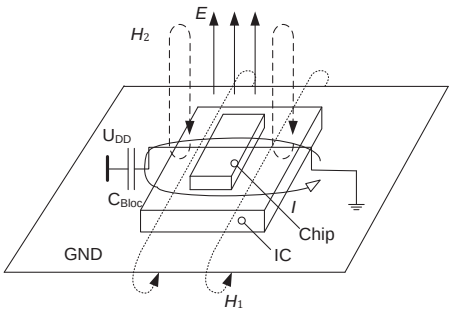


Fig. 1. The principle of direct emissions of the magnetic field of IC

were sure that we measure EM signal corresponding to the current consumption and we continued to analyze the influence of parameters on the measured EM waveform.

On the measured waveforms of the electromagnetic field was studied the influence of probe construction (number of turns, diameter of wire and so on), position of the probe and angle of probe and microchip. These important properties are not systematic written in any work. The authors want with this work to systematically describe the measurement of near electromagnetic fields microprocessor that gives true results.

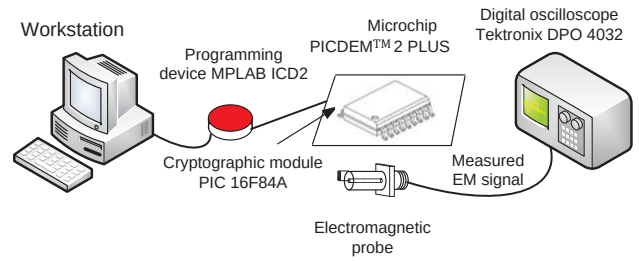
The authors follow the own work focused on power side channel [9, 10] were is in details discussed about the correct measurement of power consumption (methods of measurement, comparison of results and use of computers for cryptanalysis) and in [8] where is proposed optimization of differential power analysis.

The rest of the paper is structured as follows. Section *Side channel sources* describes the origin of power and electromagnetic leakages in CMOS (Complementary Metal Oxide Semiconductor) devices. Section *Electromagnetic probes* describes the electromagnetic probes and realized testbed. Next chapter describes the thorough EM analysis of operation `AddRoundKEy`. On the result, next chapter built description the results obtained from the comparison of probes. Evaluation of the results is in *conclusion*.

Side channel sources

Most modern cryptographic equipments are based on CMOS technology. The basic element of this logic is the inverter [2]. 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,



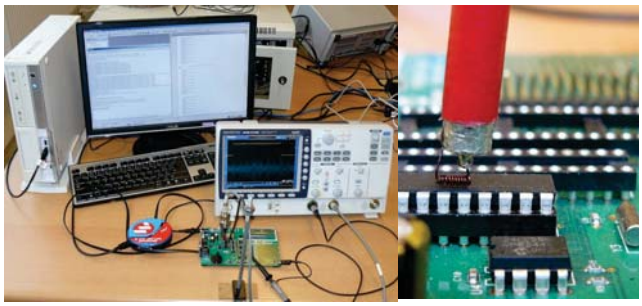


Fig. 2. Diagram of the testbed.

- 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]:

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

where C is the parasitic capacity, $P_{0\to 1}$ 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 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. Ways of EM radiation emitted by integrated circuits (IC) are the following:

- conductive emissions - 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. 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.

Fig. 3. Electromagnetic probes

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 magnetic near field. The advantage of these probes is that they can be placed as close as possible to the source of radiation and increasing the measurement accuracy. If the probe is placed further away it is possible to detect detected the microprocessor clock signal. Useful EM signals, which are dependent on the processed data, can be captured in areas of the processor and the memory of cryptosystem [11].

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 infnitesimal 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:

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

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

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 eguatins 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 be process still 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 a 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. From these assumptions it follows that the size of the induced voltage will be affected of probe position (angle) and microchip.

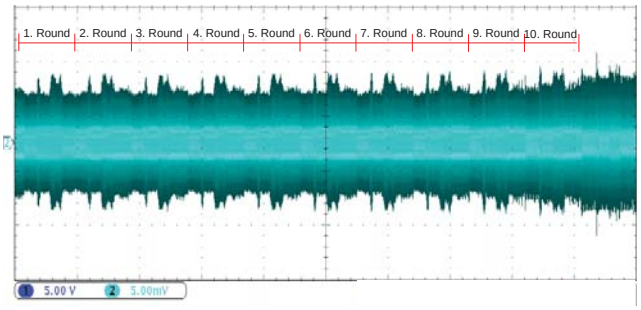


Fig. 4. Measured EM signal of whole AES algorith

Electromagnetic probes

The probes were realized to measure magnetic part of electromagnetic field in the near field according to the findings from the previous chapter. Finally four probes were made and solder to approximately 3 cm long semi-rigid coaxial cable with characteristic impedance 50 Ω with N connector. The various probes have been manufactured as follows:

- Probe 1: It was made of copper wire of diameter $d = 0.15$ mm with 6 turns reeled in the shape of the solenoid with an inner diameter of 0.7 mm (figure 3).
- Probe 2: It was made of copper wire of diameter $d = 0.15$ mm with 10 turns reeled in the shape of the solenoid with an inner diameter of 0.7 mm.
- Probe 3: It was made of copper wire of diameter $d = 0.3$ mm with 10 turns reeled in the shape of the solenoid with an inner diameter of 0.7 mm.
- Probe 4: It was made of copper wire of diameter $d = 0.3$ mm with 6 turns reeled in the shape of the solenoid with an inner diameter of 0.7 mm.

The testbed focused on the measuring direct emissions was built to verify characteristic of probes. Diagram of the testbed is shown in figure 2 and was designed from the following devices:

- cryptographic module: PIC16F84 microcontroller.
- Personal computer with installed software MPLAB allowed work with the programmer ICD2.
- Electromagnetic probe: Hand made electromagnetic probe for sensing near EM field.
- ICD2 programing device: Programing device for PIC microcontrollers with USB and RS-232 interfaces.
- Development board: PICDEM 2 PLUS to verify the functionality of 18, 28 and 40 pin microcontrollers.
- Oscilloscope: Dual-channel digital oscilloscope DPO-4032 by the company Tektronix with a maximum sampling frequency of 2.5GSa/s.

The measurement results

The whole encryption algorithm AES was implemented to the cryptographic module PIC16f84A. Figure 4 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. This direct observation of traces is based on the following facts. All algorithms that run on cryptographic devices are performed successively in a defined sequence. 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 in-

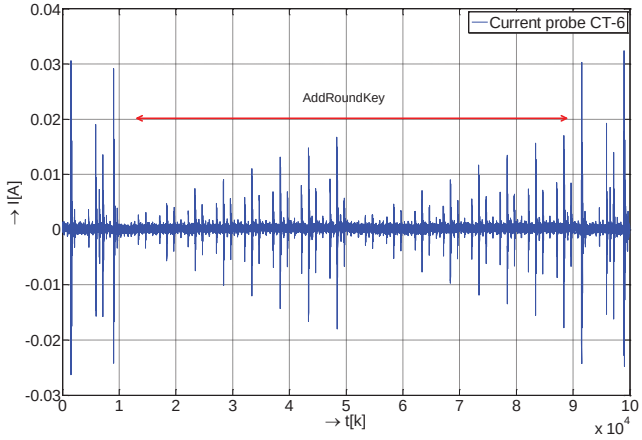


Fig. 5. Current consumption of `AddRoundKeys`

struction (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). We focused our investigation of the influence of various parameters on on short time of algorithm namely on most operation `AddRoundKey`. The implementation of AES algorithm was done in assembler because we needed to have the algorithm and performing instruction fully controlled.

Operation AddRoundkey analysis

The first operation which is carried out is copying the input data block in AES. This copy is called state block and all operations are performed successively on this block. In the following text and source code, State register is marked with letter s, secret key is marked with letter k. `AddRoundKEy` operation performs `XOR` (eXclusive OR) with block (matrix) of plaintext **S** stored in state register and with secret key **K**. The result is saved again it to the state register **S**. In the original form, the AES algorithm works with data blocks of length 128 bits this means with 4x4 matrix of bytes. The `AddRoundKey` operation can be given by the following equations:

$$\mathbf{S}' = \mathbf{S} \otimes \mathbf{K} \tag{6}$$

$$\mathbf{S}' = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ s_5 & s_6 & s_7 & s_8 \\ s_9 & s_{10} & s_{11} & s_{12} \\ s_{13} & s_{14} & s_{15} & s_{16} \end{pmatrix} \otimes \begin{pmatrix} k_1 & k_2 & k_3 & k_4 \\ k_5 & k_6 & k_7 & k_8 \\ k_9 & k_{10} & k_{11} & k_{12} \\ k_{13} & k_{14} & k_{15} & k_{16} \end{pmatrix}$$

Implementation in Assembler consisted two instructions, the first instruction loaded key value into the working register and the second instructions carry out `XOR` operation of state register and working register. The part of implementation is given below:

```
;Operation AddRoundKey
bsf Sync
movf k1,w     movf k15,w
xorwf s1,f     xorwf s15,f
movf k2,w     movf k16,w
xorwf s2,f     xorwf s16,f
...
bcf Sync
goto SubByte
```

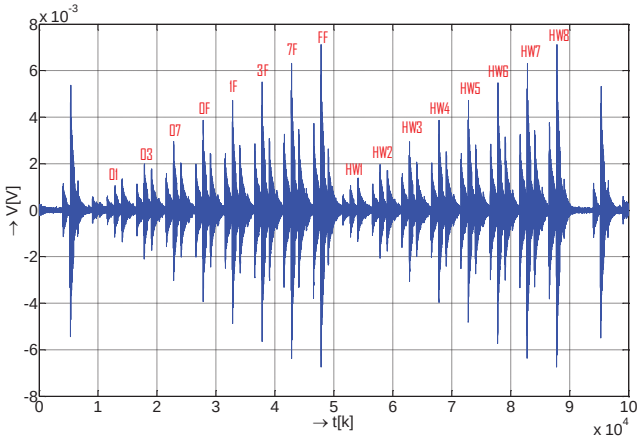


Fig. 6. EM trace of *AddRoundKeys*

In our experiment, the whole matrix of plain text **S** was set to FFh values and the matrix of secret key **K** was filled with various data. Data have value from 01h to FFh, were Hamming weight w of the next element is always greater one compared to the previous element. For example, the first value of secret key k_1 was equated 01h (B'00000001') thus the value of Hamming weight is $w(k_1)$ = 1. The following element had the value 03h (B'00000011') of the matrix thus the $w(k_1)$ = 2 and so on. The last element k_{16} takes the value FFh (B'11111111'), were $w(k_{16})$ = 8. Matrix of secret key **K** looked as follows (hexadecimal notation):

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

Electromagnetic field was measured during the execution of the algorithm and the data was recorded with oscilloscope and subsequently evaluated. The theoretical knowledge was observed on waveforms. The result of our measurement is the waveform shown in figure 6. 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. The increasing Hamming weight of the secret key is corresponding with electromagnetic peaks. We marked the corresponding peaks on measured waveform, first in hexadecimal notation and then Hamming weight. Subsequent examination regarding to the measured probes is aimed only at the highest voltage value in **highest peak**. The highest peak marked by FF in figure 6.

An Instruction Cycle consists of four clock cycles (Q1, Q2, Q3, and Q4). Fetch takes one instruction cycle while decode and execute takes another instruction cycle. However, due to Pipelining, each instruction effectively executes in one cycle except branching program instructions. The instruction fetch begins with the program counter incrementing in Q1. In the execution cycle, the fetched instruction is latched into the Instruction Register (IR) in cycle Q1. This instruction is then decoded and executed during the Q2, Q3, and Q4 cycles. Data memory is read during Q2 (operand read) and written during Q4 (destination write).

Figure 7 shows the thorough analysis of `AddRoundKey` EM trace. We marked different instruction, clock signal and sync signal which corresponds the source code of the program. At first sight, correlation is evident between the EM trace and performed instructions. For example, when the instruction `bcf` is performing which sets sync signal to zero,

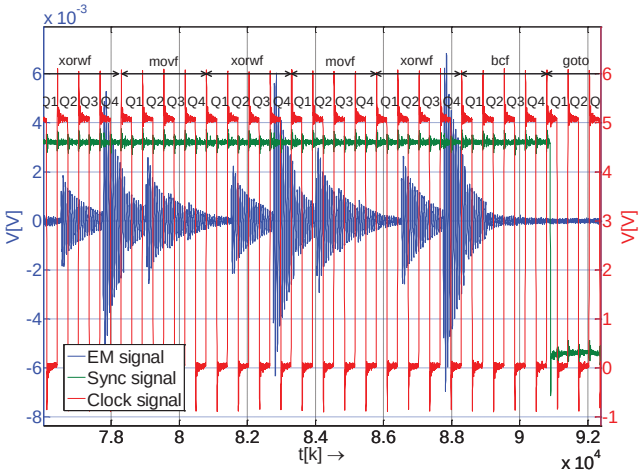


Fig. 7. Detail of `AddRoundKEy` EM trace

no data is loaded into the register as operation `mov`. Therefore the EM finger print is completely missing behind `XOR`. For sure we measured current consumption of the same microprocessor which performed identical data. The measured current consumption is shown in figure 5. From comparison of traces is clear that measured EM field corresponding with current consumption.

Comparison of the individual probes

The first measurements have been focused on comparisons of size inducted voltage for each probes. Comparison of probes was evaluated according to how much useful information is affected by the noise. The measurement was carried out as we described in previous chapters and the results are written only for maximal value of the highest peak in EM trace operation `AddRoundKey`. The maximum values of the inducted voltage for individuals probes are written to the table 1.

The results show that the Probe 3 induced the maximum voltage value. This is caused by the probe has 10 turns and form results, it was evident that it has the greatest impact to the size of the induced voltage. The following experiments were performed with probe 3 because the value of induced voltage is the largest and as well wire diameter was also greater ($d = 0.3$ mm). It was not have decisive influence to induction, but it proved that it is advantageous for probe manipulation. Because of frequent manipulation causing bending or breaking off the wire by probes with a smaller diameter wire.

Table 1. Maximum value of induced voltage

	Number of turns	Diameter wire [mm]	Induced voltage [mV]
Probe1	6	0.15	3.736
Probe2	10	0.15	4.614
Probe3	10	0.3	6.412
Probe4	6	0.3	3.658

Influence of distance the coil to microprocessor

In this measurement was measured induced voltage in the coil depending on the distance the measuring coil to the surface of microprocessor. The microprocessor was for measurement EM field slightly mechanically modified. The upper layers were abraded as shown in figure 8 to put the probe as close as possible to the chip. The reference position is considered the position where the measuring coil enclosed

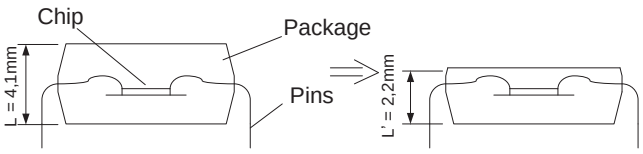


Fig. 8. Thinning of package

tightly to the surface of microprocessor. Subsequently vertical distance was increased. The size of the induced voltage decreases exponentially with increasing distance from the surface microprocessor. The table 2 are given the measured maximum peak voltage for each distance.

Table 2. The dependence of the level of induced voltage on the distance

Distance [mm]	Induced voltage [mV]
Reference	7,564
1	4,260
2	2,712
3	2,225
4	1,758
5	1,322
6	1,185

The results show that the measuring coil should be placed as close as possible to the cryptographic device. In this specific case, we can declare that the measurement would be carried out successfully on unmodified microprocessor or smart card. However, the removing (thinning) of the package we get better results. The boundary of feasibility is approximately in the distance somewhere between 3 to 5 mm from the device. Generally, success of realization depend on the implementation of specific equipment, quality and possibly sensing apparatus. The measured signal can be filtered or amplified and so on.

Conclusion

In this paper, we described the electromagnetic side channels sources and electromagnetic field of the microprocessor. We realized the testbed with cryptographic module performed the AES algorithm. At first measurement, we analyzed whole EM trace of whole algorithm AES and subsequently, we focused our measurement on operation `AddRoundKey`. We performed a thorough analysis of measured EM signal and we analyzed every performing instruction of microprocessor in EM signal which corresponded with the source code. At first sight, correlation is evident between the EM trace and performed instructions. For sure we measured current consumption of the same microprocessor which performed identical data. From comparison of traces is clear that measured EM field corresponding with current consumption.

After this deep analysis, we were sure that we measure EM signal corresponding to the current consumption and we continued to analyze the influence of parameters on the measured EM waveform. On the measured waveforms of the electromagnetic field was studied the influence of probe construction namely two parameters wire diameter and number of turns. The results of measurement show that that the main influence have the number of turns. Practical experiments have shown that the greater wire diameter is advantageous for probe manipulation but has no significant effect to the size of the induced voltage. In next measurement was measured induced voltage depending on the distance to microprocessor. The size of the induced voltage decreases exponentially with increasing distance from the surface microprocessor according Biot-Savart law. The results show that the measuring coil should be placed as close as possible to the cryptographic device. The boundary of feasibility is approximately in the distance somewhere between 3 to 5 mm from the device. The last measurement dealt with position of probe and microchip.

REFERENCES

[1] Agrawal D., Archambeault B., Rao J., Rohatgi P.: The EM Side Channel(s), 2003, pp. 29–45.

[2] Alioto M., Giancane L., Scotti G., Trifiletti A.: 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.

[3] Koç Ç. K., Rothatgi P., Schindler W., Walter C. D.: *Cryptographic Engineering*, 2009.

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

[5] Gandolfi K., Mourtel C., Olivier F.: 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.

[6] Gandolfi K., Naccache D., Paar C., Mourtel C., Olivier F.: Electromagnetic analysis: Concrete results, 2001.

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

[8] Martinasek Z., Macha T., Raso O., Martinasek J., Silhavy P.: 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`

[9] Martinasek Z., Macha T., Stancikk P.: Power side channel information measurement, in *Research in telecommunication technologies RTT2010*, September 2010.

[10] Martinasek Z., Petrik T., Stancik P.: Conditions affecting the measurement of power analysis, in *Research in telecommunication technologies RTT2011*, September 2011.

[11] Peeters E., Standaert F. X., Quisquater J. J.: Power and electromagnetic analysis: Improved model, consequences and comparisons, *Integration, the VLSI Journal*, vol. 40, no. 1, pp. 52 – 60, 2007, embedded Cryptographic Hardware.

[12] Quisquater J. J., Samyde D.: 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.

[13] Struif B.: 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`

***Authors**: Zdenek Martinasek, Vaclav Zeman, Petr Sysel, Department of Telecommunications, Faculty of Electrical Engineering and Comunication, Brno University of Technology, Purkynova 118, 612 00 Brno, Czech Republic, email: martnasek@feec.vutbr.cz, zeman@feec.vutbr.cz, sysel@feec.vutbr.cz Krisztina Trasy, Department of Garden and Open Space Design, Faculty of Landscape Architecture, Corvinus University of Budapest, email: krisztina.trasy@stud.uni-corvinus.hu*

Acknowledgement

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 and FR-TI2/220. The described research was performed in laboratories supported by the SIX project; the registration number CZ.1.05/2.1.00/03.0072, the operational program Research and Development for Innovation.