AENSI Journals

Advances in Environmental Biology

ISSN-1995-0756 EISSN-1998-1066

Journal home page: http://www.aensiweb.com/aeb.html

Increasing the Security of Smart Cards Against Power Analysis Attacks

[1]Seyed Mehdi Dadgar, [2]M. Reza Salehnamadi and [3]Somayeh Farhang Adib

[1]Faculty member of computer department of Sama technical and vocational training college, Islamic Azad University, Roudehen Branch, Roudehen, Iran.
[2]Department of computer engineering, Faculty of engineering, south Tehran branch, Islamic Azad University, Tehran, Iran.
[3]Master of Information technology engineering, Qom University, Iran.

ARTICLE INFO

Article history:
Received 23 January 2014
Received in revised form 19 April 2014
Accepted 6 April 2014
Available online 15 May 2014

Key words:
Security, power analysis attack, smart card, power consumption, FPGA, Interconnection networks.

ABSTRACT

One of the most important aspect of smart cards is the security of smart cards. In this paper we will investigate the security of smart cards and its formal attacks firstly. One type of attacks is Power Analysis attack. This type of attack is divided to 3 models: Simple, Differential and Correlation power analysis attacks, which, Differential power analysis attack is the most perilous. In this type of attack, the attacker guesses the data by measuring power consumption of card several times and comparing to each other and analyzing the results and so the important information on card is discovered. The main idea of paper is that data path, even for same data, is different form last data path, and so different power consumptions. It is proved by using a FPGA and an interconnection network implementation on it. Finally we simulate and compare it with other methods and give some results.

To Cite This Article: Seyed Mehdi Dadgar, M. Reza Salehnamadi and Somayeh Farhang Adib., Increasing the Security of Smart Cards Against Power Analysis Attacks. ***Adv. Environ. Biol., 8(5),*** *1301-1308, 2014*

INTRODUCTION

Now a day almost everyone uses a smart card with a wide variety of applications ranging from bank cards tophone cards. Smart card is a card of PVC kind with dimensions about 5.5 in 8.5 CM which is placed memory and microprocessor chips for storing data and processing them on. Placing one chip in card instead of magnetic tape, changes it into a smart card with various applications. These cards provide the possibility of processing because of having chip, being able to control the function and keeping personal information as well [3].

Smart cards play a crucial role in many security systems. These devices typicallyoperate in hostile environments and, therefore, the data they contain might berelatively easily compromised. For example, their physical accessibility sometimesallows a number of very powerful attacks against their implementation. During the last decade, side-channel attacks in general, and power analysis attacksin particular, have shaken the belief in the security of smart cards [7].

Smart card was invented in 1968 by a German scientist of rocket sciences (Helmut Grotroupe) and his colleague (Yorgen Dethlough) but it was recorded by a French person was called Ronald Mornoo in 1974. Since then, companies such as Honey well, Motorola got through an activity in this field and as a result of their activities, thefirst microprocessor based smart card was made in 1979 and the first standard was brought up for smart card in 1986 as a title of ISO 789116/1. First national level usage of Smart card was carried for phone credit cardsin France in 1986 [13].

The level of the security of smart cards evaluated by some standards such as TCSEC in the US and CCTTSE in Europe which have presented ISO 15408. This ISO is known by the name of common criteria or CC[8].

CC is a common criteria for evaluating IT products that include international standards related with the security of computer. Numerous threads introduced on smart cards after studying on smart cards that is presented methods for avoiding them.

In addition to Reverse engineering attack [11] and Micro probing attack [16] that are inherently physically methods, there are two other methods: timing analysis and power analysis. In timing analysis, the time of performing a program is a parameter that programmers are interested to decrease it. Surprisingly, the time of processing information is usually different by systemof cryptography.In timing analyzing attack, thetime measurements of algorithm execution are fed to a statistical model with many inputs. Then with calculating of

Corresponding Author: M. Reza Salehnamadi, Faculty member of Islamic Azad University, south Tehran branch, Tehran, Iran.
E-mail: m_saleh@azad.ac.ir, Tel: +98219351045323

correlation between the various measurements or the variance of measurements, guess some key bits. Number of samples for a successful attack depends on the signal to noise ratio of system. A larger amount of sample will be needed if this ratio is low [8].

Power analysis is one of the most important existed invasions on smart card whom the attacker guesses what data is processing by the consumption power of card and some comparisons. Based on ISO15408, there are three type of threats on intelligent cards: social, physical and logical. Social concerns with people who use the cards, physical aspect concerns with blocks of cards like as microcontroller and logical aspect concerns with computing, cryptography and so on. There are two types of Physical attacks: static (controller is off) and dynamic (controller is on and system is working). Most of attacks are dynamic type. Power analysis attack checks the power consumption of microcontroller and hence is a physical type, but meanwhile it is a logical types since it is going to detects the keys. It will be described in detail in next section.

The rest of paper is structured as follows: Section 2 presents the power consumption and MIN concepts, outlines an proposed system. Section 3 presents simulation results, Section 4 presents comparative analysis and final section draws conclusion.

Power consumption analysis:

Secause there is a correlation between executed instruction in card and its power consumption, the power consumption of chip can define what function is performing and causes is revealing some information. Along with the clock frequency, the power consumption of smart card is measurable simply at tow ended terminal (figure 1). A small resistor will be held with card serially and its current will be measured. Attack to system will be possible with sending samples to PC for analysis[10].

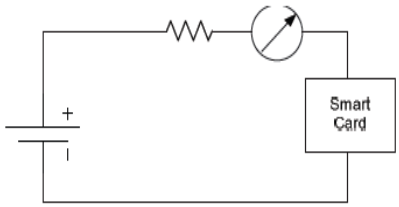


Fig. 1: The way of obtain the card voltage.

For more clarity, imagine a sequence of special program with a series of information produces a special graph of similar current in time. If that program is performed with another data the current-time graph will be varied. By using this graph variation, you can find that which data is running.There are three types for attack of power analysis: Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis (CPA).

Simple Power Analysis (SPA): this attack directly uses measurements of consumption power during the execution. The patterns of power or hardware consumption energy can gives to attacker some important information on instructions and their execute sequencing. The main idea in SPA is that some executed instructions by microcontroller (like jump and memory access) change the current intensity very much [5]. Kohen could discover the password of a Mc68H with SPA successfully [14].

Differential Power Analysis (DPA): it is one of most dangerous attack to smartcards and is more accurate than SPA. In DPA, amount of consumption is measured when the known data is running and then it is measured when the unknown data is running. These measurements will be repeated several times to reduce the average noise effects. When the measurements were completed, the differences are calculated and the related results to unknown data will be extracted.In this method, the number of measurements is very effective in increasing the accuracy of attacker's prediction. This amount differs in different cards and obtains from following formula:

$$N= \frac{8\sigma^2+\varepsilon^2(\alpha m+m-1)}{\varepsilon^2.SNR^2}$$

In this equation "σ" is the maximum voltage of entered noise in system, "ε" is the maximum voltage of spike points, "m" is the number of these spike points in a pulse and "SNR" is the signal to microcontroller noiseratio. For example, in a real measurement sample for a special card following amounts were obtained: [13] σ= 7.5 mv, ε=6.5 mv, m=8, α=0, SNR=0.67. Whit these amounts "N" will be 40. It means that theminority amounts of sampling should be 40 for this especial card.

Correlation Power Analysis (CPA): CPA is another kind of power analysis attack which implements on cards that are encrypted with DES algorithm. With much investigation on DPA, you can find a great relation between calculated powers and produced hamming weight on DES algorithm. So you can think about an attack on the base of this relation. So you can guess hamming code from power consumption and finally the key of encryption algorithm will reveal[1].

Some hardware approaches are discussed to deal with power analysis[17]. For example:

Create a noise and parasite producer which changes the consume pattern.Disadvantage is: It has an expensive implementation. Its implementation always is not possible especially on traditional systems. It might be inactivated easily by manipulation.

Filtering of consume signals: putting some filter through the path of microcontroller current. Disadvantage is: It needs a basic change in hardware.Itmight be inactivated easily by manipulation. Filtering may causes some limitations. It causes some changes in power supply.

Putting a detachable power supply: Disadvantage is: Its implementation always is not possible especially on traditional systems. The signals can lake from the other ways. It causes some changes in power supply.

Putting a high speed voltage regulator in the chip which uses from a resistor sensor for micro current supervision. Dsadvantage is: It has an expensive implementation. It consumes a lot of energy in card.

Design a modified processor in order to supply a fixed current. Disadvantages: It has an expensive implementation. It needs a basic change in hardware. It consumes a lot of energy in card[12].

Activate of some parts of the microcontroller which their functions are not needed when power analysis execution. For this purpose you can use from CRC code convertor and a coprocessor. It needs a basic change in hardware. It consumes a lot of energy in card.Disadvantage is: Its implementation always is not possible especially on traditional systems[2].

Software approaches to deal with power analysis: the simplest way of using that group of machine instructions which have similar consumption.

Having several different random processors for performing similar calculations in a hidden algorithm[4]. The random performing of instruction of NO-OP in different points of program is another way for disrupting the pattern of consumption power [2].

Martinasek describes an innovative method of the power analysis which presents the typical example of successful

Attacks against trusted cryptographic devices such as RFID (Radio-Frequency IDentification) and contact smart cards. The proposed method analyzes power consumption of the AES (Advanced Encryption Standard) algorithm with a neural network, which successively classifies the first byte of the secret key [9].

Multistage Interconnection Networks:

In general, some elements connecting to each other by communication network. These elements can be computers, processors and etc. in parallel processing systems, communication networks are so important, till the most important factor in determining the source of system performance and cost are mentioned. The idea of Multistage Interconnection Network (MIN) has been formed in this regard and at first it was the main purpose of the non-blocking switching designed with fewer switching elements rather than cross-switched networks.MIN in terms of arrangement, number of stages and the way of connecting outputs of switch elements on the next stage has different types[6].

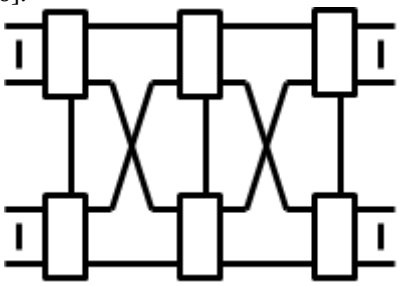


Fig. 2: One sample of a MIN with N×N dimensions.

The proposed model:

To prevent the power analysis attack, a mechanism is presented and is discussed in this paper. The proposed hardware model is based on that when data is sent to the card, power consumption is varied from beginning to end of processing. It means, if a fixed data for two or more consecutive is sent to cards and every time which attacker measures the amount of power, some different answers will be appearand attacker could not find data. In this context, the whole chip of card should be implemented on a programmable chip, that isField Programmable Logic Gate Array or FPGA in this model. It means the CPU, memory, ports are all designed on FPGA[15].

A communication network should be placed on chip at the beginning of the data. Communication network has asimple structure like figure (4).

It must be noted that this network can be one of the famous networks such as Omega, Cube, Clos and etc. however, the above model is very simple and low consumption network. Switches are 1x2 switches (1 input and 2 outputs) so they can be 1x2 De multiplexer.

Advances in Environmental Biology, 8(5) April 2014, Pages: 1301-1308

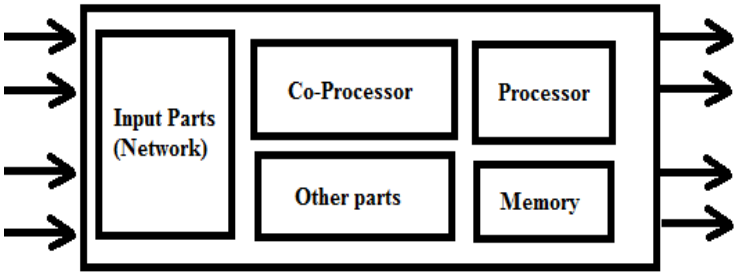


Fig. 3: Internal architecture of FPGA in our model.

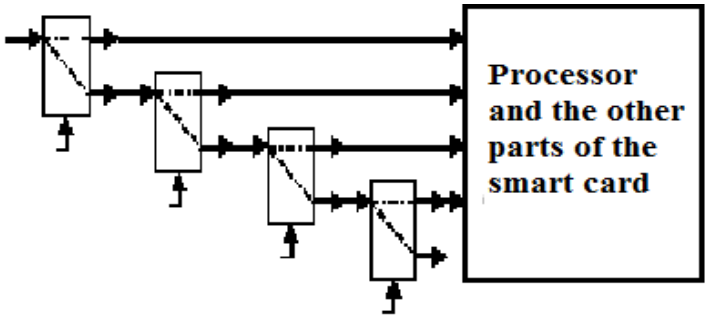


Fig. 4: Interconnection Network On Chip.

The primary input line is set to enter the data in a two ways. One path that leads directly into a processor (that we call it direct) and the second way is that the next switch (we call it indirect). If data is entered directly into the processor through one switch, the power consumption will be only one switch consumption amount. But if it is going to the next switch there are two ways again direct and indirect which they have different consumptions. So if we investigate all of the available paths we will see none of the paths are the same and as a result, the power consumption of a particular choice, depending on the directions, will vary.

So even if a fixed data is inserted several times in card, the attacker will see different amount of consumptions and probability of guessing from pattern of consumption will be decreased.

In the figure 4 example, there are four different paths in term of network energy consumption would be as follow:

The first pathway: the first switch is directly and the data is given into the processor.

The second pathway: the first switch is indirect, the second switch is direct and the data enters the processors.

The third pathway: first and second switches are indirect, the third switch is directly and the data enters the processor.

The forth pathway: first, second and third switches are indirect and the forth switch is directly and data enters the processor.

Existing routes determination: One of the four pathwill be selected. As mentioned, each of the switches has a chip select which determines direct and indirect mode.

The important note is that in a special time, only one switch should be in direct mode and the others should be set in indirect mode. As a result, we can use a 2x4 Decoder (figure 5).

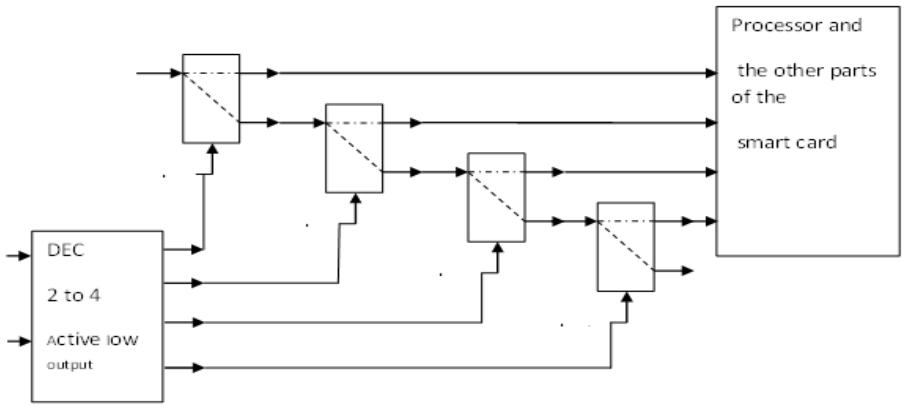
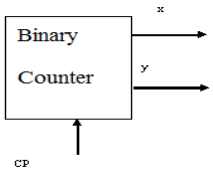


Fig. 5: Selecting the mode of each switch.

Decoder cause to have only one active output and just one switch will be in direct mode. Setting inputs x,y: to set inputs x,y we can use a two-bit binary counter that takes a binary number in any pulse. Just, we should connect a crystal to our counter. Figure (6) shows that its outputs should connect to decoder inputs.



CP	1	2	3	4	5	6
X	0	0	1	1	0	0
Y	0	1	0	1	0	1

Fig. 6: Selecting Inputs of Decoder(x,y).

Simulation and evaluation:

The proposed model was simulated in Electronic Work Bench. As shown in figure (7), we use a Signal Generator as a 2-bits binary clock input that we mentioned it before.

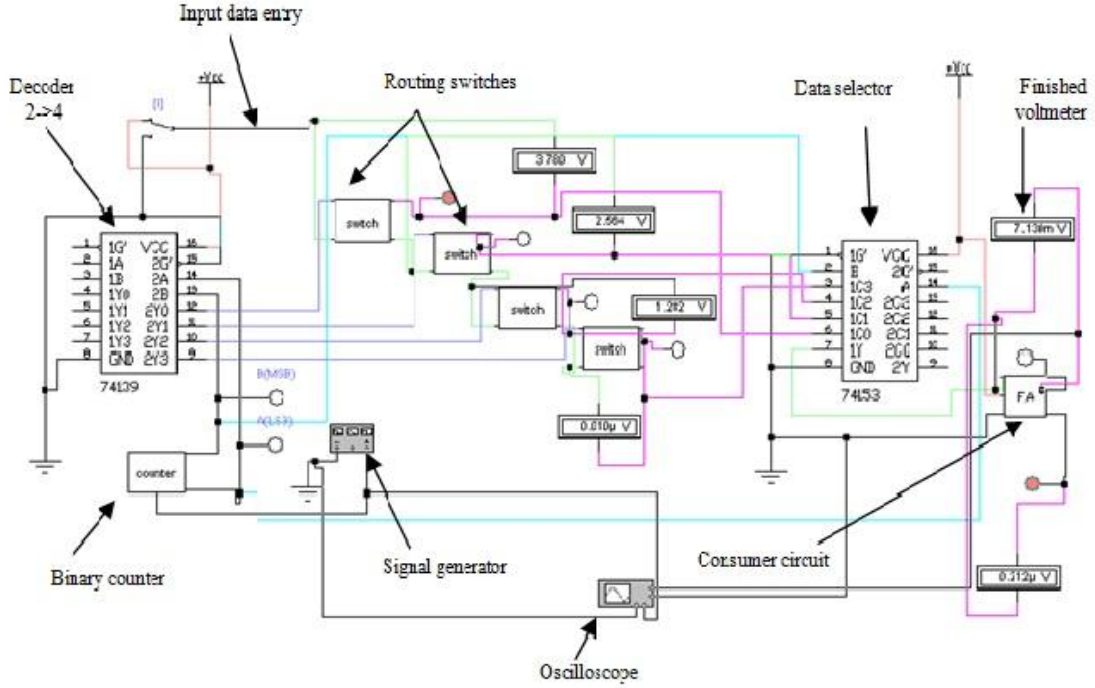


Fig. 7: Implementation of proposed model in simulation environment.

The output of counter is connected to the inputs of a Decoder with active low output (74139). The outputs of this IC are the select inputs of our switch that they determine the reaction of our switch. We connect one of the outputs of direct mode which should go to microprocessor directly, to one of the input of a full adder which is used as a simple circuit. We use a simple circuit like full adder because we just want to see the result of elimination. In fact and according to our idea, no difference between full adder and microprocessor.Of course, we use a 4-1 multiplexer (74153) to select one of the 4-input wires which should go to consumer circuit.We use some voltmeters and LEDs on some points that are shown on the figure (7) for outputs observation. One 2-chanell oscilloscope is used for view the frequency and voltage of input and output. After simulation, the following observations in table (1) are created. As it is determined in table (1), after some clock pulse, the voltage of switches is stable (or with a little change) but the voltage of the consumer circuit (which is a full adder in our model) has a great change so you can see the different range of voltage changes in first 110 clock pulses. This is exactly the same thing that we expect it. It means that, the routine of power consumption analysis is eliminated.

If we draw the diagram of these results in Math lab we can see this elimination of power consumption. So we did this operation in math lab 7.1 and gave a diagram which is shown in figure (8). Do not forget that: our input is just one bit that is controlled by a key in this simulation. If we increase the number of inputs, we will see our changes are more different and varied.

Table 1: Results of simulation.

Clock Pulse	Time(s)	Voltage(v) First switch	Voltage(v) second switch	Voltage(v) Third switch	Voltage(v) Forth switch	Output Voltage(v) (Full Adder)
3	6	4.9	140.1 m	0.001µ	0.0	1.49
12	25	4.25	1.63	810.8 m	0.006 µ	2.38
20	44	3.89	2.43	1.182	0.009 µ	1.06
40	90	3.74	2.55	1.297	0.010 µ	106 m
60	135	3.71	2.43	1.235	0.89 µ	9.17 m
84	184	3.74	2.56	1.298	0.01 µ	1.23 m
110	234	3.7	2.46	1.266	0.01 µ	1.21 m

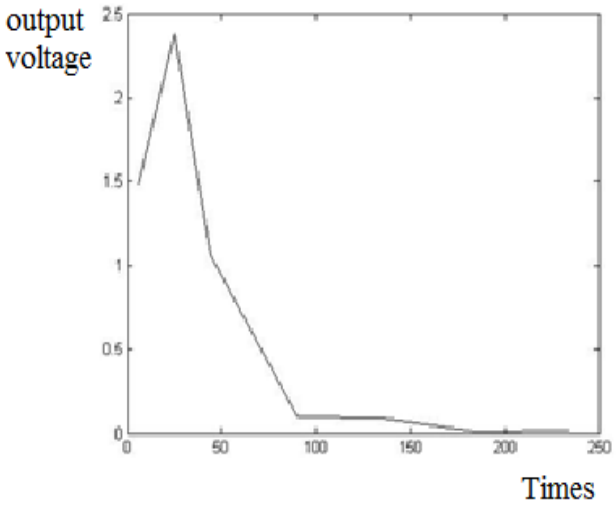


Fig. 8: Output voltage diagram.

Comparison with other solutions:

This section compares the proposed model with the other hardware solutions against power analysis attacks, which were interpreted in pervious sections:

In embedding a high speed chip voltage regulator solution which uses a micro flow sensor for monitoring resistance, the idea of using energy regulators to disrupt social order and therefore no diagnosis was given power when using chip regulator, because it will be constant and after several sampling is detectable, it is a weaker model than our model. Because we have several ways to enter data and so several power consumptions which are different each time.

In using artificial noise generators on chip solution and designing a processor to support a steady and non-modified current solution, the energy consumption of microcontroller will increase largely, which are not suitable in some telecommunication uses. Since each of these units is hardware independent units, therefore working on them for guess their behavior in face of the different is not impossible and a clever attacker can attack to it. There is a complete comparison in table (2) between them. One of the positive points of our proposed model is that we implement our model on FPGA. FPGA is one IC that is an easily programmable using hardware description languages. Using this IC is affordable in cost and exposure of sea of programmable gates causes a high volume of hardware be implemented on it and circuit size can be reduced. Using hardware description language on this IC, easy to implementation any plan on it with any algorithm. We also use FPGA to design it and this cause all units (processor, RAM and etc) along with the proposed network will be placed in a hidden or the other words, which all these things are on a chip. It means our added unit does not have any separate essence that can be have any separate studies to explore the impact of power. It is inferred that the entire of IC, is a smart card IC and each time measurement is possible (even with a fixed data and a fixed set of instructions) a different value is shown which there is not any chance to guess data. Another positive point is that because of all the plan is implemented on a single FPGA chip by software codes, the energy consumption reduces very much. However we should say that this model maybe has some negative points. For example because of the entire of plan likes processor, memory, networks, ports and etc are implemented on a FPGA, it is possible we need a larger FPGA and there are some economic problems. Another drawback is the possibility that the speed of the circuits designed by FPGA is relatively lower than real hardware models. It maybe causes some problems in cases of high-frequency switching networks. So might cause loss or interference pockets.

Table 2: Comparison of proposed model with other solutions.

Approach	Cost of implementation	Implementation possibility	Inactivated easily by manipulation	needs a basic change in hardware	signals can lake from the other ways	consuming a lot of energy
Artificial noise generators	expensive	Yes but difficult	Yes	No	No	Yes
Filtering	cheap	yes	Yes	Yes	Yes	No
Putting regulator	expensive	yes	Yes	Yes	Yes	No
Modified processor	Very expensive	No	No	Yes	No	Yes
Activate some unnecessary parts	cheap	Yes but difficult	No	Yes	Yes	Yes
Our model	cheap	Yes but difficult	No	Yes	No	No

Conclusion:

we have investigated the security of smart cards and Power Analysis attack. In this type of attack, the attacker guesses the data from power consumption of card by measuring them in several times and comparing to each other and analyzing the results and so the important information on card. To prevent the power analysis attack, a mechanism is presented and is discussed in this paper. We used in our proposed idea a FPGA and an interconnection network implementation on it. Every time which data comes to this network, it will be sent on a different path and as a result we can see different power consumption. Simulation proved our design capability in compareto other methods which are available.

This model can be implement on a FPGA IC. In future we can implement an encryption real algorithm like Data Encryption Standard (DES) or Advance Encryption Standard (AES) on it.With this routine elimination of power consumption, it is impossible to measure the power consumption and so the attacker cannot guess some data like the key, instructions and etc.

REFERENCES

[1] Brier, E., C. Clavier and F. Olivier, 2004. "Correlation Power Analysis with a Leakage Model". Springer Berlin /Heidelberg.

[2] Dragoni, N., O. Gadyatskaya, F. Massacci, 2010. "Can We Support Applications' Evaluation in Multi-application Smart Cards by security-by-contract?". 4thIFIP WG 11.2 International Workshop, WISTP, Passau, Germany, April12-14, 2010, pp: 221-218.

[3] Furletti, M., 2002. "An Overview of Smart Card Technology and Markets". Federal Reverse Bank of Philla payment cards center discussion paper No.02-14.

[4] Guilley, S., L. Sauvage, F. Flament, V. Vong, P. Hoogvorst, R. Pacalet, 2010. "Evaluation of power constant dual-rail logics countermeasures against DPA with design time security metrics", IEEE Transactions on Computers, 59(1250-1263).

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

[6] Kruskal, C.P., 2003. "Performance of Multistage Interconnection Network forMultiprocessor", IEEE.

[7] Maghrebi, H., O. Rioul, S. Guilley and J. Danger, 2012. "Comparison between Side-Channel Analysis Distinguishers", ICICS 2012, Springer-Verlag Berlin Heidelberg , 2012LNCS 7618, pp: 331-340.

[8] Mangard, S., E. Oswald, T. Popp, 2007. "Power Analysis Attacks: Revealing the Secretsof Smart Cards", Germany, Berlin conference, pp: 243-256.

[9] Martinasek, Z., V. Zeman, 2013. "Innovative Method of the Power Analysis", Radio Engineering, 22(2): 586-594.

[10] Moradi, A., M. Shalmani, M. Salmasizadeh, 2009. "Dual-rail transition logic: A logic style for counteracting power analysis attacks", Computers and Electrical Engineering, 35: 359-369.

[11] Naeem, A., K. Markantonakis, K. Mayes, 2010. "A Dynamic and Ubiquitous Smart Card Security Assurance and Validation Mechanism. Information Security GroupSmart card Centre", Royal Holloway, University of London Egham, Surrey, United Kingdom.

[12] Rossudowski, A., H. Venter, J. Eloja, 2007. "Personal Anomaly-based Intrusion Detection Smart Card Using Behavioral Analysis"Informationand Computer Security Architectures Research Group (ICSA) Department of Computer Science, University of Pretoria, South Africa.

[13] Standaert, F., T. Malkin, M. Yung, 2009. "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks". Lecture Notes in Computer Science, 5479: 443-461. Springer, Heidelberg.

[14] Skorobogatov, S., M. Kuhn, 2005. "Power analysis of the Motorola MC68HC908AZ60A microcontroller," University of Cambridge, Tech. Rep.

[15] Velegalati, R., P. Yalla, 2008. "Differential Power Analysis Attack on FPGA Implementation of AES". George Mason University publisher.

[16] Vermoen, D., M. Witteman, G. Gaydadjiev, 2007. "Reverse Engineering Java Card Applets Using Power Analysis" Computer Engineering, TU Delft, The Netherlands.
[17] Zhang, D., X. Liao, M. Qiu, J. Hu, E.H. Sha, 2012. "Randomized execution algorithms for smart cards to resist power analysis attacks". Journal of system architecture, 58(10): 426-438.