

A Study on Information Security Attack based Side-Channel Attacks

Young-Jin Kang*, Ndibanje Bruce*, SuHyun Park**, HoonJae Lee**

*Dept. Ubiquitous It, Dongseo University, Busan, Rep. of KOREA

**Div. Of Information and Communication Engineering, Busan, Rep. of KOREA

rkddudwls55@gmail.com, ndibabruce@gmail.com, {subak, hjlee}@dongseo.ac.kr

Abstract— Electronics devices are always targeted with different kind of attacks due to their activities related to data processing, data storages and data transactions. In each case, the attacker performs the attack according to what he needs from the device. In this paper, we present various attacks types on electronics devices in particularly on crypto-module devices where we focus on side channel attacks in its form of attacks such as power analysis attack, electromagnetic attack and fault injection attack. Finally, we develop a series of countermeasures against the side-channels attacks on crypto-module devices where the result shows that they are resilient and achieve better efficient.

Keywords— Side-Channel Attacks, Physical Attacks, Hardware-based Countermeasure, Software-based Countermeasure, Hardware Device

I. INTRODUCTION

Nowadays, various technologies are combined in order to perform multitask function as the users make a high demand on the market. In this case the embedded industries together with different technologies are believed to be helpful in generating new business and products. The embedded market is expected to be approximately 22 trillion in the next five years by 9.1% to fast-growing type 27 trillion in 2017 to form a scale[1].

So far, the embedded industry is focusing on how the software is mounted or embedded on the hardware or equipment. However, due to the high and growth data transaction among the hardware devices such IoT (Internet of Things) sectors, the security has become more and more important. Especially the security of the Hardware devices is at high risk.

In this regards, hardware devices are vulnerable and are always targeted by attackers using physical attacks. In particular, physical attack refers to a method of attacking the memory (ROM, RAM, EEPROM), of the cryptographic module or the encryption device. Therefore, the most common classification is divided into invasive Attacks [2], Semi-invasive Attacks and Non-invasive Attacks as shown in Figure 1. Generally, the attack is built using a physical signal or unit for the device encryption algorithm or the device itself.

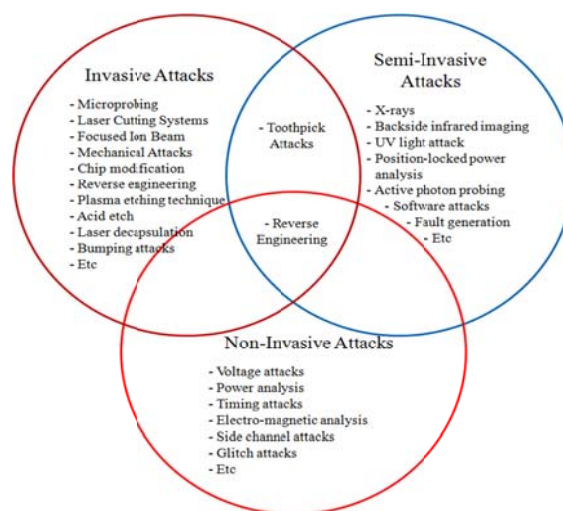


Figure 1. Classification of Physical Attacks

A. Invasive Attacks

Through direct access to the chip surface, the invasive attacks have to reverse engineering after observing the IC circuit operation. In this case the attacker must have micro probing interoperability skills in order to apply and perform such attack. Furthermore, the first step is always to remove a portion of the passivation layer of the chip. A typical example is micro probing, laser cutting.

B. Semi-Invasive Attacks

In order to get access to its surface, the semi-invasive attacks require depackaging the chip. However, the passivation layer of the chip remains intact, as semi-invasive methods do not require depassivation or creating contacts to the internal lines. This is because microprobing is not used for this attack technology and thus such expensive tools as laser cutters and FIBs are not required.

C. Non-Invasive Attacks

Non-invasive type attack is an attack method that uses timing information, power, electromagnetic signals, such as leaking from the encryption process, not a theoretical vulnerability in the cryptographic algorithm as a new form of attack called side-channel attack; the figure below is exposure

of the general encryption processing it shows the additional information.

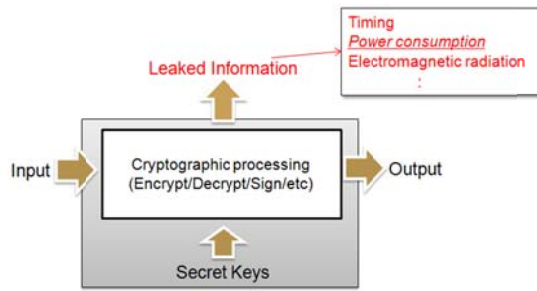


Figure 2. The Side-Channel Leakage Information

Physical attack has a variety of attacks techniques that are being introduced as very powerful attack. In this paper we describe the side-channel attack on electronics devices and we create a comparison table by analyzing the recently side channel attacks techniques and at the end we discuss about the countermeasures against these attacks.

II. OVERVIEW OF SIDE-CHANNEL ATTACKS

Side channels are the channels of information which are produced by a device in an un-intentional fashion. These channels provide to the cryptanalyst internal state information which was not available to the classical cryptanalyst. There are many types of attacks Side-channel attacks, and many studies have been worked in Electromagnetic Analysis, Power Analysis, Fault Injection Attack, and Timing Attack.

A. Electro-Magnetic Analysis Attack

This attack is as close to the coil to measure the radio wave radiation around the crypto device and the operation of each part of the device. The radio wave radiation from the device is thus obtained and can be treated in the same manner as power wave. However, it is necessary to remove in advance the package and the passivation layer of the device according to the actual measurement.

An example of information leaking from the EM radiation is proposed by Agrawal et al [3]. In fact, the attack is based on the EM has been known as a powerful means of intelligence activities, information on EM analysis has been constantly classification. According to Agrawal et al. given a distance to the crypto device (non-contact type) the EM attack is possible as well as the power to estimate the information for the side-channel.

B. Power Analysis Attack

The most powerful of the side-channel attack and representative is the power analysis method and has been reported to be the most powerful attack method that threatens over last 15 years after Paul Kocher [4] has proposed the attack on DES algorithm in 1998.

Power analysis attacks is based on Hamming weight model and the Hamming distance model, which is the power consumption of the target crypto device that has a high

correlation to the two models of the data bits to be processed during the operation. In addition, power analysis attacks are divided into simple power analysis attacks, differential power analysis attacks and correlation power analysis attack.

C. Timing Attack

This attack is mainly based on the time calculation for estimating the secret information. Many cases have performed on how to optimize the process such as program size reduction to shorten the processing time when implementing the cryptographic algorithms. The implementation of the device in this way it is possible to estimate the processing time information by monitoring the processing time which varies independent on the data. This is the principle of timing attacks.

D. Fault Injection Attack

Fault injection attack was first introduced by Bellcore Company [5] in 1996 as a kind of side-channel attack on RSA cryptography. The aim of this attack is to find out confidential information inside of the output values which has been intentioned injected by incorrect values inside of the chip and hardware for cryptographic operations. In general, an error may occur in a small hardware device as well as big equipment, such as the server of the certification authority.

Studies on Fault analysis have been reported on DES, AES, SEED, ARIA, RSA, ECC, which are the most cryptographic algorithms. In addition, the RSA cryptographic algorithm also has been reported to be attacked by CRT (Chinese Remainder Theorem).

III. ANALYSIS AND COMPARISON OF SIDE-CHANNEL ATTACKS

In this chapter, we present the experiment which has been analysed through the previous side-channel attack techniques. The result shows that the hardware devices are vulnerable to different attacks made on the equipment with the cryptographic algorithms.

Young-Jin Kang et al. [6] have proved the weakness of PingPong-128 key stream generator which increased outputs key stream of specific non-linearity by adding mutual clock-control structure to previous summation generator through Correlation power analysis attack. Construct experimental devices are the ATmega128 microprocessor and embark 8 bit calculation device and the PingPong-128 encoded algorithm, inside of ATmega128. In the process of encoded algorithm, intentionally synchronize the device and in that process of resynchronization, use digital oscilloscope to measure electrical signal. Then use computer's control program to collect and store measured electrical pattern. Measured power signal while PingPong-128 algorithm is operating, and used estimated correlation coefficient between estimated expended electricity and measured electrical signal to attack and find used encrypted middle key's first 8 bit. Furthermore, we apply the correlation coefficient for assumption of encrypted middle key's value of power consumption and measured power signal.

Jae deok Ji et al. [7] presented an attack on contactless smartcards by electromagnetic radiation which is a new modified of an existing attack method in an attack Electromagnetic disturbances (EMD). The ARIA algorithm specified in the standard cryptographic algorithm from republic of Korea was tested after equipped with the contactless smart card. After experiment, they obtain the entire 16-byte key used in the first round of the ARIA encryption by using the EMD side-channel analysis with 50,000 traces. These results show that the EMD side-channel analysis outperformed the more conventional power analysis technique.

Jung hwan Song et al. [8] described the fault injection attack attempted on the lightweight block cipher Piccolo-80, Piccolo-128 Algorithm. Fault analysis on the Piccolo has been launched by using cube attack (Cube attack was introduced by Dinur and Shamir) [11]. Cube attack is a chosen plaintext attack. The main idea of cube attack is to find linear equations consisting of secret variables by using cube sum.). They find 16 linear equations corresponding to a round function F of Piccolo by using cube attack. These equations are used to our attack.

Doo-sik Choi et al. [9] proved that it is possible to extract the private key when using the round function repeatedly during the international standard AES cryptographic algorithm to perform a cryptographic operation, and when put in a syntax fault omitted to repeat a round easily. The experimental environment was equipped with AES algorithm on a commercial microprocessor ATmega128. For the laser equipment they used the fault injection EzLaze 3. The oscilloscope for time measurement equipment, such as the round starts and finishes were used. For fault injection the chip was tested by decapping. Experimental results proved AES encryption algorithm is vulnerable to this attack.

In 2013, Yanting Ren et al. [10], experimented on a smart card the power analysis attacks where they connect the sensor node and a 32bit cpu smart card and the 3DES cryptographic algorithm. To acquire the power consumption information they control the smart card through a card reader of the ISO7816 standard with a small resistance input in the Vcc path. The voltage difference over the resistance, which indicates the power consumption of the smart card, is measured by the oscilloscope with a differential probe at a sampling rate of 200 MSa/s. The power traces acquired by the oscilloscope is sent to the PC to be analyzed.

TABLE 1. ACCURACY ANALYSIS

	Target device	Attack Point	Target Algorithm	Attack type
Youn g-Jin Kang [6]	ATmega128 Microprocessor	$iv \oplus k$	PingPong-128 key stream generator	Correlation Power Analysis Attack
Jae deok Ji[7]	Contactless Smart Card	S-box, Diffusion	ARIA algorithm	Electromagnetic Disturban

				ces
Jung hwan Song [8]	N/A	Bit positions	Piccolo-80, Piccolo-128 algorithm	Fault Injection Attack, Cube Attack
Doo-sik Choi [9]	ATmega128 Microprocessor	Repeat function behind	AES algorithm	Fault Injection Attack
Yanti ng Ren [10]	Sensor Node and 32bit cpu Smart Card	S-Box	3DES algorithm	Power Analysis Attack

IV. COUNTERMEASURE FOR DISCUSSION

A. Software-based countermeasures

Software-based countermeasures against a side-channel cryptanalysis of the Rabbit stream cipher were proposed by Jonathan et al. [12] the countermeasures build upon previous work by improving mask generation, masking and hiding other components of the algorithm, and introducing a key refreshment scheme.

1) Masking: Masking the master counter variables and IV expansion provided a layer of defense against the first-order attacks. We improve the previous masking countermeasures by also masking the master state variables, thereby preventing higher-order attacks. The masking method applied generally follows the same principle of masking the counter variables during the key setup phase and then unmasking them before calling the next-state function. However, we propose improvements to the method used for mask generation, also making higher-order attacks difficult to perform.

The first improvement is to use different masks for the counter variables, IV expansion, and master state variables. This will make it difficult for the adversaries to obtain each of these values even if they manage to find one of the masks. The second improvement is to use a stronger pseudo-random number generator for creating the masks. While the previous scheme used an unnamed random number generator that took as input a 16-bit timer and the counter register of the chip, we propose the use of the SHA-256 hash function taking as input a 64-bit timer, 64-bit IEEE EUI-64 unique node identifier, and 256-bit entropy. Code efficiency is achieved by reusing the same SHA-256 function in the key refreshment mechanism.

2) Key Exchange: A random key pre-distribution scheme proposed in [13], wherein each node receives a randomly chosen 'ring of keys,' is applied to each sensor prior to deployment. Since a node only knows a subset of potentially hundreds of keys, a shared-key discovery protocol for key distribution, revocation, and node re-keying is introduced. This scheme costs fewer resources on individual nodes and limits the damage done if a node is compromised. The authors in [14] worked on improving this scheme by exploiting

deployment knowledge to improve network performance and resilience against node capture.

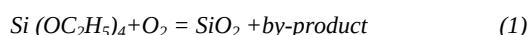
Chan and Perrig [15] built upon the work in SPINS by developing a key distribution scheme using peer intermediaries for key establishment (PIKE). The scheme uses peer sensor nodes as trusted intermediaries for establishing keys between any two nodes irrespective of the network topology or density. Basically, this protocol decentralizes the role of the trusted base station in SPINS

3) Key refreshment: We propose a key refreshment scheme that generates sub-keys that are used as session keys for communication between nodes in a wireless sensor network deployment. We assume that an initial shared master key K_M is pre-distributed in a node and that one or more of the other nodes depending on the key exchange mechanism are used. A key derivation function F is a pseudo-random number generator that takes as input the 128-bit master key, 64-bit IEEE EUI-64 unique node identifier, 64-bit values of a timer, and 64 bits of entropy. The secure hash function SHA-256 is used for processing the aforementioned input, essentially deriving a sub-key by using a keyed-hash message authentication code (HMAC). The use of system time and extra entropy ensures that the same sub-key is not generated twice. To prevent adversaries from obtaining a sufficient number of encryptions, we limit the lifetime of each sub-key to $l = 2^{43}$ encryptions.

B. Hardware-based countermeasures

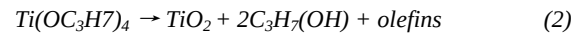
In 2014, Ndibanje et al. [16] have proposed hardware-based countermeasure against physical attacks on the integrated circuit (IC). The proposed countermeasure is based on the enhancements of the passivation layer which consist of the final layer on the top of IC.

1) First Layer Manufacturing Method: The first layer is called: "ultraviolet protection layer" because of it is the main function on the ICs protection. The process of fabrication of this layer is based on the deposition of the SiO_2 films by TEOS/ O_2 using the PECVD. The chemical reaction is described by chemically equation 1.



For the deposition of the SiO_2 , the rates to be used are TEOS: 10-100sccm, O_2 : 50-200sccm, at the RF power levels: 200-500W, in the following pressure range: 1-10torr, at the temperature: <400 C. The ultraviolet protection layer has a thickness of 200Å to 1000Å with 500Å of preferable thickness

2) Second Layer manufacturing Process: The robust layer on the top of the ultraviolet protection layer will be provided by the Ni- TiO_2 composite coating [17]. The Titanium isopropoxide is used as the TiO_2 precursor. The Ni- TiO_2 composite coating is prepared through electro-co-deposition from a bath containing dispersion of TiO_2 powder in Watt's bath. For electro-co-deposition of Ni- TiO_2 , a quantity of ml Watt's bath is used as the plating bath. The decomposition of TPT to form TiO_2 proceeds as follows:



In 2011 Amlan et al. [18] proposed a hardware countermeasure circuit, which, is integrated hardware module with the intermediate stages in S-Box. The Figure below describes the main idea about their work. The fundamental idea of our design is that, the dynamic power dissipation of a CMOS inverter is significant which apparently shows the spikes in every key guess. The basic design of the proposed hardware is shown in figure 2, which works only when the input logic to S-Box is 1. The circuitry will be idle if the input logic to S-Box is 0.

The operation of the above circuitry is explained below

- In the switching operation block, the n-MOS transistor will act as an electronic switch, which will be "ON" when logic 1 will be on the S-Box input bit.
- If the MOS switch is on, the second block will be in operation. The block will be operated at maximum possible practical frequency and consume maximum dynamic power.
- When the S-Box input will be in logic 0 states, the MOS transistor will be in "OFF" state and input to "Making sure of high frequency operation" block will be in high impedance state. Hence, the second block will not consume any power when S-Box input bit will be in logic 0 state.
- Hence in one S-Box, 8 similar circuitry will be placed parallel to the S-Box operation.

V. CONCLUSION

Current hardware device has been used over a wide range of fields. However, there are many hardware devices that are vulnerable to physical attack which is one on the side-channel attack that is the most powerful attack on crypto-hardware devices. In this paper, we described the side-channel attack in different types of attacks. In addition, in this paper we have presented an overview of a certain number of side channel attacks in recent years. Finally, however countermeasures techniques are deemed necessary, in order to overcome those attacks or changing the behaviour of the attack point in order to be more sophisticated when resisting to the attacker.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: NRF-2011-0023076).

REFERENCES

- [1] Korea Embedded Software and System Industry Association @ <http://www.kessia.kr>
- [2] [2005 Technical Report] Sergei P. Skorobogatov, Technical report No. 630 (UCAM-CL-TR-630) : "Semi-invasive attacks - A new approach to hardware security analysis," Univ. of Cambridge, Apr. 2005
- [3] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi, "The EM Side-Channel(s): Attacks and Assessment Methodologies," Available at <http://www.research.ibm.com/intsec/emf.html>, 2002

- [4] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," <http://www.cryptography.com>
- [5] Bellcore Press Release, "New threat model breaks crypto codes," Sept. 1996.
- [6] Young-Jin Kang, Hyun Ho Kim, Ndibanje Bruce, YoungGoo Park, and HoonJae Lee, "Correlation Power Analysis Attack on the PingPong-128 Key Stream Generator," IEEE 29th International Conference on Advanced Information Networking and Applications, pp. 506–509, 2015.
- [7] Jaedeok Ji, Dong-Guk Han, Seokwon Jung, SangJin Lee, and Jongsub Moon, "Practical Electromagnetic Disturbance Analysis on Commercial Contactless Smartcards," International journal of Distributed Sensor Networks, 2014.
- [8] Junghwan Song, Kwanhyung Lee, and Younghoon Jung, "The Security Weakness of Block Cipher Piccolo against Fault Analysis," International journal of Distributed Sensor Networks, 2014.
- [9] Doo-sik Choi, Yong-Je Choi, Doo-ho Choi, and Jae-cheol Ha, "A Late-Round Reduction Attack on the AES Encryption Algorithm Using Fault Injection," Korea Institute of Information Security, vol. 22, No. 3, pp. 439-445, 06. 2012.
- [10] Yanting Ren, Liji Wu, "Power analysis attacks on Wireless Sensor Nodes using CPU Smart Card," Wireless and Optical Communication Conference, pp. 665-670, 2013.
- [11] Dinur and A. Shamir, "Cube attacks on tweakable black box polynomials," in Advances in Cryptology—EUROCRYPT 2009, vol. 5479 of Lecture Notes in Computer Science, pp. 278–299, Springer, 2009.
- [12] Jonathan A. P. Marpaung, Bruce Ndibanje, and Hoon Jae Lee, "Higher-Order Countermeasures against Side-Channel Cryptanalysis on Rabbit Stream Cipher. Journal of Information and Communication Convergence Engineering. JICCE, 12(4): 237-245, Dec.2014.
- [13] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, pp. 41-47, 2002.
- [14] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, Hong Kong, China, 2004.
- [15] H. Chan and A. Perrig, "PIKE: peer intermediaries for key establishment in sensor networks," in Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, pp. 524-535, 2005.
- [16] Ndibanje, B., Hoon, J.L.: An Enhanced Passivation Layer for Secure Consumer Integrated Circuit Devices, IEEE 3rd Global Conference on Consumers Electronics(GCCE), 978-1-4799-05145-1, Pp300-301, 07-10, October 2014, Tokyo Japan.
- [17] S. Zhang, Q. Li, X. Yang, X. Zhong, Y. Dai, and F. Luo, "Corrosion resistance and mechanical properties of pulse electrodeposited Ni-TiO₂ composite coating for sintered NdFeB magnet". Journal of Alloys and Compounds, 2009.
- [18] Amlan, J.C, Beum, S.P, Ndibanje, B., Young, S.L., Hyotaek, L., Hoon, J.L. : An Efficient Hardware Countermeasure against Differential Power Analysis Attack. In the Proceedings of the ICHIT 2011, CCIS 206, pp. 153–159, 2011. © Springer-Verlag Berlin Heidelberg 2011.



Young-Jin Kang

2013: BS at Dongseo University, Republic of Korea
 2015: MS at Dongseo University, Republic of Korea
 2015 ~ current: doctor's course Dongseo University, Republic of Korea
 Research Interests: Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis



Ndibanje Bruce

2004: BS at Ngozi University, Republic of Burundi
 2013: MS at Dongseo University, Republic of Korea
 2016: Ph.D at Dongseo University, Republic of Korea
 Research Interest: Information Security, Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis



SuHyun Park

1986: BS at Pusan National University, Republic of Korea
 1988: MS at Pusan National University, Republic of Korea
 1999: Ph.D at Pusan National University, Republic of Korea

1996 ~ current: Professor of Dongseo University, Republic of Korea
 Research Interests: Maritime IT, Artificial Intelligence, Intelligent System



HoonJae Lee

1985: BS at Kyungpook National University, Republic of Korea
 1987: MS at Kyungpook National University, Republic of Korea
 1998: Ph.D at Kyungpook National University, Republic of Korea

2002 ~ current: Professor of Dongseo University, Republic of Korea
 Research Interests: Password Theory, Network Security, Side-Channel Attack, Information Communication/Information Network