

Proposal of PingPong-128 Countermeasure against Power Analysis Attack

Young-Jin Kang*, Ki-Hwan Kim*, Hoon Jae Lee**

*Department of Ubiquitous IT, Dongseo University, Busan 47011 Republic of Korea

**Division of computer engineering, Dongseo University, Busan 47011 Republic of Korea

rkddudwls55@gmail.com, ghksdl90@naver.com, hlee@dongseo.ac.kr

Abstract— Typical power analysis attack countermeasures include the ability to inject defensive logic during the hardware gate design phase, or to add additional hardware logic or software coding depending on how the cryptographic module is configured. For example, the Hardware-based high speed cryptographic module via FPGA can be protected with a gate array logic, and the firmware cryptographic module via the microprocessor module will allow you to implement defence technology with software coding. In this paper, Using Scrambler to propose a secure PingPong-128 crypto algorithm for power analysis attacks.

Keywords— Power Analysis Attack, PingPong-128, Stream Cipher, Scrambler, PA Countermeasures

I. INTRODUCTION

The most powerful were known as side-channel attack [1] is to find or weakness in the cryptographic algorithm (decryption and is different), even higher safety instead of the cryptographic algorithm itself to the indiscriminate attack cryptographic algorithm is implemented or how the implementation environment for the current cryptographic module It is subject to possible attacks by. For example, time required information, power consumption, which emits electromagnetic waves or even through the sound system provide additional information that can be exploited for breaking. Some side-channel attack would require technical knowledge of the internal workings of a system that implements cipher, but on the other side-channel attack is also effective as a black-box attack such as power difference analysis.

In particular, the most powerful of the side-channel attack was the vulnerability of a known crypto algorithm (AES, DES, ARIA etc), and many researchers say the need for countermeasures. Goubin [2] introduced a general countermeasure, 1) Remove the correlation of output tracking values based on the execution of cryptography algorithms, such as moving the execution time randomly, inserting a waiting state, inserting fake commands, randomly executing the operation. 2) Redesign critical circuits, which are treated as different commands, to be difficult to analyse important assembler commands, and to move counting or memory. 3) Modify the algorithm of the cryptographic primitive, which is used to have different values whenever the data or key is used, making the attack more difficult.

In addition, many researchers have proposed countermeasures. First, countermeasures can be divided into hardware and software. Because the nature of the power analysis [3] attempts to strike through consumption power, hardware countermeasures are aimed at designing the circuit and designing circuits to ensure constant consumption of electricity, but the cost is expensive. Software countermeasures are intended to eliminate dependencies between data and power consumption values that are handled by the algorithm itself. In this paper, we propose PingPong-128 countermeasure against power analysis attack using scrambler as software countermeasure.

II. POWER ANALYSIS ATTACKS

It is very difficult to find the secret key (K) using arbitrary plaintext (P) and cipher text (C) by designing the encryption algorithm so that the correlation between the cipher text and the secret key is so much low.

$$P_t \oplus K_t = C_t \quad (1)$$

The exclusive logical operation has the property that the operation is repeated twice as in Equation 2 and is restored to its original state. If the information of the cipher text computed by using the plaintext and the secret key can be correctly recognized, the secret key can be guessed through the characteristic of the exclusive logical operation.

$$C_t \oplus P_t = (P_t \oplus K_t) \oplus P_t = K_t \quad (2)$$

However, it is so much difficult to correctly extract arbitrary operation processes from the hardware environment. As shown in Figure 1, since the power consumption (T_t) at the moment of Equation 1 in the hardware environment has the property like cipher text, it becomes possible to mathematically substitute cipher text.

The attacker arbitrarily selects a plain text (P_t) and selects a specific moment (t) with a high degree of correlation of the guessing cipher text (C_t) to attack. Since the plaintext is known in Equation 3, but it is impossible to guess the secret key that can be guessed, the calculation result is used instead of the instantaneous power consumption when the calculation result is generated.

$$P_t \oplus C_t = P_t \oplus T_t = K_t, (if C_t = T_t) \quad (3)$$

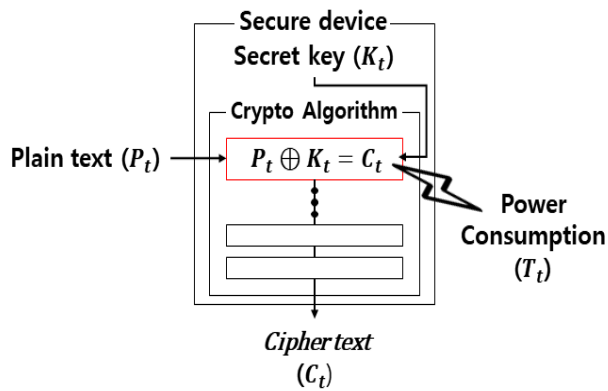


Figure 1. Power analysis attack

In this case $\oplus$ is an operator, C_t is a value of operation, P_t is a known value, it is presumably from secret key (k) but is an unknown value, and t is the moment of attacking. If it is knowable, secret key (k) is too. A power analysis attack is a method of attacking by analyzing the correlation between all secret keys that can be guessed at an arbitrary point (t) and the power signal estimated (h_t) from the measured power signal (T_t).

We can't get the value of K_t because we don't know the value of C_t at the Equation 1, and measured power signal (T_t) has high mutuality with operation value (C_t) in the statistical aspect. Assume that K_t is a possible option and by using Equation 1, we presume C_t on each of assumed K_t .

From assumed C_t , we can assume the power signal H_t . When we find the highest mutuality of H_t that is achieved by analyzing the mutuality between each of assumed H_t and T_t , The K_t applied at assuming H_t is the value we were looking for and that K_t is used for the secret key(k)'s inverse operation. For instance, we have 256 number of K_t in the 8 bit operating system. We statistically compare 256 number of H_t assumed from the 256 number of K_t with measured power signal T_t to choose the highest mutuality of H_t within them. The K_t assumed H_t is the value and from that K_t we operate backward the secret key (k). A power analysis attack takes the four steps below for the attack.

Step 1. Measurement of power signal

Measure the power signal (T_t) and select the moment of the relevant attack which operated by each of Secret intermediate key (K_t) and the Known value (P_t) released in the middle of the operation of the cryptographic algorithm form algorithm analysis.

Step 2. Estimate operated value

Assume all Secret intermediate keys(K_{ti}) are possible at the attacking point(t) and estimate the operated value(C_{ti}) on the each of Secret intermediate key(K_{ti}). Here the 8 bit operating system has 256 number of K_{ti} . ($i = 0 \dots 256$)

Step 3. Estimate the power consumption

Assuming power consumption (H_{ti}) by using the estimated operated value (C_{ti}) at the moment of the attacking.

Step 4. Statistical analysis of the correlation

We have high Correlation coefficient value to the correctly estimated H_{ti} by analysis of statistical mutuality between H_{ti} and T_t . and the rest which estimated wrong we have low Correlation

coefficient value so that enables to find Secret intermediate key(K_{ti}). With the K_{ti} we can assume, calculate secret key (k).

III. PINGPONG-128 ANALYSIS OF ALGORITHM

The PingPong-128 algorithm is a stream cipher that uses linear feedback shift registers (LFSR) [4]. As shown in Figure 2, it consists of initializing two LFSR (L_a , L_b) using secret key and initial vector, and generating key sequence using L_a and L_b .

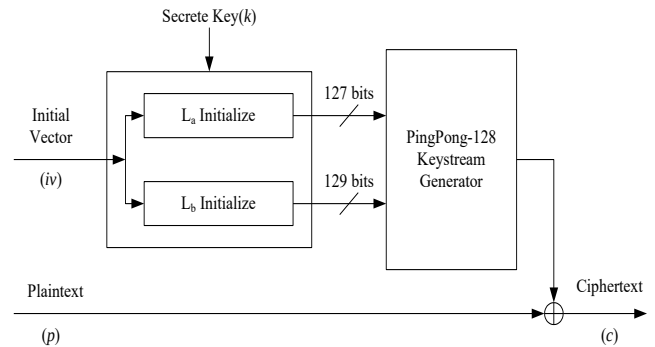


Figure 2. PingPong-128 algorithm.

If there is an error in synchronization in communication system, it demands retransmission of entire message. At this time, if the system has synchronous stream cipher, other sequence's key could be used for safety. For this, rekeying has to be done by either when the form of encrypted key and clear text are transmitted to different initial vector to resynchronize or other opened methods. We generate synchronizing error intentionally to apply resynchronization to initial vector to attack. To look for the rekeying and re-synchronizing process, it is equal to Equation 4 and 5.

$$L_a = (iv \oplus k) \bmod 2^{127} \quad (4)$$

$$L_b = (k \ll 1) \oplus (0|iv) \quad (5)$$

Secret key (k) and initial vector (iv) each have size of 128 bit, L_a has 127 bit, and L_b has 129 bit. In Equation 1 the (iv) is known value and (k) is unknown value so when the calculation of $(iv \oplus k)$, like the Equation 1, initiates, I apply power analysis attack.

In the Kang.etc [5] Paper, we found the first 8 bits of the 128-bit secret key using the correlation coefficient between the secret key and the power consumption estimated in the environment with the PingPong-128 encryption algorithm on the ATmega128 8-bit microprocessor.

IV. SCRAMBLER STRUCTURE AND OPERATION SEQUENCE

Synchronous stream ciphers require retransmission of the entire message in the event of a synchronization error. At this time, a different key sequence should be used for stability, and rekeying should be applied in such a way as to resynchronize the secret key (k) and the initial vector (iv) to be transmitted in plaintext state or other public methods. The PingPong-128 cipher consisting of two LFSRs, output function F and clock

control functions also needs to be protected against a separate power analysis attack like most known cryptographic algorithms. Common countermeasures against power analysis attacks include inserting the defence logic at the hardware gate design stage and adding hardware logic or software coding according to the configuration method of the cryptographic module. According to the encryption algorithm, countermeasures against attack of power analysis attack should be separately designed.

A scrambler is a method proposed for randomizing transmission data because clock synchronization recovery is difficult at the receiving end when the transmission data is "0" consecutively. At the receiving end of the communication equipment, it is converted back to a de-scrambler and then the data is input to the modem.

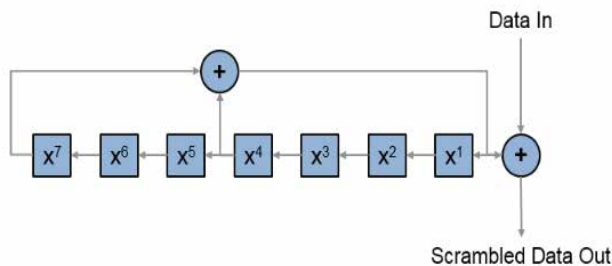


Figure 3. How to work a scrambler

The power analysis attack on the PingPong-128 algorithm attacks by using a method of artificially generating a synchronization error and resynchronizing it with the initial vector (iv). Where iv is a known value and k is an unknown value. Here, since A is a known value and B is an unknown value, attack can be performed at the time when the operation $(iv \oplus k)$ is executed. However, if a scrambler is applied as shown in Figure 2, even if artificially resynchronized, it becomes random again by the scrambler, so that a power analysis attack becomes difficult. In this study, we propose a defense technology using scrambler and descrambler which can be effectively applied to DPA defense while the circuit is simple. The power analysis countermeasures proposed in this study are key randomization and plaintext randomization. Key randomization is a method of applying a scrambler to a key value and an IV value, and a key length used for PingPong-128 is 128 bits. Whenever the key value is input in 1-bit units, the value is changed to the scrambler shown in Figure 2 and input to LFSR1 and LFSR2. The same applies to reception. The plaintext randomization is a method of applying a scrambler to the plaintext value, the length of the plain text used in PingPong-128 is unlimited, whenever the plaintext value is input in 1-bit units, the value is changed to the scrambler shown in the Figure 4 below to XOR with the keystream. The same applies to reception.

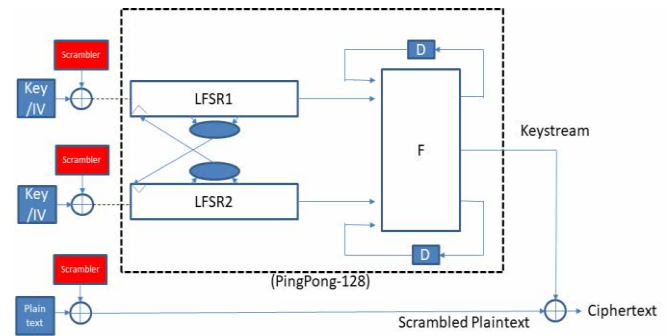


Figure 4. PingPong-128 architecture to resist power analysis.

V. CONCLUSIONS

In this paper, we added a Plain text and a key scrambler to input with synchronous stream cipher, and proposed a Countermeasures against Power Analysis Attacks. PingPong-128 corresponds to synchronous stream cipher and both sides must perform initialization when the synchronized secret key generation order of the transmitting and receiving is out of order. PingPong-128 corresponds to synchronous stream cipher and both sides must perform initialization when the synchronized secret key generation order of the transmitting and receiving is out of order. Ping Pong-128 using the scrambler proposed replaces the plaintext and key input from the existing algorithm with random scramblers to transposition the presumably information with unknown data.

Since random changes of plain text and keys can be allowed to overlap, it is not possible to associate the result with the correct data value after the power analysis attack, so it is possible to defend the power analysis attack on the weakest part. We plan to test the proposed ideas and test their defences and algorithm performance.

ACKNOWLEDGMENT

This work was supported by Institute for Information and Communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00285) and also 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-2016R1D1A1B01011908).

REFERENCES

- [1] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology - CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.
- [2] L. Goubin, J. Paratin, "DES and differential power analysis", CHES'99, LNCS 1717, pp.158-172, 1999.
- [3] J. Jaffe, "Introduction to differential power analysis," Presented at ECRYPT Summer school on Cryptographic Hardware, Side Channel and Fault Analysis. Jun. 2006.
- [4] HoonJae Lee, Kevin Chen, "PingPong-128, A New Stream Cipher for Ubiquitous Application," IEEE International Conference on Convergence Information Technology, pp. 1893-1899, 2007.

- [5] 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.



Young Jin Kang

He received the B.S in Computer Networking from Dongseo University in Korea 2013. His received the M.S. in Ubiquitous IT from Dongseo University in Korea 2015. His research interests are in the security topics of Side-Channel Attack (SCA) and Network Security and Cryptography.



Ki Hwan Kim

He received the B.S. degree in Computer Networking from Dongseo University, Republic of Korea in 2015. And his received the M.S. degree in Ubiquitous IT from Dongseo University in Korea 2017. His current research interests are in Cryptography, Information Security and Network Security.



HoonJae Lee

He received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. He had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc.