applied sciences

MDPI

Article

Side Channel Leakages Against Financial IC Card of the Republic of Korea †

Yoo-Seung Won ‡, Jonghyeok Lee ‡ and Dong-Guk Han *,‡

Department of Financial Information Security, Kookmin University, 77 Jeongneung-ro, Seongbuk-gu, Seoul 02727, Korea; mathwys87@kookmin.ac.kr (Y.-S.W.); n_seeu@kookmin.ac.kr (J.L.)

* Correspondence: christa@kookmin.ac.kr

† This paper is an extended version of paper published in the International Conference on Information Security and Cryptology, ICISC held in Seoul, Korea, 29 November–1 December 2017.

‡ These authors contributed equally to this work.

Received: 15 September 2018; Accepted: 7 November 2018; Published: 15 November 2018

Abstract: Integrated circuit (IC) chip cards are commonly used in payment system applications since they can provide security and convenience simultaneously. More precisely, Europay, MasterCard, and VISA (EMV) are widely known to be well equipped with security frameworks that can defend against malicious attacks. On the other hand, there are other payment system applications at the national level. In the case of the Republic of Korea, standards for financial IC card specifications are established by the Korea Financial Telecommunications and Clearings Institute. Furthermore, security features defending against timing analysis, power analysis, electromagnetic analysis, and TEMPEST are required. This paper identifies side channel leakages in the financial IC cards of the Republic of Korea, although there may be side channel countermeasures. Side channel leakages in the financial IC cards of the Republic of Korea are identified for the first time since the side channel countermeasures were included in the standards. The countermeasure that is applied to the IC card from a black box perspective is estimated to measure security features against power analysis. Then, in order to investigate whether an underlying countermeasure is applied, first-order and second-order power analyses are performed on the main target, e.g., a S-box of the block cipher SEED that is employed in the financial system. Furthermore, the latest proposal in ICISC 2017 is examined to apply block cipher SEED to the financial IC card protocol. As a result, it is possible to identify some side channel leakages while expanding the lemma of the paper accepted in ICISC 2017. Algebraic logic is also constructed to recover the master key from some round keys. Finally, it is found that only 20,000 traces are required to find the master key.

Keywords: side channel analysis; financial IC card; first-order analysis; second-order analysis

1. Introduction

Security plays an important role in payment system applications and is directly connected to customer's credibility. An integrated circuit (IC) chip is usually chosen to provide stable security as it offers high performance, data storage, and application processing. Europay, MasterCard and VISA (EMV) are examples. For personal identification number transaction security, physical and logical security requirements are required simultaneously for full payment security. To satisfy physical security requirements, some countermeasures [1–13] against side channel analysis [14–19] (This article is an extended version of the paper [19] accepted in Information Security and Cryptology (ICISC) 2017). The security of the financial IC card protocol will also be evaluated after expanding upon a previous suggestion.) or fault injection should be employed. Alternatively, there are some payment system applications that are only applied in their domestic markets. In the Republic of Korea, a specific payment system [20] is employed when using a credit or debit card. Specifically, the authentication

protocol below (Figure 1), which is called the financial IC card protocol in this paper, is carried out when withdrawing cash from an automated teller machine (ATM) in the domestic market.

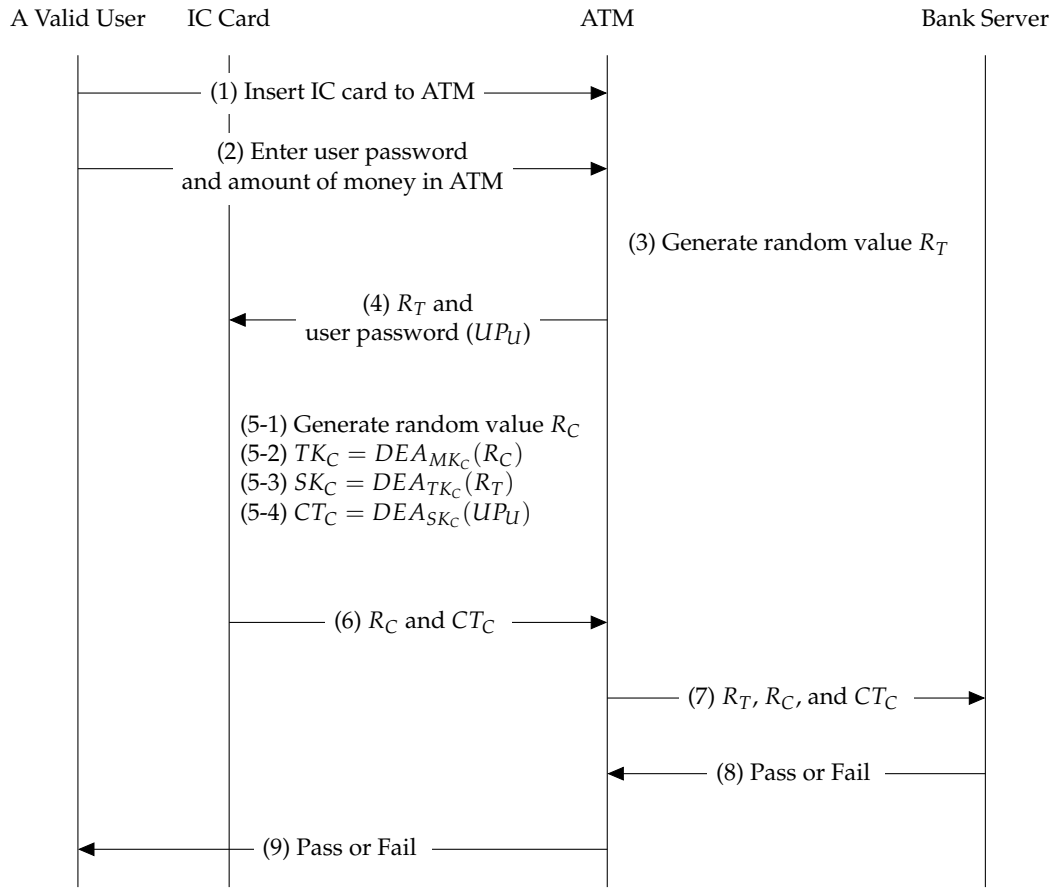


Figure 1. Financial IC (Integrated circuit) card protocol. ATM: automated teller machine.

Here, Data Encryption Algorithm (DEA) indicates block cipher SEED [21]; UP_U indicates user password; $C = DEA_K(P)$ means that the encryption function DEA takes a key K and plaintext P as input and produces a ciphertext C, and all inputs and outputs in the encryption function consist of 128 bits except for UP_U. However, UP_U is encoded to 128 bits using a padding scheme [20]. Moreover, the subscripts U, C, and T for all variables indicate user, IC chip, and ATM, respectively.

(1) A valid user inserts an IC card into an ATM in the baking system of the Republic of Korea.
(2) A valid user enters the user password and amount of desired cash through the ATM interface.
(3) The ATM generates a random number, R_T, which is composed of 128 bits.
(4) The ATM transfers R_T and the user password to the IC card.
(5-1) The IC chip generates a random value, R_C, which consists of 128 bits, for the financial IC card protocol.
(5-2) In the IC chip, R_C is encrypted to TK_C under a fixed key, MK_C, stored in the secure memory.
(5-3) In the same way, R_T is encrypted to R_T under non-fixed key TK_C generated from (5-1).
(5-4) Finally, UP_U is encrypted to CT_C under non-fixed key SK_C generated from (5-2).
(6) The IC chip passes R_C and CT_C to the ATM.
(7) The bank server receives the R_T, R_C, and CT_C from the ATM.

(8) The bank server possesses keys MK_B and UP_B, which are identical to MK_C and UP_U, respectively. Therefore, by performing a scheme identical to (5-1)∼(5-4), it can determine the truth of this protocol.

(9) The ATM informs the user whether a cash withdrawal is possible or not.

For a detailed description of this protocol, refer to [20]. In particular, the security features for the financial IC card protocol are clearly stated in Chapter I.8. This document states that there should be resilience to power analysis, timing analysis, electromagnetic leak, fault injection, TEMPEST, etc. This is due to security threats, such as the risk of IC chip duplication. There is currently only one study [22] on the side channel leakage in the financial IC card protocol. Moreover, that study only found a single byte of round key against block cipher SEED without countermeasure, because a countermeasure was not mandatory at the time.

Our Contributions. This paper examines side channel leakage in the financial IC card of the Republic of Korea. As of 2008, financial IC chips must be resilient to state-of-the-art power analysis. However, side channel leakages have not been considered in the financial IC card protocol since 2008. Three main contributions are made by this paper. The first is that it offers the only challenge to the security evaluation of the Korean financial IC card protocol since 2008. Even though the first round key is retrieved via side channel analysis, the master key cannot be recovered in reasonable time. Therefore, the recovery logic of the master key is established. For this, a black box model (the black box model means that an adversary only knows the public information while performing the general protocol, in particular, it makes sense even if a fake ATM is employed, because a fake ATM never damages the financial IC card protocol) is fundamentally employed, i.e., it assumes that the adversary does not have knowledge of the detailed countermeasures. Therefore, underlying schemes such as first-order analysis and second-order analysis can be performed.

The second contribution is that the resilience for the state-of-the-art attack technique [19] is investigated to evaluate the security of financial IC card protocol. Furthermore, we demonstrate that the correct key can be revealed by expanding upon the suggestion of [19]. That is, novel combinations are found in this paper, differing from the original suggestion [19]. Specifically, novel combinations induce that four bits of eight bits are related to second-order leakage, whereas the original combination suggested in [19] derives only two bits of eight bits.

Finally, this study recovered the round key as well as the master key for the financial IC card protocol for the first time, although the countermeasure for state-of-the-art attack techniques should be mandatory. Consequently, the master key dedicated in the IC chip can be sufficiently recovered using our suggested method in reasonable time.

Extension. As written in the footnote of this title, this paper is an extended version of our paper [19] presented at ICISC 2017. In our paper [19], we demonstrated that the diffusion layer of block cipher SEED is vulnerable to our suggestion, although first-order Boolean masking and partial shuffling countermeasures are applied. Furthermore, we found a two-bit correlation between the diffusion layer and confusion layer outputs in terms of second-order leakage. We also implemented our method on simulated trace and a well-leaked board in terms of power analysis (the board is used in academic articles because the power source is well-leaked and the platform is easy to use; detailed information can be found at http://wiki.newae.com.). However, in this paper, we show two differences compared to the previous paper [19]. One is that we extend our previously suggested equation, as shown in the present Appendix A. Therefore, we show four-bit correlation between the diffusion layer and confusion layer outputs rather than two-bit correlation for some special diffusion outputs (refer to Cases 2 and 5 in Appendix A). The other is that we apply our suggestion to the latest smart card. Additionally, the adversary assumption is even a black-box model. Therefore, we propose an attack scheme of financial IC card in terms of side channel analysis as well as the recovery mechanism of the master key in this paper.

2. Preliminaries

In this section, existing knowledge regarding details of the financial IC card, a countermeasure for block cipher SEED, and the side channel analysis for block cipher SEED's countermeasure are presented.

2.1. Known and Unknown Information on Financial IC Card Protocol

If an invalid user acquires a certain IC card, some information can be revealed without significant effort. That is, a fake ATM can be constructed by the invalid user, ignoring the bank server. In other words, a fake ATM transfers R_T and UP_U^* values to the IC chip (* indicates invalid value). Moreover, a valid UP_U value is not required, as our goal is to recover the master key, not a valid CT_C value. The following summarizes the known or unknown information when a financial IC card protocol is performed by an invalid user:

- Known information: R_T, UP_U^*, R_C, and CT_C^*
- Unknown information: MK_C, TK_C, and SK_C^*

The important point here is that R_C cannot be controlled by an invalid user. Due to this fact, a chosen plaintext attack cannot be applied to the financial IC card protocol. Furthermore, a non-profiled attack cannot be performed on second and third DEA operations, because TK_C and SK_C^* are changed whenever this protocol is conducted. In other words, assuming a non-profiled attack, the main target is naturally the first DEA operation. More precisely, the first round of the foremost DEA operation is definitely the main target, since TK_C is unknown information.

2.2. Countermeasure for Block Cipher SEED

The countermeasure of block cipher SEED [21] is analogous to that of the block cipher Advanced Encryption Standard (AES) [23] in terms of S-box operation. However, other countermeasures are required because block cipher SEED is constructed with AND and $Addition$ operations. A few countermeasures to protect the AND operation are suggested in [2]. Moreover, many suggestions [24–32] have been proposed with respect to the $Addition$ operation.

When compared with the higher-order masking scheme in software implementation, hiding schemes, such as shuffling and dummy methods, are adequately applied to reasonable countermeasures. Furthermore, the dummy operation can sometimes be employed because the number of S-boxes is four in the G-function of block cipher SEED.

In software implementation, it is sometimes considered reasonable to combine first-order masking, shuffling, and dummy operation schemes [11]. In particular, the application of this combination is relevant to the DPA contest [33].

2.3. Side Channel Analysis for Countermeasure of Block Cipher SEED

A Boolean masking scheme is normally employed, since most block ciphers can be comfortably applied in this case. However, the $(d+1)$-th order attack theoretically allows the leakage of the master key, even though the d-th order Boolean masking scheme is adopted. Thus, to improve security strength, the Boolean masking scheme is sometimes combined with a hiding countermeasure, such as shuffling and dummy operation. As previously stated, first-order Boolean masking, shuffling, and dummy schemes can be simultaneously selected as a realistic countermeasure, considering the time performance and read-only memory/random access memory (ROM/RAM) size. Some attacks have been proposed to evaluate the security of these countermeasures [13,19,33]. In general, a single signal is shuffled to p signals when a shuffling countermeasure is applied. Moreover, more p^2 traces are required to retrieve the secret key in comparison to the number required in non-shuffled traces. In [13], more p traces were only required when performing windowing attacks. That is, the shuffling complexity was decreased to $\sqrt{p}$ from p. However, there are some barriers of realistic attack in order to

perform a windowing attack. After performing the windowing scheme that derives the constant size from the original trace, the points of interest should be overlapped in each trace. Therefore, sometimes numerous traces may have to be compared in terms of theoretical complexity.

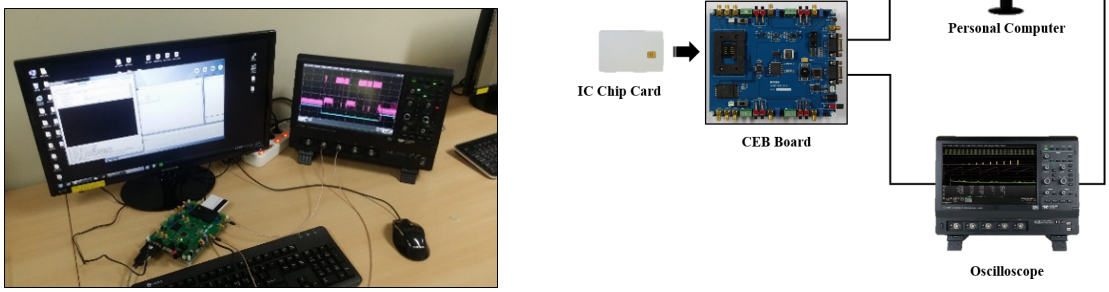
3. Evaluation Methodology for the Financial IC Card Protocol

In this section, the process of evaluating the security of the financial IC card protocol is explained. The ultimate aim of this study was to retrieve the entire master key, not just a part of it. First, the evaluation system that was constructed as a fake ATM is described. Then, the analysis methodology under the black box model is explained in order to recover the whole master key.

3.1. Construction of Side Channel Analysis for Financial IC Card Protocol

As previously stated in Section 2.1, a fake ATM can be constructed to communicate with an IC chip card. The related experimental setup can be provided via the SCARF system (Version 4.0.0.17153 (64 bit), Electronics and Telecommunications Research Institute (ETRI), Daejeon metropolitan city, Republic of Korea) [34].

As shown in Figure 2, the CEB board (this board is provided by SCARF system), which plays the role of a fake ATM in the financial IC card protocol, is controlled by the SCARF system. As previously described, R_T and UP_U were generated from script language in the SCARF system. That is, these values can take the desired form, between fixed or random values.



(**a**) The realistic experimental setup (**b**) The schematic experimental setup

Figure 2. Experimental setup for security evaluation of financial IC card protocol.

3.2. Security Evaluation Methodology of Side Channel Analysis Under Black Box Model

Before describing the security evaluation methodology, the intermediate variables were enumerated, depending on the side channel attack schemes. Basically, the intermediate variables in the first round of the foremost DEA should be the main targets, due to the constraint of public information. In other words, the second and third DEAs cannot be considered major objectives under a non-profiling attack, owing to protocol features. Moreover, the last round of the foremost DEA cannot be an available intermediate variable, because TK_C is an unknown information in the usual protocol.

The master key can also be leaked. For this, two round keys should be recovered through side channel analysis, and a brute force attack is required.

3.2.1. Enumeration For Intermediate Variables

To evaluate the security against side channel analysis, the underlying scheme is performed as first and second-order analyses. Thus, the intermediate variables should be enumerated.

1. First-order correlation power analysis
    (a) Each of the four S-boxes in the G-function
2. Second-order correlation power analysis
    (a) Combination between two of the four S-boxes in the G-function
    (b) Combination between two out of the four outputs of the G-function

First-order correlation power analysis is a fundamental attack when the countermeasure is not applied. Sometimes the first-order leakage may be exposed in spite of applying the countermeasure, due to unintended phenomena, such as optimization in the computer language compiler and human error. Therefore, item 1a should be required. Additionally, the four S-boxes in the G-function should be chosen as intermediate variables to recover the single round key.

To conduct second-order correlation power analysis, pre-processing logic must be employed [18]. In addition, two intermediate variables should be required to release the leakage of the round key. In particular, the identical masking value is usually applied to each of the S-boxes to reduce the cost of pre-computed tables when assuming the general first-order Boolean masking scheme. For this reason, item 2a is needed to disclose the masking information. Moreover, the novel leakage in connection with block cipher SEED was recently suggested in [19]. According to this proposal, second-order leakage can be revealed with low attack-complexity, despite first-order Boolean masking and restricted shuffling countermeasures being employed, although a main target is the output of G-function. In other words, first-order Boolean masking and shuffling countermeasures can usually be utilized as reasonable countermeasures in software implementation due to certain merits, such as time performance, memory size, and security. However, in terms of block cipher SEED, side channel leakage can occur via 2b. In particular, authors in [19] only explained that one combination of total six cases was showed.

3.2.2. Security Evaluation Methodology

In this section, the evaluation methodology used to perform side channel analysis under the black box model is described. The black box model assumes that the detailed countermeasure applied to block cipher SEED in the IC chip cannot be known. The first part of the approach is to observe public information such as R_T or CT_C^*, not the intermediate variable related to the secret key. This approach allows for the acquisition of two features. The first is that the operation position of block cipher SEED can be found in the whole protocol. The second is the establishment of the best solution for pre-processing information, such as compression method, compression rate, the number of traces, etc.

Before analyzing the enumeration defined in Section 3.2.1, it should be identified whether the public information can be revealed or not. The enumeration has the potential to reveal a secret key if the public information can be disclosed in traces. Moreover, the best solution for the pre-processing scheme can be found.

- Applied pre-processing scheme: none, Correlation value when performing correlation power analysis: 0.03
- Applied pre-processing scheme: average compression 30, Correlation value when performing correlation power analysis: 0.15
- Applied pre-processing scheme: average compression 50, Correlation value when performing correlation power analysis: 0.05

Here, the average compression N indicates that N points are compressed to 1 point by calculating the average.

The best solution is the average compression 30 scheme, because its correlation value is the highest among the three cases. Subsequently, side channel analysis can be performed using the stored pre-processing information.

3.2.3. Recovering the Master Key via Some Round Keys

The brute force attack for recovery of the master key after retrieving two round keys via side channel analysis is introduced here. Yoo et al. [35] explains how to recover the master key when 1 round and 16 round keys are already known. In the current study, this suggestion is not sufficient, since only 1 and 2 round keys are retrieved via side channel analysis. Therefore, it is necessary to properly apply the suggestion presented in [35] to the current context. Moreover, the recovery scheme of the master key is represented at the appropriate algorithmic level.

Note that notation of all variables used in Algorithm 1 is given in [21,35]. The size of all variables is 32 bits, with the exception of the variable MK. $X^{(n)}$ indicates the n-th significant byte of 32-bit X. $X^{(n-m)}$ means from the n-th significant byte to the m-th significant byte. Additionally, G^{-1} is the inverse of the G-function.

Algorithm 1 Recovery of the master key under two round keys K_1, K_2

Input: 1 round key $K_{1,0}$ and $K_{1,1}$, and 2 round key $K_{2,0}$ and $K_{2,1}$
Output: Candidates for a master key MK

▷ Calculating the inverse of G-function and constant value KC_0, KC_1
$TK_{1,0} \leftarrow G^{-1}[K_{1,0}] + KC_0$
$TK_{1,1} \leftarrow G^{-1}[K_{1,1}] - KC_0$
$TK_{2,0} \leftarrow G^{-1}[K_{2,0}] + KC_1$
$TK_{2,1} \leftarrow G^{-1}[K_{2,1}] - KC_1$

▷ Guessing a part of A and B for master key
for $TC = 0$ to $2^{32} - 1$ **do**
  $TA0 \leftarrow TK_{1,0} - TC$
  $TA1 \leftarrow TK_{2,0} - TC$
  if $TA0^{(3-1)} = TA1^{(2-0)}$ **then**
    Storing a pair $(TA0, TA1)$
  end if
end for
for $TD = 0$ to $2^{32} - 1$ **do**
  $TB0 \leftarrow TK_{1,1} + TD$
  $TB1 \leftarrow TK_{2,1} + TD$
  if $TB0^{(3-1)} = TB1^{(2-0)}$ **then**
    Storing a pair $(TB0, TB1)$
  end if
end for

▷ Filtering temporary keys
if $TA0^{(0)} = TB1^{(3)}$ **then**
  if $TB0^{(0)} = TA1^{(3)}$ **then**
    $MK \leftarrow (TA0)||(TB0)||(TK_{1,0} - TA0)||(TK_{1,1} + TB0)$
    Storing candidate MK
  end if
end if
return Candidate MK

The procedures are divided into three steps in Algorithm 1. In addition, the recovery algorithm can be performed in reverse order of generation for the round key. In particular, the first step is directly related to its reverse order, allowing it to be easily computed. Subsequently, the second step is that a part of A and B for the master key can be guessed. Moreover, $TA0^{(3-1)}$ and $TB0^{(3-1)}$ are identical to $TA1^{(2-0)}$ and $TB1^{(2-0)}$, respectively, because the 2 round key is derived from the rotation of 1 round key. There are 256 candidates until the second step, since $TA0$ and $TB0$ depend on the size of a single byte. In the third step, a part of $TA0$ is equal to part of $TB1$, due to the rotation in the generation of a round key. Finally, the number of candidates for the master key is less than 256.

In order to acquire only one master key, a correct single pair (R_C, R_T, UP^*_U, CT^*_C) in the financial IC card protocol is required. Then, the master key can be determined by proceeding with an exhaustive attack.

4. Experimental Results

The security strength against side channel analysis was evaluated to protect against the leakage of private information. Based on Section 3, the security can be evaluated for a specific IC card. For this, a recent IC card issued in the Republic of Korea was used. The expiration date of this specific IC card was 2023, because the issuance date was 2018. In other words, the master key dedicated to the IC chip should not be able to be revealed by any attacks, according to ChapterI.8 of [20].

As previously stated, the public information in the collected traces was first identified, and then the pre-processing information was stored. Afterwards, security evaluation was conducted against the novel side channel analysis for the defined enumeration in Section 3.2.1. Finally, the master key was recovered via the brute force attack defined in Algorithm 1.

4.1. Identifying the Public Information

This section elaborates upon the security evaluation methodology defined in Figure 3, except for the defined enumeration. For this, the experimental setup described in Figure 2 was utilized.

In Figure 4, three identical areas should be identified, due to the DEA algorithm being computed three times in the financial IC card protocol. Therefore, when performing correlation power analysis, the plaintext or ciphertext information was searched through until the occurrence of a peak. Due to time and memory limitations, not all points can be collected simultaneously. Thus, a proportion of all points should be measured after estimating the plaintext/cipher operation. Finally, the DEA algorithm operation in the red box of Figure 4 was found.

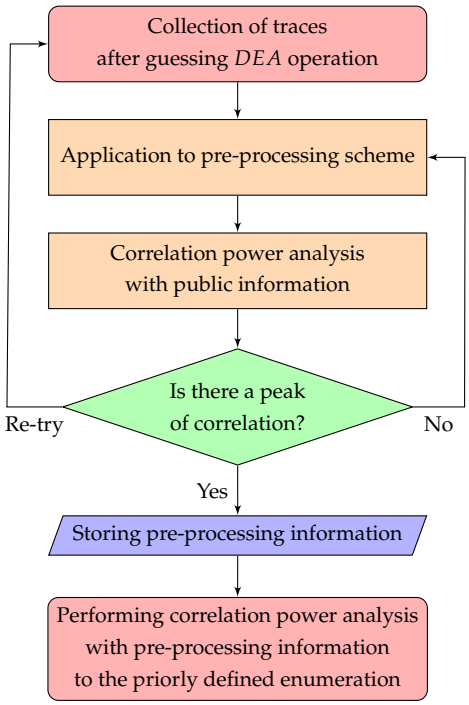


Figure 3. Security evaluation methodology for financial IC card protocol.

In particular, block cipher SEED was composed of 16 rounds. However, 16 identical rounds cannot be found in Figure 5. It can be estimated that the area of dimensions 0.9×10^4 to 1.5×10^4 is divided into 12 identical areas. There are also two identical areas in the front and rear of the middle part. Therefore, it can be estimated that some countermeasures are applied to 1, 2, 15, and 16 rounds. Additionally, the plaintext information was revealed in the front part in Figure 6. The detailed description is given in the next section.

In order to analyze the plaintext operation, the front part of the *DEA* algorithm operation was re-collected. Additionally, as shown in Figure 3, the plaintext operation was analyzed by repeating trial-and-error to obtain the best solution.

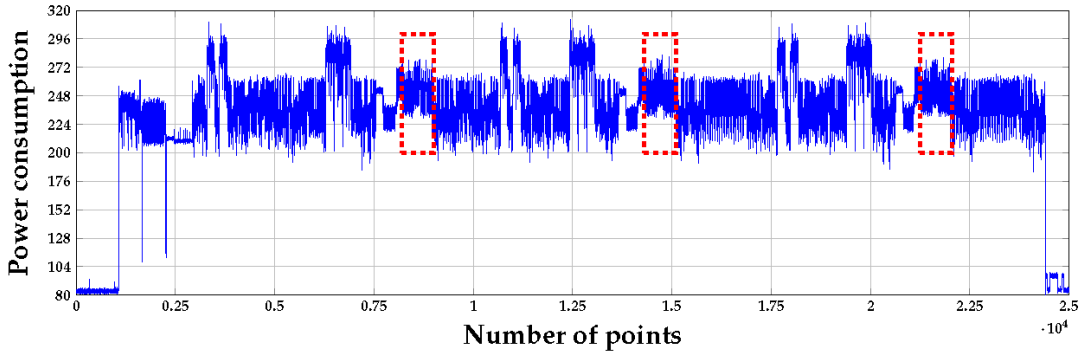


Figure 4. Measured trace when performing the financial IC card protocol.

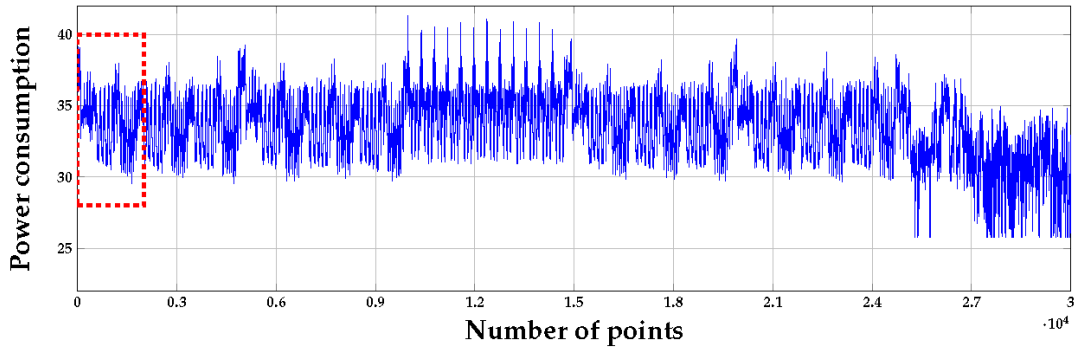


Figure 5. A trace for the *DEA* algorithm.

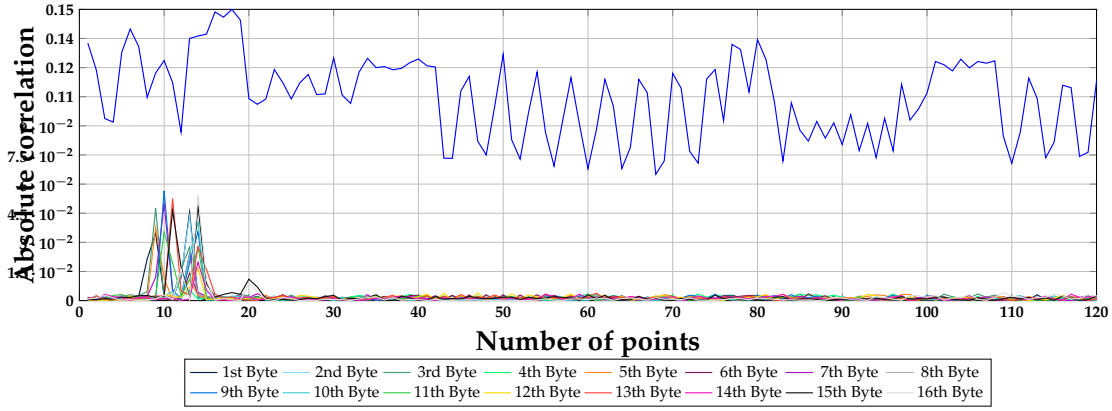


Figure 6. Result of correlation power analysis with plaintext information.

The best solution is as follows.

- Compression scheme: sum of squares
- Compression Ratio : 800

The sum of squares scheme indicates that N points were squared and summed up to a single point, where N implies the compression ratio. All 16 bytes of plaintext were analyzed at the front part of the foremost DEA operation. The alignment based on correlation was performed as a default pre-processing scheme with extensive trial-and-error. Finally, the best solution was obtained. Afterwards, the best solution was utilized to perform side channel analysis for a main target.

4.2. Security Evaluation for Financial IC Card Protocol

As shown in Figure 3, the security for a financial IC card, including state-of-the-art attack schemes described in Section 3.2.1, was evaluated. Before performing the side channel analysis defined in Section 3.2.1, the applied countermeasure was estimated in block cipher SEED by investigating some power traces.

As discussed in Section 4.1, it can be estimated that some countermeasures may be applied to only 1, 2, 15, and 16 rounds in the DEA operation of Figure 5, since the middle part can be divided into 12 rounds. Additionally, 1, 2, 15 and 16 rounds were thicker than the middle part. The first round can be split into three parts, due to the identical operation being repeated three times in 1 round. Therefore, the first part of 1 round can refer to the red box in Figure 5.

Five different behaviors were also confirmed in all the collected traces. As seen in Figure 7, the different points are the middle part of the five behaviors. The middle part of the first behavior is composed of four negative peaks. By the same logic, the middle part of the fifth behavior consists of eight negative peaks. The second, third, and fourth behaviors also have same features. Naturally, it was predicted that these behaviors may be connected to S-box operation, since the G-function of the first round has four S-box operations. It seems that the random dummy operation may be applied to that if this computation is a real S-box operation. Two possible criteria for obtaining some leakages in order to perform side channel analysis are the back and forth of S-box operations. In other words, there are two alignment points. The result of the alignment to the back of S-box operations is shown in Figure 7.

The aim of alignment to the front of the S-box operations is to analyze the plaintext and S-box operations. Furthermore, the purpose of the other alignment is to analyze the output of G-function and S-box operations. This is directly related to the suggestion of [19]. To sum up, the notations are defined as below, according to the following alignment criteria:

- Alignment 1: front of S-box operations.
- Alignment 2: rear of S-box operations (refer to Figure 7).

4.2.1. Result of Performing Side Channel Analysis Defined in Enumeration

This section describes the side channel analysis performed using the defined scheme in Section 3.2.1. As a result, we cannot identify any secret information for Alignment 1. Therefore, it is represented to all results for Alignment 2 in this section. None of the first-order leakage on the collect traces was revealed, and the second-order leakage of the combination between each of the S-boxes was also not exposed. However, by performing item 2b, two round keys can be retrieved as shown in Table 1.

Figure 8 represents the result for the first G-function of 1 round based on all combinations in Appendix A. Additionally, the x-axis and y-axis indicate the absolute correlation and key candidates, respectively. In general, the key candidate with the highest value is considered to be the correct key.

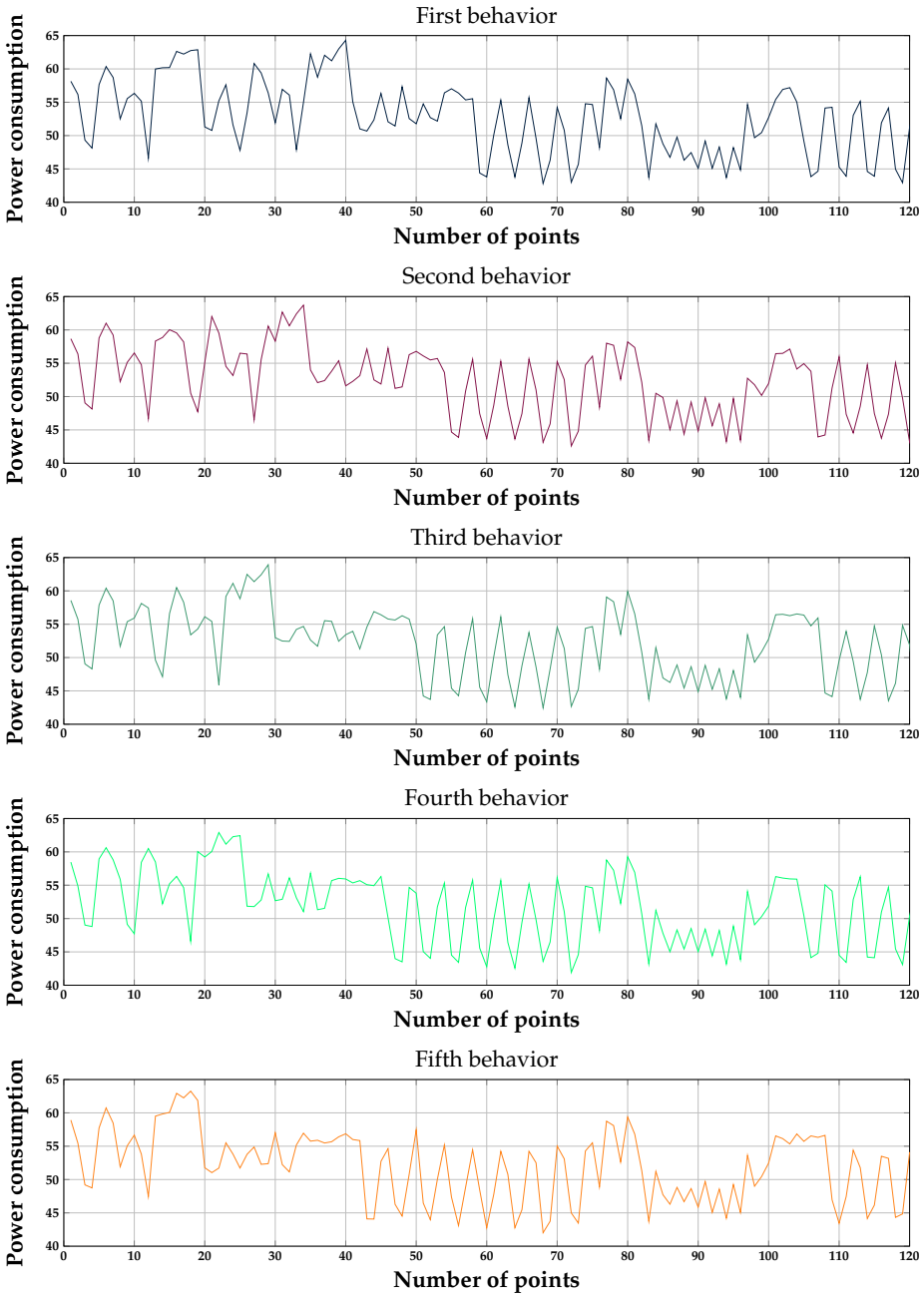
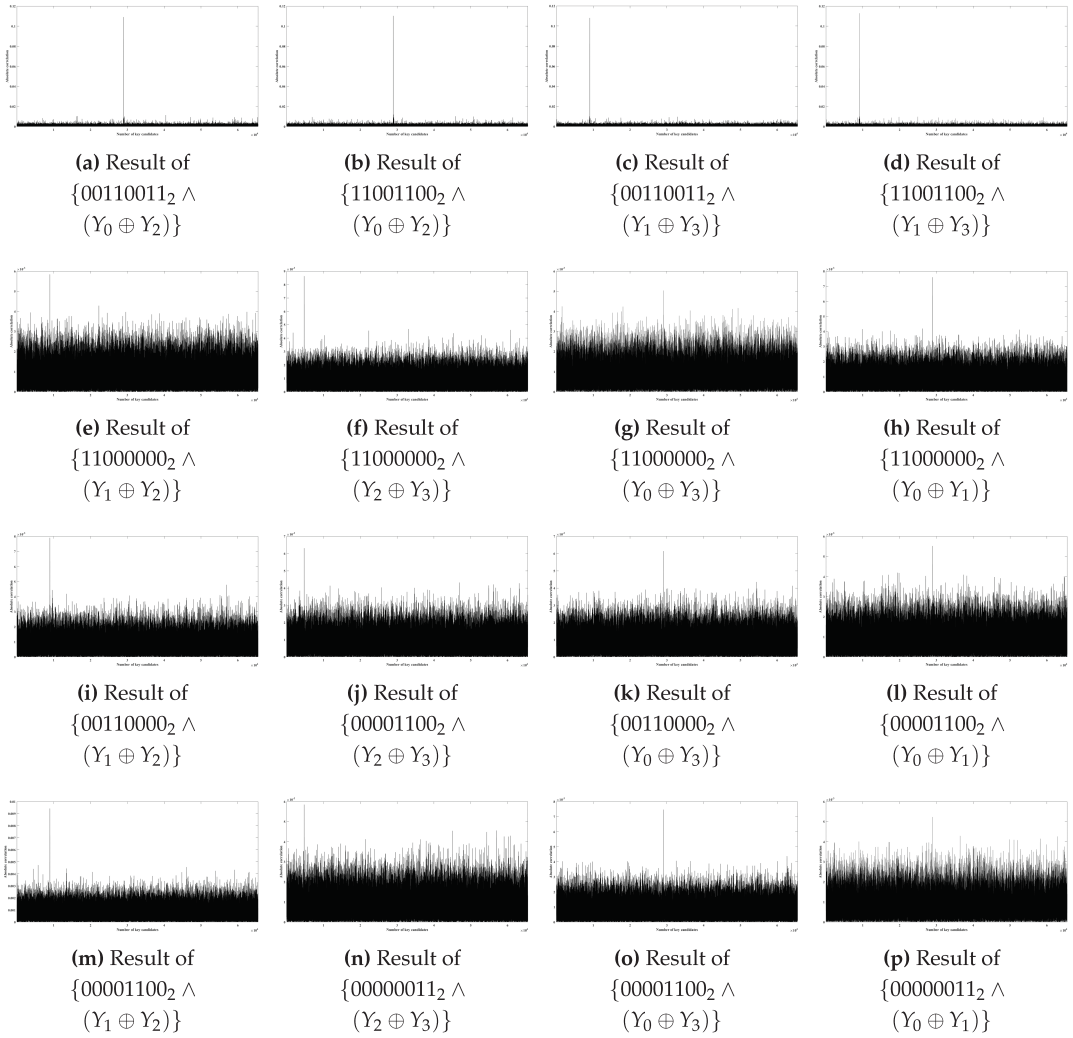


Figure 7. Five behaviors when operating DEA algorithm.

When considering all combinations, there are 20 results. As shown in Figure 8, the result is only represented if the correct key is retrieved. As described in Appendix A, the performance is superior to that of the previous proposal [19], owing to the fact that results Figure 8a–d have higher correlation. In order to analyze all combinations, 1,000,000 traces were collected. However, only 20,000 traces were required to recover the correct key in results Figure 8a–d.

By analyzing the first G-function of 1 round, the xored key $K_{1,0} \oplus K_{1,1}$ can be acquired. Therefore, it is necessary to analyze the second G-function of 1 round, the first G-function of 2 round, and the second G-function of 2 round to obtain two round keys. All results are analogous to Figure 8.



(a) Result of $\{00110011_2 \wedge (Y_0 \oplus Y_2)\}$ **(b)** Result of $\{11001100_2 \wedge (Y_0 \oplus Y_2)\}$ **(c)** Result of $\{00110011_2 \wedge (Y_1 \oplus Y_3)\}$ **(d)** Result of $\{11001100_2 \wedge (Y_1 \oplus Y_3)\}$

(e) Result of $\{11000000_2 \wedge (Y_1 \oplus Y_2)\}$ **(f)** Result of $\{11000000_2 \wedge (Y_2 \oplus Y_3)\}$ **(g)** Result of $\{11000000_2 \wedge (Y_0 \oplus Y_3)\}$ **(h)** Result of $\{11000000_2 \wedge (Y_0 \oplus Y_1)\}$

(i) Result of $\{00110000_2 \wedge (Y_1 \oplus Y_2)\}$ **(j)** Result of $\{00001100_2 \wedge (Y_2 \oplus Y_3)\}$ **(k)** Result of $\{00110000_2 \wedge (Y_0 \oplus Y_3)\}$ **(l)** Result of $\{00001100_2 \wedge (Y_0 \oplus Y_1)\}$

(m) Result of $\{00001100_2 \wedge (Y_1 \oplus Y_2)\}$ **(n)** Result of $\{00000011_2 \wedge (Y_2 \oplus Y_3)\}$ **(o)** Result of $\{00001100_2 \wedge (Y_0 \oplus Y_3)\}$ **(p)** Result of $\{00000011_2 \wedge (Y_0 \oplus Y_1)\}$

Figure 8. When performing combinations defined in item 2b, the result is only represented if the correct key is revealed.

Table 1. Analyzed two round keys.

Round Key	Value
$K_{1,0}$	0x$D555B112$
$K_{1,1}$	0x$A476A39F$
$K_{2,0}$	0x15043F29
$K_{2,1}$	0x1886$A9FA$

4.3. Recovering the Master Key via Two Round Keys

Two round keys were already retrieved to recover the master key. At first, the G-function in 1 round, the $K_{1,0} \oplus K_{1,1}$, is used for the G-function. Therefore, it was necessary to perform side channel analysis for the second G-function in order to recover each $K_{1,0}$ and $K_{1,1}$. By the same logic, the second round key can be recovered.

To calculate the master key, a correct single pair $(R_C, R_T, UP_C^*, CT*_C)$ should be acquired in the financial IC card protocol. Afterwards, Algorithm 1 is operated to recover a correct master key.

As mentioned earlier, R_T and UP_C^* were controlled by the adversary, utilizing a fake ATM. Therefore, we set to the fixed zero value. The result of performing Algorithm 1 is as follows.

As shown in Figure 9, the number of filtering temporary keys is 16. Finally, the analyzed master key (0xE73A67FFE48EF10DD542EC7BE57A9FBE) could be recovered by utilizing a correct pair defined in Table 2.

Table 2. A correct single pair.

A Correct Single Pair	Value
R_C	0x41A4E5052FC75CAB15C2715E8897C11E
R_T	0x00000000000000000000000000000000
UP_C^*	0x00000000000000000000000000000000
CT_C^*	0x9B0A4C535916A73D7E328F5$EBAF$691F9

```
Calculating the input of G-Function

G^-1[K1,0]: 1E45DAC1
G^-1[K1,1]: 9D4BCB08
G^-1[K2,0]: A6BB336F
G^-1[K2,1]: 56D8E2A6

Guessing the Master Key Candidates

Filtering the Incorrect Key

The number of Master Key Candidates : 16

Brute Force Attack

E7 3A 67 FF E4 8E F1 0D D5 42 EC 7B E5 7A 9F BE
```

Figure 9. Analyzed master key

5. Conclusions

A specific payment system is one that is only applied to its domestic market. In the Republic of Korea, the specific payment system is employed when using a credit or debit card. A side channel countermeasure should be required when using the financial IC card to prevent state-of-the-art attacks. This study demonstrated that the correct key can be revealed by expanding upon the suggestion of [19]. Consequently, the master key can be completely recovered by utilizing state-of-the-art side channel attacks and brute force attacks. Note that powerful countermeasures should be applied to financial IC card protocol, considering the expiration date and technological advances of side channel attacks.

Instant countermeasure to our attack. To defend our suggestion, each of the diffusion layer outputs should be covered with different masking values. Furthermore, this computation should be done in shuffling countermeasure and with acceptable overhead. In other words, if the diffusion layer consists of AND and XOR operations, the countermeasure should be carefully designed.

Author Contributions: This article is an extended version of [19]. Moreover, the authors evaluated the security for the financial IC card [20], expanding upon the previous paper [19]. Additionally, these authors contributed equally to this work.

Funding: This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00520, Development of SCR-Friendly Symmetric Key Cryptosystem and Its Application Modes).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. All Combinations for Novel Leakage of the Block Cipher SEED

Won et al. [19] showed novel leakage of the block cipher SEED in the output of the G-function. From the perspective of second-order analysis, the combination between the outputs of the G-function

allows low complexity in the partial bits of all bits. In other words, powerful countermeasures can sometimes be applied to only confusion layers, because the diffusion layer entail a high complexity to perform side channel analysis. That is, a low-level countermeasure can be employed in the diffusion layer. Assuming this concept, novel side channel leakage for the output of the diffusion layer has been demonstrated. Lemma 1 was established in [19] to apply the combination of second-order leakage in the output of G-function. This Appendix expands the suggestion of [19] to all cases. Note that all notations are the same as in [19].

Case 1 $Z_0 \oplus Z_1$ (Refer to [19] for a detailed description)

$$\begin{aligned} Z_0 \oplus Z_1 =& \{11000000_2 \wedge (Y_2 \oplus Y_3)\} \\ & \oplus \{00110000_2 \wedge (Y_1 \oplus Y_2)\} \\ & \oplus \{00001100_2 \wedge (Y_0 \oplus Y_1)\} \\ & \oplus \{00000011_2 \wedge (Y_3 \oplus Y_0)\} \end{aligned}$$

Case 2 $Z_0 \oplus Z_2$

$$\begin{aligned} Z_0 \oplus Z_2 =& \{(M_0 \wedge Y_0) \oplus (M_1 \wedge Y_1) \oplus (M_2 \wedge Y_2) \oplus (M_3 \wedge Y_3)\} \\ & \oplus \{(M_2 \wedge Y_0) \oplus (M_3 \wedge Y_1) \oplus (M_0 \wedge Y_2) \oplus (M_1 \wedge Y_3)\} \\ =& \{(M_0 \oplus M_2) \wedge Y_0\} \oplus \{(M_1 \oplus M_3) \wedge Y_1\} \\ & \oplus \{(M_2 \oplus M_0) \wedge Y_2\} \oplus \{(M_3 \oplus M_1) \wedge Y_3\} \\ =& (00110011_2 \wedge Y_0) \oplus (11001100_2 \wedge Y_1) \\ & \oplus (00110011_2 \wedge Y_2) \oplus (11001100_2 \wedge Y_3) \\ =& \{11001100_2 \wedge (Y_1 \oplus Y_3)\} \\ & \oplus \{00110011_2 \wedge (Y_0 \oplus Y_2)\} \end{aligned}$$

Case 3 $Z_0 \oplus Z_3$

$$\begin{aligned} Z_0 \oplus Z_3 =& \{(M_0 \wedge Y_0) \oplus (M_1 \wedge Y_1) \oplus (M_2 \wedge Y_2) \oplus (M_3 \wedge Y_3)\} \\ & \oplus \{(M_3 \wedge Y_0) \oplus (M_0 \wedge Y_1) \oplus (M_1 \wedge Y_2) \oplus (M_2 \wedge Y_3)\} \\ =& \{(M_0 \oplus M_3) \wedge Y_0\} \oplus \{(M_1 \oplus M_0) \wedge Y_1\} \\ & \oplus \{(M_2 \oplus M_1) \wedge Y_2\} \oplus \{(M_3 \oplus M_2) \wedge Y_3\} \\ =& (11000011_2 \wedge Y_0) \oplus (00001111_2 \wedge Y_1) \\ & \oplus (00111100_2 \wedge Y_2) \oplus (11110000_2 \wedge Y_3) \\ =& \{11000000_2 \wedge (Y_3 \oplus Y_0)\} \\ & \oplus \{00110000_2 \wedge (Y_2 \oplus Y_3)\} \\ & \oplus \{00001100_2 \wedge (Y_1 \oplus Y_2)\} \\ & \oplus \{00000011_2 \wedge (Y_0 \oplus Y_1)\} \end{aligned}$$

Case 4 $Z_1 \oplus Z_2$

$$\begin{aligned}
Z_1 \oplus Z_2 =& \{(M_1 \wedge Y_0) \oplus (M_2 \wedge Y_1) \oplus (M_3 \wedge Y_2) \oplus (M_0 \wedge Y_3)\} \\
& \oplus \{(M_2 \wedge Y_0) \oplus (M_3 \wedge Y_1) \oplus (M_0 \wedge Y_2) \oplus (M_1 \wedge Y_3)\} \\
=& \{(M_1 \oplus M_2) \wedge Y_0\} \oplus \{(M_2 \oplus M_3) \wedge Y_1\} \\
& \oplus \{(M_3 \oplus M_0) \wedge Y_2\} \oplus \{(M_0 \oplus M_1) \wedge Y_3\} \\
=& (00111100_2 \wedge Y_0) \oplus (11110000_2 \wedge Y_1) \\
& \oplus (11000011_2 \wedge Y_2) \oplus (00001111_2 \wedge Y_3) \\
=& \{11000000_2 \wedge (Y_1 \oplus Y_2)\} \\
& \oplus \{00110000_2 \wedge (Y_0 \oplus Y_1)\} \\
& \oplus \{00001100_2 \wedge (Y_3 \oplus Y_0)\} \\
& \oplus \{00000011_2 \wedge (Y_2 \oplus Y_3)\}
\end{aligned}$$

Case 5 $Z_1 \oplus Z_3$

$$\begin{aligned}
Z_1 \oplus Z_3 =& \{(M_1 \wedge Y_0) \oplus (M_2 \wedge Y_1) \oplus (M_3 \wedge Y_2) \oplus (M_0 \wedge Y_3)\} \\
& \oplus \{(M_3 \wedge Y_0) \oplus (M_0 \wedge Y_1) \oplus (M_1 \wedge Y_2) \oplus (M_2 \wedge Y_3)\} \\
=& \{(M_1 \oplus M_3) \wedge Y_0\} \oplus \{(M_2 \oplus M_0) \wedge Y_1\} \\
& \oplus \{(M_3 \oplus M_1) \wedge Y_2\} \oplus \{(M_0 \oplus M_2) \wedge Y_3\} \\
=& (11001100_2 \wedge Y_0) \oplus (00110011_2 \wedge Y_1) \\
& \oplus (11001100_2 \wedge Y_2) \oplus (00110011_2 \wedge Y_3) \\
=& \{11001100_2 \wedge (Y_0 \oplus Y_2)\} \\
& \oplus \{00110011_2 \wedge (Y_1 \oplus Y_3)\}
\end{aligned}$$

Case 6 $Z_2 \oplus Z_3$

$$\begin{aligned}
Z_2 \oplus Z_3 =& \{(M_2 \wedge Y_0) \oplus (M_3 \wedge Y_1) \oplus (M_0 \wedge Y_2) \oplus (M_1 \wedge Y_3)\} \\
& \oplus \{(M_3 \wedge Y_0) \oplus (M_0 \wedge Y_1) \oplus (M_1 \wedge Y_2) \oplus (M_2 \wedge Y_3)\} \\
=& \{(M_2 \oplus M_3) \wedge Y_0\} \oplus \{(M_3 \oplus M_0) \wedge Y_1\} \\
& \oplus \{(M_0 \oplus M_1) \wedge Y_2\} \oplus \{(M_1 \oplus M_2) \wedge Y_3\} \\
=& (11110000_2 \wedge Y_0) \oplus (11000011_2 \wedge Y_1) \\
& \oplus (00001111_2 \wedge Y_2) \oplus (00111100_2 \wedge Y_3) \\
=& \{11000000_2 \wedge (Y_0 \oplus Y_1)\} \\
& \oplus \{00110000_2 \wedge (Y_3 \oplus Y_0)\} \\
& \oplus \{00001100_2 \wedge (Y_2 \oplus Y_3)\} \\
& \oplus \{00000011_2 \wedge (Y_1 \oplus Y_2)\}
\end{aligned}$$

Case 1, which is suggested in [19], is significantly analogous to Cases 3, 4, and 6. However, Cases 2 and 5 are distinct from the proposal in [19]. In other words, these combinations can only be leaked information about $(Y_1 \oplus Y_3)$ and $(Y_0 \oplus Y_2)$. Although Cases 2 and 5 are only associated with two combinations, more correlation bits are leaked for these cases due to four bits of eight bits being related to second-order leakage. Therefore, side channel analysis related to Cases 2 and 5 can first be performed to discover some leakages.

References

1. Herbst, C.; Oswald, E.; Mangard, S. An AES Smart Card Implementation Resistant to Power Analysis Attacks. In Proceedings of the International Conference on Applied Cryptography & Network Security (ACNS), Singapore, 6–9 June 2006; pp. 239–252.
2. Kim, H.; Cho, Y.I.; Choi, D.; Han, D.G.; Hong, S. Efficient masked implementation for SEED based on combined masking. *ETRI J.* **2011**, 33, 267–274. [CrossRef]
3. Bonnecaze, A.; Liardet, P.; Venelli, A. AES Side-Channel Countermeasure using Random Tower Field Constructions. *Des. Codes Cryptogr.* **2013**, 69, 331–349. [CrossRef]
4. Coron, J.-S. Higher Order Masking of Look-up Tables. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Cophenhagen, Denmark, 11–15 May 2014; pp. 441–458.
5. Coron, J.-S.; Prouff, E.; Rivain, M.; Roche, T. Higher-Order Side Channel Security and Mask Refreshing. In Proceedings of the International Workshop on Fast Software Encryption (FSE), Singapore, 11–13 March 2013; pp. 410–424.
6. Fumaroli, G.; Martinelli, A.; Prouff, E.; Rivain, M. Affine Masking against Higher-Order Side Channel Analysis. In Proceedings of the International Workshop on Selected Areas in Cryptography (SAC), Waterloo, ON, Canada, 12–13 August 2010; pp. 262–280.
7. Goudarzi, D.; Rivain, M. How Fast Can Higher-Order Masking Be in Software? In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Paris, France, 30 April–4 May 2017; pp. 567–597.
8. Grosso, V.; Standaert, F.-X.; Prouff, E. Low Entropy Masking Schemes, Revisited. In Proceedings of the Smart Card Research and Advanced Application Conference (CARDIS), Berlin, Germany, 27–29 November 2013; pp. 33–43.
9. Kim, H.; Hong, S.; Lim, J. A Fast and Provably Secure Higher-Order Masking of AES S-box. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Nara, Japan, 25–27 September 2011; pp. 95–107.
10. Prouff, E.; Rivain, M. A Generic Method for Secure SBox Implementation. In Proceedings of the International Workshop on Information Security Applications (WISA), Juju Island, Korea, 27–29 August 2007; pp. 227–244.
11. Rivain, M.; Prouff, E.; Doget, J. Higher-Order Masking and Shuffling for Software Implementations of Block Ciphers. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Lausanne, Switzerland, 6–9 September 2009; pp. 171–188.
12. Tillich, S.; Herbst, C. Attacking State-of-the-Art Software Countermeasures—A Case Study for AES. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Washington, DC, USA, 10–13 August 2008; pp. 228–243.
13. Tillich, S.; Herbst, C.; Mangard, S. Protecting AES software implementations on 32-bit processors against power analysis. In Proceedings of the International Conference on Applied Cryptography & Network Security (ACNS), Zhuhai, China, 5–8 June 2007; pp. 141–157.
14. Brier, E.; Clavier, C.; Olivier, F. Correlation Power Analysis with a Leakage Model. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Cambridge, MA, USA, 11–13 August 2004; pp. 16–29.
15. Balasch, J.; Gierlichs, B.; Grosso, V.; Reparaz, O.; Standaert, F.-X. On the Cost of Lazy Engineering for Masked Software Implementations. In Proceedings of the Smart Card Research and Advanced Application Conference (CARDIS), Paris, France, 5–7 November 2014; pp. 64–81.
16. Kocher, P.; Jaffe, J.; Jun, B. Differential Power Analysis. In Proceedings of the International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 15–19 August 1999; pp. 388–397.
17. Pan, J.; den Hartog, J.I.; Lu, J. You Cannot Hide behind the Mask: Power Analysis on a Provably Secure S-Box Implementation. In Proceedings of the International Workshop on Information Security Applications (WISA), Jeju Ireland, Korea, 25–27 August 2009; pp. 178–192.
18. Prouff, E.; Rivain, M.; Bevan, R. Statistical Analysis of Second Order Differential Power Analysis. *IEEE Trans. Comput.* **2009**, 58, 799–814. [CrossRef]

19. Won, Y.-S.; Park, A.; Han, D.-G. Novel Leakage against Realistic Masking and Shuffling Countermeasures—Case study on PRINCE and SEED. In Proceedings of the International Conference on Information Security and Cryptology (ICISC), Seoul, Korea, 29 November–1 December 2017; pp. 139–154.
20. The Bank of Korea. *CFIP.ST.FINIC-02-2012: Standards for Financial IC Cards Specification Part 2–Open Platform*; The Bank of Korea: Seoul, Korea, 2012.
21. Korea Information Security Agency (KISA). *TTAS KO-12.0004: Block Cipher Algorithm SEED*; KISA: Seoul, Korea, 1999.
22. Kim, C.; Park, I. Investigation of Side Channel Analysis Attacks on Financial IC Cards. In Proceedings of the Korea Institute of Information Security & Cryptology (KIISC), Seoul, Korea, 29 November–1 December 2017; pp. 31–39.
23. Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES). Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (accessed on 10 November 2018).
24. Goubin, L. A Sound Method for Switching between Boolean and Arithmetic Masking. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Paris, France, 13–16 May 2001; pp. 3–15.
25. Coron, J.-S.; Tchulkine, A. A New Algorithm for Switching from Arithmetic to Boolean Masking. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Cologne, Germany, 7–10 September 2003; pp. 89–97.
26. Neiße, O.; Pulkus, J. Switching Blindings with a View Towards IDEA. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Cambridge, MA, USA, 11–13 August 2004; pp. 230–239.
27. Rivain, M.; Dottax, E.; Prouff, E. Block Ciphers Implementations Provably Secure Against Second Order Side Channel Analysis. In Proceedings of the International Workshop on Fast Software Encryption (FSE), Lausanne, Switzerland, 10–13 February 2008; pp. 127–143.
28. Debaize, B. Efficient and Provably Secure Methods for Switching from Arithmetic to Boolean Masking. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Leuven, Belgium, 9–12 September 2012; pp. 107–121.
29. Coron, J.-S.; Großschädl, J.; Vadnala, P.K. Secure Conversion between Boolean and Arithmetic Masking of Any Order. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (CHES), Busan, Korea, 23–26 September 2014; pp. 188–205.
30. Karroumi, M.; Richard, B.; Joye, M. Addition with Blinded Operands. In Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design, Paris, France, 14–15 April 2014; pp. 41–55.
31. Vadnala, P.K.; Großschädl, J. Faster Mask Conversion with Lookup Tables. In Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design, Berlin, Germany, 13–14 April 2015; pp. 207–221.
32. Won, Y.-S.; Han, D.-G. Efficient Conversion Method from Arithmetic to Boolean Masking in Constrained Devices. In Proceedings of the International Workshop on Constructive Side-Channel Analysis and Secure Design, Paris, France, 13–14 April 2017; pp. 120–137.
33. Available online: http://www.dpacontest.org/home (accessed on 10 November 2018).
34. SCARF Project. Available online: http://www.k-scarf.or.kr/ (accessed on 10 November 2018).
35. Yoo, H.; Kim, C.; Ha, J.; Moon, S.; Park, I. Side Channel Cryptanalysis on SEED. In Proceedings of the International Workshop on Information Security Applications (WISA), Jeju Island, Korea, 23–25 August 2004; pp. 411–424.