Breaking Korea Tansit Card with Side-Channel Analysis Attack - Unauthorized recharging -

Tae Won Kim[1,2], Tae Hyun Kim[1], and Seokhie Hong[2]

[1] SNTWORKS, Gyeonggi-do, South Korea
[2] Center for Information Security Technologies, Korea University, Seoul, South Korea

Recent side-channel attacks have shown that the security of smart devices are a matter of serious concern. In this paper, we target a real-world smartcard embedding cryptographic features. We completely restored the secret key in the device using the side-channel analysis attack, although this employs some countermeasures against side-channel attacks. We provide details on how to extract the secret key in an environment that gives the attacker only public information of the target device. As a result of our attack, 128-bit secret key for mutual authentication required when a legitimate user uses functions served by card such as payment, refund, recharging et al. can be completely restored. Finally, with the restored key we are able to free recharge balance on the card as much as attacker want without spending any money.

Keywords: smartcard, side channel analysis attack, Triple DES

I. Introduction

Side-channel analysis attacks are a serious threat to the security of embedded devices, such as credit card, mobile phone SIMs. Moreover, due to the increase in Internet of Things (IoT) market, countermeasures against side channel analysis are widely studied.

Core idea of Side-channel analysis attacks is to exploit key-dependent signals, such as timing [1], power consumption [2], and electromagnetic radiation [3,4] that was evaluated during the execution cryptosystem in device, by measuring physical quantities. Initially, P. Kocher et al. introduced the two types of side-channel attack: simple power analysis attack (SPA), differential power analysis attack (DPA) [1,2]. Many related attacks [5-11] and countermeasures [12-17] have been studied widely until now.

Power analysis attacks are one of the most powerful and efficient techniques among the these attacks. Especially, Correlation Power Analysis (CPA) attacks can retrieve secret information from the statistical tool such as correlation coefficient by using power consumption traces [7].

Electromagnetic Analysis (EMA) attacks are a powerful and popular method as much as the DPA. These attacks can be approached in the same manners as DPA. Note that the EMA do not need to connect the ground for measurement of side-channel signals as opposed to DPA. Thus, electromagnetic analysis attacks more widely have been used than power analysis attacks.

Beyond theoretical analysis and experiment with Device under Test, practical investigation with respect to real-world devices was showed by academic research and relevant to industry [18-23]. In [18], they presented how the KeeLoq, implemented in hardware and software, can be broken from power analysis attack. As presented in [19-21], these papers offer results of attack for new target (Xilinx Virtex FPGA, braking system in a car laptop PC respectively). It means that side-channel analysis attacks can be applied to various target using cryptography system. Investigations, having a significant impact on the real-world attack for the smartcard are shown in [22, 23]. Both results described how to recover the full-key of crypto algorithm equipped in target devices using power analysis attacks on commercial smartcard.

In this paper, we specifically present breaking the Korea transit card under black box attack environment using power analysis attacks. Although the target device employed countermeasure that can be typically classified as hiding [8, 13-15] against SCA attacks, we could retrieve the full key by using conventional power analysis attacks. As a result of our attack, we could increase the balance in the transit card without required any money by recharging with restored secret information. This was demonstrated by simulation in practice with capturing a video. We provide in detail how to set up for an attack environment and an attack for recovering the key and design an unauthorized recharging system in terms of our target device.

This paper is organized as follows: First, we describe information about our target device such as authentication protocol and cryptosystem etc. in Sect. II. Section III gives methods and approaches for attacking in black box environment including know-how from many trials and errors. Section IV shows practical results of power analysis attack based on described in Sect. III. We present designing an illegal recharging system and simulate practically it in Sect. V. Finally, Sect. VI concludes the paper.

II. Target Device Details

In this section, we present specifications required to attack a target device through side-channel analysis attacks. We notice that described all information in this section are based on public information. (see [24, 25] for more information).

1. Transit Card

Our target device is a pre-paid transit card for the freeway in Korea almost one out of three cars that passes freeway used this card. Over 800 million cards were issued and used, in July 2016.

This not only can pay the toll fees when passing the all toll gates across the country but also can be used to pay in cafeteria and convenience store on the freeway service area.

This card is a contact IC smartcard communicating with a card reader by direct physical contact. According to data sheet, the contact IC card interface supports an International Standard under ISO/IEC 7816. And it has been specified a KS X 6924 Korean industrial standard approved by Korean Agency for Technology and Standards (KATS) in 2014 for authentication protocol, command and cryptography algorithm.

For data encryption, signature/verification and authentication, the target smartcard runs a hardware based symmetric-key cryptosystem which employs hiding countermeasure to thwart power analysis attack in hardware level.

2. Authentication protocol

Our goal is to recharge balance of a pre-paid transit card in an unauthorized manner. Therefore, we need to examine the entire charging phase when balance stored in the card is increased through authentication. We can profile useful information for side-channel analysis attacks by analyzing the authentication protocol for recharging process. It is an important task to determine target points for side-channel analysis attacks and indicate location of target operation in a power trace. The following figure is the authentication protocol for recharging the balance.

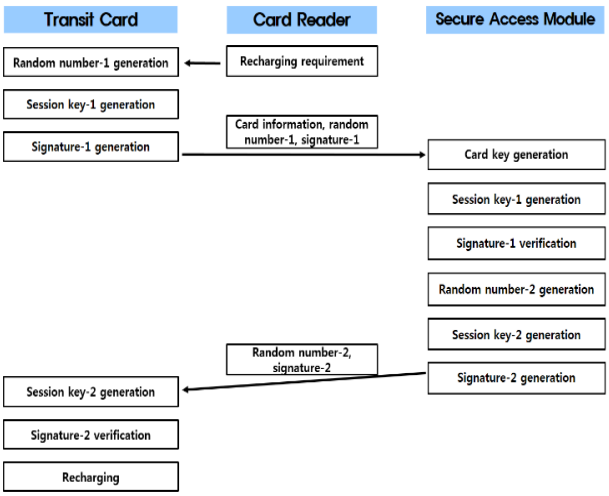

Figure 1. Authentication Protocol for Recharging the Balance.

Entities in the above authentication are the smartcard and Secure Access Module (SAM).

The first step towards recharging is that given recharging command by user, the smartcard generates a session key through cryptosystem with random numbers obtained

internally and a card key stored in ROM. The session key is used as a one-time key generated randomly in every event. To be an authorized entity, the card generates Signature-1 with the session key and the unique card information. After then, this information that was used to generate Signature-1 is send to the SAM.

Since the authentication mechanism in our target device is based on symmetric key cryptography, to verify given Signature-1, the identical key that was used to generate the signature in the smartcard is needed. There is a unique card key for each card that was generated by cryptosystem using the SAM's mater key and each card information. Thus, the SAM can generate and share the card key using the received card. After that, the SAM generates signature and verifies its validity through comparing with the received signature.

The subsequent authentication procedure is identical but reverse entities in signature and verification to mutually authenticate each other as presented in Figure 1. After the authentication protocol is completely finished, the balance can be increased.

3. Cryptosystem

Figure 2 shows the cryptosystem used in the authentication protocol. It is enough to focus on the following cryptosystem because it is the only method used in our target device.

The cryptosystem essentially includes a crypto-function that processes data blocks of 128-bit using a cipher key with lengths of 128 bits. And it is operated in Cipher Block Chaining (CBC) mode with an initialization vector (IV) which fixed to a constant value 0^{128}. If necessary, the last block is padded with 0x8000...00 to be multiple of 128-bit.

In the authentication scheme, the most significant 32-bit of the last ciphertext block becomes the signature value.

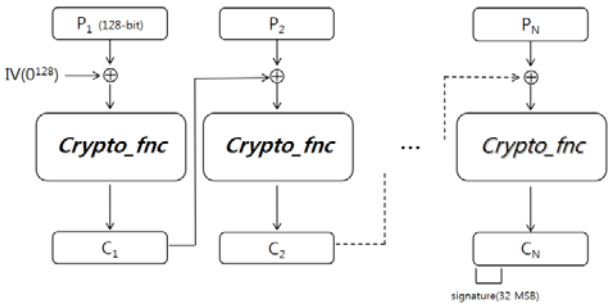

Figure 2. Cryptosystem.

In the following, we focus on the crypto-function included in the cryptosystem. Its core engine for data encryption is the Triple DES (T-DES) where processes three successive DES instances in encryption-decryption-encryption order using two 64-bit keys (K_{enc}-K_{dec}-K_{enc}) respectively.

As depicted in Figure 3, the crypto-function consists of two T-DES operations with one identical 128-bit key and 128-bit input plaintext. The input plaintext is divided into two 64-bit blocks (the most significant 64-bit and the least significant 64-bit). The XOR of two 64-bit blocks is fed into one T-DES and the least significant 64-bit block is used as the other input of T-DES. The ciphertext is generated by simply concatenating two T-DES output.

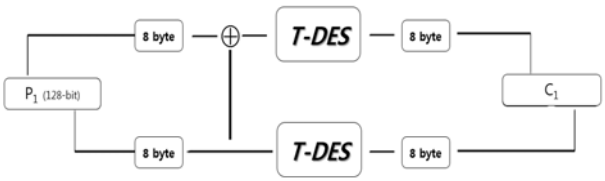

Figure 3. Crypto-function.

III. Approaches and Methods

In this section, we describe an attack scenario for our final goal - illegal recharging of balance. It starts by clarifying the secret information which we need to recover through side-channel analysis attacks. Also, we present a methodology for extracting this information. In our attack, we employ power analysis attacks as side-channel analysis attack.

This includes setup for an experimental environment to recovering the secret information being able to generate a valid signature. We describe specific step by step procedure and knowhow obtained by many trials and errors.

1. Attack Scenario

Our attack procedure can be divided into two parts. The first part is to recover secret information of the target card and second is to recharge the balance in the card.

We have to note that which information is needed to disguise as a valid user. Recall that the authentication protocol as stated in Sect.II-2. To recharge, the card verifies the validity of Signature-2 generated by the SAM. Therefore, it suffices for an attacker to generate a signature that passes authentication in the card. It means that the attacker needs the card key to generate a valid Signature-2. In other word, if an attacker recovers the card key stored in the ROM of the target card, the attacker can disguise as a valid user by sending a signature that passes verification.

2. Side-Channel Attack on Transit Card

From now on, we focus on recovering the card key. The first thing is to consider the possibility of exploiting power analysis attacks for the card key. Generally, in power analysis attacks, it requires repetitive cryptographic computations with a fixed secret key and varying plaintexts. Fortunately, this environment can be found in the authentication protocol. When the transit card generates a session key, the cryptosystem operates with our targeted card key and a random number as an input plaintext. Also as the attacker sends the recharging command to the card, it carries out these operations. This facilitates for an attacker to obtain as many side-channel signals that he can mount side-channel analysis attacks.

A. Measurement Setup

To recover information on the corresponding card key in the target device, we exploit power consumptions as physical leakage.

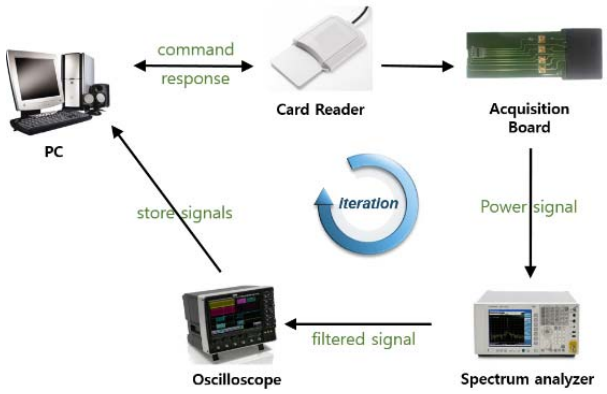

Figure 4. Measurement setup.

The exhibit above depicts our setup for measuring power consumption signal of the transit card. These composed of five hardware devices and a customized software controlling devices.

- PC

  This controls a card reader and an oscilloscope using a customized software. PC sends commands to the card reader and receives the corresponding responses from the card through the card reader. Measured side-channel signals using the oscilloscope are stored in a hard disk by the PC.

- Card Reader

  Our targeted transit card communicates with the PC through a smart card reader with ISO/IEC 7816-3 compliant electrical interface to exchange commands and data. Card readers are equipped with a USB interface or an RS-232 serial port for communication with a PC.

- Acquisition Board

  To measure power consumptions exploited in our attack, the transit card has an output pin on the microcontroller. To make it possible we fabricate an intermediary board that connect the transit card to a reader. It is equipped with a 47-Ohm resistor inserted between the GND pin on the transit card and the ground line on a reader. Also, it supports an internal I/O channel for communicating. We will use the I/O as a trigger signal in order to synchronize with an oscilloscope.

- Spectrum Analyzer

  Inevitably physical leakages such as power consumption, electromagnetic contain the noise. Thus, power consumptions measured via an acquisition board sent to a pre-processing phase in order to increase Signal-to-Noise Ratio (SNR).

  The most popular method to reduce the amount of noise in the power trace is filtering that aims at selecting the frequencies in which the success rate of the attack improves such as low-pass, high-pass, and band-pass filter [26-28].

  In view of this, a spectrum analyzer seems to be a good tool. It processes power traces by using a band-pass filter centered at a carrier frequency. And then the signal is demodulated. This processes are performed in hardware level. Thus, a spectrum analyzer comes at no additional cost for filtering phase and it leads to important advantage from attack performance perspective.

- Digital Oscilloscope

  To sample the leakage measurements, we use a digital oscilloscope which is LeCroy WaveRunner with maximum capabilities 4GHz and 40GS/s and providing 8-bit samples. It is connected to TCP/IP network to remotely control by the PC.

B. Locate the point of T-DES Execution in Measurement

We are in an attack environment without any information of internal implementations of the transit card such as operation of the system on which the cryptosystem is implemented, countermeasures against side-channel attacks and etc. So, guessing the location of cryptosystem where an attacker targets should be involved in the measurement phase before the key recovery phase.

To do so, we first mounted a correlation based attack using plaintexts and ciphertexts (here, signatures). Intuitively, it allows an attacker to detect parts relating to plaintexts and ciphertexts in a power trace. This is based on the fact that when a crypto algorithm operates in the cryptosystem, plaintext, one of the input parameters must be transferred to cryptosystem engine by data bus. When loading plaintext, power

consumption depends on the plaintext data. In this case, correlation coefficients are higher than that of cryptographic algorithm in general due to the effect of countermeasures.

Thus, by calculating correlation coefficient between input plaintexts (or output ciphertexts) and power traces, we can check where the targeted cryptographic algorithm operates in a trace. It is important to locate the target operation since it can reduce the number of trials and errors.

C. Key recovery

Note that we already mentioned that the target operation in the authentication protocol for recharging is Sessionkey-1 generation. Also, we described the mechanism for generating Sessionkey-1 in Sect. II-2. By using this information, we will present how to retrieve the card key through power analysis attacks in this subsection.

The target operation involves two T-DES encryptions using the identical keys for generating Sessionkey-1. Hence our ultimate target is T-DES implemented with two 64-bit keys (defined K_{enc}, K_{dec}). A problem recovering keys of T-DES using power analysis attacks boils down to attacking the first two successive single-DES instances among three.

For attacking the single-DES instance, we employ a divide-and-conquer strategy which is generally used in most of the differential power analysis (DPA) attacks. In the divide phase of the attack, an attacker targets the first round of the single-DES instance and recovers each 6-bit key portion of the 48-bit roundkey (usually called as sub-key). And then in the conquer phase, this information is gathered to reveal the 48-bit roundkey. In other word, it yields information about one roundkey recovered by combining the other recovered 6-bit keys in one DPA attack. After this work, the attacker needs an additional step to obtain the remaining the information for the first DES key i.e., K_{enc}. So, we apply the DPA on remaining all rounds of the DES.

Next, we calculate all intermediate values of the full sixteen rounds of DES by guessing the remaining 8 bits of 56-bit K_{enc} with the restored 48-bit round key and then perform the DPA attack on every rounds.

When guessing the remaining 8 bits of K_{enc}, we are able to find 14 peaks at each round (Round 2-16). Even though it suffices to recover the next roundkey for full key recovery, we perform the DPA attack on all remaining rounds for accuracy due to black-box attack environment.

To recover the 64-bit full key of the single-DES, i.e., K_{enc}, it requires two DPA attacks and total four DPA attacks to reveal the 128-bit card key, i.e. K_{enc}, K_{dec}. The following figure represents the flow of our attacks.

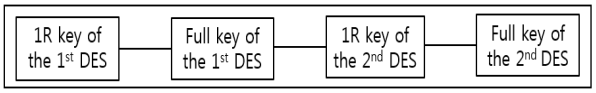

Figure 5. Block level description of key recovery mechanism

It should be noted that although we simply present here attack procedure, in practice it might be too costly to perform pre-processing by applying alignment, signal compression, correct errors for every DPA attack and so on.

To identify validity of the recovered card key, an attacker compares a valid signature with the signature generated by the obtained card key and public card information.

D. Alignment task

In the black-box attack environment, the success of the attack gives us fruitful information for the secret key and the location of the target operation at once. So, this work needs to precede varying-stage processing, associated with each other as depicted in the blow.

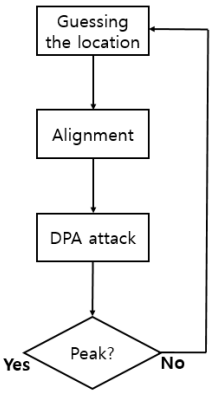

Figure 6. Processing sequence for a key recovery attack

Alignment in our attack has a lot of difficulties. One of the most difficult problems is finding a good reference pattern that can be commonly found in every power trace. This is due to hiding countermeasure such as random clock, random delay, adding intentional noise and so on in the hardware level. Hiding countermeasures disturb a successful alignment and reduce SNR. It would result in failure in recovering the secret key. So, we use a local alignment strategy and the alignment step is repetitively performed for every the DPA attack by a simple trial and error using a local alignment.

As the result of reduced SNR by hiding countermeasures, involving hardware DES engine and so on, we need the extremely large number of power traces to mount an effective DPA attack. It means that she needs a more elaborate alignment

process to increase SNR. Indeed, one or two sample points of misalignment lead to attack failure in our experiment.

E. Correction of Errors

In our attack environment, the biggest problem in key recovery aspect is that we cannot determine whether the found key is correct in each attack session or not. We only can confirm the validity of the restored key after all four DPA attacks are completely ended. Here, we note that every attack is dependent to each other. Thus, performing the next DPA attack without an error correction of the previous DPA attack, constitutes error propagation that raises failure of the remaining DPA attacks regardless of factors; the number of acquired power traces, SNR of the acquired traces etc. This error propagation increases the number of key candidates exponentially. Thus, the attack might succeed but with lots of computation that could not be finished in practical time.

Therefore, correction of errors that may be yield by DPA attack is a very crucial part of the whole 128-bit key recovery mechanism.

In the correlation power analysis attack (employed as DPA attack), the attacker classifies key candidates as the right key if correlation coefficient value is higher than given noise level[1]. Therefore, an error correction needs to be set in the context of eliminating incorrect keys having correlation higher than noise level.

To correct the errors, we employ the BS-CPA (Built-in Determined Sub-key Correlation Power Analysis) proposed by Komano et al. [29]. This is an enhanced CPA method to increase the SNR in the hardware implementation where the multiple Sbox outputs are processed in parallel. The main idea of BS-CPA is to decrease the switching noise in power consumption dependent on target secret information, by built-in the determined sub-key when recovering the next sub-key. This is indeed true for the reason that, when an attacker finds a sub-key targeting a specific Sbox, where multiple Sbox outputs are processed in parallel, portions of power consumption related to all other Sboxes are independently distributed, and they constitute switching noise.

In our attack, we utilize the idea described above and modify the BS-CPA in accordance with our purpose for correction of error. The modifying method for correction of error for one sub-key performs the following steps:

- Enumerate candidates of 6-bit sub-key having correlation coefficient value higher than given noise level by performing the classical CPA on a Sbox.
- For each sub-key candidates, built-in and then perform the CPA on other Sboxes
- Observe the seven peaks (corresponding the other seven Sbox) of CPA results for each sub-key candidate and check whether the rank maintains for each Sbox.
- Count which sub-key candidates lead to maximum peak.
- Regard candidates as more promising key by higher number of counts
- Eliminate key candidates if a count equals to zero.
- In the same manner, recursively built-in other sub-key and reduce the candidates.
- Utilize the reduced key candidates for the next DPA attack.

The method devised for the error correction applying the BS-CPA can expect more precise results since 12-bit CPA is more enhanced than 6-bit CPA. Thus, for a correct key guess, although its peak value is not the highest in 6-bit CPA, the effect of error correction appears through 12-bit CPA by change in rank close to right key guess. Also, if correct key guess has the highest peak value, its rank will remain unchanged.

By using this effect, we expect to reduce the number of enumerated key candidates and hence increase the efficiency of DPA attack for recovering the full key in single-DES instance, by prohibiting error propagation.

IV. Attack in Practice

In this section, we show the experimental results using the approach and method based on Sect. III. To extract secret information from acquired power traces, we only used public information obtained from statements in the public documentation and card response values.

Note that we did not specify all of its trials and errors but only ones that lead successful result.

1. Visual Inspection

The visual inspection phase starts with obtaining the target trace from our target device; this is depicted in Figure 7.

It represents power consumption corresponding to Signature-1 generation in the whole process of recharging. It leads to the six T-DES operations, where the first two for Sessionkey-1 generation, the remaining four for Signature-1 generation, by analyzing the recharging protocol.

[1] A theoretical noise level is bounded by 4/sqr(n), where sqr() is the square root function and n is the number of traces.

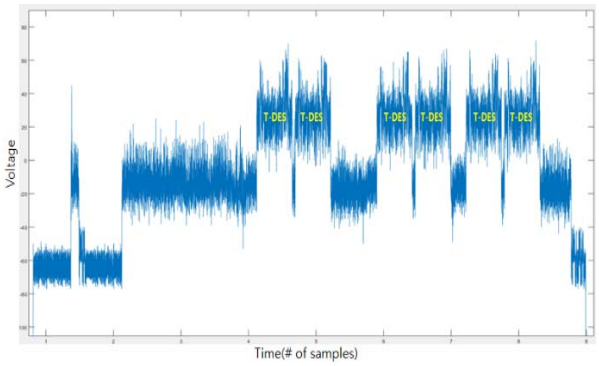

Figure 7. Full Trace.

Thanks to that information, we can easily identify the location of the six T-DES operations in the power trace by finding the six similar patterns as displayed on Figure 7. Also, it is well represented by feature typically known that power consumptions by cryptographic hardware engine with higher clock speed are higher than one by the smart card CPU.

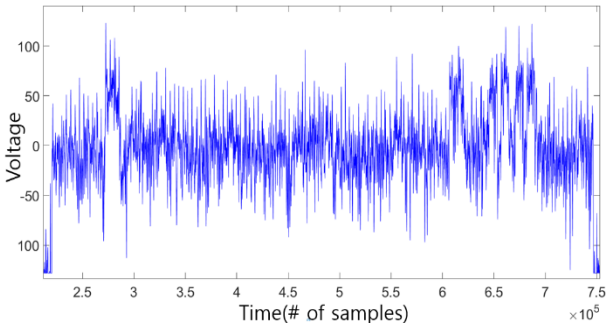

Figure 8. Zoom on the single T-DES.

Figure 8 shows a zoomed view of the single T-DES operation. To be precise, the whole interval referred to the single T-DES as in the above figure, is not leakage only depending on the single T-DES but leakage of T-DES operation and some related operations.

Since three single-DES instances are processed sequentially (Encryption-Decryption-Encryption), we can naturally predict three distinct patterns and time for the single DES instance. This is reflected in deciding the location of the target operation in order to perform the key recovery attack with the CPA.

As it turned out, a location that fulfilled these conditions through the visual inspection could not be found in our target operation. This result gives an important thing to an attacker that although visually inspecting a power trace is plausible, it is no more than pure speculation, not a significant information.

Another important property is observing the effect of implemented countermeasures against power analysis attack. By comparing numerous power traces, we can deduce that hiding methods are equipped in our target device. Hiding techniques in the hardware level such as random delay, random current, and random clock, hides key-related signals in the amplitude domain and disturbs the correct alignment in the time domain. An evidence can be found in Figure 9. When acquiring power traces, we triggered with I/O signal at the same point for every time, to obtain aligned power trace having starting point. However, we notice that the starting point we targeted is different for each measurement (see Figure 9 (a)). Also, even though the measured traces are aligned with the same starting point, we observed that the length of one DES instance varies every execution (see Figure 9 (b), (c)).

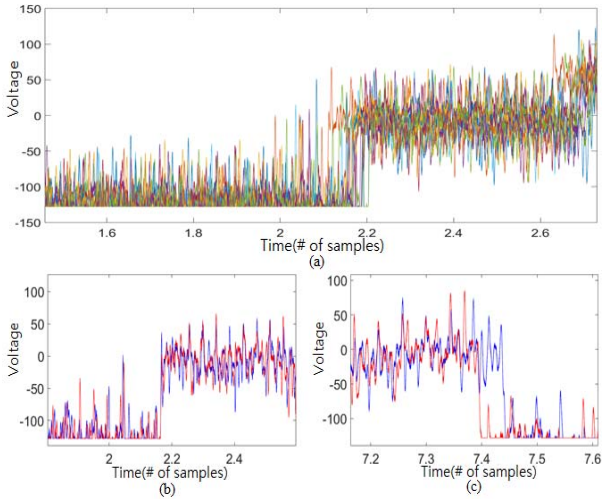

Figure 9. Countermeasure effects in the measurements

These impose preprocessing methods on the attacker which can mitigate countermeasures such as converting the frequency domain [30-32], applying various alignment methods in the time domain [7, 12, 33-36]. Also, it requires to use the large number of power traces to improve the SNR. In our attack, to overcome the misalignment problem, we use correlation coefficient based window method in the time domain, and it turned out to be the most efficient and effective method among alignment methods which we used in our attack. We further address specifically in CPA on DES instance.

2. Plaintext CPA

Intuitively, the hardware DES engine must be preceded with data loading by internal data transfer. To investigate where plaintext is loaded in power traces, clarifies the location of target operation expected information by visual inspection.

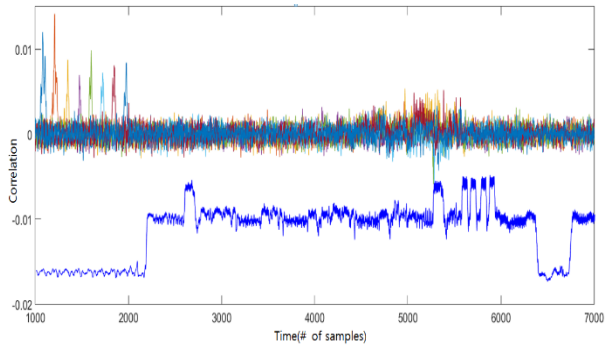

Figure 10. Result of attack with plaintext information.

Figure 10 shows an average trace of the single T-DES (plotted in blue) and correlations peak traces resulted from the 1-bytewise CPA with plaintext using hamming weight power model. Note that we compressed all power traces to reduce the time complexity. This indicates plaintext-related positions in the power trace. Interestingly peaks are divided into two groups having similar composition. One is occurred at low voltage (approximately 1000-2000 time samples), that is estimated to be the power consumption of the CPU. These significant peaks were observed in sequential order corresponding to each byte value transferred by internal data bus of the target device. The other is occurred at high voltage (approximately 5000-5500 time samples) that is estimated to be the power consumption by the cryptographic engine. These peaks were ambiguous but we could not exclude possibility of meaningful peaks since these peaks were higher than the noise level. After considering all the factors, we reached to conclusion that possible intervals for target operation are approximately 2100-5000 or 5500-6300 of time samples.

3. CPA on T-DES

We perform the CPA attack on every position inside the founded intervals, where even little possibilities for the T-DES operation exist. After tremendous trial and error, we can restore the secret information and it means that we clearly found the location of the T-DES operation at the same time.

Figure 11 shows a power trace captured during operating the T-DES. It was difficult to spot sixteen patterns for the DES round from single power trace (Figure 11(a)). Although the averaged trace (Figure 11(b)) were carried out with aligned 10,000 traces, each round in the single DES could not be distinguished. Also, we could identify random effects such as signal amplitude, length of the DES operation, that lead to misalignment and decreased the SNR by hiding. Interestingly, it was composed of four single-DES instances not three single-DES instances as depicted in Figure 11(b).

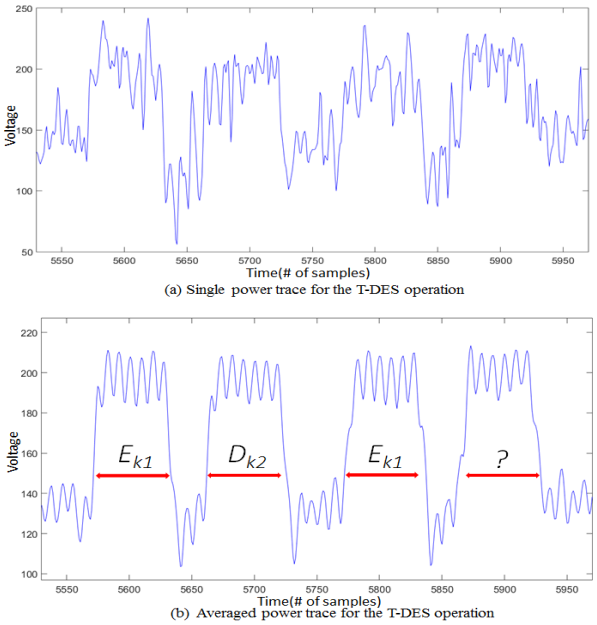

Figure 11. Zoom on the T-DES operation.

It turned out that the last DES was decryption operation with a ciphertext yielded by the prior T-DES and K_{enc}, through the CPA attack on this spot. We deduce that it is assigned as a fault countermeasure which can monitor fault injection during the T-DES operation by comparing the intermediate value of the T-DES with output value of the last DES decryption.

A. Alignment for the Single-DES

Alignment is the most time-consuming step of our attack. It requires for the reference trace to have a common pattern that could be observed in every power trace. Unfortunately, in our attack, finding this pattern was very difficult. It was impossible to perfectly arrange the power traces on time by an identical computation in the single-DES operation.

We found the best alignment technique suitable for our attack environment among existing methods which could overcome the hiding countermeasure after many trial and errors. Adopted strategy is to repeat local alignments and eliminate misalignment traces on several distinct patterns. Namely, traces having a similar pattern through Pearson correlation coefficient is only accepted, and we discarded as the dispensable ones if not. We repeatedly applied the above profiling process on the others distinct patterns to obtain well-fitted traces satisfying our preference and taste.

Figure 12 shows eight traces for the single-DES before and after alignments. We aligned on whole DES operation not considering the partial operation such as rounds, Sbox and so on.

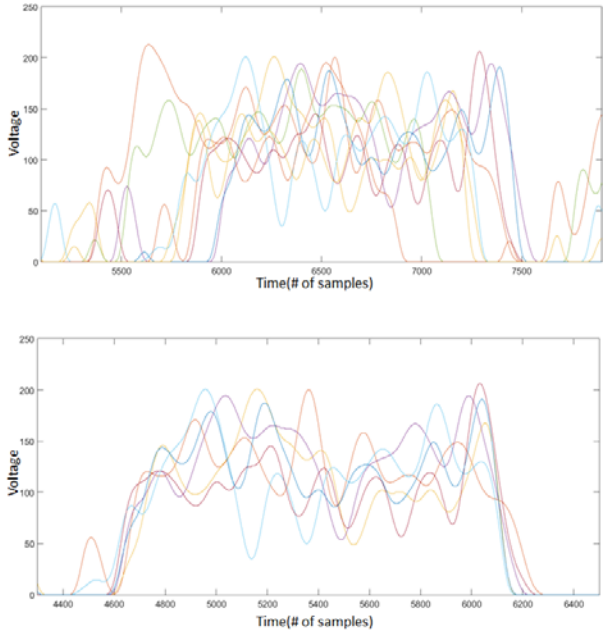

Figure 12. Example of misaligned traces (upper) and aligned traces (Bottom).

Generally, the effect of alignment is checked through visual inspection. However, since distinct patterns of power traces for the DES operation are not clear and we do not know the internal structure of the DES implementation, visual inspection might be inaccurate. Therefore, additionally, we can indirectly infer through the CPA attack result.

B. The Single-DES attack

We conduct the standard CPA on aligned and compressed traces under the Hamming distance power model between input and output of the first round of DES. The results of the attack for each Sbox are displayed in Figure 13. We are able to identify significant peaks. We note that every peak for each Sbox lies on the same location as shown in Figure 13(i) which overlaps Figure 13(a)-(h). These results indicate that the target device processes DES function, *f* including the eight Sboxs in parallel. The information deduced from the preceding attack provides a sound basis for correction of error by using the BS-CPA.

Although peaks for Sbox 5 and 7 are calculated with correct key hypotheses, it was not the highest peak in the whole interval. But, it was not difficult to correct these errors in our attack, since these peaks are the highest peak in the local interval where 1 Round is operated (between about 14-22 of samples). Indeed, sub-keys yielded by the peaks to be maximum in this local interval turn out to be correct.

As described in Sec. II-3, we performed CPA attacks on from 2 Round to 16 Round with a 32-bit Hamming distance power model by estimating the right 32-bit output of each round in the DES for 64 key candidates computed from the first round key that we recovered in the previous phase. Figure 14 shows results of attack to recover the remaining eight bits of K_{enc}.

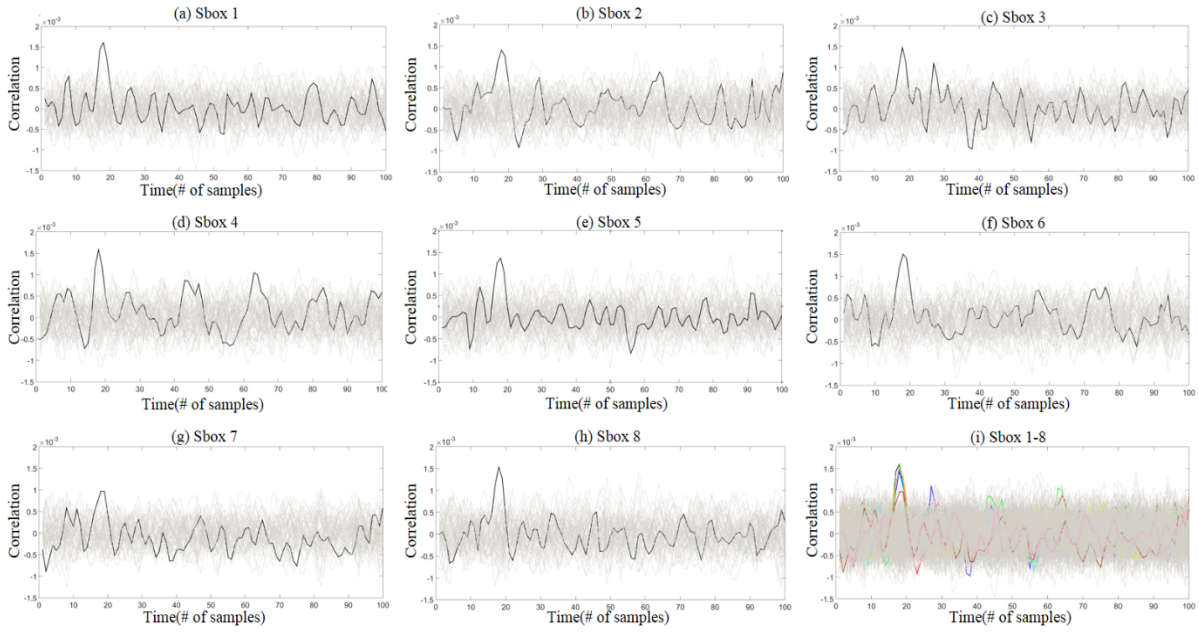

Figure 13. Correlation Coefficients for each Sbox CPA in First Round of First DES

From the upper plot, we are clearly convinced that the attack was successful, because fourteen meaningful peaks were all observed, consecutively for each round. The results are obvious since if a guessed 56-bit DES key is correct, then all intermediate values are accurate, peaks relating to these intermediate values occur at each round.

By contrast, the low plot in Figure 14 shows the correlation coefficient values for incorrect key guess. One meaningless peak was only observed because errors of the incorrectly guessed K_{enc} are influenced to the consecutive rounds due to the round key scheduling, even if the first round key is correct. So, we cannot observe any discriminable peak after 1 Round.

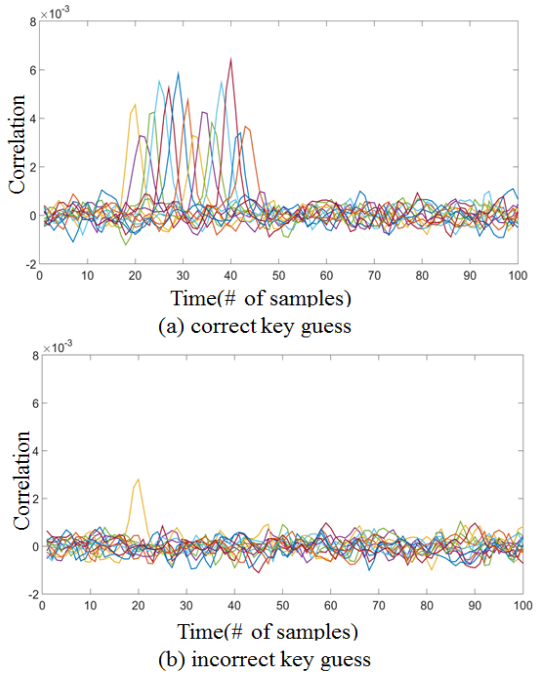

Figure 14. Comparing the result of CPA attacks for retrieve of the full DES key

C. Error Correction based the BS-CPA

After each attack to retrieve 6-bit sub-keys in the first round of the first DES and the second DES, we carried out correction of error for key candidates and obtained the correlation coefficients higher than the noise level at the time samples being executed in target operation. One example describing the error correction task is shown in the Figure 15. There are two peaks soared over given noise level (marked in black on the Y-axis of Figure 15). Also, these two peaks are placed on the meaningful interval. Thus, we performed the error correction for two peaks using the BS-CPA.

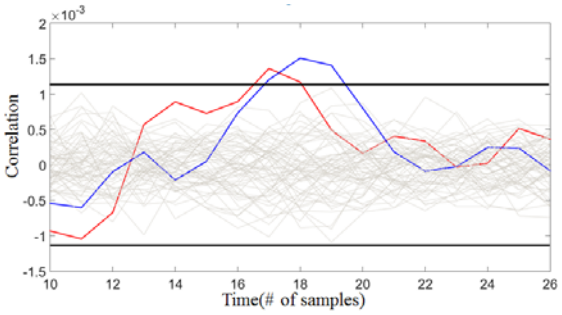

Figure 15. correlation coefficient for the sixth Sbox.

Table 1 shows correlation coefficients of BS-CPA for each key candidate for each Sbox. In Table 1, we can see that the highest peaks (referred to as Ranking 1) for all Sboxs still maintain maximum correlation coefficients after BS-CPA. As the result, we eliminated the second peak (referred to as Ranking 2) in key candidates. We also performed this step on all Sboxs.

	Sbox1	Sbox2	Sbox3	Sbox4	Sbox5	Sbox7	Sbox8
Ranking1	0.0022	0.0020	0.0021	0.0022	0.0020	0.0017	0.0021
Ranking2	0.0019	0.0018	0.0018	0.0019	0.0018	0.0015	0.0019

Table 1. Correlation coefficient value for the BS-CPA

D. Entire Key Verification

The only way to confirm the validity of a recovered T-DES key is to compare the signature value through the card response and the signature value generated with our recovered key. Figure 16 shows a practical result performed in our attack. The left side of Figure 16 is signatures generated by using the public card information and restored card key. The right side of Figure 16 shows the response value to card including 4-byte signature values. We notice that success for recovering the full key is achieved as shown Figure 16 where signatures are identical to the valid ones

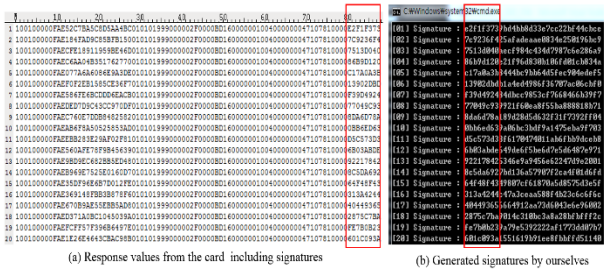

Figure 16. Comparing signatures for verification of restored card key

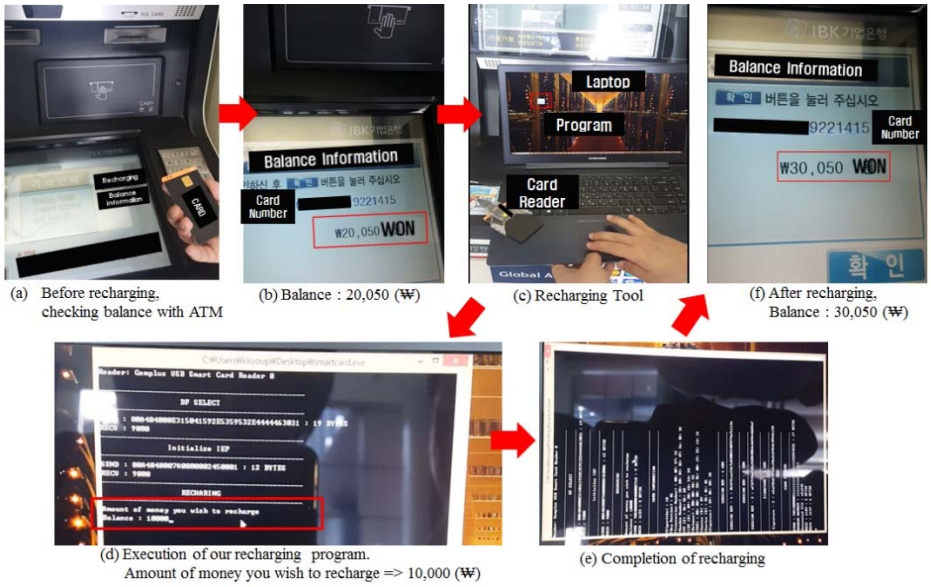

Figure 17. Captured pictures during a recharging simulation

V. Recharging Simulation

As the authentication protocol for recharging presented in Sect. II-2, to recharge balance, it needs to send two commands to the card. The first command is for requirement of recharging to be done without any secret information. After then, the card waits for the response (a valid signature) from the SAM. Here, we note that the attacker can disguise as a legitimate SAM using the restored secret key in the target transit card. Thus, the attacker can generate the valid signature with own generated random number and a session key. Recharging event is finished by sending the generated random number and signature generated by the attacker. We implemented the recharging procedure in the C++ language and executed it on a laptop.

We demonstrated unauthorized recharging in practice with recording a video. Below pictures by capturing the video show alteration of balance within target device. As shown below pictures, we can verify successfully increasing the balance with our simulation.

We notice that the best method to demonstrate validity for recharged balance in target device is to make a payment for an order. However, we did not directly use for payment after illegal recharging, due to worries for turning it into a serious legal issue

VI. Conclusion

Hacking for financial damage can be a serious threat in real-world. In this paper, we showed breaking the commercial transit card widely used in the Korea exploiting the side-channel analysis attack. Our attack was conducted in a black-box manner where everything is unknown for the target device except for public information such as standard documents. As a result of side-channel analysis attack, we could restore a secret information for an authentication, although it was equipped with hiding countermeasure in hardware level. Also by using this secret information, we constructed the hacking system to facilitate illegal recharging of balance in the transit card as much as attacker wants.

It implies that a careless implementation of IC chip in embedded device is so vulnerable. Therefore, designers of secure devices should consider not only hiding countermeasure but also additional techniques such as masking and shuffling equipped in cryptographic algorithm level.

We expect to utilize our works described in this paper for attacking other secure devices in similar environments to ours.

VII. Acknowledgments

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (No. NRF-2014M3C4A7030649)

Reference

1. Kocher, P.C.: Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996).
2. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999).
3. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: concrete results. In: Ko¸c, C¸ .K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 251–261. Springer, Heidelberg (2001).
4. Quisquater, J.-J., Samyde, D.: ElectroMagnetic Analysis (EMA): measures and counter-measures for smart cards. In: Attali, S., Jensen, T. (eds.) E-smart 2001. LNCS, vol. 2140, pp. 200–210. Springer, Heidelberg (2001).
5. Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In: Kaliski Jr., B.S., Ko¸c, C¸ .K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 13–28. Springer, Heidelberg (2002).
6. Schindler, W., Lemke, K., Paar, C.: A stochastic model for differential side channel cryptanalysis. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 30–46. Springer, Heidelberg (2005).
7. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004).
8. Clavier, C., Feix, B., Gagnerot, G., Roussellet, M., Verneuil, V.: Horizontal correlation analysis on exponentiation. In: Soriano, M., Qing, S., L´opez, J. (eds.) ICICS 2010. LNCS, vol. 6476, pp. 46–61. Springer, Heidelberg (2010).
8. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks - Revealing the Secrets of Smart Cards. Springer, New York (2007).
9. Renauld, M., Standaert, F.-X.: Algebraic side-channel attacks. In: Bao, F., Yung, M., Lin, D., Jing, J. (eds.) Inscrypt 2009. LNCS, vol. 6151, pp. 393–410. Springer, Heidelberg (2010).
10. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the Importance of Checking Cryptographic Protocols for Faults. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 37–51. Springer, Heidelberg (1997).
11. Coron, J.-S.: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. In: Ko¸c, C¸ .K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 292–302. Springer, Heidelberg (1999).
12. Clavier, C., Coron, J.-S., Dabbous, N.: Differential Power Analysis in the Presence of Hardware Countermeasures. In: Paar, C., Ko¸c, C¸ .K. (eds.) CHES 2000. LNCS, vol. 1965, pp. 252–263. Springer, Heidelberg (2000).
13. Benoit, O., Tunstall, M.: Efficient Use of Random Delays. Cryptology ePrint Archive, Report 2006/272 (2006)
14. Popp, T., Kirschbaum, M., Zefferer, T., Mangard, S.: Evaluation of the Masked Logic Style MDPL on a Prototype Chip. In: Paillier, Verbauwhede (eds.) CHES 2007, LNCS, vol. 4727, pp. 81–94. Springer, Heidelberg (2007).
15. Tiri, K., Verbauwhede, I.: A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. In: DATE, pp. 246–251. IEEE Computer Society (2004).
16. Chari, S., Jutla, C., Rao, J., Rohatgi, P.: Towards Sound Approaches to Counteract Power-Analysis Attacks. In: Wiener (ed.) CRYPTO 1999, LNCS, vol. 1666, pp. 398–412. Springer, Heidelberg (1999).
17. Goubin, L., Patarin, J.: DES and Differential Power Analysis. In: Ko¸c, C¸ .K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 158–172. Springer, Heidelberg (1999).
18. Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M.T.M.: On the power of power analysis in the real world: a complete break of the KeeLoq code hopping scheme. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 203–220. Springer, Heidelberg (2008).
19. Moradi, A., Kasper, M., Paar, C.: Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures - An Analysis of the Xilinx Virtex-4 and Virtex-5 Bitstream Encryption Mechanism. In: Dunkelman, O. (ed.) CT-RSA 2012. LNCS, vol. 7178, pp. 1–18. Springer, Heidelberg (2012).
20. Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava.: Non-invasive spoofing attacks for anti-lock braking systems. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013, LNCS, vol. 8086, pp. 55-72. Springer, Heidelberg (2013).
21. D., Genkin, I., Pipman, and E., Tromer.: Get your hands on my laptop Physical side-channel key-extraction attacks on pcs. In: Batina, L., Robshaw, M. (eds.) CHES 2014, LNCS, vol.8731, pp. 242-260. Springer, Heidelberg (2014).
22. Oswald, D., Paar, C.: Breaking Mifare DESFire MF3ICD40: power analysis and templates in the real world. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 207–222. Springer, Heidelberg (2011).
23. Kim, T.H., Kim, C., Park, I.: Side channel analysis attacks using AM demodulation on commercial smart cards with SEED. Journal of Systems and Software, vol. 85(12), pp. 2899 – 2908 (2012).
24. ISO/IEC 7816, 1999. International Organization for Standardization: ISO/IEC 7816 Identification cards – integrated circuit(s) with contacts.
25. KS X 6924, 2014, Korean industrial standard: Contactless pre-paid/post pay IC card-User card.
26. Plos, T., Hutter, M., Feldhofer, M.: On comparing side-channel preprocessing techniques for attacking RFID devices. In: Youm, H.Y., Yung, M. (eds.) WISA 2009. LNCS, vol. 5932, pp. 163–177. Springer, Heidelberg (2009).
27. Barenghi, A., Pelosi, G., Teglia, Y.: Improving first order differential power attacks through digital signal processing. In: Makarevich, O.B., El¸ci, A., Orgun, M.A., Huss, S.A., Babenko, L.K., Chefranov, A.G., Varadharajan, V. (eds.) SIN, pp. 124–133. ACM, New York (2010).
28. Kasper, T., Oswald, D., Paar, C.: Side-channel analysis of

cryptographic RFIDs with analog demodulation. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 61–77. Springer, Heidelberg (2012).

29. *Y. Komano, H. Shimizu, and S. Kawamura.: BS-CPA: Built-in determined sub-key correlation power analysis, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, pp.1745–1337, 2010.*
30. *Dehbaoui, A., Lomne, V., Maurine, P., Torres, L., Robert, M.: Enhancing electromagnetic attacks using spectral coherence based cartography. In: Becker, J., Johann, M., Reis, R. (eds.) VLSI-SoC 2009. IFIP AICT, vol. 360, pp. 135–155. Springer, Heidelberg (2011)*
31. *Gebotys, C.H., Ho, S., Tiu, C.C.: EM analysis of rijndael and ECC on a wireless java-based PDA. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 250–264. Springer, Heidelberg (2005).*
32. *Meynard, O., R´eal, D., Flament, F., Guilley, S., Homma, N., Danger, J.: Enhancement of simple electro-magnetic attacks by pre-characterization in frequency domain and demodulation techniques. In: W., Rosenstiel, B.M., Al-Hashimi. (eds.) Design, Automation and Test in Europe Conference & Exhibition, DATE 2011, pp. 1004–1009, IEEE Computer Society (2011).*
33. *van Woudenberg, J.G.J., Witteman, M.F., Bakker, B.: Improving differential power analysis by elastic alignment. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 104–119. Springer, Heidelberg (2011).*
34. *T. H. Le, J. Clediere, C. Servière, and J.-L. Lacoume.: Efficient solution for misalignment of signal in side channel analysis. In: Piscataway, N.J. (ed.): ICASSP 2007, IEEE, vol. 2, pp. 257–260, IEEE Computer Society (2007).*
35. *S. Guilley, K. Khalfallah, V. Lomne, and J. L. Danger.: Formal framework for the evaluation of waveform resynchronization algorithms. In Ardagna, C. (ed.) WISTP 2011, LNCS, vol. 6633 pp. 100–115. Springer, Heidelberg (2011).*
36. *N. Debande, Y. Souissi,M. Nassar, S. Guilley, T. H. Le, and J. L. Danger.: Re-synchronization by moments: An efficient solution to align sidechannel traces. In: A., Rocha, D., Florencio, N., Memon. (eds.) WIFS 2011, IEEE, pp. 1-6, IEEE Computer Society (2011).*