PAPER Special Section on Information and Communication System Security

Detailed Cost Estimation of CNTW Forgery Attack against EMV Signature Scheme

Tetsuya IZU[†], **Yumi SAKEMI**[††], ***and*** **Masahiko TAKENAKA**[†a)], ***Members***

SUMMARY EMV signature is one of specifications for authenticating credit and debit card data, which is based on ISO/IEC 9796-2 signature scheme. At CRYPTO 2009, Coron, Naccache, Tibouchi, and Weinmann proposed a new forgery attack against the signature ISO/IEC 9796-2 (CNTW attack) [2]. They also briefly discussed the possibility when the attack is applied to the EMV signatures. They showed that the forging cost is $45,000 and concluded that the attack could not forge them for operational reason. However their results are derived from not fully analysis under only one condition. The condition they adopt is typical case. For security evaluation, fully analysis and an estimation in worst case are needed. This paper shows cost-estimation of CNTW attack against EMV signature in detail. We constitute an evaluate model and show cost-estimations under all conditions that Coron et al. do not estimate. As results, this paper contribute on two points. One is that our detailed estimation reduced the forgery cost from $45,000 to $35,200 with same condition as [2]. Another is to clarify a fact that EMV signature can be forged with less than $2,000 according to a condition. This fact shows that CNTW attack might be a realistic threat.

key words: *ISO/IEC 9796-2 signature, EMV signature, CNTW forgery attack, cost estimation*

1. Introduction

EMV is an international specification of IC card and IC card capable POS terminals and ATMs, for authenticating credit and debit card transaction. The name of EMV comes from the initial letters of Europay, MasterCard, and VISA, and the first version of EMV specification is decided by these three companies. Now, version 4.2 EMV is effect and is widely adopted by financial facilities around the world [4]. EMV defines the interaction of various level specifications between IC card and IC card processing devices for financial transactions, which are not only physical, electrical, logical specification, but also that of application. EMV specification is constituted based on various standardize specifications. The detailed specification is published by EMVCo [4]. For example, EMV signature that is included in these specifications is a digital signature scheme conform to ISO/IEC 9796-2 Scheme 1.

Since detailed specification is published, various attacks are proposed. Especially, following two attacks against PIN brought the real world a big impact. These attacks show vulnerabilities on illegal use of credit cards. At 2010 IEEE Symposium on Security and Privacy, Murdoch et al. proposed a new bypass attack that bypassed the PIN input of the credit card [8]. At Keynote of CSI Annual Meeting 2010, Jaeger reports a brute force attack against PIN [6].

On the other hand, forgery attack against credit card information is proposed. At the 29th International Cryptology Conference CRYPTO 2009, Coron et al. proposed a new forgery attack against ISO/IEC 9796-2 Scheme 1 (CNTW attack) [2]. This attack creates a forged signature from multitude of correct signatures. In case of ISO/IEC 9796-2 Scheme 1 signature with 2048-bit RSA, a forged signature can be calculated for two days using 19 servers on the Amazon EC2 grid for a total cost of about $800. Since EMV signature scheme is conform to ISO/IEC 9796-2 Scheme 1, CNTW attack can be applied to it. Therefore, Coron et al. also showed the technique of applying their attack against EMV signature scheme. And they showed assumption applying the attack against EMV signature scheme to estimate the cost by using their experimental results of forging signature. In their estimation, a message format of EMV signature scheme was shown. The message is constituted plural fields that is set various information and data to be authenticated. They assumed to be classified these fields into alterable and locked fields for an adversary, which the cost increases according to amount of locked fields increases. They estimated the cost under the assumption. As results, they estimated the cost for forging signature by CNTW attack is $45,000. And, because large amount of correct signature must be used in attacking process, they concluded that forgery of EMV signature is hard in the operational condition.

This paper shows cost estimations in detail under all classifiable conditions of EMV signature scheme, which were not evaluated by Coron et al. Their results are derived from not fully analysis under only one condition. The condition they adopt is typical case. For security evaluation, fully analysis and an estimation in worst case are needed. For example, if an IC card processing device for EMV signature has a vulnerability that it checks the format insufficiently, their assumption is not approved. (From the fact in [8], it is clear that this case is not irrelevant.) Therefore, this paper shows cost estimations by using assumptions of all classifications for security evaluation of EMV signature. Especially, this paper also estimates the cost under the condition that have an advantage for adversary, and it is clearly beneficial for security evaluation of EMV signature scheme. In addition, in order to estimate in detail, this paper contributes a computation method of parameters for CNTW at-

Manuscript received February 1, 2011.
Manuscript revised June 1, 2011.

[†]The authors are with the FUJITSU LABORATORIES Ltd., Kawasaki-shi, 211–8588 Japan.
[††]The author is with the Okayama University, Okayama-shi, 700–8530 Japan.
a) E-mail: takenaka@labs.fujitsu.com

DOI: 10.1587/transinf.E94.D.2111

tack. As the result, we show that forgery attack can be applied to EMV signature scheme with practical cost in case of specific conditions.

This paper is organized as follows: in Sect. 2, we show ISO/IEC 9796-2 Signature and CNTW attack. Section 3 shows EMV signature scheme is shown and CNTW attack is applied to EMV. In Sect. 4, a calculating model is introduced for estimate the cost of the attack. And finally, we show results of cost estimation and discuss the security evaluation of EMV signature scheme.

2. ISO/IEC 9796-2 Signature and Attack

This section shows a specification of ISO/IEC 9796-2 Scheme 1 [5] and a forgery attack against the signature scheme by Coron, Naccache, Tibouchi, and Weinmann (CNTW attack) [2].

2.1 ISO/IEC 9796-2 Scheme 1

ISO/IEC 9796 specifies digital signature schemes giving partial (or total) message recovery. Now, there are ISO/IEC 9796-2 and ISO/IEC 9796-3 in ISO/IEC 9796 standard, which the security based on the difficulty of factorizing large numbers and based on the difficulty of discrete logarithm problem respectively. ISO/IEC 9796-2:2002 specifies three digital signature schemes (Scheme 1, 2, 3), two of which are deterministic (non-randomized) and one of which is randomized [5]. All three schemes can provide either total or partial message recovery. This paper targets only ISO/IEC 9796-2 Scheme 1 and describes it as "ISO/IEC 9796-2 signature". Followings show the specification of ISO/IEC 9796-2 signature.

2.1.1 Scheme1.KeyGen

According to security parameter k, this algorithm chooses a pair of private and public key $(\mathsf{sk}, \mathsf{pk})$, and $\mathsf{sk} = (p, q, d)$, $\mathsf{pk} = (N, e)$. Here, p, q are $k/2$-bit prime numbers, $N = p \cdot q$ is a k-bit composite number, and d, e are integer that $d \cdot e \equiv 1 \pmod{(p-1)\cdot(q-1)}$.

2.1.2 Scheme1.Sign

This algorithm signs a message m and generate a signature σ as follows:

$$\sigma = \mu(m)^d \bmod N$$

Here, padding function $\mu(\cdot)$ is defined to

$$\mu(m) = \mathtt{0x6A} \| m[1] \| H(m) \| \mathtt{0xBC}.$$

$H(\cdot)$ shows hash function with k_H (≥ 160) bits output, $m[1]$ is a most significant $(k - k_H - 16)$-bit value of message m. `0x6A` shows the header that this padding format is specified by ISO/IEC 9796-2 (partial message recovery), and `0xBC` shows the trailer that SHA-1 is used as hash function in this format. Function $\mu(\cdot)$ always generates $(k-1)$-bit data.

2.1.3 Scheme1.Verify

Receiving a signature and a message m, this algorithm verifies the signature. $\overline{\mu(m)} = \sigma^e \bmod N$ is calculated, and format-checked. In format check process, it is checked whether header, trailer, and $m[1]$ of $\overline{\mu(m)}$ are correctly included in m. Then, $\overline{H(m)}$ is extracted from $\overline{\mu(m)}$. If $\overline{H(m)}$ is equal to $H(m)$, this algorithm outputs "valid". In another case, this algorithm outputs "invalid".

Note that $m[1] = m$ when the length of m is less than or equal to $(k - k_H - 16)$-bit. Therefore, ISO/IEC 9796-2 is a total message recovery signature in this case, and a verify algorithm dose not need a message m for verifying.

2.2 CNTW Attack

In the 29th International Cryptology Conference CRYPTO 2009, Coron, Naccache, Tibouchi, and Weinmann proposed a new forgery attack against ISO/IEC 9796-2 Scheme 1 (CNTW attack) and showed experimental results that forged signature can be created by the attack [2]. In this subsection, CNTW attack is introduced.

The main technique of CNTW attack is that forged message m^* is represented by a multiplicative combination of L messages $m_1, m_2, \ldots, m_L$ as follows:

$$\mu(m^*) = \delta^e \mu(m_1)^{e_1} \mu(m_2)^{e_2} \cdots \mu(m_L)^{e_L} \bmod N,$$

and to derive a factor δ and each exponents $e_1, e_2, \ldots, e_L$ $(1 \leq e_1, e_2, \ldots, e_L < e)^\dagger$. In this instance, between forged signature σ^* and correct signatures $\sigma_1, \sigma_2, \cdots, \sigma_L$ according to these messages, following equation is satisfied:

$$\sigma^* = \delta \cdot \sigma_1^{e_1} \sigma_2^{e_2} \cdots \sigma_L^{e_L} \bmod N.$$

Therefore, forged signature σ^* is actually derived when an adversary obtains signatures $\sigma_1, \sigma_2, \ldots, \sigma_L$.

In order to derive the multiplicative combination mentioned above, Desmedt and Odlyzko proposed the method with prime factorization of $\mu(m_i)$ in 1985 [3]. Because this method is based on prime factorization, it can use only less than 200-bit $\mu(m_i)$ in practice. Thus, this method cannot apply to ISO/IEC 9796-2 signature.

In 1999, Coron, Naccache, and Stern improved the method (CNS attack) [1]. They introduced alternative padding function instead of $\mu(\cdot)$,

$$\nu_{a,b}(\cdot) = a \cdot \mu(\cdot) - b \cdot N,$$

and proposed the method based on prime factorization of $\nu_{a,b}(\cdot)$. In their method, when parameters a, b and message m are properly chosen, the padding function $\nu_{a,b}(m)$ outputs at most $(k_H + 16)$-bit value. Therefore, minimum cost for forging signature is 2^{54} in case of $k_H = 128$ (with MD5), and 2^{61} in case of $k_H = 160$ (with SHA-1). As results, they showed that ISO/IEC 9796-2 signature can be

†A derivation of a factor δ is omitted in detail in this paper. The derivation is shown in [2].

forged. However, ISO/IEC 9796-2 signature was not actually forged, and they only showed the possibility. At that time, ISO/IEC 9796-2 signature specified the hash function that has to output at least 128-bit value ($k_H \geq 128$). By their proposal, the specification is changed to $k_H \geq 160$.

In 2009, Coron, Naccache, Tibouchi, and Weinmann proposed the optimization method of CNS attack to show that the padding function $\nu_{a,b}(m)$ can output at most ($k_H + |a|$)-bit value. Here, $|a|$ is a bit-length of parameter a and a few bits value. In addition, they succeeded an experiment of forging signature in actual [2]. Their conditions used in the experiment are follows:

- N is a 2048-bit composite number,
- exponent $e = 2$,
- SHA-1 is used as hash function,
- $|a| = 10$,
- only messages that padding function $\nu_{a,b}(m)$ outputs ($k_H + |a| - 8$)-bit values are used.

Under this condition, they actually showed that a forged signature was calculated for 2 days with Amazon EC2 (Elastic Compute Cloud) service, which cost about $800.

2.3 EMV Specification and EMV Signature

EMV is an international specification of IC card and IC card capable POS terminals and ATMs, for authenticating credit and debit card transaction. EMV signature scheme, one of EMV specifications, is a digital signature scheme conform to ISO/IEC 9796-2 Scheme 1. Therefore, CNTW attack can be applied to EMV signature scheme. EMV signature scheme specifies 7 different formats, depending on the message type. In [2], Coron et al. showed approximative cost-estimation to apply their attack to them, and especially described one of these formats, the Static Data Authentication Issuer Public-key Data (SDA–IPKD). In this paper, we discuss cost-estimation in detail to apply CNTW attack to SDA–IPKD.

2.4 Applying CNTW Attack to SDA–IPKD

SDA–IPKD is one of formats for static data authentication of EMV signature. SDA–IPKD specifies a format of message m as follows:

$$m = \texttt{0x02}||D_1||D_2||D_3||D_4||D_5||D_6||D_7||N_I||\texttt{0x03}.$$

Here, D_1 is Issuer ID (32-bit), D_2 is Certification Expiration Date (16-bit), D_3 is Certificate Serial Number (24-bit), D_4 is Hash Algorithm ID (8-bit), D_5 is Issuer Public Key Algorithm ID (8-bit), D_6 is Issuer Public Key Length (8-bit), D_7 is Issuer Public Key Exponent Length (8-bit), and N_I is Issuer's modulus to be certified.

Using this format, padding function $\mu(\cdot)$ of ISO/IEC 9796-2 signature is represented as follows:

$$\mu(m) = \texttt{0x6A02}||D_1||D_2||\cdots||D_6||D_7||N_I[1]||H(m)||\texttt{0xBC}.$$

Here, $N_I = N_I[1]||N_I[2]$, and bit size of $N_I[1]$ is $|N_I[1]| = (k - k_H - 128)$-bit.

Coron et al. assumed that D_1, D_2 and N_I are alterable value, and $D_3 - D_7$ are locked values for an adversary. Then they cost-estimated the forgery by CNTW attack. As results, they reported that the cost to forge an EMV signature is $45,000 with Amazon EC2. Where, padding function $\nu_{a,b}(\cdot)$ outputs at most 204-bit value if minimum parameters a (this is represented as $\hat{a}$ in following sections) can be properly chosen. Note that, in order to calculate $\hat{a}$, they estimated that 13 years and extra $11,000 with Amazon EC2 was needed besides the cost of CNTW attack.

3. Cost-Estimation for Forging SDA–IPKD in Detail

Coron et al. assumed only a condition of alterable and locked fields for an adversary and approximative cost-estimated of forgery by CNTW attack. The consensus of their assumption, however, is not completely obtained, and it is a possibility that the attack can use another conditions according to issuer of IC cards or IC card processing devices for EMV signature. Therefore, we think that cost-estimations in detail with various conditions are necessary for security evaluation of EMV signature.

As mentioned in Sect. 2.4, it takes 13 years to calculate $\hat{a}$ under their condition. Thus cost to calculate $\hat{a}$ is not negligible. However, they cost-estimated only for CNTW attack without cost of calculating $\hat{a}$.

In this paper, we construct an evaluation model with all conditions that $D_1 - D_7$ fields are alterable or locked, and show the cost-estimation of CNTW attack in detail including cost to calculate parameter a.

3.1 Evaluation Model

In order to apply CNTW attack more efficiently, parameters a, b should be provided for output of $\nu_{a,b}(\cdot) = a \cdot \mu(\cdot) - b \cdot N$ to be as small as possible. Conditions of $D_1 - D_7$ directly concern the decision of these parameters. Therefore, to clearly show the effect of the condition, padding function $\mu_n(\cdot)$ is represented as follows:

$$\mu_n(m) = \texttt{0x6A02}||Y_1||X_1||\cdots||Y_n||X_n||N_I[1]||H(m)||\texttt{0xBC}$$

Here, X_i ($1 \leq i \leq n$) are alterable values for an adversary, and Y_i ($1 \leq i \leq n$) are locked values. n is a number of set of X_i and Y_i. X_n and Y_1 can be 0-bit values. For example, the condition of Coron et al., D_1 and D_2 are alterable values for an adversary and $D_3 - D_7$ are locked value, is represented as $n = 2$, $X_1 = D_1||D_2$, $Y_2 = D_3||D_4||D_5||D_6||D_7$, and Y_1, X_2 are 0-bit values in our model.

Since conditions are defined by 7 values $D_1 - D_7$, there are $2^7 = 128$ conditions. According to these conditions, 4 types ($n = 1, 2, 3, 4$) of padding function $\mu_n(\cdot)$ are constructed. We calculate parameters and cost-estimate for CNTW attack according to these 4 types of $\mu_n(\cdot)$.

3.2 Calculating Parameters for EMV Signature

Cost to calculate parameter a is also considered in our cost-estimation. In this subsection, we describe the cost-estimation to calculate a that constitute a padding function $\nu_{a,b}(\cdot) = b \cdot N - a \cdot \mu_n(\cdot)$ for CNTW attack.

In CNTW attack, output length of a padding function $\nu_{a,b}(m)$ is minimized by choosing proper parameters a, b. For ISO/IEC 9796-2 signature, parameter b and output length are deterministically provided by parameter a. Thus, minimum parameter a that proper output length of $\nu_{a,b}(m)$ (that is $\hat{a}$) can be found by exhaustive search.

On the other hand, in order to obtain proper output length of $\nu_{a,b}(m)$ for EMV signature, proper parameters not only a, b but also X_i those are alterable values for an adversary should be found. Because of increasing a number of variables, it is difficult that proper output length of $\nu_{a,b}(m)$ can be found by exhaustive search.

Finding small values of plural variables so as to minimize the value of polynomial in these variables is a Closest Vector Problem (CVP). Coron et al. introduced the LLL algorithm [7] to solve this problem. The LLL algorithm is a polynomial time of lattice reduction algorithm. CVP can be easily solved using the LLL algorithm[†]. Under their condition, Coron et al. found small b, X_1 and proper $\nu_{a,b}(m)$ regarding specified a. They used the LLL algorithm to solve CVP in a bi-dimensional lattice ($n = 2$). CVP in a multidimensional lattice ($n = 3, 4$) can be easily solved by the LLL algorithm. We also use the LLL algorithm for calculating and cost-estimation of CNTW attack.

3.3 Cost-Estimation of Calculating Parameters with LLL Algorithm

When small b, X_i and proper $\nu_{a,b}(m)$ is found regarding specified k_a-bit a with the LLL algorithm, the length of proper $\nu_{a,b}(m)$ ($|\nu_{a,b}(m)|$) is less than $(k - \sum_{i=1}^{n} k_{X_i})$-bit. Because b, X_i can take k_a-bit, k_{X_i}-bit values respectively. CNTW attack, however, needs a set of parameters a, b, X_i that $|\nu_{a,b}(m)| \leq (k + k_a - 16 - \sum_{i=1}^{n} k_{X_i} - \sum_{i=1}^{n} k_{Y_i})$. That is, most significant $(16 + \sum_{i=1}^{n} k_{X_i} + \sum_{i=1}^{n} k_{Y_i})$-bit of $a \cdot \mu(\cdot)$ want to be canceled by proper a, b and X_i. Here, $|\mu(\cdot)|$ is k-bit, $|a|$ and $|b|$ are both k_a-bit, and $|X_i|$, $|Y_i|$ are k_{X_i}-bit, k_{Y_i}-bit respectively.

Expectation of proper $|\nu_{a,b}(m)|$ is $(16 + \sum_{i=1}^{n} k_{Y_i} - k_a)$-bit larger than that necessary for CNTW attack. Therefore, LLL search is repeated about $2^{16+\sum_{i=1}^{n} k_{Y_i} - k_a}$ times regarding various a. Then a set of parameters a, b, X_i that $|\nu_{a,b}(m)| \leq (k + k_a - 16 - \sum_{i=1}^{n} k_{X_i} - \sum_{i=1}^{n} k_{Y_i})$ is probably found by the heuristic search. And, $|a| = k_a$ satisfies following relation:

$$k_a \geq 16 + \sum_{i=1}^{n} k_{Y_i} - k_a,$$

the minimum k_a is provided

$$k_a = \frac{16 + \sum_{i=1}^{n} k_{Y_i}}{2}.$$

Table 1 Cost of calculating the LLL algorithm by n.

n	Cost [ms]
1	~ 0
2	1.6
3	6.2
4	15.5

If a value to satisfy above condition is found, the most significant Z-bit of $\nu_{a,b}(m)$ can be adjusted to 0,

$$Z = 16 + \sum_{i=1}^{n} k_{X_i} + \sum_{i=1}^{n} k_{Y_i}.$$

Then, bit length of output of $\nu_{a,b}(m)$ is $(k + k_a - Z)$-bit. In addition, an adversary chooses proper $N_I[1]$, and the most significant $(Z + |N_I[1]|)$-bit of $\nu_{a,b}(m)$ can be adjusted to 0. Thus, using these techniques, $|\nu_{a,b}(\cdot)|$ is as follows:

$$|\nu_{a,b}(m)| = k + k_a - (Z + |N_I[1]|) = k_H + k_a + 8 \qquad (1)$$

As mentioned above, in order to provide a proper $\nu_{a,b}(m)$, it is necessary to repeatedly calculate the LLL algorithm with various a. Such a that provides a proper $\nu_{a,b}(m)$ is represented by $\bar{a}$, here. In this paper, we estimate the cost of providing $\bar{a}$ by a number of searching with various a ($= \sharp\bar{a}$) and a cost par calculating the LLL algorithm as follows:

(Cost of providing $\bar{a}$)
$= \sharp\bar{a} \cdot$ (cost par calculating LLL algorithm).

A cost of calculating the LLL algorithm, that is provided $O((\mathrm{n} + 1)^4)$, hardly depend on a number of variables. Table 1 shows the cost of calculating the LLL algorithm by n that is a number of variables X_i. Note that, a number of variables of the LLL algorithm is n because X_i $(1 \leq i \leq n-1)$ and b are the variables of CNTW attack. Note that, since X_n can be handled by concatenating to $N_I[1]$ as $X_n \| N_I[1]$, we assume that X_n is excluded in the variables. And, these costs are derived by experimental measurement with one core of Core 2 Quad 2.66 GHz. In addition, in case of $n = 1$, the cost is estimated as ~ 0 because parameters can be easily provided without the LLL (see Table 1).

On the other hand, $\sharp a$ is provided by search space of a (a number of k_a-bit integer) and existing probability of $\bar{a}$. We assume that the existing probability of $\bar{a}$ is constant, and search space increases in proportion to $(2^{k_a})^2$. Because b increases 1-bit as a increases 1-bit, the search space quadruples. Therefore, expectation of a number of $\bar{a}$ ($E(\bar{a})$) is provided as follows:

$$E(\bar{a}) = 4^{k_a - \frac{16+\sum_{i=1}^{n} k_{Y_i}}{2}}$$

Here, we assume that $E(\bar{a}) = 1$ when $k_a = (16 + \sum_{i=1}^{n} k_{Y_i})/2$. This existing probability was provided by our experiments.

[†]The LLL algorithm does not solve CVP strictly, but approximately solves it. In order to obtain proper output length of $\nu_{a,b}(m)$ for EMV signature, strict solution is not necessary. Therefore, the attack uses the LLL algorithm.

As mentioned above, $\sharp\bar{a}$ with just k_a-bit is provided as follows:

$$\sharp\bar{a} = \frac{2^{k_a-1}}{4^{k_a-\frac{16+\sum_{i=1}^{n} k_{Y_i}}{2}} - 4^{k_a-1-\frac{16+\sum_{i=1}^{n} k_{Y_i}}{2}}} = \frac{2^{16+\sum_{i=1}^{n} k_{Y_i}-k_a+1}}{3} \tag{2}$$

These equation shows that it costs too large to find small $\bar{a}$ — and vice versa. Note that, all a are $\bar{a}$ in case $k_a \geq 16 + \sum_{i=1}^{n} k_{Y_i}$.

4. Results of Estimation and Discussion

In this section, we estimate the cost of CNTW attack against EMV signature. And, our estimation is compared with the results of Coron et al.

4.1 About Experimental Results of Coron et al.

Coron et al. computer experimented to find an $\bar{a}$ with $k_a = 52$ in [2]. They reported that $\sharp\bar{a}$ was 8,303,995 $\simeq 2^{23}$ for 109 minutes with single-core 2 GHz CPU to find an $\bar{a}$. And, they assumed that minimum $\bar{a}$ ($\hat{a}$) has $(16 + \sum_{i=1}^{n} k_{Y_i})/2$-bit, and estimated the cost to find $\hat{a}$ from their results. Under their conditions, $(16 + \sum_{i=1}^{n} k_{Y_i})/2 = 36$, the cost was provided as follows:

$$\begin{aligned} &109 \cdot 2^{16+56-36}/2^{16+56-52} \\ &\quad = 7.1 \cdot 10^6\ [minutes] \simeq 13\ [years] \end{aligned} \tag{3}$$

This is converted into \$11,000 on Amazon EC2[†].

In our estimation, $\sharp\bar{a}$ with $k_a = 52$ is $\simeq 2^{20}$ from Eq. (2). Then, when we tried plural experiments with $k_a = 52$, we had results of $\sharp\bar{a}$ were 2^{19}–2^{20} values. And, Eq. (3) implies that Coron et al. estimated with 2^{20}. This contradicts their report that $\sharp\bar{a} \simeq 2^{23}$ for 109 minutes.

In addition, Coron et al. assumed that $\hat{a}$ is the best in $\bar{a}$. Using $\hat{a}$, the cost of CNTW attack is minimized certainly. They, however, consider the costs of CNTW attack and LLL algorithm independently. The cost of forgery against EMV signature includes both costs, and total cost should be estimated. Therefore, we define the best $\bar{a}$ as not $\hat{a}$ but $\tilde{a}$ that total cost is minimized with it, and estimate these costs.

As just described, their cost-estimation against EMV signature was inaccurate. In this paper, we estimate the cost in detail by using our evaluation model.

4.2 Cost-Estimation of CNTW Attack against EMV Signature

From above discussion, total costs of CNTW attack are estimated against all conditions of SDA–IPKD (with SHA-1). Our result is shown in Table 2. These results are arranged in ascending order of total cost.

Each column in Table 2 means as follows:

- "D_1–D_7" shows conditions of alterable (1) or locked (0) of D_1–D_7 fields.
- "n" is a number of set of X_i and Y_i.
- "$|\hat{a}|$" is bit size of minimum $\bar{a}$ that is provided $(16 + \sum_{i=1}^{n} k_{Y_i})/2$.
- "$|\tilde{a}|$" is bit size of optimal $\bar{a}$ that total cost is minimized with it.
- "$\sharp\tilde{a}$" is a logarithmic number of searching $\tilde{a}$.
- "$|\nu_{a,b}(\cdot)|$" is a bit size of output of padding function $\nu_{a,b}(\cdot)$.
- "LLL cost" is a cost of calculating LLL algorithm on Amazon EC2.
- "CNTW cost" is a cost of CNTW attack on Amazon EC2 that is converted from results of [2].
- "Total cost" is LLL cost + CNTW cost.

Here, $\sharp\tilde{a}$, $|\nu_{a,b}(\cdot)|$, LLL cost, CNTW cost, and total cost are provided corresponding to $\tilde{a}$. And, $|\nu_{a,b}(\cdot)|$ is 8-bit smaller than values provided Eq. (1) because we also introduce a same technique as [2]. This technique only choose values of which the most significant 8-bit is 0.

From Table 2, total cost increases according as a size of locked fields increases. Because size of a increases according as this size, both LLL cost and CNTW cost increase.

Then $\tilde{a}$ is compared with $\hat{a}$ in Table 2. Coron et al. assumed that the best $\bar{a}$ is minimum $\bar{a}$ ($\hat{a}$) because the cost of CNTW attack decreases according as a size of $\bar{a}$ decreases. However, $\tilde{a}$ (optimal $\bar{a}$) does not necessarily coincide as $\hat{a}$. LLL cost is negligible in case a size of locked fields is small. But, according as the size increases LLL cost increases and cannot be negligible. LLL cost can decrease by increasing the size of k_a. Therefore, decreasing LLL cost more improves total cost than minimizing CNTW cost in case of large size of locked fields.

4.3 Impact of CNTW Attack against EMV Signature

In this subsection, we discuss impact of CNTW attack against EMV signature. As mentioned in Sect. 4.1, cost-estimation of Coron et al. against EMV signature was inaccurate. Table 2 shows that LLL cost is \$2,036, CNTW cost is \$33,164, and total cost is \$35,200 under their condition, which is indicated the row $D_1 - D_7 = 1100000$. This estimation is compared with their results, which LLL cost is \$11,000 and CNTW cost is \$45,000. Our estimation is 40% lower than theirs.

From Table 2, EMV signature can be forged with less than \$2,000 according to a condition. This fact shows that CNTW attack is a realistic threat. Coron et al. assumed only a condition $D_1 - D_7 = 1100000$, and concluded that CNTW attack is not a realistic threat. Their estimation, however, was inaccurate, and the consensus of their assumption is not completely obtained. It is a possibility that other conditions are used according to issuer of IC cards or IC card processing devices for EMV signature.

[†]Though this is $4.3 \cdot 10^8$ [*minutes*] in [2], $7.1 \cdot 10^6$ [*minutes*] is correct. And, $7.1 \cdot 10^6$ [*minutes*] = 119057 [*hours*]. According that a cost is \$0.1 par hour par single core CPU on Amazon EC2, it seems that their estimated cost on Amazon EC2 is \$12,000 correctly.

Table 2 Cost of CNTW attack against EMV signature under all conditions.

D_1–D_7	n	$\lvert\hat{a}\rvert$ [bit]	$\lvert\tilde{a}\rvert$ [bit]	$\sharp\tilde{a}$ [log 2]	$\lvert\nu_{a,b}(\cdot)\rvert$ [bit]	LLL cost [$]	CNTW cost [$]	Total cost [$]
1111111	1	8	8	7.5	168	0	1,219	1,219
1110111	2	12	12	11.5	172	0	1,987	1,987
1111011	2	12	12	11.5	172	0	1,987	1,987
1111101	2	12	12	11.5	172	0	1,987	1,987
1111110	2	12	12	11.5	172	0	1,987	1,987
1011111	2	16	16	15.5	177	0	3,221	3,221
1110011	2	16	16	15.5	177	0	3,221	3,221
1111001	2	16	16	15.5	177	0	3,221	3,221
1111100	2	16	16	15.5	177	0	3,221	3,221
1110101	3	16	16	15.5	177	0	3,221	3,221
1110110	3	16	16	15.5	177	0	3,221	3,221
1111010	3	16	16	15.5	177	0	3,221	3,221
1101111	2	20	20	19.5	180	0	5,159	5,159
1110001	2	20	20	19.5	180	0	5,159	5,159
1111000	2	20	20	19.5	180	0	5,159	5,159
1010111	3	20	20	19.5	180	0	5,159	5,159
1011011	3	20	20	19.5	180	0	5,159	5,159
1011101	3	20	20	19.5	180	0	5,159	5,159
1011110	3	20	20	19.5	180	0	5,159	5,159
1110010	3	20	20	19.5	180	0	5,159	5,159
1110100	3	20	20	19.5	180	0	5,159	5,159
0111111	1	24	24	23.5	184	0	8,293	8,293
1100111	2	24	24	23.5	184	0	8,293	8,294
1110000	2	24	24	23.5	184	0	8,293	8,294
1010011	3	24	24	23.5	184	2	8,293	8,295
1011001	3	24	24	23.5	184	2	8,293	8,295
1011100	3	24	24	23.5	184	2	8,293	8,295
1101011	3	24	24	23.5	184	2	8,293	8,295
1101101	3	24	24	23.5	184	2	8,293	8,295
1101110	3	24	24	23.5	184	2	8,293	8,295
1010101	4	24	24	23.5	184	5	8,293	8,298
1010110	4	24	24	23.5	184	5	8,293	8,298
1011010	4	24	24	23.5	184	5	8,293	8,298
0110111	2	28	28	27.5	188	8	13,224	13,232
0111011	2	28	28	27.5	188	8	13,224	13,232
0111101	2	28	28	27.5	188	8	13,224	13,232
0111110	2	28	28	27.5	188	8	13,224	13,232
1001111	2	28	28	27.5	188	8	13,224	13,232
1100011	2	28	28	27.5	188	8	13,224	13,232
1010001	3	28	28	27.5	188	31	13,224	13,255
1011000	3	28	28	27.5	188	31	13,224	13,255
1100101	3	28	28	27.5	188	31	13,224	13,255
1100110	3	28	28	27.5	188	31	13,224	13,255
1101001	3	28	28	27.5	188	31	13,224	13,255
1101100	3	28	28	27.5	188	31	13,224	13,255
1010010	4	28	28	27.5	188	77	13,224	13,301
1010100	4	28	28	27.5	188	77	13,224	13,301
1101010	4	28	28	27.5	188	77	13,224	13,301
0011111	1	32	32	31.5	192	0	20,906	20,907
0110011	2	32	32	31.5	192	127	20,906	21,034
0111001	2	32	32	31.5	192	127	20,906	21,034
0111100	2	32	32	31.5	192	127	20,906	21,034
1000111	2	32	32	31.5	192	127	20,906	21,034
1100001	2	32	32	31.5	192	127	20,906	21,034
0110101	3	32	32	31.5	192	493	20,906	21,400
0110110	3	32	32	31.5	192	493	20,906	21,400
0111010	3	32	32	31.5	192	493	20,906	21,400
1001011	3	32	32	31.5	192	493	20,906	21,400
1001101	3	32	32	31.5	192	493	20,906	21,400
1001110	3	32	32	31.5	192	493	20,906	21,400
1010000	3	32	32	31.5	192	493	20,906	21,400
1100010	3	32	32	31.5	192	493	20,906	21,400
1100100	3	32	32	31.5	192	493	20,906	21,400

D_1–D_7	n	$\lvert\hat{a}\rvert$ [bit]	$\lvert\tilde{a}\rvert$ [bit]	$\sharp\tilde{a}$ [log 2]	$\lvert\nu_{a,b}(\cdot)\rvert$ [bit]	LLL cost [$]	CNTW cost [$]	Total cost [$]
1101000	3	32	32	31.5	192	493	20,906	21,400
0010111	2	36	36	35.5	196	2,036	33,164	35,200
0011011	2	36	36	35.5	196	2,036	33,164	35,200
0011101	2	36	36	35.5	196	2,036	33,164	35,200
0011110	2	36	36	35.5	196	2,036	33,164	35,200
0101111	2	36	36	35.5	196	2,036	33,164	35,200
0110001	2	36	36	35.5	196	2,036	33,164	35,200
0111000	2	36	36	35.5	196	2,036	33,164	35,200
1000011	2	36	36	35.5	196	2,036	33,164	35,200
1100000	**2**	**36**	**36**	**35.5**	**196**	**2,036**	**33,164**	**35,200**
0110010	3	36	36	35.5	196	7,890	33,164	41,054
0110100	3	36	36	35.5	196	7,890	33,164	41,054
1000101	3	36	36	35.5	196	7,890	33,164	41,054
1000110	3	36	36	35.5	196	7,890	33,164	41,054
1001001	3	36	36	35.5	196	7,890	33,164	41,054
1001100	3	36	36	35.5	196	7,890	33,164	41,054
1001010	4	36	38	33.5	197	4,931	41,773	46,704
0010011	2	40	42	37.5	201	8,145	65,128	73,273
0011001	2	40	42	37.5	201	8,145	65,128	73,273
0011100	2	40	42	37.5	201	8,145	65,128	73,273
0100111	2	40	42	37.5	201	8,145	65,128	73,273
0110000	2	40	42	37.5	201	8,145	65,128	73,273
1000001	2	40	42	37.5	201	8,145	65,128	73,273
0001111	1	44	44	43.5	204	1,629	81,418	83,046
0010101	3	40	43	36.5	203	15,780	72,812	88,592
0010110	3	40	43	36.5	203	15,780	72,812	88,592
0011010	3	40	43	36.5	203	15,780	72,812	88,592
0101011	3	40	43	36.5	203	15,780	72,812	88,592
0101101	3	40	43	36.5	203	15,780	72,812	88,592
0101110	3	40	43	36.5	203	15,780	72,812	88,592
1000010	3	40	43	36.5	203	15,780	72,812	88,592
1000100	3	40	43	36.5	203	15,780	72,812	88,592
1001000	3	40	43	36.5	203	15,780	72,812	88,592
0000111	1	48	48	47.5	208	26,062	127,534	153,596
0010001	2	44	49	38.5	208	16,289	142,745	159,034
0011000	2	44	49	38.5	208	16,289	142,745	159,034
0100011	2	44	49	38.5	208	16,289	142,745	159,034
1000000	2	44	49	38.5	208	16,289	142,745	159,034
0010010	3	44	50	37.5	210	31,560	159,655	191,215
0010100	3	44	50	37.5	210	31,560	159,655	191,215
0100101	3	44	50	37.5	210	31,560	159,655	191,215
0100110	3	44	50	37.5	210	31,560	159,655	191,215
0101001	3	44	50	37.5	210	31,560	159,655	191,215
0101100	3	44	50	37.5	210	31,560	159,655	191,215
0101010	4	44	51	36.5	211	39,450	177,837	217,287
0000011	1	52	55	48.5	215	52,125	274,261	326,386
0001011	2	48	56	39.5	215	32,578	305,769	338,347
0001101	2	48	56	39.5	215	32,578	305,769	338,347
0001110	2	48	56	39.5	215	32,578	305,769	338,347
0010000	2	48	56	39.5	215	32,578	305,769	338,347
0100001	2	48	56	39.5	215	32,578	305,769	338,347
0100010	3	48	57	38.5	217	63,120	340,958	404,078
0100100	3	48	57	38.5	217	63,120	340,958	404,078
0101000	3	48	57	38.5	217	63,120	340,958	404,078
0000001	1	56	62	49.5	222	104,250	589,355	693,605
0000101	2	52	62	41.5	222	130,312	589,355	719,668
0000110	2	52	62	41.5	222	130,312	589,355	719,668
0001001	2	52	62	41.5	222	130,312	589,355	719,668
0001100	2	52	62	41.5	222	130,312	589,355	719,668
0100000	2	52	62	41.5	222	130,312	589,355	719,668
0001010	3	52	64	39.5	224	126,240	727,862	854,103
0000000	1	60	69	50.5	229	208,500	1,235,081	1,443,581
0000010	2	56	69	42.5	229	260,625	1,235,081	1,495,706
0000100	2	56	69	42.5	229	260,625	1,235,081	1,495,706
0001000	2	56	69	42.5	229	260,625	1,235,081	1,495,706

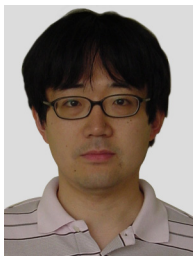
CNTW attack against EMV signature has been currently potential threat, and this attack is hard to apply in the operational condition as they say. This attack, however, has the possibility of becoming real threat in case that there are any other vulnerability, for example, credit cards are used with vulnerable IC card processing device that check the format insufficiently. The credit card systems requires the multiple-defence as fail safe, and this vulnerability should be corrected. A cause of such a problem depends on using traditional signature scheme such as ISO/IEC 9796-2 Scheme 1. Therefore, IC card of EMV specification should adopt provable secure signature methods such as ISO/IEC 9796-2 Scheme 2.

5. Concluding Remarks

This paper has shown cost-estimation of CNTW attack against EMV signature in detail. An evaluate model has been constitute and total cost included LLL cost has been estimated. In addition, we have shown cost-estimations under all conditions that Coron et al. do not estimate. As results, this paper has contributed on two points. One is that our detailed estimation reduced the forgery cost from $45,000 to $35,200 with same condition as [2]. Another is to clarify a fact that EMV signature can be forged with less than $2,000 according to a condition. This fact shows that CNTW attack might be a realistic threat. A cause of such a problem depends on using traditional signature scheme such as ISO/IEC 9796-2 Scheme 1. Therefore, IC card of EMV specification should adopt provable secure signature methods such as ISO/IEC 9796-2 Scheme 2.

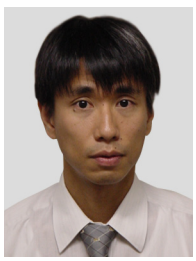
References

[1] J. Coron, D. Naccache, and J. Stern, "On the Security of RSA Padding," Proc. CRYPTO 1999, LNCS 1666, pp.1–18, Springer-Verlag, 1999.
[2] J. Coron, D. Naccache, M. Tibouchi, and R.-P. Weinmann, "Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures," Proc. CRYPTO 2009, LNCS 5677, pp.428–444, Springer-Verlag, 2009.
[3] Y. Desmedt and A. Odlyzko, "A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes," Proc. CRYPTO 1985, LNCS 218, pp.516–522, Springer-Verlag, 1986.
[4] Emv, Integrated circuit card specifications for payment systems, Book 2. Security and Key Management. Version 4.2. June 2008. www.emvco.com.
[5] International Organization for Standardization (ISO), "Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms," 2002.
[6] Keynote of Computer Security Institute 2010, available at http://www.csiannual.com/conference/keynotes.php
[7] A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász, "Factoring polynomials with rational coefficients," Mathematische Annalen, vol.261, pp.513–534, 1982.
[8] J. Murdoch, S. Drimer, R. Anderson, and M. Bond, Chip and PIN is Broken, 2010 IEEE Symposium on Security and Privacy, IEEE S&P, pp.433–446, IEEE Computer Society, 2010 available at http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf



Tetsuya Izu received his B.S. and M.S. degrees in mathematics from the University of Tokyo in 1992, and from Rikkyo University in 1994 respectively. He received his Ph.D. in engineering from the University of Electro-Communications in 2007. He has been engaged in research on cryptography and information security at FUJITSU LABORATORIES Ltd. since 1997. He was a visiting researcher at the University of Waterloo, Canada, in 2001. He received the Paper Prizes of the Symposium on Cryptography and Information Security (SCIS) in 1999 and the Computer Security Symposium (CSS) in 2002. He was awarded the Young Scientists' Prize by the Minister of Education, Culture, Sports, Science and Technology Research on side channel attacks and countermeasures in information security in 2007. He is a member of IACR, IPSJ and JSIAM.

Yumi Sakemi received her B.E. degrees in Communication Network Engineering in 2008, and her M.E. degrees in Electronic and Information Systems Engineering in 2009 from Okayama University. She received her Ph.D. in engineering from Okayama University in 2011. She has been engaged in research on cryptography and information security at FUJITSU LABORATORIES Ltd. since 2011. She was awarded Computer Security Symposium (CSS) Student Paper Prize in 2009.



Masahiko Takenaka received his B.E. and M.E. degrees in electronic engineering in 1990, 1992 respectively from Osaka University. He received his Ph.D. in engineering in 2009 from Tsukuba University. Since 1992, he has been engaged in research and development on cryptography, side channel analysis and network security at FUJITSU LABORATORIES Ltd. He is currently a research manager. He was awarded Computer Security Symposium (CSS) Paper Prize in 2002, and the OHM Technology Award in 2005.