南　華　大　學

資訊管理學系

碩士論文

一個基於單向雜湊函數的電子旅行者支票方法之密碼分析與改進

Cryptanalysis and Improvement of New Electronic Traveler's Check Scheme based on One-way Hash Function

研　究　生：陳 憲 卿

指 導 教 授：周 志 賢

中華民國　100　年　6　月　2　日

南　華　大　學

資訊管理學系(所)

碩 士 學 位 論 文

一個基於單向雜湊函數的電子旅行者支票方法之密碼分析與改進

Cryptanalysis and Improvement of New Electronic Traveler's Check Scheme based on One-way Hash Function

研究生：陳憲卿

經 考 試 合 格 特 此 證 明

口試委員：

許乙秉

周志賢

[illegible]

指導教授：周志賢

系主任(所長)：資訊管理學系呂光閔 系主任呂光閔

口試日期：中華民國 100 年 6 月 2 日

南華大學資訊管理學系碩士論文著作財產權同意書

立書人：陳憲卿 之碩士畢業論文

中文題目：一個基於單向雜湊函數的電子旅行者支票方法之密碼分析與改進

英文題目：Cryptanalysis and Improvement of New Electronic Traveler's Check Scheme based on One-way Hash Function

指導教授：周志賢 博士

學生與指導老師就本篇論文內容及資料其著作財產權歸屬如下：

☑ 共同享有著作權

☐ 共同享有著作權，學生願「拋棄」著作財產權

☐ 學生獨自享有著作財產權

學　　生：陳憲卿（請親自簽名）

指導老師：周志賢（請親自簽名）

中　華　民　國　100 年 6 月 2 月

南華大學碩士班研究生

論文指導教授推薦函

資訊管理 系碩士班 陳憲卿 君所提

之論文 Cryptanalysis and Improvement of New Electronic Traveler's Check Scheme based on One-way Hash Function

係由本人指導撰述，同意提付審查。

指導教授 周志賢

100 年 6 月 2 日

誌 謝

欲聞撲鼻香，須經寒徹骨，在老師循循善誘之下，本論文得以順利完成。我要特別感謝指導教授周志賢老師在這段期間的教導和啟發，從一知半解而能一窺密碼學殿堂之奧，獲得珍貴的資訊安全專門知識，給我無比的信心與向前的動力，讓我能在這個領域更進一步的開花結果。

在論文口試過程中，由衷感謝口試委員尤國任老師和許乙清老師不吝指教，使得本論文更加嚴謹且充實。在二年的學習中，感謝純慧、雅玲學姊及易敬學長的提攜，我的同事也是學長的宗德、一峰老師和俊傑主任叮嚀，還有一起研究的同窗其鋒、仲凱和全班同學的合作，感謝你們給我寶貴的意見，因為你們使我獲得這份期盼已久的榮耀；另外，感謝南華大學及師長，有你們的協助付出，才能讓我順利完成學業。

最後，還是向我的家人感謝他們的支持。

陳 憲 卿 謹 誌 于

南 華 大 學 資 管 所

中華民國　100　年　6　月　2　日

一個基於單向雜湊函數的電子旅行者支票方法之密碼分析與改進

學生：陳憲卿　　指導教授：周志賢博士

南　華　大　學　資訊管理學系碩士班

摘　　要

因為電子商務快速的發展近幾年，電子付款方法的研究已進行數年，但是在電子旅行者支票的研究是很少見到的。最近，劉等提出一個基於單向雜湊函數的電子旅行支票安全系統，他們宣稱這個方案是安全的。然而，在這篇文章，我們發現他們的方法容易遭受金鑰洩漏模仿攻擊和平行攻擊。我們使用公鑰去避免即使私鑰被攻擊者知道也不能假冒銀行與消費者通訊，更進一步的，讓我們提出的改善方法更堅固進而被應用在電子網際網路。

關鍵詞：電子付款, 電子支票, 單向雜湊函數, 上線, 離線, 長期安全金鑰

Cryptanalysis and Improvement of New Electronic Traveler's Check Scheme based on One-way Hash Function

Student：Hsien-Ching Chen　　Advisors：Dr. Jue-Sam Chou.

Department of Information Management
The Graduated Program
Nan-Hua University

ABSTRACT

Because of the rapid development of electronic commerce, electronic payment schemes have been intensively studied for several years. But there still lack large number of researchers devoted in electronic traveler's check system. Recently, Liaw *et al.* proposed a hash-based electronic traveler's check system. They claimed that their scheme was secure. However, in this study we will indicate that their scheme is vulnerable to the key compromise impersonation and parallel session attacks. Further, we will improve their scheme to prevent such attacks. Our improvement uses the customer's public key to avoid the deficiency such that even if an attacker knows the private key of a customer, he/she cannot masquerade as the bank to communicate with the customer. This makes our improvement a more robust electronic traveler's check scheme for adoption as a reliable method on the Internet.

Keywords: Electronic payment, electronic check, one-way hash function, on-line, off-line, KCI attack, long-term secure key

目　錄

圖　　目　　錄

Chapter 1 Introduction

Due to the rapid development of electronic commerce, electronic payment schemes are studied intensively recently. In such schemes, the payer/payee can use bank payment instrument (credit card, debit card, or even current account) without revealing any confidential data during the payment [14, 15, 16]. Generally, an electronic payment system [10, 11, 12] can be divided into three types: on-line credit card payment, electronic cash (e-cash), and electronic check (e-check) which are three extensions of credit card, cash, and check in the real life correspondingly. In fact, cash and check are two frequently used tools and a traveler's check can be used as cash in the real world. Hence, a traveler's check should have the same characteristics as both cash and check do. Similarly, an electronic traveler's check [1, 7] must also include both the characteristics of electronic cash [18] and electronic check [6, 9, 11, 16] in the Internet. If an electronic traveler's check owner loses his check, the designed scheme should be responsible for the possible loss. Many such studies [1, 4, 6, 7, 9, 11, 12, 14] had been proposed. They all have the needed security requirements of an electronic traveler's check system. For example, each entity in the payment system trusts only his bank and the transactions always go under a trusted node. The other needed security requirements of an electronic traveler's check are listed as follows [1].

(1) No forgery：The electronic traveler's check should prevent malicious users or merchants from forging it and ensure the fairness for users, merchants, and the bank in the transaction environment.

(2) No double spending：If an electronic check has been used twice, the bank is able to find out who the malicious user or merchant is during the payment phase and

deposit phase.

(3) Specific user：An electronic traveler's check must be signed by both the bank and the user. It should include the identification information regarding both the bank and the user and only the specific owner of the electronic traveler's check should be able to use it.

(4) Reissuing：When an electronic traveler's check is lost, the user should use his serial number and his payer's endorsement to report the loss. Then, the bank can easily reissue a new one for the user.

(5) Anonymity：The owner of the electronic traveler's check should be anonymous; that is, the merchant must not know the real identity of the user throughout the whole transaction process.

In 2001, Hsien et al. [7] proposed an electronic traveler's check system based on discrete logarithm problem [5, 13]. Subsequently, some other studies in this aspect [1, 4, 6] that use exponential operations and one-way hash functions are proposed. In 2007, Liaw et al. proposed a new electronic traveler's check scheme based on one-way hash function [1]. They claimed that their scheme is secure against forgery attack since when given a hash value, it is computationally infeasible for an attacker to find an input having the same hash value under a secure one-way hash function. However, we found that their method can not resist the KCI [2, 3, 8] and parallel session attack. KCI attack defined by Wilson and Menezes [2] means that if a user A's long-term secret key is compromised by an adversary, the adversary can pretend other entities to communicate with A. In parallel session attack [17], two or more runs of protocol are executed concurrently under attacker's orchestration. The concurrent runs make the answer to a difficult question in one run available to the attacker so that he can use the answer in another run. In Liaw et al.'s scheme, if a

customer's long-term secret key has been leaked, the attacker can impersonate other entity to communicate with him. We think this is caused by the improper design in the registration phase. In this paper, we will improve their scheme to prevent this kind of attack.

The rest of this paper is organized as follows. In Section 2, we review Liaw et al.'s protocol [1]. In Section 3,we show the attack on their scheme and then show our improvement in Sections 4. Finally, a conclusion is given in Section 5.

Chapter 2 Review of Liaw et al.'s scheme

Liaw et al.'s electronic traveler's check contains four roles: the consumer, the bank, the merchant, and the clearing-house. It uses X →Y:Z to denote that a sender X sends a message Z to a receiver Y, and includes two subprotocols: an on-line subprotocol and an off-line subprotocol. In their scheme, the customer only needs one-time registration to purchase an electronic traveler's check and would get an anonymous identity. Further, an optional equipment, like the Smart Card, can be applied in the scheme. In the following, we review their scheme, on-line and off-line subprotocols in Section 2.1 and 2.2 which are also shown in figure 1 and 2, respectively. (The more details can be referred to [1]).

2.1 The on-line subprotocol

The on-line scheme requires the bank and the clearing-house to be involved in the payment phase. The clearing-house verifies the identity of the user and checks whether double spending occurs. We describe the on-line scheme as follows and also is show it in Figure 1.

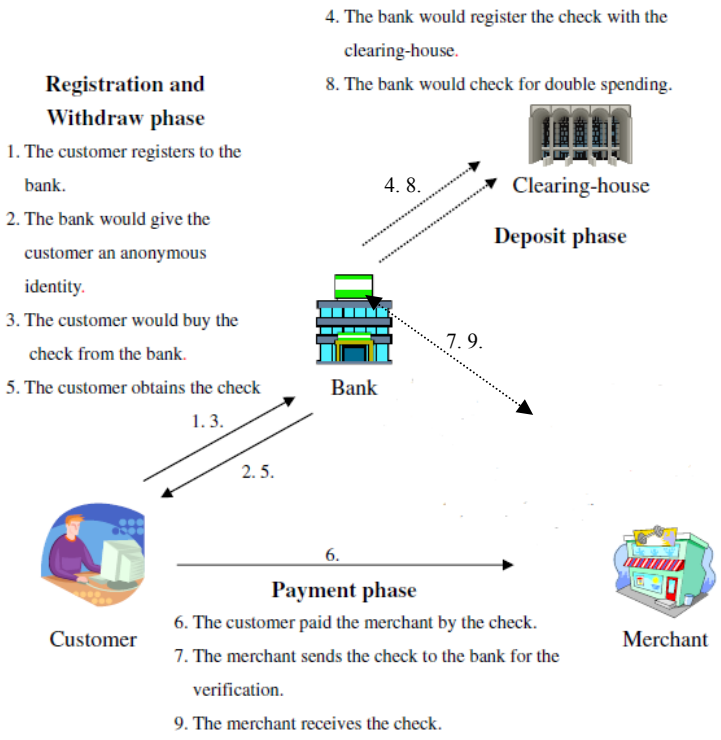

Figure 1: The steps of the on-line subprotocol (source: [1])

(a) The registration phase

In this phase, the customer would submit his real identity to the bank for registration and obtain the right to buy an electronic traveler's check. He only needs one-time registration and can buy many electronic traveler's checks at anytime without registering again. The registration phase includes following three steps:

Step 1. The customer chooses a random number K_{A1} to perform the exclusive OR operation together with his real identity ID_A. Then, he computes the partial anonymous identity $R\_ID_A = h(ID_A \oplus K_{A1})$ by using a one-way hash function h, encrypts R_ID_A by the bank's public key Y_B and then sends the result $PE_{Y_B}(R\_ID_A)$ to the bank.

Step 2. The bank decrypts the received information obtaining R_ID_A. It then chooses a random number K_{B1} and computs $B\_ID_A = h(R\_ID_A \oplus K_{B1})$. After that, it

encrypts B_ID_A by using the customer's public key Y_A and sends the result $PE_{Y_A}(B\_ID_A)$ to him.

Step 3. The customer decrypts the received information by using his private key X_A to get the anonymous identity B_ID_A.

(b) The withdraw phase

In this phase, the customer takes the anonymous identity formed in the registration phase to buy an electronic traveler's check from the bank. The withdrawal phase includes following five steps:

Step 1. The customer chooses a random number K_{A2} and computes a payer's endorsement $R_A = h(B\_ID_A \oplus K_{A2})$. He then encrypts R_A by using his anonymous identity B_ID_A and sends the result $E_{B\_ID_A}(R_A)$ to the bank.

Step 2. The bank decrypts the received information by computing $D_{B\_ID_A}(E_{B\_ID_A}(R_A))$. Then, it chooses another random number K_{B2} and use private key X_B to compute its identity $R_B = h(X_B \oplus K_{B2})$. The bank then generates the payee's endorsement R by computing $R = R_A \oplus R_B$, and encrypted R, R_B, and timestamp T_1 by using symmetric key B_ID_A. After this, it sends the result $E_{B\_ID_A}(R, R_B, T_1)$ to the customer.

Step 3. The customer decrypts the received information $E_{B\_ID_A}(R, R_B, T_1)$ obtaining R, R_B, T_1. He checks to see whether the timestamp T_1 is valid or not. If is valid, he then computes $R' = R_A \oplus R_B$ to verify whether it is equal to the payee's endorsement R. If they are equal, the customer computes the payment requirement $C_A = h(R \oplus M_i \oplus Q_{M_i})$ where M_i is the face value of the electronic

traveler's check, and Q_{M_i} is the amount of the electronic traveler's check.. Then, M_i, Q_{M_i}, C_A and a timestamp T_2 would be encrypted by the customer using symmetric key R_A, and the result $E_{R_A}(M_i, Q_{M_i}, C_A, T_2)$ would be sent to the bank.

Step 4. The bank decrypts the equation $E_{R_A}(M_i, Q_{M_i}, C_A, T_2)$ to obtain M_i, Q_{M_i}, C_A, T_2. It checks whether timestamp T_2 is within a reasonable range. If it is, the bank computes $C'_A = h(M_i \oplus Q_{M_i} \oplus R_A \oplus R_B)$ $(= h(R \oplus M_i \oplus Q_{M_i}))$ to verify whether C'_A is equal to C_A. If so, the bank computes $TC_{M_i} = h(R \oplus M_i \| S_{Q_{M_i}})$ where $S_{Q_{M_i}2}$ is a serial number, $\|$ denotes a concatenation operation, and TC_{M_i} is an electronic traveler's check. After that, the bank computes and sends $E_{R_A}(TC_{M_i}, S_{Q_{M_i}})$ to the customer. Then, the bank sends TC_{M_i} to the clearing-house for recording and safekeeping and stores it in the smart card which was issued to the customer by the bank. If this is the second time the customer buys an electronic traveler's check, he does not need to register again and can begin with a new withdrawal phase.

Step 5. The customer decrypts $E_{R_A}(TC_{M_i}, S_{Q_{M_i}})$ to obtain TC_{M_i} and $S_{Q_{M_i}}$. He then computes $TC'_{M_i} = h(R_A \oplus R_B \oplus M_i \| S_{Q_{M_i}})$ $(= h(R \oplus M_i \| S_{Q_{M_i}}))$, and compares the newly decrypted TC'_{M_i} with TC'_{M_i} to verify whether the electronic traveler's check is legitimate. If the verification succeeds, the customer would store TC_{M_i} and the serial number $S_{Q_{M_i}}$ in his smart card.

If the electronic traveler's check is lost, the customer should send $(TC_{M_i}, S_{Q_{M_i}})$ to report the loss. The bank can then reissue a new electronic traveler's check $TC_{M_i} = h(R_A \oplus R_B \oplus M_i \| S_{Q_{M_i}})$ to the customer.

(c) The payment phase

In this phase, a customer buys goods from a merchant with an electronic traveler's. This payment phase includes following four steps:

Step 1. When the customer buy goods, he should encrypt the information $TC_{M_i}, M_i, S_{Q_{M_i}}, T_3$ by using his anonymous identity B_ID_A as a symmetric key to generate the check message $E_{B\_ID_A}(TC_{M_i}, M_i, S_{Q_{M_i}}, T_3)$ send it to the merchant.

Step 2. After receiving $E_{B\_ID_A}(TC_{M_i}, M_i, S_{Q_{M_i}}, T_3)$, the merchant should forward it to the bank.

Step 3. The bank decrypts the check message to obtain TC_{M_i}, the face value M_i, $S_{Q_{M_i}}$ and timestamp T_3. Then, it checks whether timestamp T_3 is within a reasonable range and verifies whether $TC_{M_i} = h(R \oplus M_i \| S_{Q_{M_i}})$ holds or not. If both hold, The bank sends TC_{M_i} to the clearing-house via a secure channel and verifies whether it is a double spending by using the serial number $S_{Q_{M_i}}$. If it is a double spending, the bank can find out the real identity of the customer by the value B_ID_A. If all the verifications of $TC_{M_i}, M_i, S_{Q_{M_i}}, T_3$, and the identity are successful, the bank deposits it and then computes $C_{M_i} = h(TC_{M_i} \oplus R_B)$. It then computes and sends $E_{R_B}(C_{M_i}, TC_{M_i})$ to the merchant.

Step 4. After the merchant has received the electronic traveler's check by the secret message from the bank, the transaction has been finished.

(d) The deposit phase

In this phase, the merchant sends the received electronic traveler's check to the bank, the bank will verify whether this check contains its own signature. If so, the bank will deposit the amount of money on the electronic traveler's check into the merchant's account. The deposit phase includes following two steps:

Step 1. The merchant sends $E_{R_B}(C_{M_i}, TC_{M_i})$ and a timestamp T_4 to the bank.

Step 2. The bank decrypts $E_{R_B}(C_{M_i}, TC_{M_i})$ to obtain C_{M_i} and TC_{M_i}, and checks whether timestamp T_4 is within a reasonable range. If so, the bank verifies whether $C_{M_i} = TC_{M_i} \oplus R_B$ holds. If it holds, TC_{M_i} would be sent to the clearing-house via a secure channel to verify its validity. If it is valid, the bank deposits the amount on the electronic traveler's check into the customer's account.

2.2 The off-line subprotocol

The difference between the on-line and off-line scheme is that the bank and the clearing-house are not involved in the off-line scheme. This off-line scheme also contains four phases. We describe the off-line subprotocol as follows and also show it in Figure 2.

(a) The registration phase

This phase is the same as the on-line registration phase.

(b) The withdraw phase

This phase is the same as the on-line withdraw phase.

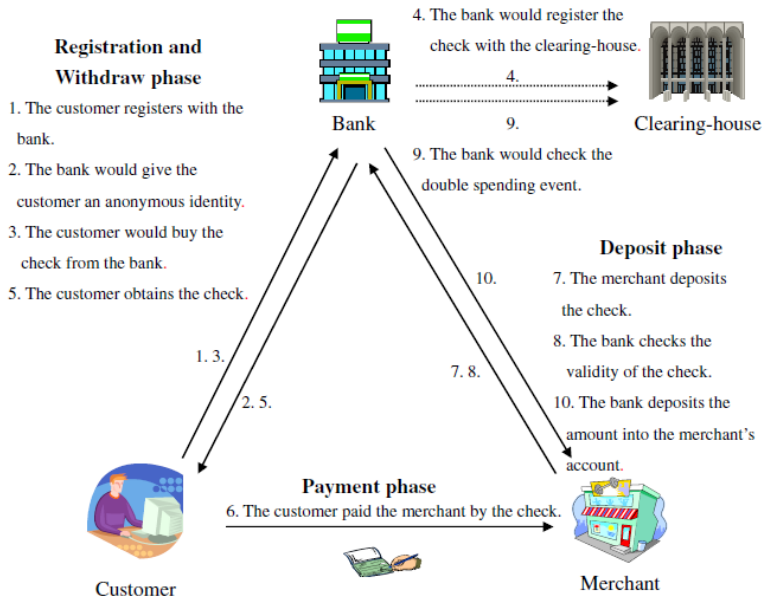

Figure 2: The steps of the off-line subprotocol (source: [1])

(c) The payment phase

After the customer has bought the merchandise, he uses the electronic traveler's check to pay the merchant. The payment phase includes the following two steps:

Step 1. After the customer has selected goods to buy, he encrypts the electronic traveler's check TC_{M_i}, serial number $S_{Q_{M_i}}$ and timestamp T_3 by using the merchant's public key Y_C to generate the check message $E_{Y_C}(TC_{M_i}, M_i, S_{Q_{M_i}}, T_3)$, and then sends it to the merchant.

Step 2. After receiving the check message $E_{Y_C}(TC_{M_i}, M_i, S_{Q_{M_i}}, T_3)$ and the merchant decrypts it by using its private key X_C to obtain $TC_{M_i}, M_i, S_{Q_{M_i}}$, and T_3, and checks whether timestamp T_3 is within a reasonable range. After the merchant has confirmed that T_3 is in time and the amount M_i is correct, the merchant delivers the goods to the customer.

(d) The deposit phase

In this phase, the merchant sends the electronic traveler's check to the bank. The bank would verify whether it is legal and valid. If so, the bank sends the check to the clearing-house to confirm whether double spending happens. If it does not occur, the bank deposits the amount of the electronic traveler's check to the merchant's account. The deposit phase includes the following two steps:

Step 1. The merchant encrypts $TC_{M_i}, M_i, S_{Q_{M_i}}$, and the timestamp T_4 by using bank's public key Y_B and send the result $E_{Y_B}(TC_{M_i}, M_i, S_{Q_{M_i}}, T_4)$ to the bank:

Step 2. The bank decrypts the received $E_{Y_B}(TC_{M_i}, M_i, S_{Q_{M_i}}, T_4)$ by using his private key X_B, obtaining TC_{M_i}, the amount M_i, serial number $S_{Q_{M_i}}$ and T_4. It would then check whether timestamp T_4 is within a reasonable range. If so, the bank computes $TC_{M_i} = h(R \oplus M_i \| S_{Q_{M_i}})$ and verifies whether it is equal to TC_{M_i}. If it is, the bank sends this check to the clearing-house to check whether double depositing or double spending occurs. If both do not exist, the bank deposits the amount of this check into the merchant's account.

Chapter 3 KCI and PS attacks on Liaw *et al.*'s scheme

In a KCI attack, an attacker E who knows the private key of A can masquerade as some other entity to communicate with A [2]. In a PS attack, two or more runs of the protocol are executed concurrently by the attacker [17], as described in the Introduction. In the registration phase, Liaw *et al.*'s scheme does not require a secure channel. We found that this makes their scheme susceptible to KCI and PS attacks. In Sections 3.1 and 3.2, we describe KCI and PS attacks on their online and offline versions, respectively.

3.1 KCI and PS attack on the online subprotocol

Assume that attacker E obtains the secret key X_A of customer A. He/she can then masquerade as bank B to communicate with A and carry out a site spoofing attack. We now describe the attacks that can take place during the registration and withdrawal phases, as shown in Figures 3 and 4, respectively.

(a) During the registration phase

An attack during the registration phase can take place as follows:

Step 1. When customer A registers with bank B, he/she chooses a random number K_{A1} following which his/her anonymous identity R_ID_A is generated by computing $R\_ID_A = h(ID_A \oplus K_{A1})$. He/she then encrypts it by using the bank's public key Y_B and sends this encrypted result $PE_{Y_B}(R\_ID_A)$ to E who is now pretending to be bank B, as shown in window 1 of Figure 3.

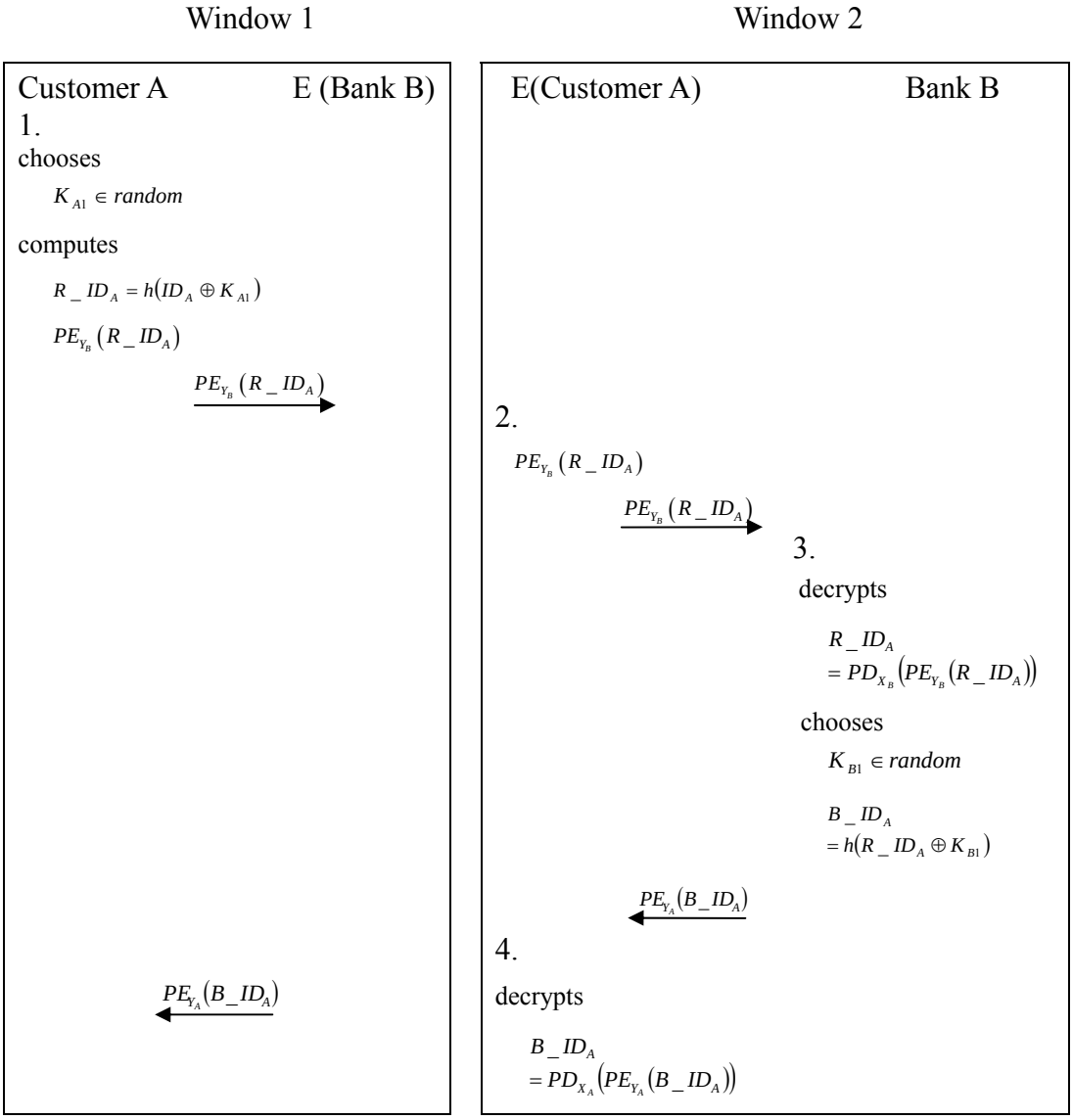

Figure 3: Our attack on the registration phase

Step 2. After receiving $PE_{Y_B}(R\_ID_A)$, E opens window 2 and masquerades as customer A to communicate with B. He/she retransmits the received encryption to B.

Step 3. Bank B decrypts the received information by using its private key X_B and obtains R_ID_A. Then, B chooses a random number K_{B1} and computes $B\_ID_A = h(R\_ID_A \oplus K_{B1})$. It encrypts B_ID_A by using the customer's public key Y_A and sends the result $PE_{Y_A}(B\_ID_A)$ to E who is pretending to be

customer A.

Step 4. After receiving $PE_{Y_A}(B\_ID_A)$, E decrypts it by using the private key X_A to get the anonymous identity B_ID_A. He then encrypts B_ID_A by using A's public key and sends the result $PE_{Y_A}(B\_ID_A)$ to A, as shown in window 1 of Figure 3.

(b) During the withdrawal phase

After obtaining the anonymous identity B_ID_A during the registration phase, E can masquerade as customer A to buy an electronic traveler's check from bank B. We now describe the attack during the withdrawal phase, as shown in Figure 4.

Step 1. E again masquerades as customer A. He/she chooses a random number K_{A2}, computes $R_A = h(B\_ID_A \oplus K_{A2})$, and encrypts R_A by using B_ID_A as a symmetric key. He/she then sends the result $E_{B\_ID_A}(R_A)$ to bank B.

Step 2. Bank B decrypts the received message to obtain R_A. Then, it chooses a random number K_{B2}, computes $R_B = h(X_B \oplus K_{B2})$ by using its private key X_B and calculates $R = R_A \oplus R_B$. It then encrypts R, R_B, and timestamp T_1 by using the symmetric key B_ID_A and sends the result $E_{B\_ID_A}(R, R_B, T_1)$ to E.

Step 3. E decrypts the received message by using B_ID_A and obtains R, R_B, and timestamp T_1. E computes $R' = R_A \oplus R_B$ to verify whether this newly computed R' is equal to R, and checks whether the timestamp T_1 is valid. If both are correct, E computes $C_A = h(R \oplus M_i \oplus Q_{M_i})$, where R is the payee's endorsement; M_i, the face value of the electronic traveler's check; Q_{M_i}, the

amount of the electronic traveler's check; and C_A, the payment requirement. E then chooses a timestamp T_2 and encrypts M_i, Q_{M_i}, C_A, and T_2 by using symmetric key R_A and sends the result $E_{R_A}(M_i, Q_{M_i}, C_A, T_2)$ to bank B.

Step 4. Bank B decrypts $E_{R_A}(M_i, Q_{M_i}, C_A, T_2)$ to obtain M_i, Q_{M_i}, C_A, and T_2. Then, B checks whether T_2 is within a predefined range. If it is, bank B computes $C'_A = h(M_i \oplus Q_{M_i} \oplus R_A \oplus R_B)$ to verify whether C'_A is equal to C_A. If it is, B generates the electronic traveler's check TC_{M_i} by computing $TC_{M_i} = h(R \oplus M_i \| S_{Q_{M_i}})$, where $S_{Q_{M_i}}$ is the serial number of the electronic traveler's check chosen by B. Then, B sends TC_{M_i} to the clearinghouse for recording and safekeeping. Finally, bank B encrypts and sends $E_{R_A}(TC_{M_i}, S_{Q_{M_i}})$ to E.

Step 5. E decrypts $E_{R_A}(TC_{M_i}, S_{Q_{M_i}})$ by using R_A to obtain TC_{M_i} and $S_{Q_{M_i}}$. He/she then computes $TC'_{M_i} = h(R_A \oplus R_B \oplus M_i \| S_{Q_{M_i}})$ and compares it with TC_{M_i} to verify whether both are equal. If they are, E stores TC_{M_i} and the serial number $S_{Q_{M_i}}$ in his/her smart card.

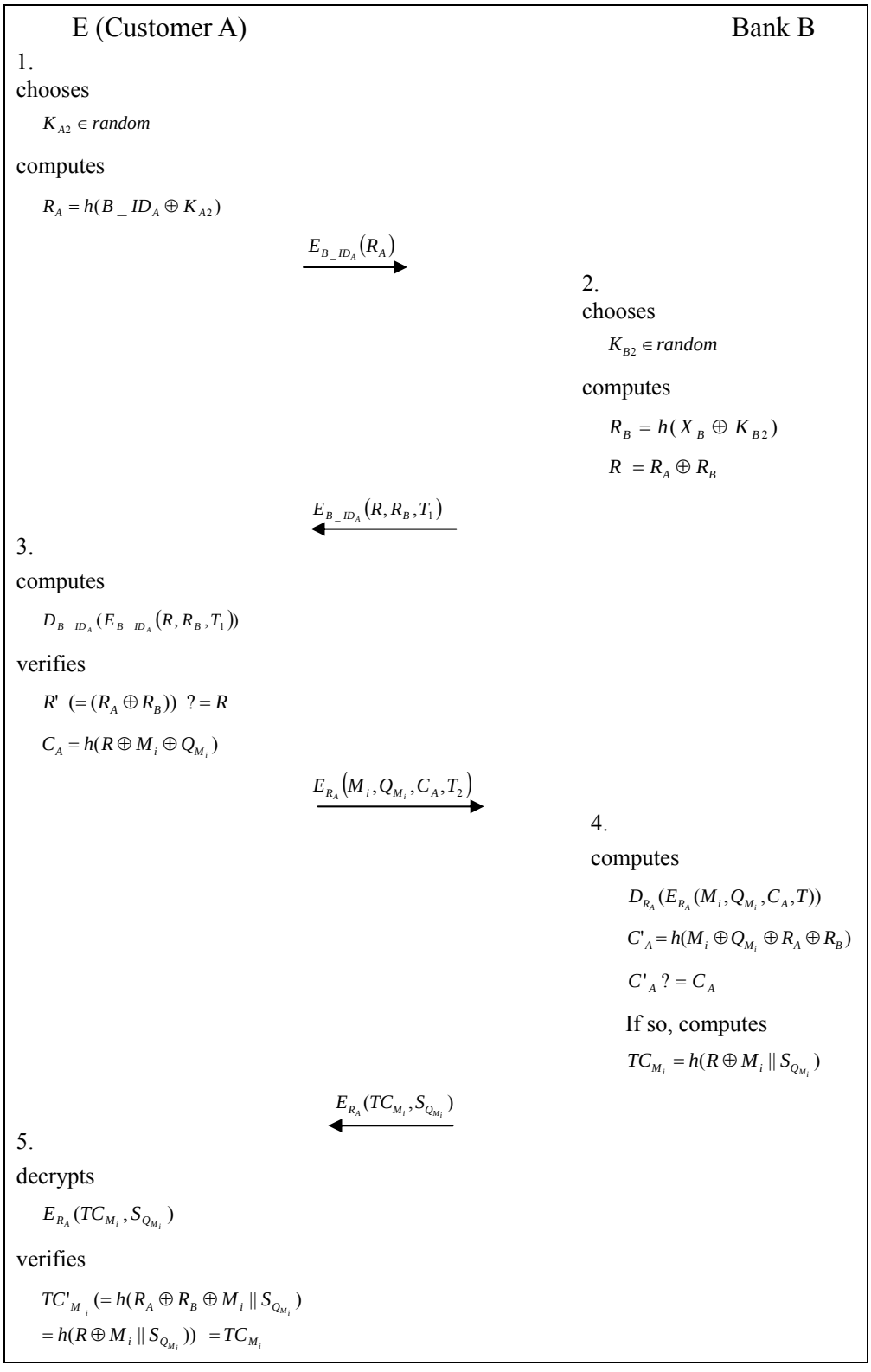

Figure 4: Our attack on the withdraw phase

When the electronic traveler's check is lost, E sends $(TC_{M_i}, S_{Q_{M_i}})$ to report the loss. In response, bank B reissues a new electronic traveler's check $TC_{M_i} = h(R_A \oplus R_B \oplus M_i \| S_{Q_{M_i}})$ to E.

(c) During the payment phase

E can buy goods from a merchant using an electronic traveler's check withdrawn from bank B. The payment phase includes the following four steps, as shown in Figure 5.

Step 1. When buying goods, E encrypts the information $TC_{M_i}, M_i, S_{Q_{M_i}}, T_3$ by using his anonymous identity B_ID_A as a symmetric key to form the message $E_{B\_ID_A}(TC_{M_i}, M_i, S_{Q_{M_i}}, T_3)$, where T_3 is system timestamp. This message is then sent to the merchant.

Step 2. After receiving $E_{B\_ID_A}(TC_{M_i}, M_i, S_{Q_{M_i}}, T_3)$, the merchant forwards it to bank B.

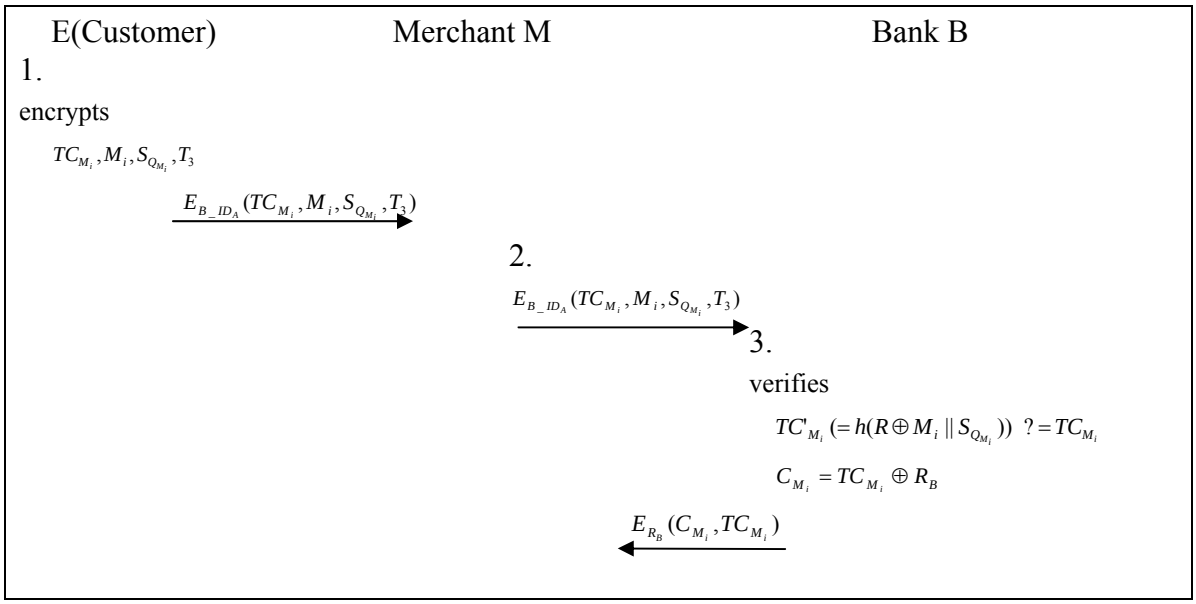

Figure 5: Our attack on the payment phase

Step 3. B decrypts the message to obtain TC_{M_i}, the face value M_i, the serial number $S_{Q_{M_i}}$, and timestamp T_3. Then, it checks to see whether timestamp

T_3 is within a predefined range. If it is, B computes $TC'_{M_i} = h(R \oplus M_i \,||\, S_{Q_{M_i}})$ and compares it with TC_{M_i} to verify whether TC_{M_i} is valid. If it is valid, B will also send TC_{M_i} to the clearinghouse via a secure channel to verify whether it is being double spent, by using the serial number $S_{Q_{M_i}}$. If it is, bank B determines the real identity of the customer by using the value of B_ID_A. If the verification of all the parameters—$TC_{M_i}, M_i, S_{Q_{M_i}}, T_3$, and the identity—is successful, the bank computes $C_{M_i} = TC_{M_i} \oplus R_B$ and encrypts both C_{M_i} and TC_{M_i} by using R_B as a symmetric key. The result $E_{R_B}(C_{M_i}, TC_{M_i})$ is then sent to the merchant. Only after the electronic traveler's check TC_{M_i} has passed the bank's verification procedure, can it be deposited in the bank.

Step 4. When the merchant receives the electronic traveler's check from the bank, the transaction is completed.

(d) During the deposit phase

In this phase, merchant M sends the electronic traveler's check to bank B. Bank B then verifies its own digital signature on the electronic traveler's check. If the signature is valid, B deposits the amount on the electronic traveler's check into the merchant's account. The deposit phase includes the following two steps, as shown in Figure 6.

Step 1. The merchant sends both $E_{R_B}(C_{M_i}, TC_{M_i})$ and a timestamp T_4 to bank B.

Step 2. Bank B checks whether timestamp T_4 is within a predefined range. If it is, it decrypts $E_{R_B}(C_{M_i}, TC_{M_i})$ to obtain C_{M_i} and TC_{M_i}. Then, B computes and verifies whether $C'_{M_i} \ (= TC_{M_i} \oplus R_B) \ = C_{M_i}$ holds. If it does, TC_{M_i} is sent to

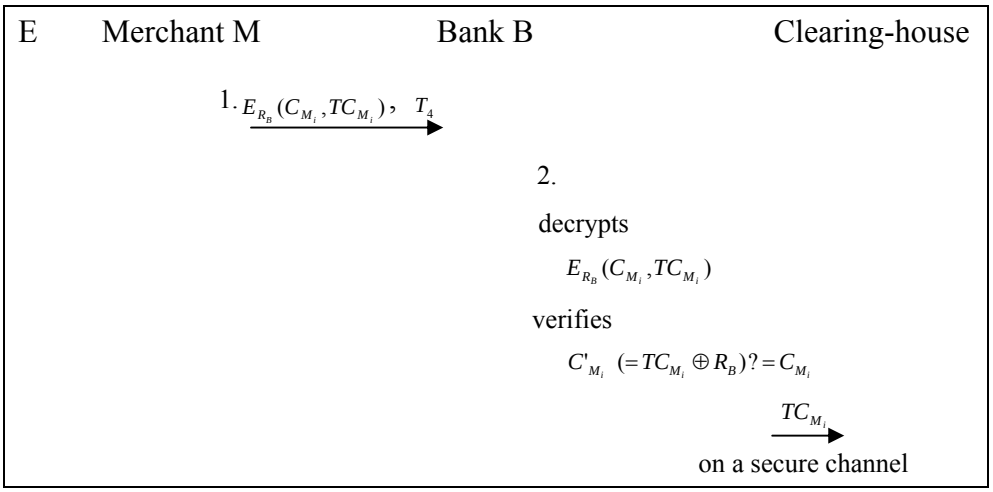

Figure 6: Our attack on the deposit phase

the clearinghouse via a secure channel to check whether it is unredeemed. If the electronic traveler's check is unredeemed, bank B deposits the amount on the electronic traveler's check into E's account.

As a result, adversary E has successfully used the electronic traveler's check. In other words, attacker E has perpetrated the fraud through the payment and deposit phases successfully.

3.2 KCI and PS attack on the offline subprotocol

The difference between the online and the offline versions is that bank B and the clearinghouse are not involved in the offline subprotocol. Our attacks on the offline subprotocol are similar to the online version. Hence, we omit them here.

Chapter 4 Our improvement

To prevent the KCI and PS attacks in Liaw *et al.*'s scheme, we improve both the registration and the withdrawal phases in the online and offline subprotocols. The other phases are identical to those in Liaw *et al.*'s scheme. The details of our improvement for the online subprotocol are described in Section 4.1. Our improvement for the offline subprotocol is similar to that for the online version, as has been stated in Section 4.2.

4.1 Improvement for the online subprotocol

In this section, we describe our improvements for the registration and withdrawal phases in subsections (a) and (b), respectively; these render the scheme impregnable against the KCI and PS attacks. The other two phases are identical to those in the original version.

(a) Registration phase

We improve on the registration phase through the following steps, as shown in Figure 7.

Step 1. The customer chooses a random number K_{A1}. He/she also randomly chooses K_{BA} as the session key to be shared with bank B. He/she then uses his private key X_A to encrypt K_{BA}, and computes $h(K_{BA})$ and $R\_ID_A = h(ID_A \oplus K_{A1})$. Then, he/she encrypts R_ID_A, $PE_{X_A}(K_{BA})$, and $h(K_{BA})$ by using the bank's public key Y_B and sends the result $PE_{Y_B}(R\_ID_A,\ PE_{X_A}(K_{BA}),\ h(K_{BA}))$ to bank B.

Step 2. After receiving the message, B decrypts it using its private key to obtain R_ID_A, $PE_{X_A}(K_{BA})$, and $h(K_{BA})$. It then uses A's public key to decrypt $PE_{X_A}(K_{BA})$ and obtain K_{BA}. It also uses hash function $h(\bullet)$ to compute $h(K_{BA})$ and compares it with the one in the decryption result. If they are equal, it chooses a random number K_{B1}, computes $B\_ID_A = h(R\_ID_A \oplus K_{B1})$, and signs on B_ID_A by using its private key. Then, B encrypts both B_ID_A and the signature $PE_{X_B}(B\_ID_A)$ by using K_{BA} and sends the result to customer A.

Step 3. After receiving the message, A decrypts it, to obtain B_ID_A and B's signature. He/she verifies the signature. If it is valid, A chooses a random number K_S as the session key shared with B and another key K_r as the encryption key for K_S. He/she computes $C = K_{BA} \oplus K_r$ and sends ID_A, C, $E_{K_r}(K_S)$, and $E_{K_s}(K_{A1})$ to B.

Step 4. After receiving the message from A, B computes $K_r = C \oplus K_{BA}$, $K_S = D_{K_r}(E_{K_r}(K_S))$, and $K_{A1} = D_{K_S}(E_{K_S}(K_{A1}))$, and verifies whether $R\_ID_A = h(ID_A \oplus K_{A1})$ holds. If it does, B accepts A's registration.

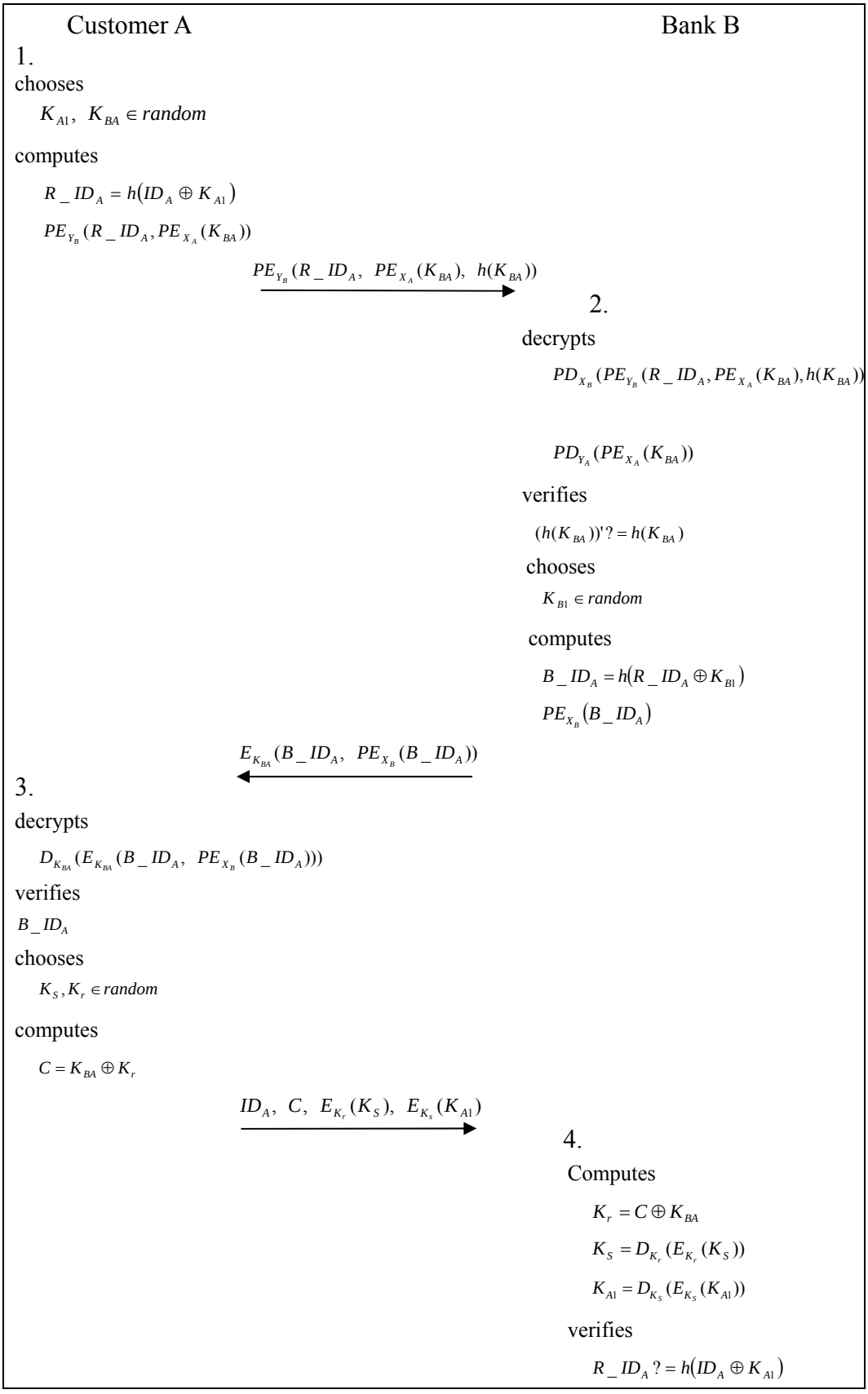

Figure 7: Our improvement for the registration phase

(b) Withdrawal phase

In this phase, both communicating parties (A and B) use K_S as the session key to communicate with each other. We improve on the withdrawal phase through the following steps, as shown in Figure 8.

Step 1. Customer A chooses a random number K_{A2} and computes $R_A = h(B\_ID_A \oplus K_{A2})$. Then, he encrypts B_ID_A and R_A by using session key K_S and sends the result $E_{K_S}(B\_ID_A, R_A)$ to the bank.

Step 2. B chooses a random number K_{B2} and computes $D_{K_S}(E_{K_S}(B\_ID_A, R_A))$, $R_B = h(X_B \oplus K_{B2})$, and $R = R_A \oplus R_B$. It then encrypts R, R_B, and timestamp T_1 by K_S and sends the result $E_{K_S}(R, R_B, T_1)$ to A.

Step 3. A decrypts the received message, to obtain R, R_B, and T_1. He/she checks whether T_1 is valid. If it is, A computes $C_A = h(R \oplus M_i \oplus Q_{M_i})$ and encrypts M_i, Q_{M_i}, C_A and timestamp T_2 by using R_A, and sends the result $E_{R_A}(M_i, Q_{M_i}, C_A, T_2)$ to B.

Step 4. B decrypts the message from A, to obtain M_i, Q_{M_i}, C_A, and T_2. It checks whether T_2 is valid. If it is, B computes $TC_{M_i} = h(R \oplus M_i \| S_{Q_{M_i}})$, chooses a random number K_{S2} to be the new session key for A's next withdrawal, and encrypts $TC_{M_i}, S_{Q_{M_i}}, K_{S2}$ by using R_A. It then sends the result $E_{R_A}(TC_{M_i}, S_{Q_{M_i}}, K_{S2})$ to A.

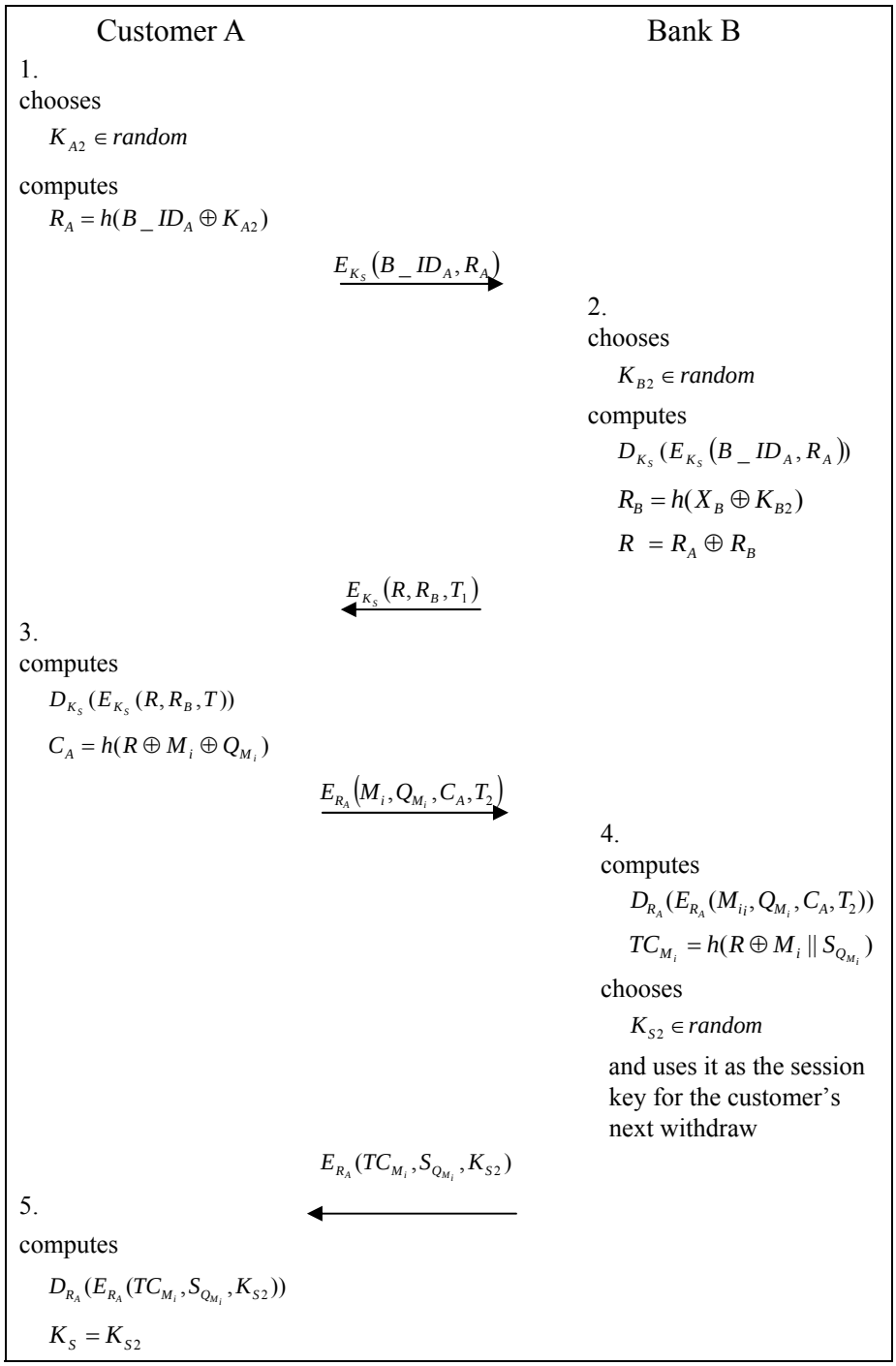

Figure 8: Our improvement for the withdraw phase

Step 5. A decrypts the received message, to obtain $TC_{M_i}, S_{Q_{M_i}}$, and K_{S2}. He/she replaces session key K_S with K_{S2} for the next protocol run.

4.2 Improvement for the off-line subprotocol

The difference between the on-line and off-line subprotocols is that bank B and the clearing-house are not involved in the off-line version but the on-line version involves both of them. Since our improvement makes no relationship to this point, our improvement on the off-line subprotocol is thus the same as the one on the on-line version. We therefore omit it here.

Chapter 5 Conclusion

In this paper, we propose a KCI and parallel session attack on both Liaw et al.'s on-line and off-line electronic traveler's check subprotocols. We also propose an improvement to resist against the attack we launch. Our improvement uses the customer's public key to avoid the deficiency such that even if an attacker knows the private key of a customer, he/she cannot masquerade as the bank to communicate with the customer. Our improvement makes the electronic traveler's check scheme more secure for adoption as a faithful method in the Internet.

Although our improvement makes the electronic traveler's check scheme more secure but the merchant can not reject the double spent check in the payment phase. It will be our future work to solve this problem.

References

[1] Horng-Twu Liaw, Jiann-Fu Lin, Wei-Chen Wu, “A new electronic traveler’s check scheme based on one-way hash function,” Electronic Commerce Research and Applications 6, 2007, pp. 499–508.

[2] Simon Blake-Wilson, Alfired Menezes, “Authenticated Diffie-Hellman key agreement protocols”, Proceedings of the 5th Annual Workshop on Selected Areas inCryptography (SAC’98), Lecture Notes in Computer Science, 1999, pp. 339-361.

[3] WANG Xiao-fen, DONG Qing-kuan, ZHOU Yu, XIAO Guo-zhen “Improvement of McCullagh-Barreto key agreement with KCI-security,” The Journal of China Universities of Posts and Telecommunications, April 2009, 16(2), pp. 68–71.

[4] Yong Xu, Jindi Liu, “Electronic Check System Design Based on RFID,” Information Science and Engineering (ICISE), 2009 1st International Conference on IEEE Conferences , 2010, pp. 5345 – 5348.

[5] Taher ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithm,” IEEE Trans. Inform. Theory IT-31 (4) 1985, pp. 469–472.

[6] Chang-Jinn Tsao, Chien-Yuan Chen, Cheng-Yyuan Ku, “An electronic bearer check system,”IEICE Trans. Commun. E85-B (1), 2002, pp. 325–331.

[7] Jong-E Hsien, Chih-Cheng Hsueh, Chien-Yuan Chen, “An electronic Travele’s check system,” in: 2001 Conference on Theory and Practice for Electronic Commerce, Taiwan, 2001, pp. 164–169.

[8] Shengbao Wang, Zhenfu Cao, Maurizio Adriano Strangio and Lihua Wang, “Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol,” December 14, 2007.

[9] Wei-Kuei Chen, “Efficient on-line electronic checks,” Applied Mathematics and Computation 162, 2005, pp. 1259–1263.

[10] Jianhong Zhang1,2, Wei Zou1, Dan Chen3 and Yumin Wang.” On the Security of a Digital Signature with Message Recovery Using Self-certified Public Key,” Informatica 29, 2005, pp. 343–346.

[11] WANG Jian-hui, LIU Jing-wei, LI Xiao-hui, KOU Wei-dong,” Fair e-payment protocol based on blind signature,” The Journal of ChinaUniversities of Posts and

Telecommunications October 2009, 16(5), pp. 114–118.

[12] Jesus Tellez Isaac a , Jose Sierra Camara b, Sherali Zeadally c, Joaquin Torres Marquez b. “A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks,” Computer Communications 31, 2008, pp 2478–2484.

[13] Whitfield Diffie, Martin E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, Vol. IT-22, No.6, November, 1976, pp. 644-654

[14] Zhang, Q. Markantonakis, K. Mayes, K. “A Mutual Authentication Enabled Fair-Exchange and Anonymous E-Payment Protocol,” 26-29 June 2006, pp.20 – 20.

[15] Zhao Huawei Liu Ruixia, “A Scheme to Improve Security of SSL,Circuits, Communications and Systems,” 2009. PACCS '09. Pacific-Asia Conference on IEEE Conferences, 2009, pp. 401 – 404.

[16] Hany Harb, Hassan Farahat, Mohamed Ezz, “SecureSMSPay: Secure SMS Mobile Payment model,” Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on IEEE Conferences, 2008 , pp. 11 – 17.

[17] Wenbo Mao, “*Modern Cryptography-Theory & Practice*”, Practice Hall Inc, 2004.

[18] Jue-Sam Chou, Yalin Chen, Ming-Hsun Cho, Hung-Min Sun, “A Novel ID-based Electronic Cash System from Pairings, “http://eprint.iacr.org/2009/339.pdf”.