E-TRAVELER'S CHECKS WITH RECIPROCAL AUTHENTICATION

Ya-Fen Chang
Department of Computer Science and Information Engineering,
National Chung Cheng University,
Chiayi 621, Taiwan, R.O.C.
cyf@cs.ccu.edu.tw

Chin-Chen Chang
Department of Computer Science and Information Engineering,
National Chung Cheng University,
Chiayi 621, Taiwan, R.O.C.
ccc@cs.ccu.edu.tw

ABSTRACT

As life becomes more and more convenient with all sorts of high-techs around, traveling has become more and more popular. Travelers nowadays can choose to use either common metallic/paper currency or credit cards to pay their bills. However, money in pockets or wallets/purses is subject to being robbed of, while credit cards are at the risk of being cloned. The traveler's check, which is a third choice, comes in to get travelers around such risks and to protect their rights. However, traditional traveler's checks cannot keep impostors from forging and cashing them illegally. This will result in serious damages to the check-issuing banks. In this paper, we shall propose a brand-new type of check called the e-traveler's check to preserve the rights of the e-traveler's check holders and prevent the check-issuing banks from being damaged.

Keywords: password authentication, smart card, traveler's check

1. Introduction

In recent years, overseas traveling has become a commonplace way of spending holidays and vacations as a result of the improvement in the living standard. People may change their domestic currency into foreign currencies or bringing credit cards with them to cover their expenditures during their trips. However, travelers are at the risk of being robbed or picked or losing their purses/wallets accidentally. People with malicious intensions may use the credit cards by forging the signatures. In such cases, travelers may probably have no way to fully recover their losses. To lower the risks, the traveler's check has come to existence. To get a traveler's check, one has to pay equivalent money to the bank. After getting the check, the user signs his/her name on it and keeps a copy of it in case the traveler's check is lost. Once the traveler's check is unfortunately lost, the check holder can show the copy and get the reissued check. When the check holder wants to cash the check, he/she needs to sign the check again and show his/her passport for authentication. However, artful imposters can still manage to forge traditional traveler's checks and cash them by taking the following steps: (1) forging the check or the passport; (2) impersonating the innocent check holder. Such crimes are actually being committed around the world any minute. The criminals may forge checks and passports to gain illegal benefits from the check-issuing banks. Or, the imposter may simply take the passport and the traveler's check away without being noticed and then impersonate the check holder to have the check cashed. This can happen easily, for it is hard for bank tellers to tell fine differences between the face of the imposter and the passport picture.

To save travelers and banks from losses, we now propose a brand-new traveler's check called the e-traveler's check. No imposter can get the proposed e-traveler's check cashed even if it is stolen or forged. Furthermore, with the e-traveler's check, the check validity authentication process can be done without the presence of the passport. These two properties are of special significance because they can solve all the above-mentioned problems. The proposed method is based on the definition of the cross product in an n-dimensional linear space [Laih et al. 1991]. This approach ensures that any malicious check casher cannot retrieve the essential secret information to impersonate the legal check holder even when the e-traveler's check has been cashed several times, and the check-cashing organization can not cheat in any way. In our design, a smart card [Chen and Ku 2002], [Jablon 1996], [Yi et al. 2002] is used to record some important information. When the e-traveler's check is to be cashed, what the

check holder needs to bring with him/her to the check-cashing organization is the smart card only, which means the passport is no longer necessary. The fingerprint is used to authenticate the ownership. The card holder has the smart card, which can authenticate his/her ownership by matching the fingerprint [Lee et al. 2002]. This approach makes the proposed e-traveler's check more secure and the e-traveler's check holder unable to transfer the check to other users by giving the password away. Moreover, passwords are used to protect the rights of the e-traveler's check holders and to defend against the professional criminals. Thus, the fingerprint and the password replace the signature and the passport for authenticating the validity of the e-traveler's check holder. In the proposed method, reciprocal authentication can be done to ensure that no imposters or intruders can cheat or impersonate the check-issuing bank, the check-cashing organization, and the e-traveler's check holder.

Nowadays, e-cash is proposed to be used as another kind of e-payment [Liu et al. 2001], [Maat 1997], [Wang and Zhang 2001]. E-cash includes an electronically-stored value designed to be used in a single transaction or in many. All kinds of e-cash store and convey value in and of themselves rather than merely representing a value residing elsewhere, such as a deposit account. If the electronic cash smart card is lost, the card holder will lose the balance of electronic cash held on that card because electronic cash is like physical cash. If you lose your smart card, it would be the same as losing bills or coins [http://www.myiris.com/cards/cardArt.php?cardartno=2]. Moreover, e-cash ought to be untraceable. That is, the user can spend e-cash anonymously. On the other hand, the e-traveler's check holder does not need to have an account of his/her own. Instead, he/she just only pays the equivalent money to get the e-traveler's check. Moreover, the e-traveler's check is only cashed by the check holder. If the e-traveler's check is lost, no one can cash it; in addition, the check holder can be reissued the lost check.

This paper is organized as follows. In Section 2, we shall introduce the definition of the cross product in an n-dimensional linear space. In Section 3, some standards the e-traveler's check should live up to will be listed. Then, the brand-new e-traveler's check will be presented in Section 4, followed by the security analyses and discussions in Section 5. Finally, the conclusions will be in Section 6.

2. Preliminaries

In this section, we shall introduce the definition of the cross product in an n-dimensional linear space. The cross product of n-1 linearly independent n-dimensional row vectors U_1, U_2, …, U_{n-1}, where $U_i = (u^i{}_1, u^i{}_2, ..., u^i{}_n)$ and i is in [1, n-1], is defined as follows.

$U_1 \times U_2 \times \ldots \times U_{n-1} =$

$$\left(\begin{vmatrix} u^1{}_2, & u^1{}_3, \cdots, & u^1{}_n \\ u^2{}_2, & u^2{}_3, \cdots, & u^2{}_n \\ & \cdots & \\ u^{n-1}{}_2, & u^{n-1}{}_3, \cdots, & u^{n-1}{}_n \end{vmatrix}, \begin{vmatrix} u^1{}_3, & u^1{}_4, \cdots, & u^1{}_n, & u^1{}_1 \\ u^2{}_2, & u^2{}_3, \cdots, & u^2{}_n, & u^2{}_1 \\ & \cdots & & \\ u^{n-1}{}_2, & u^{n-1}{}_3, \cdots, & u^{n-1}{}_n, & u^{n-1}{}_n \end{vmatrix}, \cdots, \begin{vmatrix} u^1{}_1, & u^1{}_2, \cdots, & u^1{}_{n-1} \\ u^2{}_1, & u^2{}_2, \cdots, & u^2{}_{n-1} \\ & \cdots & \\ u^{n-1}{}_1, & u^{n-1}{}_2, \cdots, & u^{n-1}{}_{n-1} \end{vmatrix} \right).$$

In [Laih et al. 1991], it is claimed that the determinants of (n-1)*(n-1) matrices mentioned above can be computed by using the probabilistic algorithm proposed in [Wiedemann 1986]. Wiedemann showed that the probabilistic algorithm to find the n determinants of an (n-1)*(n-1) matrix requires as many as O(n(n-1)(w+n-1)) field operations, where w is approximate to the number of field operations needed to apply the matrix to a test vector.

3. Requirements

In this section, let's see how our e-traveler's check works. The e-traveler's check is similar to a conventional traveler's check in that the user needs to pay equivalent money to get one. Unlike conventional traveler's checks, however, e-traveler's checks provide reciprocal authentication to ensure that no imposters or intruders can cheat or impersonate the check-issuing bank, the check-cashing organization, or the e-traveler's check holder. To make it even user-friendlier, the check holder only needs to use the issued smart card to have the check cashed without having to show the passport. The user password chosen by the applicant replaces the signature and the passport on the side of the conventional traveler's check. In the smart card, some secret information is stored and protected by the user password. The protected information generated by the check-issuing bank tells which one the check-issuing bank is and what the number of times of cashing the check holder can do. Furthermore, the procedures of retrieving the secrets for cashing the e-traveler's check are simple and efficient.

In our opinion, a scheme involving the e-traveler's check must satisfy the following requirements:

(1) The e-traveler's check must have a unique identity.

(2) The e-traveler's check can only be generated by the check-issuing bank or the authorized organization with the applicant.
(3) Only the valid check holder can have the e-traveler's check cashed.
(4) The check-issuing bank, the check-cashing organization, and the e-traveler's check holder can authenticate one another to ensure that no one cheats.

Requirement 1 provides the uniqueness of the e-traveler's check for the check-issuing bank to identify. With this property, the check-issuing bank can easily find the corresponding maintained data to check the validity of the check holder, the number of cashing times and other essential information. Requirement 2 ensures that only the applicant and the check-issuing bank can generate the smart card. This can prevent the e-traveler's check from being forged and keep imposters from cheating. Requirement 3 is an extension of Requirement 2. The idea is that the imposter cannot have the stolen or forged e-traveler's check cashed since he/she does not know the secret of the e-traveler's check chosen by the valid check holder. This requirement is very important because it protects the rights of the check-issuing bank and the check holder. Requirement 4 is to enhance the security so that the rights of all participants, not only the check-issuing bank and the check holder but also the check-cashing organization, are protected.

4. The Brand-new E-traveler's Check

In this section, we shall present our proposed e-traveler's check based on the definition of cross product in an n-dimensional linear space. The proposed method is divided into three phases: the initialization phase, the application phase, and the payment phase. The three phases are described in Subsections 4.1, 4.2, and 4.3, respectively.

4.1 The Initialization Phase

In this subsection, we introduce the basic infrastructure of the proposed scheme. First of all, there exists a bank that provides the e-traveler's check service by issuing the smart card to the applicant. The check center (CC) of the bank takes the responsibility of managing the procedures of issuing or checking the e-traveler's check. CC maintains a database to record the information about the issued e-traveler's checks. With PKI, each of the e-traveler check issuers and the check-issuing organizations owns a public key and a corresponding private key.

4.2 The Application Phase

In the following, we are going to show how the user applies to the bank for the valid e-traveler's check.

Step1. The user U applies to CC of the bank for the e-traveler's check by paying the equivalent money. U may prefer to cash the e-traveler's check n times, where n is an integer and is greater than or equal to one.

Step 2. CC selects n linearly independent (n+2)-dimensional row vectors, V_1, V_2, …, and V_n.

Step 3. CC randomly selects an n*n matrix A, which is a full rank square and

$$A = \begin{bmatrix} a_{11}, & a_{12}, & \cdots, & a_{1n} \\ a_{21}, & a_{22}, & \cdots, & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}, & a_{n2}, & \cdots, & a_{nn} \end{bmatrix} .$$

Step 4. CC then computes

$$\begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_n \end{bmatrix} = \begin{bmatrix} a_{11}, & a_{12}, & \cdots, & a_{1n} \\ a_{21}, & a_{22}, & \cdots, & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}, & a_{n2}, & \cdots, & a_{nn} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_n \end{bmatrix} .$$

For j = 1 to n, where j is an integer, CC repeats Step 5, Step 6, and Step 7.

Step 5. CC then selects a linearly independent (n+2)-dimensional row vector, V^j_{n+1}.

Step 6. CC evaluates a new vector $U^j = (u^j_1, u^j_2, \ldots, u^j_{n+1}) = V_1 \times V_2 \times \ldots \times V_n \times V^j_{n+1}$ and calculates

$$K^j = \prod_{i=2}^{n+2} \text{abs}(u^j_i) \text{ , where abs}(u^j_i) \text{ denotes the absolute value of } u^j_i.$$

Step 7. CC randomly selects an (n+1)-dimensional row vector b^j and computes

$$P^j = b^j \times \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_n \\ V^j{}_{n+1} \end{bmatrix} .$$

Step 8. CC randomly chooses a smart card identity SC that does not exit in the current database and stores SC, K^j, $u^j{}_1$, and P^j, for j = 1, 2, …, n, in the database. Moreover, CC maintains a corresponding integer counter initialized to be one and is in [1, n] for each e-traveler's check.

Step 9. U chooses the user password P_U by himself/herself and imprints his/her fingerprint on the fingerprint input device. Then, CC stores $H(P_U) \oplus S_i$, for i = 1, 2, …, n, SC, ID_{CC}, and PK_{CC}, where ID_{CC} denotes the identity of CC and PK_{CC} denotes the public key of CC, in the smart card, which can authenticate the ownership by matching U's fingerprint [Lee et al. 2002], and issues the smart card to U, where H() is a one-way hash function and $\oplus$ denotes the bit-wise XOR operation. //* Note that $S_i = (s_{i1}, s_{i2}, ..., s_{i,n+1}, s_{i,n+2})$ and $H(P_U) \oplus S_i = (H(P_U) \oplus s_{i1}, H(P_U) \oplus s_{i2}, ..., H(P_U) \oplus s_{i,n+1}, H(P_U) \oplus s_{i,n+2})$, where $|H(P_U)|$ is equal to the maximum length of $|s_{i1}|, |s_{i2}|, ..., |s_{i,n+1}|$, and $|s_{i,n+2}|$. If the length of $|s_{i,k}|$, for k = 1, 2, …, n+2, is smaller than $|H(P_U)|$, additional zeros are added to make the length equal to $|H(P_U)|$, e.g. $|H(P_U)| = 5$, $H(P_U) = 17$, $s_{1,n+2} = 5$ and $H(P_U) \oplus s_{1,n+2} = (10001)_2 \oplus (00101)_2 = (10100)_2 = 20$. *//

4.3 The Payment Phase

On the side of the organization ECO that can cash the e-traveler's check, there should be a smart card reader. When U wants to cash the check the j-th time, the payment phase performs as shown in Figure 1. The details are shown as follows:

Step 0. U inserts the issued smart card in the card reader and imprints his/her fingerprint on the fingerprint input device. If U's fingerprint is successfully verified, the phase continues; otherwise, the phase is terminated.

Step 1. Then U chooses a random number R and computes $E_{PK_{CC}}(R)$ and sends it to ECO, where E is the public key encryption function.

Step 2. After getting $E_{PK_{CC}}(R)$, ECO sends $E_{PK_{CC}}(ID_{ECO} \| SC \| E_{PK_{CC}}(R))$ to CC to get the retrieval pattern P^j and $u^j{}_1$, where "||" denotes the concatenation symbol and ID_{ECO} denotes the identity of ECO.

Step 3. After getting the request from ECO, CC uses his/her own private key to retrieve ID_{ECO}, SC, and R. CC finds that the corresponding counter is equal to j, $u^j{}_1$, and P^j and sends $E_{PK_{ECO}}(j \| u^j{}_1 \| P^j \| ID_{CC} \| H(R))$ to ECO, where PK_{ECO} is the public key of ECO.

Step 4. After receiving the transmitted message, ECO gets the retrieval patterns $u^j{}_1$ and P^j by decrypting $E_{PK_{ECO}}(j \| u^j{}_1 \| P^j \| ID_{CC} \| H(R))$ with his/her own private key and sends $u^j{}_1$, P^j, and H(R) to U via a secure channel.

Step 5. First, U checks whether H(R) is equal to the hash value of R chosen in Step 1. If it is, U inputs the password P_U through the secure channel and retrieves S_1, S_2, …, and S_n by computing $H(P_U) \oplus (H(P_U) \oplus S_i)$, for i = 1, 2, …, n. U uses P^j and retrieves S_1, S_2, …, and S_n to compute $S_1 \times S_2 \times \ldots \times S_n \times P^j = (w^j{}_1, w^j{}_2, \ldots, w^j{}_{n+2})$ and calculates $K^{j\prime} = \prod_{i=2}^{n+2} abs(w^j{}_i / h^j)$, where $h^j = w^j{}_1 / u^j{}_1$. Then, U sends $E_{PK_{CC}}(K^{j\prime})$ to ECO via the secret channel. Otherwise, U considers ECO or CC not trustworthy.

Step 6. ECO sends $E_{PK_{CC}}(j \| ID_{ECO} \| SC \| E_{PK_{CC}}(K^{j\prime}))$ to CC.

Step 7. CC decrypts the transmitted message with his/her own private key to get $K^{j\prime}$ and j. First, CC checks whether this j is equal to that j sent in Step 3. If it is not, CC will consider ECO to be dishonest; otherwise, CC checks whether $K^{j\prime}=K^j$ is true or not. If $K^{j\prime}$ is equal to K^j, CC sends $E_{PK_{ECO}}(accept \| E_{SK_{CC}}(H(E_{PK_{CC}}(j \| ID_{ECO} \| SC \| E_{PK_{CC}}(K^{j\prime})))))$ to ECO, where SK_{CC} denotes the private key of CC, and adds one to the counter;

otherwise, CC sends $E_{PK_{ECO}}(\text{reject} \| E_{SK_{CC}}(H(E_{PK_{CC}}(j \| ID_{ECO} \| SC \| E_{PK_{CC}}(K^{j\prime})))))$ to ECO.

Step 8. ECO uses his/her own private key SK_{ECO} to decrypt the received massage and PK_{CC} to determine the validity of the received message by checking whether $E_{PK_{CC}}(E_{SK_{CC}}(H(E_{PK_{CC}}(j \| ID_{ECO} \| SC \| E_{PK_{CC}}(K^{j\prime})))))$ $= H(E_{PK_{CC}}(j \| ID_{ECO} \| SC \| E_{PK_{CC}}(K^{j\prime})))$ holds or not. If it holds, ECO decides whether or not to cash the e-traveler's check according to the retrieved message; otherwise, ECO just refuses to cash the check since the message is not valid.

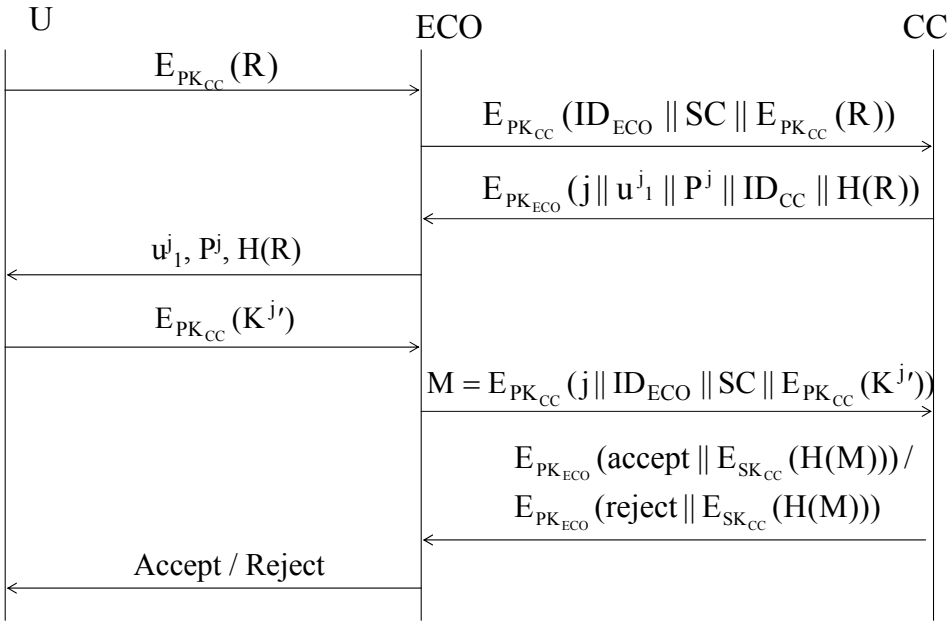

Figure 1: The payment phase

5. Discussions and Security Analyses

First, we shall show whether the proposed scheme satisfies the requirements mentioned earlier. Then, we will demonstrate that the proposed method is secure.

5.1 The Achieved Requirements

In this subsection, we demonstrate that our proposed scheme satisfies the requirements mentioned in Section 3.

5.1.1 The e-traveler's check contains a unique identity.

As mentioned in the application phase in Section 4, CC randomly chooses a smart card identity SC, which does not exit in the maintained database. SC and the CC's identity ID_{CC} are stored in the smart card for the unique e-traveler's check to be distinguished from others. Because CC can choose SC, CC can avoid existing ones. Hence, the proposed e-traveler's check indeed contains a unique identity to be distinguished.

5.1.2 The e-traveler's check can only be generated by the check-issuing bank or the authorized organization with the applicant.

As mentioned in Section 4, the applicant applies to the check-issuing bank for the e-traveler's check by paying the equivalent money. In the application phase, the applicant chooses his/her password to protect the secret information generated by CC. This approach ensures that only CC and the user U can generate the e-traveler's check, since they have to cooperate to generate the secret stored in the smart card. Hence, the proposed method achieves Requirement 2.

5.1.3 Only the valid check holder can have the e-traveler's check cashed.

As mentioned above, the holder needs to imprint his/her fingerprint on the fingerprint input device for authenticating the ownership. That is, the e-traveler check cannot be transferred to other users. Moreover, the check holder chooses the password by himself/herself in the application phase. When having the e-traveler's check cashed, the check holder has to input his/her password to retrieve the protected information generated by CC. Even if the

smart card is stolen or duplicated, and the professional criminal can get U's fingerprint, the user password is still unknown to anybody but the check holder. As a result, only the valid check holder can have the check cashed.

5.1.4 The check-issuing bank, the check-cashing organization, and the e-traveler's check holder can authenticate one another to ensure that no one cheats.

As mentioned in Subsection 4.3, the user U generates a random number R and encrypts it with CC's public key in Step 1. Then ECO sends $E_{PK_{CC}}(ID_{ECO} \| SC \| E_{PK_{CC}}(R))$ to CC in Step 3. CC will retrieve R with his/her private key and compute H(R). In Step 5, U needs to check whether the hash value of R is equal to the received value sent from ECO. This ensures that U can determine whether ECO and CC are valid. It is because only CC can retrieve R and encrypt H(R) with ECO's public key. With PKI, CC needs to verify whether the public key is valid before using it for encrypting any data. Since only ECO knows his/her private key, only he/she can retrieve H(R) and send it to U via the secure channel. In Step 2, ECO sends $E_{PK_{CC}}(ID_{ECO} \| SC \| E_{PK_{CC}}(R))$ to CC. As above, ECO can determine whether CC is the valid check-issuing bank in Step 4 according to the received information. CC can easily determine whether U and ECO are legal and valid as shown in Step 7. ECO authenticates U in Step 8. For the above reasons, we can make sure that the proposed method can prevent imposters or malicious users from cheating.

5.2 Security Analyses

In this subsection, we are going to show that the proposed e-traveler's check is secure.

5.2.1 Suppose the smart card is duplicated or lost.

In this case, we can expect a malicious user in an attempt to masquerade. The user's fingerprint is used to ensure the ownership. Even though the smart card is duplicated or lost, the malicious user cannot make the smart card work. Moreover, as mentioned in Subsections 5.1.1 and 5.1.2, the malicious user still cannot have the check cashed because the e-traveler's check is generated by both U and CC. In other words, the malicious user does not know the user password even if he/she is a professional criminal to get the card holder's fingerprint, so there is no way to get the secret information stored in the smart card for authentication.

5.2.2 Suppose that an imposter wants to impersonate ECO.

It is impossible for this trick to work out since ECO will be authenticated in Step 5 and Step 7 of the payment phase by U and CC, respectively. Since the validity of ECO is ensured before any important data is inputted or transmitted, the imposter cannot get any meaningful information this way.

5.2.3 Suppose that an imposter wants to impersonate CC.

As mentioned in Subsection 5.1.4, CC is authenticated in Step 4 and Step 5 of the payment phase by ECO and U, respectively. No one can impersonate CC since CC's public key needs to be verified before being used with PKI, and CC's private key is supposed to be secure.

5.2.4 Suppose the malicious ECO tries to retrieve the secret information stored in U's smart card.

As mentioned in Subsection 4.3, U uses P^j and retrieves S_1, S_2, …, and S_n to compute $S_1 \times S_2 \times \ldots \times S_n \times P^j = (w^j_1, w^j_2, \ldots, w^j_{n+2})$ and calculates $K^{j\prime} = \prod_{i=2}^{n+2} \mathrm{abs}(w^j_i / h^j)$, where $h^j = w^j_1 / u^j_1$. P^j and u^j_1 are transmitted to U by ECO. If any v previous secrets K^g's, where g is in [1, n-1], are known, the secrecy of the hidden information stored in U's smart card is decreased from n to n-v. In other words, if v previous secrets K^g's and (n-v) secrets S_i's are known, the remaining v secrets S_i's will be able to be retrieved. However, S_i, for i = 1, 2, …, n, are protected by the user's password, and U sends $E_{PK_{CC}}(K^{j\prime})$ to ECO via the secure channel. ECO still cannot get the secret $K^{j\prime}$ since CC's private key is unknown. Hence, it is impossible for ECO to retrieve the secret information stored in U's smart card.

5.3 More Discussions

First of all, we will show the essential features of real-life traveler's checks and discuss how to modify the proposed method so that the e-traveler's check can possess the same characteristics.

As we know, the traveler's check holder can be reissued the traveler's check after proving the ownership of the lost check by showing the copy. Moreover, check-issuing banks can sell traveler's checks of different denominations. The above two characteristics are quite important and essential. Here, we shall show some possible modifications on our proposed method to equip it with these characteristics.

First, CC only needs to store more information to record the identity of the applicant—the passport number for example. This way, the check holder only needs to show the passport to prove his/her own identity when asking for a

reissue. CC and the organization need to authenticate each other before generating the check. Then, CC secretly informs the organization of the detailed information of the checks such as the remaining amount of to be cashed and the denominations of the checks. Then, CC authorizes the reissuing of the e-traveler's check. The remaining part of the procedure is the same as shown in Subsection 4.3. After reissuing the e-traveler's check, the organization will secretly send the needed data, which have to be maintained in CC's database, to CC. As a result, the check holder can be reissued the e-traveler's check. Second, CC can sell e-traveler's checks of different denominations by recording the individual face value of each e-traveler's check. If the denominations of the e-traveler's checks are stored in order, then the check holder must have the checks cashed in that order. Hence, CC can keep track of the remaining cashing times of each denomination. The above two approaches ensure that the proposed method can possess the same characteristics the original traveler's check does.

Second, users may use "old smart cards." The computation ability of the smart card is sufficient to execute multiplication operations and RSA en/decryptions [Zhu et al. 2002] and to authenticate the ownership [Lee et al. 2002]. In the proposed paper, RSA public key cryptosystem can be employed. With PKI, certificates are needed to prove the legality of the public keys. Because the user will apply to the bank for the e-traveler's check by himself/herself, the validity of CC's public key is ensured. Moreover, the user does not need to verify the validity of ECO or CC's public key while cashing the e-traveler's check. This approach will greatly lighten the computation load of the user. On the other hand, the smart card only needs to execute multiplication and hash operations in addition. The time of the execution can be shortened by parallel computation since no dependence exists among the inputs of the computed outputs.

Third, because the user needs to apply the e-traveler's check by himself/herself, no attacks such as the man-in-the-middle attacks can be successfully mounted on the proposed method in the application phase. What is more, since the equivalent amount of money needs to be gotten to issue the e-traveler's check, and the corresponding retrieval patterns of the issuing e-traveler's check need to be stored in the maintained database, the attacks made by international criminals can be detected by the auditing functions.

At last, the possible drawbacks of the proposed e-traveler's checks are shown as follows. Though the old smart card can be used in the proposed scheme, the smart card must own the ability of authenticating the ownership by matching the fingerprint. Moreover, extra fingerprint input devices are needed for the user to imprint his/her fingerprint. Thus, the cost of the infrastructure will increase. People can trust PKI in local systems. It is possible that proposed application may cause problems to wait. However, for the increasing requirements of the transnational commerce, there is no doubt that users of overseas PKI's will be able to communicate with those of local PKI's soon. That is, the proposed application will be used globally without causing problems to wait.

5.4 The Achieved Properties

Here, we demonstrate that the proposed method confirms confidentiality, identification and non-repudiation in Subsections 5.4.1, 5.4.2, and 5.4.3, respectively.

5.4.1 The proposed method ensures confidentiality.

As mentioned in Subsection 5.1.2, only CC and U can cooperate to generate the secret stored in the smart card. Moreover, the communication between the smart card and the card reader is authenticated by each other [Lee et al. 2002]. That is, no one can get the transmitted data of the communication. In addition, the user password is used to make the secret data stored in the smart card unable to be retrieved. We can conclude that the proposed method ensures confidentiality.

5.4.2 The proposed method ensures identification.

As shown in Subsection 5.1.3, the holder needs to imprint his/her fingerprint on the fingerprint input device for authenticating the ownership. And, the check holder chooses the password by himself/herself in the application phase. That is, the e-traveler's check cannot be transferred to other users. Moreover, even if the professional criminal can get U's fingerprint, the user password is still unknown to anybody but the check holder. As a result, identification is ensured in the proposed method.

5.4.3 The proposed method ensures non-repudiation.

As mentioned in Subsection 5.2, it is sure that no one can impersonate ECO, CC, or U. In addition, ECO, CC, and U can authenticate one another to ensure that no one cheats as shown in Subsection 5.1.4. It is sure that non-repudiation is ensured in the proposed method.

6. Conclusions

As we mentioned earlier, traveling has taken a more and more dominant part of our lives. Making the trip safer and more convenient is a major concern. In this paper, we have shown that the proposed e-traveler's check is

convenient and secure; the e-traveler's check holder only needs to bring the smart card with him/her to the check-cashing organization without having to show the passport, and no imposter can have the check cashed. Even if the check is unfortunately lost, the check holder can still ask an authorized organization to reissue the e-traveler's check. Moreover, check-issuing banks can sell e-traveler's checks of different denominations just the same way they do traditional traveler's checks. In a word, our e-traveler's check is practical, secure, and convenient.

REFERENCES

Chen, C.M. and Ku, W.C., "Stolen-verifier Attack on Two New Strong-password Authentication Protocol," IEICE Transactions on Communications, Vol. E85-B, No. 11, pp. 2519-252, November 2002.

http://www.myiris.com/cards/cardArt.php?cardartno=2

Jablon, D., "Strong Password-only Authenticated Key Exchange," ACM Computer Communication Review, Vol. 26, No. 5, pp. 5-26, September 1996.

Laih, C.S., Harn, L., Lee, J.Y., and Hwang, T., "Dynamic Threshold Scheme Based on the Definition of Cross-product in an N-dimensional Linear Space," Journal on Information Science and Engineering, Vol. 7, No. 1, pp. 13-23, March 1991.

Lee, J.K., Ryu, S.R., and Yoo, K.Y., "Fingerprint-based Remote User Authentication Scheme Using Smart cards," IEE Electronics Letters, Vol. 38, No. 12, pp. 554-555, June 2002.

Liu, J.K., Wei, V.K., and Wong, S.H., "Recoverable and Untraceable E-cash," Proceedings of International Conference on Trends in Communications, EUROCON'2001, Vol. 1, Bratislava, Slovak Republic, pp. 132–135, July 2001.

Maat, M., "The Economics of E-cash," IEEE Spectrum, Vol. 34, No. 2, pp. 68–73, February 1997.

Wang, H. and Zhang, Y., "Untraceable Off-line Electronic Cash Flow in E-commerce," Proceedings of 24th Computer Science Conference, ACSC 2001, Australasian, pp. 191–198, February 2001.

Wiedemann, D.H., "Solving Sparse Linear Equations over Finite Fields," IEEE Transactions on Information Theory, Vol. IT-32, pp.54-62, 1986.

Yi, X., Tan, C.H., Siew, C.K. and Syed, M.R., "ID-based Key Agreement for Multimedia Encryption," IEEE Transactions on Consumer Electronics, Vol. 48, No. 2, pp. 298-303, May 2002.

Zhu, F., Wong, D.S., Chan, A.H., and Ye, R., "Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks," Proceedings of ISC 2002, LNCS 2433, Tsukuba, Japan, pp. 150-161, January 2002.