Improved E-cash Protocol

Aye Thandar Swe, Khin Khat Khat Kyaw

Abstract: - Electronic cash (e-cash) has been more and more popular in the electronic commerce transaction protocol. Ronggong Song and Larry Korba present their views on e-cash to improve Abe and Fujisaki's protocol. Their protocol achieves non-repudiation and anonymity services between customer and merchant. However, there still has weak fairness in their protocol. Therefore, we propose a modified e-cash protocol to avoid weak fairness. The properties of our protocol include: (1) fair exchange for everyone that include in the protocol (2) anonymity for the customer and (3) non-repudiation for the customer, merchant and bank.

Keywords: - anonymity, electronic cash, electronic commerce, fairness, non-repudiation

1 Introduction

Electronic cash is an electronic payment system. It is designed and implemented for making purchases over open networks such as the Internet. When an e-cash system is performed on the Internet, there still exist some problems between customers and merchants. For example, a customer has paid e-cash to a merchant. But he cannot ensure that the merchant will send the e-goods which he has paid for. Similarly, a merchant has sent e-goods to a customer but he also cannot ensure that the customer will send payment. Fairness guarantees that either all parties can receive the items they expect, or no one can control the protocol outcome. Weak fairness means that if an honest party does not receive its expected item, while the other party does, then the first party receives a proof of this fact. Non-repudiation is one of the important security services in electronic commerce. Non-repudiation means that an entity cannot deny its participation in a message exchange. Thus, non-repudiation protocols provide for undeniable data exchange between two or more principle. J. Zhou and D. Gollmann proposed a two-party fair non-repudiation protocol [1]. It is a popular beginner for reducing the involvement of trusted third party (TTP). The protocol works as follows. First, the sender A directly sends the receipt B his encrypted message. Then, B returns the evidence of receipt (NRR) to A. Next, A sends his message key and proof of submission to the TTP in order to win the commitment later. Finally, B fetches the confirmation and the key from TTP and decrypts the message. In this protocol, both A and B have the responsibility to retrieve the key and evidence from TTP. Therefore, both parties fairly get the advantage of non-repudiation. The same authors modified the above protocol in order to reduce online trust third party [2]. TTP comes online only when one party cannot obtain the expected non-repudiation evidence from the other party. This variant protocol is suitable for environments where the two parties are likely to resolve communication problems between themselves and rely on TTP only as a last recourse. E-cash is the important payment for anonymous digital money on the Internet in electronic commerce, which is regarded as equivalent of coin in physical world. Basic security services for e-cash system are anonymity and privacy. Many researchers have improved privacy for e-cash system. One problem not addressed by existing true fair exchange protocols is anonymity. Anonymity ensures that the identity of a customer and, optionally, that of a merchant is not revealed during an e-commerce transaction. For example, a customer may not want outsiders to reveal a pattern of his spending habits. Therefore, the customer may want an anonymous identity. Similarly, a merchant may also want to remain anonymous. An e-cash system must prevent a user from double-spending because it is easy to duplicate electronic data. Ideally, the anonymity of honest users must be protected and the identity of cheaters must be recovered without using a TTP. An electronic payment system must also prevent a merchant from depositing the same coin twice. Partially Blind Signature techniques played an important role in building e-cash systems for anonymity service. It allows the signer to include pre-agreed information such as expiration date or collateral conditions in the resulting signature. In [3], the author proposed a non-repudiation and anonymous e-cash scheme based on partially blind signature that enables the Judge to specify a dishonest customer, bank, or blind office. In [4], the author proposed an efficient and secure on-line electronic check system. By generating an anonymous identity for payer from bank at registration phase, that scheme solved the Chang et al.'s anonymity, large computation, and time synchronous issues. At paying phase, the payer can use the anonymous identity to buy some goods from payee. In [5], the author proposed an efficient e-cash system. To provide the non-repudiation service, a one-time public key is embedded in the partial blind signature. In order to get anonymity service and non-repudiation service for the customers and build a fair e-cash system, the author proposed a new e-cash system using a modified partial blind signature scheme proposed by Abe [6]. Their protocol achieves non-repudiation and anonymity services between customer and merchant. However, there still has weak fairness in their protocol. In this paper, we will propose a modified protocol to avoid weak fairness and analyze to show that our modified protocol can achieve more secure. The paper is organized as follows. The next section describes the review of Ronggong Song and Larry Korba's Protocol and analyzes that protocol. The section following next introduces the proposed protocol. In section 4 we analyze the security of our protocol. The last section presents our conclusion.

- Aye Thandar Swe is assistant lecturer in information technology department in University of Technology (Thanlyin), Myanmar.
  E-mail: ayethandarswe84@gmail.com
- Dr. Khin Khat Khat Kyaw is associate professor in information and communication technology department in University of Technoloy (Yadanarpon cyber city), Myanmar. E-mail: khat81@gmail.com

2 Review of Ronggong Song and Larry Korba's Protocol

2.1 Terminology and Notations

Terminology and notations used in the paper are defined as follows.

- A: a customer
- B: a bank
- ES: an e-commerce store
- ID_A: customer A's identity
- $H()$: one-way hash function
- Z_n : the integers modulo n
- Z^*_n: the multiplicative group of Zn
- $M \bmod n$: residue of M divided by n
- $Time_A$: time stamp made by customer A
- $Sign_A$: customer A's signature
- $gcd(m, n)$: greatest common divisor of m and n
- $A \rightarrow B{:}M$: customer A sends message M to the bank B
- RM: remainder money after A purchases the e-goods
- EMD: e-goods message digest

2.2 E-cash Issue Protocol

When a customer wants to buy e-goods by using online shopping, he/she first needs to buy some e-cashes. It is issued by the bank using the following protocol where all communications are supported by the SSL security channel.

1. $A \rightarrow B$: ID_A, $Account_A$, PK_A, α, v, $Time_A$, $Sign_A$

2. $B \rightarrow A$: ID_A, ID_B, β, $Time_B$, $Sign_B$

Step 1: If a customer decides to purchase an e-cash from the bank, he/she first makes a temporary public key (e_t, n_t), and keeps its private key (d_t, p_t, q_t) secret (using RSA public key cryptosystem). Then, the customer selects a random integer r in Z^*_{nb}, and computes $\alpha \equiv (r^{ebv} H(e_t \| n_t) \bmod n_b)$ where || denotes the concatenation symbol, and v contains the following basic information predefined by the bank, i.e. expiration date and money. Then, the customer computes the signature $Sign_A$ as follows.

$$Sign_A \equiv (H(ID_A, Account_A, PK_A, \alpha, v, Time_A)^{dA} \bmod n_A$$

Finally, the customer sends the bank the messages (ID_A, $Account_A$, PK_A, α, v, $Time_A$, $Sign_A$) by using SSL security channel.

Step 2: After achieving the above messages through the SSL security channel, the bank checks whether or not the messages: $Account_A$, $Time_A$, $Sign_A$, and v are correct. If they are correct, the bank computes $\beta \equiv (\alpha^{(ebv)-1} \bmod n_b\ )$ and the signature:

$$Sign_B \equiv (H\ (ID_A, ID_B, \beta, Time_B))^{db} \bmod n_b$$

Then, it sends the messages (ID_A, ID_B, β, $Time_B$, $Sign_B$) to the customer through the SSL security channel. In the meantime the bank deducts the money from the customer's account. Finally, after achieving the messages sent by the bank through the SSL security channel, the customer checks whether or not the messages: $Time_B$ and $Sign_B$ are correct. If they are correct, he/she then computes $s \equiv (r^{-1}\beta \bmod n_b)$ as the signature of the bank and gets his/her e-cash (e_t, n_t, v, s).

2.3 Online Shopping Protocol

When the customer wants to buy some e-goods like e-book, software, and movie, etc. from the Internet, since it is not necessary for the shipping service, he/she could use the following protocol. When the customer wants to download the licenses of the e-goods and hide his/her identity, he/she could use that online shopping protocol.

1. A→ES: E-goods, Cost, $\text{Account}_{\text{ES}}$, e_t, n_t, v, s, Time_A, Sign_t

2. ES→B: Cost, $\text{Account}_{\text{ES}}$, e_t, n_t, v, s, Time_A, EMD, Sign_t

3. B→ES: $\text{Receipt}_{\text{ES}}$, e_t, n_t, v, s, RM, s', Time_B , Sign_B

4. ES→A: License, Receipt_A, e_t, n_t, v, s, RM, s', Time_{ES}, Sign_{ES}

2.4 Ronggong Song and Larry Korba's Protocol Security Analysis

In this section, we analyze the security of Ronggong Song and Larry Korba's Protocol, and indicate weak fairness of their protocol. In the system, the bank and merchant cannot determine that who purchases the e-goods. The bank and merchant do not know anything about the customer except how much money the customer spends for e-cashes. This provides anonymity property for the customers. The owners of the messages signed all transferred messages with their own signatures in the protocol, they can ask a Court to judge it if there is a dispute later. Therefore, the protocol provides the non-repudiation service for the customer, merchant and bank. However, their protocol still provides weak fairness for customer. After receiving the correct payment from the bank in step 3, the merchant can deny to send the product decryption key to the customer because the merchant did not sent Non-repudiation of Receipt (NRR) to anyone. Therefore, that protocol has weak fairness for customer.

3 The Proposed System

3.1 Architecture

In the modified e-cash protocol, we only modify the online shopping protocol. We reuse e-cash issue protocol from the above protocol. The modified e-cash system consists of three parties: merchant, customer and bank. In the system, the bank behaves as TTP. In the modified system, the merchant and customer first need to apply and get their certificates from the bank by opening their accounts in the bank. When a merchant ES want to sell electronic goods (e-goods), he must register e-goods himself with the bank (TTP). ES sends the e-goods, its description which includes the cost, and a key pair (K, K^{-1}) to the bank. ES encrypts the e-goods with key K and advertises it on the web.

3.2 Online Shopping Protocol

1. $A \rightarrow ES$: E-goods, Cost, $Account_{ES}$, e_t, n_t, v, s, $Time_A$, $Sign_t$

2. $ES \rightarrow B$: E-goods, Cost, $Account_{ES}$, e_t, n_t, v, s, $Time_A$, $Sign_t$, $Sign_{ES}$

3. $B \rightarrow A$: License, $Receipt_A$, e_t, n_t, v, s, RM, s', $Time_B$, $Sign_B$

4. $B \rightarrow ES$: $Receipt_{ES}$, $Account_{ES}$, $Time_B$, $Sign_B$

Step 1: The protocol starts with the customer (A). The customer downloads an encrypted product from the merchant (ES). Then, A sends ES a purchase order, and computes the following signature $Sing_t$ with the private key corresponding to the temporary public key of the e-cash.

$$Sign_t \equiv (H\ (Cost,\ Account_{ES}\ ,\ e_t,\ n_t,\ v,\ s,\ Time_A)\ ||H\ (E\text{-}goods))^{dt}\ mod\ n_t.$$

Then A sends the messages (*E-goods, Cost,* $Account_{ES}$, e_t, n_t, v, s, $Time_A$, $Sign_t$) to the ES by using the SSL security channel.

Step2: After receiving the above messages, the merchant checks whether or not the messages: *Cost,* $Account_{ES}$, $Time_A$, $Sign_t$, and $s^{ebv} \equiv (H\ (e_t||n_t)\ mod\ n_b)$ are correct. If they are correct, the merchant forwards the bank the messages (*E-goods, Cost,* $Account_{ES}$, e_t, n_t, v, s, $Time_A$, $Sign_t$).

Step3: The bank verifies whether or not the messages: $Account_{ES}$, $Time_A$, and $Sign_t$ are correct. If they are correct, it deducts the money from the e-cash. Then, the bank computes the remainder money *RM* and the signature

$$s' \equiv (H(e_t,\ n_t,\ v,\ s,\ RM)\ )^{db}\ mod\ n_b$$

$$Sign_B \equiv (H\ (License,\ Receipt_A,\ e_t,\ n_t,\ v,\ s,RM,\ s',\ Time_B,)\ )\ ^{dB}\ mod\ n_B$$

Finally, the bank makes a receipt for the customer and sends the customer the messages (*License,* $Receipt_A$, e_t, n_t, v, s, RM, s', $Time_B$, $Sign_B$). After achieving the messages, the customer obtains the licenses of the e-goods and his/her remainder e-cash.

Step4: Finally, the bank then deposits the money into the merchant's account and the bank makes a statement (receipt) for the merchant and sends the messages ($Receipt_{ES}$, $Account_{ES}$, $Time_B$, $Sign_B$) to the merchant.

$$Sign_B \equiv (H\ (Receipt_{ES},\ Account_{ES},\ Time_B,\ Sign_B))^{db}\ mod\ n_b.$$

4 Analysis

Our modified protocol still supports the anonymity service for customers and non-repudiation services for all players in the protocol. First, in the e-cash issue protocol, the customer sends the bank the message that is signed with the customer's certificate. When the customer repudiates this action, the bank can show the customer's signature. On the other hand, if the customer does not do this, the bank also cannot charge the customer because it cannot give an evidence (i.e., signature) to prove it. Secondly, in the modified online shopping protocol, the customer sent the merchant the messages that are signed with the private key of the e-cash. If the owner of the e-cash signed the message, he/she cannot deny his/her action because he/she has only the private key of the e-cash. On the other hand, the security of e-cash is safer because other person cannot spend the e-cash if he does not have the private key of the e-cash. Moreover, as we mentioned in the above anonymity analysis, the signature *Signt* does not reveal the identity of the e-cash owner because the temporary public key does not contain any information about the identity of the e-cash owner. Then, the temporary anonymous public key is embedded into the blind message in the e-cash issue protocol. In addition, since the e-cash cannot link with the real identity of e-cash owner, the bank would not know anything about the customer except how much money the customer uses for the e-cash. On the other hand, since the merchant only would have the record message about the e-cash, it also would know nothing about his customers. Therefore, the customers get strong privacy protection for the e-cash. Thirdly, the bank needs only to keep the still-alive e-cashes in its database for double-spending checking because its database can remove all expired e-cash. Moreover, our modified protocol gives fairness property for customer because the bank acts as TTP. If the merchant did not send the product decryption key to the customer, the bank would directly send the customer the product decryption key *License*.

5 Conclusion

We have proposed a modified on-line shopping e-cash protocol. Our protocol has some desirable features. First, it provides fair exchange for everyone that include in the protocol. Second, the protocol uses the bank like as trusted third party (TTP). Third, before actually paying for the e-goods, the customer is confident by paying for the correct product. Fourth, the protocol provides anonymity for the customer. Fifth, the protocol supports non-repudiation service for customer, merchant and bank. The future work is to evaluate the correctness of the protocol by using formal methods or model checker like theorem proving, Avispa, SVO, and MOCHA, etc.

Acknowledgment

The author would like to express her special thanks to Dr.Khin Khat Khat Kyaw, Associate Professor, Information and Communication Technology Department, University of Technology (Yadanarpon Cyber City), Myanmar for her initiation of this research and for her constructive comments. The author is indebted to her parents for their constant support and strong encouragements throughout her life.

References

[1] J. Zhou , D. Gollmann, "*A fair non-repudiation protocol",* In Proceedings of 1996 IEEE Symposiumon Security and Privacy, Oakland, California, pages 55–61, May 1996

[2] J. Zhou , D. Gollmann, "*An Efficient Non-repudiation Protocol"*

[3] Hani M. AL-Matari, Abdalnaseer A. Hajer and Nidal F. Shilbayeh, *"Anonymous and Non-Repudiation E-Cash Scheme with Partially Blind Signature",* Journal of Computing, Volume 3,Issue2, February 2011

[4] Chin-Ling Chen, Cheng-Hsiung Wu, Wei-Chech Lin, "*Improving An on-line Electronic Check System with Mutual Authentication",* International Conference on Advanced Information Technologies, 2010

[5] Ronggong Song and Larry Korba, “*How to Make E-cash with Non-Repudiation and Anonymity”* , Proceedings of the International Conference on Information Technology: Coding and Computing, 2004

[6] M.Abe and E.Fujisaki, “*How to Date Blind Signatures”* ,Advances in Cryptology-*ASIACRYPT'96* (LNCS 1163),pp.244-251,1996