An Efficient E-Payment Scheme

Sattar J Aboud
Iraqi Council of Representatives
Department of Information Technology
Baghdad-Iraq

ABSTRACT

The present e-payment schemes permit anonymity property to protect customer privacy. However, the majority of these schemes have not offered a non-denial property. For example, several difficulties subsist in the schemes such as repudiation, loss, abuse, theft, and overspend-tracing. This article suggests an e-payment scheme wherein a temporary anonymous public key is embedded in a partial blind signature protocol to give a non-denial protection challenging the above mentioned attacks. This paper also shows that the combination of both a partial blind digital signature scheme and anonymous digital signature scheme will build a new e-payment scheme that will be stronger and safer than before.

General Terms

Security

Keywords

E-payment scheme, e-coin issue, partial blind signature, Transport Layer Security TLS channel, online shopping

1. INTRODUCTION

Internet is developed to ensure that computers communicate without difficulty and to guarantee that network communications is sustained even if different connections may be harmed [1]. But this flexibility also makes it easy to cooperate information security and privacy [2]. However, to provide security and privacy protection for e-commerce services, in 1982 Chaum [3] suggested a blind signature protocol. The blind signature protocol not just maintains the characteristics of conventional digital signature but also holds the characteristics of the document contents blind to the signer and the document cannot be traced by the signer when the signature is exposed [4]. These characteristics can be employed for various e-commerce services, for example e-payment schemes [5, 6]. One property of e-coin is that it is easily reproduced [7]. This makes it essential for the bank to employ overspend-tracing [8]. But, the overspend-tracing does not give the non-denial property [9], for example the bank cannot decide whether the e-coin is spent by the actual owner or by a robber because the non-denial property wants the customer signature that can uncover the customer identity.

However, to give robust privacy and non-denial protection for the customer and to construct a safer e- payment scheme, we suggest an e-payment scheme using a tailored partial blind signature protocol. In the proposed scheme, the customer first wants to purchase e-coin from the bank. If the customer needs to use e-coin for online shopping via the internet later, he can employ e-coin for payment. In a tailored partial blind signature protocol, we embed a one-time anonymous public key into a blind document, which have no data regarding a customer. Because only the owner of e-coin has a secret key similar to a one-time anonymous public key, the proposed e-payment scheme gives a non-denial protection with an anonymous signature of the owner of e-coin,.For example when a customer actually spend e-coin before, he cannot repudiate the case since a bank has a signature to demonstrate the owner of e-coin has spent it, but a bank still does not know who the customer is. Also, except for the robust privacy protection, the customer can obtain one more advantage from the proposed scheme: no other entity but the owner can demonstrate that he is the owner of e-coin even when other entity has a copy of e-coin. This forms e-coin fair compare with any other scheme.
The remainder of this article is organized as follows. The partial blind signature protocol is briefly described in section 3. In section 4, the proposed e-payment scheme is suggested. In section 5, the properties of the proposed scheme are explained. In section 6, the security of the proposed scheme is analyzed. Finally, is the conclusions are given in section 7.

2. NOTATIONS USED

The notations used in this article are defined as follows:
C : Customer
B : Bank
M : Merchant
T : Trusted authority
E : E-commerce store
Id_C : Customer identity
e_C : Customer public key
$h(.)$: One-way hash function
Z_n^* : Multiplicative group of Z_n
Ti_C : Time stamp made by customer C
S_C : Customer signature
Acc_C : Customer account
gcd : Greater common divisor
g : E-goods
Co : Cost of the e-goods
L : License
R_C : Customer receipt
$C \to B$: A customer C sends message m to the bank B
y : Remainder money after customer C buys the e-goods
D : E-goods message digest
$||$: Concatenation

3. PARTIAL BLIND SIGNATURE

In this paper, a partial blind signature scheme is developed to control the bank database from rising without limitations, since the bank wants to keep all spent e-coin in its database for overspend-tracing [10]. In this scheme, every e-coin issued by the bank has an expiration date where all expired e-coin recorded in the bank database is eliminated [11]. The algorithm of the partial blind signature scheme is illustrated as follows.

3.1 Initialization Phase

By using RSA public key encryption scheme [12], the steps of the initialization phase are as follows:

Step 1: The bank B

1. Selects randomly two large prime numbers p and q equally likely.
2. Finds $n = p * q$.
3. Computes $\theta(n) = (p-1)(q-1)$.
4. Chooses a public key e .
5. Finds a private key by $e * d \equiv 1 \bmod \theta(n)$ with $\gcd(e, \theta(n)) = 1$.
6. Determines the public by (e, n) and private key by (d, θ) .
7. Selects a secure one-way hash function h [13].
8. Assumes that each u is a document determined by the bank B and have an expiration date of e-coin and each e-coin issued by the bank worth w dollars.

3.2 Withdrawal Phase

The steps of the withdrawal phase are as follows:

Step 1: The Customer C

When the customer C wants to withdraw e-coin issued by the bank, s/he should do the following:

1. Selects arbitrarily message m and an integervalue $k \in Z_n^*$.
2. Finds $b \equiv k^{e*u} * h(m) \bmod n$.
3. Passes b and u to the bank B .

Step 2: The Bank B

1. Checks whether u is true or not. If true,
2. Passes $z \equiv (b^{(e*u)^{-1}} \bmod n)$ to the customer C .
3. Subtracts w dollars from the customer C account.

Step 3: The Customer C

1. Finds $s \equiv (k^{-1} * z \bmod n)$.
2. Obtains the e-coin (m, s, u) .

3.3 Deposit Phase

The steps of depositing phase are as follows:

Step 1: The Merchant M

If a customer C uses the e-coin to pay a merchant M , the merchant M should do the following:

1. Checks if both u and $s^{e*u} \equiv h(m) \bmod n$ are true. If yes,
2. Contacts with the bank B to verify if the e-coin has been already spent, it means overspend-tracing. But, when the e-coin has not been spent, the merchant M accepts the payment and adds the e-coin to his account.

Step 2: The Bank B

1. Keeps (m, s, u) in its database for overspend-tracing and inserts w dollars to the merchant M account.

4. THE PROPOSED E-PAYMENT

The proposed e-payment scheme has four participants: customer C , bank B , merchant M , and trusted authority T . In the proposed scheme, the bank B , merchant M , and customer C first want to request and obtain their certificates from T trusted authority. After that, each secure exchange among them will be started using Transport Layer Security TLS channel [14] through the internet. The new scheme is a combination of the suggested partial blind signature scheme and the proposed e-payment scheme. However, the proposed e-payment scheme contains three protocols. The description of these protocols are as follows:

4.1 E-coin Issue Protocol

In this protocol, we use the suggested partial blind signature scheme and embed a one-time anonymous public key into the blind document where it goes well with e-payment scheme and supports a non-denial property. If the customer C needs to carry out online shopping, he should initially purchase e-coin from a bank employing the following protocol so that each interaction uses Transport Layer Security TLS channel.

$$C \rightarrow B : (Id_C, Acc_C, e_C, b, u, Ti_C, S_C)$$
$$B \rightarrow C : (Id_C, Id_B, B, Ti_B, S_B)$$

By using RSA public key encryption scheme, suppose that the public and corresponding secret key of the bank B are (e_B, n_B) and (d_B, p_B, q_B) while the public and corresponding secret key of the customer C are (e_C, n_C) and (d_C, p_C, q_C) respectively. The description of the protocol is as follows:

Step 1: **The Customer** C

When the customer C chooses to purchase e-coin issued by the bank B , he must do the following:

1. Create the one-time public key (e_t, n_t) and store its private key (d_t, p_t, q_t) in secret employing the RSA public key encryption scheme.
2. Select an arbitrary integer value $k \in Z_B^*$.
3. Find $b \equiv (k^{e_B * u} * h(e_t \| n_t) \bmod n_B)$ and u holds the basic data prearranged by the bank B , that is expiration date $(dd / mm / yyyy)$ and cash $(\$xxx.xx)$.
4. Find $S_C \equiv (h(Id_C, Acc_C, e_C, b, u, Ti_C))^{d_C} \bmod n_C$
5. Use TLS channel to pass the parameter $(Id_C, Acc_C, e_C, b, u, Ti_C, S_C)$ to the bank B .

Step 2: **The Bank** B

1. Checks if the parameter (Acc_C, Ti_C, S_C, u) is true. If yes,
2. Finds $z \equiv (b^{(e_B * u)^{-1}} \bmod n_B)$.
3. Finds $S_B \equiv (h(Id_C, Id_B, B, Ti_B))^{d_B} \bmod n_B$.
4. Uses the TLS channel to pass a document $(Id_C, Id_B, B, Ti_B, S_B)$ to the customer C .
5. Subtracts the cash from a customer C account.

6. Passes by TLS channel, a customer C checks if the pair (Ti_B, S_B) is true. If yes,
7. Finds $s \equiv (k^{-1} * z \bmod n_B)$ as a signature.
8. Obtains the e-coin (e_t, n_t, u, s).

4.2 Online Shopping Protocol

In this protocol, if the customer C wishes to carry out online shopping for certain e-goods such as e-publications and software, s/he can employ the following protocol to buy and download the licenses of e-goods when the customer C wishes to conceal his identity. In this protocol, we suppose that the communications also are secured by the TLS channel.

$$C \to E : (g, Co, Acc_E, e_t, n_t, u, s, Ti_C, S_t)$$

$$E \to B : (Co, Acc_E, e_t, n_t, u, s, Ti_C, D, S_t)$$

$$B \to E : (R_E, e_t, n_t, u, s, y, s', Ti_B, S_B)$$

$$E \to C : (L, R_C, e_t, n_t, u, s, y, s', Ti_E, S_E)$$

Step 1: **The Customer** C

When the customer C wishes to carry out online shopping for certain e-goods using the e-coin, s/he must do the following:

1. Choose g the e-goods.
2. Find a signature S_t with the secret key corresponding to a one-time public key of e-coin, satisfying $S_t \equiv (h(Co, Acc_E, e_t, n_t, u, s, Ti_C) \,||\, h(g))^{d_t} \bmod n_t$
3. Passe a parameter $(g, Co, Acc_E, e_t, n_t, u, s, Ti_C, S_t)$ to a merchant by using TLS channel.

Step 2: **The Merchant** M

1. Checks if parameters (Co, Acc_E, Ti_C, S_t) and $(s^{e_B * u} \equiv (h(e_t \,||\, n_t) \bmod n_B)$ are true. If yes,
2. Finds e-goods message digest $D = h(g)$.
3. Sends a parameter $(Co, Acc_E, e_t, n_t, u, s, Ti_C, D, S_t)$ to a bank, that issued e-coin, by TLS channel.

Step 3: **The Bank** B

1. Checks if the message (Acc_E, Ti_C, S_t) is true. If yes,
2. Puts the e-coin into a merchant account.
3. Subtracts the money from g e-coin.
4. Finds a remainder money y.
5. Computes $s' \equiv (h(e_t, n_t, u, s, y)^{d_B} \bmod n_B)$.
6. Finds $S_B \equiv (h(R_E, e_t, n_t, u, s, y, s', Ti_B))^{d_B} \bmod n_B$
7. Creates a receipt for the merchant.
8. Passes a message $(R_E, e_t, n_t, u, s, y, s', Ti_B, S_B)$ to the merchant by TLS channel.

Step 4: **The Merchant** M

1. Checks if all messages are true. If yes,
2. Creates a receipt for the customer
3. Finds $S_E \equiv (h(L, R_C, e_t, n_t, u, s, y, s', Ti_E))^{d_E} \bmod n_E$
4. Passes $(L, R_C, e_t, n_t, u, s, y, s', Ti_E, S_E)$ to a customer by the TLS channel.

Step 5: **The Customer** C

1. Obtains the licenses of e-goods g.
2. Obtains the remainder e-coin.

4.3 E-coin Renew Protocol

In this protocol, the customer can renew his e-coin if the e-coin is close to the expiration date by the below protocol. Additionally, the bank also cannot construct a relationship between the old e-coin and the new e-coin by the protocol.

$$C \to B : (b, u, e'_t, '_t, u', s', ti_t, S_t)$$

$$B \to C : (e'_t, n'_t, u', s', z, ti_B, S_B)$$

Step 1: **The Customer** C

1. Fills a new e-coin form
2. Finds the new blind document b and u as an above e-coin issue protocol.
3. Employs an old e-coin to find $S_t \equiv (h(b, u, e'_t, n'_t, u', s', ti_t))^{d_t} \bmod n_t$.
4. Passes the parameter $(b, u, e'_t, n'_t, u', s', ti_t, S_t)$ to the bank by TLS channel.

Step 2: **The Bank** B

1. Checks if the parameter is true. If yes,
2. Finds $z \equiv (b^{(e_B * u)^{-1}} \bmod n_B)$
3. Finds $S_B \equiv (h(e'_t, n'_t, u', s', z, ti_B))^{d_B} \bmod n_B$.
4. Records the old e-coin is cancelled awaiting the expiration date.
5. Following the expiration date, can erase all data concerning the old e-coin.
6. Passes the new e-coin to the customer by TLS channel.

5. PTOTOCOL PROPERTIES

In this section, we are going to describe the properties of the above mentioned protocols. These properties are as follows:

5.1 Robust privacy Protection

In the proposed scheme, any participant such as the bank and merchant cannot find out who buys the e-goods. The bank and merchant know nothing concerning the purchaser think for how much funds the purchaser spends for e-coins. This gives robust privacy confidence for the customers.

5.2 Robust Safety Protection

The proposed scheme only allows the customer of the e-coin to use the e-coin. Other participants, such as the bank and merchant, cannot use the e-coin because they cannot generate the signature without the secret key of the e-coin and prove that they are the holder of the e-coin. Thus, the purchasers must not be concerned regarding the loss, abuse, or theft of their e-coins.

5.3 Non-denial Property

Because every transmitted document is signed by the signatures of the owner of the document in the proposed scheme, they can be raise at a Court to judge, when there is a case afterward, that the proposed scheme gives the non-denial protection. Alternatively, the signature of the customer does not disclose the secret information. The section below gives more details.

6. SCHEME ANALYSIS

In this section, we will show that the proposed scheme gives robust privacy protection for customers, and non-denial protection, and then study the security of the proposed scheme against other passive and active attacks.

6.1 Anonymity Analysis

The proposed scheme provides the anonymity of customers by using the partial blind signature and anonymous one-time public key. As the one-time public key is embedded into the blind document of the partial blind signature, and the contents of the document u are the same as the other e-coin, the bank and merchant cannot trace an identity of owner of e-coin if the customer employs e-coin later, that is the bank and merchant cannot know who buys the e-goods using the e-coin. This gives unlinkability characteristic inherent to the partial blind signature scheme. Also, because the e-coin is unlikable with the owner identity, the bank knows nothing regarding the customer except how much funds the customer exchanges for e-coin. Alternatively, as the merchant only will have the record document regarding the e-coin, it will also know no more concerning its customers, as will any outsider. Therefore, it provides the customers robust privacy protection.

6.2 Non-denial analysis

The proposed scheme gives non-denial protection in every step of the protocols with the signatures.

1. In the online shopping protocol, the document passed to the merchant is also signed with the secret key of the e-coin. Because just the owner of the e-coin has the secret key, the owner cannot refute his act when he signed the document. Alternatively, this also makes the e-coin safer because other entities cannot spend the e-coin without the secret key. Also, as mentioned in the above anonymity analysis, this signature does not reveal the identity of the owner of the e-coin because the one-time public key does not contain any data regarding the identity of the owner, and also is embedded in the blind document in the e-coin issue protocol.
2. In the e-coin issue protocol, the document that a customer passes to the bank is signed with the customer certificate. When a customer refutes this act, the bank can illustrate the customer signature to the Court. Alternatively, when the customer cannot perform this, the bank also cannot charge the customer because it cannot provide an evidence that is signature to demonstrate it.

6.3 Security Analysis

Information transmitted over e-lines is vulnerable to passive attack which threatens secrecy, and to active attack, which threatens authenticity [15]. So, in this paper we will look into the security of the proposed scheme for anti-passive and anti-active attacks.

1. Passive Attacks

In the proposed scheme, each document passed to the determined receiver is protected by the TLS channel. As a result, a hacker other than the determined receiver cannot disclose document contents because the hacker knows nothing regarding these contents. Alternatively, in the e-coin issue protocol, as the one-time public key (e_t, n_t) is embedded in the blind document $b \equiv (k^{e_B * u} * h(e_t \,||\, n_t) \bmod n_B)$, the bank also cannot know r and $h(e_t \,||\, n_t)$, that is the bank cannot easily guess who owns the one-time public key.

2. Active Attacks

The proposed scheme also gives protection for anti-respond and for arbitrary changes attacks. Using the time stamp in every document, the receiver can certainly determine a replayed document. Also, when a certain hacker wants to modify the document or imitate the customer, the bank and the merchant, the determined receiver can certainly discover by checking the signature because each document passed to the receiver has been hashed, and the hashing result has been signed, that is other entities cannot modify or make the document without the secret key.

7. CONCLUSION

In this paper, we introduced a new e-payment scheme with a robust privacy and non-denial property. This proposed scheme has some advantages over conventionally e-payment schemes such as providing a robust privacy protection for customers, adding a non-denial property, protecting the customer, bank and merchant from over-spending, loss, abuse, and theft of the e-coin and can be employed with the TLS channel.

8. REFERENCES

[1] Wen-Shenq Juang, "A practical Anonymous Off-line Multi-authority Payment Scheme", Electronic Commerce Research and Applications, Volume 4, No.3, pp. 240-249, Summer 2005.

[2] Chang and Lai, "A Flexible Date-attachment Scheme on E-cash", Computers and Security, pp. 160-166, 2003.

[3] Chaum D., "Blind Signature for Untraceable Payments", Advances in Cryptology-Crypto'82, pp. 199-203, 1983.

[4] Ziba Eslami, and Mehdi Talebi, "A New Untraceable Off-line Electronic Cash System", Journal of Electronic Commerce Research and Applications, Volume 10, Issue 1, January 2011, Elsevier Science Publishers B. V. Amsterdam, The Netherlands.

[5] Liu J.,. We V., and Wong S., "Recoverable and Untraceable E-cash", EUROCON'2001, Trends in communications, International Conference, Volume 1, July 2001.

[6] Katsuyuki Takashima, "Scaling Security of Elliptic Curves with Fast Pairing Using Efficient Endomorphism", SCIS 2006, Hiroshima., IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume E90-A, No.1, pp.152-159, January 2007.

[7] Chun-I Fan, "Ownership-attached Un-blinding of Blind Signatures for Untraceable Electronic Cash", Information Sciences: An International Journal, Volume 176, No.3, pp. 263-284, February 2006.

[8] Susan Hohenberger, and Ronald L. Rivest, "Advances in Signatures, Encryption, and E-cash from Bilinear Groups", Massachusetts Institute of Technology, Cambridge, MA, 2006.

[9] Yu P., and Lei C., "An User Efficient Fair E-cash Scheme with Anonymous Certificates", Electronic and Electronic Technology, TENCON, Proceedings of IEEE Region 10 International Conference, Volume 1, August 2001.

[10] Chang-Ji Wang, Yong Tang, and Qing Li, "ID-based Fair Off-line Electronic Cash System with Multiple Banks", Journal of Computer Science and Technology, Volume 22, No.3, pp. 487-493, May 2007.

[11] Isabelle Simplot-Ryl, Issa Traore, and Patricia Everaere, "Distributed Architectures for Electronic Cash Schemes: A Survey", International Journal of Parallel, Emergent and Distributed Systems, Volume24, No. 3, pp. 243-271, June 2009.

[12] Rivest R., Shamir A., and Adleman L., "A Method For Obtaining Digital Signature and Public-key Cryptosystems", Communication of ACM, Volume 21, No. 2, pp. 120-126, February 1978.

[13] FIPS PUB 180-2, 2004, "Secure Hash Standard, National Institute of Standards and Technology", US Department of Commerce, 2004.

[14] Network Working Group, "The TSL Protocol Version 1.2. RFC 5246 (Proposed Standard)", August 2008.

[15] Tianjie Cao, Dongdai Lin, and Rui Xue, "A randomized RSA-based Partially Blind Signature Scheme for Electronic Cash", Computers and Security, pp. 44-49, 2005.