

An Traceable Electronic Cash Model Based on Group Signature¹

Chaoqin Lei, Weidong Kou, Kai Fan and Wei Fan
The State Key Laboratory of Integrated Service Networks
Xidian University Xi'an, P. R. China

Abstract - *With the development of e-commerce, choosing a proper electronic payment method has become more and more important. Competing with other payment methods on the Internet, electronic cash has much more attractive properties, such as anonymity and off-line payment, and is generally considered as an ideal electronic payment method. However, the traceability of the customer or the cash in case of double-spending or other disputes is always a difficult problem to solve. In this paper, we will focus on the problem of traceability in the electronic cash model. We propose a new electronic cash model based on group signature. In our model, traceability can be easily realized using the special property of the group signature.*

Keywords: Electronic Cash Traceability Group Signature Blind Signature

1 Introduction

The e-commerce on the Internet is currently witnessing an explosive growth. To develop a proper electronic payment method is of considerable importance. Since the concept of electronic cash was first proposed by D.chaum [1,2], much research [3,4,5] has been performed in the area of off-line electronic cash system and a great deal of electronic cash schemes have been proposed. That is out of the reason that of various electronic payment methods, electronic cash is a real one. Except for the basic security property, electronic cash has many other special properties such as offline property, anonymity and so on. To some extent it is the same as the paper cash. However, the complete anonymity in electronic cash system may lead to many crimes such as money double-spending, laundering and blackmailing from which criminals can easily get away without leaving any trace. Therefore, a practically electronic-cash system should be only anonymous for legitimate users. The bank cannot link to the legitimate users, but it will identify the criminals.

As a result, to be widely acceptable and therefore successful, electronic cash systems will ultimately have to strike a balance between anonymity and traceability [6]. In this letter, we propose an electronic cash model based on group signature. In our model the anonymity of the customers is also based on the traditional method - blind signature. We use group signature to realize traceability in case of double-spending or other disputes.

The rest of this paper is organized as follows: the next section provides the definition of group signature and its properties. Section 3 presents the new electronic cash model based on the group signature. Section 4 proposes a specific electronic cash System and in section 5 we discuss our new model. Finally, our works are concluded in section 6.

2 Group Signature

Group signatures were introduced by Chaum and Heijst[7] in 1991. This type of digital signatures allows the registered group member to produce a digital signature on a message; any one can verify the digital signature but

¹ This work was supported by the NSFC Grant 90304008, Graduate Innovation Fund of Xidian University (05017), the CUDSFC 20040701001 and Graduate Innovation Fund of Xidian University (05019).

he/she does not know the identity of the signer. The group manager has some auxiliary information, which can be used to discover the identity of the signer.

The definition and properties of group signatures are introduced as follows.

Definition: A group signature scheme is a digital signature scheme comprising the following procedures:

Setup: An algorithm can generate the initial group public key and a group manager's secret key.

Join: A protocol makes the user become a new group member. The output of this step is a membership certificate and a membership secret key for each group member.

Sign: An algorithm outputs group signature of m after inputting a group public key, a membership certificate, a membership secret key, and a message m .

Verify: An algorithm indicates the correctness of an alleged group signature of a message with respect to a group public key.

Open: An algorithm determines the identity of the signer on inputting a message, a valid group signature on it, a group public key and a group manager's secret key.

A group signature scheme has the following properties:

Unforgeability: Only the group members are able to sign messages on behalf of the group.

Anonymity: Given a valid signature, identifying the actual signer is computationally hard without knowing the group manager's secret key.

Unlinkability: It is computationally hard for anyone except the group manager to decide whether two different signatures are signed by the same group member.

Exculpability: Neither a group member nor the group manager is able to sign on behalf of other group members.

Traceability: The group manager is always able to open a signature and identify the actual signer.

3 The new electronic cash model based on group signature

In this section, the payment system is presented. In section 4 appropriate mathematical methods will be chosen to realize the system that are treated here only generically.

Our electronic model consists of four entities: the bank, the customers, the shops and TTP (trust third party). Their relations are as follows:

- TTP is the group manager, and the customer is the group member. Before the initiation of any transaction, the customer should register at TTP. After the registration, the customer will obtain a valid membership certificate and a secret key, while the TTP will update its customer database with the customer's identity information.
- The bank is responsible for issuing the valid electronic cash. In order to protect the privacy of the customers, the bank use the blind signature technique to sign the cash message.
- The customer spends electronic cash by participating in a payment protocol with a shop over an anonymous channel. The shop performs a deposit protocol with the bank to deposit the customer's cash into his account.

A complete transaction procedure is as follows.

- *SETUP* The customer registers at TTP and obtain a valid membership certificate and a secret key.
- *Opening an Account* Both the customer and the shop should open an account in the bank. And the customer should deposit some cash in that account. Then later they can withdraw electronic cash from their account.
- *Withdrawal* The customer prepares the withdrawal message for the bank to sign. This message is in a

fixed form, which is determined by the bank, and it contains at least the amount of the currency. Before send the message to the bank, the customer should sign it with his private membership key. In order to protect the anonymity of the customer, the customer blinds the signed message and then sends it to the bank. The bank signs the message using the blind signature technique. Then the bank deducts the correct amount from the customer's account.

- *Payment* With the electronic cash applied from the bank, the customer can buy commodities from the shop on the Internet. After sending the payment message to the shop. The shop can verify the validity of the cash by the bank's signature and the shop can also verify the group signature with the group public key published by TTP.
- *Deposit* The shop deposits the received cash by sending the cash message to the bank. It is assumed that the bank maintains its database. Using this database, it keeps the received cash, which has been deposited yet. First the bank verifies the bank's signature and the group signature as the shop. If both signatures are holds, the bank searches its database to find out if the same cash has been stored before. If the same cash is not found, the bank accepts the cash and credits the correct amount to the shop's account. Otherwise, it means that the cash is double-spent. Cooperating with TTP, the bank can open the customer's group signature and discover the identity of the double-spender. Then the bank can deduct the correct amount from the customer's account again and credit the correct amount to the shop's account.

4 Proposed Electronic Cash Systems

In this section, we will provide an instance of the application of the electronic payment model proposed in section 3.

4.1 The SETUP of the scheme

Here we use the group signature scheme introduced in [8]. In our system, the customer is the group member, and TTP is the group manager or group authority. The specific use of group signature scheme in [8] is as follows.

Let p and q be two large primes such that $q \mid p - 1$. Let g be a generator with order q in $GF(p)$. Each customer U_i chooses the secret key x_i , and computes the public key $y_i = g^{x_i} \bmod p$. Let x_T be the secret key of TTP. The public key is $y_T = g^{x_T} \bmod p$. For each customer U_i , TTP computes $r_i = g^{-k_i} \cdot y_i^{k_i} \bmod p$ and $s_i = k_i - r_i \cdot x_T \bmod q$, where k_i is a random number in Z_q^* . Then TTP sends (r_i, s_i) to the customer U_i secretly. After receiving (r_i, s_i) , U_i may verify the information by checking the equation $g^{s_i} \cdot y_T^{r_i} \cdot r_i \equiv (g^{s_i} \cdot y_T^{r_i})^{x_i} \bmod p$. Then the customer keeps (r_i, s_i, x_i) as his/her membership key.

4.2 The Withdrawal Protocol

The withdrawal protocol contains three steps:

Step 1: The customer generates a message m for the bank to sign, and this message represents electronic cash. This message is in a fixed form, which is determined by the bank, and it contains at least the amount of the currency.

Step 2: U_i signs the message m with his private membership key. U_i chooses two random integers a and

b in Z_q^* and computes $\{A, B, C, D, E\}$ using (r_i, s_i) as

$$A = r_i^a \bmod p \quad (1)$$

$$B = s_i - b \bmod q \quad (2)$$

$$C = r_i \cdot a \bmod q \quad (3)$$

$$D = g^a \bmod p \quad (4)$$

$$E = g^{a \cdot b} \bmod p \quad (5)$$

U_i computes $\alpha_i = D^B \cdot y_T^C \cdot E \bmod p = g^{a \cdot k_i} \bmod p$ and $R = \alpha_i^t \bmod p$, where t is a random number in Z_q^* . Then, U_i solves the congruence relation $h(m) = R \cdot x_i + t \cdot S \bmod q$ for the parameter S , where

$h()$ is a one-to-one one-way hash function. The customer's group signature for the message m is

$$\{R, S, h(m), A, B, C, D, E\}$$

Step3: In order to protect the anonymity of the customer, the bank sign the cash message using the RSA blind signature technique [9]. The bank's public key is e and private key is d . The cash message is $M = \{R, S, h(m), A, B, C, D, E\} \parallel m$. The customer U_i chooses blind factor k and computes

$$Y = Mk^e \bmod n. \text{ Then } U_i \text{ send } Y \text{ to the bank. The bank signs } Y: Y^d = (Mk^e)^d \bmod n \text{ and sends it}$$

back to U_i . U_i removes the blind factor k to get the valid electronic cash $W = M^d \bmod n$. Practically, we should use cut-and-choose technique [10] here to obtain the blind signature of the bank. To simplify the procedure, we directly use blind signature, because the key point in this paper is not on the anonymity.

4.3 The payment protocol

If the customer U_i buys some commodities from a shop V , he will send the electronic cash W to V . Receiving W, V will verify its validity by the following steps:

Step 1: Using the public key e of the bank, V computes $W^e = M \bmod n$. Then he obtains $M = \{R, S, h(m), A, B, C, D, E\} \parallel m$. From m , V can determine whether the bank's signature is correct.

Step 2: V verifies the customer's group signature as follows:

(i) Compute $\alpha_i = D^B \cdot y_T^C \cdot E \bmod p = g^{a \cdot k_i} \bmod p$

(ii) Compute $DH_i = \alpha_i \cdot A \bmod p = g^{a \cdot k_i \cdot x_i} \bmod p$

(iii) Check the congruence relation $\alpha_i^{h(m)} = DH_i^R \cdot R^S \bmod p$

(iv) If the above equation holds, then the group signature is verified.

If both the bank's signature and the group signature hold, V can accept the payment.

4.4 The deposit protocol

In this protocol the shop sends the electronic cash W to the bank. The bank first verifies the validity of the cash as V . Then if both the bank's signature and the group signature hold, the bank searches its database to find out if the same cash has been used before. If it has not been used, the bank accepts the cash and credits the correct amount to the shop's account. If the same cash has been stored in the database, it indicates that double spending takes places. We will deal with this situation in detail in the following passage.

5 System Issues

Using the group signature technique, our proposed model solves the traceability of the customer or the cash in case of double-spending or other disputes successfully. By the following analysis, we can see this property clearly.

If a customer tries to double spend the same cash. We will now prove that the bank and TTP can cooperate to discover the identity of the double-spending customer. Since the payment message M has the group signature of the customer, TTP as the group manager can identifies the signer. Because TTP has access to (r_i, s_i, k_i) of each member U_i , TTP can acquire (r_i, s_i, k_i) of U_i satisfying the equation $D^B \cdot y_T^C \cdot E \equiv D^{k_i} \pmod{p}$, for $i = 1, \dots, n$, where n is the number of group members. So TTP can determine the signer. That is to say, the bank can determine the double-spending customer. Then the bank can deduct the correct amount from the customer's account again and credit the correct amount to the shop's account.

If the customer is blackmailed to give some person some amount of money. When the criminal tries to deposit the received money in the bank, the customer, the bank and TTP can cooperate to discover the identity of the criminal. The proving procession is as above.

Except for the traceability, our model can also satisfy the following two properties:

- *Anonymity*
We use the traditional method — blind signature technique to protect the anonymity of the customer.
- *Unforgeability*
Since the group signature satisfies the property of unforgeability and the cash message is signed by the group signature, there is no doubt that the electronic cash in our model can satisfy the property of unforgeability.

6 Conclusions

In this paper, we have proposed an efficient offline electronic cash scheme. It satisfies all the basic requirements for the electronic payment scheme such as cash unforgeability, cash anonymity etc. Particularly, based on the group signature technique, our scheme has easily realized traceability in cases of double-spending and other disputes.

However, although our model can discover the identity of the double-spending person after the double-spending having taken place based on the group signature, we could not prevent double-spending beforehand. In an offline system, this is a difficult problem to solve. We have to do some further study about it.

References

- [1] Chaum D. "Blind signatures for untraceable payments," Advances in Cryptology, ProcofCrypto 82[C]. SantaBarbara, California: Springer Verlag, pp.199~203, 1983.
- [2] Chaum D, Fiat A, Naor M. "Untraceable electronic cash," In: Goldwasser S, ed. Proceedings of the Crypto'88. LNCS 403, New York: Springer-Verlag, pp.319~327, 1990.
- [3] L.A.M.Schoenmakers, "An efficient electronic payment system withstanding parallel attacks", CWZ Technical Report CSX9.522, 1995.
- [4] Y.Yacobi, "An efficient off-line cash", Advances of Cryptology-Asiaclyst'94 Proceedings, Springer-Verlag, 1994.
- [5] W. Qiu, K. Chen, and D. Gu, "A new off-line privacy protecting ecash system with revokable anonymity", Proceedings of ISC 2002, pp177-190, 2002.
- [6] Peter S. Gemmell "Traceable e-cash Spectrum", IEEE Volume 34, Issue 2, Page(s):35 - 37 Digital Object Identifier 10.1109/6.570827, Feb. 1997
- [7] D. Chaum and E. van Heijst. "Group signature,". Advances in Cryptology–Eurocrypt'91, Lecture Notes in Computer Science, Springer-Verlag, pages 257–265, 1991.
- [8] Yuh-Min Tseng and Jim-Ke Jan, "Improved group signature scheme based on discrete logarithm problem," Electronics Letters Volume 35, Issue 16, Page(s): 1324 – 1325, 5 Aug. 1999.
- [9] Yuming wang and Jianwei liu, "Communication Network Security—Theory and technique", Xidian university press, pages 285-287, 2002.
- [10] Chan A, Frankel Y, and Tsiounis Y, "An efficient off-line electronic cash scheme as secure as RSA," Research report nu-ccs-96-03, Northeastern University, Boston, Massachusetts, 1995.