Electronic Cash System Based on Group Signatures With Revokable Anonymity

Hyungki Choi, Fangguo Zhang, and Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

Abstract

After Lysyanskaya and Ramzan proposed group blind signatures in FC '98, there have been several electronic cash system proposed using group blind signatures. In this paper, we propose a new electronic cash system based on group signature using the group signature scheme proposed by Ateniese, Camenish, Joye, and Tsudik [2] which allows our system to be unlikable and double spending resistant. Furthermore, comparing with Fair Electronic Cash (E-Cash) system proposed by Maitland and Boyd [3], our system provides owner and coin tracing to prevent perfect crimes [8] such as blackmailing and money laundering.

I. Introduction

Since Chaum [1] introduced the blind signature scheme, which allows to design anonymous payment systems, many E-Cash systems providing unforgeability, anonymity, and offline have been proposed in the recent years. The problem was unconditional privacy protecting systems might be misused for blackmailing or money laundering. Therefore, additional solution, a trustee or a set of trustees can selectively revoke the anonymity of the participants involved in suspicious transactions, was incorporated in the electronic payment system.

After Chaum and Van Heyst introduced the concept of group signature schemes at Eurocrypt '91, several applications using group signatures have been proposed. Among properties of group signatures, especially anonymity, unlikability, and revocation got the attention for applying to E-Cash system. Lysyanskaya and Ramzan [6] firstly introduced the concept of group blind signature schemes. Group blind signatures combines the properties of both blind signature and group signatures. In their schemes, multiple banks can securely apply anonymity and untraceable E-Cash. In their system, only designated entity can identify the bank who issued a given coin. Recently, Qiu, Chen, and Gu [4] proposed a new offline privacy protecting E-Cash system with revokable anonymity using group signatures.

In their system, they showed the coin tracing and owner tracing is possible, the anonymity of the system can be revokable by an offline trusted third authority, and the system is untraceable, unlikable, and double-spending resistant. However, we found that during the withdrawal protocol Bank can identify the user who spent the coin. Thus, the anonymity could not be guaranteed.

1. Our Approach

In this paper, we consider privacy protecting E-Cash system based on group signatures. In our system, we used group signature scheme proposed by Atniese, Camenish, Joye, and Tsudik [2] which allows our system to provide anonymity in normal cases, designated entity can revoke the identity of the user, and the system is unlikable and double-spending resistant. Furthermore, comparing with Fair E-Cash system proposed by Maitland and Boyd [3], our system provide owner and coin tracing to prevent perfect crimes [8] such as blackmailing and money laudering.

2. Organization of the Paper

In Section 2, we define the notations and introduce our assumptions used in the paper. In Section 3, we proposed our scheme. Finally, we conclude our paper in Section 4 with our concluding remark.

II. Preliminaries

In this section, we describe some basic notations we used throughout the paper, and cryptographic assumptions necessary in the design of our system.

1. Basic Notations

The symbol || we denote the concatenation of two strings. The notation $x \in_R Z$ means that x is chosen uniformly at random from the set Z. The notation $x \stackrel{?}{=} y$ means that the party must check whether x is equal to y. H will denote a collision resistant hash function.

2. Number Theoretic Assumptions

We describe the cryptographic assumptions necessary in the following construction of E-cash system. We omit the building blocks of the group signature scheme in [2]. Those building blocks are proof systems for the group signature schemes. For further details we refer the readers to [2]. Let l_g be a security parameter and G be the group of order with length l_g factored into two primes of length $(l_g - 2)/2$.

Problem 1. (Strong-RSA Problem) *Given* G, $z \in G$, *and* $M \subset M(G, z)$ *with* $|M| = O(l_g)$, *find a pair* $(u, e) \in G \times Z$ *such that* $u^e = z$, $e \in \{2_1^l, 2^{\tilde{l}}, \cdots, 2_1^l + 2^{\tilde{1}}\}$, *and* $(u, e) \notin M$.

Assumption 1. (Strong-RSA Assumption) *There exists a probablistic algorithm* T *such that for all probabilistic polynomial -time Algorithms* A, *all polynomials* $p(\cdot)$, *the probability that* A *can solve the Strong-RSA Problem is negligible.*

In addition to Strong-RSA Assumption, Atniese, Camenish, Joye, and Tsudik's group signature scheme relies on the Decisional Diffie-Hellman assumption.

Assumption 2. (DDH Assumption) *Let* $G = \langle g \rangle$ *be a cyclic group generated by* g *of order* $u = \#G$ *with* $\lceil \log_2(u) \rceil = l_g$. *Given* $T = \{g^x, g^y, g^z\}$ *in* G^3, *it is hard to decide whether* T *is a Diffie-Hellman triplet* $T = (g^x, g^y, g^{xy})$ *or a random triplet.*

III. Our Proposed Schemes

As we stated earlier, our scheme is similar to Maitland and Boyd [3] scheme that is directly applied group signature schemes proposed by Atniese, Camenish, Joye, and Tsudik [2]. However, our scheme can provide tracing protocols which allows us to execute coin or owner tracing.

1. Setup

Let $\varepsilon > 1$, k, and l_p be security parameters. Let $\lambda_1, \lambda_2, \gamma_1$, and γ_2 denote lengths satisfying $\lambda_1 > \varepsilon(\lambda_2 + k) + 2$, $\lambda_2 > 4l_p$, $\gamma_1 > \varepsilon(\gamma_2 + k) + 2$, and $\gamma_2 > \lambda_1 + 2$. Define integral ranges $\Lambda = [2^{\lambda_1} - 2^{\lambda_2}, 2^{\lambda_1} + 2^{\lambda_2}]$ and $\Gamma = [2^{\gamma_1} - 2^{\gamma_2}, 2^{\gamma_1} + 2^{\gamma_2}]$. Then, let H be a collision-resistant hash function $H: \{0,1\}^* \rightarrow \{0,1\}^k$. (The parameter ε controls the tightness of the statistical zero-knowledgeness and the parameter l_p sets the size of the modulus to use.)

Group Manager(GM)

Select random secret l_p-bit primes p' and q' such that $p = 2p' + 1$ and $q = 2q' + 1$ are prime. Set the modulus $n = pq$. Choose random elements $a, a_0, g, h \in_R QR(n)$ (of order $p'q'$). The group public key is $\nu = (n, a, a_0, g, h)$ and the corresponding secret key (known only to GM) is $S = (p', q', x)$.

Revocation Manager(RM)

Choose a random secret element $x \in_R Z^*_{p'q'}$ and set $y = g^x \bmod n$.

The Bank

The bank sets appropriate parameters to be used in blind signature scheme for issuing *Auth*.

2. The Customer Join

Any customer who wishes to join the group has to interact with GM and obtain membership certificate to generate the group signature.

- ·lect a private key $x_i \in \Lambda$ only known to user and the associated public key is $C_2 = a^{x_i} \bmod n$ with $C_2 \in Q_n$.
- membership certificate is $[A_i, e_i]$ where e_i is a random prime chosen by GM such that $e_i \in_R \Gamma$ and A_i has been computed by the GM as $A_i = (C_2 a_0)^{1/e_i} \bmod n$.
- ·M makes a new entry in the

membership table for the certificate $[A_i, e_i]$.

3. Withdrawal Protocol

This protocol is between the customer and the bank for the customer to obtain $Auth$ required during payment and deposit protocols from the bank. The customer and the bank complete following procedures:

- ;enerate a random value $w \in_R \{0,1\}^{2l_p}$ and compute $T_1 = A_i y^w \bmod n$,

  $T_2 = g^w \bmod n$, and $T_3 = g^{e_i} h^w \bmod n$
- ;hoose randomly

$r_1 \in_R \pm\{0,1\}^{\varepsilon(\gamma_2 + k)}$, $r_2 \in_R \pm\{0,1\}^{\varepsilon(\lambda_2 + k)}$,

$r_3 \in_R \pm\{0,1\}^{\varepsilon(\gamma_1 + 2l_p, k+1)}$, and $r_4 = \in_R \pm\{0,1\}^{\varepsilon(\lambda_2 + k)}$

Then compute

$d_1 = T_1^{r_1} / (a^{r_2} y^{r_3}) \bmod n, d_2 = T_2^{r_1} / g^{r_3} \bmod n$

$d_3 = g^{r_4} \bmod n$, and $d_4 = g^{r_3} h^{r_4} \bmod n$

- The customer gets $Auth$ by a blind signature protocol. The messages can be chosen from the set $\{T_1, T_2, T_3, d_1, d_2, d_3, d_4\}$. If $Auth$ is signed on the message (T_1, T_2), then the customer's identity can be bound to $Auth$ because $a^{x_i} a_0$ is the value whicht is ElGamal type in (T_1, T_2).

4. Payment Protocol

In this protocol, the customer (group member) signs the payment information m with the customer's membership certificate. To generate the group signature, the customer compute the challenge and response phase as follows:

- ;hallange Phase: Calculate

$c = H(g \| h \| y \| a_0 \| a \| T_1 \| T_2 \| T_3 \| d_1 \| d_2 \| d_3 \| d_4 \| m)$

- ;esponse Phase: Compute

$s_1 = r_1 - c(e_i - 2^{\gamma_1})$, $s_2 = r_2 - c(x_i - 2^{\lambda_1})$,

$s_3 = r_3 - c e_i w$, $s_4 = r_4 - cw$. (all in Z)

Therefore, the group signature is $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$.

- The customer sends the group signature and the $Auth$.
- The merchant verifies the group signature as follows:

  Compute :

  $c' = H(g \| h \| y \| a_0 \| a \| T_1 \| T_2 \| T_3 \|$

  $a_0^c T_1^{s_1 - c2^{\gamma_1}} / (a^{s_2 - c2^{\lambda_1}} y^{s_3}) \bmod n \|$

  $T_2^{s_1 - c2^{\gamma_1}} / g^{s_3} \bmod n \| T_2^c g^{s_3} \bmod n \|$

  $T_3^c g^{s_1 - c2^{\gamma_1}} h^{s_4} \bmod n \| m)$

  Accept the signature if and only if

$c \overset{?}{=} c'$, and $s_1 \in \pm\{0,1\}^{\varepsilon(\gamma_2 + k)+1}$,

$s_2 \in \pm\{0,1\}^{\varepsilon(\lambda_2 + k)+1}$, $s_3 \in \pm\{0,1\}^{\varepsilon(\lambda_1 + 2l_p + k + 1)+1}$,

$s_4 \in \pm\{0,1\}^{\varepsilon(2l_p + k)+1}$

5. Deposit Protocol

This protocol is similar to Payment

protocol. The only difference is who involves during the protocol. After verifying the payment by the customer, the merchant sends the group signature and $Auth$ to the bank. Then bank verifies the group signature and $Auth$ using the same procedures as the merchant. If the bank verifies them both, the bank checks whether it is already used or not (double-spending). If it hasn't been used before, the bank accepts the payment as valid, add it to the list such as $[m, (c, s_1, s_2, s_3, T_1, T_2, T_3), Auth]$ which used for the validity of the payment later. If it is rejected, then the bank sends the information to RM for identifying who issued the payment, and revoking the customer.

6. Identity Revocation

In case there is a problem occurred, we can open a signature and reveal the identity of the customers who generate the signature, Revocation Manager (RM) does the following procedure to recover the identity of the signature.

- ıeck the signature's validity as per the merchant's verification procedure.
- ecover A_i (and thus the identity of C_i) as $A_i = T_1 / T_2^x \mod n$.
- enerate a proof that $\log_g y = \log_{T_2}(T_1/A_i \mod n)$.

7. Tracing Protocol

In this protocol, it consists of owner tracing protocol and coin tracing protocol. The details of these protocols as follows:

Owner Tracing

In some cases, the RM (acts as trusted third party) can expose the identity of the owner in the E-cash with the information received during the deposit protocol.

- Γhe bank sends T_1, and T_2 during the deposit protocol to the RM.
- ℷM computes the license information $A_i := T_1 / T_2^x \bmod n$,
- earch through the list to get the user's identity corresponding to A_i, and returns the identity to the bank.

The identity of specific E-cash can be revealed and can prevent like money laundering [8].

Coin Tracing

During the withdrawal protocol, RM can compute the corresponding E-cash and trace them. When blackmailing occurs, the following procedure will trace the coin and freezes it.

- `he customer sends identity A_i to the bank.
- `he bank then searches through the list that has been maintained for accepting or rejecting the payment.

Since all the payment is stored in the form $[m, (c, s_1, s_2, s_3, T_1, T_2, T_3), Auth]$, given the customer identity A_i and payment information m, the bank can freeze the corresponding E-cash.

IV. Concluding Remarks

We proposed the modified E-cash system based on group signature with revokable anonymity. Our protocol allows the owner and coin tracing. Additionally, the properties of group signatures are providing unlikability, anonymity, and revocation.

As a further work, we need to provide more rigorous security proof in the provable sense especially for the tracing protocols. Furthermore, the dynamical customer deletion protocol is to be provided.

References

[1]. D. Chaum, "Blind Signatures for Untraceable Payments", Crypto 1982, pp. 199-203, Plenum Press, 1983.

[2]. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme", Crypto 2000, pp. 255-270, Plenum Press, 2000.

[3]. G. Maitland, and C. Boyd, "Fair Electronic Cash Based on a Group Signature Scheme", ICICS 2001, LNCS 2229, pp. 461-465, Springer-Verlag 2001.

[4]. W. Qiu, K. Chen, and D. Gu, "A New Offline Privacy Protecting E-Cash System with Revokable Anonymity", ISC 2002, LNCS 2433, pp. 177-190, Springer -Verlag 2002.

[5] A. de Solages, and J. Traore, "An Efficient Fair Offline Electronic Cash System with Extensions to Checks and Wallets with Observers", FC 1998, LNCS 1465, pp. 275-295, Springer-Verlag 1998.

[6] A. Lysyanskaya, and Z. Ramzan, "Group Blind Digital Signatures: A Scalable Solution to Electronic Cash", FC 1998, LNCS 1465, pp. 184-197, Springer-Verlag 1998.

[7] S. von Solms, and D. Naccache, "Blind Signatures and Perfect Crimes", Computers and Security, 11:581-583, 1992.

[8] D. Coppersmith, "Finding a Small Root of a Bivariatre Integer Equation; Factoringwith High Bits Known", Eurocrypt 1996, LNCS 1070, pp. 178-189, Springer -Verlag, 1996.