Journal of Information Security, **2012, 3, 177-183**
http://dx.doi.org/10.4236/jis.2012.32021 Published Online April 2012 (http://www.SciRP.org/journal/jis)

A Fair Electronic Cash System with Identity-Based Group Signature Scheme

Khalid. O. Elaalim[1,2], Shoubao Yang[2]
[1]Department of Statistic and Computer Science, Faculty of Applied Sciences, Red Sea University, Port Sudan, Sudan
[2]School of Computer Science and Technology, University of Science and Technology of China, Hefei, China
Email: Osman64@mail.ustc.edu.cn, syang@ustc.edu.cn

Received November 10, 2011; revised February 15, 2012; accepted March 24, 2012

ABSTRACT

A fair electronic cash system is a system that allows customers to make payments anonymously. Furthermore the trusted third party can revoke the anonymity when the customers did illegal transactions. In this paper, a new fair electronic cash system based on group signature scheme by using elliptic curve cryptography is proposed, which satisfies properties of secure group signature scheme (correctness, unforgeability, etc.). Moreover, our electronic cash contains group members (users, merchants and banks) and trusted third party which is acted by central bank as group manager.

Keywords: Elliptic Curve; Bilinear Pairings; Group Signature; Electronic Cash; Trusted Third Party; Tracing Protocol

1. Introduction

The first group signature scheme was proposed by David Chaum and van-Heyst in 1991 [1]. Group signature schemes allow a group member to sign messages on behalf of the group. Such signatures must be anonymous and unlinkable but, whenever needed, a designated group manager can reveal the identity of the signer [1-3]. Shamir proposed an identity based signature to simplify key management procedures of certificate-based public key infrastructures (PKI) [4]. A lot of identity based group signatures have been proposed after Shamir [5-8]. Many group signatures scheme have been proposed recently, but several of them were suggested application electronic cash. [9-11] introduced group signatures into electronic cash schemes which are anonymous and unlinkability.

Main Contribution

In this paper, identity based group signature scheme is proposed, which satisfies the electronic cash based on group signatures. Furthermore it provides to keep group member anonymous and unlinkability if he does not cheat. In this scheme we use trusted third party, which acts the group manager. The user is a group member who should register at TTP before start any interaction with the bank.

The rest of this paper is as follows: in the next section, we introduce some preliminaries work. Our identity based group signature is presented in Section 3. In Section 4, we propose a new electronic cash system. We explain security analysis of our scheme in Section 5. Final section concludes.

2. Preliminaries

In this section, we will describe the definition and properties of elliptic curve cryptography, bilinear pairings, Gap Diffie-Hellman Group and Group signature models.

2.1. Elliptic Curve Cryptography

2.1.1. Definition1: Addition Rules of Elliptic Curve [12]

It is possible to define an addition rule to add points on E. The addition rule is specified as follows:

Identity: $P+O=O+P=P \quad \forall P \in E(Z_q)$

Negation: if $P=(x,y) \in E(Z_q)$ then $P+Q=0$ where $Q=(x,-y) \in E(Z_q)$ and denoted by $-P$.

Note: $O=-O$

Add two points with different x-coordinates:

Let $P=(x_1,y_1)$ *and* $Q=(x_2,y_2) \in E(Z_q)$ be two points such that $x_1 \neq x_2$ then $P+Q=R=(x_3,y_3)$ as shown in **Figure 1**, where

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2$$

$$y_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)-y_1$$

Add a point to itself (double a point) with $x_1 \neq 0$:

Let $P=(x_1,y_1) \in E(Z_q)$, then $P+P=2P=(x_3,y_3)$, where:

$$x_3=\left((3x^2+a)/2y\right)^2-2x_1$$

$$y_3=\left((3x^2+a)/2y\right)^2(x_1-x_3)-y_1$$

Copyright © 2012 SciRes.

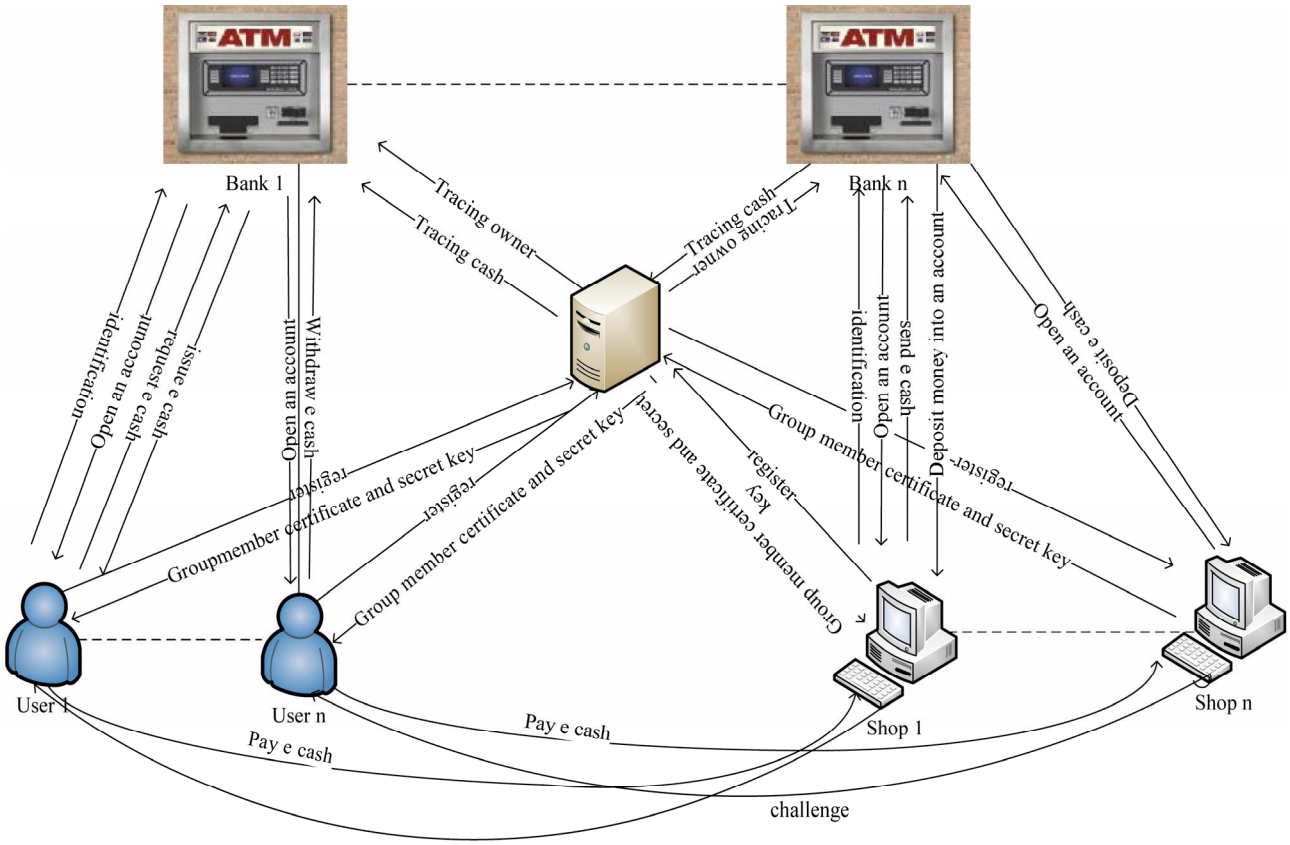

Figure 1. Architecture of our electronic cash scheme.

2.1.2. Definition 2 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve E defined over a finite field Z_q, a point $P and Q \in E(Z_q)$ of order n, find the integer $x \in [0, n-1]$ such that $Q = xP$. The integer x is called the discrete logarithm of Q to the base P denoted as $x = \log_P Q$. If x is sufficient large, then it is infeasible to compute it [13].

2.2. Bilinear Pairings

Let G_1 and G_2 be two cyclic groups generates by P, whose order is a prime q, where G_1 is additive groups and G_2 is multiplicative group. A pairing is a function:

$e: G_1 \times G_1 \to G_2$

All pairing will satisfy the following properties:

1) Bilinear: For all $P, Q \in G_1$ and $a, b \in Z_q^*$ then $e(aP, bQ) = e(P, Q)^{ab}$

2) Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$

3) Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

2.3. Gap Diffie-Hellman Group

We first introduce the following problems in G [14].

1) Discrete Logarithm Problem (DLP): if given P and Q, to find $n \in Z_q^*$ from $Q = nP$.

2) Computation Diffie-Hellman Problem (CDHP). Given (P, aP, bP) for $a, b \in Z_q^* / q$, to compute abP.

3) Decisional Diffie-Hellman Problem (DDHP).

Given (P, aP, bP, cP), or $a, b, c \in Z_q^* / q$, to decide whether $\mathrm{c} = ab$.

We call G_1 a GDH group if DDHP can be solved in polynomial time but no polynomial times an algorithm can solve CDHP or DLP with non-negligible advantage within polynomial time.

2.4. Group Signature Model

A group signature scheme is comprised of the following procedures [5]:

1) Setup: An algorithm that generates the group public key and a group master key for the group manager.

2) Extract: A protocol between the group manager and a group member that generates the user's secret key and public key.

3) Sign: A probabilistic algorithm (with inputs as a group public key, a membership secret and a message m) outputs a group signature of m.

4) Verify: An algorithm for establishing the validity of an alleged group signature of a message with respect to the group public key.

Copyright © 2012 SciRes.

5) Reveal: An algorithm that, given a message, a valid group signature on it, a group public key and a group manager's master key, determines the identity of the actual signer.

A secure group signature scheme should satisfy all or part of the properties:

1) Correctness: Group signatures produced by a group member must be valid.

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

3) Anonymity: It is infeasible to find out the group member who signed a message without the group manager's secret key.

4) Unlinkability: Deciding whether two different valid signatures were computed by the same group member is computationally hard.

5) Exculpability: Neither a group member nor the group manager can sign on behalf of other group members.

6) Traceability: The group manager is always able to identify the actual signer for a valid signature in case of disputes.

7) Coalition-resistance: No coalition of members can prevent a group signature from being opened.

3. Our Identity Based Group Signature

In this section we consider ID-based group signature scheme from bilinear pairings, which can be implemented as follows:

3.1. Setup

Setup is a system generation. The group manager executes the following:

Choose p, q, G_1, G_2 as defined in 2.2 and choose $G_3 \in E(Z_q)$ .Select three hash function cryptography H_1, H_2 and H_3 which satisfy $H_1 : \{0,1\}^* \times G_1 \to Z_q^*$ $H_2 : \{0,1\}^* \times G_1 \to G_1$ and $H_3 : \{0,1\}^* \to G_1$ Select $x_t \in Z_q^*$ as secret key.

Compute $P_t = x_t G, P_1 = x_t G_1, P_2 = x_t G_2$ *and* $P_3 = x_t G_{31}$ and publish $(E(Z_q), n, q, G, G_1, G_2, P, P_1, P_2, P_3, H_1)$ as public key.

3.2. Extract

Before the user joins the group, manager should execute this step:

1) Select random number $x_i \in Z_q^*$ as private key.

2) Compute $P_i = x_i G$ as public key.

When the user wants to become the member of group then the user *i* and the group manager can cooperates as follows:

1) The user sends his public key with ID (identification) to the group manager.

2) Group manager select random numbers $v_i \in Z_q^*$ for every member who want become group member.

3) Group manager calculate $sk_i = (v_i + x_t) Q_{ID_i}$ where $Q_{ID_i} = H_1(ID_i, P_i)$ and then sends (v_i, sk_i) to the user as the membership certificate.

3.3. Sign

When the user wants to sign message *m*, the user can do the followings:

The user selects random elements k,x,d,$\alpha, \beta, \gamma, r_1, r_2 \in Z_q^*$ and $M, W \in G_1$, and then calculates the followings:

$A_1 = e(M, P_i)$, $A_2 = e(S_{ID_i}, G)$

$A_4 = e(M, W)$, $A_3 = e(W, G)$

$B_0 = x_i (v_i M + \alpha A_3)$, $U = x_i^{-1} B_0 + kG - \alpha A_3$

$B = e(S_{ID_i}, U)$, $B_1 = kP_i + vxx_i A_2$

$C = x_i^{-1} B_1 + \alpha A_3 - kP_i$, $B_2 = r_1 A_1 + dA_4$

$D = B_2 + r_2 B - dA_4$, $B_3 = r_2 B + \beta W$

$E = B_3 + dA_4 - r_2 B$ $U_1 = P_t + v_i G$

$F = H_2(ID \| U + C + D + W)$

$H = k\alpha dG$ $R = \gamma F + H$

$h = H_1(m \| U + C + D + W + R)$

$S = hk\alpha dP_i + x_i R \bmod p$

The resulting signature on the message *m* is (*U*, *C*, *D*, *W*, *R*, *S*).

3.4. Verify

When the receiver wants to verify the group signature (*U*, *C*, *D*, *W*, *R*, *S*) of the message *m* which is signed by the signer, the receiver first computes $h = H_1(m \| U + C + D + W + R)$ and then verifies $e(S, G) = (hH + R, P_i)$.

3.5. Open

This algorithm is only executed by the group manager. Given valid group signatures the group manager can easily find the identity of the signer. The signer cannot deny his group signatures after group manager presents the followings:

$e(S_{ID_i}, G) = e(Q_{ID_i}, U_1)$

$e(U + C, P_i) e(D + E, G) = e(B_0 + B_1 + B_2 + B_3, G)$

4. Our Electronic Cash System

4.1. Electronic Cash Architecture

In this section, we describe our system architecture and how each protocol of e-cash works. **Figure 1** shows configuration of group signatures, which involves three protocols: withdraw protocol, payment protocol and deposit

Copyright © 2012 SciRes.

protocol. Thus group signatures architecture consists four main parties: Trust Third Party (TTP) acts the group manager; banks, users and shops acts the group member. Their relation between each part with other as follows:

1) Trusted Third Party (TTP) is acting as group manager and the users act group membership. The user should be registering at TTP before start any interaction with the bank. After registration, the user will get a valid membership certificate and a secret key from TTP.

2) The bank issues the valid electronic cash. The bank protects the privacy of the customers, and also uses the blind signature technique to sign the electronic cash.

3) The customer spends electronic cash in a payment protocol with a shop over an anonymous channel.

4) The shop deposits electronic cash that he gets from the user in the payment protocol into his bank account.

4.2. Setup

TTP (Central Bank (CB)) generates and publishes the same system parameters that proposed in Section 3.1.

When the bank i (B_i) registers in CB, they should perform the following steps:

1) B_i selects random number $x_{B_i} \in Z_q^*$ as private key and computes $P_{B_i} = x_{B_i} G$ as public key.

2) B_i sends public key with his identification ID_{B_i} to the CB.

3) The CB does the same in Section 3.2 and sends (sk_{B_i}, v_{B_i}) to B_i as membership certificate.

And also the user $i(u_i)$ and merchant i (M_i) should do the same steps that B_i does when they want to register in CB.

Then the central bank will send the group member ship $(sk_{u_i}, v_{u_i}) and (sk_{M_i}, v_{M_i})$ to u_i *and* M_i respectively.

4.3. Open an Account

Every group member should open an account in any bank he needs it. They need to do as follows:

1) The group member sends $\mathrm{ID_i}$ to the bank B_i.

2) B_i opens an account and sends it to the group member.

4.4. Withdraw Protocol

The withdrawal protocol involves u_i and B_i which the user opens an account in. When legal u_i wants to withdraw electronic cash from his account in the bank, the user must prove himself to the bank. The withdraw protocol request contains the amount of electronic cash, which is less than or equal the balance. If the amount is greater than balance then the withdraw protocol should be stopped, otherwise, the user and the bank execute the following steps:

1) the user chooses random number $s \in Z_q^*$ and computes $A_1 = s^{-1}(P_{u_i} + P_2) + P_1 \quad A_2 = sG_1 + G$ sends A_1 and A_2 to the bank *i*.

2) the bank selects random number $a \in Z_q^*$ and $W_1, W_2 \in G_1$ and computes

$$a_1 = e(aA_1, W_1)$$
$$a_2 = e(x_{B_i} A_1, W_2)$$
$$a_3 = e(W_2, P_{B_i})$$
$$a_4 = e(W_1, aG)$$
$$a_5 = e(A_1, ax_{B_i} W)$$

sends $a_1, a_2, a_3, a_4 and\ a_5$ to u_i.

3) the u_i calculates $Z = P_{u_i} + P_2 + sP_1 = sA_1$
$Z_1 = x_{u_i} A_2 + P_{u_i}$ selects random numbers
$s_1, r_1, r_2, x_1, x_2, u, v \in Z_q^*$ and computes
$A = s_1(P_{u_i} + G_1)$, $B = x_1 G_1 + x_2 G_2 + uv_{u_i} G_3$,
$C = r_2 G + r_1 x_1 G_3$, $Y_1 = x_1 a_1 + uG_2$
$Y_2 = r_1 a_3 + x_2 G_4$, $Y_3 = v_{u_i} sa_5 + x_1 sk_{u_i}$
$Y_4 = r_2 a_2 + s_1 G_2$, $Y_5 = ur_1 a_4 + x_2 G_3$
$c = H(Z, Z_1, A, B, C, Y_1, Y_2, Y_3, Y_4, Y_5)$
$c' = c/u$ sends c' to B_i.

4) the B_i computes $S_1 = c'aW_1 + x_{B_i} W_2$ sends S to u_i.

5) the u_i checks

$$e(S_1, G) \stackrel{?}{=} a_4^{c'} a_3 \tag{1}$$

and

$$e(A_1, S_1) \stackrel{?}{=} a_1^{c'} a_2 \tag{2}$$

If (1) and (2) holds, then the user accepts and computes $S_2 = uS_1 + vQ_{ID_{u_i}}$

We can proof (1) and (2) as follows:

$$e(S_1, G) = e(c'aW_1 + x_{B_i} W_2, G)$$
$$= e(c'aW_1, G) e(x_{B_i} W_2, G)$$
$$= e(W_1, aG)^{c'} e(W_2, x_{B_i} G)$$
$$= a_4^{c'} a_3$$
$$e(A_1, S_1) = e(A_1, c'aW_1 + x_{B_i} W_2)$$
$$= e(A_1, c'aW_1) e(A_1, x_{B_i} W)$$
$$= e(aA_1, W_1)^{c'} e(x_{B_i} A_1, W_2)$$
$$= a_1^{c'} a_2$$

4.5. Payment Protocol

The payment protocol involves the customer and the merchant. If the customer wants to buy some goods from the merchant, they should execute the follows:

1) The customer chooses a random $w_1, w_2 \in Z_q^*$ and computes $D = w_1 uG_1 + w_2 vG_2$

User sends A, B, C, D, Z, Z_1, S_2 to merchant.

2) The merchant generates a transaction message of payment for the customer *d* as challenge and sends to user

Copyright © 2012 SciRes.

$d = H_0(A, B, C, D, Z, Z_1, S_2, P_{M_i}$,*amount, amount type, date/time*)

3) User calculates responses

$$f_1 = w_1 u G_1 + ds_1 x_{u_i} P_t$$
$$f_2 = w_2 v G_2 + ds_1 P_1$$
$$f_3 = x_1 \left(dP_1 + r_1 P_3 \right)$$
$$f_4 = d\left(x_2 P_2 + u x_{u_i} S_1 \right)$$
$$f_5 = d\left(uv_{u_i} P_3 + v x_{u_i} Q_{ID_{u_i}} \right) + r_2 P_t$$

User sends f_1, f_2, f_3, f_4 *and* f_5 to merchant.

4) The signature of electronic cash is A, B, C, D, S_2, f_1, f_2, f_3, f_4 *and* f_5.

5) Merchant accepts if and only if

$$e\left(f_1 + f_2, G\right) \stackrel{?}{=} e\left(D, G\right) e\left(A, P\right)^d \quad (3)$$

$$e\left(f_3 + f_4 + f_5, G\right) \stackrel{?}{=} e\left(B, P_t\right)^d e\left(C, P_t\right) e\left(dS_2, P_{u_i}\right) \quad (4)$$

Now we can proof (3) and (4) as followings:

$$\begin{aligned} e\left(f_1 + f_2, G\right) &= e\left(w_1 u G_1 + ds_1 x_{u_i} P_t + w_2 v G_2 + ds_1 P_1, G\right) \\ &= e\left(w_1 u G_1 + w_2 v G_2, G\right) e\left(ds_1 \left(x_{u_i} P_t + P \right)_1, G\right) \\ &= e\left(D, G\right) e\left(P_1 ds_1 \left(x_{u_i} x_t G + x_t G_1 \right), G\right) \\ &= e\left(D, G\right) e\left(ds_1 \left(P_{u_i} + G_1 \right), P_t\right) \\ &= e\left(D, G\right) e\left(dA, P_t\right) \end{aligned}$$

$$\begin{aligned} & e\left(f_3 + f_4 + f_5, G\right) \\ &= e\left(x_1 \left(dP_1 + r_1 P_3 \right) + d\left(x_2 P_2 + u x_{u_i} S_1 \right) + d\left(uv_{u_i} P_3 + v x_{u_i} Q_{ID_{u_i}} \right) + r_2 P_t, G\right) \\ &= e\left(d\left(x_1 P_1 + x_2 P_2 + uv_{u_i} P_3 \right) + dx_{u_i} \left(uS_1 + vQ_{ID_{u_i}} \right) + x_1 r_1 P_3 + r_2 P_t, G\right) \\ &= e\left(x_t d\left(x_1 G_1 + x_2 G_2 + uv_i G_3 \right), G\right) e\left(dx_{u_i} \left(uS_1 + vQ_{ID_{u_i}} \right), G\right) e\left(x_t \left(x_1 r_1 G_3 + r_2 G \right), G\right) \\ &= e\left(dB, P_t\right) e\left(dS_2, P_{u_i}\right) e\left(C, P_t\right) \end{aligned}$$

4.6. Deposit Protocol

In this protocol the merchant *i* sends electronic cash to his bank *i*. There are two cases we will discuss as follows:

First case: if the shop *i* and user *i* have accounts in the same bank. Since the deposit protocol involves merchant and bank, they will execute the following steps:

1) The merchant sends signatures of electronic cash $A, B, C, D, Z, Z_1, S_2, f_1, f_2, f_3, f_4$ *and* f_5 to the bank.

2) The bank verifies the validity of signature of e cash $A, B, C, D, Z, Z_1, S_2, f_1, f_2, f_3, f_4$ *and* f_5.

3) If the signature of e cash $A, B, C, D, Z, Z_1, S_2, f_1, f_2, f_3, f_4$ *and* f_5 is hold, then the bank searches the deposit database to find out the same electronic cash has been deposited before or not. If it has not been in its deposit database, the bank accepts the electronic cash and credits the amount to the shop account, otherwise the bank *i* rejects transaction.

Second case: if the user i and merchant i have accounts in different banks such as user i has an account in the bank i and shop i has an account in bank j.

Assume merchant i wants to deposit the received electronic cash from user i to his bank j, they will do the following steps:

1) The merchant sends signature of electronic cash $A, B, C, D, Z, Z_1, S_2, f_1, f_2, f_3, f_4$ *and* f_5 to bank j.

2) Bank j verifies the validity of signature of e cash $A, B, C, D, Z, Z_1, S_2, f_1, f_2, f_3, f_4$ *and* f_5 with bank i's public key.

3) If it succeeds then bank j sends the electronic cash to bank i.

4) Bank i searches the deposit database to find out whether electronic cash has been deposited before, if it is not has been stored in deposit database then bank i debits the amount from user i account and sends it to the merchant i account in his bank j, otherwise bank i can detect double depositing or double spending.

4.7. The Tracing Protocol

Customer Tracing Protocol

The customer tracing protocol involves the bank and the trusted third party. This protocol is used to determine the identity of the customer in a specific payment transaction. Money laundering is big problem of electronic cash; here it can be protected by detecting the identity of the illegal customers.

1) The customer tracing protocol is as follows:

The bank sends to the CB the signatures of electronic cash $A, B, C, D, Z, Z_1, S_2, f_1, f_2, f_3, f_4$ *and* f_5 that received from the merchant in the deposit protocol.

2) The CB verifies the validity of the signature of electronic cash as the merchant does in the deposit protocol.

3) The CB can calculate P_{u_i} from $\left(Z, A_2\right)$ as follows:

$$\begin{aligned} Z &= P_{u_i} + P_2 + sP_1 \\ &= P_{u_i} + P_2 + s\left(x_t G_1 \right) \\ &= P_{u_i} + P_2 + x_t \left(sG_1 \right) \end{aligned} \quad (5)$$

From $sG_1 = A_2 - G$ then put it into (5)

$Z = P_{u_i} + P_2 + x_t A_2 - P_t$

Copyright © 2012 SciRes.

Finally we get

$P_{u_i} = Z + P_t - (P_2 + x_t A_2)$

The CB sends P_{u_i} to the bank.

Then the bank can find the actual identity corresponding to P_{u_i} in his database.

5. Analysis of Security

Theorem 1

A group member and the group manager cannot sign electronic cash on behalf of the other group members with non-negligible probability.

Proof:

Assume there is a group member who has ID_j wants to sign electronic cash on behalf of the group member who has ID_i.

He chooses random number $s \in Z_q^*$, computes and sends A_1 *and* A_2 to bank *i*.

$A_1 = s^{-1}\left(P_{u_j} + P_2\right) + P_1$

$A_2 = sG_1 + G$

The bank calculates and sends a_1, a_2, a_3, a_4 *and* a_5 back to him as withdraw protocol.

He selects random numbers $s_1, r_1, r_2, x_1, x_2, u, v \in Z_q^*$ and computes Z, C, Y_1, Y_2, Y_4, Y_5 as withdraw protocol, computes Z_1, A, B, Y_3 as follows:

$A = s_1\left(P_{u_j} + G_1\right)$, $B = x_1 G_1 + x_2 G_2 + uv_j G_3$,

$Y_3 = v_j s a_5 + x_1 s k_j$, $Z_1 = x_{u_j} A_2 + P_{u_j}$

Finally he calculates *c* as

$c = H\left(Z, Z_1, A, B, C, Y_1, Y_2, Y_3, Y_4, Y_5\right)$

This equation can be equal to that equation in withdraw protocol, if and only if

$s_1 P_{u_i} = s_1 P_{u_j}, uv_i G_3 = uv_j G_3, v_i s a_5 = v_j s a_5,$

$x_1 sk_i = x_1 sk_j$ *and* $x_{u_i} A_2 = x_{u_j} A_2$

The probability of $x_i = x_j$ is $1/(q-1)$, $x_i, x_j \in Z_q^*$. If he wants to choose exactly $x_j = x_i$, he needs to solve discrete logarithm problem $P_{u_i} = x_{u_i} G$ as $x_{u_i} = \log_G P_{u_i}$.

Theorem 2

The proposed fair electronic cash system can protect the customer's privacy and keep the system anonymous.

Proof:

Deciding whether a payment signature from a customer requires knowing ID_{u_i} of the user. However, to know ID_{u_i} of the user in our scheme requires solving discrete logarithm problem $P_{u_i} = x_{u_i} G$ to find out the user secret key. Since solving discrete logarithm problem is very difficult, then no one can know ID_{u_i} except CB.

Theorem 3

In the payment protocol, only users that register in the CB are able to sign a payment message with his membership key.

Proof:

It is difficult to find x_{u_i} from $P_{u_i} = xG$. The forger cannot find the same x_{u_i} then it is impossible to get certificate membership (sk_i, v_i) to sign a payment message.

Theorem 4

Our proposed scheme keeps the system unlinkability.

Proof: To decide whether two signatures of electronic cash $A, B, C, D, Z, Z_1, S_2, f_1, f_2, f_3, f_4$ *and* f_5 and $A', B', C', D', Z', Z_1', S_2', f_1', f_2', f_3', f_4'$ *and* f_5' are from the same customer requires deciding whether

$$d' \log_{P_{u_i}} \left(e(f_1 + f_2, G)/e(D, G)\right) = d \log_{P_{u_i}} \left(e(f_1' + f_2', G)/e(D', G)\right)'$$

it is not easy to compute it.

From the four theorems and traceable protocol above, it is easy to deduce that our scheme satisfies the security properties of group signatures and provides electronic cash against double spending, blackmailing and money laundering.

6. Conclusion

We have presented new fair electronic cash system with identity based group signature scheme. It satisfies all basic requirements to protect electronic cash. Furthermore, we show how our group signature scheme could construct fair electronic cash, which satisfy properties of secure group signature scheme.

REFERENCES

[1] D. Chaum and E. van Heyst, "Group Signatures," In: J. Feigenbaum, Ed., *Advances in Cryptology*: *EUROCRYPT* '91—*Workshop on the Theory and Application of Cryptographic Techniques*, Springer-Verlag & GmbH & Co. K, Berlin and Heidelberg, 1991, pp. 257-265.

[2] S. Canard and M. Girault, "Implementing Group Signature Schemes with Smart Cards," *Proceedings of the* 5*th Conference on Smart Card Research and Advanced Application*, San Jose, 21-22 November 2002, pp. 1-10.

[3] L. Chen and T. Pedersen, "New Group Signatures Schemes," In: A. D. Santis, Ed., *Advances in Cryptology—EUROCRYPT* 94: *Workshop on the Theory and Application of Cryptographic Techniques*, Springer-Verlag, Berlin, 1995, pp. 171-181.

[4] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Proceedings of CRYPTO* 84 *on Advances in Cryptology*, Santa Barbara, 19-22 August 1984, pp. 47-53.

[5] X. Chen, F. Zhang and K. Kim, "A New ID-Based Group Signature Scheme from Bilinear Pairings," 2003. http://eprint.iacr.org/2003/116.2003

[6] S. Han, J. Wang and W. Liu1, "An Efficient Identity-Based Group Signature Scheme over Elliptic Curves," *Proceedings of the ECUMN* 2004, Porto, 25-27 October 2004, pp. 417-429.

[7] Z. Tan and Z. Liu, "A Novel Identity-Based Group Signature Scheme from Bilinear Maps," MM Research Pre-

Copyright © 2012 SciRes.

prints, 2003, pp. 250-255.

[8] J. Cha and J. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," *Proceedings of the PKC* 2003, Miami, 6-8 January 2003, pp. 18-30.

[9] A. Lysyanskaya and Z. Ramzan, "Group Blind Digital Signatures: A Scalable Solutionto Electronic Cash," *Proceedings of the Financial Cryptography*: *Second International Conference*, *FC*'98, Anguilla, 23-25 February 1998, pp. 184-197.

[10] T. Nakanishi, N. Haruna and Y. Sugiyama, "Unlinkable Electronic Couponprotocol with Anonymity Control," *Proceedings of the International Workshop on Information Security* (*ISW* 99), Kuala Lumpur, 6-7 November 1999, pp. 37-46.

[11] J. Traor´e, "Group Signatures and Their Relevance to Privacy-Protecting Off-Line Electronic Cash Systems," *Proceedings of the Australasian Conference on Information Security and Privacy* (*ACISP* 99), Wollongong, 7-9 April 1999, pp. 228-243.

[12] D. B. Johnson and A. J. Menezes, "Elliptic Curve DSA (ECDSA): An Enhanced DSA," 2000. http://www.certicom.com

[13] D. Hankerson, A. Menezes and S. Vanstone, "Guide to Elliptic Curve Cryptography," Springer-Verlag, New York, 2004.

[14] J. Cha and J. Cheon, "An Identity-Based Signature from Gap DiffieHellman Groups," *Proceedings of the PKC* 2003, Miami, 6-9 January 2003, pp. 18-30.

Copyright © 2012 SciRes.