# Dynamic Fair Electronic Cash Model without Trustees

Jingliang Zhang [1,2], Lizhen Ma [3] and Yumin Wang [1]
1 State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China zjlmlz@yahoo.com.cn
2 Department of Mathematics, Ocean Univ. of China, Qingdao 266071, China
3 Department of Physics, Ocean Univ. of China, Qingdao 266071, China

**Abstract**. A new fair electronic cash system is proposed based on group blind signature and secret sharing scheme. Our proposed system is dynamic: we propose a method to delete the dishonest banks that maybe attack the system, which was not mentioned in the previous literatures. Our proposed scheme does not need a trusted third party to trace users: a shop owning suspicious e-coin and the bank having issued the coin can collaborate to find the user using secret sharing scheme, however, any one of them can't trace the user alone. Furthermore, a novel e-coin tracing method is used to prevent criminal activities: under normal situation, the bank issues ordinary e-coin, while under abnormal situation such as blackmailing, kidnapping etc., the bank issues marked e-coin, and at the step of deposit, any bank in the group can recognize the marked e-coin. Also, our scheme is constructed for multiple banks as in the real life, thus it is more practical.

## 1 Introduction

With the popularization of internet, people are engaged in electronic commerce with high frequency. Secure and efficient electronic payment systems are significant for electronic commerce. As an important electronic payment system, electronic cash (E-cash or digital cash) develops rapidly. Chaum [1] proposed the first electronic cash system with unconditional anonymity by use of blind signature in 1982. However, this unconditional anonymity may be misused for criminal activities such as money laundering, blackmailing, kidnapping etc. [2]. From then, many fair electronic cash systems were proposed which need a trusted third party (TTP) to revoke the anonymity of the users when necessary. Figure 1 is the flow chart of a basic fair electronic cash model with multiple banks.

As a powerful tool, group signature has been widely used to design fair electronic cash system [5-9]. However, any bank in the group is supposed to be

honest in the previous electronic cash systems based on group signature. But it is possible that there exist dishonest banks probably in the real life, so it is reasonable to consider that there maybe exist dishonest banks in an electronic cash system.

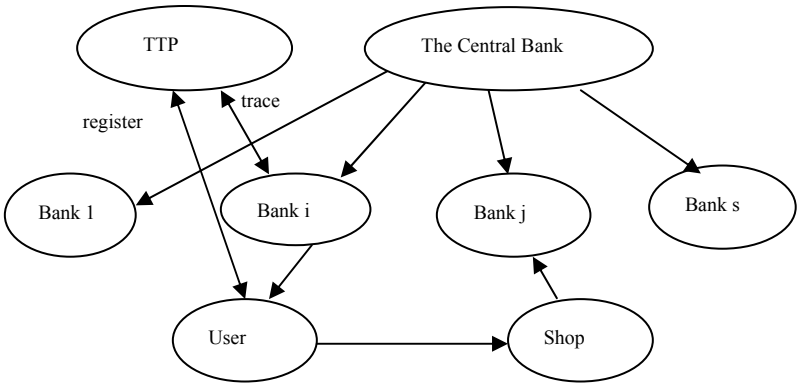


**Figure 1** Fair Electronic Cash Model with Multiple Banks

In this paper we propose a member deletion method to CS97 group signature scheme [3] and according to it construct a dynamic fair electronic cash model with multiple banks: a bank can join the group, also, the group manager can delete a bank when he breaks the rules of the group. Our proposed scheme has the following properties: a user can spend his e-cash anonymously, any bank can't trace the user; there is only one public key in the group of the banks, and the length of the public key don't change with the increase of the number of the banks; given an e-cash, nobody but the Central Bank can know by which bank it is issued, which can provide anonymity for the banks; no banks including the Central Bank can issue e-cash on behalf of another bank; the previous e-cash issued by the deleted bank cannot be disclosed and it is impossible for the deleted bank to issue e-cash continuously. In particular, our scheme can realize user tracing without trustees and can prevent users from blackmailing, kidnapping etc... Figure 2 is the flow chart of our proposed model.

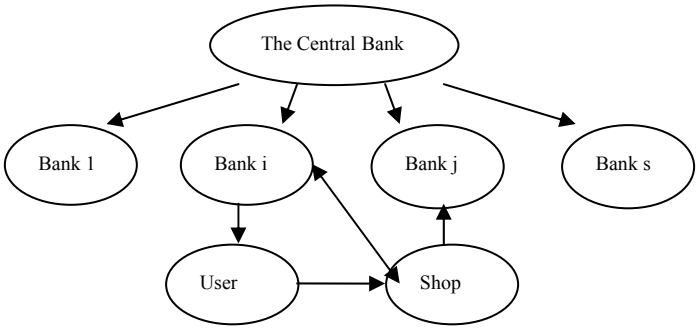


**Figure 2** Fair Electronic Cash Model without Trustees

## 2 Dynamic group blind signature

### 2.1 Signature of knowledge of discrete logarithm

Besides the blind signature of knowledge of double discrete logarithm BSKLOGLOG[ $\alpha \mid y = g^{a^{\alpha}}$ ](m) and the signature of knowledge of e-th root of discrete logarithm BSKROOTLOG[ $\alpha \mid y = g^{\alpha^{e}}$ ] (m) as in LR98 [5] group blind signature, we also need the following definition:

**Definition** An ( $l$ +1)-tuple ( $c$ , $s_1$ , … , $s_l$ ) $\in \{0,1\}^k \times Z_n^{*l}$ satisfying $c = H_l$ (m|| $y_1 \| \ldots \| y_t \| g_1 \| \ldots \| g_t \| g_1^{s_1}\ y_1^{c[1]} \| \ldots \| g_1^{s_l}\ y_1^{c[l]} \| \ldots \| g_t^{s_1}\ y_t^{c[1]} \| \ldots \| g_t^{s_l}\ y_t^{c[l]}$ ) is a signature of knowledge of a representation of the discrete logarithms of $y_1$ ,….., $y_t$ to the bases $g_1$ ,….., $g_t$ on a message m, with security parameter $l$ , denoted: SKREPLOG[ $\alpha : y_1 = g_1^{\alpha} \wedge \ldots \wedge y_t = g_t^{\alpha}$ ](m).

We can obtain the blind one, denoted BSKREPLOG[ $\alpha : y_1 = g_1^{\alpha} \wedge \ldots \wedge y_t = g_t^{\alpha}$ ]( m), as follows:

**User** Round 0: User wants message m signed and sends a sign request to the signer.

**Signer** Round 1: For $1 \le i \le l$ , generate random $2^{\lambda} \le r_i \le 2^{\lambda+\mu}$ -1, set $P_{ji} = g_j^{r_i}$ and send { $P_{ji}$ } to the user, j=1,….,t.

**User** Round 2:Obtain a random permutation $\sigma$ : {1,…, $l$ } $\rightarrow$ {1,…, $l$ } and set $Q_{ji} = P_{j\sigma(i)}$ ,for $1 \le$ i,j $\le l$ , generate random $2^{\lambda+\mu} \le a_i \le 2^{\lambda+2\mu}$ -1, and set $R_{ji} = Q_{ji}\ g_j^{a_i}$ ,calculate $c = H_l$ ( m|| $y_1 \| \ldots \| y_t \| g_1 \| \ldots \| g_t \| R_{11} \| \ldots \| R_{1l} \| \ldots \| R_{t1} \| \ldots \| R_{tl}$ ), calculate $c'$ such that $c'[i] = c[\sigma^{-1}(i)]$ , send $c'$ to the signer.

**Signer** Round 3: Compute, for $1 \le i \le l$ , $t_i = r_i$ ,if $c'[i] = 0$ ; $t_i = r_i - x$ ,if $c'[i] = 1$ , send { $t_i$ } to the user.

**User** Round 4: Verify that $P_{ji} = g_j^{t_i}\ y_j^{c'[i]}$ , compute $s_i = t_{\sigma(i)} + a_i$ ,$1 \le i \le l$ ,output BSKREPLOG[ $\alpha : y_1 = g_1^{\alpha} \wedge \ldots \wedge y_t = g_t^{\alpha}$ ](m) : ( $c$ , $s_1$ , … , $s_l$ ).

### 2.2 Dynamic group blind signature

The main idea is: the group manager issues the membership keys of the deleted members on a bulletin board, every group member must prove with zero knowledge that his membership key is not on the bulletin board when he signs a message. Our scheme is based on LR98 [5] group blind signature. We mainly introduce the steps of **revoke** and **sign** because the steps of **setup**, **join** and **open** are the same as that in LR98 [5].

**Setup** The group manager constructs the group's public key ( $n$ , $e$ , $G$ , $g$ , $a$ , $\lambda$ , $\mu$ ).

**Join** A group member picks a secret key $x$ , calculates $y = a^x$ (mod n) and the membership key $z = g^y$ , obtains his membership certificate $v = (y+1)^{1/e}$ (mod n) from the group manager.

**Revoke** When a member is deleted, the group manager issues his membership key $z = g^y$ on a bulletin board.

**Sign signer:** Look up the bulletin board issued by the group manager, suppose that there are t deleted members: $z_1, z_2, \ldots, z_t$ . Obtain $q \in_R Z_n^*$ and set $\tilde{g} = g^q$ , $\tilde{z} = \tilde{g}^y$ , $P_i^{LOG} = \tilde{g}^{a^{u_i}}$ , $P_i^{ROOT} = \tilde{g}^{v_i^e}$ , $v_1 = (z/z_1)^q, \ldots, v_t = (z/z_t)^q$ , send them to U.

**U:** Check $v_i \neq 1$, obtain $b \in_R \{0,1,\ldots, 2^{\lambda} -1\}$, $f \in_R Z_n^*$ , set $\omega = (af)^{eb}$ mod $q$ , $\hat{g} = \tilde{g}^{\omega}$ , $\hat{z} = \tilde{z}^{\omega}$ , $\hat{P}_i^{LOG} = (P_i^{LOG})^{\omega}$, $\hat{P}_i^{ROOT} = (P_i^{ROOT})^{\omega}$ , $v_1' = v_1^{\omega}, \ldots, v_t' = v_t^{\omega}$ , $z_1' = z_1^{\omega}, \ldots, z_t' = z_t^{\omega}$ , take $\hat{P}_i^{ROOT}$ and $\hat{P}_i^{LOG}$ as input, execute BSKROOTLOG and BSKLOGLOG, and execute BSKREPLOG taking $\hat{z}/v_i'$ , $z_i'$ as $y_i$ , $g_i$ respectively ,

then the signature is ( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ ), where $V_1$ =SKLOGLOG[ $x : \hat{z} = \hat{g}^{a^x}$ ](m), $V_2$ =SKROOTLOG[ $v : \hat{z}\ \hat{g} = \hat{g}^{v^e}$ ](m), $V_3$ = BSKREPLOG[ $q : \hat{z}/v_1' = z_1'^q \wedge \ldots \wedge \hat{z}/v_t' = z_t'^q$ ](m).

**Open** Given a signature ( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ ), the group manager can determine the signer by testing if $\hat{g}^{y_p} = \hat{z}$ for every group member P.

**Validity of the revocation:** From $V_3$ , we obtain $\hat{z}/v_i' = z_i'^q$ , that is, $\tilde{z}^\omega/v_i^\omega = z_i^{\omega q}$ , so $v_i^\omega = \tilde{z}^\omega/z_i^{\omega q} = z^{\omega q}/z_i^{\omega q} = (z/z_i)^{\omega q}$ , however, $v_i \neq 1$, thus $(z/z_i)^{\omega q} \neq 1$, this concludes $z \neq z_i$ .

## 3. Dynamic electronic cash system without trustees

All banks form a group, the group manager is the Central Bank of the country.

**Setup:** The Central Bank chooses a security parameter $l$ , and computes an RSA public key ( $n$ , $e$ ), where the length of $n$ is at least $2l$ bits; chooses a cyclic subgroup $G =< g >$ of order $n$ of $Z_p^*$ ; selects $a \in Z_p^*$ where $a$ has large multiplicative order modulo all the prime factors of $n$ ; chooses an upper bound $\lambda$ on the length of the secret keys and a constant $\mu$ >1.The group's public key is ( $n$ , $e$ , $G$ , $g$ , $a$ , $\lambda$ , $\mu$ ).

A bank can obtain his certificate from the Central Bank as follows: the bank picks a secret key $x \in_R \{0,1,\ldots, 2^\lambda - 1\}$, calculates $y = a^x$ (mod n) and the membership key $z = g^y$ , sends ( $y$ , $z$ )to the Central Bank, obtains his membership certificate $v = (y+1)^{1/e}$ (mod n) from the group manager.

The Central Bank need issue the deleted banks' membership keys $z_1, z_2, \ldots, z_t$ on a bulletin board.

**Withdrawal:** A user U has an account in a bank $B_i$ , U takes $u \in_R Z_p^*$ as his secret key, sends $I = g^u$ to $B_i$ and takes $I$ as his identity.

1 U chooses $1 \neq r \in_R Z_p^*$ , $c_0 = I^r$ ., $c_1 = r$ , f(x) = $c_0 + c_1$ x (mod $q$ ),and chooses $x_1 \in_R Z_p^*$ ,computes f( $x_1$ ), $C_0 = g^{c_0} \bmod p$ , $C_1 = g^{c_1} \bmod p$ . After authenticated by $B_i$ , U sends a withdrawal request and < $x_1$ , f( $x_1$ )>, $C_0$ , $C_1$ to the bank and with a proof: SKREPLOG[ $\gamma : I = g^\gamma \wedge C_0 = g^{C_1^\gamma}$ ].

2 $B_i$ checks the validity of SKREPLOG[ $\gamma : I = g^\gamma \wedge C_0 = g^{C_1^\gamma}$ ]and $C_0\ C_1^{x_1} = g^{f(x_1)}$ , then chooses X $\in_R Z_q^*$ ,computes $\alpha = g^X$ (mod $p$ )and sends $\alpha$ to U.

3 (1) Under the normal situation, U calculates $\alpha' = \alpha^r$ and sends $\alpha'$ to $B_i$ . $B_i$ validates $\alpha' = C_1^X$ , let $\beta = \alpha'$ ,then $B_i$ signs U's withdrawal message m with group blind signature as the step of **sign** in section 2.2, then the e-coin is m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $C_0$ , $C_1$ , $\alpha$ , $\beta$ );

(2) Under the abnormal situation such as blackmailing, kidnapping etc., U selects $\delta \neq r$ , sends $\alpha' = \alpha^\delta$ to $B_i$ . $B_i$ validates $\alpha' \neq C_1^X$ , selects $t \in_R Z_q^*$ and computes $\beta = \alpha^t$ , then $B_i$ signs U's withdrawal message m with group blind signature as the step of **sign** in section 2.2. Then the e-coin is m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $C_0$ , $C_1$ , $\alpha$ , $\beta$ ).

(3) $B_i$ stores m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $\alpha$ , $\beta$ , $x_1$ , f ( $x_1$ ))into his database and stores $t$ into the tracing database of the group manager.

**Pay and deposit:**

1 U chooses $x_2 \in_R Z_p^*$ , computes f ( $x_2$ ), sends < $x_2$ ,f( $x_2$ )> and m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $C_0$ , $C_1$ , $\alpha$ , $\beta$ )to the shop .

2 Shop checks the validity of ( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ ) and $C_0\ C_1^{x_2} = g^{f(x_2)}$ ,then sends m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $C_0$ , $C_1$ , $\alpha$ , $\beta$ )to his bank $B_j$ .

3 $B_j$ validates ( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ ), checks if $\alpha = \beta^{t_i}$ for all $t_i$ in the tracing database managed by the group manager. If for all $t_i$ , $\alpha \neq \beta^{t_i}$ , checks if the e-coin is double-spent via the online database of the group manager, if not, then deposits m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $C_0$ , $C_1$ , $\alpha$ , $\beta$ ) into the shop's account and informs the shop, the shop sends the merchandise to U; If there exists some $t_i$ such that $\alpha = \beta^{t_i}$ , then freezes m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $C_0$ , $C_1$ , $\alpha$ , $\beta$ ) and informs the shop, the shop refuses sending the merchandise to U.

**Identity revocation:** If the shop or $B_j$ checks that there's something suspicious on the e-coin , such as $\alpha = \beta^{t_i}$ for some $t_i$ , $B_j$ sends m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $C_0$ , $C_1$ , $\alpha$ , $\beta$ ) to the group manager, the group manager opens ( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ ) using the **open** technique in the group blind signature and finds the bank $B_i$ , sends the e-coin to $B_i$ . $B_i$ looks up his database and finds m( $\hat{g}$ , $\hat{z}$ , $v_1'$ ,…, $v_t'$ , $V_1$ , $V_2$ , $V_3$ , $\alpha$ , $\beta$ , $C_0$ , $C_1$ , $x_1$ , f( $x_1$ )), then $B_i$ and the shop can recover f(x) = $c_0 + c_1$ x by use of Shamir's secret sharing scheme with < $x_1$ , f( $x_1$ )>and < $x_2$ , f( $x_2$ )>. $B_i$ can find U's identity by testing if $c_0 = I^{c_1}$ for every user $I$ .

## 4. Analysis

**Prevention of blackmailing:** When a user U is blackmailed, he selects $\delta \neq r$ , sends $\alpha' = \alpha^{\delta}$ to $B_i$ , $B_i$ can find the deference $\alpha^r$ from $\alpha^{\delta}$ and gives U the marked e-coin, but, the blackmailer can't find the deference $\alpha^r$ from $\alpha^{\delta}$ ,and he is cheated successfully. Later, he can't buy back anything because any bank can identify the marked coin and freezes it. Also, the kind shop and the bank issuing the coin can identify the victim by using the **identity revocation** technique in the proposed scheme and give back the coin to the victim.

**Anonymity of coins:** Nobody but the Central Bank can know by which bank the e-coin is issued because of the anonymity of the group signature. However, the anonymity is conditional under an abnormal situation, i.e., the marked coin can be recognized.

**Anonymity of users:** A user can spend his e-coin anonymously; no bank or shop can trace the user alone without the help of the group manager because the coin is issued using blind signature.

**Traceability:** With the help of the group manager, the bank issuing the e-coin and the shop owning the coin can collaborate to find the user of the e-coin by use of Shamir's secret sharing scheme.

**Revocation of dishonest banks:** A dishonest bank can be deleted by the group manager via issuing his membership key on a bulletin board. The deleted bank can't issue e-coin continuously with his old certificate because he can't prove that his identity is not on the bulletin board; the previous e-coin issued by a deleted bank will not be disclosed because any other party can't obtain his secret key $x$ and certificate $v$ by his published identity $z$ due to RSA assumption.

## 5. Conclusions

In this paper, we propose a fair electronic cash system with member deletion. Besides having the general functions in other e-cash systems based on group signature, our scheme can also revoke the dishonest banks without disclosing their previous data. Also, in our scheme the bank uses a novel method to issue e-coin in order to prevent from blackmailing, kidnapping etc. Furthermore, our scheme is a system without trustees and is constructed for multiple banks as in the real life, thus it is more practical.

## REFERENCES

1. D. Chaum, Blind Signatures for Untraceable Payments, R. L.Rivest, *A. Sherman and D. Chaum* (Eds.): CRYPTO'82, Plenum Press, New York, 199-203 (1983).
2. B.V. Solms and D. Naccache, On Blind Signatures and Perfect Crimes, *Computers and Security*, Vol. 11(6), 581-583 (1992).
3. J. Camenisch and M. Stadler, *Efficient Group Signature Schemes for Large Groups*, *B.S.Kaliski Jr. (Ed.)*: CRYPTO'97, LNCS 1294, Springer-Verlag Berlin Heidelberg, 410-424 (1997).
4. E. Bresson and J. Stern, *Efficient Revocation in Group Signatures*, K. Kim (Ed.): PKC 2001, LNCS 1992, Springer-Verlag Berlin Heidelberg, 190-206 (2001).
5. A. Lysyanskaya and Z. Ramzan, Group Blind Digital Signatures: *a Scalable Solution to Electronic Cash*, R. Hirschfeld(Ed.): FC'98, LNCS 1465, Springer-Verlag Berlin Heidelberg, 184-197 (1998).
6. L. Chen, X.Q. Huang and J.Y. You, *Fair Tracing without Trustees for Multiple Banks*, J. Zhang, J.H. He and Y. Fu (Eds.): CIS 2004, LNCS 3314, Springer-Verlag Berlin Heidelberg, 1061-1066 (2004).
7. F.G, Zhang, F.T. Zhang and Y.M. Wang, Electronic Cash System with Multiple Banks, *Chinese J. Computers*, Vol. 24(5), 455-462 (2001).
8. S. canard and J. Traore, *On Fair E-Cash Systems Based on Group Signatures*, R. Safavi-Naini and J. Seberry(Eds.): ACISP 2003, LNCS 2727, Springer-Verlag Berlin Heidelberg, 237-248 (2003).
9. G. Maitland and C. Boyd, *Fair Electronic Cash based on a Group Signature Scheme*, S. Qing, T. Okamoto and J. Zhou (Eds.): ICICS 2001, LNCS 2229, Springer-Verlag Berlin Heidelberg, 461-465 (2001).