# Fair Electronic Cash Systems with Multiple Banks

FANGGUO ZHANG, FUTAI ZHANG, YUMIN WANG
*P.O.Box119 Key Lab. on ISN,Xidian univ.,Xi'an, P.R.China, 710071*

Key words: Fair Electronic Cash, Group Signature, Elliptic Curve Discrete Logarithms.

Abstract: We propose a model for fair electronic cash issued by multiple banks for the first time. A scheme of electronic cash with multiple banks in which a user can be traced is presented by using the improved group signature scheme of Cam97[4] and the group blind signature scheme of Lys98[14]. A weakness in the design of withdrawal and payment protocols using the existing group signature schemes is pointed out with its reasons analyzed.

## 1. INTRODUCTION

Secure and efficient electronic payment systems are significant for electronic commerce. Electronic cash (or digital cash) can be considered as an imitation of paper money, but is more convenient and economical. In the simplified model of off-line electronic cash system, three types of parties are involved: the users, shops and bank. Four possible transactions may occur between them: registration, withdrawal, payment and deposit. The first electronic cash scheme was suggested by chaum[8] in 1982. But this complete anonymity of electronic cash can be used for criminal activities, such as money laundering, blackm- ailing [16]. For this reason the electronic cash of future should be not fully or conditional anonymous. In 1995, M.Stadler et. al.[15]proposed the concept of 'Fair Blind Signatures'. It can be employed for conditional anonymous of electronic payment systems. In 1996, J.Camenisch et. al.[14] and Y. Frankel et. al.[11] proposed the concept of 'Fair Off-line Electronic Cash' independently. The untraceability of fair off-line electronic cash is not completely, it can be revoked by a trusted third party(TTP)so that the criminal activities making use of the complete anonymity of electronic cash can be prevented.

By now the electronic coins in every fair electronic cash scheme available are issued by one bank. However, in practice it is more convenient to use electronic

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

coins issued by multiple banks. Since in a country or district there may be more than one banks who are able to issue electronic cash. Each of these banks can issue electronic cash of its own. In this paper we propose a model for fair electronic cash issued by multiple banks for the first time. A scheme of fair electronic cash with multiple banks in which a user can be traced is presented by using the improved group signature scheme of Cam97[4] and group blind signature scheme of Lys98[14].

## 2. RELATED WORK

There have been many schemes of fair electronic cash issued by only one bank[6][11][15][16]. Two kinds of traceability can be realized in a fair electronic cash scheme, i.e., the traceability of user and the traceability of coin.There are many ways to control anonymity in electronic cash schemes[10], but the technique of fair blind signatures is a commonly used one[6][15]. The techniques of anonymity control in electronic payment systems were well described by J.Claessens et. al. in [10].

In a group signature scheme each member of an arbitrary large group is allowed to sign messages on behalf of the whole group, whereas no one but the unique designated group manager can open the signature to find who is the signer, so the anonymity of the signer is protected. For this reason, the techniques of group signatures can be employed in anonymity controlled electronic payment systems. In such systems the group manager takes the role of the TTP. Recently, J.Traore[17] proposed a group signature scheme with which he designed a privacy protected off-line electronic cash scheme. However, Traore's electronic cash scheme is not perfect. In the last part of section four, we point out this weakness with its reason analyzed.

We did not find any fair electronic cash schemes with multiple banks in the literature until we were prepared to complete this paper. The concept of electronic cash systems with multiple banks was first proposed by A. Lysyanskaya and Z.Ramzan in FC98[14].They also presented an anonymous off-line electronic cash scheme with multiple banks using the techniques of group blind signatures originated from themselves. Their scheme is not practical since it is completely anonymous, and there are too many data need to be transferred in their scheme, and the signature is too long. Next we will propose a model for fair electronic cash with multiple banks and present a fair electronic cash scheme using the improved group signature scheme of Cam97 and group blind signature scheme of Lys98 based on elliptic curves.

## 3. A MODEL FOR FAIR ELECTRONIC CASH SYSTEMS WITH MULTIPLE BANKS

In our model there are many banks. They form a group under control of the Central Bank(CB). The CB takes the role of the group manager. Each bank can issue

electronic cash. The principals participate in this system are the CB, many local banks $B_i$, $B_j$, etc., a TTP, some users (U has his own bank $B_i$ ), and some shops (S has its own bank $B_j$). Figure 1 shows the basic mode.

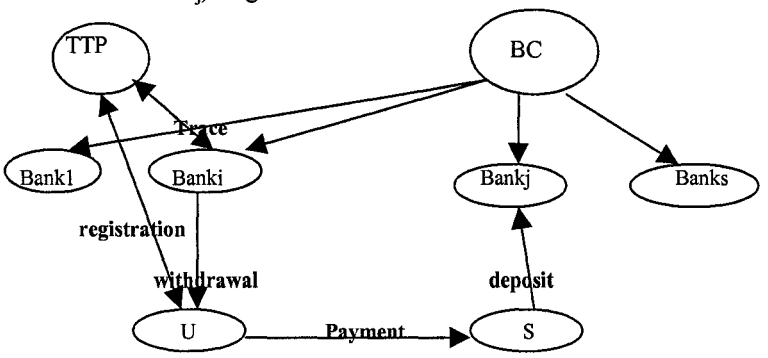


Figure1:A model for fair electronic cash with multiple banks

The model includes the following procedures:

- **Registration:** The user U establishes the releationship of his identity and pseudonym to the TTP so that with this relationship the TTP can revoke user anonymity when necessary. At the same time the user get a certificate issued by the TTP that proves his registration.
- **Open account:** The user U has his account in his bank $B_i$.
- **Withdrawal:** The user U withdraws an coin from his bank $B_i$.
- **Payment:** The user U purchases something in the shop S and pays the coin to the shop S.
- **Deposit:** The shop S deposits the received coin in his bank $B_j$.
- **Trace:** Bank $B_j$ send the received coin to the CB,CB finds bank $B_i$.. Finally the user can be traced with the help of the TTP.

Our systems of fair electronic cash with multiple banks have the following properties:

1.The user can spend his electronic coin anonymously.

2.To check the validity of a received coin the shop performs a simple verification procedure using the single public key of the bank group.

3.The group of all banks just has one public key, and the length of the group public key does not change with the increase of the number of banks.

4.Given an electronic coin, nobody but the CB can know by which bank it is issued. This can provide anonymity for the banks.

5.No banks including CB can issue coin on behalf of another bank.

6.The CB can determine which bank issued it when an electronic coin is found something wrong(e.g.double spent), and then this bank can find who is the owner of this coin with the help of the TTP.

7. Each bank can trace an electronic coin with the help of the TTP according to the information supplied by its user.

In the next section we design a fair electronic cash scheme that satisfies the properties 1—6 above. In our scheme the user can be traced.

# 4. AN USER TRACEABLE ELECTRONIC CASH SCHEME WITH MULTIPLE BANKS

## 4.1 Group Signatures and Signatures of Proof of Knowledge Based on Elliptic Cuirves

The concept of group signatures was proposed by Chaum and V.Heyst in 1991[9]. Since then many researchers have studied it, and many good schemes[1][4][10] have been presented. For the definition and the secyrity requirements of group signature scheme we refer the readers to [1][4][10]. A.Lysyanskaya et. al[14] introduced the concept of group blind signatures and proposed the first realizations of such schemes. Group blind signatures incorporate the properties of both blind signatures and group signatures.

Among many of the proposed schemes, the group signature scheme of Can97 and group blind signature scheme of A98 are relatively efficient ones. They are based on the same techniques, i.e., the signatures of proof of knowledge of double discrete logarithm (SKLOGLOG) and the *e*-th root of discrete logarithm. The discrete logarithms used in these two kinds of signatures are in ordinary multiplicative groups. The amount of data need to be transferred is very large and the signatures are too long, so they are not very practical. In our fair electronic cash scheme we extend the above two schemes to elliptic curves so that the amount of data and the length of signatures are greatly decreased, hence the efficiency is improved.

The detailed discussion of proofs of knowledge of discrete logarithm can be found in [3][4][7].They are often used to establish signature schemes and identity authentication schemes. The proofs of knowledge of discrete logarithms often used are: proof of knowledge of one discrete logarithm denoted by $SPK\{(\alpha): y = g^{\alpha}\}(m)$, proof of knowledge of the equ- ality of two logarithms denoted by $SPK\{(\alpha): y_1 = g^{\alpha} \wedge y_2 = h^{\alpha}\}(m)$, proof of knowledge of one of the two discrete logarithms denoted by $SPK\{(\alpha): y_1 = g^{\alpha} \wedge y_2 = h^{\alpha}\}(m)$, and proof of knowledge of a logarithm in an given interval denoted by $SPK\{(\alpha): y = g^{\alpha} \wedge \alpha \in [a,b]\}(m)$. These discrete logarithms in multiplicative groups can be extended to elliptic curves easily.

The double discrete logarithm of $y$ with respect to base $g$ and $h$ is defined to be $x$ such that $y = g^{h^x}$ ,where $g$ is a generator of a group of order $p$, $h$ is a specified element of $Z_p$* with a large order. The assumption of double discrete logarithm is: it is hard to find $x$ given $y = g^{h^x}$ .The $e$-th root of discrete logarithm of $y$ with respect to base g is the integer $x$ satisfying $y = g^{x^e}$ . We call the group generated by $g$ the base group, and the one generated by $h$ the exponent group. Since $h^x$and $x^e$ can be looked as integers modulo $p$, we can not extend exponent group to elliptic curves. However we may use a group over elliptic curves as the base group. Next we will extend SKLOGLOG, SKROOTLOG, blind SKLOGLOG and blind SKROOTLOG[14] to elliptic curves. This is very important for our new scheme.

Let $p$ be a large prime,$a,b \in GF(p)$ satisfy $4a^3+27b^2 \neq 0$. The elliptic curve $E_{(a,b)}(GF(p))$ is defined to be the set of points $(x,y) \in GF(p) \times GF(p)$ satisfying equation $y^2=x^3+ax+b$ and a special point $O$ (called infinity). These points form an abelian group. Let $G$ be an element of $E_{(a,b)}(GF(p))$ with prime order $q$ at least 160 bits in length, and $R_x(A)$is the $x$-coordinate of point $A$. More detailed description of elliptic curves can be found in [12][13]. Let $H$ be a one way hash function, $H : \{0,1\}^* \rightarrow \{0,1\}^k \ (k \approx 160)$,$(n, e)$ be a RSA public key pair, $a$ be a specified element of $Z_n^*$ with large multiplicative order modulo both factors of $n$. The double discrete logarithm and the $e$-th root of the discrete logarithm with base group $E_{(a,b)}(GF(p))$ are described as $Q=a^xG$ and $Q=x^eG$ respectively. $c[i]$denotes the $i$-th rightmost bit of the string $c$, and $H_l$ the first $l$ bits of $H$. We use $(\bullet \| \bullet)$ to denote the concatenation of two strings.

**Definition 4.1.2** Let $l<k$ be a security parameter. An $l+1$ tuple $(c, s_1, s_2 \Lambda\ , s_l) \in \{0,1\}^k \times Z_q^{*l}$ satisfying the equation

$c=H(m||R_x(G)||\ R_x(Q)||a||t_1...||t_l)$ with $t_i = \begin{cases} R_x(a^{s_i}G) & \text{if } c[i]=0 \\ R_x(a^{s_i}Q) & \text{otherwise} \end{cases}$ is called a signature of knowledge of a double discrete logarithm of $Q$ to the bases $G$ and $a$, and is denoted by $SKLOGLOG[x:Q=a^xG](m)$.

**Definition 4.1.3** Let $l<k$ be a security parameter, An $l+1$ tuple $(c, s_1, s_2 \Lambda\ , s_l) \in \{0,1\}^k \times Z_q^{*l}$ is called a signature of knowledge of an $e$-th root of the discrete logarithm of $Q$ to the base $G$ on m if it satisfies equation $c=H(m||R_x(G)||\ R_x(Q)||e||t_1...||t_l)$ with $t_i = \begin{cases} R_x(s_i^eG) & \text{if } c[i]=0 \\ R_x(s_i^eQ) & \text{otherwise} \end{cases}$

It is denoted by $SKROOTLOG[x:Q=x^eG](m)$.

Similar to the case of multiplicative groups, if $x$ is known, then it is simple to construct the two signatures defined above. [4]. The above two kinds of signatures can also be used to sign messages blindly[14]. We will extend them to elliptic curves.

In the following protocol, $\lambda$, $\mu$ are specified open security parameters, and $S_l$ is a permutation group of order $l$.

**Blind SKLOGLOG protocols based on elliptic curves BSKLOGLOG :**

User U Signer S

$\sigma \in_R S_l$ $\xleftarrow{P_i}$ $2^\lambda \le r_i \le 2^{\lambda+\mu}-1$ $P_i = (a^{r_i} \bmod q)G$

$Q_i = P_{\sigma(i)}$, $2^{\lambda+\mu} \le b_i \le 2^{\lambda+2\mu}-1$

$R_i = a^{b_i}Q_i$, compute

$c=H_l(m||R_x(G)||\ R_x(Q)||\ R_x(R_1)||...||\ R_x(R_l))$

compute,$c'$ $c'[i] = c[\sigma^{-1}(i)]$ $\xrightarrow{c'}$ $t_i = \begin{cases} r_i & \text{if } c'[i]=0 \\ r_i - x & \text{otherwise} \end{cases}$

verify $\xleftarrow{t_i}$

$$P_i = \begin{cases} a^{t_i} G & \text{if } c[i] = 0 \\ a^{t_i} Q & \text{otherwise} \end{cases}$$

compute $s_i = t_{\sigma(i)} + b_i, \quad 1 \le i \le l$

$(c, s_1, \Lambda, s_l)$ is a blind signature on *m*.

To verify the signature one needs to check whether $c=H(m||R_x(Q)||R_x(G)||a||t_1||...||t_l)$ with $t_i = \begin{cases} R_x(a^{s_i} G) & \text{if } c[i] = 0 \\ R_x(a^{s_i} Q) & \text{otherwise} \end{cases}$

Blind SKROOTLOG protocols based on elliptic curves BSKROO TLOG is similar to BSKLOGLOG described above, and we omit the details because of the limitation of space.

## 4.2 Our Scheme of Electronic Cash with Multiple Banks

In our scheme we consider all banks forming a group with the CB as group manager and all users also forming a group with a TTP as group manager. Our scheme is as follows.

**Setup:**

The TTP selects the parameters: an RSA public key pair $(n,e)$, an elliptic curve $E_{(a,b)}(GF(p))$ over $GF(p)$, a large prime $p$ at least 160 bits in length an element $G$ of $E_{(a,b)}(GF(p))$ with order $q$, a specified element $a$ of $Z_n^*$ with large order modulo both factors of $n$, an up bound $\lambda$ of the length of the keys, and a constant $\varepsilon$. The group public key of the user is $\Omega = (n,e,a, E_{(a,b)}(GF(p)), G, q, \lambda, \varepsilon)$. When a user U registers in TTP, sh/he gets a membership certificate and becomes a legal member of the user group. To do so, sh/he needs to perform the following protocol with the TTP.

| U | | TTP |
|---|---|---|
| $l_1 \in_R Z_{2^{\lambda-1}}$ | $\xrightarrow{a^{l_1}}$ | |
| compute $x = l_1 + l_2$ | $\xleftarrow{l_2}$ | $l_2 \in_R Z_{2^{\lambda-1}}$ |
| verify whether $x \in \{0,1,2,\Lambda, 2^{\lambda} - 1\}$ | | |
| if not repeat the above procedures. | | |
| $y = a^x, Z = (y \bmod q)G$ | | |
| | $\xrightarrow{y,Z,SPK\{(x): y=a^x \wedge x \in Z_{2^{\lambda-1}}\},\ commitment\ to\ z}$ | verify $y = a^{l_1+l_2}$, and $SPK\{(x): y = a^x \wedge x \in Z_{2^{\lambda-1}}\}$ |
| | $\xleftarrow{A}$ | If succeed, compute $A=(y+1)^d \bmod n$, add $(A.Z,y)$ to database. |

$A$ is the membership certificate of U, U has data$(A,x,y,Z)$.

The CB establishes the group of banks similar to the TTP esta- blishes the group of users. Let the group public key be $\Omega = (n', e', a', E_{(a,b)}(GF(p)), G, q, \lambda', \varepsilon')$. Similar to a user joining the group of users, a bank $B_i$ joins the group of banks and

gets its membership certificate $(V_i, v_i)$, $V_i = (y'+1)^{d'}$, $y_i' = a'^{v_i}$. $B_i$ has data $(V_i, v_i, y_i')$.

**The Withdrawal Protocol:**

A user $U(A,x,ID_U)$ has her/his account number in her/his bank $B_i$, $ID_U$ is the identity of user U in bank $B_i$. When U wants to withdraw an electronic coin, sh/he first perform a protocol with $B_i$ to authenticate her/his identity and account number. If succeed, U generates an electronic coin $m$ and gets the group blind signature of $B_i$ on m by perform the following protocol.

Bank $B_i$ selects $k \in_R Z_q^*$, let $G'=kG$, $Z'=y'G'$, $P_i^{LOG}=(a^{r_i} \bmod q)G'$, $P_i^{ROOT} = (r_i^{e'} \bmod q)G'$, and sends them to user U, U randomly chooses $b \in \{0,1,\Lambda\ ,2^{\lambda}-1\}$, $f \in Z_n^*$, let $w = (a' f)^{e'b}$ $modq, G''=wG', Z''=wZ', P''^{LOG}_i = wP_i^{LOG}, P''^{ROOT}_i = wP_i^{ROOT}$ be parameters in **BSKROOTLOG** and **BSKLOGLOG** execute the two blind signature schemes. .The resulting signature of $B_i$ on $m$ is $m(G'',Z'',S_1,S_2)$ where $S_1=SKLOGLOG[v_i : Z'' = a'^{v_i} G''](m)$, $S_2=SKROOTLOG[V_i:Z''G''=V_i^{e'}G''](m)$.

**Payment Protocol:**

For a user to pay for a shop sh/he needs to perform the following protocol with the shop.

**U** **Shop**

$\xrightarrow{m(G'',Z'',s_1,s_2)}$ verify the validity of the coin using the group public key of banks, if valid , then let $M=ID_{shop}||time$, *time* is the time of the transaction.

$\xleftarrow{M}$

sign on $M$ with key pair $(A,x)$
signature: $M(G',Z',S_1',S_2')$
where $G'=rG, Z'=yG'$ $r \in_R Z_p^*$
$S_1'=SKLOGLOG[x:Z'=a^xG'](M)$
$S_2'=SKROOTLOG[A:Z'G'=A^eG'](M)$

$\xrightarrow{M(G',Z',S_1',S_2')}$ verify U's group signature $M(G',Z',S_1',S_2')$ on $M$. if valid, send the merchandise to U

**Deposit protocol:**

Each bank has an on-line database of the list of spent coins which is issu-ed by the CB. This assures that each bank can check whether a coin is double spent.

When a Shop deposits in his bank $B_j$ an electronic coin $m(G'',Z'',S_1,S_2)$ he receives, he needs do the following: The shop sends the coin $m(G'',Z'', S_1,S_2)$and $M(G',Z',S_1',S_2')$ to $B_j$; $B_j$ verifies the validity of $m(G'',Z'',S_1,S_2)$; $B_j$ looks up in the on-line database of the list of spent coins to check whether this coin is double spending; if it is not double spending and there is no other problem with it, $B_j$ credits the shop's account the value of the coin.

**User tracing:**

The bank $B_j$ should send $m(G'',Z'',S_1,S_2)$ and $M(G',Z',S_1',S_2')$ to the CB if he finds the coin $m(G'',Z'',S_1,S_2)$ is double spent or there is some other problem. The

CB will find the bank $B_i$ who issued the coin $m(G'',Z'',S_1,S_2)$ using the open protocol of the group blind signature scheme. To do so B looks for the bank $B_i$ such that its $y_i'$ satisfying $y_i'G''=Z''$. When $B_i$ is found, the user or the double spender will be found by $B_i$ and TTP using the open protocol of group signature scheme.

## 4.3 Analysis of our scheme

Our system is mainly based on the techniques of group signatures and group blind signatures. Its security is based on RSA assumption and the problem of discrete logarithm over elliptic curves(ECDLP). The security properties of group signatures and group blind signatures assure that every procedure of our scheme is feasible and secure. The analysis of the security of our group signature scheme and group blind signature scheme is similar to the analysis in Cam97[4] and Lys98[14].

Since we make use of discrete logarithms over elliptic curves, the amount of computation and the amount of data need to be transferred are greatly decreased. The lengths of elements of the multiplicative groups in the schemes of Cam97[4] and Lys98[14] are required to be 800 bits, while in our scheme the order q of the cyclic subgroup of the elliptic curve group just needs to be at least 160 bits. Furthermore the speed of our scheme is much faster than that of the original group signature scheme of Cam97, and the lengths of signatures in our scheme are much shorter.

## 4.4 Weakness of Electronic cash Schemes with Multiple Banks

So far the research of group signatures is in theoretical, there is still some distance to practical use. Although we have used discrete logarithms over elliptic curves so that the amount of computation and the amount of data need to be transferred are greatly decreased, our scheme is not perfect. Because of the unforgeability of group signatures, in our scheme as well as in other schemes of electronic cash with multiple banks no illegal user can spend electronic coins not belonging to himself. But there is a problem: if dishonest users A and B collude such that A signs messages supplied by a shop with B's secret key and membership certificate, the shop will be cheated and A can double spend this coin or use this coin for criminal activities. When user tracing protocol is executed, it is B not A that is traced. If B revoked his membership before he told his secret key and membership certificate to A, this problem is really hard to solve. The reason resulting in this weakness is that so far there is no group signature scheme that can supply the function of secure member deletion. This weakness also exists in the electronic cash scheme of Traore[17]. In fact the group manager can issue CRLs(Certificate Revocation Lists) to publish the certificates and private keys of deleted group members. So the shop can check whether a user signs a message using a deleted certificate and private key. This method can get rid of the above weakness. However to do so the anonymity of the signatures of a deleted group member before his deletion will be removed.If we designed an effective group signature scheme with secure member deletion. then a fair electronic cash scheme without the above weakness can be designed using the ideas of this paper.

# 5. CONCLUSION

In real life, electronic cash issued by multiple banks is more practical than the one issued by a single bank. So it is necessary to do research on electronic cash systems with multiple banks. This paper has presented the first model for fair electronic cash with multiple banks and has designed a user traceable fair electronic cash scheme using the improved group signature scheme of Cam97[4] and blind group signature scheme of Lys98[14]. A weakness in the design of withdrawal and payment protocols of electronic cash scheme using the existing group signature schemes is pointed out with its reason analyzed. A way of removing this weakness is also suggested. Finally, two open problems in the research of fair electronic cash systems with multiple banks are presented.

# 6. ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China under the reference number 69931010.

# 7. REFERENCES

[1] Giuseppe Ateeniese and Gene Tsudik, *Group signatures à la carte*, Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'99), January 1999. Available at http://www.isi.edu/~gts/pubs.html.

[2] Giuseppe Ateeniese and Gene Tsudik, *Some Open Issues and New Direction in Group Signatures*, Financial Cryptography (FC'99), February,1999. Available at http://www.isi.edu/~gts/pubs.html.

[3] S. Brands. *An efficient off-line electronic cash system based on the representation problem.* Technical Report CS-R9323, CWI (Centre for Mathematics and Computer Science), Amsterdam, 1993.

[4] Jan Camenisch and Markus Stadler, *Efficient group signature schemes for large groups,* in CRYPTO'97 (B.S. Kaliski Jr., ed.), LNCS-1294, Springer-Verlag, 1997, pp. 410-424.

[5] Jan Camenisch, J.M. Piveteau and A.M. Stadler, *Blind signatures Based on The Discrete Logarithm Problem,* in EUROCRYPT'92 Proceedings, pp.428-432, Springer-Verlag, 1992.

[6] Jan Camenisch, U. Maurer and A.M. Stadler, *Digital payment systems with passive anonymity-revoking trustee.* In Esorics'96 (LNCS-1146), Springer-Verlag, Italy 1996, pp. 33-43. Available at http://www.inf.cthz.ch/personal/camenisc/publications.html.

[7] Jan Camenisch, *Group signature scheme and payment systems based on the discrete logarithm problem,* 174 pages, Vol.2 of ETH-Series in Information Security and Cryptolography, 1998.

[8] D. Chaum, *Blind Signature for Untraceable Payments,* in UROCRYPT' 82 Proceedings, pp.199-203, Plenum Press, 1983.

[9] D. Chaum and E. van Heijst, *Group Signatures,* Proceedings of EUROCRYPT'91, LNCS-547, Springer-Verlag, pp. 257-265, 1991.

[10] J. Claessens, B. Preneel and J. Vandewalle, *Anonymity controlled electronic payment systems,* Proceedings of the 20th symposium on information theory in the benclux, Haasrode, Belgium, May 27-28 1999, pp. 109-116.

[11] Y. Frankel, Y. Tsiounis and M. Yung. *Indirect discourse proofs: achieving fair off-line e-cash.* in Asiacrypt'96 (LNCS-1163), pp. 286-300,Kyongju, South Korea, November 3-7 1996, Springer-Verlag.

[12] N. Koblitz, *Elliptic Curve Cryptosystems,* Mathematics of Computation, 48(1987), pp. 203-209.

[13] N. Koblitz, *Algebraic Aspects of Cryptography,* Algorithms and Computation in Math. Vol. 3, 1998.

[14] Anna Lysyanskays and Zulfikar Ramzan, *Group blind signatures: A scalable solution to electronic cash,* Financial Cryptography (FC'98) (R. Hirschfeld, ed.), LNCS-1465, Springer-Verlag, 1998, pp. 184-197.

[15] M. Stadler, J.M. Piveteau and Jan Camenisch, *Fair blind signatures,* Proceedings of EUROCRYPT'95, LNCS-921, pp. 209-219, Springer-Verlag.

[16] Y. Tsiounis, *Efficient electronic cash: new notions and techniques.* PhD thesis. College of Computer Sci, Northeastem University, Boston. MA. 1997. Available at http://www.ccs.neu.edu/home/yiannis/pubs.html.

[17] J. Traor, *Group signatures and their relevance to privacy-protecting off-line electronic cash systems,* Proceedings of the 4th Australasian conference on information security and privacy, Australia, April 1999, LNCS-1587, Springer-Verlag, pp. 228-243.