INFORMATICA, 2006, Vol. 17, No. 4, 551–564

An Electronic Cash System Based on Group Blind Signatures

Constantin POPESCU
Department of Mathematics and Computer Science, University of Oradea
Str. Universitatii 1, Oradea, Romania
e-mail: cpopescu@uoradea.ro

Received: February 2006

Abstract. One important requirement of electronic cash systems is the anonymity of customers. Unconditional anonymity is also very well suited to support criminals in blackmailing. Maitland and Boyd proposed at ICICS 2001 an offline electronic cash system based on a group signature scheme. Their scheme cannot be used to solve blackmailing and other anonymity problems such as money laundering and illegal purchases. Chen, Zhang and Wang suggested an offline electronic cash scheme to prevent blackmailing by using the group blind signature. In their payment system, they used a group signature scheme of Camenisch and Stadler for large groups which is not secure. In this paper we improve these electronic cash systems to prevent blackmailing, money laundering and illegal purchases by using a secure coalition-resistant group blind signature scheme.

Key words: cryptography, electronic cash system, blackmailing, group blind signatures.

1. Introduction

Blackmailing is the most serious drawback of the known payment systems offering unconditional anonymity. Solms and Naccache (1992) showed that anonymity could be used for blackmailing or money laundering by criminals without revealing their identities. A blackmailer can receive blackmailed money from his victim so that neither the victim nor the bank are able to recognize the blackmailed coins later. Furthermore, blackmailed coins can be transferred anonymously via an unobservable broadcasting channel. This attack is called the perfect crime, as it is impossible to identify or trace the blackmailer. To solve anonymity of customers, electronic payment systems with revokable anonymity have been proposed in (Camenisch *et al.*, 1997; Juels, 1999; Lee *et al.*, 2002). Also, various electronic cash systems using group signature schemes have been proposed in (Lysyanskaya and Ramzan, 1998; Maitland and Boyd, 2001; Traore, 1999). (Traore, 1999) proposed a solution that combine a group signature scheme and a blind signature scheme in order to design a fair off-line electronic cash. Recently, Qiu *et al.* (2002) presented a new electronic cash system using a combination of a group signature scheme and a blind signature scheme. Canard and Traore (2003) and Choi *et al.* (2003) suggested that the Qiu's system does not provide the anonymity of the customers.In these payment systems trusted third parties are able to revoke the anonymity of the customers in case of suspicious transactions. When illegal acts like blackmailing are disclosed, the trusted third party can block various attacks on payment systems by tracing the coins or the customer.

Kugler and Vogt (2001) proposed an online payment system without trusted third parties to defeat blackmailing. Depending on the power of the blackmailer, blackmailing can be categorized as follows (see (Kugler and Vogt, 2001) for more details):

- Perfect crime: The blackmailer contacts the victim via an anonymous channel and threatens him to withdraw some coins which are chosen and blinded by the blackmailer. The blackmailer communicates only with the victim but cannot observe the victim's communication with the bank.
- Impersonation: The blackmailer gains access to the victim's bank account and withdraws coins by himself. The blackmailer communicates directly with the bank but cannot observe the victim's communications with the bank.
- Kidnapping: The blackmailer has physical over the blackmailed victim and withdraws the coins similar to the impersonation scenario. The blackmailer communicates directly with the bank and prevents the victim from communicating with the bank.

The main idea of the payment system in (Kugler and Vogt, 2001) is to defeat blackmailing by using marked coins. In this case, the bank can issue marked coins by using a different private key (marking key) instead of the normal private key to generate the undeniable signature (Chaum and van Antwerpen, 1989; Chaum, 1991). When the bank receives a coin, which was not generated with the normal private key, the bank has to check whether the coin has been created with a marking key. Based on this idea, Chen *et al.* (2003) suggested in (Chen *et al.*, 2003) an offline electronic cash scheme to prevent blackmailing by using the group blind signature. In their payment system, they used a group signature scheme of Camenisch and Stadler (1997) for large groups which is not secure. Ateniese (1999) proved that this group signature scheme does not satisfy the property of coalition-resistance. Maitland and Boyd (2001) proposed an offline electronic cash system based on the group signature scheme of Ateniese *et al.*(2000). Their scheme cannot be used to solve blackmailing and other anonymity problems such as money laundering and illegal purchases.

In this paper, we improve the electronic cash systems of Maitland and Boyd (2001) and Chen *et al.* (2003) to prevent blackmailing, money laundering and illegal purchases by using a practical and secure coalition-resistant group blind signature scheme (Popescu, 2003). To achieve our aims, an entity called supervisor and the bank form a group and a trusted party is the group manager. The second group is comprised by all customers who open a bank account. The trusted party is the second group manager. The supervisor would play the role of the bank in case of blackmailing and he would sign instead of the bank on the message of the criminals. However, the bank only accepts the cash signed by himself. When the blackmailed cash is deposited, the bank could distinguish it with the valid cash. Our electronic cash system satisfies all advantages mentioned in the electronic cash scheme of Kugler and Vogt without any unpractical assumptions.

The remainder of this paper is organized as follows. In the next section, we review some cryptographic tools necessary in the subsequent design of our payment system.

Then, we present our offline electronic payment system in Section 3. Furthermore, we discuss some some aspects of security and efficiency in Section 4. Finally, Section 5 concludes the work of this paper.

2. Cryptographic Tools

In this section, we review the properties of a group blind signature scheme and some techniques for proving knowledge of discrete logarithms.

2.1. *Group Blind Signatures*

Group signature schemes are a relatively recent cryptographic concept introduced by Chaum and van Heijst (1991). An application of a group signature scheme is electronic cash as was pointed out in (Choi *et al.*, 2003; Juels, 1999; Maitland and Boyd, 2001). In (Juels, 1999), several banks issue coins, but it is impossible for shops to find out which bank issued a coin that is obtained from a customer. The central bank plays the role of the group manager and all other banks issuing coins are group members. A group blind signature scheme (Popescu, 2001; Popescu, 2000) allows the members of a group to sign messages on behalf of the group such that the following properties hold:

1. Blindness of signatures: The signer (a group member) signs on group's behalf a message without knowing its content. Moreover, the signer should have no recollection of having signed a particular document even though he can verify that he did indeed sign it.
2. Unforgeability: Only group members are able to sign messages on behalf of the group.
3. Anonymity: Given a signature, identifying the actual signer is computationally hard for everyone but the group manager.
4. Unlinkability: Deciding whether two different signatures were computed by the same group member is computationally hard.
5. Traceability: The group manager can always establish the identity of the member who issued a valid signature.
6. No framing: Even if the group manager and some of the group members collude, they cannot sign on behalf of non-involved group members.
7. Coalition-resistance: A colluding subset of group members cannot generate a valid signature that the group manager cannot link to one of the colluding group members.

2.2. *Signatures of Knowledge*

We present some well studied techniques for proving knowledge of discrete logarithms (for more details see (Camenisch and Michels, 1998)).

Signatures of knowledge were used by Camenisch and Michels (1998) and their construction is based on the Schnorr signature scheme (Schnorr, 1991) to prove knowledge.

A signature of knowledge is a construct that uniquely corresponds to a given message m that cannot be obtained without the help of a party that knows a secret such that as the discrete logarithm of a given $y \in G$ to the base g ($G =< g >$). We assume a collision-resistant hash function (à la Fiat–Shamir (Fiat and Shamir, 1987)) $H : \{0,1\}^* \rightarrow \{0,1\}^k$ which maps a binary string of arbitrary length to a k-bit hash value.

Let G be a cyclic subgroup of $\mathbb{Z}_n^*$ of order $\#G$, $\lceil \log_2(\#G) \rceil = l_G$. Let $\epsilon > 1$ be a security parameter. We use the symbol $\|$ to denote the concatenation of two binary string (or of the binary representation of group elements and integers).

Showing the knowledge of a discrete logarithm (Camenisch and Michels, 1998) can be done easily as stated by the following definition.

Definition 1 *Let $y, g \in G$. A pair $(c, s) \in \{0,1\}^k \times \pm\{0,1\}^{\epsilon(l_G+k)+1}$ satisfying $c = H(m \parallel g \parallel y \parallel g^s y^c)$ is a signature of knowledge of the discrete logarithm of $y = g^x$ with respect to base g, on a message $m \in \{0,1\}^*$ and is denoted $SPK\,\{(x) : y = g^x\}\,(m)$.*

A slight modification of the previous definition enables to show the knowledge and equality of two discrete logarithms as is described in (Camenisch and Michels, 1998).

Definition 2 *Let $g, h, y_1, y_2 \in G$. A pair $(c, s) \in \{0,1\}^k \times \pm\{0,1\}^{\epsilon(l_G+k)+1}$ satisfying $c = H(m \parallel g \parallel h \parallel y_1 \parallel y_2 \parallel y_1^c g^s \parallel y_2^c h^s)$ is a signature of knowledge of the discrete logarithm of both $y_1 = g^x$ with respect to base g and $y_2 = h^x$ with respect to base h, on a message $m \in \{0,1\}^*$ and is denoted $SPK\,\{(x) : y_1 = g^x \wedge y_2 = h^x\}\,(m)$.*

The next block is based on a proof that the secret the prover knows lies in a given interval. This building block is related to the new Range Bounded Commitment protocol (RBC) of Chan et al. (1998). It is also related to a protocol given by Camenisch and Michels (1998).

Definition 3 *Let $y, g \in G$. A pair $(c, s) \in \{0,1\}^k \times \pm\{0,1\}^{\epsilon(l+k)+1}$ satisfying $c = H(m \parallel g \parallel y \parallel g^{s-cX} y^c)$ is a signature of knowledge of the discrete logarithm $\log_g y$ that lies in the interval $]X - 2^{\epsilon(l+k)}, X + 2^{\epsilon(l+k)}[$, on a message $m \in \{0,1\}^*$.*

3. Our Offline Electronic Cash System

In this section we improve the electronic cash systems of Maitland and Boyd (2001) and Chen *et al.* (2003) to prevent blackmailing, money laundering and illegal purchases by using a practical and secure coalition-resistant group blind signature scheme (Popescu, 2003). Also, we use a group signature scheme proposed by Ateniese *et al.* (2000). The system is modelled by six types of participants: customers, blackmailers, merchants, banks, supervisors and trusted parties. The customers honestly withdraw money from the bank and pay money to the merchant. The merchants get money from customers and deposit it in the bank. The banks manage customer accounts, issue and redeem money. The bank can legally trace a dishonest customer with the help of the trusted parties.

A supervisor and a bank form the first group and a trusted party acts as the first group manager (GM1). All customers who open a bank account form the second group and a trusted party is the second group manager (GM2). When a customer, who shares a secret with the bank, wants to withdraw electronic coin m from his account, the bank applies a group blind signature protocol to m and decreases appropriate amount from the customer's account. Everyone including the merchant can verify the validity of group blind signature with the public key of the group.

If a blackmailer kidnaps a customer and forces the bank to sign the coin m, the supervisor, instead of the bank, applies a group blind protocol to m . The blackmailer cannot detect the coin was marked by supervisor. When the merchant deposits the marked coins in the bank, the bank can verify the coin is not signed by himself. Thus, the bank can detect all marked coins.

3.1. *System Setup*

The first group manager (GM1) executes the next steps to setup parameters of the group comprised of the bank and the supervisor:

1. Let k, l_p and $\epsilon > 1$ be security parameters and let $\lambda_1, \lambda_2, \gamma_1, \gamma_2$ denote lengths satisfying $\lambda_1 > \epsilon(\lambda_2 + k) + 2, \lambda_2 > 4l_p, \gamma_1 > \epsilon(\gamma_2 + k) + 2$ and $\gamma_2 > \lambda_1 + 2$. Define the integral ranges $\Lambda =]2^{\lambda_1} - 2^{\lambda_2}, 2^{\lambda_1} + 2^{\lambda_2}[$ and $\Gamma =]2^{\gamma_1} - 2^{\gamma_2}, 2^{\gamma_1} + 2^{\gamma_2}[$.
2. Select random secret l_p-bit primes p', q' such that $p = 2p' + 1$ and $q = 2q' + 1$ are prime. Set the modulus $n = pq$. It is a good habit to restrict operation to the subgroup of quadratic residues modulo n, i.e., the cyclic subgroup $QR(n)$ generated by an element of order $p'q'$. This is because the order $p'q'$ of $QR(n)$ has no small factors.
3. Choose random elements $a, a_0, g, h \in QR(n)$ of order $p'q'$.
4. Choose a random secret element $x \in \mathbb{Z}^*_{p'q'}$ and set $y = g^x \bmod n$.
5. Finally, let H be a collision-resistant hash function $H : \{0,1\}^* \rightarrow \{0,1\}^k$.
6. The group public key is $P = (n, a, a_0, H, y, g, h, l_G, \lambda_1, \lambda_2, \gamma_1, \gamma_2)$.
7. The corresponding secret key is $S = (p', q', x)$. This is the GM1's secret key.

The second group manager (GM2) executes the same steps as GM1 to setup parameters of the customers group with the following modifications:

1. Choose random elements $a', a_0, g', h \in QR(n)$ of order $p'q'$.
2. Choose a random secret element $x' \in \mathbb{Z}^*_{p'q'}$ and set $y' = g'^{x'} \bmod n$.
3. The group public key is $P' = (n, a', a_0, H, y', g', h, l_G, \lambda_1, \lambda_2, \gamma_1, \gamma_2)$.
4. The corresponding secret key is $S' = (p', q', x')$. This is GM2's secret key.

3.2. *Join the Group*

We assume that communication between the group member and the group manager is secure, i.e., private and authentic.

3.2.1. *The Bank and the Supervisor*

To obtain his membership certificate, each user U_i (the supervisor and the bank) must perform the following protocol with GM1:

1. Generates a secret key $x_i \in \Lambda$. The corresponding public key is $C_2 = a^{x_i} \bmod n$. The user U_i also proves to GM1 that the discrete logarithm of C_2 with respect to base a lies in the interval Λ (see definition 3).
2. GM1 sends U_i the new membership certificate (A_i, e_i), where e_i is a random prime chosen by GM1 such that $e_i \in \Gamma$ and A_i has been computed by GM1 as $A_i = (C_2 a_0)^{1/e_i} \bmod n$.
3. The GM1 creates a new entry in the membership table and stores (A_i, e_i) in the new entry.

3.2.2. *The Customers*

To obtain his membership certificate, each customer $Cust_i$ must perform the following protocol with GM2:

1. Generates a secret key $x_i'' \in \Lambda$. The corresponding public key is $C_2' = a'^{x_i''} \bmod n$. The user $Cust_i$ also proves to GM2 that the discrete logarithm of C_2' with respect to base a' lies in the interval Λ (see definition 3).
2. GM2 sends $Cust_i$ the new membership certificate (A_i', e_i'), where e_i' is a random prime chosen by GM2 such that $e_i' \in \Gamma$ and A_i' has been computed by GM2 as $A_i' = (C_2' a_0)^{1/e_i'} \bmod n$.
3. The GM2 creates a new entry in the membership table and stores (A_i', e_i') in the new entry.

3.3. *The Blinding Protocol*

The protocol for obtaining a group blind signature is as follows. The signer (the bank and the supervisor) does the following:

1. Computes:

$$\tilde{A} = A_i y^{x_i} \,(\bmod n)\,,\ \tilde{B} = g^{x_i} \,(\bmod n)\,,\ \tilde{D} = g^{e_i} h^{x_i} \,(\bmod n)\,. \tag{1}$$

2. Chooses random values $\tilde{r_1} \in \pm\{0,1\}^{\epsilon(\gamma_2+k)}$, $\tilde{r_2} \in \pm\{0,1\}^{\epsilon(\lambda_2+k)}$, $\tilde{r_3} \in \pm\{0,1\}^{\epsilon(\gamma_1+2l_p+k+1)}$, $\tilde{r_4} \in \pm\{0,1\}^{\epsilon(2l_p+k)}$ and computes:

$$\tilde{t_1} = \tilde{A}^{\tilde{r_1}} / \left(a^{\tilde{r_2}} y^{\tilde{r_3}}\right),\ \tilde{t_2} = \tilde{B}^{\tilde{r_1}}/g^{\tilde{r_3}},\ \tilde{t_3} = g^{\tilde{r_4}}, \tilde{t_4} = g^{\tilde{r_1}} h^{\tilde{r_4}}. \tag{2}$$

3. Sends $(\tilde{A}, \tilde{B}, \tilde{D}, \tilde{t_1}, \tilde{t_2}, \tilde{t_3}, \tilde{t_4})$ to the user.

In turn, the user does the following:

1. Chooses $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \delta \in_R \{0,1\}^{\epsilon(l_p+k)}$ and computes:

$$t_1 = a_0^{\delta} \tilde{t_1} \tilde{A}^{\alpha_1 - \delta 2^{\gamma_1}} / (a^{\alpha_2 - \delta 2^{\lambda_1}} y^{\alpha_3}),\ t_2 = \tilde{t_2} \tilde{B}^{\alpha_1 - \delta 2^{\gamma_1}} / g^{\alpha_3}, \tag{3}$$

$$t_3 = \tilde{t_3} \tilde{B}^{\delta} g^{\alpha_4},\ t_4 = \tilde{t_4} \tilde{D}^{\delta} g^{\alpha_1} h^{\alpha_4}. \tag{4}$$

2. Computes:

$$c = H(m \| g \| h \| y \| a_0 \| a \| \tilde{A} \| \tilde{B} \| \tilde{D} \| t_1 \| t_2 \| t_3 \| t_4), \tag{5}$$

$$\tilde{c} = c - \delta. \tag{6}$$

3. Sends $\tilde{c}$ to the signer.

The signer does the following:

1. Computes:

$$\tilde{s_1} = \tilde{r_1} - \tilde{c}(e_i - 2^{\gamma_1}),\ \tilde{s_2} = \tilde{r_2} - \tilde{c}(x_i - 2^{\lambda_1}), \quad (7)$$

$$\tilde{s_3} = \tilde{r_3} - \tilde{c}e_i x_i,\ \tilde{s_4} = \tilde{r_4} - \tilde{c}x_i. \quad (8)$$

2. Sends $(\tilde{s_1}, \tilde{s_2}, \tilde{s_3}, \tilde{s_4})$ to the user.

The user does the following:

1. Computes:

$$s_1 = \tilde{s_1} + \alpha_1,\ s_2 = \tilde{s_2} + \alpha_2,\ s_3 = \tilde{s_3} + \alpha_3, \quad (9)$$

$$s_4 = \tilde{s_4} + \alpha_4,\ A = \tilde{A}^{H(c\|s_1\|s_2\|s_3\|s_4)} \bmod n, \quad (10)$$

$$B = \tilde{B}^{H(c\|s_1\|s_2\|s_3\|s_4)} \bmod n, D = \tilde{D}^{H(c\|s_1\|s_2\|s_3\|s_4\|A\|B)} \bmod n. \quad (11)$$

2. The resulting group blind signature of a message m is $(c, s_1, s_2, s_3, s_4, A, B, D)$.

3.4. *The Withdrawal Protocol*

The withdrawal protocol involves the customers and the bank. It is very important for the blackmailed user to notify the bank the blackmailing without being detected by blackmailer (for more details see (Chen *et al.*, 2003)). When a customer opens an account in the bank, he shares a secret with the bank to authenticate his identity for future withdrawal. Suppose the shared secret is $s = k_1 \parallel k_2$ and an agreed symmetric algorithm E_K with the key K.

When a legitimate customer wants to withdraw a coin m from his account, the bank firstly sends him two random messages m_1, m_2. The customer then computes $(E_{k_1}(m_1),\ E_{k_2}(m_2))$ and sends the pair to the bank. The bank uses the agreed symmetric algorithm with keys k_1, k_2 to decrypt the pair $(E_{k_1}(m_1), E_{k_2}(m_2))$. Suppose the decrypted messages are (n_1, n_2). We have three possibilities:

a) If $n_1 \neq m_1$ then the bank rejects to serve for the customer. The withdrawal protocol is invalid and ends.

b) If $n_1 = m_1$ and $n_2 = m_2$ then the bank knows that the customer is the owner of the account. The bank applies the above group blind signature protocol to sign the coin m.

c) If $n_1 = m_1$ and $n_2 \neq m_2$, then the bank is convinced that the customer is controlled by a blackmailer. Suppose that this blackmailer forces the customer to reveal his secret shared with the bank. Then, the customer tell the blackmailer the secret is $s' = k_1 \parallel k_2'$, while his true secret is $s = k_1 \parallel k_2$. Then the supervisor mark the coin m, created by blackmailer, by applying the group blind protocol to the coin m. Suppose that the resulting group blind signature is $\sigma = (c, s_1, s_2, s_3, s_4, A, B, D)$. The blackmailer can verify the validity of the group blind signature σ but cannot detect the coin was marked by supervisor.

3.5. *The Payment Protocol*

The payment protocol involves the customers and the merchant.

1. The merchant first verifies the validity of the group blind signature $\sigma = (c, s_1, s_2, s_3, s_4, A, B, D)$ with the public key P as follows:
   a) Computes:

$$\begin{aligned} b_1 &= 1/H(c\|s_1\|s_2\|s_3\|s_4), && (12)\\ b_2 &= 1/H(c\|s_1\|s_2\|s_3\|s_4\|A\|B), && (13)\\ t_1' &= a_0^c A^{b_1(s_1-c2^{\gamma_1})}/(a^{s_2-c2^{\lambda_1}} y^{s_3}) \bmod n, && (14)\\ t_2' &= B^{b_1(s_1-c2^{\gamma_1})}/g^{s_3} \bmod n, && (15)\\ t_3' &= B^{cb_1} g^{s_4} \bmod n, && (16)\\ t_4' &= D^{cb_2} g^{s_1-c2^{\gamma_1}} h^{s_4} \bmod n, && (17)\\ c' &= H(m\|g\|h\|y\|a_0\|a\|A^{b_1}\|B^{b_1}\|D^{b_2}\|t_1'\|t_2'\|t_3'\|t_4'). && (18) \end{aligned}$$

   b) Accept the group blind signature if and only if:

$$\begin{aligned} &c = c', && (19)\\ &s_1 \in \pm\{0,1\}^{\epsilon(\gamma_2+k)+1}, \qquad s_2 \in \pm\{0,1\}^{\epsilon(\lambda_2+k)+1}, && (20)\\ &s_3 \in \pm\{0,1\}^{\epsilon(\lambda_1+2l_p+k+1)+1}, \quad s_4 \in \pm\{0,1\}^{\epsilon(2l_p+k)+1}. && (21) \end{aligned}$$

2. The customer computes $m' = H(c\|s_1\|s_2\|s_3\|s_4\|A\|B\|D)$ and signs m' using the group signature scheme proposed by Ateniese *et al.* (2000):
   (a) Chooses a random integer $w' \in \{0,1\}^{2l_p}$ and computes:

$$T_1 = A_i' y'^{w'} \,(\bmod n)\,, T_2 = g'^{w'} \,(\bmod n)\,, T_3 = g'^{e_i'} h'^{w'} \,(\bmod n)\,.(22)$$

   (b) Randomly chooses:

$$\begin{aligned} &r_1 \in \pm\{0,1\}^{\epsilon(\gamma_2+k)}, \qquad r_2 \in \pm\{0,1\}^{\epsilon(\lambda_2+k)}, && (23)\\ &r_3 \in \pm\{0,1\}^{\epsilon(\gamma_1+l_p+k+1)}, \quad r_4 \in \pm\{0,1\}^{\epsilon(2l_p+k)}. && (24) \end{aligned}$$

   (c) Computes:

$$d_1 = T_1^{r_1}/(a'^{r_2} y'^{r_3}), d_2 = T_2^{r_1}/g'^{r_3}, d_3 = g'^{r_4}, d_4 = g'^{r_1} h^{r_4}. \qquad (25)$$

   (d) Computes:

$$\begin{aligned} c_1 &= H(m'\|g'\|h\|y'\|a_0\|a'\|T_1\|T_2\|T_3\|d_1\|d_2\|d_3\|d_4), && (26)\\ s_1' &= r_1 - c_1(e_i' - 2^{\gamma_1}),\ s_2' = r_2 - c_1(x_i'' - 2^{\lambda_1}), && (27)\\ s_3' &= r_3 - c_1 e_i' w',\ s_4' = r_4 - c_1 w'. && (28) \end{aligned}$$

   (e) The resulting group signature of a message m' is $(c_1,s'_1,s'_2,s'_3,s'_4,T_1,T_2,T_3)$.

3. The customer sends the merchant the group signature $(c_1, s'_1, s'_2, s'_3, s'_4, T_1, T_2, T_3)$ of the message m'.
4. The merchant verifies the group signature $(c_1, s'_1, s'_2, s'_3, s'_4, T_1, T_2, T_3)$ of the message m' with public key P' as follows:

   (a) Computes:

$$d'_1 = a_0^{c_1} T_1^{s'_1 - c_1 2^{\gamma_1}} / (a'^{s'_2 - c_1 2^{\lambda_1}} y'^{s'_3}) \bmod n, \tag{29}$$
$$d'_2 = T_2^{s'_1 - c_1 2^{\gamma_1}} / g'^{s'_3} \bmod n, \tag{30}$$
$$d'_3 = T_2^{c_1} g'^{s'_4} \bmod n, \tag{31}$$
$$d'_4 = T_3^{c_1} g'^{s'_1 - c_1 2^{\gamma_1}} h^{s'_4} \bmod n, \tag{32}$$
$$c'_1 = H(m' \| g' \| h \| y' \| a_0 \| a' \| T_1 \| T_2 \| T_3 \| d'_1 \| d'_2 \| d'_3 \| d'_4). \tag{33}$$

   (b) Accept the group signature if and only if:

$$c_1 = c'_1, \tag{34}$$
$$s'_1 \in \pm\{0,1\}^{\epsilon(\gamma_2+k)+1}, \qquad s'_2 \in \pm\{0,1\}^{\epsilon(\lambda_2+k)+1}, \tag{35}$$
$$s'_3 \in \pm\{0,1\}^{\epsilon(\gamma_1+l_p+k+1)+1}, \quad s'_4 \in \pm\{0,1\}^{\epsilon(2l_p+k)+1}. \tag{36}$$

3.6. *The Deposit Protocol*

The deposit protocol involves the merchant and the bank as follows:

1. The merchant sends to the bank the group signature $(c_1, s'_1, s'_2, s'_3, s'_4, T_1, T_2, T_3)$ on the message m'.
2. The bank first verifies the validity of the group signature $(c_1, s'_1, s'_2, s'_3, s'_4, T_1, T_2, T_3)$ using the same operations as the merchant (see Step 4 from Subsection 3.5).
3. If the group signature $(c_1, s'_1, s'_2, s'_3, s'_4, T_1, T_2, T_3)$ is valid, the bank verifies the validity of the group blind signature $\sigma = (c, s_1, s_2, s_3, s_4, A, B, D)$ using the same operations as the merchant (see Step 1 from Subsection 3.5). Then the bank checks whether:

$$D = (g^{e_b} h^{x_b})^{H(c \| s_1 \| s_2 \| s_3 \| s_4 \| A \| B)} \bmod n. \tag{37}$$

   where e_b, x_b are membership keys of the bank. If this test fails but the group blind signature σ is valid the bank knows that m is a marked coin. In this case, the coin m can be rejected. If the group blind signature σ is valid, the test (37) succeeds and the coin m was not deposited before, the bank accepts the coin m and then the merchant sends the goods to the customer.

If the coin m was deposited before, double spending is found. Then the bank requests the GM2 that the identity of the dishonest customer to be revoked.

4. Security and Efficiency of our System

In this section we discuss some aspects of security and efficiency of our offline electronic cash system.

a) Unforgeability of coins: Every blackmailed coin can be distinguished by a different mark by applying a group blind signature to this coin. A dishonest supervisor cannot forge the coin. When a blackmailing happens, the bank notifies a supervisor to sign instead of him and gives him a proof. If the supervisor was not notified to mark a coin by the bank it can be deduced that the supervisor forged the coin. After a marked coin was detected, the GM1 can find out which supervisor issued the group blind signature $(c, s_1, s_2, s_3, s_4, A, B, D)$, by checking its correctness by using the Step 1 from Subsection 3.5. He aborts if the group blind signature is not correct. Otherwise, the GM1 computes:

$$A_i = \left(\frac{A}{B^x}\right)^{1/H(c\|s_1\|s_2\|s_3\|s_4)} \bmod n \tag{38}$$

and issues a signature:

$$SPK\left\{(x) : y = g^x \wedge A/A_i^{H(c\|s_1\|s_2\|s_3\|s_4)} = B^x\right\}(m) \tag{39}$$

(see Definition 2). He then looks up A_i in the group member list and will find the corresponding A_{sup} and the supervisor's identity, where A_{sup} is membership key of the supervisor. Also, from the property of a group blind signature, when different coins with the same marking were detected, the corresponding supervisor is identified and he answers for his dishonest actions. Furthermore, from the property of coalition-resistance of a group blind signature scheme, the bank will not collude with the supervisor, such that the issued group blind signature could not be open by the group manager.

b) Tracing of dishonest customers: To open a group signature $(c_1, s'_1, s'_2, s'_3, s'_4, T_1, T_2, T_3)$ and reveal the identity of the actual dishonest customer (e.g., double spender) who created a given group signature, the GM2 performs the following steps:

1. Verifies the validity of the group signature $(c_1, s'_1, s'_2, s'_3, s'_4, T_1, T_2, T_3)$ with public key P' using the same operations as the merchant (see Step 4 from Subsection 3.5).
2. Computes $A'_i = T_1/T_2^{x'} \bmod n$ and issues a signature:

$$SPK\{(x') : y' = g'^{x'} \wedge T_1/A'_i = T_2^{x'}\}(m') \tag{40}$$

   (see Definition 2) and recovery the identity of $Cust_i$. The GM2 looks up A'_i in the customer group member list and will find the corresponding $Cust_i$ and the customer's identity.

Also, since the GM2 knows the relation between customer's identification and the group public key, money laundering is prevented. When money laundering happens, the GM2 reveals the identity of dishonest customer using the above steps.

Table 1

Comparison of the Signature Size

E-cash Protocol	Modulus	Signatures
Chen, Zhang and Wang'protocol	1200 bit	3 KBytes
Our e-cash Protocol	1200 bit	1 KBytes

c) Tracing of the blackmailed customer: Every marked coin can be detected by the bank at deposit. This enables tracing of the blackmailed customer and allows rejection of marked coins. The second group manager (GM2) reveals the identity of the actual blackmailed customer using the steps in the case b). Also, the bank will reject the marked coin at deposit.

d) Anonymity of honest customers: Assuming that the group signature scheme and the group blind signature scheme are computationally secure and the symmetric algorithm E_K is strong, our system is secure against tracing a honest customer by the bank. If a customer receives unmarked coins at withdrawal, identifying the actual honest customer is computationally hard for everyone, but the GM2, due to the group signature. Also, since the group blind signature σ can not give any information for the coin m, the bank can not link the blind coin with the identity of the customer. If a customer receives marked coins at withdrawal, the second group manager (GM2) can legally trace this customer using the steps in the case b). Therefore, it is infeasible for the bank to trace honest customers without the help of the GM2.

e) Undetectability of marking: From the property of a group blind signature, it results that only the bank can detect whether a coin is marked or not. Furthermore, for other parties, even for the blackmailer, marked coins are indistinguishable from unmarked coins.

The security and efficiency of our offline electronic cash system follows from the security and efficiency of the underlying group signature scheme (Atheniese, 2000). It is possible to extend our electronic cash system in the case of the supervisor forges the coin. In this case, the first group manager (GM1) can expel a dishonest supervisor from the group, by using a method for revocation in a group signature scheme (Atheniese, 2002).

The computational and communicational costs for withdrawing and storing a coin do not depend on the number of times it can be spent. The costs in our electronic cash system depend on the signatures used. We compare the e-cash system of Chen–Zhang–Wang (see Table 1) which has a modulus of 1200 bits, $k = 160$ and $\epsilon = 7/6$ with our e-cash system which has a modulus of 1200 bits, $k = 160$ and $\epsilon = 7/6$. The size of the signatures in our e-cash system is 1 KBytes and 3 KBytes in the e-cash system of Chen–Zhang–Wang. Therefore, our electronic cash system is about three times more efficient than the scheme in (Chen, 2003), and signatures are about three times shorter when choosing the same modulus for both schemes. However, the e-cash scheme in (Chen, 2003) is based on a group signature scheme which is not secure (Atheniese, 1999). The efficiency of our electronic cash system is the same with the scheme of Maitland and Boyd (Maitland, 2001). But, our electronic cash system is resistant against blackmailing, money laundering and illegal purchases.

5. Conclusion

In this paper we proposed an offline electronic cash system based on a secure coalition-resistant group blind signature scheme. Our scheme is an extension of the electronic cash scheme of Maitland and Boyd. The main advantage of the proposed system is that our electronic cash system is resistant against blackmailing, money laundering and illegal purchases. Also, the main benefits of our offline electronic cash system, compared to the scheme of Chen–Zhang–Wang, relate to the underlying group signature scheme's improved efficiency and provable security.

References

Ateniese, G., G. Tsudik (1999). Some open issues and new directions in group signatures. In *Proceedings of Financial Cryptography (FC'99)*. Anguilla, British West Indies. pp. 196–211.

Ateniese, G., J. Camenisch, M. Joye, G. Tsudik (2000). A practical and provably secure coalition-resistant group signature scheme. In *Proceedings of Crypto 2000*. Santa Barbara, USA. pp. 255–270.

Ateniese, G., D. Song, G. Tsudik (2002). Quasi-efficient revocation in group signatures, *Proceedings of Financial Cryptography 2002*. Southampton, Bermuda.

Camenisch, J., U. Maurer, M. Stadler (1997). Digital payment systems with passive anonymity-revoking trustees. *Journal of Computer Security*, **5**(1), 254–265.

Camenisch, J., M. Stadler (1997). Efficient group signature schemes for large groups. In *Proceedings of Crypto'97*, Santa Barbara, USA. pp. 410–424.

Camenisch, J., M. Michels (1998). A group signature scheme with improved efficiency. In *Proceedings of Asiacrypt'98*. Beijing, China. pp. 160–174.

Canard, S., and J. Traore (2003). On fair e-cash systems based on group signature schemes. In *Proceedings of ACISP 2003*. pp. 237–248.

Chan, A., Y. Frankel, Y. Tsiounis (1998). Easy come – easy go divisible cash. In *Proceedings of Eurocrypt'98*. Helsinki, Finland. pp. 561–574.

Chaum, D., H. van Antwerpen (1989). Undeniable signatures. In *Proceedings of Crypto'89*. Santa Barbara, USA. pp. 212–216.

Chaum, D. (1991). Zero-knowledge undeniable signatures. In *Proceedings of Eurocrypt'90*. Aarhus, Denmark. pp. 458–464.

Chaum, D., E. Van Heijst (1991). Group signatures. In *Proceedings of Eurocrypt'91*. Brighton, UK. pp. 241–246.

Chen, X., F. Zhang, Y. Wang (2003). A new approach to prevent blackmailing in e-cash. In *Cryptology ePrint Archive*, Report 2003/055, available at `http://eprint.iacr.org`.

Choi, H., F. Zhang, K. Kim (2003). Electronic cash system based on group signatures with revokable anonymity. In *Proceedings of Workshop of Korea Information Security Institute*. pp. 29–34.

Fiat, A., A. Shamir (1987). How to prove yourself: practical solutions to identification and signature problems. In *Proceedings of Crypto'86*. Santa Barbara, USA. pp. 186–194.

Juels, A. (1999). Trustee tokens: simple and practical anonynous digital coin tracing. In *Proceedings of Financial Cryptography (FC'99)*. Anguilla, British West Indies. pp. 33–43.

Kugler, D., H. Vogt (2001). Marking: a privacy protecting approach against blackmailing. In *Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography*. Cheju Island, Korea. pp. 137–152.

Lee, M., G. Ahn, J. Kim, J. Park, B. Lee, K. Kim, H. Lee (2002). Design and implementation of an efficient fair off-line e-cash system based on elliptic curve discrete logarithm problem. *Journal of Communications and Networks*, **4**(2), 81–89.

Lysyanskaya, A., Z. Ramzan (1998). Group blind signature: a scalable solution to electronic cash. In *Proceedings of Financial Cryptography (FC'98)*. Anguilla, British West Indies. pp. 184–197.

Maitland, G., C. Boyd (2001). Fair electronic cash based on a group signature scheme. In *Proceedings of ICICS 2001*. Xian, China. pp. 461–465.

Popescu, C. (2000). An efficient group blind signature scheme based on the strong RSA assumption. *Romanian Journal of Information Science and Technology*, **3**(4), 365–374.

Popescu, C. (2001). A practical coalition-resistant group blind signature scheme. *Studia Universitatis Babes–Bolyai Informatica*,**XLVI**(1), 55–66.

Popescu, C. (2003). A secure and efficient group blind signature scheme. *Studies in Informatics and Control Journal*, **12**(4), 269–276.

Qiu, W., K. Chen, D. Gu (2002). A new off-line privacy protecting e-cash system with revokable anonymity. In *Proceedings of ISC 2002*. pp. 177–190.

Schnorr, C.P. (1991). Efficient signature generation for smart cards, *Journal of Cryptology*, **4**(3), 239–252.

von Solms, B., D. Naccache (1992). On blind signatures and perfect crimes. *Computers and Security*, **11**(6), 581–583.

Traore, J. (1999). Group signatures and their relevance to privacy-protecting off-line electronic cash systems. In *Proceedings of Information Security and Privacy*. Wollongong, Australia. pp. 228–243.

C. Popescu received the PhD degree in computer science (cryptography) at the Babes–Bolyai University, Cluj Napoca, Romania. Since 2005 he is a professor at the Department of Mathematics and Computer Science, University of Oradea, Romania. His research interests include cryptography, network security, group, security protocols and electronic payment systems.

Grupiniais aklais parašais pagrįsta elektroninių atsiskaitymų sistema

Constantin POPESCU

Vartotojų anonimiškumas yra vienas pagrindinių elektroninių atsiskaitymų sistemų reikalavimų. Tačiau besąlyginis anonimiškumas padeda nusikalstamumui ir šantažui. Maitland ir Boyd pasiūlė grupinių parašų schema pagrįstą elektroninių atsiskaitymų sistemą be prisijungimo. Jų schema negali būti naudojama šantažo ir kitų anonimiškumo problemų, kaip pinigų plovimas ir nelegalūs pirkimai, sprendimui. Apsisaugojimui nuo šantažo Chen, Zhang ir Wang pasiūlė elektroninių atsiskaitymų sistemą be prisijungimo panaudojant grupinius aklus parašus. Jų apmokėjimo sistemoje naudojama nesaugi Camenisch ir Stdler grupinių parašų schema didelėms grupėms. Šiame straipsnyje, apsisaugojimui nuo šantažo, pinigų plovimo ir nelegalių pirkimų, mes pageriname šias elektroninių atsiskaitymų sistemas panaudodami saugią koalicijoms atsparią aklų grupinių parašų schemą.