An Off-line Electronic Cash System with Revokable Anonymity

C. Popescu
University of Oradea, Department of Mathematics, Oradea, Romania
E-mail: cpopescu@uoradea.ro

Abstract—Many electronic cash systems have been proposed with the proliferation of the Internet and the activation of electronic commerce. Maitland and Boyd proposed at ICICS 2001 an offline electronic cash system based on a group signature scheme proposed by Ateniese, Camenisch, Joye and Tsudik. Their scheme cannot be used to solve blackmailing and other anonymity problems such as money laundering and illegal purchases. In this paper we extend the electronic cash system of Maitland and Boyd to prevent blackmailing, money laundering and illegal purchases by using a secure coalition-resistant group blind signature scheme.

I. INTRODUCTION

Von Solms and Naccache showed in [1] 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 [2], [3], [4]. 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. Fair electronic cash systems have been suggested independently by Brickell, Gemmel and Kravitz [5] and Stadler, Piveteau and Camenisch [6] as a solution to prevent blackmailing and money laundering. The efficiency and the security of the scheme in [5] have been later improved in [7]. Also, various fair electronic cash systems using group signature schemes have been proposed in [8], [9], [10]. Traore [10] 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. [11] presented a new electronic cash system using a combination of a group signature scheme and a blind signature scheme. Canard and Traore [12] and Choi, Zhang and Kim [13] suggested that the Qiu’s system does not provide the anonymity of the customers.

Kugler and Vogt [14] proposed an online payment system without trusted third parties to defeat blackmailing. Depending on the power of the blackmailer, blackmailing can be categorized as (see [14] for more details): perfect crime, impersonation, kidnapping. The main idea of the payment system in [14] is to defeat blackmailing using the marked coins. Based on this idea, Chen, Zhang and Wang suggested in [15] an on-line electronic cash scheme to prevent blackmailing by using a group blind signature scheme. Also, the authors in [16] proposed an off-line electronic cash system with multiple banks based on a group signature scheme. In both payment systems [15], [16], the authors used a group signature scheme of Camenisch and Stadler [17] for large groups which is not secure. Ateniese proved in [18] that this group signature scheme does not satisfy the property of coalition-resistance. Maitland and Boyd proposed in [9] an offline electronic cash system based on the group signature scheme of Ateniese, Camenisch, Joye and Tsudik [19]. Their scheme cannot be used to solve blackmailing and other anonymity problems such as money laundering and illegal purchases.

In this paper, we extend the electronic cash system of Maitland and Boyd [9] to prevent blackmailing, money laundering and illegal purchases by using a practical and secure coalition-resistant group blind signature scheme [20]. Our electronic cash system satisfies all advantages mentioned in the electronic cash scheme of Kugler and Vogt without any impractical assumptions.

II. OUR FAIR OFF-LINE E-CASH SYSTEM

In this section we improve the electronic cash system of Maitland and Boyd [9] to prevent blackmailing, money laundering and illegal purchases by using a secure coalition-resistant group blind signature scheme [20]. Also, we use the group signature scheme proposed by Ateniese, Camenisch, Joye and Tsudik [19]. 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 from his account, the bank applies a group blind signature protocol to 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 blackmailerkidnaps 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 markedcoins in the bank, the bank can verify the coin is not signed by himself. Thus, the bank can detect all markedcoins.

### A. 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 \( \lambda_1 > \epsilon(\lambda_2 + k) + 2, \lambda_2 > \gamma_2 + k \). 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 \( x \in Z_{p'q'}^* \) and set \( y = g^x \mod n \).

5. Finally, let \( H \) be a collision-resistant hash function \( H : \{0, 1\}^* \rightarrow \{0, 1\}^k \).

6. The group public key is \( P = (n, a, a_0, H, y, g, h, l_p, \lambda_1, \lambda_2, \gamma_1, \gamma_2) \).

7. The corresponding secret key is \( S = (p', q', x) \). This is 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 \( x' \in Z_{p'q'}^* \) and set \( y' = g^{x'} \mod n \).

3. The customers group public key is \( P' = (n, a', a_0, H, y', g', h, l_p, \lambda_1, \lambda_2, \gamma_1, \gamma_2) \).

4. The corresponding secret key is \( S' = (p', q', x') \). This is GM2’s secret key.

### B. Join the Group

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

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 \( C_2 = a^{x_i} \mod n \). The user \( U_i \) also proves to GM1 that the discrete logarithm of \( C_2 \) with respect to base \( a \) lies in the interval \( \Lambda \).

   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 \( A_i = (C_2^{a_i})^{1/e_i} \mod n \).

   3. The GM1 creates a new entry in the membership table and stores \( (A_i, e_i) \) in the new entry.

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 \( C'_2 = a^{x'_i} \mod n \). The user \( Cust_i \) also proves to GM2 that the discrete logarithm of \( C'_2 \) with respect to base \( a' \) lies in the interval \( \Lambda \).

   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 \( A'_i = (C'_2^{a'_i})^{1/e'_i} \mod n \).

   3. GM2 creates a new entry in the membership table and stores \( (A'_i, e'_i) \) in the new entry.

### C. The Blinding Protocol

The blinding protocol is performed by the bank or by the supervisor with the customer during the withdrawal protocol.

The protocol for obtaining a group blind signature of a coin \( m \) is as follows. The signer (the bank or the supervisor) does the following:

1. Computes
   \[
   \tilde{A} = A_i y^{x_i} \mod n \quad \text{and} \quad \tilde{B} = g^{x_i} \mod n, \]
   \[
   \tilde{D} = g^{x'_i} h^{x_i} \mod n. \]

2. Chooses random values \( \tilde{r}_1 \in \{0, 1\}^{(\gamma_2 + k)}, \tilde{r}_2 \in \{0, 1\}^{(\lambda_2 + k)}, \tilde{r}_3 \in \{0, 1\}^{(\gamma_1 + 2\lambda + 2k + 1)}, \tilde{r}_4 \in \{0, 1\}^{(2\lambda + k)} \) and computes:
   \[
   \tilde{t}_1 = A_i^{\tilde{r}_1} / (a^{\tilde{r}_2} y^{\tilde{r}_3}), \quad \tilde{t}_2 = \tilde{B}^{\tilde{r}_1} / g^{\tilde{r}_3}, \quad \tilde{t}_3 = \tilde{r}_3 \tilde{B} / g^{\tilde{r}_4}, \quad \tilde{t}_4 = \tilde{r}_4 \tilde{D} / g^{\tilde{r}_4}. \]

3. Sends \( (\tilde{A}, \tilde{B}, \tilde{D}, \tilde{t}_1, \tilde{t}_2, \tilde{t}_3, \tilde{t}_4) \) to the customer.

In turn, the customer does the following:

1. Randomly chooses \( \alpha_1, \alpha_2, \alpha_3, \alpha_4, \delta \in \{0, 1\}^{(l_p + k)} \) and computes:
   \[
   t_1 = a_0 \delta \tilde{t}_1 \tilde{A}^{\alpha_1} / (a^{\alpha_2} y^{\alpha_3}), \quad t_2 = \tilde{t}_2 \tilde{B}^{\alpha_1} / g^{\alpha_3}, \quad t_3 = \tilde{t}_3 \tilde{B} / g^{\alpha_4}, \quad t_4 = \tilde{t}_4 \tilde{D} / g^{\alpha_4}. \]

2. Computes
   \[
   c = H(m||g|h||y|a_0||\tilde{A}||\tilde{B}||\tilde{D}||t_1||t_2||t_3||t_4) \quad \text{and} \quad \tilde{c} = c - \delta. \]

3. Sends \( \tilde{c} \) to the signer.

The signer does the following:

1. Computes
   \[
   s_1 = \tilde{r}_1 - \tilde{c}(e_i - 2^{\gamma_1}), \quad s_2 = \tilde{r}_2 - \tilde{c}(x_i - 2^{\lambda_1}), \quad s_3 = \tilde{r}_3 - \tilde{c} e_i x_i, \quad s_4 = \tilde{r}_4 - \tilde{c} x_i. \]
2) Sends \((s_1, s_2, s_3, s_4)\) to the customer.
The customer does the following:

1) Computes
\[
\begin{align*}
s_1 &= \tilde{s}_1 + \alpha_1, \quad s_2 = \tilde{s}_2 + \alpha_2, \quad s_3 = \tilde{s}_3 + \alpha_3 \\
s_4 &= \tilde{s}_4 + \alpha_4, \quad A = \tilde{A}H(c || s_1 || s_2 || s_3 || s_4) \mod n, \\
B &= \tilde{B}H(c || s_1 || s_2 || s_3 || s_4) \mod n, \\
D &= \tilde{D}H(c || s_1 || s_2 || s_3 || s_4 || A || B) \mod n. 
\end{align*}
\]

2) The resulting group blind signature of the coin \(m\) is \((c, s_1, s_2, s_3, s_4, A, B, D)\).

D. 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 [15]). 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 \(s = k_1 || k_2\) and an agreed symmetric algorithm \(E_K\) with the key \(K\). In the case when a blackmailer forces the customer to reveal his secret shared with the bank, the customer tells the blackmailer that the secret is \(s' = k_1 || k_2'\), while his true secret is \(s = k_1 || k_2\). The blackmailer cannot distinguish the true secret from the false one.

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 blind protocol to sign the coin \(m\). The resulting group blind signature of the coin \(m\) is \(\sigma = (c, s_1, s_2, s_3, A, B, D)\). The customer gets the coin \(m\) from his account.

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. In this case, the bank notifies the supervisor to mark the coin \(m\) created by blackmailer by applying the group blind protocol to the coin \(m\). Suppose that the resulting group blind signature of the coin \(m\) is \(\sigma = (c, s_1, s_2, s_3, s_4, A, B, D)\). The blackmailer can validate the authenticity of the group blind signature \(\sigma\) but cannot detect the coin \(m\) was marked by supervisor. The blackmailer thus receives a coin \(m\) from the blackmailed customer’s account, not knowing whether it is marked or not. However, the bank will reject the marked coin \(m\) at deposit.

E. The Payment Protocol

The payment protocol involves the customers and the merchant.

1) The customer computes \(m' = H(m || c || s_1 || s_2 || s_3 || s_4 || A || B || D)\) and signs \(m'\) using the group signature scheme proposed by Ateniese, Camenisch, Joye and Tsudik [2]:

a) Chooses a random integer \(w' \in \{0, 1\}^{2l_p}\) and computes:
\[
\begin{align*}
T_1 &= \tilde{A}' g'^w' \mod n, \\
T_2 &= g'^w' \mod n, \\
T_3 &= g'^{d_1} h'^{w'} \mod n.
\end{align*}
\]

b) Randomly chooses:
\[
\begin{align*}
r_1 &\in \{0, 1\}^{(\gamma_2 + k)}, \quad r_2 \in \{0, 1\}^{(\gamma_3 + k)}, \\
r_3 &\in \{0, 1\}^{(\gamma_4 + p + k + 1)}, \quad r_4 \in \{0, 1\}^{(2l_p + k)}
\end{align*}
\]

C) Computes:
\[
\begin{align*}
d_1 &= T_1' / (a'^{r_1} g'^{r_2}), \\
d_2 &= T_2' / g'^{r_3}, \\
d_3 &= g'^{r_4}, \\
d_4 &= g'^{d_1} h'^{r_4}.
\end{align*}
\]

d) Computes:
\[
\begin{align*}
e_1 &= H(m' || g'|| h || y || a_0 || a'|| T_1 || T_2 || T_3 || d_1 || d_2 || d_3 || d_4), \\
e_2' &= r_1 - c_1 (e_1' - 2^{\gamma_1}), \\
e_2'' &= r_2 - c_2 (x_1' - 2^{\gamma_1}), \\
e_3' &= r_3 - c_3 e_1' w', \\
e_4' &= r_4 - c_4 w'.
\end{align*}
\]

e) The resulting group signature of a message \(m'\) is \((c_1, e_1', e_2', e_3', e_4', T_1, T_2, T_3)\).

2) The customer sends the group signature \((c_1, e_1', e_2', e_3', e_4', T_1, T_2, T_3)\) to the merchant.

3) The merchant verifies the group signature \((c_1, e_1', e_2', e_3', e_4', T_1, T_2, T_3)\) of the message \(m'\) with public key \(p'\) as follows:

a) Compute:
\[
\begin{align*}
d_1' &= a_0'' T_1'' / (a' e_2' - c_1 2^{\gamma_1} g'^{e_2'}), \\
d_2' &= T_2'' / g'^{e_3'}, \\
d_3' &= T_3'' g'^{e_4'}, \\
c_1' &= H(m' || g'|| h || y || a_0 || a'|| T_1 || T_2 || T_3 || d_1' || d_2' || d_3')
\end{align*}
\]

b) Accept the group signature if and only if:
\[
\begin{align*}
c_1 &= c_1', \\
s_1' &\in \{0, 1\}^{(\gamma_2 + k)}, \\
s_2' &\in \{0, 1\}^{(\gamma_3 + k)}, \\
s_3' &\in \{0, 1\}^{(\gamma_4 + p + k + 1)}, \\
s_4' &\in \{0, 1\}^{(2l_p + k)}.
\end{align*}
\]

F. The Deposit Protocol

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

1) The merchant sends to the bank the group signature \((c_1, e_1', e_2', e_3', e_4', T_1, T_2, T_3)\) on the message \(m'\).

2) The bank first verifies the validity of the group signature \((c_1, e_1', e_2', e_3', e_4', T_1, T_2, T_3)\) using the same operations as the merchant (see step 3 from subsection E).
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 \(\sigma = (c, s_1, s_2, s_3, s_4, A, B, D)\) of the coin \(m\) with the public key \(P\) as follows:

a) Compute:

\[
\begin{align*}
    b_1 &= 1/H(c || s_1 || s_2 || s_3 || s_4) \\
    b_2 &= 1/H(c || s_1 || s_2 || s_3 || s_4 || A || B) \\
    t'_1 &= a_0 B_{t_1} A_1 (s_1 - c_2^t) / (a_3 s_2 - c_2^t y^s) \mod n \\
    t'_2 &= B_{t_2} b_1 \mod n \\
    t'_3 &= B_{t_3} c_4 \mod n \\
    t'_4 &= D_{t_4} g_a^s \mod n \\
    c' &= H(m || g || h || a || A || t'_3) \\
\end{align*}
\]

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

\[
\begin{align*}
    c &= c' \\
    s_1 &\in \{0, 1\}^\epsilon (\gamma_2 + k) + 1, s_2 &\in \{0, 1\}^\epsilon (\lambda_2 + k) + 1 \\
    s_3 &\in \{0, 1\}^\epsilon (\lambda_1 + 2 p_r + k) + 1 \\
    s_4 &\in \{0, 1\}^\epsilon (2 p_r + k) + 1 \\
\end{align*}
\]

4) Then the bank checks whether:

\[
D = (g_a^s h^{x_4})^{H(c || s_1 || s_2 || s_3 || s_4 || A || B)} \mod n \tag{1}
\]

where \(e_b, x_b\) are membership keys of the bank. If this test fails but the group blind signature \(\sigma\) 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 \(\sigma\) is valid, the test in (1) 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 same coin \(m\) was deposited before, double spending is found and the bank requests the GM2 that the identity of the dishonest customer to be revoked.

### G. The Tracing Protocol

The bank can legally trace the customer of a paid coin with the help of the second group manager (GM2). The bank sends the group signature \((c_1, s'_1, s'_2, s'_3, s'_4, T_1, T_2, T_3)\) to the GM2. 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 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 3 from subsection E).
2) Computes \(A'_1 = T_1/T_2' \mod n\) and generates a proof that:

\[
\log_B y' = \log_B T_1 / A'_1.
\]
3) Search through the group member list to get the identity of the customer \(Cust_{t_1}\) corresponding to \(A'_1\).

### III. Security and Efficiency Analysis

In this section we discuss some aspects of security and efficiency of our off-line electronic cash system. We will state the theorems and sketch the proofs, showing that the proposed system satisfies the following properties: unforgeability of coins, security against money laundering, anonymity of honest customer, undetectability of marked coins and security against blackmailed bank.

#### Theorem 1: If the group blind signature scheme is secure against forgery and the hash function \(H\) is collision-resistant, the e-cash system is secure against forgery of the coin.

**Proof:** Every blackmailed coin can be distinguished by a different mark by applying a group blind signature to this coin. Since the group blind signature scheme is secure against forgery, this allows only the legal bank (and the supervisor when is notified by the bank to sign a coin) to generate the blind signature for the coin \(m\). As the hash function \(H\) is collision-resistant, the customer cannot forge the coin \(m\). Also, a dishonest supervisor cannot forge the coin \(m\). When a blackmailing happens, the bank notifies a supervisor to sign the coin \(m\), instead of him, and gives him a proof. If the supervisor was not notified to mark a coin \(m\) by the bank it can be deduced that the supervisor forged the coin \(m\). After a marked coin \(m\) 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 same operations as the bank (see step 3 from subsection F). He aborts if the group blind signature is not correct. Otherwise, the GM1 computes

\[
A_i = (A/B)^{k_1/H(c || s_1 || s_2 || s_3 || s_4)} \mod n
\]

and generates a proof that:

\[
\log_B y = \log_B A_i^{H(c || s_1 || s_2 || s_3 || s_4)}
\]

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 (GM1).

#### Theorem 2: Assuming that the group signature scheme and the group blind signature scheme are computationally secure, the e-cash system is secure against money laundering.

**Proof:** Every marked coin can be detected by the bank at deposit. This enables tracing of the blackmailed customer and allows rejection of marked coins. Also, since the group manager (GM2) know the relation between customer’s identification and his secret key, money laundering is prevented. When money laundering happens, the GM2 reveal the identity of dishonest customer using the tracing protocol.

\[
\text{log}_y y' = \text{log}_B T_1/A'_1
\]
Theorem 3: The e-cash system achieves anonymity with respect to the bank, that is, it is infeasible for the bank to trace legal customers without the help of the GM2.

Proof: 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 scheme. Also, since the group blind signature $\sigma$ can not give any information for the coin $m$, the bank can not link the blind coin with the identity of the customer. Therefore, it is infeasible for the bank to trace honest customers without the help of the GM2. ■

Theorem 4: Assuming that the group blind signature scheme are computationally secure, the e-cash system is secure against detectability of marked coins.

Proof: From the property of a group blind signature scheme, 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. Also, no one can obtain a blinded coin without the bank’s knowledge that this particular coin has been blinded. If the customer knows two valid group blind signatures only after one interaction with the bank, this contradicts the unforgeability of group blind signature scheme.

Theorem 5: The e-cash system is secure in the case when the bank is blackmailed.

Proof: If the blackmailer threatens the bank to reveal his signing key $(A_b, c_b, x_b)$ to him, the bank sends the signing key $(\hat{A}_{b\sup}, c_{b\sup}, x_{b\sup})$ of the supervisor to the blackmailer. The blackmailer can not distinguish the signing keys. If the blackmailer signs the coin $m$ with the signing key $(\hat{A}_{b\sup}, c_{b\sup}, x_{b\sup})$ of the supervisor, the bank will detect the marked coin $m$ at deposit and reject it. ■

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. Compared to the scheme in [15], our electronic cash system is about three times more efficient and signatures are about three times shorter when choosing the same modulus for both schemes. However, the e-cash scheme in [15] is based on a group signature scheme which is not secure [18].

IV. CONCLUSION

In this paper we proposed an off-line e-cash system based on a secure coalition-resistant group blind signature scheme. Comparing with e-cash system proposed by Maitland and Boyd, our e-cash system is resistant against blackmailing, money laundering and illegal purchases. Also, the main benefits of our off-line e-cash system, compared to the scheme of Chen-Zhang-Wang, relate to the underlying group signature scheme’s improved efficiency and provable security.

As a further work, we need to design an e-cash system that requires more efficiency computation and data store.

ACKNOWLEDGMENTS

The author would like to thank prof. Svein J. Knapskog and dr. Tønnes Brekke for valuable comments and discussions.

REFERENCES