International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 12, Issue 8 (August 2016), PP.46-53

An Off-line E-Cash Scheme based on Group Blind Signature Scheme

Israt Jahan[1]*, Kangkhita Keam Psyche[2] and Mithun Dutta[3]
[1,2,3]*Department of Computer Science and Engineering Jahangirnagar University, Savar, Dhaka, Bangladesh.*

Abstract: In t*his paper* we have *describe*d *the signature scheme inwhich an individual can sign a document ormessage onbehalf of entire group. Here, a group blind signaturescheme has been proposed*. *Our scheme combines the already existing notions of blind signatures and group signatures. It is an extension of Camenisch and Stadler'sGroup Signature Scheme [12] that adds the blindness property.One important requirement of electronic cash systems is the anonymity of customers.Unconditional anonymity is also very well suited to support criminals inblackmailing. Chen, Zhang and Wang suggested an offline electroniccash scheme[10] 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 launderingand illegal purchases by using a secure coalition-resistant group blind signature scheme.*

Keywords:*anonymity, blackmail, group blind signaturescheme*

I. INTRODUCTION

Blackmailing is the most serious drawback of the known payment systems offering unconditional anonymity. Solms and Naccache [2,10] 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 thevictim nor the banks are able to recognize the blackmailed coins later. Furthermore, blackmailedcoins 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 revocable anonymity have been proposed.Also, various electronic cash systems using group signature schemes have been proposedinInternational Conferences.

Traoreproposed a solution [14] that combines a group signature schemeand a blind signaturescheme in order to designing fair off-line electronic cash. Recently, Qiu*et*[15] presentedthe new electronic cash system using a combination of a group signature scheme and a blind signature scheme. Canard and Traore (2003) and Choi suggested[16] that the Qiu's system does not provide the anonymity of the customers.In these paymentsystems 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 trustedthird party can block various attacks on payment systems by tracing the coins or thecustomers.Kugler and Vogt proposed an online payment system [17] without trusted third parties to defeat blackmailing. Depending on the power of the blackmailer, blackmailing can be categorized as follows:

• Perfect crime: The blackmailer contacts the victim via an anonymous channel andthreatens 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.

II. BASIC MODEL

An anonymous off-line electronic cash system consists of three collections of probabilistic, polynomially-bounded parties, a bank *B*, users *U*, shops *S* and three main procedures [1]: withdrawal, payment and deposit (Figure 1). Users and shops maintain an account with bank, while

-*U* withdraws electronic coins from his account, by performing a withdrawal protocol with bank *B* over an authenticated channel.

-*U* spends a coin by participating in a payment protocol with a shop *S* over an anonymous channel and

-*S* performs a deposit protocol with the bank *B*, to deposit the user's coin into his account.

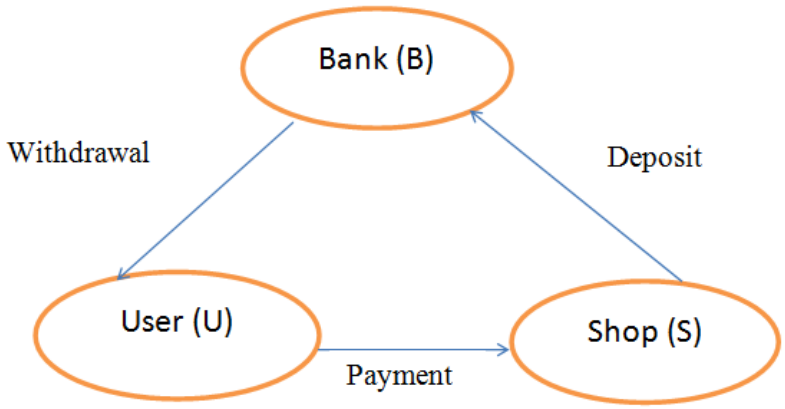

Fig.1: Basic model an anonymous off-line electronic cash system

III. GROUP BLIND SIGNATURE

Group Signatures preserve the anonymity of the signer. Blind Signatures preserve the privacy of the message to be signed. Group Blind Signatures combine properties of the above and thus preserve both the anonymity of the signer and theprivacy of the message. [18]The primitive which combines the properties of a blind signature and a group signature was introduced byLysyanskaya and Zulfikar [12].

IV. OUR OFF-LINE ELECTRONIC CASH SYSTEM

In this section we improve the electronic cash systems of Maitland and Boyd [19]and Chen. [20]to prevent blackmailing, money laundering and illegal purchases by using a practical and secure coalition-resistant group blind signature scheme. Also, we use a group signature scheme proposed by Ateniese[21]. The system is modeled 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 FirstGroup 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.

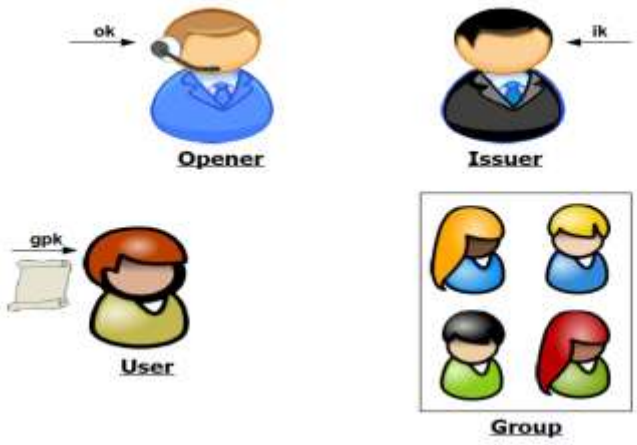

Fig 2.1: Group Blind Signature Schema

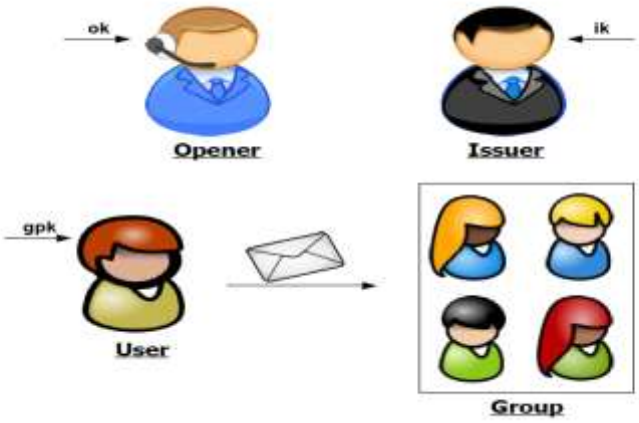

Fig 2.2: Group Blind Signature Schema

Fig 2.3: Group Blind Signature Schema

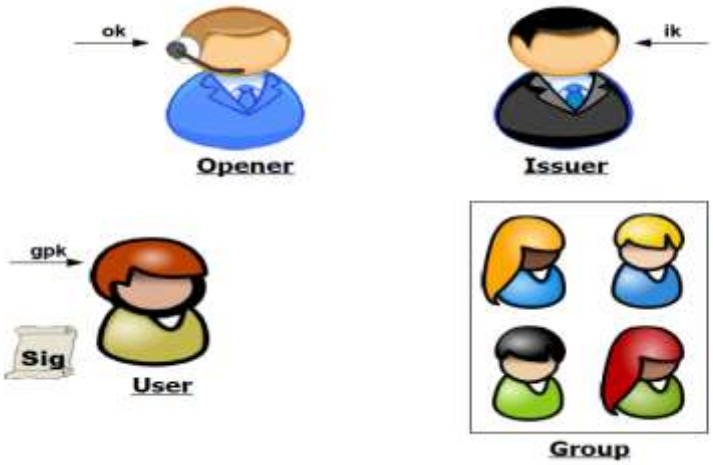

Fig 2.4: Group Blind Signature Schema

4.1 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 $\varepsilon>1$ be security parameters and let λ_1, λ_2, γ_1, γ_2 denote lengths satisfying $\lambda_1>\varepsilon(\lambda_2 + k) + 2$, $\lambda_2>4l_p$, $\gamma_1> \varepsilon(\gamma_2 + k) + 2$ 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 $x \in z^*_{p'q'}$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 $P = (n, a, a_0, H, y, g, h, l_G, \lambda_1, \lambda_2, \gamma_1, \gamma_2)$.
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 $x' \in z^*_{p'q'}$and set $y'=g'^{x'} mod n$.
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 the GM2's secret key.

4.2 Join the Group:

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

The Bank and the Supervisor*:*

To obtain his membership certificate, each userU_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 $C_2 = a^{xi} \bmod n$.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.
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 $A_i=(C_{2a0})^{1/ei} \bmod n$.
3. The GM1 creates a new entry in the membership table and stores $(A_{i,\ ei})$ in the new entry.

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 tobase a'lies in the interval Λ .
2. GM2 sends $Cust_i$ *the* new membership certificate (A'_i, e'_i), where $e'_i$is a random primechosen by GM2 such that $e'_i \in \Gamma$ and A'_ihas been computed by GM2 as $A'_i=(C'_{2a0})^{1/e'i} \bmod n$.
3. The GM2 creates a new entry in the membership table and stores (A'_i, e'_i) in the new entry.

4.3 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**

$\tilde{A}= A_i y^{xi} (\bmod n)$

$\tilde{B}= g^{xi} (\bmod n)$

$\tilde{D}= g^{ei} h^{xi} (\bmod n)$.

2. **Chooses random values**

$\tilde{r_1} \epsilon \pm\{0,1\}^{\varepsilon(\gamma_2+k)}$

$\tilde{r_2} \epsilon \pm\{0,1\}^{\varepsilon(\lambda_2+k)}$

$\tilde{r_3} \epsilon \pm\{0,1\}^{\varepsilon(\lambda_1+2l_p+k)}$

$\tilde{r_4} \epsilon \pm\{0,1\}^{\varepsilon(2l_p+k)}$
and computes
$\tilde{t_1}=\tilde{A}^{\tilde{r}_1}/\tilde{a}^{\tilde{r}_2}\tilde{y}^{\tilde{r}_3}$
$\tilde{t_2}=\tilde{B}^{\tilde{r}_1}/\tilde{g}^{\tilde{r}_3}$
$\tilde{t_3}=\tilde{g}^{\tilde{r}_4}$
$\tilde{t_4}=\tilde{g}^{\tilde{r}_1}\tilde{h}^{\tilde{r}_4}$

3. Sends $(\tilde{A},\tilde{B},\tilde{D},\tilde{t_1},\tilde{t_2},\tilde{t_3},\tilde{t_1})$ to the user. In turn, the user does the following:

1. Chooses $\alpha 1, \alpha 2, \alpha 3, \alpha 4, \delta \in_R \{0,1\}^{\varepsilon(l_p+k)}$ and computes:
$t_1 = a_0^{\delta}\,\tilde{t_1}\tilde{A}^{\alpha_1-\delta 2^{\gamma_1}}/(a^{\alpha_2-\delta 2^{\lambda_1}}\ y^{\alpha_3})$
$t_2 = \tilde{t_2}\tilde{B}^{\alpha_1-\delta 2^{\gamma_1}}/(g^{\alpha_3})$
$t_3 = \tilde{t_3}\tilde{B}^{\delta}g^{\alpha_4}$
$t_4 = \tilde{t_4}\tilde{D}^{\delta}g^{\alpha_1}h^{\alpha_4}$

2. Computes:
$c = H(m\|g\|h\|y\|a_0\|a\|\ \tilde{A}\ \|\ \tilde{B}\ \|\ \tilde{D}\ \|t_1\|t_2\|t_3\|t_4)$
$\tilde{c} = c - \delta$

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

The signer does the following:

1. Computes:
$\tilde{s_1} = \tilde{r_1} - \tilde{c}\,(e_i - 2^{\gamma_1})$
$\tilde{s_2} = \tilde{r_2} - \tilde{c}\,(x_i - 2^{\lambda_1})$
$\tilde{s_3} = \tilde{r_3} - \tilde{c}e_i x_i$
$\tilde{s_4} = \tilde{r_4} - \tilde{c}\,x_i$

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

The user does the following:

1. Computes:
$s_1 = \tilde{s_1} + \alpha_1$
$s_2 = \tilde{s_2} + \alpha_2$
$s_3 = \tilde{s_3} + \alpha_3$
$s_4 = \tilde{s_4} + \alpha_4$
$A = \tilde{A}^{H(c\|s_1\|s_2\|s_3\|s_4)} \mod n$
$B = \tilde{B}^{H(c\|s_1\|s_2\|s_3\|s_4)} \mod n$
$D = \tilde{D}^{H(c\|s_1\|s_2\|s_3\|s_4)} \mod n$

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

4.4 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 [3, 5]. 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.

When a legitimate customer wants to withdraw a coin m from his account, the bank firstly sends him two random messages $m1, m2$. The customer then computes $(E_{k1}(m_1), E_{k2}(m_2))$ and sends the pair to the bank. The bank uses the agreed symmetric
algorithm with keys k_1, k_2 to decrypt the pair $(E_{k1}(m_1), E_{k2}(m_2))$. 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 $s' = k_1 \| k_2'$ while his true secret is $s = k_1 \| k_2$. 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.

4.5 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:

$$b_1 = 1/H(c\|s_1\|s_2\|s_3\|s_4)$$

$$b_2 = 1/H(c\|s_1\|s_2\|s_3\|s_4\|A\|B)$$

$$t_1' = a_0^c A^{b_1(s_1 - c2\gamma_1)}/(a^{s_2 - c2^{\lambda_1}} \; y^{s_3}) \bmod n$$

$$t_2' = B^{b_1(s_1 - c2\gamma_1)}/g^{s_3} \bmod n$$

$$t_3' = B^{cb_1} g^{s_4} \bmod n$$

$$t_4' = D^{cb_2} g^{(s_1 - c2\gamma_1)} h^{s_4} \bmod n$$

$$c' = H(m\|g\|h\|y\|a_0\|a\|A^{b_1}\|B^{b_1}\|D^{b_2}\|t_1'\|t_2'\|t_3'\|t_4')$$

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

$$c = c'$$

$$s_1 \epsilon \pm \{0,1\}^{\varepsilon(\gamma_2 + k)+1}$$

$$s_2 \epsilon \pm \{0,1\}^{\varepsilon(\lambda_2 + k)+1}$$

$$s_3 \epsilon \pm \{0,1\}^{\varepsilon(\lambda_1 + 2l_p + k)+1}$$

$$s_4 \epsilon \pm \{0,1\}^{\varepsilon(2l_p + k)+1}$$

2. 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

3. (a) Chooses a random integer $w' \epsilon \{0,1\}^{(2l_p}$ and computes:

$$T1 = A_i' y'^{w'} \pmod n$$

$$T2 = g'^{w'} \pmod n$$

$$T3 = g'^{ei'} h'^{w'} \pmod n$$

(b) Randomly chooses:

$$r1 \epsilon \pm \{0,1\}^{\varepsilon(\gamma^2 + k)}$$

$$r2 \epsilon \pm \{0,1\}^{\varepsilon(\lambda 2 + k)}$$

$$r3 \epsilon \pm \{0,1\}^{\varepsilon(\lambda 1 + lp + k + 1)}$$

$$r4 \epsilon \pm \{0,1\}^{\varepsilon(2lp + k)}$$

(c) Computes:

$$d1 = T_1^{r1}/(a'^{r2} y'^{r3})$$

$$d2 = T_2^{r1}/g'^{r3}$$

$$d3 = g'^{r4}$$

$$d4 = g'^{r1} T'^{r4}$$

(d) Computes

$$c1 = H(m'\|g'\|h\|y'\|a0\|a'\|T_1\|T_2\|T_3\|d1\|d2\|d3\|d4)$$

$$s'1 = r1 - c1(e_i' - 2^{\gamma 1})$$

$$s'2 = r2 - c1(x_i'' - 2^{\lambda 1})$$

$$s'3 = r3 - c1 e_i' w'$$

$$s'4 = r4 - c1 w'.$$

(e) The resulting group signature of a message m′is (c1, s′1, s′2, s′3, s′4, T1, T2, T3).

4. The customer sends the merchant the group signature (c1, s′1, s′2, s′3, s′4, T1, T2, T3) of the message m′.

5. The merchant verifies the group signature (c1, s′1, s′2, s′3, s′4, T1, T2, T3) of the message m′with public key P′as follows:

(a) Compute:

$$d'1 = a_1^{c1} T_1^{s'_1 - c12\gamma 1} / (a'^{s'_2 - c12\lambda 1}_2 \; y'^{s'_3}_3) \bmod n$$
$$d'2 = T_2^{s'_1 - c12\gamma 1} / g'^{s'_3} \bmod n$$
$$d'3 = T_2^{c1} g'^{s'_4} \bmod n$$
$$d'4 = T_3^{c1} \; g'^{s'_1 - c12\square 1} h'^{s'_4} \bmod n$$
$$c'1 = H(m' \| g' \| h \| y' \| a0 \| a' \| T_1 \| T_2 \| T_3 \| d1 \| d2 \| d3 \| d4)$$

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

$$c1 = c'1$$
$$s'1 \; \epsilon \pm \{0, 1\}^{\varepsilon(\square 2+k)+1}$$
$$s'2 \; \epsilon \pm \{0, 1\}^{\varepsilon(\lambda 2+k)+1}$$
$$s'3 \; \epsilon \pm \{0, 1\}^{\varepsilon(\lambda 1+lp+k+1)+1}$$
$$s'4 \; \epsilon \pm \{0, 1\}^{\varepsilon(2lp+k)+1}$$

4.6 The Deposit Protocol:

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

1. The merchant sends to the bank the group signature (c1, s′1, s′2, s′3, s′4, T1, T2, T3) on the message *m′*.

2. The bank first verifies the validity of the group signature (c1, s′1, s′2, s′3, s′4, T1, T2, T3) using the same operations as the merchant (see Step 4 from Subsection of payment protocol).

3. If the group signature(c1, s′1, s′2, s′3, s′4, T1, T2, T3) is valid, the bank verifies the validity of the group blind signature $\sigma = (c, s1, s2, s3, s4, A, B, D)$ using the same operations as the merchant (see Step 1 from Subsection payment protocol). Then the bank checks whether:

$$D = (g^{eb} h^{xb}) H^{(c\|s1\|s2\|s3\|s4\|A\|B)} \bmod n. \qquad (1)$$

Where*eb*, *xb*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 (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 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.

V. SECURITY OF OUR SYSTEM

Our model allows the members of a group to sign messages on behalf of the group such that the following properties hold for the resulting signature:

1. **Blindness of Signatures:** The signer is unable to view the messages he signs. Moreover, the signer should have no recollection of having signed a particular document even though he can verify that he did indeed sign it.This is new with our scheme.

2. **Unforgeability:** Only group members can issue valid signatures.

3. **Undeniable Signer Identity:** The group manager can always establish the identity of the member who issued a valid signature.

4. **Signer Anonymity:** It is easy to check that a message/signature pair was signed by a group member, but only the group manager can determine which member issued the signature.

5. **Unlinkability:** Two message-signature pairs where the signature was obtained from the same signer cannot be linked.

6. **Security against Framing Attacks:** Neither the group manager, nor the group members can sign on behalf of other group members.

VI. Conclusion

We have proposed a group blind signature scheme that is secure and efficient, and therefore practical based on an efficient and provably coalition-resistant group signature scheme. The group blind signature properties are used to deliver anonymity, unlink ability and revocation services. We showed how our construction could be used to set up an electronic cash system in which more than one bank can dispense anonymous e-cash. A blindly signed authority from the bank is used to detect double-spending. Comparing with e-cash system proposed by Maitland and Boyd [11] our electronic cash system is resistant against blackmailing, money laundering and illegal purchases. Careful consideration to the insider threats will need to be taken for offline-cash systems to be truly practical. Other countermeasures against the insider threats such as audit and

logging will also need to be deployed with forensics techniques. The scheme discussed in this paper is susceptible to diversion and this can lead to perfect crimes. The potential applications of the e-cash technology will be useful for realizing copy and access control mechanisms with privacy protection. Designing an authority mechanism which is resistant to diversion is an open problem with respect to the underlying group blind signature scheme used in this paper.

REFERENCES

[1]. IsratJahan, MohammadZahidurRahman, and Md. GolamMoazzem. Review of anonymous electronic payment system. Journal of Electronics and computer science, 2:35-39, 2003.

[2]. Olivier Blazy, Georg Fuchsbauer, David Pointcheval and Damien Vergnaud, Short Blind Signatures, Journal of Computer Security, Volume 21, Number 5, pages 627-661. 2013.

[3]. Girraj Kumar Verma, Probable Security Proof of a Blind Signature Scheme over Braid Groups, International Journal of Network Security, Vol.12, No.2, PP.118{120, Mar. 2011.

[4]. Y.-M. Tseng, T.-Y.Wu and J.-D. Wu, An efficient and provably secure id-based signature scheme with batch verifications, International Journal of Innovative Computing, Information and Control, vol.5, no.11(A), pp.3911-3922, 2009.

[5]. J. S. Chou, Y. Chen, M. H. Cho and H. M. Sun, A novel id-based electronic cash system from pairings, Cryptology–PrintArchive, Report 2009/339, 2009.

[6]. S. Wang, Z. Chen and X. Wang, A new certificate less electronic cash scheme with multiple banks based on group signatures, Proc. of 2008 International Symposium on Electronic Commerce and Security, pp.362-366, 2008.

[7]. J.-H. Yang and C.-C. Chang, An efficient fair electronic payment system based upon non-signature authenticated encryption scheme, International Journal of Innovative Computing, Information and Control, vol.5, no.11(A), pp.3861-3873, 2009.

[8]. C.-I Fan, C.-I Wang and W. Z. Sun, Fast randomization schemes for Chaum blind signatures, International Journal of Innovative Computing, Information and Control, vol.5, no.11 (A), pp.3887-3900, 2009.

[9]. Ming-Te Chen, Chun-I Fan, Wen-ShenqJuang and Yi-Chun Yeh , An Efficient Electronic Cash Scheme With Multiple Banks Using Group Signature. International Journal of Innovative Computing, Information and Control, Volume 8, Number 7(A), pp. 4469-4482, July 2012.

[10]. ConstantinPopescu, An Electronic Cash System Based on Group Blind Signatures, Institute of Mathematics and Informatics, Vilnius. INFORMATICA, Vol. 17, No. 4, 551–564, 2006.

[11]. AtenieseG., 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.

[12]. Anna Lysyanskaya and ZulfikarRamzan, Group Blind Digital Signatures: A Scalable Solution to Electronic Cash, Financial Cryptography, Vol. 1465 of the series Lecture Notes in Computer Science, 184-197,2006.

[13]. Takashi Nishide, Shingo Miyazaki and Kouichi Sakurai, Security Analysis of Offline E-cash Systems with Malicious Insider.

[14]. Traore J., Group signatures and their relevance to privacy-protecting off-line electronic cash systems, Information Security and Privacy, Wollongong, Australia, 228–243, 1999.

[15]. Qiu, W., K. Chen, D. Gu (2002), A new off-line privacy protecting e-cash system with revocable anonymity,ISC 2002, 177–190, 2002.

[16]. Choi, H., F. Zhang, K. Kim, Electronic cash system based on group signatures with revocable anonymity, Workshop of Korea Information Security Institute, 29–34, 2003.

[17]. Kugler, D., H. Vogt, Marking: a privacy protecting approach against blackmailing, 4th International Workshop on Practice and Theory in Public Key Cryptography, Cheju Island, Korea,137–152, 2001.

[18]. EssamGhadafi, formalizing group blind signatures and Practical constructions without random oracles, ACISP, University of Bristol, 2013.

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

[20]. 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

[21]. 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.