A Secure and Efficient Group Blind Signature Scheme

Constantin Popescu

Department of Mathematics, University of Oradea

Str. Armatei Romane 5, Oradea

ROMANIA

E-mail: cpopescu@uoradea.ro

Abstract: A group blind signature require that a group member signs on group's behalf a document without knowing its content. In this paper we propose an efficient and secure group blind signature scheme. Our scheme is an extension of the group signature scheme proposed by Ateniese, Camenisch, Joye and Tsudik that adds the blindness property. We prove that our group blind signature scheme has the properties of correctness and blindness.

Keywords: Cryptography, group blind signatures, anonymity, coalition-resistance.

Constantin Popescu was born at Danesti, Romania, on 21st October , 1967. He received the MSc. degree in Computer Science from the University of Timisoara, Timisoara, Romania, in 1992. In 1992 he became an Assistant Professor at the Department of Mathematics, University of Oradea, Oradea, Romania. Since 1998 he has been Lecturer at the Department of Mathematics, University of Oradea. In 2001 he received the Ph. D degree in Informatics (cryptography) at the Babes-Bolyai University, Cluj Napoca. Since 2003 he has been Associate Professor at the Department of Mathematics, University of Oradea. His current research interests include cryptography, network security, group signatures, security protocols, and identification schemes. The author is presently at "Centre for Quantifiable Quality of Service in Communication Systems" (Q2S), NTNU, Trondheim, Norway. The centre is appointed Centre of Excellence by The Research Council of Norway.

1. Introduction

Group signatures are publicly verifiable but anonymous in that, no one, with the exception of a designated group manager, can establish the identity of a signer. Furthermore, group signatures are unlinkable which makes it computationally hard to establish whether or not multiple signatures are produced by the same group member. At the same time, no one, including the group manager, can misattribute a valid group signature. A group signature scheme could for instance be used in many specialized applications, such as voting and bidding. They can, for example, be used in invitations to submit tenders. All companies submitting a tender form a group and each company signs its tender anonymously using the group signature. Once the preferred tender is selected, the winner can be traced while the other bidders remain anonymous. More generally, group signatures can be used to conceal organizational structures, e.g., when a company or a government agency issues a signed statement. Also, a group signature scheme could be used by an employee of a large company to sign documents on behalf of the company.

Group signatures were first introduced by Chaum and van Heijst [7]. A number of improvements and enhancements followed [1], [15], [17], [18], [19]. The first group signature suitable for large groups is that of Camenisch and Stadler [4], where both the length of the group public key and the group signatures are independent of the group's size. The Camenisch-Michels in [5] scheme was improved by Ateniese, Camenisch, Joye and Tsudik [2], which undoubtedly represents the state of the art in the field.

A further application of a group signature schemes is electronic cash as was pointed out in [12]. In this case, 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. Also, Chen, Zhang and Wang suggested in [10] an offline electronic cash scheme to prevent blackmailing by using a group blind signature scheme. In [20], Popescu extended the electronic cash system of Maitland and Boyd [13] to prevent blackmailing, money laundering and illegal purchases by using a practical and secure coalition-resistant group blind signature scheme [14], [16]. In this case, an entity called supervisor and the bank form a group and a trusted party is the group manager. 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 first 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.

In this paper we propose a group blind signature scheme which combines the notions of group signatures and blind signatures [8], [9]. Our scheme is an extension of the group signature scheme proposed by Ateniese, Camenisch, Joye and Tsudik [2] that adds the blindness property and is more efficient and secure than the Lysyanskaya-Ramzan's scheme [12].

The remainder of this paper is organized as follows. In the next section, we review the group blind signature model. In Section 3 we present several cryptographic tools necessary in the subsequent design of our group blind signature scheme. Then, we present our group blind signature scheme in Section 4. Furthermore, we discuss some some aspects of security and efficiency in Section 5. Finally, Section 6 concludes the work of this paper.

2. The Group Blind Signature Model

Group signature schemes are a relatively recent cryptographic concept introduced by Chaum and van Heijst [7] in 1991.

A group blind signature scheme is a digital signature scheme comprised of the following procedures:

1. **Setup**: On input a security parameter l this probabilistic algorithm outputs the initial group public key P and the secret key S for the group manager.
2. **Join**: An interactive protocol between the group manager and a user that results in the user becoming a new group member.
3. **Sign**: An interactive protocol between the group member Alice and an external user, which on input message m from the user, the Alice's secret key and the group's public key P outputs a blind signature of m.
4. **Verify**: An algorithm for establishing the validity of an alleged group signature of a message with respect to a group public key.
5. **Open**: An algorithm that given a message, a valid group blind signature on it, a group public key and a group manager's secret key determines the identity of the signer.

A secure group blind signature scheme allows the members of a group to sign messages on behalf of the group so that the following properties hold:

1. Correctness: Signatures produced by a group member using **Sign** procedure must be accepted by **Verify** procedure.
2. 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.
3. Unforgeability: Only group members are able to sign messages on behalf of the group.
4. Anonymity: Given a signature, identifying the actual signer is computationally hard for everyone but the group manager.
5. Unlinkability: Deciding whether two different signatures were computed by the same group member is computationally hard.
6. Traceability: The group manager can always establish the identity of the member who issued a valid signature.
7. No framing: Even if the group manager and some of the group members collude, they cannot sign on behalf of non-involved group members.
8. 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.

3. Signatures of Knowledge

We present some well-studied techniques for proving knowledge of discrete logarithms (for more details see [5]).

Signatures of knowledge were used by Camenisch and Michels [5] and their construction is based on the

Schnorr signature scheme [21] 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 [11]) $H : \{0,1\}^* \to \{0,1\}^k$ which maps a binary string of arbitrary length to a k-bit hash value.

Let G be a cyclic subgroup of Z_n^* of order $\#G, \lceil \log_2(\#G) \rceil = l_G$. Let $\varepsilon > 1$ 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 [2] can be done easily as stated by the following definition.

Definition 1. Let $y, g \in G$. A pair $(c,s) \in \{0,1\}^k \times \pm\{0,1\}^{\varepsilon(l_G+k)+1}$ satisfying $c = H(m \| g \| y \| g^s y^c)$ 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 [2].

Definition 2. Let $g, h, y_1, y_2 \in G$. A pair $(c,s) \in \{0,1\}^k \times \pm\{0,1\}^{\varepsilon(l_G+k)+1}$ satisfying $c = H(m \| g \| h \| y_1 \| y_2 \| y_1^c g^s \| y_2^c h^s)$ 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. [6]. It is also related to a protocol given by Camenisch and Michels [5].

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

4. Our Proposed Group Blind Signature Scheme

This section presents a group blind signature scheme based on the group signature scheme proposed by Ateniese, Camenisch, Joye and Tsudik [2]. This group signature scheme is provably coalition-resistant and quite efficient.

4.1. Setup

Let k, l_p and $\varepsilon > 1$ be security parameters and let $\lambda_1, \lambda_2, \gamma_1, \gamma_2$ 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 $\Gamma =]2^{\gamma_1} - 2^{\gamma_2}, 2^{\gamma_1} + 2^{\gamma_2}[$. Finally, let H be a collision-resistant hash function $H : \{0,1\}^* \to \{0,1\}^k$.

The group manager (GM) executes the next steps to setup parameters of the group:

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

4.2. Join

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

To obtain his membership certificate, each user U_i must perform the following protocol with GM:

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

4.3. Sign

The protocol for obtaining a group blind signature on a message $m \in \{0,1\}^*$ is as follows. The signer does the following:

1. Computes
   $\tilde{A} = A_i y^{x_i} \pmod n, \tilde{B} = g^{x_i} \pmod n, \tilde{D} = g^{e_i} h^{x_i} \pmod n.$
2. Chooses random values $\tilde{r}_1 \in \pm\{0,1\}^{\varepsilon(\gamma_2+k)}$, $\tilde{r}_2 \in \pm\{0,1\}^{\varepsilon(\lambda_2+k)}$, $\tilde{r}_3 \in \pm\{0,1\}^{\varepsilon(\gamma_1+2l_p+k+1)}$, $\tilde{r}_4 \in \pm\{0,1\}^{\varepsilon(2l_p+k)}$ and computes:
   $\tilde{t}_1 = \tilde{A}^{\tilde{r}_1} / \left(a^{\tilde{r}_2} y^{\tilde{r}_3}\right), \tilde{t}_2 = \tilde{B}^{\tilde{r}_1} / g^{\tilde{r}_3}, \tilde{t}_3 = g^{\tilde{r}_4}, \tilde{t}_4 = g^{\tilde{r}_1} h^{\tilde{r}_4}.$
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 $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \delta \in_R \{0,1\}^{\varepsilon(l_p+k)}$ 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
$$s_1 = \tilde{s}_1 + \alpha_1, s_2 = \tilde{s}_2 + \alpha_2, s_3 = \tilde{s}_3 + \alpha_3$$
$$s_4 = \tilde{s}_4 + \alpha_4, A = \tilde{A}^{H(c\|s_1\|s_2\|s_3\|s_4)} \bmod n,$$
$$B = \tilde{B}^{H(c\|s_1\|s_2\|s_3\|s_4)} \bmod n, D = \tilde{D}^{H(c\|s_1\|s_2\|s_3\|s_4\|A\|B)} \bmod n.$$
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. Verify

A verifier can check the validity of a group blind signature $\sigma = (c, s_1, s_2, s_3, s_4, A, B, D)$ of the message m with the public key P as follows:

1. Compute
$$b_1 = 1/H(c \| s_1 \| s_2 \| s_3 \| s_4)$$
$$b_2 = 1/H(c \| s_1 \| s_2 \| s_3 \| s_4 \| A \| B)$$
$$t_1' = a_0^c A^{b_1(s_1 - c2^{\gamma_1})} / \left(a^{s_2 - c2^{\lambda_1}} y^{s_3}\right) \bmod n$$
$$t_2' = B^{b_1(s_1 - c2^{\gamma_1})} / g^{s_3} \bmod n$$
$$t_3' = B^{cb_1} g^{s_4} \bmod n$$
$$t_4' = D^{cb_2} g^{s_1 - c2^{\gamma_1}} h^{s_4} \bmod n$$
$$c' = H(m \| g \| h \| y \| a_0 \| a \| A^{b_1} \| B^{b_1} \| D^{b_2} \| t_1' \| t_2' \| t_3' \| t_4')$$
2. Accept the group blind signature if and only if:
$$c = c'$$
$$s_1 \in \pm\{0,1\}^{\varepsilon(\gamma_2 + k)+1}, s_2 \in \pm\{0,1\}^{\varepsilon(\lambda_2 + k)+1}$$
$$s_3 \in \pm\{0,1\}^{\varepsilon(\gamma_1 + 2l_p + k + 1)+1}, s_4 \in \pm\{0,1\}^{\varepsilon(2l_p + k)+1}$$

4.5. Open

Given a group blind signature $\sigma = (c, s_1, s_2, s_3, s_4, A, B, D)$ of a message m, the group manager can find out which one of the group members issued this signature by checking its correctness via **Verify**. He aborts if the signature is not correct. Otherwise, he computes:

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

and issues a signature

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

(see Definition 2). He then looks up A_i in the group member list and will find the corresponding A_i and the group member's identity.

5. Security and Efficiency of Our Scheme

The security and efficiency of our group blind signature scheme follows from the security and efficiency of the underlying group signature scheme [2].

The proposed group blind signature scheme is more secure and efficient than group blind signature scheme of Lysyanskaya and Ramzan [12]. Our Join protocol is an order of magnitude more efficient since all proofs that the new group member must provide are efficient proofs of knowledge of discrete logarithms. We show only the correctness and the blindness of our group blind signature scheme. The other security properties of the proposed group blind signature scheme are like in [2].

Theorem 1 (***Correctness).*** If the user follows the blind signing protocol and accepts, then the tuple $(c, s_1, s_2, s_3, s_4, A, B, D)$ is a correct group signature on $m \in \{0,1\}^*$.

Proof. The group signature $(c, s_1, s_2, s_3, s_4, A, B, D)$ is a correct group signature on m if the equality

$$c = H(m \| g \| h \| y \| a_0 \| a \| A^{1/H(c\|s_1\|s_2\|s_3\|s_4)} \| B^{1/H(c\|s_1\|s_2\|s_3\|s_4)} \| D^{1/H(c\|s_1\|s_2\|s_3\|s_4\|A\|B)} \|$$

$$a_0^c A^{\left(s_1 - c2^{\gamma_1}\right)/H(c\|s_1\|s_2\|s_3\|s_4)} / \left(a^{s_2 - c2^{\lambda_1}} y^{s_3}\right) \| B^{\left(s_1 - c2^{\gamma_1}\right)/H(c\|s_1\|s_2\|s_3\|s_4)} / g^{s_3} \|$$

$$B^{c/H(c\|s_1\|s_2\|s_3\|s_4)} g^{s_4} \| D^{c/H(c\|s_1\|s_2\|s_3\|s_4\|A\|B)} g^{s_1 - c2^{\gamma_1}} h^{s_4})$$

is verified. If it can be assumed that $H(\cdot)$ is a collision-resistant, then this is equivalent to proving that

$$t_1 = a_0^c A^{\left(s_1 - c2^{\gamma_1}\right)/H(c\|s_1\|s_2\|s_3\|s_4)} / \left(a^{s_2 - c2^{\lambda_1}} y^{s_3}\right),\ t_2 = B^{\left(s_1 - c2^{\gamma_1}\right)/H(c\|s_1\|s_2\|s_3\|s_4)} / g^{s_3},$$

$$t_3 = B^{c/H(c\|s_1\|s_2\|s_3\|s_4)} g^{s_4},\ t_4 = D^{c/H(c\|s_1\|s_2\|s_3\|s_4\|A\|B)} g^{s_1 - c2^{\gamma_1}} h^{s_4}.$$ We have:

$$a_0^c A^{\left(s_1 - c2^{\gamma_1}\right)/H(c\|s_1\|s_2\|s_3\|s_4)} / \left(a^{s_2 - c2^{\lambda_1}} y^{s_3}\right) = a_0^{\tilde{c}+\delta} \tilde{A}^{\tilde{s}_1 + \alpha_1 - (\tilde{c}+\delta)2^{\gamma_1}} / \left(a^{\tilde{s}_2 + \alpha_2 - (\tilde{c}+\delta)2^{\lambda_1}} y^{\tilde{s}_3 + \alpha_3}\right) =$$

$$a_0^{\delta} \tilde{t}_1 \tilde{A}^{\alpha_1 - \delta 2^{\gamma_1}} / \left(a^{\alpha_2 - \delta 2^{\lambda_1}} y^{\alpha_3}\right) = t_1$$

$$B^{\left(s_1 - c2^{\gamma_1}\right)/H(c\|s_1\|s_2\|s_3\|s_4)} / g^{s_3} = \tilde{B}^{\tilde{s}_1 + \alpha_1 - (\tilde{c}+\delta)2^{\gamma_1}} / g^{\tilde{s}_3 + \alpha_3} = \tilde{t}_2 \tilde{B}^{\alpha_1 - \delta 2^{\gamma_1}} / g^{\alpha_3} = t_2$$

$$B^{c/H(c\|s_1\|s_2\|s_3\|s_4)} g^{s_4} = \tilde{B}^{\tilde{c}+\delta} g^{\tilde{s}_4 + \alpha_4} = \tilde{t}_3 \tilde{B}^{\delta} g^{\alpha_4} = t_3$$

$$D^{c/H(c\|s_1\|s_2\|s_3\|s_4\|A\|B)} g^{s_1 - c2^{\gamma_1}} h^{s_4} = \tilde{D}^{\tilde{c}+\delta} g^{\tilde{s}_1 + \alpha_1 - (\tilde{c}+\delta)2^{\gamma_1}} h^{\tilde{s}_4 + \alpha_4} = \tilde{t}_4 \tilde{D}^{\delta} g^{\alpha_1} h^{\alpha_4} = t_4.$$ □

Theorem 2 (***Blindness).*** If the user follows the protocol, then even a signer with unlimited computing power gets no information about $m \in \{0,1\}^*$ and the group signature $(c, s_1, s_2, s_3, s_4, A, B, D)$.

Proof. To prove that the protocol is blind we show that for every possible signer's view there exists a unique tuple of blind factors $(\delta, \alpha_1, \alpha_2, \alpha_3, \alpha_4)$. Given any view consisting of $\tilde{r}_1, \tilde{r}_2, \tilde{r}_3, \tilde{r}_4, \tilde{t}_1, \tilde{t}_2, \tilde{t}_3, \tilde{t}_4, \tilde{c}, \tilde{s}_1, \tilde{s}_2, \tilde{s}_3, \tilde{s}_4$ and any group signature $(c, s_1, s_2, s_3, s_4, A, B, D)$ of a message m, we consider $\delta = c - \tilde{c}, \alpha_1 = s_1 - \tilde{s}_1, \alpha_2 = s_2 - \tilde{s}_2, \alpha_3 = s_3 - \tilde{s}_3, \alpha_4 = s_4 - \tilde{s}_4,$. It is easy to verify that the following equations hold:

$$a_0^{\delta}\tilde{t}_1\tilde{A}^{\alpha_1-\delta 2^{\gamma_1}}/\left(a^{\alpha_2-\delta 2^{\lambda_1}}y^{\alpha_3}\right)=a_0^{c}\tilde{A}^{\tilde{s}_1+\alpha_1-\delta 2^{\gamma_1}}/\left(a^{\tilde{s}_2+\alpha_2-\delta 2^{\lambda_1}}y^{\tilde{s}_3+\alpha_3}\right)=a_0^{c}A^{\left(s_1-c2^{\gamma_1}\right)/H(c\|s_1\|s_2\|s_3\|s_4)}/\left(a^{s_2-c2^{\lambda_1}}y^{s_3}\right)=t_1$$

$$\tilde{t}_2\tilde{B}^{\alpha_1-\delta 2^{\gamma_1}}/g^{\alpha_3}=\tilde{B}^{\tilde{s}_1+\alpha_1-\delta 2^{\gamma_1}}/g^{\tilde{s}_3+\alpha_3}=B^{\left(s_1-c2^{\gamma_1}\right)/H(c\|s_1\|s_2\|s_3\|s_4)}/g^{s_3}=t_2$$

$$\tilde{t}_3\tilde{B}^{\delta}g^{\alpha_4}=\tilde{B}^{c-\tilde{c}}g^{\tilde{r}_4+s_4-\tilde{s}_4}=B^{c/H(c\|s_1\|s_2\|s_3\|s_4)}g^{s_4}=t_3$$

$$\tilde{t}_4\tilde{D}^{\delta}g^{\alpha_1}h^{\alpha_4}=\tilde{D}^{\delta}g^{\tilde{r}_1+\alpha_1-\delta 2^{\gamma_1}}h^{\tilde{r}_4+\alpha_4}=D^{c/H(c\|s_1\|s_2\|s_3\|s_4\|A\|B)}g^{s_1-c2^{\gamma_1}}h^{s_4}=t_4.\qquad\square$$

Therefore, the above protocol is blind and our group signature is blind.

It is possible to extend our group blind signature scheme in the case of the group member leave a group. In this case, the group manager can revoke membership of a group member, by using a method for revocation in a group signature scheme [3]. The revoked group member cannot produce a valid group blind signature after being revoked.

6. Conclusion

In this paper we proposed a group blind signature scheme based on the group signature scheme proposed by Ateniese, Camenisch, Joye and Tsudik [2]. Our group blind signature scheme is more efficient and secure than the group blind signature scheme proposed in [12] because our scheme's registration protocol Join for new members is an order of magnitude more efficient. The main benefits of our group blind signature scheme, compared to the scheme of Lysyanskaya and Ramzan, relate to the underlying group signature scheme's improved efficiency and provable security.

REFERENCES

1. G. ATENIESE, G. TSUDIK, **Some open issues and new directions in group signatures**, Financial Cryptography (FC'99), Lecture Notes in Computer Science, Springer-Verlag, 1999.
2. G. ATENIESE, J. CAMENISCH, M. JOYE, G. TSUDIK, **A Practical and Provably Secure Coalition-Resistant Group Signature Scheme**, Advances in Cryptology - CRYPTO 2000, vol. 1880, Lecture Notes in Computer Science, Springer Verlag, pp. 255-270, 2000.
3. G. ATENIESE, D. SONG, G. TSUDIK, **Quasi-efficient Revocation in Group Signatures, Proceedings of Financial Cryptography 2002**, Southampton, Bermuda, March 11-14, 2002.
4. J. CAMENISCH, M. STADLER, **Efficient group signature schemes for large groups**, Advances in Cryptology-CRYPTO'97, Lecture Notes in Computer Science, vol. 1296, Springer-Verlag, pp. 410-424, 1997.
5. J. CAMENISCH, M. MICHELS, **A group signature scheme with improved efficiency**, Advances in Cryptology-ASIACRYPT'98, Lecture Notes in Computer Science, Springer-Verlag, vol. 1514, pp. 160-174, 1998.
6. A. CHAN, Y. FRANKEL, Y. TSIOUNIS, **Easy Come - Easy Go Divisible Cash**, Advances in Cryptology - Eurocrypt '98, Lecture Notes in Computer Science, Springer-Verlag, Vol 1403, pp. 561-574, 1998.
7. D. CHAUM, E. VAN HEIJST, **Group signatures**, Advances in Cryptology-EUROCRYPT'91, Lecture Notes in Computer Science, vol. 547, Springer-Verlag, pp. 241-246, 1991.
8. D. CHAUM, **Blind signatures for untraceable payments**, Advances in Cryptology-CRYPT0'82, Plenum Press, pp. 199-203, 1983.
9. D. CHAUM, **Blind signature systems**, Advances in Cryptology-CRYPT0'83, Plenum Press, pp. 153, 1984.
10. X. CHEN, F. ZHANG, Y. WANG, **A New Approach to Prevent Blackmailing in E-Cash**, http://eprint.iacr.org/2003/055/.

11. A. FIAT, A. SHAMIR, **How to Prove Yourself: Practical Solutions to Identification and Signature Problems**, Proceedings of CRYPTO'86, Lecture Notes in Computer Science, Springer-Verlag, vol. 263, pp. 186-194, 1987.

12. A. LYSYANSKAYA, Z. RAMZAN, **Group blind signature: A scalable solution to electronic cash**, Financial Cryptography (FC'98), Lecture Notes in Computer Science, vol. 1465, Springer-Verlag, pp. 184-197, 1998.

13. G. MAITLAND, C. BOYD, **Fair electronic cash based on a group signature scheme,** Proceedings of ICICS 2001, Lecture Notes in Computer Science, Springer-Verlag, pp. 461-465, 2001.

14. C. POPESCU, **An efficient group blind signature scheme based on the Strong RSA assumption**, Romanian Journal of Information Science and Technology, Volume 3, Number 4, pp. 365-374, 2000.

15. C. POPESCU, **Group Signature Schemes Based on The Difficulty of Computation of Approximate E-th roots**, Proceedings of Protocols for Multimedia Systems (PROMS2000), Cracow, Poland, pp. 325-331, 2000.

16. C. POPESCU, **A Practical Coalition-Resistant Group Blind Signature Scheme**, Studia Universitatis Babes-Bolyai Informatica, vol. XLVI, No. 1, pp. 55-66, 2001.

17. C. POPESCU, **An Efficient Group Signature Scheme for Large Groups**, Studies in Informatics and Control Journal, vol. 10, No. 1, pp. 7-14, 2001.

18. C. POPESCU, I. MANG, E. MANG, **Improving the Xia-You Group Signature Scheme,** Proceedings of The 11th Conference on Applied and Industrial Mathematics (CAIM 2003), Oradea, Romania, pp. 51-56, 2003.

19. C. POPESCU, D. NOJE, B. BARNABAS, I. MANG, **A Group Signature Scheme with Revocation**, Proceedings of 4th EURASIP Conference focused on Video/Image Processing and Multimedia Communications, Zagreb, Croatia, pp. 245-250, 2003.

20. C. POPESCU, **A secure electronic cash system based on group blind signatures**, Proceedings of International Conference on Applied Informatics, Innsbruck, Austria, to appear, 2004.

21. C.P. SCHNORR, **Efficient signature generation for smart cards**, Journal of Cryptology, 4(3), pp. 239-252, 1991.