STUDIA UNIV. BABEŞ–BOLYAI, INFORMATICA, Volume **XLVI**, Number 1, 2001

A PRACTICAL COALITION-RESISTANT GROUP BLIND SIGNATURE SCHEME

CONSTANTIN POPESCU

Abstract. A group signature allow any member of a group to sign on behalf of the group. A group blind signature requires that a group member signs on group's behalf a document without knowing its content. In this paper we propose a practical coalition-resistant group blind signature scheme based on the strong RSA and the decisional Diffie-Hellman assumptions. Our scheme is an extension of the group signature scheme proposed in [3] that adds the blindness property.

Keywords: Group blind signature scheme, group signatures, blind signatures, strong RSA assumption

1. Introduction

Group signature schemes are a relatively recent cryptographic concept introduced by Chaum and van Heyst [12] in 1991. 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 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. A further application of a group signature schemes is electronic cash as was pointed out in [18]. In this case, several banks issue coins, but it is impossible for shops to find out which bank issued a coin

2000 *Mathematics Subject Classification.* 68P25.
1998 *CR Categories and Descriptors.* E.3 [**Data**]: Data Encryption.

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.

Group signatures were first introduced by Chaum and van Heijst [12]. A number of improvements and enhancements followed [1, 17, 21, 25, 26]. However, in the schemes presented in [8, 12, 19, 20, 21, 22] the length of signatures and the size of the group's public key depend on the size of the group and thus these schemes are not suitable for large groups. The first group signature suitable for large groups is that of Camenisch and Stadler [7], where both the length of the group public key and the group signatures are independent of the group's size. The Camenisch-Stadler scheme was improved by Camenisch and Michels in [5], which undoubtedly represents the state of the art in the field.

In this paper we propose a group blind signature scheme which combines the notions of group signatures and blind signatures [6, 10, 11, 16]. Our scheme is an extension of the group signature scheme from reference [3] that adds the blindness property and is more efficient and secure than [23] and the Lysyanskaya-Ramzan scheme [18]. In particular, our scheme's registration protocol (Join) for new members is an order of magnitude more efficient. Our scheme is based on the strong RSA and the decisional Diffie-Hellman assumptions and is as secure and efficient as the basic group signature scheme proposed in [3].

2. The Group Blind Signature Scheme

Our group blind signature scheme is an extension of the group signature scheme from reference [3] that adds the blindness property. Participants are group members, a group manager and several users. Our group blind signature scheme 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) Anonimity: 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.

Definition 1. *A group blind signature scheme is a digital signature scheme comprised of the following algorithms:*

(1) ***Setup****: The public output is the group's public key P. The private outputs are the individual secret keys x_G for each group member, the secret key x_M 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 A and an external user, which on input message m from the user, the A's secret key x_G and the group's public key P outputs a blind signature σ.*
(4) ***Verify****: An algorithm that for an input composed of a message m, a signature σ and the group's public key P returns 1 if and only if σ was generated by any group member using the protocol* ***Sign*** *on input x_G, m and P.*
(5) ***Tracing****: A tracing algorithm that for an input composed of a signature σ, a message m, the group manager's secret key x_M and the group's public key P returns the identity ID of the group member who issued the signature σ together with an argument arg of this fact.*
(6) ***Vertracing****: A tracing verification algorithm that for an input composed of a signature σ, a message m, the group's public key P, the identity ID of a group member and an argument arg outputs 1 if and only if arg was generated by tracing with respect to m, σ, P and x_M.*

In this section we review some cryptographic assumptions necessary in the subsequent design of our group blind signature scheme. The Strong RSA Assumption was independently introduced by Baric and Pfitzman [4] and by Fujisaki and Okamoto [14].

Definition 2 (Strong RSA Problem)**.** *Let $n = pq$ be an RSA-like modulus and let G be a cyclic subgroup of $\mathbb{Z}_n^*$ of order l_g. Given n and $z \in G$, the Strong RSA Problem consists of finding $u \in G$ and $e \in \mathbb{Z}_{>1}$ satisfying $z \equiv u^e (mod\ n)$.*

Assumption 1 (Strong RSA Assumption)**.** *There exists a probabilistic polynomial time algorithm K which on input 1^{l_g} outputs a pair (n, z) such that for all probabilistic polynomial-time algorithms P the probability that P can solve the Strong RSA Problem is negligible.*

Assumption 2 (Decisional Diffie-Hellman Assumption)**.** *Let $n = pq$ be an RSA-like modulus and let α be a quadratic residue modulo n that has a large order in $\mathbb{Z}_n^*$. Let $G =< \alpha >$. Given as input a triplet $(\alpha^a, \alpha^b, \alpha^c)$ in G^3, it is hard to decide whether $(\alpha^a, \alpha^b, \alpha^c)$ is a Diffie-Hellman triplet $(\alpha^a, \alpha^b, \alpha^{ab})$ or a random triplet.*

For the Decisional Diffie-Hellman Assumption see [5] for more details.

The security of our group blind signature scheme is based on these assumptions.

3. Signatures of Knowledge

In this section we present some well studied techniques for proving knowledge of discrete logarithms. 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 ($G =< g >$). Let $k, l_1, l_2 < l_g$ and $\varepsilon > 1$ be security parameters.

We use the following notations:

- The symbol $\|$ denotes the concatenation of two binary string (or of the binary representation of group elements and integers).
- We assume a collision-resistant hash function $H : \{0,1\}^* \rightarrow \{0,1\}^k$ which maps a binary string of arbitrary length to a k-bit hash value.
- The notation $H(m \parallel g \parallel y \parallel g^s y^c)$ denotes the message digest of the block of data $m \parallel g \parallel y \parallel g^s y^c$.
- The notation $r \in_R \{0,1\}^{\varepsilon(l_g+k)}$ denotes that r is random in $\{0,1\}^{\varepsilon(l_g+k)}$.
- We denote $\log_g y = \alpha$.
- $SPK\{(\alpha) : y = g^\alpha\}(m)$ is a signature of a message $m \in \{0,1\}^*$ with respect to y.
- $SPK\{(\alpha) : y_1 = g^\alpha \wedge y_2 = h^\alpha\}(m)$ is a signature of a message $m \in \{0,1\}^*$ with respect to y_1 and y_2.
- $SPK\left\{(\alpha) : h = g^\alpha \wedge \delta = \beta^\alpha \wedge (2^{l_1} - 2^{\varepsilon(l_2+k)+1} < \alpha < 2^{l_1} + 2^{\varepsilon(l_2+k)+1})\right\}(m)$ is a proof of knowledge of the discrete logarithm of h with respect to base g and of δ with respect to β, $log_g h = log_\beta \delta$ and $log_g h$ is in the interval $\left\{2^{l_1} - 2^{\varepsilon(l_2+k)+1}, ..., 2^{l_1} + 2^{\varepsilon(l_2+k)+1}\right\}$.

A proof of knowledge is a way for one person to convince another person that he knows some fact without actually revealing that fact. A signature of knowledge is used both for the purpose of signing a message and proving knowledge of a secret. Signatures of knowledge were used by Camenisch and Michels [5] and their construction is based on the Schnorr signature scheme [24] to prove knowledge.

Showing the knowledge of a discrete logarithm [5] can be done easily as stated by the following definition.

Definition 3. *Let $\varepsilon > 1$ be a security parameter. A pair $(c, s) \in \{0,1\}^k \times \left\{-2^{l_g+k}, \ldots, 2^{\varepsilon(l_g+k)}\right\}$ satisfying $c = H(m \parallel g \parallel y \parallel g^s y^c)$ is a signature of a message $m \in \{0,1\}^*$ with respect to y and is denoted by $SPK\{(\alpha) : y = g^\alpha\}(m)$.*

A signature $(c, s) = SPK\{(\alpha) : y = g^\alpha\}(m)$ of a message $m \in \{0,1\}^*$ can be computed as follows. An entity knowing the secret key $\alpha \in \{0,1\}^{l_g}$ such that

$y = g^{\alpha}$, chooses $r \in_R \{0,1\}^{\varepsilon(l_g+k)}$ and computes $t = g^r,\ c = H(m \parallel g \parallel y \parallel t),\ s = r - c\alpha$.

A slight modification of the previous definition enables to show the knowledge and equality of two discrete logarithms described in [5].

Definition 4. *A pair* $(c,s) \in \{0,1\}^k \times \left\{-2^{l_g+k}, ..., 2^{\varepsilon(l_g+k)}\right\}$ *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 a message* $m \in \{0,1\}^*$ *with respect to* y_1 *and* y_2 *and is denoted by* $SPK\{(\alpha) : y_1 = g^{\alpha} \wedge y_2 = h^{\alpha}\}(m)$.

A signature $(c,s) = SPK\{(\alpha) : y_1 = g^{\alpha} \wedge y_2 = h^{\alpha}\}(m)$ of a message $m \in \{0,1\}^*$ can be computed as follows. An entity knowing the secret key $\alpha \in \{0,1\}^{l_g}$ such that $y_1 = g^{\alpha}$ and $y_2 = h^{\alpha}$, chooses $r \in_R \{0,1\}^{\varepsilon(l_g+k)}$ and computes $t_1 = g^r,\ t_2 = h^r,\ c = H(m \parallel g \parallel h \parallel y_1 \parallel y_2 \parallel t_1 \parallel t_2),\ s = r - c\alpha$.

Definition 5. *A tuple* $(c_1, c_2, s_1, s_2) \in \{0,1\}^k \times \{0,1\}^k \times \left\{-2^{l_g+k}, ..., 2^{\varepsilon(l_g+k)}\right\} \times \left\{-2^{l_g+k}, ..., 2^{\varepsilon(l_g+k)}\right\}$ *satisfying* $c_1 \oplus c_2 = H(m\|g\|h\|y_1\|y_2\|y_1^{c_1} g^{s_1} \| y_2^{c_2} h^{s_2})$ *is a signature of a message* $m \in \{0,1\}^*$ *with respect to* y_1 *and* y_2 *and is denoted by* $SPK\left\{(\alpha,\beta) : y_1 = g^{\alpha} \vee y_2 = h^{\beta}\right\}(m)$.

This definition shows the knowledge of one out of two discrete logarithms [5]. If the signer knows the secret key $\alpha \in \{0,1\}^{l_g}$ such that $y_1 = g^{\alpha}$, then he can compute this signature as follows. The signer chooses $r_1 \in_R \{0,1\}^{\varepsilon(l_g+k)},\ r_2 \in_R \{0,1\}^{\varepsilon(l_g+k)},\ c_2 \in_R \{0,1\}^k$ and computes $t_1 = g^{r_1},\ t_2 = h^{r_2} y_2^{c_2},\ c_1 = c_2 \oplus H(m \parallel g \parallel h \parallel y_1 \parallel y_2 \parallel t_1 \parallel t_2),\ s_1 = r_1 - c_1\alpha,\ s_2 = r_2$.

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. [9]. It is also related to a protocol given by Camenisch and Michels [5].

Definition 6. *A proof of knowledge of the discrete logarithm of* h *with respect to base* g *and of* δ *with respect to* β*, which also proves that* $log_g h = log_\beta \delta$ *and that* $log_g h$ *is in the interval* $\left\{2^{l_1} - 2^{\varepsilon(l_2+k)+1}, ..., 2^{l_1} + 2^{\varepsilon(l_2+k)+1}\right\}$ *is a pair* (c,s)*, and is denoted by*
$SPK\left\{(\alpha) : h = g^{\alpha} \wedge \delta = \beta^{\alpha} \wedge (2^{l_1} - 2^{\varepsilon(l_2+k)+1}) < \alpha < (2^{l_1} + 2^{\varepsilon(l_2+k)+1})\right\}(m)$,
where $c = H(m\|g\|h\|\beta\|\delta\|g^{s-c2^{l_1}} h^c \| \beta^{s-c2^{l_1}} \delta^c)$ *and* s *is in the interval*
$\left\{-(2^k-1)(2^{l_2}-1), ..., 2^{\varepsilon(l_2+k)}\right\}$.

This signature can be computed as follows. If the signer knows an integer $\alpha \in \left\{2^{l_1}, ..., 2^{l_1} + 2^{l_2} - 1\right\}$ such that $h = g^{\alpha}$ and $\delta = \beta^{\alpha}$, he chooses a random $t \in \{0,1\}^{\varepsilon(l_2+k)}$ and computes $c = H(m\|g\|h\|\beta\|\delta\|g^t\|\beta^t),\ s = t - c(\alpha - 2^{l_1})$.

The security of all the presented building blocks has been proven in the random oracle model [13] under the strong RSA assumption in [5, 14, 15].

4. The Proposed Group Blind Signature Scheme

We propose a realization of a group blind signature scheme the security of which is based on the Strong RSA Assumption and Decisional Diffie-Hellman Assumption. Our scheme is as secure and efficient as the basic group signature scheme proposed in [3].

Let G be a cyclic subgroup of $\mathbb{Z}_n^*$ of order l_g. Let $k, l_1, l_2 < l_g$ and $\varepsilon > 1$ be security parameters. Finally, let H be a collision-resistant hash function $H : \{0,1\}^* \to \{0,1\}^k$.

4.1. **Setup.** The setup procedure of our scheme (as in [3]) is as follow. The group manager executes the following steps:

(1) Select random secret l_g-bit primes p', q' and computes $p = 2p' + 1$ and $q = 2q' + 1$. Set the modulus $n = pq$. It is a good habit to restrict the 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 $x \in \mathbb{Z}_{p'q'}^*$ and set $y = g^x \bmod n$.
(4) The group public key is $P = (n, a, a_0, y, g, h)$.
(5) The corresponding secret key is $S = (p', q', x)$.

4.2. **Join.** Suppose now that a user wants to join the group. 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 the group manager.

(1) The user U_i generates a secret exponent $x_i' \in \left[0, 2^{l_2}\right]$, a random integer $r \in \left[0, 2^{n^2}\right]$ and sends $C_1 = g^{x_i'} h^r \bmod n$ to group manager and proves him knowledge of the representation of C_1 with respect to bases g and h.
(2) The group manager checks that $C_1 \in QR(n)$. If this is the case, the group manager selects $\alpha_i, \beta_i \in \left[0, 2^{l_2}\right]$ at random and sends (α_i, β_i) to U_i.
(3) The user U_i computes $x_i = 2^{l_1} + \left(\alpha_i x_i' + \beta_i \bmod 2^{l_2}\right)$ and sends to group manager the value $C_2 = a^{x_i} \bmod n$. The user also proves to group manager:
   (a) that the discrete logarithm of C_2 with respect to base a lies in the interval $\left[2^{l_1} - 2^{l_2}, 2^{l_1} + 2^{l_2}\right]$.
   (b) knowledge of integers u, v, w such that: u lies in the interval $\left[-2^{l_2}, 2^{l_2}\right]$, u equals the discrete logarithm of $C_2/a^{2^{l_1}}$ with respect to base a and $C_1^{\alpha_i} g^{\beta_i}$ equals $g^u \left(g^{2^{l_2}}\right)^v h^w$.

(4) The group manager checks that $C_2 \in QR(n)$. If this is the case and all the above proofs were correct, group manager selects a random prime $e_i \in \left[2^{l_1} - 2^{l_2}, 2^{l_1} + 2^{l_2}\right]$ and conmputes $A_i = (C_2 a_0)^{1/e_i} \pmod n$. Finally, group manager sends to U_i the new membership certificate (A_i, e_i).
(5) The user U_i verifies that $a^{x_i} a_0 \equiv A_i^{e_i} \pmod n$.
(6) The group manager creates a new entry in the membership table and stores (A_i, e_i) in the new entry.

4.3. **Sign.** In this subsection we present our signature protocol which is blind, unlike [3]. First, we define a group blind signature and then we show how a group member can generate such a group blind signature.

Definition 7. *Let ε, l_1, l_2 be security parameters such that $\varepsilon > 1, l_2 < l_1 < l_g$ and $l_2 < \frac{l_g - 2}{\varepsilon} - k$ holds. A group blind signature of a message $m \in \{0,1\}^*$ is $(c, s_1, s_2, s_3, s_4, A, B, D) \in \{0,1\}^k \times \left\{-2^{\varepsilon(l_2+k)+1}, ..., 2^{\varepsilon(l_2+k)+1}\right\} \times \left\{-2^{\varepsilon(l_2+k)+1}, ..., 2^{\varepsilon(l_2+k)+1}\right\} \times \left\{-2^{\varepsilon(l_1+2l_g+k+1)+1}, ..., 2^{\varepsilon(l_1+2l_g+k+1)+1}\right\} \times \left\{-2^{\varepsilon(2l_g+k)+1}, ..., 2^{\varepsilon(2l_g+k)+1}\right\} \times G^3$ satisfying $c = H(m \parallel g \parallel h \parallel y \parallel A \parallel B \parallel D \parallel a_0^c A^{s_1 - c2^{l_1}} / \left(a^{s_2 - c2^{l_1}} y^{s_3}\right) \parallel B^{s_1 - c2^{l_1}} / g^{s_3} \parallel B^c g^{s_4} \parallel D^c g^{s_1 - c2^{l_1}} h^{s_4})$.*

The protocol for obtaining a group blind signature is as follows. When responding to a sign request, the signer (the group member U_i) does the following:

(1) Chooses an integer $w \in_R \{0,1\}^{2l_g}$ and computes

$$A = A_i y^w \pmod n, \; B = g^w \pmod n, \; D = g^{e_i} h^w \pmod n.$$

(2) Chooses $\tilde{r_1} \in_R \{0,1\}^{\varepsilon(l_2+k)}$, $\tilde{r_2} \in_R \{0,1\}^{\varepsilon(l_g+l_1+k)}$, $\tilde{r_3} \in_R \{0,1\}^{\varepsilon(l_g+k)}$, $\tilde{r_4} \in_R \{0,1\}^{\varepsilon(l_2+k)}$ and computes

$$\begin{aligned} \tilde{t_1} &= A^{\tilde{r_1}} / \left(a^{\tilde{r_2}} y^{\tilde{r_3}}\right) \\ \tilde{t_2} &= B^{\tilde{r_1}} / g^{\tilde{r_3}} \\ \tilde{t_3} &= g^{\tilde{r_4}} \\ \tilde{t_4} &= g^{\tilde{r_1}} h^{\tilde{r_4}}. \end{aligned}$$

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

In turn, the user does the following:

(1) Chooses $\gamma_1, \gamma_2, \gamma_3, \gamma_4, \delta \in_R \{0,1\}^{\varepsilon(l_g+k)}$ and computes

$$\begin{aligned} t_1 &= a_0^{\delta} \tilde{t_1} A^{\gamma_1 - \delta 2^{l_1}} / \left(a^{\gamma_2 - \delta 2^{l_1}} y^{\gamma_3}\right) \\ t_2 &= \tilde{t_2} B^{\gamma_1 - \delta 2^{l_1}} / g^{\gamma_3} \\ t_3 &= \tilde{t_3} B^{\delta} g^{\gamma_4} \\ t_4 &= \tilde{t_4} D^{\delta} g^{\gamma_1} h^{\gamma_4}. \end{aligned}$$

(2) Computes

$$\begin{aligned} c &= H(m\|g\|h\|y\|A\|B\|D\|t_1\|t_2\|t_3\|t_4) \\ \tilde{c} &= c - \delta. \end{aligned}$$

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

The signer does the following:

(1) Computes

$$\begin{aligned} \tilde{s_1} &= \tilde{r_1} - \tilde{c}(e_i - 2^{l_1}) \\ \tilde{s_2} &= \tilde{r_2} - \tilde{c}(x_i - 2^{l_1}) \\ \tilde{s_3} &= \tilde{r_3} - \tilde{c}e_i w \\ \tilde{s_4} &= \tilde{r_4} - \tilde{c}w. \end{aligned}$$

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

The user does the following:

(1) Computes

$$\begin{aligned} s_1 &= \tilde{s_1} + \gamma_1 \\ s_2 &= \tilde{s_2} + \gamma_2 \\ s_3 &= \tilde{s_3} + \gamma_3 \\ s_4 &= \tilde{s_4} + \gamma_4. \end{aligned}$$

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

The tuple $(c, s_1, s_2, s_3, s_4, A, B, D)$ is a group signature of a message $m \in \{0,1\}^*$ and the above protocol is a group blind signature scheme.

4.4. **Verifying Signatures, Tracing and Verifying Tracing.** The resulting signature $(c, s_1, s_2, s_3, s_4, A, B, D)$ of a message m can be verified as follows:

(1) Compute $c' = H(m \parallel g \parallel h \parallel y \parallel A \parallel B \parallel D \parallel a_0^c A^{s_1 - c2^{l_1}} / \left(a^{s_2 - c2^{l_1}} y^{s_3}\right) \parallel B^{s_1 - c2^{l_1}} / g^{s_3} \parallel B^c g^{s_4} \parallel D^c g^{s_1 - c2^{l_1}} h^{s_4})$.

(2) Accept the signature if and only if $c = c'$ and $s_1 \in \left\{-2^{\varepsilon(l_2+k)+1}, ..., 2^{\varepsilon(l_2+k)+1}\right\}$, $s_2 \in \left\{-2^{\varepsilon(l_2+k)+1}, ..., 2^{\varepsilon(l_2+k)+1}\right\}$, $s_3 \in \left\{-2^{\varepsilon(l_1+2l_g+k+1)+1}, ..., 2^{\varepsilon(l_1+2l_g+k+1)+1}\right\}$, $s_4 \in \left\{-2^{\varepsilon(2l_g+k)+1}, ..., 2^{\varepsilon(2l_g+k)+1}\right\}$.

Given a 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. He aborts if the signature is not correct. Otherwise, he computes $u' = A/B^x$, issues a signature

$$P := SPK\{(\alpha) : y = g^\alpha \wedge A/u' = B^\alpha\}(u'\|\sigma\|m)$$

(see Definition 4) and reveals $arg := u' \| P$. He then looks up u' in the group member list and will find the corresponding u and the group member's identity. Checking whether the group manager correctly revealed the originator of a signature $\sigma = (c, s_1, s_2, s_3, s_4, A, B, D)$ of a message m can simply be done by verifying σ and arg.

5. Security and Efficiency of Our Scheme

Our group blind signature scheme is as secure and efficient as the group signature scheme proposed in [3], but more secure and efficient than group blind signature scheme from reference [23]. This, because our Join protocol is an order of magnitude more effiecient 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 the signature. The others security properties of the proposed group blind signature scheme are like in [3].

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

$$\begin{aligned} c &= H(m \parallel g \parallel h \parallel y \parallel A \parallel B \parallel D \parallel a_0^c A^{s_1 - c2^{l_1}} / \left(a^{s_2 - c2^{l_1}} y^{s_3}\right) \parallel B^{s_1 - c2^{l_1}} / g^{s_3} \\ &\parallel B^c g^{s_4} \parallel D^c g^{s_1 - c2^{l_1}} h^{s_4}) \end{aligned}$$

is verified. If it can be assumed that $H(\cdot)$ is a collision-resistant, then this is equivalent to proving that $t_1 = a_0^c A^{s_1 - c2^{l_1}} / \left(a^{s_2 - c2^{l_1}} y^{s_3}\right)$, $t_2 = B^{s_1 - c2^{l_1}} / g^{s_3}$, $t_3 = B^c g^{s_4}$, $t_4 = D^c g^{s_1 - c2^{l_1}} h^{s_4}$. We have:

$$\begin{aligned} a_0^c A^{s_1 - c2^{l_1}} / \left(a^{s_2 - c2^{l_1}} y^{s_3}\right) &= a_0^{\tilde{c}+\delta} A^{\tilde{s_1} + \gamma_1 - (\tilde{c}+\delta)2^{l_1}} / \left(a^{\tilde{s_2} + \gamma_2 - (\tilde{c}+\delta)2^{l_1}} y^{\tilde{s_3} + \gamma_3}\right) = \\ \tilde{t_1} a_0^{\delta} A^{\gamma_1 - \delta 2^{l_1}} / (a^{\gamma_2 - \delta 2^{l_1}} y^{\gamma_3}) &= t_1 \\ B^{s_1 - c2^{l_1}} / g^{s_3} &= B^{\tilde{s_1} + \gamma_1 - (\tilde{c}+\delta)2^{l_1}} / g^{\tilde{s_3} + \gamma_3} = \tilde{t_2} B^{\gamma_1 - \delta 2^{l_1}} / g^{\gamma_3} = t_2 \\ B^c g^{s_4} &= B^{\tilde{c}+\delta} g^{\tilde{s_4} + \gamma_4} = \tilde{t_3} B^{\delta} g^{\gamma_4} = t_3 \\ D^c g^{s_1 - c2^{l_1}} h^{s_4} &= D^{\tilde{c}+\delta} g^{\tilde{s_1} + \gamma_1 - (\tilde{c}+\delta)2^{l_1}} h^{\tilde{s}_4 + \gamma_4} = \tilde{t_4} D^{\delta} g^{\gamma_1} h^{\gamma_4} = t_4. \end{aligned}$$

This completes the proof. □

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 $(\delta, \gamma_1, \gamma_2, \gamma_3, \gamma_4)$. 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 $\delta = c - \tilde{c}$, $\gamma_1 = s_1 - \tilde{s_1}$, $\gamma_2 = s_2 - \tilde{s_2}$, $\gamma_3 = s_3 - \tilde{s_3}$, $\gamma_4 = s_4 - \tilde{s_4}$. It is easy to verify that the following equations hold:

$$\tilde{t_1} a_0^{\delta} A^{\gamma_1 - \delta 2^{l_1}} / \left(a^{\gamma_2 - \delta 2^{l_1}} y^{\gamma_3}\right) = a_0^{c} A^{\tilde{s_1} + \gamma_1 - \delta 2^{l_1}} / \left(a^{\tilde{s_2} + \gamma_2 - \delta 2^{l_1}} y^{\tilde{s_3} + \gamma_3}\right) =$$

$$\begin{aligned}
a_0^{c} A^{s_1 - c2^{l_1}} / \left(a^{s_2 - c2^{l_1}} y^{s_3}\right) &= t_1 \\
\tilde{t_2} B^{\gamma_1 - \delta 2^{l_1}} / g^{\gamma_3} = B^{\tilde{s_1} + \gamma_1 - \delta 2^{l_1}} / g^{\tilde{s_3} + \gamma_3} = B^{s_1 - c2^{l_1}} / g^{s_3} &= t_2 \\
\tilde{t_3} B^{\delta} g^{\gamma_4} = g^{\tilde{r_4} + s_4 - \tilde{s_4}} B^{c - \tilde{c}} = B^{c} g^{s_4} &= t_3 \\
\tilde{t_4} D^{\delta} g^{\gamma_1} h^{\gamma_4} = g^{\tilde{r_1} + \gamma_1 - \delta 2^{l_1}} D^{\delta} h^{\gamma_4 + \tilde{r_4}} = D^{c} g^{s_1 - c2^{l_1}} h^{s_4} &= t_4. \ \square
\end{aligned}$$

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

6. Conclusion

In this paper we proposed a group blind signature scheme that is secure and efficient and it is an extension of the group signature scheme from reference [3]. Our group blind signature scheme is more efficient and secure than the group blind signature scheme proposed in [23] because our scheme's registration protocol Join for new members is an order of magnitude more efficient. Also, the proposed scheme is as efficient and secure as the basic group signature scheme proposed in [3].

References

[1] ATENIESE, G. and TSUDIK, G., **Group signature a la carte**, Tenth Anual ACM-SIAM Symposium on Discrete Algorithms (SODA'99), 1999.

[2] ATENIESE, G. and TSUDIK, G., **Some open issues and new directions in group signatures**, Financial Cryptography (FC'99), Lecture Notes in Computer Science, Springer-Verlag, 1999.

[3] ATENIESE, G., CAMENISCH J., JOYE M., TSUDIK G., **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.

[4] BARIC, N. and PFITZMANN, B., **Collision-free accumulators and fail-stop signature schemes without trees**, In Advances in Cryptology-EUROCRYPT'97, Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, 1997, pp. 480–494.

[5] CAMENISCH, J. and MICHELS, M., **A group signature scheme with improved efficiency**, Advances in Cryptology-ASIACRYPT'98, Lecture Notes in Computer Science, vol. 1514, Springer-Verlag, 1998, pp. 160–174.

[6] CAMENISCH, J., PIVETEAU, J., and STADLER, M., **Blind signatures based on the discrete logarithm problem**, Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1994, pp. 428–432.

[7] CAMENISCH, J. and STADLER, M., **Efficient group signature schemes for large groups**, Advances in Cryptology-CRYPTO'97, Lecture Notes in Computer Science, vol. 1296, Springer-Verlag, 1997, pp. 410–424.

[8] CAMENISCH, J., **Efficient and generalized group signatures**, Advances in Cryptology-EUROCRYPT'97, Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, 1997, pp. 465–479.

[9] CHAN, A., FRANCHEL, Y. and TSIOUNIS, Y., **Easy come-easy go divisible cash**, Updated version with corrections on the Range Bounded Commitment protocol. Available at http://www.ccs.neu.edu/home/yiannis/pubs.html.

[10] CHAUM, D., **Blind signatures for untraceable payments**, Advances in Cryptology-CRYPT0'82, Plenum Press, 1983, pp. 199–203.

[11] CHAUM, D., **Blind signature systems**, Advances in Cryptology-CRYPT0'83, Plenum Press, 1984, pp. 153.

[12] CHAUM, D. and VAN HEYST, E., **Group signatures**, Advances in Cryptology-EUROCRYPT'91, Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 257–265.

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

[14] FUJISAKI, E. and OKAMOTO, T., **Statistical zero knowledge protocols to prove modular polynomial relations**, In Advances in Cryptology-CRYPTO'97, Lecture Notes in Computer Science, vol. 1297, Springer-Verlag, 1997, pp. 16–30.

[15] FUJISAKI, E. and OKAMOTO, T., **A practical and provably secure scheme for publicly verifiable secret sharing and its applications**, In Advances in Cryptology-EUROCRYPT'98, Lecture Notes in Computer Science, vol. 1403, Springer-Verlag, 1998, pp. 32–46.

[16] HORSTER, P., MICHELS, M. and PETERSEN, H., **Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications**, Advances in Cryptology-ASIACRYPT'94, Lecture Notes in Computer Science, vol. 917, Springer-Verlag, 1995, pp. 224–237.

[17] LEE, W. and CHANG, C., **Efficient group signature scheme based on the discrete logarithm**, IEE Proc. Comput. Digit. Tech. 145, no. 1, 1998, pp. 15–18.

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

[19] KIM, S., PARK, S. and WON, D., **Convertible group signatures**, Advances in Cryptology-ASIACRYPT'96, Lecture Notes in Computer Science, vol. 1163, Springer-Verlag, 1996, pp. 311–321.

[20] PARK, S., LEE, I. and WON, D., **A practical group signature**, Proceedings of the 1995 Japan-Corea Workshop on Information Security and Cryptography, 1995, pp. 127–133.

[21] KIM, S., PARK, S. and WON, D., **ID-based group signature schemes**, Electronics Letters, 1997, pp. 1616–1617.

[22] PETERSEN, H., **How to convert any digital signature scheme into a group signature scheme**, Security Protocols Workshop, Paris, 1997.

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

[24] SCHNORR, C.P., **Efficient signature generation for smart cards**, Journal of Cryptology, 4(3): 1991, pp. 239–252.

[25] TSENG, Y. and JAN, J., **A novel ID-based group signature**, In T.L. Hwang and A.K. Lenstra editors, 1998 International Computer Symposium, Workshop on Cryptography and Information Security, Tainan, 1998, pp. 159–164.

[26] TSENG, Y. and JAN, J., **Improved group signature scheme based on the discrete logarithm problem**, Electronics Letters 35, no. 1, 1999, pp. 37–38.

University of Oradea, Department of Mathematics, Str. Armatei Romane 5, Oradea, Romania

E-mail address: cpopescu@math.uoradea.ro