MATHEMATICA MORAVICA
VOL. 4 (2000), 99–108

A GROUP BLIND SIGNATURE SCHEME BASED ON THE STRONG RSA ASSUMPTION

Constantin Popescu

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 provably secure group blind signature scheme. Our scheme is an extension of Camenisch and Michels's group signature scheme [2] that adds the blindness property. The proposed group blind signature scheme is more efficient and secure than Lysyanskaya-Ramzan scheme [12].

1. Introduction

A group signature allow any member of a group to sign on behalf of the group. Group singatures 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 an bidding. 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 [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 rôle of the group manager and all other banks issuing coins are group members.

Group signatures were first introduced by Chaum and van Heijst [8] in 1991. A number of improvements and enhancements followed [1], [11], [16],

AMS (MOS) Subject Classification 1991. Primary:. Secondary: 94A60.
Key words and phrases: Group blind signature scheme, group signatures, blind signatures.

[18, 19]. However, in the schemes presented in [5], [8, 9], [13–16] 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 [4], 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 [2], which undoubtedly represents the state of the art in the field.

In this paper we propose a group blind signature shceme which combines the notions of group signatures and blind signatures [3], [6, 7], [10]. It is an extension of Camenisch and Michels's group signature scheme [2] that adds the blindness property and is more efficient and secure than Lysyanskaya-Ramzan scheme [12]. Our scheme is as secure and efficient as the basic group signature scheme proposed by Camenisch and Michels.

2. The Group blind Signature Scheme

Our group blind dignature scheme is an extension of Camenisch-Michels group signature scheme that adds the blindness property. Therefore, the proposed group blind signature scheme inherit almost all of the merits of the Camenisch-Michels scheme [2]. Participants are group members, a group manager, a revocation 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 signers (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 compytationally hard for everyone but the revocation manager.
4. Unlinkability: Deciding whether two different signatures were computed by the same group member is computationally hard.
5. Traceability: The revocation manager can always establish the identity of the member who issued a valid signature.
6. No framing: Even if the group manager, the revocaation manager and some of the group members collude, they cannot sign on behalf on non-involved group members.

7. Unforgeability of tracing verification: The revocation manager cannot accuse a signer of having originated a given signature.

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

1. **Setup:** *An interactive protocol between the group manager, the group members and the revocation manager. The public output is the group's public key* Y. *The private outputs are the individual secret keys* x_G *for the each group member, the secret key* x_M *for the group manager and the secret key* x_R *for the revocation manager.*
2. **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* x_G *and the group's public key* Y *outputs a signature* σ.
3. **Verify:** *An algorithm that on input a message* m, *a signature* σ *and the group's public key* Y *returns 1 if and only if* σ *was generated by any group member using the protocol* **Sign** *on input* x_G, m *and* Y.
4. **Tracing:** *A tracing algorithm that on input a signature* σ, *a message* m, *the revocation manager's secret key* x_R *and the group's public key* Y *returns the identity ID of the group member who issued the signature* σ *together with an argument arg of this fact.*
5. **Vertracing:** *A tracing verification algorithm that on input a signature* σ, *a message* m, *the group's public key* Y, *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, Y *and* x_R.

Definition 2. *The efficiency of a group blind signature scheme is typically based on the size of the group public key Y, the length of signature and the efficiency of the algorithms* **Sign**, **Verify**, **Setup**, **Tracing** *and* **Vertracing**.

The security of our grup blind signature scheme is based on the strong RSA assumption [2]. Let $n = pq$ be an RSA-like modulus and let G be a cyclic subgroup of Z_n^* of order l_g. Let k, l_1, $l_2 < l_g$ and $\varepsilon > 1$ be security parameters, and $\tilde{l} = \varepsilon(l_2 + k) + 1$.

Assumption 1 (Strong RSA Assumption). *There exists a probabilistic polynominal time algorithm* K *which on input* 1^{l_g} *outputs a pair* (n, z) *such that for all probabilistic polynominal-time algorithms* A *the probability that* A *can find* u *and* $e \in \{2^{l_1} - 2^{\tilde{l}}, \ldots, 2^{l_1} + 2^{\tilde{l}}\}$ *satisfying* $z \equiv u^e \pmod{n}$ *is negligible.*

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 iniquely 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 $g(G = <g>)$. 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 boty for the purpose of signing a message and profing knowledge of a secret. Signatures of knowledge were used by Camenisch and Michels [2] and their construction is based on the Schnorr signature scheme [17] to prove knowledge.

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

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

The next definition show the equality of two discrete logarithms.

Definition 4. *Let $\varepsilon > 1$ be a security parameter. A pair $(c, s) \in \{0,1\}^k \times \{-2^{l_g+k}, \ldots, 2^{\varepsilon(l_g+k)}\}$ satisfying $c = H(g||h||y_1||y_2||y_1^c g^s||y_2^c h^s||m)$ is a signature of a message $m \in \{0,1\}^*$ with respect to y_1 and y_2 and is denoted $SPK\{(\alpha) : y_1 = y^g \wedge y_2 = h^\alpha\}(m)$.*

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

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

This definition shows the knowledge of one out of two discrete logarithms. If the signer knows the secret key $x \in \{0,1\}^{l_g}$ such that $y_1 = g^x$, then be 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 $t_1 = g^{r_1}$, $t_2 = h^{r_2} y_2^{c_2}$, $c_1 = c_2 \oplus H(g||h||y_1||y_2||t_1||t_2||m)$, $s_1 = r_1 - c_1 x$, $s_2 = r_2$. The next block is based on a proof that the secret the prover knows lies in a given interval.

Definition 6. *Let $\varepsilon > 1$ be a security parameter. A pair $(c, s) \in \{0,1\}^k \times \{-2^{l_2+k}, \ldots, 2^{\varepsilon(l_2+k)}\}$ satisfying $c = H(g||y||g^{s-c2^{l_1}} y^c||m)$ is a signature of a message $m \in \{0,1\}^*$ with respect to y and is denoted $SPK\{(\alpha) : y = g^\alpha \wedge (2^{l_1} - 2^{\varepsilon(l_2+k)+1} < \alpha < 2^{l_1} + 2^{\varepsilon(l_2+k)+1})\}(m)$.*

This signature can be computed as follows. If the signer knows an integer $x \in \{2^{l_1}, \ldots, 2^{l_1} + 2^{l_2}\}$ such that $y = g^x$, he chooses $r \in_R \{0,1\}^{\varepsilon(l_2+k)}$ and computes $t = g^r$, $c = H(g\|y\|t\|m)$, $s = r - c(x - 2^{l_1})$.

The security properties and proofs of these building blocks follow from [1].

4. Our 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 [2].

4.1 Setup

The setup procedure of our scheme (as in [2]) is as follow. The group manager chooses a group $G =< g >$ and two random elements $z, h \in G$ with the same order 2^{l_g} such that the strong RSA assumption hold. He publishes z, g, h, G and l_g and proves that g, h and z have the same order which is non-prime, of the order 2^{l_g} and non-smooth. The group manager must further prove that z and h where chosen at random. The revocation manager chooses his secret key x randomly in $\{0, \ldots, 2^{l_g} - 1\}$ and publishes $y = g^x$ as his public key. Let be a collision resistant hash function $H : \{0,1\}^* \to \{0,1\}^k$ and security parameters $\hat{l}, l_1, l_2$ and ε. A possible choice of $G =< g >$ is a subgroup of Z_n^* such that $(g|n) = 1$. As in [1], to become a group member Alice chooses a random prime $\hat{e} \in_R \{2^{\hat{l}-1}, \ldots, 2^{\hat{l}} - 1\}$ and $e \in_R \{2^{l_1}, \ldots, 2^{l_1} + 2^{l_2} - 1\}$ such that $\hat{e}$, $e \not\equiv 1 \ (mod\ 8)$ and $\hat{e} \not\equiv e \ (mod\ 8)$. Alice computes $\tilde{e} := e\hat{e}$ and $\tilde{z} := z^{\hat{e}}$, commits to $\tilde{e}$ and $\tilde{z}$, sends $\tilde{e}$, $\tilde{z}$ and their commitments to the group manager and carries out the interactive protocol correpsonding to $SPK\{(\alpha, \beta) : z^{\tilde{e}} = \tilde{z}^{\alpha} \wedge \tilde{z} = z^{\beta} \wedge (2^{l_1} - 2^{\varepsilon(l_2+k)+1}) < \alpha < (2^{l_1} - 2^{\varepsilon(l_2+k)+1})\}(\tilde{z})$, with the group manager. The group manager computes $u := \tilde{z}^{\frac{1}{\tilde{e}}}$ and sends u to Alice, who checks that $\tilde{z} = u^{\tilde{e}}$ holds. The group manager stores $(u, \tilde{e}, \tilde{z})$ together with Alice's identity and her commitments to $\tilde{e}$ and $\tilde{z}$ in a group member list. Finally, Alice stores the pair (u, e) as her membership key.

4.2 Siogn

In this subsection we present our signature protocol which is blind, unlike [2]. First, we define a group blind signature and then we show how a group member can generate such a ggroup blind signature.

Definition 7. *Let ε, l_1, l_2 be security parameters such that $\varepsilon > 1$, $l_2 < l_1 < l_g$ and $l_2 < \dfrac{l_g - 2}{\varepsilon} - k$ holds. A group blind signature $sign(x_G(g, h, y, z), m)$ of a message $m \in \{0,1\}^*$ is a tuple $(c, s_1, s_2, s_3, a, b, d) \in \{0,1\}^k \times \{-$*

$2^{l_2+k}, \ldots, 2^{\varepsilon(l_2+k)}\} \times \{-2^{l_g+l_1+k}, \ldots, 2^{\varepsilon(l_g+l_1+k)}\} \times \{-2^{l_g+k}, \ldots, 2^{\varepsilon(l_g+k)}\} \times$ G^3 *satisfying*

$$c = H(g||h||y||z||a||b||d||z^c b^{s_1-c2^{l_1}}/y^{s_2}||a^{s_1-c2^{l_1}}/g^{s_2}||a^c g^{s_3}||d^c g^{s_1-c2^{l_1}} h^{s_3}||m).$$

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

1. Chooses an integer $\omega \in_R \{0,1\}^{l_2}$ and computes

$$a = g^\omega, \quad b = uy^\omega, \quad d = g^e h^\omega.$$

2. Chooses $\tilde{r}_1 \in_R \{0,1\}^{\varepsilon(l_2+k)}$ $\tilde{r}_2 \in_R \{0,1\}^{\varepsilon(l_g+l_1+k)}$ $\tilde{r}_3 \in_R \{0,1\}^{\varepsilon(l_g+k)}$ and computes

$$\begin{aligned} \tilde{t}_1 &= b^{\tilde{r}_1}/y^{\tilde{r}_2} \\ \tilde{t}_2 &= a^{\tilde{r}_1}/g^{\tilde{r}_2} \\ \tilde{t}_3 &= g^{\tilde{r}_3} \\ \tilde{t}_4 &= g^{\tilde{r}_1} h^{\tilde{r}_3}. \end{aligned}$$

3. Sends $(a, b, d, \tilde{t}_1, \tilde{t}_2, \tilde{t}_3, \tilde{t}_4)$ to the user.

In turn, the user doses the following:

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

$$\begin{aligned} t_1 &= \tilde{t}_1 b^{\gamma_1-\delta 2^{l_1}} z^\delta/y^{\gamma_2} \\ t_2 &= \tilde{t}_2 a^{\gamma_1-\delta 2^{l_1}} z^\delta/g^{\gamma_2} \\ t_3 &= \tilde{t}_3 a^\delta g^{\gamma_3} \\ t_4 &= \tilde{t}_4 d^\delta g^{\gamma_1-\delta 2^{l_1}} h^{\gamma_3}. \end{aligned}$$

2. Computes

$$\begin{aligned} c &= H(g||h||y||z||a||b||d||t_1||t_2||t_2||t_2||m) \\ \tilde{c} &= c - \delta. \end{aligned}$$

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

The signer does the following:

1. Computes

$$\begin{aligned} \tilde{s}_1 &= \tilde{r}_1 - \tilde{c}(e - 2^{l_1}) \\ \tilde{s}_2 &= \tilde{r}_2 - \tilde{c}e\omega \\ \tilde{s}_3 &= \tilde{r}_3 - \tilde{c}\omega. \end{aligned}$$

2. Sends $(\tilde{s}_1, \tilde{s}_2, \tilde{s}_3)$ to the user.

The user does the following:

1. Computes

$$\begin{aligned} s_1 &= \tilde{s}_1 + \gamma_1 \\ s_2 &= \tilde{s}_2 + \gamma_2 \\ s_3 &= \tilde{s}_3 + \gamma_3. \end{aligned}$$

2. The resulting signature of a message m is $(c, s_1, s_2, s_2, a, b, d)$.

The typle $(c, s_1, s_2, s_3, a, b, d)$ is a Camenisch-Michels group signature of a message m and the above protocol is a group blind signature scheme.

4.3 Verifying Signatures, Tracing and Verifying Tracing

The resulting singature $(c, s_1, s_2, s_3, a, b, d)$ of a message m can be verified as follows:

1. Compute

$$c' = H\Big(g||h||y||z||a||b||d||z^c b^{s_1 - c2^{l_1}} / y^{s_2} || a^{s_1 - c2^{l_1}} / g^{s_2} || a^c g^{s_3} || d^c g^{s_1 - c2^{l_1}} h^{s_3} || m\Big).$$

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

Given a signature $(c, s_1, s_2, s_3, a, b, d)$ of a message m, the revocation manager can find out which one of the group members issued this signature by checking its correctness. He aborts if the cignature is not correct. Otherwise, hte computes $u' = b/a^x$, issues a dignature

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

and reveals $arg := u'||P$. He then looks up u' in the group member list and will fond the corresponding u, the group members's identity and his commitment to $\tilde{e}$ and $\tilde{z}$.

Checking whether the revocation manager correctly revealed the originator of a signature $\sigma = (c, s_1, s_2, s_3, a, b, d)$ 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 Camenisch-Michels's group signature scheme [2], but more secure and efficient than Lysyanskaya-Ramzan's group blind signature scheme [12]. The proposed scheme is more secure and efficient than Lysyanskaya-Ramzan's scheme because the basic scheme Cameinsch-Michels [2] is more secure and efficient than the basic scheme Camenisch-Stadler [4]. We show only the correctness and the blidness of the signature. The others 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 $(c, s_1, s_2, s_3, a, b, d)$ is a correct group signature on m.*

Proof. The group signature $(c, s_1, s_2, s_3, a, b, d)$ is a correct group signature on m if the equality

$$c = H\left(g\|h\|y\|z\|a\|b\|d\|z^c b^{s_1 - c2^{l_1}} / y^{s_2} \| a^{s_1 - c2^{l_1}} / g^{s_2} \| a^c g^{s_3} \| d^c g^{s_1 - c2^{l_1}} h^{s_3} \| m\right)$$

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

$$\begin{aligned} z^c b^{s_1 - c2^{l_1}} / y^{s_2} &= z^{\tilde{c}+\delta} b^{\tilde{s}_1 + \gamma_1 - (\tilde{c}+\delta)2^{l_1}} / y^{\tilde{s}_2 + \gamma_2} = \tilde{t}_1 b^{\gamma_1 - \delta 2^{l_1}} z^{\delta} / y^{\gamma_2} = t_1 \\ a^{s_1 - c2^{l_1}} / g^{s_2} &= a^{\tilde{s}_1 + \gamma_1 - (\tilde{c}+\delta)2^{l_1}} / g^{\tilde{s}_2 + \gamma_2} = \tilde{t}_2 a^{\gamma_1 - \delta 2^{l_1}} / g^{\gamma_2} = t_2 \\ a^c g^{s_3} &= a^{\tilde{c}+\delta} g^{\tilde{s}_3 + \gamma_3} = \tilde{t}_3 a^{\delta} g^{\gamma_3} = t_3 \\ d^c g^{s_1 - c2^{l_1}} h^{s_3} &= d^{\tilde{c}+\delta} g^{\tilde{s}_1 + \gamma_1 - (\tilde{c}+\delta)2^{l_1}} h^{\tilde{s}_3 + \gamma_3} = \tilde{t}_4 d^{\delta} g^{\gamma_1 - \delta 2^{l_1}} = t_4. \quad \square \end{aligned}$$

Theorem 2. (Blindness) *If the user follows the protocol, then even a signer with unlimited computing power gets no information about m and the group signature $(c, s_1, s_2, s_3, a, b, d)$.*

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 $(\delta, \gamma_1, \gamma_2, \gamma_3)$. Given any view consisting of $\tilde{r}_1, \tilde{r}_2, \tilde{r}_3, \tilde{t}_1, \tilde{t}_2, \tilde{t}_3, \tilde{t}_4, \tilde{c}, \tilde{s}_1, \tilde{s}_2, \tilde{s}_3$ and any group signature $(c, s_1, s_2, s_3, a, b, d)$ of a message m, we consider $\delta = c - \tilde{c}$, $\gamma_1 = s_1 - \tilde{s}_1$ $\gamma_2 = s_2 - \tilde{s}_2$ $\gamma_3 = s_3 - \tilde{s}_3$. It is easy to verify that the following equations hold:

$$\begin{aligned} \tilde{t}_1 b^{\gamma_1 - \delta 2^{l_1}} z^{\delta} / y^{\gamma_2} = b^{\tilde{r}_1 + \gamma_1 - \delta 2^{l_1}} z^{\delta} / y^{\tilde{r}_2 + \gamma_2} = z^c b^{s_1 - c2^{l_1}} / y^{s_2} &= t_1 \\ \tilde{t}_2 a^{\gamma_1 - \delta 2^{l_1}} / g^{\gamma_2} = a^{\tilde{r}_1 + \gamma_1 - \delta 2^{l_1}} / g^{\tilde{r}_2 + \gamma_2} = a^{s_1 - c2^{l_1}} / g^{s_2} &= t_2 \\ \tilde{t}_3 a^{\delta} g^{\gamma_3} = g^{\tilde{r}_3 + s_3 - \tilde{s}_3} a^{c - \tilde{c}} = a^c g^{s_3} &= t_3 \\ \tilde{t}_4 d^{\delta} g^{\gamma_1 - \delta 2^{l_1}} = g^{\tilde{r}_1 + \gamma_1 - \delta 2^{l_1}} d^{\delta} h^{\gamma_3 - \tilde{r}_3} = d^c g^{s_1 - c2^{l_1}} h^{s_3} &= t_4. \end{aligned}$$

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

In order to improve the efficiency of our group blind signature scheme a better choice for G is the set of quadratic residues modulo n, denoted by Q_n and to extend the certificate structure in [1].

6. Conclusion

In this paper we proposed a group blind signature scheme that is secure and efficient and it is an extension of Camenisch-Michels's group signature scheme [2]. Our group blind signature scheme is more efficient and secure than Lysyanskaya-Ramzan's group blind signature scheme [12]. Also, the proposed scheme is as efficient and secure as the basic group signature scheme proposed by Camenisch and Michels.

7. References

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

[2] J. Camenisch, M. Michels, *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.

[3] J. Camenisch, J. Piveteau, M. Stadler, *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.

[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, 1997, pp. 410-424.

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

[6] D. Chaym, *Blind signatures for untraceable payments*, Advances in Cryptology-CRYPTO'82, Plenum Press, 1983, pp. 199-203.

[7] D. Chaum, *Blind signature systems*, Advances in Cryptology-CRYPTO'83, Plenum Press, 1984, pp. 153.

[8] C. Chaum, E. van Heyst, *Group signatures*, Advances in Cryptology-EUROCRYPT'01, Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 257-265.

[9] L. Chen, T. Pedersen, *New group signature schemes*, Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1995, pp. 171-181.

[10] P. Horster, M. Michels, H. Petersen, *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.

[11] W. Lee, C. Chang, *Efficient group signature scheme based on the discrete logarithm*, IEE Proc. Comput. Digit. Tech. 145, No. 1, 1998, pp. 15-18.

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

[13] S. Kim, S. Park, D. Won, *Convertible group signatures*, Advances in Cryptology-ASIACRYPT'96, Lecture Notes in Computer Science, vol. 1163, Springer-Verlag, 1996, pp. 311-321.

[14] S. Park, I. Lee, D. Won, *A practical group signature*, Proceedings of the 1995 Japan-Corea Workshop on Information Security and Cryptography, 1995, pp. 127-133.

[15] S. Park, S. Kim, D. Won, *ID-based group signature schemes*, Electronics Letters, 1997, pp. 1616-1617.

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

[17] C. P. Schnorr, *Efficient signature genration for smart cards*, Journal of Cryptology, 4(3): 1991, pp. 239-252.

[18] Y. Tseng, J. Jan, *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.

[19] Y. Tseng, J. Jan, *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, 3700 Bihor, Romania
E-mail: cpopescy@math.uoradea.ro

Received 15 Jan. 2000.