A New Efficient Group Signature With Forward Security

Jianhong Zhang, Qianhong Wu and Yumin Wang
State key Lab. of Integrated Service Networks, Xidian Univ, Xi'an
Shannxi 710071, China
E-mail: jhzhs@hotmail.com, woochanhoma @hotmail.com, ymwang@xidian.edu.cn

Keywords: group signature, forward security, revocation, anonymity, unlikability

Received: October 15, 2003

A group signature scheme allows a group member to sign a message anonymously on behalf of the group. In case of a dispute, the group manager can reveal the actual identity of signer. In this paper, we propose a novel group signature satisfying the regular requirements. Furthermore, it also achieves the following advantages: (1) the size of signature is independent of the number of group members; (2) the group public key is constant; (3) Addition and Revocation of group members are convenient; (4) it enjoys forward security; (5) The total computation cost of signature and verification requires only 8 modular exponentiations. Hence, our scheme is very practical in many applications, especially for the dynamic large group applications.

Povzetek: Predstavljena je nova shema skupinskega podpisa.

1 Introduction

Digital signatures play an important role in our modern electronic society because they have the properties of integrity and authentication. The integrity property ensures that the received messages are not modified, and the authentication property ensures that the sender is not impersonated. In well-known conventional digital signatures, such as RSA and DSA, a single signer is sufficient to produce a valid signature, and anyone can verify the validity of any given signature. Because of its importance, many variations of digital signature scheme were proposed, such as blind signature, group signature, undeniable signature etc, which can be used in different application situations.

A group signature was introduced by Chaum and van Heyst [1]. It allows any member of a group to anonymously sign a document on behalf of the group. A user can verify a signature with the group public key that is usually constant and unique for the whole group. However, he/she cannot know which individual of the group signs the document. Many group signature schemes have been proposed [1,2,3,5,6,7,8]. All of them are much less efficient than regular signature schemes. Designing an efficient group signature scheme is still an open problem. The recent scheme proposed by Ateniese et al. is particularly efficient and provably secure [2]. Unfortunately, several limitations still render all previous solution unsatisfactory in practice. Giuseppe Ateniese pointed out two important problems of group signature in [3]. One is how to deal with exposure of group signing keys; the other is how to allow efficient revocation.

In this paper, we propose a novel and efficient group signature scheme with forward security to solve the above two important problems. The concept of forward security was proposed by Ross Anderson [4] for traditional signature. Several schemes have recently been proposed for traditional signatures and threshold signatures that satisfy the efficiency properties. Previous group signature schemes don't provide forward security. Forward secure group signature schemes allows individual group member to join or leave a group or update their private signing keys without affecting the public group key. By dividing the lifetime of all individual private signing keys into discrete time intervals, and by tying all signatures to the time interval when they are produced, group members who are revoked in time interval *i* have their signing capability effectively stripped away in time interval *i*+1, while all their signature produced in time interval *i* or before remain verifiable and anonymous. In 2001, Song [5] firstly presented a practical forward security group signature scheme. Our proposed scheme is a little more efficient than Song's scheme.

The rest of this paper is organized as follows. In section 2, we overview the informal model of a secure group signature scheme and security requirements. After our group signature scheme is proposed in section 3, we give the corresponding security analysis to the scheme in section 4. in section 5, we analyze the efficiency of our proposed scheme and compares the cost with the Song's scheme. Finally, we conclude this paper.

2 Group Signature Model and Security Requirements

The concept of group signature was introduced by Chaum and van Heyst [1]. It allows a group member to sign anonymously a message on behalf of the group. Any one can verify group signature with the group public key. In case of a dispute, the group manager can open the signature to identify the signer.

Participants: A group signature scheme involves a group manager (responsible for admitting/deleting members and for revoking anonymity of group signature, e.g., in case of dispute or fraud), a set of group members, and a set of signature verifiers, all participants are modeled as probabilistic polynomial-time interactive Turing machines. A group signature scheme is comprised of the following procedure.

Communication: All communication channels are assumed asynchronous, The communication channel between a signer and a receiver is assumed to be anonymous.

A group signature scheme is comprised of the following procedure:

Setup: On inputting a security parameter *l*, this probabilistic algorithm outputs the initial group *PK* and the secret key *SK* for the group manager.

Join: An interactive protocol between the group manager and a user that results in the user becoming a valid group member.

Sign**:** An interactive protocol between a group member and a user whereby a group signature on a message supplied by a user is computed by the group member.

Verify**:** A deterministic algorithm for verifying the validity of a group signature given a group public key and a signed message.

Open**:** A deterministic algorithm that, given a signed message and a group secret key, determines the identity of the signer.

A secure group signature should meet the following requirements:

Correctness: Signature produced by a group member using Sign must be accepted by **Verifying**.

Unforgeability: Only group members are able to sign messages on behalf of the group

Anonymity: Given a signature, identifying the actual signer is computationally hard for any one except the group manager.

Unlinkability: Deciding whether two different signatures were generated by the same group member is computationally hard.

Exculpability: Even if the group manager and some of the group member collude, they cannot sign behalf of non-involved group members.

Traceability: The group manager can always establish the identity of the member who issued a valid signature.

Coalition-resistance: a colluding subset of group members cannot generate a valid group signature that cannot be traced.

To achieving practicability, in this paper, we propose a group signature scheme supporting the above properties and another two attributes, revocation and forward security, as well.

Revocability: the group manager can revoke membership of a group member so that this group member cannot produce a valid group signature after being revoked.

Forward security: When a group signing key is exposed, previously generated group signatures remain valid and do not need to be re-sign.

3 Preliminaries

The building block presented in this subsection is an protocols for proving the knowledge of a discrete logarithm to the setting with a group of unknown order.

Definition 1. Let $\varepsilon > 1$ be a security parameter. A pair $(c,s) \in \{0,1\}^k \times \{-2^{l+k},\dots,2^{\varepsilon(k+l)}\}$ 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 denotes SPK$\{\alpha\colon y=g^{\alpha}\}$(m).

An entity knowing the secret key $x \in \{0,1\}^l$ such that $x = \log_g y$ can compute such a signature $(c, s) =$ SPK$\{\alpha\colon y=g^{\alpha}\}$(m) of a message $m \in \{0,1\}^*$ by

- choosing $r \in \{0,1\}^{\varepsilon(l+k)}$ and computing $t = g^r$
- $c = h(g \| y \| t \| m)$ and
- $s=r-cx$ (*in Z*)

SPK$\{\alpha\colon y=g^{\alpha}\}$(“”) denotes Signature of Knowledge on space message.

The security of all these building blocks has been proven in the random oracle model under the strong RSA assumption.

4 Our Proposed Group Signature

parameter:

GM: group manager,

ID_{GM} :Identity of group manager,

ID_B : Identity of group member Bob

n : a RSA modular number.

$h(.)$: a one-way hash function $\{0,1\}^* \rightarrow \{0,1\}^k$

SPK : signature of knowledge.

4.1 System Parameters

The group manager (GM) randomly chooses two large primes p_1, p_2 of the same size such that $p_1 = 2p_1' + 1$ and $p_2 = 2p_2' + 1$, where both p_1' and p_2' are also primes. Let $n = p_1 p_2$ and $G = \langle g \rangle$ a cyclic subgroup of Z_n^*. GM randomly chooses an integer x as his secret key and computes the corresponding public key $y = g^x (\bmod n)$. GM selects a random integer e (e.g., $e = 3$) which satisfies $\gcd(e, \varphi(n)) = 1$ and computes d satisfying $de = 1 \bmod \varphi(n)$ where $\varphi(n)$ is the Euler Totient function. $h(\cdot)$ is a coalition-resistant hash function (e.g., SHA-1, MD5). The time period is divided into T intervals and the intervals are publicly known. $(c,s) = SPK\{\gamma : y = g^{\gamma}\}('')$ denotes the signature of knowledge of $\log_g y$ in *G* (See [2,6] for details). Finally, the group manager publishes the public key $(y, n, g, e, h(\cdot), ID_{GM}, T)$, where ID_{GM} is the identity of the group manager.

4.2 Join Procedure

If a user, say Bob, wants to join to the group, Bob executes an interactive protocol with GM. Firstly, Bob chooses a random number $k \in Z_n^*$ as his secret key and computes his identity $ID_B = g^k (\bmod n)$ and the signatures of knowledge $(c,s) = SPK\{\gamma : ID_B = g^\gamma\}('')$, which shows that he knows a secret value to meet $ID_B = g^k (\bmod n)$. Finally, Bob secretly preserves k and sends $(ID_B, (c,s))$ to the group manager.

After the group manager receives $(ID_B, (c,s))$, he firstly verifies the signatures (*c*, *s*) of knowledge by $(ID_B, (c,s))$. If the verification holds, GM stores $(ID_B, (c,s))$ in his group member database and then generates membership certificate for Bob. Thereby, GM randomly chooses a number $\alpha \in Z_n^*$ and computes as follows.

$$r_B = g^\alpha \bmod n \text{ , } s_B = a + r_B x$$

$$w_{B_0} = (ID_{GM} r_B ID_B)^{-d^T} \bmod n$$

GM sends (s_B, r_B, w_{B_0}) to Bob via a private channel. GM stores (s_B, r_B, w_{B_0}) together with $(ID_B, (c,s))$ in his local database.

After Bob receives (s_B, r_B, w_{B_0}), he verifies the following relations

$$g^{s_B} = r_B y^{r_B} \bmod n$$

$$ID_{GM} ID_B r_B = w_{B_0}{}^{-e^T} (\bmod n)$$

If both the above equations hold, Bob stores (s_B, r_B, w_{B_0}) as his resulting initial membership certificate.

4.3 Evolving Procedure

Assume that Bob has the group membership certificate (s_B, r_B, w_{B_j}) at time period *j*. Then at time period *j*+1, he can compute new group membership certificate via **Evolving** function $f(x) = x^e (\bmod n)$ and then his new group membership certificate becomes $(s_B, r_B, w_{B_{j+1}})$ where $w_{B_{j+1}} = (w_{B_j})^e \bmod n$.(**Note that** $w_{B_j} = (g^{s_B} ID_{GM} ID_B)^{-d^{T-j}} \bmod n$).

4.4 Sign Procedure

Suppose that Bob has the group membership certificate (s_B, r_B, w_{B_j}) at time period *j*. To sign a message *m* at time period *j*, Bob randomly chooses three numbers $q_1, q_2, q_3 \in Z_n^*$ and computes

$$z_1 = g^{q_1} y^{q_2} q_3^{e^{T-j}} \bmod n \text{ ,}$$

$$u = h(z_1, m)$$

$$r_2 = q_3 w_{B_j}^u \bmod n \text{ ,}$$

$$r_1 = q_1 + (s_B + k)u$$

$$r_3 = q_2 - r_B u \text{ ,}$$

The resulting group signature on *m* is (u, r_1, r_2, r_3, m, j).

4.5 Verify Procedure

Given a group signature (u, r_1, r_2, r_3, m, j), a verifier validates whether the group signature is valid or not. He computes as follows

1) $z_1' = ID_{GM}^u g^{r_1} r_2^{h(r_2)e^{T-j}} y^{r_3} \bmod n$

$$\begin{aligned}
&= ID_{GM}^u g^{q_1+(k+s_B)u} q_3^{e^{T-j}} w_{B_j}^{ue^{T-j}} y^{r_3} \bmod n \\
&= ID_{GM}^u g^{q_1} g^{s_B u} q_3^{e^{T-j}} g^{ku} (r_B ID_{GM} ID_B)^{-e^{T-j} d^{T-j} u} y^{q_2 - r_B u} \\
&= ID_{GM}^u g^{q_1} q_3^{e^{T-j}} g^{s_B u} ID_B^u (r_B ID_{GM} ID_B)^{-u} y^{-r_B u} y^{q_2} \\
&= g^{q_1} y^{q_2} q_3^{e^{T-j}}
\end{aligned} \tag{1}$$

2) checks $u' = h(z_1', m)$

and checks whether the equation $u \overset{?}{=} u'$ holds or not. If it holds, the verifier is convinced that (*u*,r$_1$,r$_2$,r$_3$,*m*,*j*)is a valid group signature on *m* from a legal group member.

4.6 Open Procedure

In case of a dispute, GM can open signature to reveal the actual identity of the signer who produced the signature. Given a signature(*u*,r$_1$,r$_2$,r$_3$,*m*,*j*), GM firstly checks the validity of the signature via the **VERIFY** procedure. Secondly, GM computes the following steps:

Step 1: computes $\eta = 1/u \bmod \phi(n)$.

Step2: computes $z_1' = ID_{GM}^u g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n$.

Step 3: checks $r_2 / w_B^\eta = (z' / g^{r_1} y^{r_3}{}_1)^{d^{T-j}} \bmod n$.

If there is the corresponding w_B with (r_B, ID_B) satisfying the above Step3, it is concluded that ID_B is the actual identity of the signer.

4.7 Revoking Procedure

Suppose the membership certificate of the group member Bob need to be revoked at time period *j*, the group manager computes the following quantification:

$$R_j = w_B (r_B ID_B)^{d^{T-j}} \bmod \mathrm{n}$$

and publishes duple (R_j, j) in the CRL(the Certificate Revocation List). Given a signature (,*u*,r$_1$,r$_2$,r$_3$,*m*,*j*), when a verifier identifies whether the signature is produced by a revoked group member or not, he computes the following quantification

Step 1: $z_1' = ID_{GM}^{u} g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n$

Step 2: $z_1'(r_2^{-1} R_j^{u})^{e^{T-j}} = g^{r_1} y^{r_3} \bmod n$ (2)

For the signature (u, r_1, r_2, r_3, m, j), if the signature satisfies the above equation (2). We can conclude that the signature is revoked.

5 Security Analysis

In this subsection we show that our proposed group signature scheme is a secure group signature scheme and satisfies forward security.

Correct: we can conclude that a produced group signature by a group member can be identified from **equation (1)** of the above **Verifying Procedure.**

Anonymity: Given a group signature(u,r$_1$,r$_2$,r$_3$,m,j), z_1 is generated through two random numbers q_1 and q_2 which are used once only and $u = h(z_1, m)$, so that we can infer that u is also a random number generated by random seed z_1**.** Any one (except for a group manager) cannot obtain any information about the identity of this signer from the group signature(u,r$_1$,r$_2$,r$_3$,m,j).

Unlinkability: Given time period j, two different group signatures(u,r$_1$,r$_2$,r$_3$,m,j)and (u',r'$_1$,r'$_2$,r'$_3$,m', j), we can know that u (or u') is a random number generated by random seed z_1**,** and u **is** different in each signing procedure and used once only, and u **or** random number q_1 and q_2 are included in r_1 and r_2 . However, an adversary cannot get the relation between the signature (u,r$_1$,r$_2$,r$_3$,m,j)and the signature(,u',r'$_1$,r'$_2$,r'$_3$,m', j).

Unforgeability: In this group signature scheme, the group manager is the most powerful forger in the sense. If the group manager wants to forge a signature at time period j, he chooses (z$_1$, r_2, r_3, j) (or (z$_1$, r_2, r_1, j)) and computes u=h(z$_1$, m). According to the equation (1), for solving r_1, he needs solve the discrete logarithm so that he cannot forge a group signature.

Furthermore, as an adversary, because an adversary hasn't a valid membership certificate, he cannot forge a group signature satisfying the verification procedure. And in view of the group manager, he cannot forge a valid group signature without knowing private k of group member.

Forward Security: Assume an attacker breaks into a group member's system in time period j and obtains the member's membership certificate. Because of the one-way property of $f(x)$, the attacker cannot compute this member's membership certificate corresponding to previous time period. Hence the attacker cannot generate the group signature corresponding to the previous time.

Assume that the group member Bob is revoked at time period j, the group manager only revokes the group membership certificate of the time period j. then any valid signature with corresponding time period before j is still accepted. Because of the obtained signature (u,r$_1$,r$_2$,r$_3$,m,t),t<j. the signature (u, r$_1$,r$_2$,r$_3$,m,j) is still a valid signature on m and Bob would not need to produce a new signature on m .

Revocation: When a user, say Bob, is expelled from the group starting from the time period i, R_i and i will be published in CRL. Assume a verifier has a signature for period j, where $j \geq i$. To check whether the membership certificate of the group member has been expelled, the verifier simply computes $R_j = (R_i)^{e^{j-i}}$ and checks whether the equation $z_1'(r_2^{-1} R_j^{u})^{e^{T-j}} = g^{r_1} y^{r_3} \bmod n$ holds or not. If it holds, it means that the signature has been revoked.

Collision-resistant: Assume that two group members collude to forge a signature. Because they don't know factorization of n and membership certificate of Bob, Furthermore, in Join phase, though the identification for each group member is computed by themselves according to number k , for two conspiracy group members, it is equivalent to forge group manager Schnorr signature to produce a new membership certificate for them. So that they cannot produce a valid membership certificate. Suppose that the group manager and a group member collude to produce the signature of a group member Bob. because they don't know the private key k or $(r_B, s_B w_{B_i})$ of group member Bob respectively, they cannot forge Bob 's signature.

Efficiency**:** for the whole signature phase and verification phase, our scheme only needs 7 modular exponentiations, however, Song's scheme needs more than 20 modular exponentiations. This implies that our scheme is very practical in large group applications.

6 Efficiency Analysis

In this section we show the efficiency of our scheme over that of Song scheme. In a signature scheme, the computational cost of signature is mainly determined by modular exponentiation operator. Let E, M and H respectively denote the computational load for exponentiation, multiplication and hash. Then the following table shows the comparison of computational load of our scheme vs. Song scheme.

Table1: our scheme vs. Song scheme

Scheme	Signing phase computation	Verifying phase computation	Total computation
Song's Scheme	22E+1H+6M	14E+1H+6M	36E+2H+12M
Proposed Scheme	4E+3H+5M	4E+3M+1H	8E+8M+4H

Signing phase and verifying phase in our scheme have less computation against Song's scheme. Modular exponentiation is a complicated operator and plays a determinate role in a signature scheme. From the above data, we conclude that our scheme has computational advantage over that of Song. To the best of our knowledge, it takes the much least computation in group signature schemes. Hence, Our proposed scheme is suitable to large group.

7 Conclusion

In this paper, we propose a new group signature scheme with forward-security. Our scheme satisfies not only the traditional security properties of the previous group signature schemes, but also forward security. Our scheme is efficient in the sense in that it is independent of the number of the group members and the size of group signature and the size of group key are independent of the number of time periods and the number of revoked members. Our scheme is a practical group signature scheme.

Reference

[1] D. Chaum, F. Heyst. (1992) Group Signature. Proceeding EUROCRYPT'91. Springer-verlag, pp. 257-265.

[2] G.Ateniese,J. Camenish, M. Joye, and G. Tsudik. (2000) A Practical and Provably Secure Coalition-Resistant Group signature Scheme. In M.Bellare, editor, Crypto'2000, vol(1880) of LNCS, Springer–Verlag, pp. 255-270.

[3] G. Ateniese and G. Tsudik.(1999)Some Open Issues and New Direction in Group Signature. In Financial Cryptograph'99,

[4] Ross Anderson. (1997) Invited Lecture, 4th ACM Computer and Communications Security.

[5] Dawn Xiaodong Song,(2000) Practical forward secure group signature schemes. Proceedings of the 8th ACM conference on Computer and Communications Security, Pennsylvania, USA, November, pp. 225-234.

[6] J. Camenish and M. Michels. (1999) A Group Signature with Improved Efficiency. K. Ohta and. Pei, editors, Asiacrypt'98.Vol 1514 of LNCS, Springer-Verlag, pp. 160-174.

[7] W. R. LEE, C. C. CHANG. (1998)Efficient Group Signature Scheme Based on the Discrete Logarithm. IEE Proc. Computer Digital Technology, vol.145 (1), pp.15-18.

[8] Constantin Popescu. (20001)An Efficient Group Signature Scheme for Large Groups. STUDIES ININFORMATICS AND CONTROL With Emphasis on Useful Applications of Advanced Technology, Vol.10 (1), pp. 3-9.

[9] Emmanuel Bresson and Jacques Stern.(2001)Efficient Revocation in Group Signature.PKC'2001, LNCS 1992, Springer-verlag, Berlin Heidelberg pp. 190-206, 2001.

[10] Michel Abdalla and Leonid Reyzin.(2000) A new forward secure digital signature scheme. In ASIACRYPT, Springer-Verlag, pp. 116-129.

[11] Y. Tseng, J. Jan. (1998) A novel ID-based group signature, In T.L Hwang and A.K.Lenstra, editors, international Computer Symposium, Workshop on Cryptology and Information Security, Tainan, 1998, pp. 159-164.

[12] C. Popescu. (2000)Group signature schemes based on the difficulty of computation of approxi-mate e-th roots, Proceedings of Protocols for Multimedia Systems (PROMS2000), Poland, pp. 325-331,

[13] S.Kim, S.Park, D.Won, (1998) Group signatures for hierarchical multi-groups, Information Security Workshop, Lecture Notes in Computer Sciences 1396, Springer-Verlag, pp. 273-281.

[14] M.Stadler,(1996)Publicly verifiable secret sharing, Advances in Cryptology, EUROCRYPT'96 lecture Notes in Computer Sciences 1070, Springer-Verlag, 1996, pp. 190-199.

[15] A. Fiat and A. Shamir.(1986) How to prove yourself: practical solutions to identification and signature problems. In Advances in Cryptology-CRYPTO'86, vol. 263 of LNCS, pp.186–194, Springer -Verlag,

[16] S. Goldwasser, S. Micali,and R.Rivest.(1988) A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 17(2): 281–308,

[17] J. Kilian and E. Petrank.(1998) Identity escrow. In Advances in Cryptology —CRYPTO'98, vol.1642 of LNCS, pp. 169–185, Springer-Verlag,

[18] A. Lysyanskaya and Z. Ramzan. (1998)Group blind digital signatures: A scalable solution to electronic cash. In Financial Cryptography (FC'98), vol. 1465 of LNCS, pp. 184–197, Springer-Verlag

[19] R.Gennaro, H.Krawczyk,and T.Rabin (2000) RSA-based Undeniable Signature. J. Cryptology, Volume (13)4, pp 397-416

[20] Giuseppe Ateniese, B. de Medeiros,Efficient Group Signatures without Trapdoors , In ASIACRYPT 200