A New Group Signature Scheme

XUN YI[1], CHIK HOW TAN[1], CHEE KHEONG SIEW[1] and YIMING YE[2]

[1]Information Communication Institute of Singapore
School of Electrical and Electronic Engineering
Nanyang Technological University
SINGAPORE 639798
e-mail: exyi@ ntu.edu.sg

[2] IBM T.J. Watson Research Center
P. O. Box 704, Yorktown Heights, NY 10598
USA
e-mail: yiming@us.ibm.com

Abstract: – This paper comes up with a new group signature scheme based the discrete logarithm in which a group member can sign messages on behalf of group. This scheme can provide anonymity and untraceability for the signer with respect to the signature verifier but not to the group manager.

Key-words: – Cryptography, digital signature, group signature

1 Introduction

In [1] Chaum and Van Heyst proposed a new type of signature scheme for a group of entities, called group signatures. Such a scheme allows a group member to sign a message on the group's behalf such that everybody can verify the signature but no one can find out which group member produces it. However, there is a trusted third party, call the group manager, who can reveal the identity of the originator of a signature in the case of later dispute. This act is referred to as "opening" a signature or also as revocation of a signer's anonymity.

Group signature could for instance be used by a company for authenticating price lists, press releases, or digital contracts. The customers need to know only a single company public key to verify signatures. The company can hide any internal organizational structures and responsibilities, but can still find out which employee (i.e., group member) has signed a particular document.

Four group signature schemes were first presented in [1], but none of them perform optimally with respect to inclusion of new group member and identification of the signer by the group manager. Both of these problems were solved in [2], however, the proposed schemes are inefficient. In 1998, Lee and Chang suggested an efficient group signature scheme based on the discrete logarithm in [3]. In this scheme, different group signatures of a signer for different messages contain some identical information, there is a connotative linkage between signature and the signer. In 1999, Tseng and Jan proposed an improved group signature scheme in [4], which is based on the Lee-Chang scheme. The improved scheme is designed to avoid the connotative linkage in Lee-Chang scheme. However, Sun showed in [5] that the scheme is still not unlinkable. After that, Tseng and Jan presented another improvement in [6] to avoid the signature linkage. Recently, Li, Hui and et al. gave two efficient forgery attacks on two Tseng-Jan schemes in [7].

As far as we know, most of the previous group signature schemes are either inefficient or insecure. In this paper, we present a novel group signature scheme which is not only secure but also efficient. The proposed scheme provides anonymity and untraceability for the signer with respect to the signature verifier but not to the group manager.

2 Proposed Group Signature Scheme

The proposed scheme involves three parties, viz., group manager (GM), group members (U_i) and signature verifier (V). The GM is a trusted third party. Similar to Digital Signature Standard (DSS), we assume:

(1) This scheme chooses three parameters (p, q, g), where p is a large prime, q is a large prime factor of $p-1$, $g = \ell^{(p-1)/q}\ (mod\ p)$ with ℓ being an integer satisfying $1 < \ell < p-1$ and $\ell^{(p-1)/q}\ (mod\ p) > 1$ and (p, q, g) is public.

(2) The GM has a pair of signature private-public key $(x_{\rm GM}, y_{\rm GM})$, where $y_{\rm GM}(= g^{x_{\rm GM}}\ (mod\ p))$ is public to all participants in this scheme and $x_{\rm GM}$ is the private key chosen randomly from $GF(q)^*(= \{1, 2, \cdots, q-1\})$ and known only to itself. It is reasonable to assume $y_{\rm GM} \neq g\ (mod\ p)$.

(3) An one-way hash function (h), mapping its input with arbitrary length into a substantial subset of $GF(q)$, is public to all participants in this scheme.

Under the above assumptions, the proposed scheme can be described in the following phases:

2.1 Certificate issuing

The proposed scheme begins with certificate issuing phase in which the group member U_i applies for his signature certificate from the group manager GM and the GM issues a certificate to the U_i as follows:

1. The U_i randomly chooses a private key x_i from $GF(q)^*$ and then computes $y_i = g^{x_i}$ $(mod\ p)$. x_i is known only to himself. Then, the U_i submits his identity I_i with y_i to the GM through a secure internal channel.

2. After receiving the (I_i, y_i), the GM constructs the U_i's certified information by concatenating y_i with the common information C validating signatures of the U_i. It should be pointed out that the C must not leak out any information by which the U_i may be identified or traced by any verifier. The signature of the GM on the certified information $y_i \| C$ is the pair (α_i, γ_i) produced in the following formulae:

$$\alpha_i = g^w \cdot y_i^{-1}\ (mod\ p),\ w \in_R GF(q)^* \quad (1)$$

$$\gamma_i = h(C) \cdot w + \alpha_i \cdot x_{\rm GM}\ (mod\ q) \quad (2)$$

where the symbol $\in_R$ $GF(q)^*$ represents randomly choosing the element from $GF(q)^*$; y_i^{-1} (the inverse of y_i) can be obtained by Euclid algorithm because $gcd(y_i, p) = 1$; the symbol "$\|$" denotes the concatenation of two messages. Whereafter, the GM replies to the U_i with the certificate $y_i \| C \| (\alpha_i, \gamma_i)$ through the secure internal channel.

Note: The GM must assign distinct $\alpha_i (mod\ q) (\neq 0 (mod\ q))$ to distinct group members and save $(I_i, \alpha_i (mod\ q))$ in order to uniquely identify the originator of a group signature later.

3. The certified U_i can verify whether (α_i, γ_i) is indeed a genuine signature of the GM on $y_i \| C$ by checking the following congruence:

$$g^{\gamma_i} \;=\; (\alpha_i \cdot y_i)^{h(C)} \cdot y_{\mathrm{GM}}^{\alpha_i} \;(mod\ p) \quad (3)$$

The certified U_i can accept the certificate if the above congruence holds.

2.2 Signing

Knowing the certificate $y_i \| C \| (\alpha_i, \gamma_i)$ issued by the GM and x_i such that $y_i = g^{x_i}\ (mod\ p)$, the U_i can generate group signature on any message M as follows:

$$\begin{aligned}
t &= g^{\varphi}\ (mod\ p),\ \varphi \in_R GF(q)^* && (4)\\
\eta &= \alpha_i \cdot t\ (mod\ q) && (5)\\
\theta &= \alpha_i \cdot t\ (mod\ p) && (6)\\
\alpha &= p \cdot \eta - (p-1) \cdot \theta\ (mod\ p \cdot q) && (7)\\
\beta &= \alpha^{t}\ (mod\ p) && (8)\\
\gamma &= \gamma_i \cdot t + (\varphi - x_i) \cdot t \cdot h(C)\ (mod\ q) && (9)\\
\mu &= (\alpha^{\xi}\ (mod\ p))(mod\ q),\ \xi \in_R GF(q)^* && (10)\\
\nu &= \xi^{-1}(h(\alpha, \beta, \gamma, \mu, M) + \mu \cdot t)\ (mod\ q) && (11)
\end{aligned}$$

The group signature of U_i on M takes the form of $(\alpha, \beta, \gamma, \mu, \nu)$.

2.3 Verifying

The group signature $(\alpha, \beta, \gamma, \mu, \nu)$ on M can be verified by the verifier V on basis of C, y_{GM} and the following incongruence and congruences:

$$\begin{aligned}
\alpha \cdot \gamma &\neq 0\ (mod\ q) && (12)\\
g^{\gamma} &= \beta^{h(C)} \cdot (y_{\mathrm{GM}})^{\alpha}\ (mod\ p) && (13)\\
\mu &= ((\alpha^{h(\alpha,\beta,\gamma,\mu,M)} \cdot \beta^{\mu})^{\nu^{-1}} \\
&\quad (mod\ p))(mod\ q) && (14)
\end{aligned}$$

The group signature is genuine if all of the above incongruence and congruences hold.

2.4 Identifying

In case of later dispute, the group manager GM can open a group signature $(\alpha, \beta, \gamma, \mu, \nu)$ on M generated by a group member U_i or revoke the signer's anonymity in the following way (Note: The signature is usually provided by V):

1. The GM verifies the authenticity of the group signature $(\alpha, \beta, \gamma, \mu, \nu)$ on the message M in accordance with incongruence (12) and congruences (13)-(14). If all are ture, the group signature is valid.

2. For each record $(I_x, \alpha_x\ (mod\ q))$, the GM checks whether the following congruence holds:

$$\beta^{\alpha_x} = \alpha^{\alpha}\ (mod\ p) \quad (15)$$

We can prove the above congruence has a unique solution $(I_i, \alpha_i\ (mod\ q))$. In this way, the identity of the U_i can be revealed by the GM.

3 Features of the Proposed Scheme

As far as the proposed scheme is concerned, we can conclude two theorems.

Theorem 1: The difficulty of forging a group signature $(\alpha, \beta, \gamma, \mu, \nu)$ on a message M which satisfies incongruence (12) and congruences (13)-(14) without holding a group member's certificate $y_i \| C \| (\alpha_i, \gamma_i)$ and knowing x_i such that $y_i = g^{x_i}\ (mod\ p)$ is equivalent to that of computing discrete logarithm over $GF(q)^*$.

The above theorem implies only group members can produce valid group signatures.

Theorem 2: Given a group member U_i's signature $(\alpha, \beta, \gamma, \mu, \nu)$ on a message M which satisfies incongruence (12) and congruences (13)-(14), except for the group manager GM, the difficulty for determining $\alpha_i(mod\ q)$ is equivalent to the difficulty for computing discrete logarithm over $GF(q)^*$.

The above theorem offers the signer anonymity and untraceability with respect to the verifier but not to the group manager.

In addition, the proposed scheme is more efficient than those in [1,2] in terms of communications because our scheme is noninteractive. In order to open group signatures in case of later dispute, the group manager in our scheme only need store each $(I_i, \alpha_i (mod \quad q))$. The storage costs much less than both of two Tseng-Jan schemes in which the group manager has to reserve each $(I_i, r_i \ (mod \ p), s_i \ (mod \ q), k_i (mod \ q))$. Furthermore, changes of the group in our scheme due to inclusion of new group member or revocation of some group member do not affect other members.

4 Conclusion

In this paper, we have presented a new group signature scheme based on discrete logarithm. The proposed scheme is secure against forgery and provide signer anonymity and untraceability with respect to verifiers but not to the group manager. Moreover, the scheme is efficient in terms of communication and storage cost.

Reference

[1] D. Chaum and E. Van Heyst, Group Signatures, *Proc. Eurocrypt'91*, Brighton, UK, 8-11 April 1991, pp. 257-265.

[2] L. Chen and T. P. Pedersen, New Group Signature Schemes, *Proc. Eurocrypt'94*, Perugia, Italy, 9-12 May 1994, pp. 163-173.

[3] W. Lee and C. Chang, Efficient Group Signature Scheme Based on the Discrete Logarithm, *IEE Proc. Comput. Digital Techniques*, 145 (1) (1998) 15-18

[4] Y. -M. Tseng and J. -K. Jan, Improved Group Signature Based on Discrete Logarithm Problem, *Electron. Lett.*, 35 (1) (1999) 37-38.

[5] H. Sun, Comment: Improved Group Signature Scheme Based on Discrete Logarithm Problem, *Electron. Lett.*, 35 (16) (1999) 1323-1324.

[6] Y. -M. Tseng and J. -K. Jan, Reply: Improved Group Signature Scheme Based on Discrete Logarithm Problem, *Electron. Lett.*, 35 (16) (1999) 1324-1325.

[7] Z. Li, L. C. K. Hui, K. P. Chow, C. F. Chong, W. W. Tsang, H. W. Chan, Security of Tseng-Jan's Group Signature Schemes, *Information Processing Letters*, 75 (2000) 187-189.