ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2013, Vol.42, No.1

A New Group Signature Scheme Based on RSA Assumption

Chou-Chen Yang

National Chung Hsing University, Department of Management Information Systems
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.

Ting-Yi Chan

National Changhua University of Education, Graduate Institute of e-Learning
No.1, Jin-De Road, Changhua City, Taiwan, R.O.C.

Min-Shiang Hwang*

National Asia University, Department of Computer Science & Information Engineering
500, Lioufeng Rd., Wufeng, Taichung, Taiwan 402, R.O.C.
e-mail:mshwang@nchu.edu.tw

crossref http://dx.doi.org/10.5755/j01.itc.42.1.1185

Abstract. In this paper, we present a new group signature scheme based on RSA assumption. It not only achieves the same objective as the Lee-Chang scheme but also reduces the amount of computing time as compared to the Lee-Chang scheme and the Lee-Chang-Hwang scheme.

Keywords: Cryptosystem; Digital signature; Group signature; RSA assumption.

1. Introduction

Digital signature schemes such as RSA [25] and DSA [10] allow a signer to generate a signature on a chosen message by using a secret signing key. Any recipient can be a verifier to verify the signature together with the message by using the signer's public key. Until now, there are many kinds of signatures proposed to achieve different purposes [1–4, 18, 22, 34]. In 1991, Chaum and Heyst [7] proposed a group signature which is allow individual members to make signatures on behalf of the group and has the following properties [5, 6, 14, 15, 19, 32]:

- Only the legitimate members of the group can sign messages.
- The receiver is able to verify if the signature is a valid group signature, but she/he has no ability to find out which member of the group signed the message.
- In case of any dispute, the signature must be 'opened' only by the group authority or all the group members' cooperation.

Four signature schemes were presented in [7]. However, in those schemes, when the group members are changed, all the distributed secret keys will be affected. To make things worse, the signature schemes belong to the interactive system [11, 23, 27, 28].

In 1997, Park, Kim and Won [24] proposed an ID-based group signature. The main advantage of this scheme is that the signer's public key itself is an identification (ID) that does not need to be verified, so there is no need to set up a trust center to verify huge numbers of public keys. Nevertheless, an ID-based group signature must use a set of member identities in the signing phase. When changes occur among the members of the group, the group signature turns invalid. Moreover, the length of the signature increases as the number of members grows.

Lee and Chang [16], and Lee et al. [17] separately proposed an efficient group signature based on the

* Corresponding author

discrete logarithm assumption. They used ElGamal's signature [10, 13] scheme to realize the group signature. The Lee-Chang scheme was more efficient in terms of computation, communication and storage costs, while allowing the group to be changed without having the members choose the new keys. On the other hand, based on RSA assumption, Cui et al. [9] and Chen et al. [8] separately proposed the group signature scheme. They used the advantage that verifying RSA's signature is faster than ElGamal's signature such that their group signature schemes are more efficient. However, each group member's signing private key is distributed by the group authority that means that the group authority has the ability to impersonate the group member to generate the group signature.

In this article, we shall propose an alternative group signature scheme based on the RSA signature. It not only achieves the same objective as the Lee-Chang scheme but also reduces the amount of computing time as compared to the Lee-Chang scheme and the Lee-Chang-Hwang scheme. The remainder of our paper is organized as follows. In Section 2, we shall briefly review the Lee-Chang scheme. In Section 3, we shall propose our new efficient group signature based on RSA. In Section 4, we shall analyse the security of our scheme. In Section 5, we shall discuss the identification phase and compare the performance of our scheme with Lee-Chang scheme and Lee-Chang-Hwang scheme. Finally, a brief conclusion will be given in Section 6.

2. Review of the Lee-Chang Scheme

The Lee-Chang scheme is composed of three phases as follows:

Initiation phase:

Let p and q be two large primes such that $q|p-1$. Let g be a generator ordered q in $GF(p)$. Every group member U_i chooses a secret key x_i and computes the public key $y_i = g^{x_i} \bmod p$. Let T be the group authority (GA) which has the secret key x_T and the public $y_T = g^{x_T} \bmod p$. T chooses a random number k_i, where $\gcd(k_i, q) = 1$, and computes $r_i = g^{-k_i} y_i^{k_i} \bmod p$ and $s_i = k_i r_i x_T \bmod q$ for each group member. Then T sends (r_i, s_i) to group member U_i secretly. After receiving (r_i, s_i), U_i may verify the information by checking the congruence relation $g^{s_i} y_T^{r_i} r_i = \left(g^{s_i} y_T^{r_i}\right)^{x_i} \bmod p$.

Signing and verification phase:

To sign message m, U_i chooses a random number $t \in Z_p^*$. Then U_i computes $r = \alpha^t \bmod p$ and solves the congruence relation $h(m) = rx_i + ts \bmod q$ for the parameter s, where $h(\cdot)$ is a one-way hash function [12]. The group signature is $\{h(m), r, s, (r_i, s_i)\}$. After receiving the information $\{h(m), r, s, (r_i, s_i)\}$, the receiver can verify the group signature through the following steps:

1. Compute $\alpha_i = g^{s_i} y_T^{r_i} \bmod p$.
2. Compute $DH_i = \alpha_i r_i \bmod p$.
3. Check the congruence relation $\alpha_i^{h(m)} = r^s DH_i^r \bmod p$.

If the above relations hold, the group signature is valid.

Identification phase:

In case of a dispute, the group authority has the ability to identify the signature that a group member has signed and announce some information to convince the verifier that U_i is indeed the signer. Because the authority has the knowledge of the secret key x_T, k_i can be solved via the following equation:

$$k_i = s_i + r_i x_T \bmod q.$$

The authority can further obtain y_i from DH_i:

$$DH_i y_i^{k_i} = \bmod p.$$

When the signer has been identified, the authority announces to the verifier who is the real signer. Then the authority must update the pair (r_i, s_i) and send it to U_i. This phase will be further discussed in Section 5.

3. The Proposed Scheme

In this section, we propose a group signature scheme which is based on the RSA signature [25]. RSA signature builds its security upon the difficulty of factoring large numbers. The time complexity of the RSA's signature generation is the same as El-Gamal's signature, but RSA's signature verification can be 10 to 40 times faster than ElGamal's signature [21, 26, 33]. Without loss of generality, our proposed scheme is composed of three phases just like the scheme in [16]. The details are in the following three subsections.

3.1. Initiation Phase

We assume that there are n members in the group. Every group member U_i hooses two distinct large primes p_i and q_i and then U_i computes $n_i = p_i q_i$ and $(\phi(n_i) = (p_i - 1)(q_i - 1)$. Then U_i finds d_i and d_i' to satisfy the following three equations:

$$\begin{cases} e_i d_i = 1 \bmod \phi(n_i), \\ e_i' d_i' = 1 \bmod \phi(n_i), \\ [(e_i + e_i') \oplus a](d_i + d_i') = 1 \bmod \phi(n_i), \end{cases}$$

where a is a random number.

Then U_i sends (e_i, e_i', a) to GA over a secure channel. GA chooses two distinct large primes P and Q and then computes $N = PQ$ and $\phi(N) = (P-1)(Q-1)$. The authority's public are E_1, E_2 and

secret keys are D_1, D_2 such that $E_1 D_1 = 1 \, mod \, \phi(N)$ and $E_2 D_2 = 1 \, mod \, \phi(N)$. GA chooses a hash function H and the output of H should be smaller than N, chooses $d_{U_i} \in Z_N^*$, and compute $d_{SM_i} = D_1 - -D_{U_i} \, mod \, \phi(N)$. Then GA makes two signatures for D_1 and $(e_1 \| e_2 \| \ldots \| e_n)$ as follows:

$$S_{D_1} = (D_1)^{D_2} \, mod \, N$$

and

$$S_{(e_1 \| e_2 \| \ldots \| e_n)} = (e_1 \| e_2 \| \ldots \| e_n)^{D_2} \, mod \, N.$$

Then $\left(D_1, S_{D_1}, (e_1 \| e_2 \| \ldots \| e_n), S_{(e_1 \| e_2 \| \ldots \| e_n)}, d_{U_i}\right)$ is sent to the group member U_i secretly. After receiving $\left(D_1, S_{D_1}, (e_1 \| e_2 \| \ldots \| e_n), S_{(e_1 \| e_2 \| \ldots \| e_n)}, d_{U_i}\right)$, U_i can verify the signatures for D_1 and $(e_1 \| e_2 \| \ldots \| e_n)$ by following the congruence relation:

$$D_1 \stackrel{?}{=} \left(S_{D_1}\right)^{E_2} \, mod \, N$$

and

$$(e_1 \| e_2 \| \ldots \| e_n) \stackrel{?}{=} S_{(e_1 \| e_2 \| \ldots \| e_n)}^{E_2} \, mod \, N.$$

A trusted on-line third party "secure mediator (SM)" is in the proposed scheme. The main function of SM is to help the group member to generate valid group signatures. GA sends d_{SM_i} to SM over a secure channel.

3.2. Signing and Verification Phase

To sign a message M, U_i collaborates with SM to perform the following steps:

1. Compute $S_1 = H(M)^{D_1} mod \, N$.
2. Compute $S_2 = S_1^{d_i + d_i'} mod \, n_i$.
3. Compute $S_3 = S_1^{d_{U_i}} mod \, N$.
4. Compute $E' = [(e_i + e_i') \oplus a] E_1$.
5. Send $S_1, S_2, S_3, M, E', n_i, S_{(e_1 \| e_2 \| \ldots \| e_n)}$ to SM.

After receiving the information $\{S_1, S_2, S_3, M, E', n_i, S_{(e_1 \| e_2 \| \ldots \| e_n)}\}$, SM verifies the mediated group signature by the following steps: (If any of the congruence relations is not met, the signature is invalid.)

1. Use the authority's public key E_2 to compute $S_{(e_1 \| e_2 \| \ldots \| e_n)}^{E_2} \, mod \, N$.
2. Check $e_i \stackrel{?}{\in} (e_1, e_2, \ldots, e_n)$.
3. Compute $S_1 = S_2^{E'/E_1} mod \, n_i$.
4. Verity $H(M) \stackrel{?}{=} S_1^{E_1} mod \, N$.

If the relations hold, then the signature is valid.

The correctness of the verification equation $H(M) \stackrel{?}{=} S_1^{E_1} mod \, N$ can be verified as follows.

$$\begin{aligned} H(M) &= S_1^{E_1} mod \, N \\ &= \left(S_2^{E'/E_1} mod \, n_i\right)^{E_1} mod \, N \\ &= \left(S_2^{(e_i + e_i') \oplus a} mod \, n_i\right)^{E_1} mod \, N \\ &= \left(S_1^{(d_i + d_i') \cdot [(e_i + e_i') \oplus a]} mod \, n_i\right)^{E_1} mod \, N \\ &= S_1^{E_1} mod \, N \\ &= (H(M)^{D_1})^{E_1} \, mod \, N \\ &= H(M). \end{aligned}$$

5. Compute $S_4 = S_1^{d_{SM_i}}$ and send it back to the user.

After receiving S_4, the user computes the group signature σ on the message M as $\sigma = S_3 S_4 \, mod \, N$. The group signature can be verified by any receiver as $H(M) \stackrel{?}{=} \sigma^{E_1^2} mod \, N$. The correctness of the verification equation can be verified as follows:

$$\begin{aligned} H(M) &= \sigma^{E_1^2} mod \, N \\ &= (S_3 S_4)^{E_1^2} mod \, N \\ &= \left(S_1^{d_{U_i} + d_{SM_i}}\right)^{E_1^2} mod \, N \\ &= \left(S_1^{D_1}\right)^{E_1^2} mod \, N \\ &= (H(M)^{D_1^2})^{E_1^2} \, mod \, N \\ &= H(M)^{(D_1 E_1)^2} \, mod \, N \\ &= H(M). \end{aligned}$$

3.3. Identification Phase

In case of any dispute, the group authority has the ability to identify which group member signed the message. Here we demonstrate how the authority identifies the signer. The authority has the knowledge of each U_i, e_i' and a, and can compute which group member satisfies the following two equations:

1. $S_1 = S_2^{(e_i + e_i') \oplus a} mod \, n_i$.
2. $H(M) = S_1^{E_1} mod \, N$.

So, the authority can easily 'open' the signature to discover the identity of the signer.

In this phase, after identifying the signer, the authority announces to the verifier who the real signer is. Then every group member must renew (e_i, e_i', a) and send them to the authority. Here we think the authority need not announce to the verifier who the real signer is. In Section 5, we will explain the reason for this.

4. Security Analysis

Because the authority has no knowledge about any user's secret keys (d_i, d_i'), the authority cannot forge the signature of any user. Even though the users' keys (e_i, e_i', a) are sent to the authority, the authority cannot obtain them. Moreover, our scheme allows new members to join without affecting any distributed secret keys.

According to the description of the group signature in Section 1, if an adversary or illegal user wants to forge a signature in our scheme, it is as hard as

breaking an RSA signature. Please refer to [25] for more details if necessary. Even if the adversary acquires the authority's D_1, he/she still cannot make a valid signature because he/she cannot forge a signature for $(e_1 \| e_2 \| \ldots \| e_n)$. In the signing and verification phase, the verifier will use the authority's public key E_2 to verify the signature $S_{(e_1 \| e_2 \| \ldots \| e_n)}$.

Anyone can find nothing from the group signature σ on the message M about the signer since all the group members generate the same group signature on the same message. There is no information that reveals or points the signer's identity. For example, U_i signs another message M', the group signature for M' is (σ', M'). There are not the same parameters in the two group signatures (σ, M) and (σ', M'). The proposed group signature scheme satisfies the unlinkability.

If the verifier decides to try to 'open' the signature to discover the identity of the signer, he/she will have to face the difficulty of obtaining the value of e_i'. Though the verifier has the knowledge of the value of $(e_i + e_i') \oplus a$, the verifier has no knowledge of e_i and a. So the verifier cannot discover which group member was the signer.

5. Discussion and Performance Analysis

In the Lee-Chang scheme, when the authority announces to the verifier that U_i is indeed the signer, the authority must update his/her signing key (r_i, s_i). If the authority does not update the signing key, the linkage between (r_i, s_i) and y_i, which has been constructed now, will be a threat to the security. Tseng and Jan [30] aimed to improve the aforementioned problem and proposed an improved group signature scheme based on the Lee-Chang scheme. In the same year, Sun showed in [29] that the Tseng-Jan scheme is still not unlinkable. After that, Tseng-Jan [31] proposed to improve their scheme. In 2000, Li et al. [20] demonstrated that the two schemes in [30, 31] by Tseng and Sun both fall for forgery.

In real-world practice, after identifying the signer, the authority should not announce to the verifier who the real signer is.We quote an example in the Chaum-Heyst's paper [7] to explain as follows:

A company has several computers, each connected to the local network. Each department of that company has its own printer (also connected to the network) and only the staff of that department is allowed to use the department's printer. Before printing, the printer must be convinced that the user is working in that department. At the same time, the company wants privacy: the user's name should not be revealed. If, however, someone discovers that a printer has been used too often, the director needs to discover who misused that printer and sends that person a bill.

In this example, when someone misuses the printer, the director can discover who is responsible for it and does not need to announce who misused the printer. The director can then punish that user according to the company's regulations. For this reason, in the Lee-Chang scheme and in our scheme, it is not required to announce to the verifier who the real signer is.

The Lee-Chang scheme [16]and the Lee-Chang-Hwang scheme [17] used ElGamal's cryptosystem to give a better performance than previous schemes. Because the computational complexity of exponent operation is higher than others, we analyze the number of exponent operations of our scheme and compare it with the Lee-Chang scheme in Table 1.

Table 1. Exponent operations of the Lee-Chang scheme and our scheme

	Initiation Phase	Signing and Verification Phase	Identification Phase	Total
Lee-Chang Scheme	9	6	1	16
Lee-Chang-Hwang Scheme	9	13	6	28
Our Scheme	4	7	2	13

From Table 1, it is obvious that our scheme is more efficient than the Lee-Chang scheme and the Lee-Chang-Hwang scheme. Our scheme is total 3 and 12 times of exponent operation less than the Lee-Chang scheme and the Lee-Chang-Hwang scheme respectively. Although the Lee-Chang scheme is 1 time of exponent operation less than our scheme in the identification phase, to identify a signer is not often used. Unless it occurs a dispute, the signature does not be 'open' by the group authority or all the group members' cooperation. On the other hand, to produce a group signature is often to perform the signing and verification phase. We have discussed that both the Lee-Chang scheme and our scheme are not required to announce to the verifier who the real signer is. In the other words, the initiation phase is not often performed. Moreover, the verification of RSA's signature can be 10 to 40 times faster than that of ElGamal's signature.

6. Conclusions

In this article, we have proposed a new scheme based on RSA assumption. We have proved that our group signature is secure against forgery and can achieve signer anonymity and signer identification. We have also considered the application of our group signature scheme in practice and compared the performance of our scheme with the Lee-Chang scheme and the Lee-Chang-Hwang scheme. Our scheme can achieve the same objective as the Lee-Chang scheme and provide another route to the group signature.

Acknowledgment

We would like to thank the referees for many valuable comments and suggestions which have resulted in several improvements of the presentation of the paper. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC100-2221-E-018-025 and NSC100-2622-E-018-004-CC3.

References

[1] **R. Baušys, A. Kriukovas.** A new scheme for image authentication framework. In: *Information Technology and Control*, 2008, Vol. 37, No. 4, pp. 294–300.

[2] **T. Y. Chang.** A convertible multi-authenticated encryption scheme for group communications. In: *Information Sciences*, 2008, Vol. 178, No. 17, pp. 3426-3434.

[3] **T. Y. Chang.** An ID-based group-oriented decryption scheme secure against adaptive chosen-ciphertext attacks. In: *Computer Communications*, 2009, Vol. 32, No. 17, pp. 1829–1836.

[4] **T. Y. Chang, M. S. Hwang, W. P. Yang.** An improved multi-stage secret sharing scheme based on the factorization problem. In: *Information Technology and Control*, 2011, Vol. 40, No. 3, pp. 246-251.

[5] **T. Y.Chang, C. C. Yang, M. S. Hwang.** Threshold untraceablesignature for group communications. In: *IEE Proceedings: Communications*, 2004, Vol. 151, No. 2, pp.179-184.

[6] **T. Y. Chang, W. P. Yang, M. S. Hwang.** A threshold signature scheme for group communications without a shared distribution center. In: *Future Generation Computer Systems*, 2004, Vol. 20, No. 6, pp. 1013-1021.

[7] **D. Chaum, E. Heyst.** Group signatures. In: *Advances in Cryptology, Eurocrypt'91*, Springer, 1991, pp. 257-265. Lecture Notes in Computer Science.

[8] **Y. H. Chen, C. Q. Ye, P. Zhang.** Efficient group signature scheme based on RSA cryptosystem. In: *International Conference on Computing & Informatics.* 2006, pp. 1-3.

[9] **S. Cui, X. Cheng, C. W. Chan.** Practical group signatures from RSA. In: *International Conference on Advanced Information Networking and Applications,* 2006, pp. 1–3.

[10] **T. ElGamal.** A public-key cryptosystem and a signature scheme based on discrete logarithms. In: *IEEE Transactions on Information Theory*, 1985, Vol. IT-31, No. 4, pp. 469–472.

[11] **H. Ge.** An effective method to implement group signature with revocation. In: *International Journal of Network Security*, 2007, Vol. 5, No. 2, pp. 134–139.

[12] **M. S. Hwang.** A remote password authentication scheme based on the digital signature method. In: *International Journal of Computer Mathematics*, 1999, Vol. 70, pp. 657–666.

[13] **M. S. Hwang, C. C. Chang, K. F. Hwang.** An elgamallike cryptosystem for enciphering large messages. In: *IEEE Transactions on Knowledge and Data Engineering*, 2002, Vol. 14, No. 2, pp. 445–446.

[14] **M. H. Ibrahim.** Resisting traitors in linkable democratic group signatures. In: *International Journal of Network Security*, 2009, Vol. 9, No. 1, pp. 51–60.

[15] **A. A. Kamal.** Cryptanalysis of a polynomial-based key management scheme for secure group communication. In: *International Journal of Network Security*, 2013, Vol. 15, No. 1, pp. 68–70.

[16] **W. B. Lee, C. C. Chang.** Efficient group signature scheme based on the discrete logarithm. In: *IEE Proceedings - Computer Digital Technology*, 1998, Vol. 145, No. 1, pp. 15–18.

[17] **C. C. Lee, T. Y. Chang, M. S. Hwang.** A new group signature scheme based on the discrete logarithm. In: *Journal of Information Assurance and Security*, 2010, Vol. 5, No. 1, pp. 54–57.

[18] **C. C. Lee, I. E. Liao, M. S. Hwang.** An extended certificate-based authentication and security protocol for mobile networks. In: *Information Technology and Control*, 2009, Vol. 38, No. 1, pp. 61–66.

[19] **C. C. Lee, P. F. Ho, M. S. Hwang.** A secure E-auction scheme based on group signatures. In: *Information Systems Frontiers*, 2009, Vol. 11, No. 3, pp. 335–343.

[20] **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. In: *Information Processing Letters*, 2000, Vol. 75, No. 5, pp. 187–189.

[21] **C. Y. Liu, C. C. Lee, T. C. Lin.** Cryptanalysis of an efficient deniable authentication protocol based on generalized ElGamal signature scheme. In: *International Journal of Network Security*, 2011, Vol. 12, No. 1, pp. 58–60.

[22] **J. W. Lo, S. C. Lin, M. S.** Hwang. A parallel password-authenticated key exchange protocol for wireless environments. In: *Information Technology and Control*, 2010, Vol. 39, No. 2, pp. 146–151.

[23] **C. Ma, J. Ao.** Certificateless group oriented signature secure against key replacement attack. In: *International Journal of Network Security*, 2011, Vol. 12, No. 1, pp. 1–6.

[24] **S. Park, S. Kim, D. Won.** Id-based group signature. In: *Electronics Letters*, 1997, Vol. 33, No. 19, pp. 1616–1617.

[25] **R. L. Rivest, A. Shamir, L. Adleman.** A method for obtaining digital signatures and public key cryptosystems. In: *Communications of the ACM*, 1978, Vol. 21, No. 2, pp. 120–126.

[26] **B. Schneier.** Applied Cryptography, 2nd Edition. John Wiley & Sons, New York, 1996.

[27] **Z. Shao.** Repairing efficient threshold group signature scheme. In: *International Journal of Network Security*, 2008, Vol. 7, No. 2, pp. 218–222.

[28] **R. Srinivasan, V. Vaidehi, R. Rajaraman, S. Kanagaraj, R. C. Kalimuthu, R. Dharmaraj.** Secure group key management scheme for multicast networks. In: *International Journal of Network Security*, 2010, Vol. 11, No. 1, pp. 33–38.

[29] **H. M. Sun.** Comment improved group signature scheme based on discrete logarithm problem. In: *Electronics Letters*, 1999, Vol. 35, No. 16, pp. 1323-1324.

[30] **Y. M. Tseng, J. K. Jan.** Improved group signature scheme based on discrete logarithm problem. In: *IEE Electronics Letters*, 1999, Vol. 35, No. 1, pp. 37–38.

[31] Y. M. Tseng, J. K. Jan. Reply improved group signature scheme based on discrete logarithm problem. In: *IEE Electronics Letters*, 1999, Vol. 35, p. 1324.

[32] **C. Xu, J. Zhou, Z. Xiao.** General group oriented ID-based cryptosystems with chosen plaintext security. In:

International Journal of Network Security, 2008, Vol. 6, No. 1, pp. 1-5.

[33] **C. C. Yang, T. Y. Chang, J. W. Li, M. S. Hwang.** Simple generalized group-oriented cryptosystems using ElGamal cryptosystem. In: *Informatica*, 2003, Vol. 14, No. 1, pp. 111–120.

[34] E. J. Yoon. An Efficient and secure identity-based strong designated verifier signature scheme. In: *Information Technology and Control*, 2011, Vol. 40, No. 4, pp. 323–329.

Received June 2010.