A Secure Group Signature Scheme

Cheng-Yi Tsai[1], Pi-Fang Ho[2], Min-Shiang Hwang[1,3]
(Corresponding author: Min-Shiang Hwang)
Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung 41354, Taiwan
(Email: mshwang@asia.edu.tw)
Department of Information Management, Chaoyang University of Technology[2]
Department of Medical Research, China Medical University Hospital, China Medical University[3]
No.91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Invited Mar. 12, 2017)

Abstract

Group signature scheme could be applied to the valid members to represent the group. The validity of the signature could be verified by the receiver. On the other hand, the member who signs the message could not be found. However, the group manager could reveal and identify the signer if it is necessary. Concerning with a high performance on security, a new group signature scheme based on a discrete logarithm problem to achieve the characteristics of group signatures is proposed. With this proposed scheme, the signature could be generated rapidly. Also, the verification procedure of the group signature could be spent in a short time. This group signature scheme can protect important messages. Compare with other schemes, the proposed scheme is more secure and efficient than others. The analysis of the security and the performance evaluation of the proposed scheme are provided. The proposed group signature scheme could be suitable for e-commerce applications.

Keywords: Authenticated Encryption; Digital Signature; Group Signature

1 Introduction

A digital signature is used to prove the signed message that no non-valid person could sign [7, 38]. Anyone has the ability to verify the signature is signed or not by the signer. The basic requirements of the digital signature are the non-repudiation and unforgeable. No one can deny that he/she sign the message and forge a valid signature [9, 11, 30]. Furthermore, a group signature is a variation of the digital signature [4, 15, 16, 21, 25, 34, 37] that allows the valid member of the group to sign a message to represent the group. Hence, a group signature scheme has the following characters [2]. First, the valid members of the group could use the signature to sign messages. Second, the group signature could be verified. However, the exact signer could not be found. Finally, the identity of the signer could be revealed if it is necessary.

Based on the discrete logarithm problem, an efficient group signature scheme has been proposed [19]. However, some insecure questions in that scheme were pointed out [32]. Then, two improved group signature schemes were proposed by Tseng and Jan, respectively [32]. However, the proposed schemes did not satisfy the requirement of unlinkability and unforgeability [23,35]. Although there were some schemes proposed [3, 5, 19, 20, 26, 28, 29, 35], there exit insecure concerns. Based on the Diffie-Hellman technique, the contributory group key exchange protocol was proposed [33]. However, the protocol is weak to a man-in-the-middle attack [24]. Without bilinear pairings, an anonymous ID-based group key agreement protocol was proposed [14]. A group key agreement protocol based on braid groups which require only multiplication operations was provided [8].

In this paper, based on the discrete logarithm problem, the group signature scheme is proposed with the secure and efficient concerns. With an authenticated encryption, the signer might generate the signature for a message. The signed message could be recovered by the only specified receiver to verify. The concept of the encryption scheme desires to achieve the authenticity, the confidentiality, the integration, and the property of non-repudiation. Therefore, if the message with a group signature belongs to an important message, it is not expected to let unrelated others learn. By the way, a group signature has to be generated at the first step. Then, it encrypts the group signature and the relative message. In order to achieve this goal, this work proposes a group signature scheme based on authenticated encryption. It is expected to generate the group signature and the ciphertext simultaneously. The validity of the group signature could be verified and the encrypted message could be recovered [6, 13].

Hence, the expected secure group signature scheme has

to meet the characteristics of correction, unforgeability, anonymity, unlinkability, exculpability, traceability and Coalition-resistance [1, 10, 12, 27]. The signature generated by the group member must be accepted by verification process. The only valid members in the group have an ability to sign the messages on behalf of the group. To find the exact signer is difficult within the computing sense. However, it could be revealed by the group manager. Besides, it is hard to tell if the two different signatures have been computed by the same member. The only valid member could use the signature on behalf of the belonged group. The group manager could identify the valid member to use the signature. Moreover, the group member of a colluding subset could not generate a valid signature. With the mentioned above, the secure group signature scheme is developing in this paper.

The following section describes the proposed scheme. The performance and the security analysis of the proposed scheme are shown in Section 3 and Section 4, respectively. Finally, the conclusion is given in Section 5.

2 Discrete Logarithm Problem

Based Scheme Based on discrete logarithm problem [17, 18, 22, 31], the group signature scheme is proposed in this paper. The proposed scheme includes three portions, initial phase, generation and verification, and identification.

2.1 Initiation Phase

Let p and q be two large primes such that $q|p-1$, and let g be a generator with order q in $GF(p)$. Each group member U_i selects a secret key x_i and computes the public key $y_i = g^{x_i} \bmod p$. The group manager T has the secret key x_T and the public key $y_T = g^{x_T} \bmod p$. For each group member U_i, the group manager randomly chooses an integer k_i in Z_q* and computes $r_i = y_i k_i - x_T \bmod q$ and $s_i = y_i k_i \bmod p$. Then, the group manager sends (r_i, s_i) to the group member U_i discreetly. After receiving (r_i, s_i), U_i may verify the validity by checking the equation $s_i y_i = (g^{r_i} y_T)^{x_i} \bmod p$.

2.2 Generation and Verification

A group member U_i signs the message M with the following steps,

1) choose two random numbers R_1, R_2 in Z_q*.

2) Compute A, B, C, and D as follows:

$$\begin{aligned} A &= x_i \cdot R_1 \cdot R_2 \bmod q. && (1)\\ B &= h^{-1}(M||A||D) g^{-R_1 \cdot A \cdot h(M||A||D)} \bmod p. \\ C &= g^{R_1 - r_i \cdot h(B)} \bmod p. \\ D &= s_i^{R_1 \cdot R_2 \cdot y_i} \bmod p. && (2) \end{aligned}$$

where $h()$ and $||$ denote a collision-resistant hash function and a concatenation, respectively.

3) The group signature becomes $\{A, B, C, D, M\}$.

The verification to the group signature is hold with the following the equation,

$$[Bh(M||A||D)]^{-e} \stackrel{?}{=} [C^A (y_T{}^{-A} D)^{h(B)}]^{Ch(M||A||D)} \bmod p. \quad (3)$$

2.3 Identification

The signature has to be revealed to identify the signer if it is needed. The group manager accesses the (y_i, k_i) of each member U_i, it require all (y_i, k_i)s to satisfying the following equation:

$$D == g^{Ak_i y_i} \bmod p, \quad \text{for} \quad i = 1, 2, \cdots, n, \qquad (4)$$

where n is the number of group members. By the way, the group manager could determine who the signer is.

3 Performance Evaluation

The complexity of computing time is usually employed for the performance evaluation of the proposed scheme. In this work, some notations are used for convenience.

1) T_h denotes the time used for executing the one-way hash function $h()$.

2) T_{exp} is the time to execute a modular exponentiation operation.

3) T_{Nmul} is the time for multiplication with modulo N.

In the proposed group signature scheme based on a discrete logarithm problem, the signer requires $3T_{exp} + 8T_{Nmul} + 2T_h$ to generate a group signature. The verifier requires $5T_{exp} + 4T_{Nmul} + 2T_h$ to verify the group signature. Compared with our scheme and other schemes, the proposed scheme is better than that of the others schemes in performance.

4 Security Analysis

Based on the difficulty of the discrete logarithm problem, the security analysis to the proposed scheme is provided. The proposed scheme should meet all the security properties requests.

Correctness.

The receiver could verify the group signature $\{A, B, C, D, M\}$ by Equation (3).

Unforgeability and Exculpability.

A valid group signature could be generated by the valid membership (r_i, s_i) and the corresponding secret key x_i. In the case, the eavesdropper intercepts a valid member-ship (r_i, s_i) and intends to forge a group signature. According to the proposed scheme, he has to compute the parameters A, B, C and D

from Equation (1) to Equation (2). Without the secret key x_i, the eavesdropper could not forge a group signature. Either, Equation (3) could not be hold.

Anonymity.

Since the group signature scheme is designed for the group manager to identify the exact signer, all confidential information is protected by random parameters. Within a valid group signature $\{A, B, C, D, M\}$, A and D relates the identity information. Hence, the anonymity of A and D should be examined. With a valid group signature, Equation (1): $A = x_i \cdot R_1 \cdot R_2 \bmod q$,

$$g^A = g^{x_i \cdot R_1 \cdot R_2} = y_i^{R_1 \cdot R_2} \bmod p, \tag{5}$$

where R_1 and R_2 are integers. If R_1 and R_2 are known, y_i could be found, i.e. the exact signer could be identified. However, since the number R_1 and R_2 are unknown, no one could find the exact signer, i.e. the proposed scheme has anonymity.

Unlinkability.

Similarly to anonymity, to identify whether the signatures $\{A, B, C, D, M\}$ and the signature $\{A', B', C', D', M'\}$ are generated by the same group member is difficult. With Equations (3) and (4), the modified equations is given as the following,

$$g^A / g^{A'} = g^{x_i \cdot R_1 \cdot R_2} / g^{x_i \cdot R_1' \cdot R_2'} \bmod p \tag{6}$$

and

$$\begin{aligned} D/D' &= s_i^{y_i \cdot R_1 \cdot R_2} / s_i^{y_i \cdot R_1' \cdot R_2'} \\ &= \left(g^{x_i \cdot R_1 \cdot R_2} / g^{x_i \cdot R_1' \cdot R_2'}\right)^{k_i \cdot y_i} \bmod p. \end{aligned} \tag{7}$$

If one desired to check whether the two signatures are generated by the same signer, the equation

$$\left(g^A / g^{A'}\right)^{k_i \cdot y_i} = D/D' \bmod p, \tag{8}$$

should be hold. However, k_i and y_i are unknown. No one could determine whether the two group signatures are generated by the same signature.

Traceability.

The group manager could access the (y_i, k_i) for each member U_i. Hence, the group manager can request the (y_i, k_i) of U_i to meet the requirement in Equation (4). For the traceability, the group manager can determine the exact signer.

Coalition-resistance.

The group manager generates the (r_i, s_i) with the secret key x_T for each group member. Then, the group manager sends (r_i, s_i) to the group member j. If the colluding subset of the group members desires to generate a valid group signature, they have to keep the secret key x_T. However, the colluding subset of group members does not keep the secret key. The valid (r_i, s_i) could not be forged. Hence, a valid group signature could not be generated. The group manager could not link to any member in the colluding group.

Based on the above security analysis of the proposed scheme, it is shown the proposed scheme could approach all security property requirements.

5 Conclusions

Group signature scheme functions to protect the important messages. In this paper, a new group signature scheme based on discrete logarithm problem has been proposed. The performance and security analysis are given to show the proposed scheme has a superior capacity. With the proposed scheme, the signers could generate a group signature swiftly, and the verification could be quickly complemented. For the applications with the time efficiency concern, the proposed scheme could be employed in the e-commerce.

Acknowledgment

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: MOST 104-2221-E-468-004 and MOST 105-2410-H-468-009.

References

[1] B. E. Ayebie, H. Assidi, El M. Souidi, "A new dynamic code-based group signature scheme," *Lecture Notes in Computer Science*, vol. 10194, pp. 346-364, Springer-Verlag, 2017.

[2] N. Begum, T. Nakanishi, S. Sadiah, Md. E. Islam, "Implementation of a revocable group signature scheme with compact revocation list using accumulator," in *4th International Sym-posium on Computing and Networking (CANDAR'16)*, pp. 610-615, 2017.

[3] L. Boongasame, P. Temdee, F. Daneshgar, "A group signature based buyer coalition scheme with trustable third party," *International Journal of Production Research*, vol. 55, no. 17, pp. 5050-5061, 2017.

[4] D. Chaum and E. Heyst, "Group signatures," in *Advances in Cryptology (Eurocrypt'91)*, pp. 257-265, 1991.

[5] E. M. Cho, T. Koshiba, "Secure deduplication in a multiple group signature setting," *Proceedings of International Conference on Advanced Information Networking and Applications (AINA'17)*, pp. 811-818, 2017.

[6] H. Ge, "An effective method to implement group signature with revocation," *International Journal of Network Security*, vol. 5, no. 2, pp. 134-139, 2007.

[7] M. Hassouna, E. Bashier, and B. Barry, "A strongly secure certificateless digital signature scheme in the

random oracle model," *International Journal of Network Security*, vol. 18, no. 5, pp. 938-945, 2016.

[8] P. Hiranvanichakorn, "Provably authenticated group key agreement based on braid groups - The dynamic case," *International Journal of Network Security*, vol. 19, no. 4, pp. 517-527, 2017.

[9] M. S. Hwang and C. C. Lee, "Research issues and challenges for multiple digital signatures," *International Journal of Network Security*, vol. 1, no. 1, pp. 1-7, 2005.

[10] M. H. Ibrahim, "Resisting traitors in linkable democratic group signatures," *International Journal of Network Security*, vol. 9, no. 1, pp. 51-60, 2009.

[11] A. U. Khan and B. K. Ratha, "A secure strong designated verifier signature scheme," *International Journal of Network Security*, vol. 19, no. 4, pp. 599-604, 2017.

[12] S. Khomejani and A. Movaghar, "Privacy consideration for trustworthy vehicular ad hoc networks," in *2010 International Conference On Electronics and Information Engineering*, pp. 437-442, 2010.

[13] K. Kim, I. Yie, S. Lim, and D. Nyang, "Batch verification and finding invalid signatures in a group signature scheme," *International Journal of Network Security*, vol. 13, no. 2, pp. 61-70, 2011.

[14] A. Kumar and S. Tripathi, "Anonymous ID-based group key agreement protocol without pairing," *International Journal of Network Security*, vol. 18, no. 2, pp. 263-273, 2016.

[15] C. C. Lee, T. Y. Chang, M. S. Hwang, "A new group signature scheme based on the discrete logarithm," *Journal of Information Assurance and Security*, vol. 5, no. 1, pp. 54-57, 2010.

[16] C. C. Lee, P. F. Ho, M. S. Hwang, "A secure E-auction scheme based on group signatures," *Information Systems Frontiers*, vol. 11, no. 3, pp. 335-343, July 2009

[17] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms", *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343-349, July 2003.

[18] C. C. Lee, M. S. Hwang, and W. P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability", *Applied Mathematics and Computation*, vol. 164, no. 3, pp. 837-841, May 2005.

[19] W. B. Lee and C. C. Chang, "Efficient group signature scheme based on the discrete logarithm," *IEE Proceedings - Computer Digital Technology*, vol. 145, no. 1, pp. 15-18, 1998.

[20] L. H. Li, C. Y. Liu, and M. S. Hwang, "Cryptanalysis of an efficient secure group signature scheme," *ACM Operating Systems Review*, vol. 38, no. 4, pp. 67-69, 2004.

[21] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms," *Computers & Security*, vol. 22, no. 3, pp. 245-255, 2003.

[22] L. H. Li, S. F. Tzeng, M. S. Hwang, "Improvement of signature scheme based on factoring and discrete logarithms", *Applied Mathematics and Computation*, vol. 161, no. 1, pp. 49-54, Feb. 2005.

[23] Z. Li, L. C. K. Hui, K. P. Chow, C. F. Chong, W. W. Tsang, and H. W. Chan, "Security of Tseng-Jan's group signature schemes," *Information Processing Letters*, vol. 75, no. 5, pp. 187-189, 2000.

[24] C. H. Ling, S. M. Chen, and M. S. Hwang, "Cryptanalysis of Tseng-Wu group key exchange protocol," *International Journal of Network Security*, vol. 18, no. 3, pp. 590-593, 2016.

[25] E. J. L. Lu, M. S. Hwang, and C. J. Huang, "A new proxy signature scheme with revocation," *Applied Mathematics and Computation*, vol. 161, no. 3, PP. 799-806, Feb. 2005.

[26] K. M. Nomura,S. Masami, M. M. Yoshiaki, "A multigroup signature scheme for local broadcasting," *14th IEEE Annual Consumer Communications and Networking Conference (CCNC'17)*, pp. 449-454, 2017.

[27] F. M. Salem, M. H. Ibrahim, and I. I. Ibrahim, "Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks," in *Sixth International Con-ference on Networking and Services*, pp. 156-161, 2010.

[28] Z. Shao, "Repairing efficient threshold group signature scheme," *International Journal of Network Security*, vol. 7, no. 2, pp. 218-222, 2008.

[29] R. H. Shi, "An efficient secure group signature scheme," in *Proceedings of IEEE (TENCON'02)*, pp. 109-112, 2002.

[30] N. Tiwari and S. Padhye, "Provable secure multi-proxy signature scheme without bilinear maps," *International Journal of Network Security*, vol. 17, no. 6, pp. 736-742, 2015.

[31] C. Y. Tsai, C. Y. Liu, S. C. Tsaur, and M. S. Hwang, "A publicly verifiable authenticated encryption scheme based on factoring and discrete logarithms", *International Journal of Network Security*, vol. 19, no. 3, pp. 443-448, May 2017.

[32] Y. M. Tseng and J. K. Jan, "Improved group signature scheme based on discrete logarithm problem," *IEE Electronics Letters*, vol. 35, no. 1, pp. 37-38, 1999.

[33] Y. M. Tseng and T. Y Wu, "Analysis and improvement on a contributory group key exchange protocol based on the Diffie-Hellman technique," *Informatica*, vol. 21, no. 2, pp. 247-258, 2010.

[34] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61-71, Mar. 2004.

[35] G. Wang, "Security analysis of several group signature schemes," *Lecture Notes in Computer Science*, vol. 2904, pp. 252-265, Springer, 2003.

[36] Y. Wang J. Zhang, X. Chen, "Security analysis of the improved group signature," in *Information Theory Workshop*, pp. 171-174, 2003.

[37] C. C. Yang, T. Y. Chang, M. S. Hwang, "A new group signature scheme based on RSA assumption," *Information Technology and Control*, vol. 42, no. 1, pp. 61-66, 2013.
[38] X. Zhang, R. Lu, H. Zhang, and C. Xu, "A new digital signature scheme from layered cellular automata," *International Journal of Network Security*, vol. 18, no. 3, pp. 544-552, 2016.

Biography

Cheng-Yi Tsai received his B.S. degree from Department of Business Administration, Chaoyang University of Technology (CYUT), Taiwan in 2001 and M.S. degree from Computer Science & Information Engineering, Asia University, Taiwan in 2005 . He is currently pursuing the Ph.D. degree from Department of Computer Science and Information Engineering, Asia University, Taiwan. His research interests include blockchain, information security, and cloud computing.

Pi-Fang Ho received the B.S. in Applied Mathematics, Providence University, Taiwan, in 2003; the M.S. in Information Management, Chaoyang University of Technology, Taiwan, in 2005. Her current research interests include communication and information security.

Min-Shiang Hwang received Ph.D. degree in computer and information science from the National Chiao Tung University, Taiwan in 1995. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories, Ministry of Transportation and Communications. He was also the Chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor with University of California (UC), Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of the Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include information security, electronic commerce, database and data security, cryptography, steganography, and mobile computing. Dr. Hwang has published over 200+ articles on the above research fields in international journals.