International Journal of Science and Engineering Applications
Volume 3 Issue 6, 2014, ISSN-2319-7560 (Online)

A New Group Signature Scheme with Efficient Membership Revocation

Thu Thu Mon Oo
University of Technology
(Yatanarpon Cyber City)
Pyin Oo Lwin, Myanmar

Abstract: In group signature schemes, the members of the group are allowed to sign messages anonymously on the behalf of the group. In this case, other group members and the outsiders from the group cannot see which member signed the messages. The organizational structure which should support the safety of privacy may need to provide a degree of anonymity to the individuals conducting the transactions. Moreover, the current methods of revocation property of the group signature scheme do not revoke to allow valid signature under an old secret key of the group manager. And it is remaining as a challenge to be independent on the size of the group public key when the group size is increasing. For this above facts, this paper will be proposed to achieve anonymous revocation based on the concept of group signature more effectively.

Keywords: Cryptograph, Digital Signature, Group Digital Signature, Anonymity, Revocation

1. INTRODUCTION

With the rapid improvement of technology, digital signatures have become as an important role in the aspects of information security, identity authentication, data integrity, anonymity, message authentication, and so on.

Group signatures are one kind of digital signatures with special efforts. This signature can allow any group members to sign message on behalf of the group while remaining anonymity. When the case of disputes will be occurred, the group manager opens the signatures to revoke anonymity of group members. Group signatures can be applied with most of the activities of electronic polities and electronic commerce such as e-voting, e-bidding, e-cash, e-banking and so forth. It is more suitable for some application in which desirable to hide organizational structure.

Most group signatures can usually be used to conceal the internal structures of the group. The security and efficiency of most group signature schemes proposed previously, are not very ideal. In some previous group signature schemes, they cannot protect adversaries from colluding attacking or universally forging. As a result, they cannot serve the whole advantage of groups. And then most of group signature schemes cannot delete group members effectively so that they cannot meet the needs of dynamic groups in reality.

The group signatures are a "generalization" of the credential/ membership authentication schemes, in which one person proves that he belongs to a certain group. It has the following properties:

- only members of the group can sign messages
- the receiver can verify that it is a valid group signature, but cannot discover which group member made
- if necessary, the signature can be opened, so that the person who signed the message is revealed

Some schemes were described to split the functions of the group manager as two manages. The authorities and tasks of the group manager are divided into two parts in this proposed scheme. This desirable fact allows the distribution of the trust. In the proposed signature scheme, the membership certificate is in fact the zero-knowledge for others except one of the group managers who can add new members. To design a group signature scheme profitably, it is still an open problem to be secure and efficient.

In this proposed scheme, the group digital signature with distributed authorities can be used to decrease the managing workloads of the managers in the group. The members can be added or removed from the group as a result of join and revoke algorithms. The proposed scheme may be supported the properties of anonymity and revocation particularly. While generating the group signature, the requested message from one of group members can only be signed with the private key of issuing manager. Furthermore, no knowledge of the information about the members in this signature can be given. In the case of cheating, this member who cheated must be revoked by the opening manager anonymously, and was made to be unable to sign in the future. With improving awareness about security of the group, how to protect the source of the signature and confirm the integrity of the transmitted message from the view of Outsider is an important issue.

The rest of this paper is organized as follows. In Section 2, the related work of group signature schemes will be described. Section 3 describes the proposed group signature scheme. Section 4 introduces the procedures of the proposed signature scheme. And preliminaries for analysis of the proposed scheme will be expressed in Section 5. In Section 6, the security analysis of the proposed scheme will be expressed. Finally, the paper concludes in Section 7.

2. RELATED WORK

To conceal organizational structures group signature can be used. For example, an employee of a company can use group signature to sign document on behalf of the company. In this situation, it is sufficient for a verifier to know that some behalf of the company has signed. Verifier does not need to check whether the employee is allowed to sign document on behalf of the company.

Killan and Petrank [3] also indicate the concept of separability. That is, if the group manager is split into a membership manager and a revocation manager, the revocation manager and the membership manager work in

concert to open the identity of the signer. But they did not propose any group signature scheme to achieve this function.

Bellare, Shi and Zhang [4] strengthened the security model to include dynamic enrollment of members. This security model also separated the group manager's role into two parts: issuer and opener. The issuer is responsible for enrolling members, but cannot trace who has signed a group signature. The opener on the other hand cannot enroll members, but can open a group signature to see who signed it. More-over, it was required that this opener should be able to prove that said member made the group signature to avoid false accusations of members. [5] demonstrated that trapdoor permutations suffice also for constructing group signatures in this model. Both of these schemes use general and complicated primitives and are very inefficient.

Jan Camenisch presented an efficient group signature scheme in [6]. Providing computational anonymity, ability to add (or remove) group members after the initial setup, and the possibility of being generalized by allowing authorized set of group members to sign collectively on behalf of the group. This scheme can be extended to allow the functionality of the group manager to be shared among several entities. The drawbacks include the size of the public key and the signature size both which are proportional to group size.

In [7], most previous results are shown the following disadvantages: the size of the group public and the length of the group signature depend on the size of the group. And then new member addition requires restarting the entire system or involves re-issuing all members' keys and changing the group public key. Furthermore, revocation of group members also requires that.

3. PROPOSED GROUP SIGNATURE SCHEME

The entities of the group involved in this proposed scheme are:

- The central manager (CM) will establish the group with the whole authority and is served as the trusted party. It can be performed as the owner of the group. CM controls the group responsibilities that are divided into two authorities: the issuing manager (IM) and the opening manager (OM), and then CM creates all of the group keys.
- The issuing manager (IM) will produce the signature on the behalf of the group. IM has read –only access to the group storage for the authentication of the member to sign the message. Although IM can only be signed the message to create group signature with his private key as the group private key, IM cannot know the content of the message that is to send to outsider.
- The opening manager (OM) can add new members of the group, and has both read and write accesses to the group storage. OM can also generate the membership certificates to group members for joining and revoking processes.
- Members of the group, who have already joined the group and accepted the membership certificates, will send the message for producing the signature to IM. The group members create the hash value of the original message that sends to the outsider for the authentication of the message.
- The outsiders do not belong to the group but have the access to the public key of group to verify the group signature.

In this proposed scheme, the results that can be obtained are the efficiency of revoking the members and signing the group signature for some special tasks of anonymity and revocation. Because the group members cannot sign themselves on the behalf of the group, this proposed scheme will be given the advantage that the cheated member cannot use the abilities of signing the message in this group. The collaboration of the group member and OM can generate the valid group signature in the proposed scheme. As a result, it can be implemented with better improvements in the signing procedure.

In the event of dispute, OM extracts the identity of the member from the membership certificate in the signature, and revokes this member from the group. Although OM do not reveal the identity of this member to the outsider, he sends the notified message that is not a valid signature at the current time and suggest to discard the corresponding message of this signature. But this notified message has no knowledge of the information about the originator of signature for protecting the privacy of the group member. In the case of cheating, this member who cheated must be revoked by the opening manager anonymously, and was made to be unable to sign in the future. With improving awareness about security of the group, how to protect the source of the signature and confirm the integrity of the transmitted message from the view of Outsider is an important issue.

4. PROCEDURES OF PROPOSED SCHEME

In the proposed group signature scheme, it will be provided the secrecy of the group identities of new members effectively by encrypting their own NRC numbers that can be known themselves only. The procedures of the proposed group signature scheme are:

1. Setup
2. Join
3. Sign
4. Verify
5. Open
6. Revoke

The above six steps of the proposed scheme are described briefly as follow:

In setup algorithm, CM runs to generate the key pair of the group, and the secret key for membership certificates. The private key of the group is assigned as the secret key of IM and the remaining one from the key pair is also assigned as the group public key. The secret key to produce the membership certificate is used as the own key of OM.

Join algorithm is required to check the existence of the member whether already joined the group or not. If the new one is not a member, OM will add all of the data of this one to the group storage. Then OM sends the membership certificate and member identity (M_ID) to this new member, and updates the group storage. OM encrypts the required data of the member with his private key as the group certificates, and like this way, OM encrypts the group ID with the NRC number of new member. And the members can obtain the group ID by decrypting with their corresponding NRC number. Members do not know anything about their certificates.

The member computes the member identity with his NRC number to get his group ID. Before the member does not accept the group signature, the member who wants to sign the message produces the hash value of the message to send to the outsiders. After hashing the message, the member sends member ID, hash value of message and his membership certificate to IM. When IM receives the request to sign, IM checks member ID that is compared as the same one in the group storage. If it is already existed, IM will produce the signature with his secret key by encrypting both the membership certificate and hash value, and send this signature to the group member who sent the request to produce the signature. The member sends the original message, the hash value of this message and the signature by concatenating to the outsider.

According to the verify algorithm, the verifier or outsider can verify the signature with the group public key. After verifying the signature, he extracts the hash value of the original message from the signature, and compares both of the hash value what he extracts. If they are all the same, the outsider will accept as the valid signature and the authentication of the message. Unfortunately if they cannot verify that, they will send the signature to OM to verify.

In the case of cheats or disputes, the open algorithm will be ran by OM and returned the identity of the member who signs the corresponding message. In this event, OM will reply to the outsider what the message is the valid signature or not.

After OM got the member ID from the membership certificate of this member, OM deletes the record of the identity of member from member list and adds this record of deleted member to Blacklist of member.

5. PRELIMINARIES

Some cryptographic assumptions are reviewed that are intended to satisfy some security properties of proposed group signature scheme.

5.1 Discrete Logarithm Problem

Discrete logarithms are logarithms defined with regard to multiplicative cyclic groups. If G is a multiplicative cyclic group and g is a generator of G, then from the definition of cyclic groups, it is known that every element h in G can be written as g^x for some x. The discrete logarithm to the base g of h in the group G is defined to be x. For example, if the group is Z_5^*, and the generator is 2, then the discrete logarithm of 1 is 4 because $2^4 \equiv 1 \bmod 5$.

The discrete logarithm problem is defined as: given a group G, a generator g of the group and an element h of G, to find the discrete logarithm to the base g of h in the group G. Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups. For example, a popular choice of groups for discrete logarithm based crypto-systems is Z_p^* where p is a prime number.

5.2 Computational Diffie-Hellman Assumption

The computational Diffie–Hellman (CDH assumption) is the assumption that a certain computational problem within a cyclic group is hard.

Consider a cyclic group G of order q. The CDH assumption states that, given (g, g^a, g^b). For a randomly chosen generator g and random $a,b \in \{0,\dots, q-1\}$, it is computationally intractable to compute the value g^{ab}.

5.3 Decisional Diffie-Hellman Assumption

The decisional Diffie–Hellman (DDH) assumption is a computational hardness assumption about a certain problem involving discrete logarithms in cyclic groups. It is used as the basis to prove the security of many cryptographic protocols.

Consider a (multiplicative) cyclic group G of order q, and with generator g. The DDH assumption states that, given g^a and g^b for uniformly and independently chosen $a,b \in Z_q$, the value g^{ab} "looks like" a random element in G.

This intuitive notion is formally stated by saying that the following two probability distributions are computationally indistinguishable:

- (g^a, g^b, g^{ab}), where a and b are randomly and independently chosen from Z_q.
- (g^a, g^b, g^c), where a, b and c are randomly and independently chosen from Z_q.

6. SECURITY ANALYSIS OF PROPOSED SCHEME

An overview of the proposed group signature scheme will be defined as follow. This proposed scheme is based on the above mentioned assumptions. The symbol || denotes the concatenation of two binary strings.

6.1 Setup

The setup procedure is as follow. The Central Manager of the group must perform the following steps:

1. Chooses random primes p, q and then the central manager computes an RSA modulus $n=pq$.
2. Chooses a public exponent e randomly such that e is relatively prime, and compute $d=e^{-1} \bmod (p-1)(q-1)$.
3. Selects an element g of Z_n^* of order n. Let G be a cyclic subgroup of Z_n^*.
4. Chooses a secret key $X \in G$ randomly.
5. Finally, a collision-resistant hash function H: $\{0,1\}^* \rightarrow \{0,1\}^k$.

The public key of the group is $P= (n, e, g)$ and the secret key of the Issuing Manager is $S = (n, d)$.

6.2 Join

In the proposed scheme, if a user wants to join the group, the scheme is assumed that the communication between the group member and the group manager as the Opening Manager is secure. To obtain the membership certificate of the group, each user must perform the following steps with the Opening Manager.

1. The user U_i selects an element x_i as his own identity (ID), and sends x_i and his data D_i.
2. The Opening Manager checks x_i from the group storage. If it is not in the group database, he selects random

number (id_i) for group ID, and computes the membership ID (ID_i) and the group certificate C_i.

- $ID_i = x_i.id_i$
- $C_i = X.(D_i \,||\, id_i)$.

3. The Opening Manager sends ID_i and C_i to user U_i. After the user U_i gets the pair (ID_i, C_i), he can be as a member of the group.
4. The user U_i computes $id_i' = x_i^{-1}.\ ID_i = x_i^{-1}.\ x_i.id_i$. The pair ($id_i$, C_i) is the membership certificate of the new member.

Consequently, at the end of the steps, the Opening Manager creates a new entry in the group database and stores id_i and D_i in the new entry. And group certificates cannot be identified by anyone except the Opening Manager because this group certificates can be issued with the secret key that is known only by the Opening Manager. As a result, the proposed group signature scheme can be satisfied with anonymity property.

6.3 Sign

A group member U_i with a membership certificate (id_i, C_i), can generate group signatures with the Issuing Manager on a message m as follows:

1. The member U_i computes $H(m)$, the hashed value of the message, and he sends $(id_i \,||\, C_i \,||\, H(m))$ to the Issuing Manager to issue the group signature.
2. The Issuing Manager gets id_i and compares whether this member is valid or not from the group database.
3. If this member is valid, the Issuing Manager computes the signature σ and sends the signature to the member.

- $\sigma = (C_i \,||\, H(m))^d \bmod n$.

4. The member U_i sends the group signature with the message $(\sigma \,||\, m \,||\, H'(m))$ to Outsider.

The Issuing Manager can issue the signature σ if the member who has the validity of the existence in the group is true by checking his group ID. Therefore the proposed signature can be identified that has the property of unforgeability.

6.4 Verify

The resulting signature $(\sigma \,||\, m \,||\, H'(m))$ of a message m can be verified by the Outsider as follows:

1. Computes $\sigma^e \bmod n = (((C_i \,||\, H(m))^d)^e \bmod n = C_i \,||\, H(m)$.
2. Accept the group signature $(\sigma \,||\, m \,||\, H'(m))$ if and only if $H'(m) = H(m)$.

As a result, if the Outsider accepts what the group signature is valid after Verify algorithm, the proposed group signature is satisfied with the property of correctness.

6.5 Open

Unless the Outsider can verify the group signature, he resends the signature σ to the Opening Manager to check whether the originator of the signature is valid or not. In the case of dispute, the Opening Manager can find out which one of the group members issued this signature and perform the following steps:

1. Computes $\sigma^e \bmod n = (((C_i \,||\, H(m))^d)^e \bmod n = C_i \,||\, H(m)$.
2. Computes $X^{-1}.C_i = X^{-1}.(X.(D_i \,||\, id_i)) = (D_i \,||\, id_i)$.

6.6 Efficiency

The proposed scheme is attempted in that a member performs a constant amount of work in generating signature. As every file that needs to be signed is of fixed length, the group signatures of the proposed scheme satisfy the security property of unlinkability.

In each Sign operation, this proposed scheme can also be implemented by using the hash function H: $\{0,1\}^* \rightarrow \{0,1\}^k$ where k = 128 bits. Consequently, the signature of the message can be improved with the small size, and then the authentication of message can be obtained from this signature.

With a 1024 bit modulus, a proposed signature is about 1 Kbytes long. To be efficient with the time complexity, the proposed scheme can be supported as follows:

- In Sign operation, a group signature is required $2T_h + 1T_{exp} + 1T_N$ to generate, and
- The Outsider requires $2T_{exp} + 1T_N$ to verify the group signature.

In the above mentioned facts, some notations are used to analyze the computational complexity. These are:

- T_h is the time for executing the hash function $H(.)$.
- T_{exp} is the amount of time to execute a modular exponentiation operation.
- T_N is the time for multiplication with modulo n.

7. CONCLUSION

The signature scheme can be proposed an innovative application of group signature scheme for some organizations that wish to hide their internal organizational structures. This work proposes new prospects for the group signature scheme. In the proposed scheme, a group signature can be particularly generated with the collaboration of the group member and the issuing manager. As the procedures of this scheme, the storage space of group database can be saved because the proposed scheme does not need to store the lists of public keys of each member. Because of the control of issuing the signature from the authority of the issuing manager, the revoked members are not allowed to sign on behalf of group in future. In addition, every proposed signature can also give the authentication of the corresponding message by using hashing algorithm. The proposed scheme is attempted with better efficiency, and consequently, this signature scheme can be resulted to reduce the time complexity more than other previous scheme in Sign and Verify algorithm. As the future work, the group signature scheme will be implemented with stronger assumptions to be efficient for larger groups that are needed the dynamic revocation immediately. In addition, the group signature should be improved to apply among multi-groups efficiently.

8. REFERENCES

[1] M. S. H. Khiyal, A. Khan, S. Bashir, F. H. Khan and S. Aman. "Dynamic Blind Group Digital Signature Scheme in E-Banking", International Journal of Computer and Electrical Engineering, vol.3, No.4, pp. 514-519, 2011.

[2] X. Cheng, C. Yang and J. Yu. "A new approach to group signature schemes", Journal of Compters, vol.6, No.4, pp. 812-817, 2011.

[3] Petrank, E. and Kilian, J.: *Identity Escrow*, in Advances in Cryptology Crypto, (1998).

[4] Bellare, M., Shi, H. and Zhang, C.: "Foundations of Group Signatures: The Case of Dynamic Groups", In proceedings of CT-RSA '05, LNCS series, 3376, (2005) 136-153.

[5] Tsudik, G. and Ateniese, G.: "Quasi-efficient Revocation for Group Signatures", in To Appear in Financial Cryptography 2002, (2002).

[6] Camenisch, J.: *Efficient and Generalized Group Signatures*. In Proc. EURO-CRYPT 97, Springer-Verlag, Lecture Notes in Computer Science No. 1233, (1997) 465-479.

[7] J. Camenisch and M. Stadler. "Efficient group signature scheme for large groups", in Advances in Cryptology, Crypto '97, Lecture Notes in Computer Science, pp. 410-424, 1997.