A Novel Group Signature Scheme based upon DLP

Sujata Mohanty, Banshidhar Majhi
Department of Computer Science and Engineering,
National Institute of Technology
Rourkela, Orissa, India
{sujata.nitr@gmail.com, bmajhi@nitrkl.ac.in}

ABSTRACT: *This paper presents a novel group signature scheme based on the discrete logarithm problem. In this scheme the length of the signature is independent of the number of members of the group and it supports message recovery feature. In case, some members left the group or joins the group, the group signature remains valid. All valid signatures are traceable by only the group manager. Every member of the group has a pair of secret keys: one is generated by the member himself and the other is provided by the group manager. Neither the group manager nor any group members can produce a valid signature on behalf of a member. The proposed scheme provides signer's anonymity, i.e., the verifier can verify the group signature by knowing only the group's public information. This scheme has wide applications in real life scenarios, such as, e-cash, e-auction, press releases and secures electronic transactions.*

Keywords: Group Signature, Anonymity, Discrete Logarithm Problem, Unlinkability

Received: 10 September 2011, Revised 18 November 2011, Accepted 24 November 2011

1. Introduction

The concept of group signature was first introduced by [1] that allows any member of a group to sign messages on behalf of a group. As compared to conventional signature schemes it provides anonymity to the signer, i.e., the receiver can verify that it is a valid group signature, but can not identify which member of the group has made it. No one, including the group manager can produce a valid group signature on behalf of any member. However, in some exceptional cases, such as a legal dispute, any group signature can be opened by the group manager to reveal the identity of the signature's originator.

Anonymity and unlinkability are two important properties of group signature. Because of the anonymity and unlinkability of group signature, the internal structure of a group remains hidden for a verifier, while only the group manager can reveal the signer's identity. The security features of group signature schemes make them attractive for many practical applications, such as e-voting, e-bidding and e-cash, where the privacy and anonymity of signers or the organization is of utmost important. Group signatures can be used to conceal organizational structures, e.g., when a company or a government agency issues a signed statement. They can also be integrated into an electronic cash system in which several banks can securely distribute anonymous and untraceable e-cash. The group property presents then the further advantage to also conceal the identity of the issuing bank [4].

After Chaum's proposal, a number of improvements and enhancements followed in the area of group signature. Chen and Pedersen proposed a group signature scheme that allows the addition of new members after the setup of the system. However, this scheme has a major drawback that the group manager can falsely accuse a group member of having signed a message. This problem was solved when Camenisch and Stadler proposed the first efficient group signature scheme, where the size of the group’s public key and the length of signatures and computational complexity of signing as well as verifying are independent of the number of group members. Also, the public key remains same irrespective of addition of new members to the group. Kim et al.’s proposed a group signature scheme in which, the secret key of each member is a pair of integers, one chosen by the user and the other computed by the group center. The main contribution of their scheme is that signer’s public key is an identification (ID) that does not need to be verified, so there is no need to set up a trusted center to verify a huge number of public keys. Nevertheless, an ID-based group signature must use a set of group member identities in the signing phase. When the group changes, the signature becomes invalid. This scheme is also not secure enough to resist inside attacks. In [9] proposed an efficient group signature based on the discrete logarithm. The scheme was more efficient in terms of computational, communication and storage costs, while allowing the group to be changed without having the members choosing the new keys. However, when the signer has been identified, the authority must redistribute the keys of this signer and send the keys to him/her.

Later, some group signature protocols are proposed in which the length of a signature and/or the computational effort for signing and verifying depends on the number of the group members. That is, if some group members left the group, the signature becomes invalid [5]. Full anonymity and full traceability features are introduced to group signature scheme by [6]. The concept of strong unforgeability in pairing based group signature scheme is introduced by [7]. At present, there are two most popular public-key algorithms which can provide digital signatures: One is the RSA type signature scheme [11], the security of which is based on factoring; the other is the ElGamal-type signature scheme [10], the security of which is based on the discrete logarithm problem over the finite field GF(p).

In this paper, we propose a novel group signature scheme based upon discrete logarithm. In this scheme, when the signer has been identified, the group authority needs not to redistribute any of the keys of this signer. Moreover, the length of the signature is independent of the number of members of the group. In case, some members left the group or joins the group, the group signature remains valid. In this scheme, neither the group manager nor any group members can produce a valid signature on behalf of a member. All valid signatures are traceable by only the group manager. The proposed scheme achieves confidentiality of each group member as each group member has two sets of private keys, out of which one key is unknown to the group manager. This scheme also supports message recovery features as message is recovered by a verifier from the signature.

The rest of this paper is organized as follows. Section 2 discusses a formal introduction of group signature scheme. The proposed scheme is presented in section 3. Security analysis of the scheme is done in section 4. There is a performance evaluation of this scheme in section 5. Finally, we conclude in section 6.

2. Preliminaries

2.1 Group signature scheme

A group signatures scheme is a special form of digital signature scheme comprised of the following phases [9].

- Setup: Generates group public key and group private key.
- Join: A protocol between the group manager and a user that results in the user becoming a new group member.
- Sign: The protocol through which a member signs a document on behalf of a group.
- Verify: An algorithm for establishing the validity of a group signature given a group public key and a signed message.
- Open: An algorithm by which only the group manager determines the identity of the signer from a signed message.

A group signature scheme must satisfy the following security requirements [9].

- Anonymity: Given a signature, it is computationally hard to identify the signer, except the designated group manager.
- Unlinkability: Given two valid signatures, it is computationally hard to determine whether they are generated by the same member or not.
- Unforgeability: Only group members are able to sign messages on behalf of the group.
- Exculpability: Neither a group member nor the group manager can sign on behalf of other group members.
- Traceability: The group manager is always able to open a valid signature and identify the actual signer.
- Coalition-resistance: There is no colluding subset of group members can generate a valid signature that the group manager can not link to one of the colluding group members.

3. The proposed scheme

In this section, we present the proposed designated verifier group signature scheme. Here a group G consists of N group members ($A_1, A_2, \ldots, A_N$) and a group manager (GM). Each group member can sign a document on behalf of the group and the signature can only verified by a designated receiver (R). This scheme consists of five phases, namely, setup, join, group signature generation, group signature verification and opening of signature. The parameters used in the scheme are shown in Table 1.

3.1 Setup

A trusted authority generates two large prime numbers p and q. Then he computes $n = p.q$, such that, $p = 2p' +1$ and $q = 2q'+1$, where p' and q' are all distinct primes. Then the trusted authority chooses g as a generator of order q such that $g \in Z_q^*$. Then he publishes n, g and an one way hash function $h(.)$ but keeps p' and q' secret.

3.2 Join

When a new user wants to join the group G, he sends a request to the group manager (GM). After checking all details, the GM confirms the membership of the user by sending a unique membership number (ID_i). The selection of group members is the sole responsibility of the GM. After joining, the private and public key of the group are generated as per following steps.

Step 1*:* The GM computes $ed \equiv 1 mod\ \phi (n)$, where $\phi (n)$ is Euler's Totient function. Then the GM sends d to every legitimate member, while keeps e secret.

Step 2*:* Each group member (A_i) selects a random number $s_i \in Z_n^*$ and computes y_i as follows.

$$y_i = g^{si} \bmod n \tag{3.1}$$

and sends y_i to the GM along with its own identity ID_i.

Step 3*:* The GM checks the ID_i and computes x_i as follows.

$$x_i = (x_G \, . \, y_i)^{-d} \bmod n \tag{3.2}$$

The GM sends (x_A, d) to member A_i in a secure way and stores (ID_i, y_i, x_i) in its database for future references. The secret key pair of member A_i is (x_i, s_i).

3.3 Group signature generation

To sign a message m, a group member A_i first chooses two random integers, $k, u \in Z_n^*$ and computes (r, s, t) as follows.

$$V = s_i + k \pmod n \tag{3.3}$$

$$s = (Y_G)^d \pmod n \tag{3.4}$$

$$r = s + m.g^{-uV(yi)^{-1}} \pmod n \tag{3.5}$$

Then he computes t from the following expression.

$$s + t \equiv Vu\,(x_i)^e \pmod n \tag{3.6}$$

The member A_i attaches a time stamp δ , which is the current date or time of generating signature and sends the group signature $\xi = (r, s, t, \delta)$ of message m to the receiver. Then he sends the tuple (δ , y_i) to the group manager. The GM stores ä along with the value of y_i in its database.

3.4 Group signature Verification

After receiving the signature ξ, the verifier checks the validity of the signature by computing the following expression.

$$s^e = (Y_G) \pmod n \tag{3.7}$$

The receiver recovers the message *m* by computing the following expression.

$$m = (r - s)\,(Y_G)^{s+t}\,(\mathrm{mod}\ n) \qquad (3.8)$$

3.4 Opening phase

This phase is specially used in case of a legal dispute or to claim non-repudiation of the group signature. To identify a signer from a signature ξ, the group manager matches δ with its corresponding value of y_i in its database. Then he computes the identity of the group member who signed the message from the following expression.

$$x_i = (x_G \,.\, y_i)^{-d} \mathrm{mod}\ n \qquad (3.9)$$

From the value of x_i the group manager can reveal the identity (ID_i) of the signer.

4. Security analysis of the proposed scheme

The security of the proposed scheme is based on two well known computationally hard problems (Schneider, 1996; Stinson, 1995), namely,

(1) *Integer factorization problem*: If *N* is the product of two large primes and two integers *e* and *d* satisfying $e.d \equiv 1\ mod\ \phi(N)$, it is computationally infeasible to find the factors of *N*. Given integers *M* and *C*, it is also difficult to find d such that $C^{d} = M\ \ mod\ N$

(2) *Discrete logarithm Problem* (*DLP*): Given a large prime *p*, a generator *g* over *GF* (*p*) and an integer *y* in (1, *p*-1), it is computationally infeasible to find x such that $y=g^{x}$ mod *p* [10].

The presented scheme allows any group member to sign messages anonymously on behalf of the group. In the event of legal dispute, the GM can identify the signature's originator. Once the system has been set up, the combination of (x_G , Y_G) is fixed. However, our scheme permits any new user to join the group signature scheme and it is not necessary to modify our group public key. It may be noted that, there is no relationship between the length of the signature and the number of members in a group. Thus the running time of the verification and signing algorithms are independent to the number of group members.

Theorem 1: *The proposed group signature is indeed a valid signature.*

Proof: The correctness of above theorem is given below.

$$m = (r - s)\,(Y_G)^{s+t}\,(\mathrm{mod}\ n)$$

$$= m.g^{-uV(yi)^{-1}}(Y_G)^{s+t}(\mathrm{mod}\ n) \qquad \text{[As derived from Equation 3.5]}$$

$$= m.g^{-uV(yi)^{-1}}(g^{xG})^{s+t}(\mathrm{mod}\ n)$$

$$= m.g^{-uV(yi)^{-1}}(g^{xG})^{uV(x_i)^e}(\mathrm{mod}\ n)$$

$$= m.g^{-uV(yi)^{-1}}[g^{(y_i)^{-1}(x_i)^{-e}}]^{uV(x_i)^e}(\mathrm{mod}\ n) \qquad \text{[As derived from Equation 3.6]}$$

Lemma 1: *The proposed scheme is resistant against forgery attack.*

Proof: Any adversary Æ outside the group having the signature ξ can not forge a valid group signature as he/she does not have the values of *d*, *v* and *k*. The solving for *V* and *k* involves complexity of discrete logarithm problem. As we have used strong primes for computing *d*, obtaining *d* involves the complexity of integer factorization. Also a colluding subset of group members cannot generate a valid group signature. A valid group signature is generated by using the secret key pair (x_i, y_i) and randomized parameters (*k*, *u*, *V*) which are kept secret by a group member. No one inside the group can able to get all the above parameters to create a valid signature on behalf of another member. The proposed scheme achieves confidentiality of each group member as the private key used for signing consists of x_i and y_i, out of which only y_i is known to the group manager. Hence the group manager cannot produce a valid signature himself as s_i is unknown to him.

Lemma 2: *No one, but the group manager can reveal the identity of the signer from the group signature.*

Proof: Given the group signature ξ, a verifier or receiver verifies the signature using group's public key Y_G, as shown in Equation 3.7. From the signature, any adversary Æ can not obtain the values of s_i and x_i. The signature is considered to be provided by the group itself. The verifier can not know the identity of the group member who has signed the message *m*. So the anonymity of the group member is completely preserved. In case of a legal dispute or denial of signature, only the group manager reveals the identity of the signer. The value of x_i is computed by the GM as shown in Equation 3.9. From the value of x_i, corresponding (y_i, ID_i) can be found by matching the database maintained by the GM. No one, not even other group members can have the scret parameters x_i, x_G and y_i, as it is computationally infeasible to compute. Also it is clearly a DLP problem to compute s_i from y_i.

Lemma 3: *It is computationally hard to identify whether two different valid signatures are produced by the same group member.*

Proof: Given two group signatures (r_1, s_1, t_1) and (r_2, s_2, t_2) and group's public key Y_G, an adversary Æ can not determine whether they are signed by the same member. Let us consider the signatures are generated on messages m_1 and m_2 respectively. The values of m_1 and m_2 can be recovered from the signature itself, as per Eq. 3.8. It is computationally infeasible to reveal the identity of the signer, i.e., (y_1, ID_1) or (y_2, ID_2), from the two signatures. Each group member has different sets of y_i and x_i. A valid signature consists of all the three parameters: y_i , x_i and s_i. Hence, the proposed scheme preserves unlinkability property.

5. Performance evaluation

The complexity of any signature scheme mostly depends on four operations, namely, exponentiation, multiplication, inverse operation and hash functions. The proposed scheme is compared with some well known schemes and the result is shown in Table 1. In this evaluation, the time for performing modular addition and subtraction computations are ignored. The following notations are used to analyze the performance of the schemes.

- T_E is the time complexity of modular exponentiation
- T_M is the time complexity of modular multiplication
- T_I is the time complexity of modular inverse operation
- T_H is the time complexity of performing hash functions

Phases	Kim et al.'s scheme	Zhang et al.'s scheme	Qi's Scheme	Proposed scheme
Group signature generation	$3T_E + 4T_M + 1T_H$	$4T_E + 5T_M + 1T_H$	$8T_E + 4T_M + 3T_H$	$2T_E + 4T_M + 2T_I$
Group signature verification	$3T_E + 3T_M + 1T_H$	$4T_E + 2T_M + 2T_H$	$5T_E + 3T_M + 2T_H$	$2T_E + 2T_M$

Table 1. Performance comparison

It is observed from Table 1 that, the computational cost of verification of the proposed group signature scheme is considerably reduced, which makes it user friendly. Also the proposed scheme supports message recovery feature unlike Kim's scheme, which results less communication overhead. The signature generation of the proposed scheme is slightly costlier than Kim's scheme due to use of one inverse operation. But the proposed scheme is highly secure and unlinkable as discussed in section 4. So, if security is the utmost priority, then the proposed scheme will be more advantageous. Also, the proposed scheme has considerably lower modular exponentiation operations as compared to Qi's scheme.

6. Conclusion

In this paper, we propose a novel universally verifiable group signature scheme based upon DLP. 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 members. The proposed scheme achieves confidentiality of each group member as every member has two sets of private keys, out of which one key is unknown to the group manager. Every valid group signature is traceable by only the group manager. Moreover the verification cost of the signature is considerably low. Furthermore, the individual signers are anonymous to the verifier outside the group. The verifier can only verify the signature using group's public parameters. Also, this scheme supports message recovery. Thereby, the proposed scheme provides signer's anonymity. The verification cost of the signature is considerably low. The proposed scheme can be applicable in real word applications such as, e-voting, e-cash and e-commerce applications.

Reference

[1] Chaum, D., Van Heyst, E. (1991). Group signatures. *In*: Advances in Cryptology, EUROCRYPT'91, LNCS 547, p. 257-265. Springer-Verlag.

[2] Chen, L., Pedersen, T. P. (1995). New group signature schemes. *Advances in Cryptology-EuroCrypt '94*, p. 171–181, LNCS 950. Berlin, Springer-Verlag.

[3] Camenisch, J., Stadler, M. (1997). Efficient group signature schemes for large groups. *Advances in Cryptology - CRYPTO'97*, p. 410–424. LNCS 1296, Springer-Verlag.

[4] Lysyanskaya, A., Ramzan, Z. (1998). Group blind signatures: A scalable solution to electronic cash. *In*: Financial Cryptography (FC '98), LNCS 1465, p. 184-197. Springer-Verlag.

[5] Bresson, E., Steren, J. (2001). Efficient revocation in group signatures. *In*: Kim K, ed. Public Key Cryptology (PKC2001). New York: Springer-Verlag, 190.206.

[6] Bellare, M., Micciancio, D., Warinschi, B. (2003). Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions, *In:* Proceedings of Advances in Cryptology –Eurocrypt'03, Lecture Notes in Computer Science, vol. 2656, 614–629. Springer-Verlag.

[7] Park, H., Lim, S. , Yie, I., Kim, K. , Song, J. (2009). Strong unforgeability in group signature schemes, Computer Standards & Interfaces 31, p. 856–862.

[8] Kim, S. J., Park, S. J., Won, D. H. (1996). Convertible group signatures, *In:* Advances in Cryptology (Proceedings of Asia Crypt '96), LNCS 1163, p. 311–321, Springer, Berlin.

[9] Lee, W. B., Chang, C. (1998). Efficient group signature scheme based on the discrete logarithm. IEE. *In*: Proc. Comput. Digit. Tech., 145 (1) 15-18.

[10] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theory,* 31(4) 469-472.

[11] Rivest, R. L., Shamir, A., Adleman, L. A. (1978). method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM,* 21, 120-126.

[12] Ateniese, G.,Tsudik, G. (1999). Some open issues and new directions in group signatures. *In*: Proc. of Financial Crypto'99, LNCS, 1648, 196–211. Springer-Berlin.

[13] Zhang, J., Wu, Q., Wang, Y. (2005). A new efficient group signature scheme with forward security. Informatica, 29, 321-325.

[14] Qi, C. (2009). An Improved Group Signature Scheme based upon discrete Logarithm. Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications, p. 266-269.

Author Biography

Sujata Mohanty received her MTech degree in Computer Science from College of Engineering and Technology, Bhubaneswar, India in 2008. Presently, she is working as assistant professor in department of Computer Science at National Institute of Technology, Rourkela, India. She is doing her PhD in the area of information security in National Institute of Technology, Rourkela, India.

Banshidhar Majhi received his ME degree in Computer Science from National Institute of Technology, Rourkela, Orissa, India in 1998. In 2003 he received his PhD degree in Computer Science from Sambalpur University, Orissa, India. He is working as a professor in department of Computer Science at National Institute of Technology, Rourkela, Orissa, India. His current research interest includes information security, cryptography and biometric security.