Hierarchical Identity based Group Signature with enhanced privacy of the signers

Kitae Kim, Seongan Lim, Ikkwon Yie
Inha University
Department of Mathematics
Incheon City
Korea

Haeryong Park
Korea Information Security Agnecy
Cryptographic technology team
Seoul
Korea

Abstract: Supporting the privacy of the signer with controlled anonymity is an important feature of group signatures. However, since the group manager controls the anonymity of signer, the group manager can be a threat to the privacy of honest signers. Recently, OneCard service is popular in many ID card systems. In order to protect the singer's privacy against third party one can use group signature to verify that the user is a valid user for a specific service. If One Card service includes different levels of traceability requirements, then it must contain different sets of group signatures in order to preserve the privacy of the signer against the group manager. In this paper we propose a hierarchical identity based group signature scheme and introduce a way to provide enhanced privacy protection for signers against the group manager efficiently in the services with different levels of traceability requirements.

Key–Words: Group signature, Hierarchical ID based signature, traceability, privacy of signer

1 Introduction

Currently, OneCard system has been adopted in many ID Card system. In particular, many College ID card provides students, faculty and staff with a wide variety of services. For students planning to reside on campus, the card provides access to the residence halls. Resident students swipe their card in the dining hall to use their meal plan. The ID card also allows students to use Campus Library, and gain entrance to certain College sponsored events. ID cardholder privacy must be protected, including the cardholder's data and card system activity. A group signature can be a useful cryptographic technique to protect the cardholder's privacy since a group signature scheme can be used to verify that the card holder is a valid user of each service anonymously. Since one can use various services using his/her ID card, one card must support services with different levels traceability requirements. If the same group signature scheme is used for services with different traceability requirements, then the tracing ability of group manager could threaten the privacy of signers. Since the tracing can be done without any permission of the signer and no notices from the group manager can be sent to the traced signer, it violates the privacy rule. If different group signatures are used for each service then the card must support the implementation of several sets of group signature schemes, and this degrades the efficiency of the card.

In this paper, we shall introduce two-level identity based group signature and propose a method to implement group signatures with selective traceability with a few more parameters. Hence our scheme supports selective level of traceability in a efficient manner. In our system, it allows the signer to select the appropriate level of traceability in the service. The complexity of our scheme is almost as the same as a regular group signature but supports two different levels of traceability. And thus it enhances the privacy protection level of users when the user uses One card service with different levels of traceability requirements.

2 Preliminaries

2.1 Bilinear Pairings and the underlying complexity assumptions

The definition of bilinear group of composite order is given below.

1. G, G_T are multiplicative cyclic groups whose operations are efficiently computable. We assume that g is a generator of G. Both groups have the same composite order $n = pq$, where the factorization of n is hard.

2. The map $e : G \times G \rightarrow G_T$ has the following properties:

- Bilinearity : for all $A, B \in G$ and $a, b \in Z$, we have $e(A^a, B^b) = e(A, B)^{ab}$.
- Non-degeneracy : $e(g, g) \neq 1$.

If such a map $e : G \times G \rightarrow G_T$ can be computed efficiently, it is called a Bilinear Mapping or Pairing and the group G is called a Bilinear group.

The two-level ID-based group signature scheme is defined over bilinear group G of order n and its subgroup G_p, G_q of order p, q, respectively. The security of the two-level ID-based group signature scheme rely on the following computationally hard problems.

- Computational Diffie-Hellman Assumption on G_p: There is no probabilistic polynomial time(PPT) adversary that, given a triple $(g, g^a, g^b) \in G_p^3$ for random exponents $a, b \in Z_p$, computes $g^{ab} \in G_p$ with non-negligible probability.
- Subgroup Decision Assumption on G: For a bilinear group G of composite order $n = pq$, the uniform distribution on G is computationally indistinguishable from the uniform distribution on a subgroup of G.

And the security of group signature with selective traceability rely on the security of two-level ID based group signature scheme.

2.2 ID based signature schemes

In ID based signature scheme, Public Key Generator(PKG) sets up the system parameter and generate signing key K_{ID} for each user with identity ID in the system and gives K_{ID} to the user with ID in a secure manner. The user with the identity ID can sign on a message using his signing key K_{ID} and anyone can verify the signature using the ID of the signer.

One way to obtain ID based signature is using ID based encryption. Suppose there is a ID based encryption(IBE) and a method to generate each user's decryption key is specified. Using the IBE, an user with ID can sign on message M with the signature computed as the decryption key $K_{ID,M}$ that corresponds to (ID, M) from the underlying IBE. The signer sends $(ID, M, K_{ID,M})$ to the verifier, and the verifier checks the validity of $K_{ID,M}$ as the correctness of the decryption key. In fact, the correctness of the decryption key $K_{ID,M}$ can be checked easily by checking if $Dec_{K_{ID,M}}(Enc_{ID,M}(M')) = M'$ for randomly chosen message M' by the verifier. In this method, an attacker can obtain a decryption key of an user for the underlying IBE from a signing oracle. Hence one has to distinguish signing and decryption key extraction by using some expedient. This method can be extended to the case when users have identities of hierarchical structure.

3 Two level ID based Group signature schemes

Two level ID-based group signature is a group signature on the group of users with identity in two level hierarchies. It is based on two-level ID based signature scheme in [8]. If the identity has two independent components, then one can split the management policy for the identity system with each component. We consider one interesting feature of two-level ID based signature as selective traceability level of group signatures. We now propose a two level ID based group signature. It is very similar to the compact group signature of [5].

3.1 A two-level ID based group signature scheme

Suppose that the signer has ID-tuple

$$(ID_1||ID_2) = (d_{1,1}, \ldots, d_{1,\lambda}||d_{2,1}, \ldots, d_{2,k})$$

Setup(1^ℓ): Let $\tilde{k} = \lambda + k$. Suppose we wish to support up to $2^{\tilde{k}}$ signers in the group, and sign messages in $\{0,1\}^m$.

- System parameter : The input is a security parameter ℓ. Assume that the number of signers is at most $2^{\tilde{k}}$ in the group and that the messages to be signed are in $\{0,1\}^m$, where $\tilde{k}$ and m are polynomially related functions of ℓ. GM chooses $n = pq$ where p and q are random primes and the integer factorization of n is hard. Let G be a bilinear group of order n and denote G_p and G_q its subgroups of respective order p and q. GM chooses a generator g of G, a generator h of G_q. Next, GM chooses a random exponent $\alpha \in Z_n$.
- GM chooses following generators of G;

$$u'_1, u_{1,1}, \ldots, u_{1,\lambda},$$

$$u'_2, u_{2,1}, \ldots, u_{1,k},$$

$$v', v_1, \ldots, v_m$$

- Public Information : PP with the bilinear group (n, G, G_T, e)

$$PP = (u'_1, u_{1,1}, \ldots, u_{1,\lambda}; u'_2, u_{2,1}, \ldots, u_{2,k}; g, h, v', v_1, \ldots, v_m; A = e(g,g)^\alpha)$$

- Secret Information :
  - The master key for user Enroll, MK= $g^{\alpha} \in G$,
  - The group manager's tracing key, TK= $q \in Z$.

Enroll(PP,MK,ID): In this step, GM generates the private key $K_{ID} = (K_1, K_2, K_3, K_4, K_5)$ for the identity $ID = (ID_1||ID_2)$ and the member ID checks the validity of K_{ID}. Then ID is given the private key K_{ID} to generate signatures. For simplicity, let us define,

$$U_1 = u_1' \prod_{j=1}^{\lambda} u_{1,j}^{d_{1,j}} \text{ and } U_2 = u_2' \prod_{j=1}^{k} u_{2,j}^{d_{2,j}}$$

- GM Chooses random numbers $r_1, r_2 \in Z_n$ and creates a private key K_{ID} for the group member ID as,

$$\begin{aligned} K_{ID} &= (K_1, K_2, K_3, K_4, K_5) \\ &= (g^{\alpha} U_1^{r_1} U_2^{r_2}, g^{-r_1}, g^{-r_2}, h^{r_1}, h^{r_2}). \end{aligned}$$

Group member ID verifies the validity of K_{ID} as follows.

$$e(K_1, g)e(K_2, U_1)e(K_3, U_2) = A.$$

Sign(PP,ID,K_{ID}, M): Suppose that a group member $ID = (ID_1||ID_2)$ wishes to generate a signature σ on the message M. Note that the message M can be of any sizes. Let $k_1 = \lambda, k_2 = k$.

The signer ID first chooses random exponents $t_{1,1}, \ldots, t_{1,\lambda}; t_{2,1}, \ldots, t_{2,k} \in Z_n$ and sets for each $i = 1, 2; j = 1, \ldots, k_i$,

$$\begin{aligned} c_{i,j} &= u_{i,j}^{d_{i,j}} h^{t_{i,j}} \\ \pi_{i,j} &= \left(u_{i,j}^{2d_{i,j}-1} h^{t_{i,j}}\right)^{t_{i,j}} \end{aligned}$$

To sign a message $M = (\mu_1, \ldots, \mu_m)$, the signer sets

$$t_i := \sum_{j=1}^{k_i} t_{i,j}, \quad c_i := U_i h^{t_i}, \quad V := v' \prod_{i=1}^{m} v_i^{\mu_i}.$$

Then, the signer chooses $s_1, s_2, s \in Z_n$ and computes

$$\begin{aligned} \sigma_1 &= K_1 \cdot K_4^{t_1} \cdot K_5^{t_2} \cdot c_1^{s_1} \cdot c_2^{s_2} \cdot V^s \\ &= g^{\alpha} U_1^{r_1} U_2^{r_2} (h^{r_1})^{t_1} (h^{r_2})^{t_2} c_1^{s_1} c_2^{s_2} V^s \\ &= g^{\alpha} (U_1 h^{t_1})^{r_1+s_1} (U_2 h^{t_2})^{r_2+s_2} V^s \\ \sigma_2 &= K_2 g^{-s_1} = g^{-(r_1+s_1)} \\ \sigma_3 &= K_3 g^{-s_2} = g^{-(r_2+s_2)} \\ \sigma_4 &= g^{-s}. \end{aligned}$$

The final signature σ on the message M is given as

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \{c_{i,j}\}, \{\pi_{i,j}\}).$$

Verify(PP,M,σ): Given a signature σ on a message M, the verification proceeds in two phases.

- Phase 1 : Check if $c_{i,j} = u_{i,j}^{d_{i,j}} h^{t_{i,j}}$ for each $i = 1, 2$ and $j = 1, \ldots, k_i$.
  - For each $i = 1, 2, j = 1, \ldots, k_i$, check if $e(c_{i,j}, u_{i,j}^{-1} c_{i,j}) = e(h, \pi_{i,j})$.
- Phase 2 : Check if the signature σ for M is valid.
  - Compute $c_i = u_i' \prod_{j=1}^{k_i} c_{i,j}$ for $i = 1, 2$.
  - Compute $V = v' \prod_{j=1}^{m} v_j^{\mu_j}$ from the message $M = (\mu_1, \ldots, \mu_m)$.
  - Check if $e(\sigma_1, g) \cdot e(\sigma_2, c_1) \cdot e(\sigma_3, c_2) \cdot e(\sigma_4, V) = A$ holds.

If all tests are successful, the verifier outputs `valid`; otherwise, it outputs `invalid`.

Trace(PP, TK, σ): Assumed to pass the verification test for signature σ on some message M that is not needed here.

Let $ID = (d_{1,1}, \ldots, d_{1,\lambda}||d_{2,1}, \ldots, d_{2,k})$ denote the bits of the signer's identity that is to be determined. To recover the bits of ID, for each $i = 1, 2, j = 1, \ldots, k_i$, the tracer sets, if $(c_{i,j})^q = 1$, then $d_{i,j} = 0$; otherwise, $d_{i,j} = 1$.

3.2 Security of two-level ID based group signature scheme

The security requirements of group signature schemes are characterized as "Full Anonymity" and "Full Traceability" from Bellare et. al. The requirement "Full Anonymity" ensures the group signatures do not reveal their signer's identity. The requirement "Full Traceability" ensures that all signatures trace to a member of the signer and it includes the signatures those created by the collusion of multiple users and the group manger trace to a member of the forging coalition. The compact group signature scheme by Boyen and Waters is based on two-level Identity based signature scheme and they have shown that the security proof of the compact group signature reduces to the security of the underlying signature scheme. We introduced a group signature scheme based on the three-level identity based signature and the security of our group signature reduces to the security of the underlying signature scheme. We omit the security proof due to the length constraint.

Theorem 1 *If there exists a (t, ϵ) adversary for the full tracing game for two-level ID based group signature then there exists a $(\tilde{t}, \epsilon)$ forgery with chosen message attack (UF-CMA) against the underlying two-level ID based signature scheme, where $t \approx \tilde{t}$.*

Theorem 2 *The Two-level ID based Group Signature scheme has Full Anonymity if Subgroup Decision Problem is hard in G.*

4 Selective traceability using two-level ID based group signatures

Now we describe our proposed how to support a selective traceability using 2-level ID based group signatures. Suppose users in a group have hierarchical identities $ID = id_1||id_2||\cdots||id_l$. We also assume that the component id_i never be zero bit strings for any $i = 1, 2, \ldots, l$.

We say that a group signature for a group of users with hierarchical identities has traceability of t level if

- any user with the identity of the form $ID = id_1||id_2||\cdots||id_l$ can sign on a message on the behalf of the group anonymously
- In the case of disputes, the group manager can trace back to $id_1||\cdots||id_t$ but no information on the remaining part $id_{t+1}||\cdots||id_l$.

In some cases such as One Card service, it is desirable to support the traceability level selectively. A simple solution for services with two different level of traceability is to use two group signatures independently. Two different set of system parameters must be integrated in the Card, it degrades the efficiency of the system. Now we introduce how to set up a group signature that supports the selective level of traceability requirement efficiently using a two-level ID based group signature.

4.1 A group signature scheme with selective traceability

Suppose that the user in our system has hierarchical identity system with depth l. We split $ID = id_1 id_2 \cdots id_l = (ID_1||ID_2)$ with $ID_1 = id_1||\cdots||id_t$ and $ID_2 = id_{t+1}||\cdots||id_l$. Suppose that we have

$$(ID_1||ID_2) = (d_{1,1}, \ldots, d_{1,\lambda}||d_{2,1}, \ldots, d_{2,k}).$$

We also assume that none of id_i's are zero bit strings.

Our scheme is how to give a signing key K_{ID} to the user with identity ID so that the user can select the traceability level depends on the service he uses. We use two-level ID based group signature scheme in the previous section. The difference occurs in the **Enroll** phase. In the **Enroll** phase, the group manager generates the private key K_{ID} so that the user with the ID can compute the corresponding signing key with the selected traceability. We only describe the **Enroll** phase. Other phases are exactly the same as two-level ID based group signature.

Enroll(PP,MK,ID): In this step, GM generates the private key $K_{ID} = (K_1, K_2, K_3, K_4, K_5, K_6)$ for the identity $ID = (ID_1||ID_2)$ where $ID_1 = d_{1,1}, \ldots, d_{1,\lambda}$ and $ID_2 = d_{2,1}, \ldots, d_{2,k}$.

Let us denote U_i by

$$U_1 = u_1' \prod_{j=1}^{\lambda} u_{1,j}^{d_{1,j}}, \quad U_2 = u_2' \prod_{j=1}^{k} u_{2,j}^{d_{2,j}}$$

- GM chooses $r_1, r_2, r_3 \in Z_n$ at random and creates a private key K_{ID} for the group member $ID = (ID_1||ID_2)$ as,

  $$K_{ID} = (K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7)$$

  where

  $$K_0 = U_2^{-r_2}(u_2')^{r_3}, g^{\alpha} \cdot {U_1}^{r_1} \cdot {U_2}^{r_2}),$$
  $$(K_1, K_2, K_3) = g^{-r_1}, g^{-r_2}, g^{-r_3}),$$
  $$(K_5, K_6, K_7) = (h^{r_1}, h^{r_2}, h^{r_3}).$$

- Group member ID verifies the validity of K_{ID} as follows.

  $$\begin{aligned} e(K_1, g) \cdot e(K_2, U_1) \cdot e(K_3, U_2) &= A \\ e(K_0 K_1, g) \cdot e(K_2, U_1) \cdot e(K_4, u_2') &= A \end{aligned}$$

- Group member ID computes two signing keys K_{ID}^l, K_{ID}^t from the given K_{ID} as follows.

  $$\begin{aligned} {K^l}_{ID} &= (K_1, K_2, K_3, K_5, K_6) \\ &= (g^{\alpha} \cdot {U_1}^{r_1} \cdot {U_2}^{r_2}, g^{-r_1}, g^{-r_2}, h^{r_1}, h^{r_2}) \end{aligned}$$

  $$\begin{aligned} {K^t}_{ID} &= (K_0 K_1, K_2, K_4, K_5, K_7) \\ &= (g^{\alpha} \cdot {U_1}^{r_1} \cdot {U_2'}^{r_3}, g^{-r_1}, g^{-r_3}, h^{r_1}, h^{r_3}) \end{aligned}$$

  .

  Here, one sees that

  $${U_1}^{r_1} \cdot {U_2'}^{r_2} = u_1' \left(\prod_{j=1}^{\lambda} u_{1,j}^{d_{1,j}} \right) u_2' \left(\prod_{j=1}^{k} u_{2,j}^{0} \right),$$

and hence ${K^t}_{ID}$ is the signing key for the user with the identity (ID_1, ID_2') for $ID_2' = (00\cdots00) \in \{0,1\}^k$ of two-level ID based group signature from the previous section. If the user signs using the signing key K_{ID}^t, then the signature will be traced only down to ID_1. The user with ID uses the key ${K^l}_{ID}$ in the two-level ID based group signature to generate regular group signature, and the key ${K^t}_{ID}$ in the two-level ID based group signature to generate a group signature with traceability level t. For a given signature

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \{c_{i,j}\}, \{\pi_{i,j}\}),$$

the verifier determine the traceability level of the signature from the length of the signature and verify the signature appropriately.

4.2 Security Analysis of group signature with selective traceability

Our scheme is how to make two signing keys with different traceability level in a memory efficient way. We use the same set of public parameters for two group signatures.

$$\begin{aligned} PP \;=\; & (u_1', u_{1,1}, \ldots, u_{1,\lambda}; u_2', u_{2,1}, \ldots, u_{2,k}; \\ & g, h, v', v_1, \ldots, v_m; A = e(g,g)^{\alpha}) \end{aligned}$$

The signature of the $ID = ID_1||ID_2$ on the message M computed in **l-level-Sign(PP,ID,K_{ID}, M)** is a two-level hierarchical signature on the message M with the identity $ID = ID_1||ID_2$ using signing key $K_{ID}^l = (K_1, K_2, K_3, K_5, K_6)$. And the signature of $ID = ID_1||ID_2$ on the message M computed in **t-level-Sign(PP,ID,K_{ID}, M)** is a two-level group signature on the message M with the identity $ID' = ID_1||0\cdots0$ using signing key $K_{ID}^t = (K_0K_1, K_2, K_4, K_5, K_7)$. Moreover, the signing keys K_{ID}^l, K_{ID}^t are signing keys generated by the group manager using two independent nonce sets (r_1, r_2) and (r_1, r_3), respectively. Hence the security of our scheme rely the security of the two-level hierarchical group signature scheme.

5 Conclusion

In this paper, we proposed a two-level ID based group signature and its use as group signature with selected level of traceability. In terms of traceability, the identity of a user has only two parts, one is the part to be traced and the other is the part should kept anonymous. And we used two level ID-based group signature in order to control the traceability level of the group manager. Our scheme is an extension of compact group signature but allows to select the traceability level. Our scheme supports One card service that has two different traceability requirements, and the users can select the traceability level that is appropriate to the service. Hence our scheme can be a tool for privacy enhancing mechanism in services that deal with different traceability levels such as in the One Card service.

Acknowledgement

This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD)(KRF-2004- R03-10023).

References:

[1] G. Ateniese, J/ Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme", *Crypto'00*, LNCS 1880, pp.255-270, Springer-Verlag, 2000.

[2] G. Ateniese and G. Tsudik, "Some Open issues and directions in group signature", *Financial Crypto'99*, LNCS 1648, pp.196-211, Springer-Verlag, 1999.

[3] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures:Formal definitions, simplified requirements and a construction based on general assumptions", *Eurocrypt'03*, LNCS 2656, pp.614-629, Springer-Verlag, 2003.

[4] D. Boneh, E. Shen, and B. Waters, "Strongly Unforgeable Signatures based on computational Diffie-Hellman", *PKC'06*, LNCS 3958, pp.229-240, Springer-Verlag, 2006.

[5] X. Boyen and B. Waters, "Compact Group Signatures Without Random Oracles", *Eurocrypt'06*, LNCS 4004, Springer-Verlag, 2006.

[6] D. Chaum and E. van Heyst, "Group signatures", *Eurocrypt'91*, LNCS 547, pp.257-265, Springer-Verlag, 1991.

[7] L. Chen and T.P.Pedersen, "New group signature schemes", *Eurocrypto'94*, LNCS 950, pp.171-181, Springer-Verlag, 1994.

[8] B. Waters, "Efficient identity-based encryption without random oracles", *Eurocrypto'05*, LNCS 3494, pp.114-127, Springer-Verlag, 2005.