Group Signatures with Observers

Seungjoo Kim†, Sangjoon Park‡ and Dongho Won†

† Dept. of Information Engineering, Sung-Kyun-Kwan Univ.,
300 Chunchun-dong, Suwon, Kyunggi-do, 440-746, Korea
E-mail : {sjkim, dhwon}@simsan.skku.ac.kr

‡ #0710, ETRI, Yusong P.O.BOX 106, Taejon, 305-600, Korea
E-mail : sjpark@dingo.etri.re.kr

Abstract

At Eurocrypt'91, D. Chaum and E. Heyst introduced the notion of group signatures, which allow members of a group to make signatures on behalf of the group while remaining anonymous. This paper first presents a new type of group signatures with observers. In group signatures with observers, Our solution is the most practical group signature scheme, under the assumption that Chaum's electronic wallet is secure.

1 Introduction

At Eurocrypt'91, D. Chaum and E. Heyst introduced the notion of group signatures, which allow members of a group to make signatures on behalf of the group while remaining anonymous [1]. Furthermore, in case of disputes later a trusted authority, who is given some auxiliary information, can identify the signer.

Improved solutions were later presented by Chen and Pedersen [2], Petersen [3], and Camenisch [4]. However, all previously proposed solutions have the following undesirable properties :

- the length of the group's public key and/or the size of a signature depends on the size of the group. This is very problematic for large groups.

- to add new group members, it is necessary to modify at least the public key.

So, in [5], Camenisch and Stadler present the first efficient group signature schemes which overcome these problems. The length of the public key and of the signatures are, as well as the computational effort for signing and verifying, independent of the number of group members. Furthermore, the public key remains unchanged if new members are added to the group.

However, as they employ a non-interactive minimum disclosure proof, such as proofs of knowledge of double discrete logarithms, of e-th roots of discrete logarithms, and of e-th roots of components of representations, a signature of their solution is at least 1.4 KByte long and the operations for signing/for verifying signatures require the computation of at least 18,000 modular multiplications with 600 bit modulus (this corresponds to about 20 exponentiations with full 600 bit exponents).

Also, in [6], S.J. Kim, S.J. Park and D.H. Won presented a group signatures for hierarchical multigroups by using [7]. In group signatures for hierarchical multigroups, a user who is a member of a higher group is not only able to make a group signature of his higher group, but also able to make a group signature of lower affiliated group without disclosing his higher membership, while the size of the secret data is independent of the number of the groups in which the user participates (In [5], the public key and signatures have length independent of the number of group members of one group, but isn't independent of the number of groups).

And, in [8], Chaum and Pedersen presented the excellent way to store personal databases, called "electronic wallets with observers". Their protocols allow the organizations to control and validate all messages from the user to the outside world, as well as allow the individuals to ensure that the privacy of the person is not compromised. They provided organizations with security against abuse by individuals that relies on the assumption that the tamper-proofness cannot be broken.

In this paper we present the first definition of group signatures with observers and its models. Our solution is the most practical group signature scheme, under the assumption that Chaum's electronic wallet is secure.

2 Definitions

Definition 1. (*group signatures* [1]) A group signature scheme must satisfy the following properties :

1. (*unforgeability*) Only group members are able to correctly sign messages.
2. (*anonymity & unlinkability*) It is neither possible to find out which group member signed a message (anonymity) nor to decide whether two signatures have been issued by the same group member (unlinkability).
3. (*security against framing attacks*) Group members can neither circumvent the opening of a signature nor sign on behalf of other group members; even the group manager cannot do so.

Definition 2. (*electronic wallet* [8]) An electronic wallet consists of two parts :

- A small, hand-held computer controlled by the user – denoted by C, for "computer"; and
- A tamper-proof module, (some times called an *observer*), issued by the organizations – denoted by T, for "tamper-proof".

These two parts are arranged in such a way that T can only talk with C and not the outside world. This might be achieved by embedding T inside C. All communication with organizations is via C.

Definition 3. (*group signatures with observers*) A group signature scheme in wallets with observers must satisfy the following properties :

1. (*unforgeability*) Only group members, valid C and T, are able to correctly sign messages.
2. (*anonymity & unlinkability*) It is neither possible to find out which group member signed a message nor to decide whether two signatures have been issued by the same C and T.
3. (*security against framing attacks*)

(a) No matter how C deviate from the prescribed protocol, if T follows the protocol, C can neither circumvent the opening of a signature nor sign on behalf of other group members.

(b) No matter how T and the organization deviate from the prescribed protocol, if C follows the protocol, the organization cannot correctly sign messages.

(c) Even the deviated (C, T)'s cannot sign on behalf of other honest C's.

3 Conceptual Model

System Parameter

- (sig, ver) : an ordinary digital signature scheme.
- $(encr_{GA}, decr_{GA})$: a probabilistic public-key encryption scheme of a group authority GA.
- (x_T, y_T) : T's common group key pair of (sig, ver).

Registration

1. User C_i chooses a random secret key x_i and computes a public key corresponding to x_i. C_i sends y_i to the group authority GA.
2. GA keeps (C_i, y_i) in his database, stores the common group secret key x_T and C_i's public key y_i in C_i's TRM, T_i, and sends it to C_i.

Signing

1. C_i computes a signature on the message m, $v = sig_{x_i}(m)$, and sends it to T_i.
2. (a) T_i verifies the signature, v, with C_i's public key y_i.
   (b) T_i selects a random number r and computes the ciphertext $d = encr_{GA}(v, r)$.

(c) T_i signs m and d with common group secret key x_T, $z = sig_{x_T}(m||d)$, and sends $(m||d, z)$ to C_i.

3. C_i verifies $(m||d, z)$, then the group signature is $(m||d, z)$.

Verifying

The recipient of the group signature, $(m||d, z)$, checks if

$$ver_{y_T}(m||d, z) \stackrel{?}{=} valid$$

Identifying the Signer

1. Decrypt $v = decr_{GA}(d) = decr_{GA}(encr_{GA}(v, r))$.
2. From v, find C_i which meets,

$$ver_{y_i}(m, v) \stackrel{?}{=} valid.$$

3.1 Security

- (*unforgeability*) If an ordinary digital signature scheme (*sig*, *ver*) is secure, then only group members having valid T can correctly sign messages.
- (*anonymity & unlinkability*) The recipient of the signature cannot discover which group member made it, also cannot decide whether two signatures have been issued by the same group member, if a probabilistic public-key encryption scheme of a group authority GA, $encr_{GA}$ is secure.
- (*open*) In case of dispute later, the signature can be opened by a group authority having $decr_{GA}$, so that the person who signed the message is revealed.
- (*security against framing attacks*)

- framing by C : No matter how C deviates, if T follows the protocol and ($encr_{GA}$, $decr_{GA}$) is secure, then C can neither circumvent the opening of a signature nor sign on behalf of other group members.
- framing by T : No matter how T deviates, if C follows the protocol and (sig, ver) is secure, the organization cannot correctly sign messages.
- framing by (C,T) : If (sig, ver) is secure, even the deviated (C,T)'s cannot sign on behalf of other honest C's.

4 Future Work

This paper has presented the concept of "group signatures with observers". We have shown the group signatures that allow T to ensure that the user does not deviate from the opening of a signature. These protocols also allow C to ensure that the privacy of the person is not compromised. Our solution is the most practical one, under the assumption that the tamper-proofness cannot be broken and that the signature cannot be forged.

However, accidentally if the user C_i gets x_T from his TRM, T_i, and reveals it to other $C_j (j \neq i)$, then not only C_i but also C_j can circumvent the opening of a signature. Now, we are trying to solve this problem and improve our model.

References

[1] D. Chaum and E. van Heyst, "Group signatures," *Advances in Cryptology - Eurocrypt'91*, Springer–Verlag, *Lecture Notes in Computer Science* Vol. 547, 1992, pp.257-265.

[2] L. Chen and T.P. Pedersen, "New group signature schemes," *Advances in Cryptology - Eurocrypt'94*, Springer–Verlag, *Lecture Notes in Computer Science* Vol. 950, 1995, pp.163-173.

[3] H. Petersen, "How to convert any digital signature scheme into a group signature scheme," *The Proceedings of Security Protocols Workshop'97*, 1997.

[4] J. Camenisch, "Efficient and generalized group signatures," *Advances in Cryptology - Eurocrypt'97*, Springer-Verlag, *Lecture Notes in Computer Science* Vol. 1233, 1997, pp.465-479.

[5] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," *Advances in Cryptology - Crypto'97*, Springer-Verlag, *Lecture Notes in Computer Science*, Vol. 1294, 1997, pp.410-424.

[6] S.J. Kim, S.J. Park and D.H. Won, "Group signatures for hierarchical multigroups," *Proc. of ISW'97, Information Security Workshop*, Springer-Verlag, *Lecture Notes in Computer Science*, 1997.

[7] S.J. Park, S.J. Kim and D.H. Won, "ID-based group signature," *Electronics Letters*, 1997, pp.1616-1617.

[8] D. Chaum and T.P. Pedersen, "Wallet databases with observers," *Advances in Cryptology - Crypto'92*, Springer-Verlag, *Lecture Notes in Computer Science*, Vol. 740, 1993, pp.89-105.

[9] S.J. Kim, S.J. Park and D.H. Won, "Convertible group signatures," *Advances in Cryptology - Asiacrypt'96*, Springer-Verlag, *Lecture Notes in Computer Science*, Vol. 1163, 1996, pp.311-321.