Revealing the linkability of Popescue ID-based Group Signature Scheme

Hyungki Choi, Fangguo Zhang, and Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

Abstract

Group signature schemes allow a group member to sign a document on behalf of the group anonymously. In addition, in case of anonymity misuse, a group authority can recover the issuer of a signature. In this paper, we analyze the security of a group signature scheme proposed by Popescu which is a modification of the Tseng-Jan group signature scheme. We show that the scheme can't provide an important requirement of the group signature, *unlikability*. Thus, other members are allowed to identify whether two signatures have been issued by the same group member or not.

I. Introduction

In 1991, Chaum and van Heyst proposed the concept of a group signature scheme [4]. A group signature scheme allows a group member to sign messages anonymously on behalf of the group. More specifically, signatures can be verified with respect to a single public key of the group and do not reveal the identity of the signer. Futhermore, it must be infeasible to decide whether two signatures have been issued by the same group member. However, there exists a designated group manager who can, in case of later dispute, reveal the identity of the signer. The group signature schemes could be used by a company for authenticating digital documents, contracts, or press releases.

Most group signature schemes [4] are based on the discrete logarithm problem. The first ID-based [5] group signature scheme was proposed by Park, Kim, and Won [6]. However, their scheme was breakable by Mao and Lim [7]: exploiting the prime order subgroup structure of the scheme, they showed that the anonymity wasn't guaranteed. They also pointed out that the length of the group public-key and the group signatures are proportional to the size of the group. Futhermore, these scheme is 'static' if new group members added, the previously signed message can't be verified with the updated public-key.

Tseng and Jan in [8] propsed a scheme overcome this limitation but Joye, Kim and Lee in [2], however, showed that the Tseng-Jan scheme is universally forgeable. Anyone (not necessary a group member) is able to produce a valid group signature on an arbitrary message, which cannot be traced by the group authority. In [1], Popescu proposed a modification of the Tseng-Jan group signature scheme. In this paper, we show that his scheme can not guarantee the unlikability of the group signature's requirement, *i.e.*, we can decide whether signature is signed by the same group member or not.

The remainder of the paper is organized as follows. In Section 2, we review the requirements of the group signatures and Popescu ID-based group signature scheme. In Section 3, we point out that unlinkability can not be guaranteed in this scheme. Finally, we conclude in Section 4.

II. Popescu ID-based Group Signature Scheme

In this section, we overview security properties of group signatures that must be provided and describe Popescue ID-based group signature scheme. Refer to the origianl paper

[1] for more details in brief.

1. Security Properties

The following properties should be provided by a group signature scheme.

- Unforgeability of signatures : Only group members are able to sign messages. Furthermore, they must only be able to sign in a way that, when the signature is (later) presented to the group authority, he will be able to reveal the identity of the signer.
- Anonymity of signatures : It is infeasible to find out the group member who signed a message without knowing the group authority's secret key.
- Unlinkability of signatures : It is infeasible to decide whether two signatures have been issued by the same group member or not.
- Correctness : Any signature generated by a registered group member is valid.
- Coalition-resistance : No coalition of members can prevent a group signature from being opened.

2. Popescu ID-based Group Signature

This scheme is divided into four kinds of participants: a *trusted center*, a *group authority*, *signers*, and *receivers*. The *trusted center* acts as a helper to setup the system parameters. The group authority issues membership certificates to new users who wish to join the group and identifies a signer; and, in case of later disputes, opens the group signatures to reveal the identity of the actual signer. The *signer* anonymously sign on behalf of the group using their membership certificates, and the *receiver* can verify it by using the group public key.

The scheme consists of 5 algorithms: *setup*, *join*, *sign*, *verify*, and *open*. In the *setup* algorithm, *group authority* and *trusted center* select the parameters of the scheme; the *join* algorithm adds a new user to the group; the *sign* algorithm is signature algorithm itself; the *verify* algorithm is to check the validity of the signature; and the *open* algorithm allows to reveal the identity of the signer in case of later disputes.

1) Setup

To setup the system, a trusted center selects two large primes $p_1(\equiv 3 \bmod 8)$ and $p_2(\equiv 7 \bmod 8)$ such that $(p_1-1)/2$ and $(p_2-1)/2$ are smooth, odd and relatively co-prime [3]. Let $n=p_1p_2$. A trusted center also selects a large integer e with $\gcd(e,\phi(n))=1$ and selects g of large order in $Z_n^*=\{a \le n,(a,n)=1\}$, n is prime, $Z_n^*=Z_n/[0]$ where Z_n is the integer ring. The group authority chooses a secret key x and computes the corresponding public key $y=g^x(\bmod n)$. The public parameters are (n,e,g,y), and the secret parameters are (p_1,p_2,x). Let $ID_i \in Z_n$ be an identity information of a user U_i. Finally, let h be a collision resistant hash function.

2) Join

When a new member U_i joins the group, the trusted center computes

$$s_i=ID_i^{\perp e}(\bmod n)$$

and the group authority computes

$$x_i=(ID_i+eg)^x(\bmod n)$$

The user membership certificate is the pair (s_i,x_i).

3) Sign

To sign a message M, the user U_i, with certificate (s_i,x_i), chooses two random number r_1 and r_2 and computes

$$A=y^{r_2e}(\bmod n)$$

$$B=x_iy^{s_i+r_1}(\bmod n)$$

$$C=x_iy^{r_2}(\bmod n)$$

$$D=s_ih(M\|A)+r_1h(M\|A).$$

where $h(\cdot)$ is a publicly known hash function.

4) Verify

To verify that (A,B,C,D) is a valid group signature for message M, one checks whether

$$C^{eh(M\|A)}y^{eD} \equiv B^{eh(M\|A)}A^{h(M\|A)}(\bmod n).$$

5) Open

In case of disputes, the group authority can open the signature to recover who issued it by checking which identity ID_t satisfies

$$(ID_t + eg)^{xe} \equiv C^e A^{-1} (\bmod n).$$

III. Analysis

In this section, we show that Popescu ID-based group signature can't provide the unlinkability. Our attack can suggest a way to distinguish whether the group signature is signed by the same person or not.

We describe our analysis as follows: For two given messages m_1 and m_2, we want to sign group signatures respectively. We need (s_i, x_i) and (s_j, x_j) to compute $\{A_1, B_1, C_1, D_1\}$ and $\{A_2, B_2, C_2, D_2\}$. From the original Popescue scheme, we can do the followings:

$$D = s_i h(M \mid A) + r_1 h(M \mid A)$$

$$= h(M \mid A) \cdot (s_i + r_1)$$

Then, we can substitute

$$B = x_i y^{s_i + r_1} (\bmod n)$$

$$B = x_i y^{D/h(M \mid A)}$$

$$B / y^{D/h(M \mid A)} = x_i$$

For messages m_1 and m_2, we can get

$$B_1 / (y^{D_1/h(M_1 \mid A_1)}) = x_i$$

$$B_2 / (y^{D_2/h(M_2 \mid A_2)}) = x_j$$

If two group signatures were signed by the same person, $x_i = x_j$. Thus, the *unlinkability* of the group signature requirement is violated.

IV. Concluding Remarks

There have been many trials for making ID-based group signature scheme. However, many proposals have been failed to provide some important properties. In this paper, we show that a modified ID-based group signature scheme proposed by Popescue could not provide unlinkability of group signature requirement which is one of important properties the group signature scheme.

References

[1]. C. Popescu, "A Modification of the Tseng-Jan Group Signature Scheme", STUDIA Universitatis Babes-Bolyai Informatica 2, Volume XLV, pp. 36-40, 2000.

[2]. M. Joye, S. Kim, and N. Lee, "Cryptanalysis of Two Group Signature Scheme", ISW'99, LNCS 1729, pp. 271-275, 1999.

[3]. U. M. Maurer and Y. Yacobi, "Non-interactive Public-Key Cryptography", Eurocrypt '91, LNCS 547, pp.489-507, 1991.

[4]. D. Chaum and E. Heyst, "Group Signatures", Advanced in Cryptology, Eurocrypt'91, LNCS 950, pp. 257-265, 1991.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology, Crypto'84, LNCS 196, pp. 47-53, 1985.

[6] S. Park, S. Kim, and D. Won, "ID-based group signature", Electronics Letters Vol. 33, No. 19, pp. 1616-1617, 1997.

[7] W. Mao and C. Lim, "Cryptanalysis in prime order subgroups of Z_n", Advances in Cryptology, Asiacrypt'98, LNCS 1514, pp. 214-226, 1998.

[8] Y. Tseng and J. Jan, "A novel ID-based group signature", 1998 International Computer Symposium, Workshop on Cryptology and Information Security, pp. 159-164, 1998.