Two Attacks on Xia-You Group Signature*

(Zhang Jianhong ,Wang Ji-lin ,Wang Yumin)
(National Key Lab of Integrated Service Networks , Xidian Univ, Xi'an 710071,China)

Abstract: Group signature is very important primitive in cryptography. A group signature scheme allows any group member to sign on behalf of the group in an anonymous and unlinkable fashion .In case of dispute, group manager can reveal the identity of the signer. Recently, S.Xia and J.You proposed a group signature scheme based on identity with strong separability in which the revocation manager can work without the involvement of the membership manger. In this paper, we analyze the security of Xia-You group signature and indicate that two or more group members can collude to construct a valid signature and any group member can forge a valid membership certification.

Keywords: group signature, coalition attack, individual attack, security

1.Introduction

Digital signature, one of the most important application of public key cryptosystem, can be used to authenticate the identity of the sender of a message or the signer of a document and to identify data integrality. With high internet development, digital signature plays an important role in electronic commerce and identity authentication. Group signature is very important signature with additional functionality.

Group signature is a relatively new concept introduced by Chaum and van Heijst [1] in 1991. A group signature, akin to its traditional counterpart, allows the signer to demonstrate knowledge of a secret with respect to a special document. A group signature is publicly verifiable : it can be validated by anyone in possession of a group public key. However, group signatures are anonymous in that no one, with the exception of a designated group revocation manager, can determine the identity of the signer. Furthermore, group signature are unlikable which makes it computationally hard to establish whether or not multiple signatures are produced by the same group member. In exceptional cases any group signature can be "opened" by a group manager to reveal unambiguously the identity of the actual signer. At the same time, no one(including the group manager) can misattribute a valid group signature.

Group signature schemes have many features such as anonymity, unforgeability, unlinkability and so on. These features make group signatures attractive for many special application such as voting and bidding . Recently, several group signatures based on identity [2,4] was proposed. Unfortunately, these schemes have been attacked soon. In 2002, Xia-You [3] present a novel group signature scheme based on identity. In this paper, we present two methods to attack the group signature. With our attack, any legal group member can fabricate a new membership

*supported by National funds (19931010)

certification to make a valid signature and two or more group member can collude to create a new membership certification. all the above attacks cannot be traced by the group revocation manger.

The organization of this paper is as follows: in Section 2 we describe Xia-You's group signature, and in Section 3, we propose two attack methods. We make a concluding remark in the final section.

2.Xia-You's Group Signature Scheme

In 2002, S.Xia and J.You [3] presented a novel group signature scheme with strong separability based on the identity cryptographic system firstly introduced by Shamir [6]. A simple description is as follows, more detail description refers to the original paper [3].

2.1 Trusted Authority Setup

The trusted authority chooses two big prime number $p_1 \equiv \pm 1 (\mathrm{mod}\, 8)$, $p_2 \equiv \pm 3 (\mathrm{mod}\, 8)$ of about 100 decimal digits such that $p_1 - 1$ and $p_2 - 1$ contains several prime factors of $13 \sim 15$ decimal digits, but no larger on, and that $(p_1 - 1)/2$ and $(p_2 - 1)/2$ are relatively prime. Let $n_1 = p_1 * p_2$. According the selection of p_1 and p_2, the Jacobi symbol $(2/n_1)$ is equal to -1. According to (p_1, p_2) selection ,the trusted authority can easily find the discrete logarithms modulo p_1 and p_2 respectively. Finally, the trusted authority randomly chooses a number g which meets $g < \min(p_1, p_2)$ and publishes (n_1, g) and keeps (p_1, p_2) secret.

2.2 Group member 's Private Key generation

Suppose Alice wants to join a group, Alice submits her own identity information D_A to the trusted authority and the trusted authority sets $ID_A = D_A$ if $(D_i / n_1) = 1$ or $ID_A = 2D_A (\mathrm{mod}\, n_1)$ if $(D_i / n_1) = -1$. Finally, the trusted authority computes the private key x_A of Alice as follows $ID_A = g^{x_A} (\mathrm{mod}\, n_1)$.

2.3 Group Manager's Setup

The group manager chooses two strong primes p_3, p_4 and computes a RSA modulo number $n_2 = p_3 * p_4 \quad (n_1 < n_2)$, the public exponent is e and the private exponent is d ,The group manager chooses two integers $x \in Z_{n_1}, h \in Z_{n_1}^*$ and computes $y = h^x (\mathrm{mod}\, n_1)$ satisfying $y \in Z_{n_1}^*$ .Let $H(.)$ be a hash function that maps $\{0,1\}^* \to Z_{n_1}$ .The public key of the group manager is $(n_2, e, h, y, H(.))$ and his secret key (x, d, p_3, p_4).

2.4 Generating Membership Keys

When Alice wants to join the group, the group manager computes $z_A = ID_A^d (\mathrm{mod}\, n_2)$ and sends it to Alice in a secure way. Alice verifies the validity of z_A by $ID_A = z_A^e (\mathrm{mod}\, n)$.

2.5 Signing Phase

When a group member Alice with (x_A, z_A) signs a message M, She chooses random integers $\alpha, \beta, \theta, \omega \in Z_{n_1}$ and $\delta \in Z_{n_2}$ and computes as follows:

$$A = (y^{\alpha} z_A)(\mathrm{mod}\, n_2)$$
$$B = y^{\omega} ID_A$$
$$C = h^{\omega}(\mathrm{mod}\, n_1)$$
$$D = H(y \| g \| h \| B \| \hat{B} \| C \| v \| t_1 \| t_2 \| t_3 \| M)$$

where $\hat{B} = B(\mathrm{mod}\, n_1), v = (A^e / B)(\mathrm{mod}\, n_2), t_1 = y^{\sigma}(\mathrm{mod}\, n_2), t_2 = (y^{\beta} g^{\theta})(\mathrm{mod}\, n_1)$, $t_3 = h^{\beta}(\mathrm{mod}\, n_1)$. $E = \delta - D(\alpha e - \omega), F = \beta - D\omega$, $G = \theta - Dx_A$. Finally, the group signature on M is (A, B, C, D, E, F, G).

2.5 Verification Phase

If the verifier validates the message-signature pair $\{M, (A, B, C, D, E, F)\}$, verifier computes

$$\hat{B}' = B(\mathrm{mod}\, n_1), v' = (A^e / B)(\mathrm{mod}\, n_2)$$
$$t_1' = (v'^D y^E)(\mathrm{mod}\, n), t_2' = (\hat{B}'^D y^F g^G)(\mathrm{mod}\, n_1), t_3' = (C^D h^F)(\mathrm{mod}\, n_1)$$
$$D' = H(y \| g \| h \| B \| \hat{B}' \| C \| v' \| t_1' \| t_2' \| t_3' \| M)$$

if and only if $D' = D$,the verifier accepts the signature .

3. Two Attacks on Xia-You's Group Signature Scheme

In this section, we present security analysis of Xia-You's Group Signature Scheme and propose two attack methods.

3.1Coalition Attack

We now show how to fabricate a valid membership certification without the help of the group manager and the trusted authority.

Let U_i and U_j respectively denote user i and user j and their identities are ID_i and ID_j ,if the two users collude, then they can fabricate a new member certification. Suppose user i and user j receive the private key x_i, x_j respectively from the trusted authority and x_i, x_j satisfy the following relation.

$$ID_i = g^{x_i}(\mathrm{mod}\, n_1), ID_j = g^{x_j}(\mathrm{mod}\, n_1)$$

At the same time, member certifications of U_i and U_j are z_i, z_j respectively and have the following relations.

$$ID_i = z_i^{\,e}(\mathrm{mod}\, n_2), ID_j = z_j^{\,e}(\mathrm{mod}\, n_2)\,.$$

U_i and U_j can forge a valid membership certification by the following collusion :

1) U_i and U_j compute a false identity $ID' = ID_i * ID_j$

2) compute a false private key $x' = x_1 + x_2$.

3) compute a false member key $z' = z_i z_j$

Then a new member certification is (x', z'). Obviously, (x', z') satisfy the following relations

$ID' = g^{x'} (\mathrm{mod}\, n_1) = g^{x_i + x_j} (\mathrm{mod}\, n_1) = g^{x_i} (\mathrm{mod}\, n_1) * g^{x_j} (\mathrm{mod}\, n_1) = ID_i * ID_j$ and

$ID' = ID_i * ID_j = (z_i^e \bmod n_2)(z_j^e \bmod n_2) = (z_i z_j)^e (\mathrm{mod}\, n_2) = z'^e (\mathrm{mod}\, n_2)$

thereby membership certification (x', z') is a valid member certification . the user U_i and the user U_j can collude to produce valid signatures by member certification (x', z'). In case of dispute , though the group manager can determine ID' ,but if he want to check out the colluder ,he must search the products of any t out of n members ' ID . $(2 \le t \le n)$ to trace the identities of the user U_i and the user U_j .This is impossible in computation. Furthermore we will improve this kind of attack in the end of section **3.2.**

3.2 Individual A ttack

In the section, we now show how to produce a valid membership certification by a legal group member without the help of the group manager and the trusted authority.

Suppose the user U_i of identity ID_i has a private key x_i from the trusted authority and x_i satisfies the relation $ID_i = g^{x_i} (\mathrm{mod}\, n_1)$; The membership key of user U_i is z_i which satisfy $ID_i = z_i^e (\mathrm{mod}\, n_2)$.

Individual attack is as follows:

1) Randomly choose a number k ,and compute false identity $ID' = (ID_i)^k$
2) Compute private key $x' = kx_i$.
3) Compute member key $z' = z_i^k (\mathrm{mod}\, n_2)$

Then a new member certification is (x', z'). Obviously, (x', z') satisfy the following relations

$$ID' = ID_i^k = (g^{x_i} \bmod n_1)^k = (g^{x_i k} \bmod n_1) = g^{x'} \bmod n_1$$

$$ID' = (ID_i)^k = (z_i^{\,e})^k = (z_i^k)^e = (z')^e \bmod n_2$$

From the above relation, we can infer that (x', z') is a valid member certification.

According to the above two attacks, we can also construct a strong attack by combining coalition attack with individual attack

1) user U_i and user U_j randomly choose k_i, k_j respectively and compute a false identity $ID' = (ID_i)^{k_1} (ID_j)^{k_2}$.

2) Compute private key. $x' = k_i x_i + k_j x_j$

3) Compute member key $z' = (z_i)^{k_i}(z_j)^{k_j}$

A new produced member certification is (x', z') satisfy the following relation

$$ID' = (ID_i)^{k_i}(ID_j)^{k_j} = g^{x_i k_i} g^{x_j k_j} = g^{x_i k_i + x_j k_j} = g^{x'} (\mathrm{mod}\, n_1) \text{ and}$$

$$ID' = (ID_i)^{k_i}(ID_j)^{k_j} = (z_i^{\,e})^{k_i}(z_j^{\,e})^{k_j} = (z_i^{k_i} z_j^{k_j})^{e} (\mathrm{mod}\, n_2).$$

As is described above , one or more group members can forge a valid membership certification to produce a valid signature without identity tracing ..

5.Conclusion

Group signature scheme allows a group member to anonymously sign on behalf of group, it can ensure the anonymity of the signer. This paper analyzes the security of the Xia-You group signature and presents two primitive attack methods and one combination attack. We have shown the Xia-You's signature scheme can been forged by constructing a new member certification and the group manager cannot trace the forger's identity. The open work is how to revise the group signature scheme.

References

[1] D.Chaum and E.Hijst ,Group signatures[C] Advances in Cryptology-Eurocrypt 91 ,LNCS 547,pp 257-265 ,Springer-Verlag ,1991

[2] J.Camenisch and M.Stadler, Efficient group signature schemes for large groups[C],Advances in Cryptology-CRYPTO97 ,LNCS 1294 ,pp 410-424 ,Springer-Verlag, 1997

[3]S.Xia and J.You ,A group signatures scheme with strong separability ,The Journal of systems and software ,Vol.60, Issue 3, pp 177-182,in 2002

[4]Yuh-Min Tseng and Jinn-Ke Jan ,A novel ID-based group signatures, 1998 International Computer Symposium, Workshop on Cryptology and Information Security ,Tainan ,December 17-19,1998,pp 159-164.

[5]J.Traore, Group signatures and their relevance to privacy protecting offline electronic cash systems, Proc of ACSIP 99 ,LNCS 1587 ,pp 228-243 ,Springer-Verlag,1999

[6]A. Shamir ,Identity-based cryptosystems and signature schemes ,Advances in Cryptology-Crypto 84,LNCS 196 ,pp 47-53,Springer-verlag ,1984

[7]G. Maitland ,and C. Boyd, Fair electronic cash based on a group signature scheme ,ICICS 2001,LNCS 2229,pp 461-465 ,Springer-verlag ,2001.