ICS2002

Workshop on Cryptology and Information Security

Forgery Attack on Xia-You's Group Signature

Abstract

Recently, Xia and You proposed an ID-based group signature scheme with strong separability. This article shows a universal forgery attack on the scheme.

Index term: Cryptography, group signature.

Dr. Hung-Yu Chien

Department of Information Management,

NanKai College,

NanTou, Taiwan, R.O.C.

E-mail: redfish6@ms45.hinet.net

Comments: Forgery Attack on Xia-You's Group Signature

Abstract

Recently, Xia and You proposed an ID-based group signature scheme with strong separability. This article shows a universal forgery attack on the scheme.

Index term: Cryptography, group signature.

1. Introduction

Chaum and Heijst first proposed the concept and a scheme of group signature [1] by which a group member can represent his group to sign a signature without revealing his identity. However, the group manager can open the signer's identity, in case of a later dispute. Since then, several group signature schemes [2-5] have been proposed to either improve the performance or improve the functionalities. However, some schemes [4-5] were found insecure later.

A secure group signature scheme should satisfy the following properties:

Unforgeability: Only group members are able to sign messages on behalf of the group.

Anonymity: Given a valid group signature of some message, it is computationally hard for anyone except the group manager to identify the actual signer.

Unlinkability: Deciding whether two different valid group signatures were signed by the same member is computationally hard.

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.

An ID-based cryptosystem [7] has the advantage of eliminating the cost of maintaining the public key directory and verifying a user's public key, since a user's identity is his public key. The schemes [4-5] are ID-based group signature schemes. Recently, Xia and You [6] proposed a new ID-based group signature scheme with strong separability, where the role of a group manager is further divided into two parts: a membership manager and a revocation manager. A membership manager maintains the membership of a group, and a revocation manager can alone open the identity of a valid group signature, without the co-operation of the membership manager. This separation of the privilege has important applications in E-commerce [6]. This article shows a universal forgery attack on Xia-You's group signature scheme.

2. Review of Xia-You's group signature scheme

Initialization:

Initially, the Trusted Authority (TA) randomly chooses two primes p_1 and p_2 of about 100 decimal digitals, and lets $m = p_1 \cdot p_2$, where $p_1 \equiv \pm 1 \bmod 8$ and $p_2 \equiv \pm 3 \bmod 8$ so that the Jocobi symbol $(2/m)$ equals –1 [8]. TA publishes m and a generator g, where $g < \min(p_1, p_2)$. A signer U_i's ID_i is defined in Equation (1) to ensure each ID_i has a discrete logarithm modulo a composite number m, where D_i is the signer's public identity information [6]. TA now computes x_1 as U_i's secret key, such that $g^{x_i} \equiv_m ID_i$.

$$ID_i = \begin{cases} D_i & \text{if } (D_i/m)=1 \\ 2D_i & \text{if } (D_i/m)=-1 \end{cases}, \text{ where } (D_i/m) \text{ is the Jacobi symbol.} \qquad (1)$$

Now the membership manager computes $n = p_3 \cdot p_4$, where p_3 and p_4 are two large primes such that p_3-1 and p_4-1 are not smooth and $n > m$. He publishes (e, n) and $h()$ as the group public parameters, where $h()$ is a secure one-way hash function and e is the RSA's public key satisfying $e \cdot d = 1 \bmod f(n)$. When a signer U_i wants to join the group, the membership manager computes $z_i \equiv_n ID_i^d$ as U_i's secret membership key.

Next, the revocation manager randomly chooses two integer $x \in Z_m$ and $h \in Z_m^*$, computes $y = h^x \bmod m$ satisfying $y \in Z_m^*$, and publishes h and y as the group's public parameters, in addition to (e, n, $h()$).

Signing phase:

To sign a message M, U_i randomly chooses five integers $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{q}, \boldsymbol{w} \in Z_m$ and $\boldsymbol{d} \in Z_n$, computes $A \equiv_n (y^a \cdot z_i)$, $B = y^w \cdot ID_i$, $\hat{B} \equiv_m B$, $C \equiv_m h^w$, $v \equiv_n (A^e / B)$, $t_1 \equiv_n y^d$, $t_2 \equiv_m (y^b \cdot g^q)$, $t_3 \equiv_m h^b$, $\boldsymbol{e} = \boldsymbol{a} \cdot e - \boldsymbol{w}$, $E = \boldsymbol{d} - D \cdot \boldsymbol{e}$, $F = \boldsymbol{b} - D \cdot w$, $G = \boldsymbol{q} - D \cdot x_i$, and $D = h(y \| g \| h \| A \| B \| \hat{B} \| C \| v \| t_1 \| t_2 \| t_3 \| M)$. Finally, he sends (A, B, C, D, E, F, G) as a signature for message M.

Verification phase:

A verifier can verify the signature (A, B, C, D, E, F, G, M) as follows. He computes $\hat{B}' \equiv_m B$, $v' \equiv_n (A^e / B)$, $t_1' \equiv_n v'^D \cdot y^E$, $t_2' \equiv_m \hat{B}'^D \cdot y^F \cdot g^G$, $t_3 \equiv_m C^D \cdot h^F$, and $D' = h(y \| g \| h \| A \| B \| \hat{B}' \| C \| v' \| t_1' \| t_2' \| t_3' \| M)$. The verifier will accept the signature if D' equals D.

3. Universal forgery attack

This section will show a universal forgery attack on Xia-You's scheme, where an attacker can easily forge a valid group signature for any message. Let M' be a message on which the attacker is about to forge a signature. The attacker randomly chooses five integers k_1 and $G \in Z_m$, and k_2, k_3, and $k_4 \in Z_n$. He then computes $C \equiv_m h^{k_1}$, $A \equiv_n y^{k_2}$, $B = y^{k_1}$, $v \equiv_n \frac{A^e}{B}$, $t_1 \equiv_n y^{k_3}$, $t_2 \equiv_m y^{k_4} \cdot g^G$, $t_3 \equiv_m h^{k_4}$, and $D = h(y \| g \| h \| A \| B \| \hat{B} \| C \| v \| t_1 \| t_2 \| t_3 \| M')$. He finally sends ($A, B, C, D, E, F, G$) as a group signature on message M'.

A verifier will accept the signature. It can be easily checked that D' equals D, since the verifier will computes $v' \equiv_n \frac{A^e}{B} \equiv_n y^{e \cdot k_2 - k_1} \equiv_n v$, $\hat{B}' \equiv_m B$, $t_1' \equiv_n v'^D \cdot y^E \equiv_n y^{k_3} \equiv_n t_1$, $t_2' \equiv_m \hat{B}'^D \cdot y^F \cdot g^G \equiv_m y^{k_4} \cdot g^G \equiv_m t_2$, $t_3' \equiv_m C^D \cdot h^F \equiv_m h^{k_4} \equiv_m t_3$.

4. Conclusions

In this article, we have shown that an attacker can easily forge a signature for any message on Xia-You's group signature scheme.

References

1. Chaum, D., and Heijst, E., "Group signature", *in: Advance in Cryptography-EUROCRYPT'91*, LNCS547, Springer-Verlag, Berlin, 1992, pp. 257-265.
2. Chen, L., Pedersen, T.P., "New group signature schemes", *in: Advance in Cryptography-EUROCRYPT'94*, LNCS950, Springer-Verlag, Berlin, 1995, pp. 171-181.
3. Camenisch, J., and Stadler, M., "Efficient group signature schemes for large groups", *in: Advance in Cryptography-CRYPTO'97*, LNCS1296, Springer-Verlag, Berlin, 1997, pp. 410-424.
4. Park, S., Kim, S., and Won, D., "ID-based group signature", *Electron. Lett. 33(19)*, 1997, pp. 1616-1617.
5. Tseng, Y.-M., and Jan, J.-K., "A novel ID-based group signature", *Inf. Sci. 120*, 1999, pp. 131-141.
6. Xia, S., and You, J., "A group signature scheme with strong separability", *The Journal of Systems and Software 60*, 2002, pp. 177-182.
7. Shamir, A., "Identity-based cryptosystem based on the discrete logarithm", *in:*

Advance in Cryptography-CRYPT' 84, LNCS196, 1985, pp. 47-53.