Cryptanalysis of Two New Signature Schemes

Fangguo Zhang and Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{zhfg, kkj}@icu.ac.kr

Abstract. Group signature and blind signature are very important primitives in cryptography. A group signature scheme allows a group member to sign messages anonymously on behalf of the group and a blind signature scheme can ensure anonymity of the sender of a message. Recently, S. Xia and J. You [14] proposed a group signature scheme with strong separability in which the revocation manager can work without the involvement of the membership manager and J.J-R. Chen and A.P. Chen [5] proposed a blind signature scheme based on dual complexities (which combines factorization and discrete logarithm problem). In this paper, we give a universal forgery attack on Xia-You's group signature scheme which any one (not necessarily a group member) can produce a valid group signature on an arbitrary message, and it is untraceable by the group revocation manager. For Chen-Chen's blind signature scheme, we show that it could not meet the untraceability property of a blind signature, *i.e.*, it could not ensure anonymity of the user.

Key words: Group signature, Blind signature, Cryptanalysis.

1 Introduction

Digital signatures, one of the most important applications of public key cryptosystem, can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signing is at the heart of Internet based transactions and e-commerce. Sometimes additional conditions are imposed upon digital signature. Blind signature and group signature are very important signatures with additional functionality.

Group signature is a relatively new concept introduced by Chaum and van Heijst [4] in 1991. In a group signature, the participants are group members, a group manager (It can be split into a membership manager and a revocation manager). Members of a given group are allowed to sign on behalf of the entire group. In addition, the 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. The membership manager is responsible for the system setup and for adding group members while the revocation manager has the ability to revoke the anonymity of signatures. At the same time, no one including the group manager can misattribute a valid group signature. Because the scheme allows us to anonymously verify user's ownership of some privilege, it is applied to various security protocols such as anonymous electronic cash, electronic auction, *etc.* [8][9][11][15]. In the other hand, various group signature schemes are also proposed [1][2][7][14].

The concept of blind signatures was introduced by Chaum [3], which provides anonymity of users in applications such as electronic voting, electronic payment systems, *etc.* In contrast to regular signature schemes, a blind signature scheme is an interactive two-party protocol between a user and a signer. It allows the user to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature. Blind signatures play a vital role in ensuring anonymity while still being able to provide the authentication of digital signatures.

A blind signature should have two requirements: *Blindness* (*i.e.*, the signer does not know the content of the message) and *Untraceability* (*i.e.*, the signer can not link the message-signature pair after the blind signature has been revealed to the public).

Recently, S. Xia and J. You [14] presented a group signature scheme with strong separability in which the revocation manager can work without the involvement of the membership manager, and claimed that their scheme was secure.

In InfoSecu'02, J.J-R. Chen and A.P. Chen [5] proposed a blind signature scheme based on dual complexities (which combines factorization and discrete logarithm problem).

In this paper, we present an attack on Xia and You's group signature scheme and Chen and Chen's blind signature scheme together. With our attack, any one (not necessarily a group member) can produce a valid group signature on an arbitrary message on Xia-You's group signature scheme, which cannot be traced by the group revocation manager. For Chen and Chen's blind signature scheme, we show that it could not meet the untraceability property of a blind signature.

The organization of this paper is as follows: In Section 2 we describe Xia-You's group signature scheme, and in Section 3, we propose a universal forgery attack on this scheme. After describing the blind signature scheme proposed by Chen and Chen in Section 4, we show that Chen-Chen's blind signature could not meet the untraceability property in Section 5. We make a concluding remark in the final section.

2 Xia-You's Group Signature Scheme

Recently, S. Xia and J. You [14] proposed a group signature scheme with strong separability based on the idea of identity-based cryptographic system first introduced by Shamir [12], and claimed that their scheme satisfied all the security properties of group signature.

We first give a short description of the group signature scheme proposed by S. Xia and J. You and refer to the original paper [14] for more details. Xia-You's group signature scheme is identity-based, and consists of four entities: a trusted authority for generating secrets keys of all signers, a group manager for managing the memberships and identifying the signers, several signers (group members) for issuing group signatures and several verifiers for checking them.

$$[Setup\ of\ Trusted\ Authority]$$

The trusted authority generates two prime numbers p_1 and p_2 of about 100 decimal digits such that $p_1 - 1$ and $p_2 - 1$ contains several prime factors of 13-15 decimal digits, but no larger one, and $(p_1 - 1)/2$ and $(p_2 - 1)/2$ are relatively prime. Let $m = p_1 p_2$. p_1 and p_2 can be chosen to satisfy $p_1 \equiv \pm 1 \pmod 8$ and $p_2 \equiv \pm 3 \pmod 8$ so that the Jacobi symbol $(2/m)$ is equal to -1. In this case, it is easy for the trusted authority to find the discrete logarithms modulo p_1 and p_2, respectively. g is chosen such that $g < min(p_1, p_2)$. The trusted authority publishes (m, g) and keeps (p_1, p_2) to be secret.

$$[Generating\ Users'\ Private\ Keys]$$

For a user U_i with identity information D_i, the trusted authority computes $ID_i = D_i$ (if $(D_i/m) = 1$), or $ID_i = 2D_i \pmod m$ (if $(D_i/m) = -1$). In this case, the Jacobi symbol (ID_i/m) will be sure to equal to 1. The trusted authority computes the private key x_i for U_i such that $ID_i = g^{x_i} \pmod m$.

$$[Setup\ of\ Group\ Manager]$$

The group manager setup RSA cryptosystem, $n = p_3 p_4, m < n$, the public exponent is e and the private exponent is d. The group manager chooses two integers $x \in Z_m, h \in Z_m^*$, and computes $y = h^x \pmod m$ satisfying $y \in Z_m^*$. Let $H()$ be a hash function that maps $\{0,1\}^*$ to Z_m. The public key of the group manager is $(n, e, h, y, H())$ and his secret key is (x, d, p_3, p_4).

$$[Generating\ Membership\ Keys]$$

When a user U_i wants to join the group, the group manager computes $z_i = ID_i^d \pmod n$ and sends it to U_i in a secure way. U_i checks the validity of z_i by verifying $ID_i = z_i^e \pmod n$.

$$[Signing\ Phase]$$

To sign a message M, U_i chooses random integers $\alpha, \beta, \theta, \omega \in Z_m$ and $\delta \in Z_n$, and computes

$$A = (y^\alpha \cdot z_i) \pmod n,\ B = y^\omega \cdot ID_i,\ C = h^\omega \pmod m,$$

$$D = H(y \parallel g \parallel h \parallel B \parallel \hat{B} \parallel C \parallel v \parallel t_1 \parallel t_2 \parallel t_3 \parallel M),$$

where $\hat{B} = B \pmod{m}, v = (A^e/B) \pmod{n}, t_1 = y^\delta \pmod{n},\ t_2 = (y^\beta \cdot g^\theta) \pmod{m},\ t_3 = h^\beta \pmod{m}$.

$$E = \delta - D \cdot (\alpha \cdot e - \omega),\ F = \beta - D \cdot \omega,\ G = \theta - D \cdot x_i.$$

The group signature on M is (A, B, C, D, E, F, G).

$$[Verification\ Phase]$$

After the verifier receives the message-signature pair $\{M, (A, B, C, D, E, F, G)\}$, he computes

$$\hat{B}' = B \pmod{m},\ v' = (A^e/B) \pmod{n},$$

$$t'_1 = (v'^D \cdot y^E) \pmod{n},\ t'_2 = (\hat{B}'^D \cdot y^F \cdot g^G) \pmod{m},\ t'_3 = (C^D \cdot h^F) \pmod{m},$$

$$D' = H(y \parallel g \parallel h \parallel B \parallel \hat{B}' \parallel C \parallel v' \parallel t'_1 \parallel t'_2 \parallel t'_3 \parallel M),$$

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

The signature verification is correct, and this scheme has strong separability. The reader can refer to [14] for details.

3 A Universal Forgery Attack on Xia-You's Group Signature Scheme

In this section, we propose a universal forgery attack on Xia-You's group signature scheme.

The public key of the trusted authority is (m, g) and the public key of the group manager is $(n, e, h, y, H())$. For any one, say Alice, (not necessarily a group member), she can do as follows to produce a valid group signature on an arbitrary message M without the membership key:

$$[Forging\ a\ Signature]$$

Alice chooses random integers $\alpha, \beta, \theta, \omega \in Z_m$ and $\delta \in Z_n$, and computes

$$A = y^\alpha \pmod{n},\ B = y^\omega,\ C = h^\omega \pmod{m},$$

$$\hat{B} = B \pmod{m},\ v = (A^e/B) \pmod{n},$$

$$t_1 = y^\delta \pmod{n},\ t_2 = (y^\beta \cdot g^\theta) \pmod{m},\ t_3 = h^\beta \pmod{m},$$

$$D = H(y \parallel g \parallel h \parallel B \parallel \hat{B} \parallel C \parallel v \parallel t_1 \parallel t_2 \parallel t_3 \parallel M),$$

$$E = \delta - D \cdot (\alpha \cdot e - \omega),\ F = \beta - D \cdot \omega,\ G = \theta.$$

The group signature on M is (A, B, C, D, E, F, G). We see that Alice can produce (A, B, C, D, E, F, G) without any private information.

$$[Verification\ Phase]$$

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

$$\hat{B}' = B \pmod m, \; v' = (A^e/B) \pmod m,$$

$$t_1' = ({v'}^D \cdot y^E) \pmod n, \; t_2' = ({\hat{B}'}^D \cdot y^F \cdot g^G) \pmod m, \; t_3' = (C^D \cdot h^F) \pmod m,$$

$$D' = H(y \parallel g \parallel h \parallel B \parallel \hat{B}' \parallel C \parallel v' \parallel t_1' \parallel t_2' \parallel t_3' \parallel M),$$

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

The correctness of verification of the forgery signature can be easily seen as follows:

$$\begin{aligned} t_1' = ({v'}^D \cdot y^E) &\pmod n \\ &= (A^e/B)^D \cdot y^{\delta - D\cdot(\alpha\cdot e - \omega)} \pmod n \\ &= y^{(\alpha\cdot e-\omega)\cdot D} \cdot y^{\delta - D\cdot(\alpha\cdot e-\omega)} \pmod n \\ &= y^\delta \pmod n \\ &= t_1 \\ t_2' = ({\hat{B}'}^D \cdot y^F \cdot g^G) &\pmod m \\ &= (B^D \cdot y^{\beta - D\cdot\omega} \cdot g^\theta) \pmod m \\ &= (y^{\omega\cdot D} \cdot y^{\beta - D\cdot\omega} \cdot g^\theta) \pmod m \\ &= (y^\beta \cdot g^\theta) \pmod m \\ &= t_2 \\ t_3' = (C^D \cdot h^F) &\pmod m \\ &= (h^{\omega\cdot D} \cdot h^{\beta - D\cdot\omega}) \pmod m \\ &= h^\beta \pmod m \\ &= t_3 \end{aligned}$$

From above, an adversary can forge a valid group signature on an arbitrary message. So the security of Xia-You's group signature scheme relies on neither RSA nor the discrete logarithm problem as they claimed.

4 Chen-Chen's Blind Signature Scheme

In InfoSecu'02, J.J-R. Chen and A.P. Chen [5] proposed a blind signature scheme based on dual complexities (*i.e.*, combines the factorization [10] and the discrete logarithm problem [6]). The details of this scheme are described as follows:

Signer Alice chooses a strong prime number p which satisfies: $p = 4p_1q_1 + 1$, and both p_1, q_1 are also strong prime number. Let $n = p_1q_1$. Then chooses a number g with the order of g modulo p is n. Selects a number $x \in Z_n^*$, and computes $y = g^x \pmod p$. Alice publishes $\{p, n, g, y\}$ as her public keys, and stores $\{x, p_1, q_1\}$ as her private keys.

Assuming that user Bob requests Alice generating a blind signature for message m, they perform the following steps:

1. Alice chooses a random number $k \in Z_n^*$ and computes $r = g^k \pmod p$, then sends r to Bob.
2. Bob chooses two numbers $a_2, a_3 \in Z_n^*$ and computes:

$$R = r^{a_2} g^{a_3^2} (\text{mod } p),\ a_1 = (Ra_3)^{-2} (\text{mod } n),$$

$$b_1 = a_1 m^2 (\text{mod } n),\ b_2 = R^2 a_1 a_2 (\text{mod } n).$$

   Then send b_1, b_2 to Alice.
3. Alice computes:

$$b_3 = b_1 x + b_2 k (\text{mod } n),\ b_4 = (b_3 + 1)^{\frac{1}{2}} (\text{mod } n).$$

   If $b_3 + 1$ is not a square modulo n, then requests Bob go through step 2 again until $b_3 + 1$ is a square modulo n. Alice sends b_4 to Bob.
4. Bob computes:

$$s = Ra_3 b_4 (\text{mod } n).$$

   s, R are defined as the blind signature for message m.

The verification of the blind signature (m, s, R) is as follows:

$$g^{s^2} = y^{m^2} R^{R^2} (\text{mod } p).$$

If this holds, then accept this blind signature, else refuse it.

About the correctness of verification and the blindness of above blind signature scheme, we refer to [5] for details.

5 Cryptanalysis of Chen-Chen's Blind Signature Scheme

In this section, we show Chen-Chen's blind signature scheme could not meet the untraceability property of a blind signature. The signer Alice will keep a set of records for all the blinded messages and use them to link a valid signature (m, s, R) to its previous signing process instance. In other word, after the blind signature has been revealed to the public by Bob, the signer Alice can link the message-signature pair. The details of this cryptanalysis are described as follows:

- For every message-signature pair (m, s, R), it corresponds to the signing session (r, b_1, b_2, b_4). After every signing process, Alice can compute $w = b_4 b_1^{-\frac{1}{2}} (\text{mod } n)$, and store $\{w, ID, Time, (r, b_1, b_2, b_4)\}$ in his/her database. Here ID is the identity of sender of message m, and $Time$ is the date of signing.
- Alice wants to trace (or link) a message-signature pair (m, s, R), then computes $v = sm^{-1} (\text{mod } n)$, and searches v in her database. If she finds $w = v$, then the signing session $\{w, ID, Time, (r, b_1, b_2, b_4)\}$ corresponds (m, s, R).

If a message-signature pair (m, s, R) corresponds to the signing session (r, b_1, b_2, b_4), then we have

$$sm^{-1}(\text{mod } n) = w = b_4 b_1^{-\frac{1}{2}}(\text{mod } n).$$

Since

$$a_1 = (Ra_3)^{-2}(\text{mod } n),$$

$$b_1 = a_1 m^2(\text{mod } n) = (Ra_3)^{-2}m^2(\text{mod } n),$$

$$b_1^{\frac{1}{2}} = (Ra_3)^{-1}m(\text{mod } n),$$

and

$$s = Ra_3 b_4(\text{mod } n),$$

so we have

$$sm^{-1}(\text{mod } n) = w = b_4 b_1^{-\frac{1}{2}}(\text{mod } n).$$

Blind signatures play a central role to guarantee anonymity in electronic cash by ensuring the untraceabilty and unlinkability of electronic cash. From this attack, we found that Chen-Chen's blind signature scheme could not ensure the untraceability of users.

6 Conclusion

Group signature schemes allow a group member to anonymously sign on group's behalf, it can ensure the anonymity of the signer, and blind signature can ensure the anonymity of the sender of a message. This paper analyzed the security of the group signature scheme recently proposed by S. Xia and J. You and the blind signature scheme proposed by J.J-R. Chen and A.P. Chen. We have shown that Xia-You's group signature scheme is universally forgeable, that is, any one (not necessarily a group member) can produce a valid group signature on an arbitrary message, which cannot be traced by the group revocation manager. For Chen-Chen's blind signature scheme, we have shown that it could not meet the untraceability property of a blind signature. We suggest open problems to revise their signature schemes against our attacks.

References

1. G. Ateeniese and G. Tsudik, *Some open issues and new direction in group signatures*, Proceeding of Financial Cryptography (FC'99), LNCS 1648, pp.196-211, Springer-Verlag, 1999.
2. J. Camenisch and M. Stadler, *Efficient group signature schemes for large groups*, Advances in Cryptology-CRYPTO 97, LNCS 1294, pp.410-424, Springer-Verlag, 1997.
3. D. Chaum, *Blind signatures for untraceable payments*, Advances in Cryptology-Crypto 82, pp.199-203, Plenum, NY, 1983.
4. D. Chaum and E. Heijst, *Group signatures*, Advances in Cryptology-Eurocrypt 91, LNCS 547, pp.257-265, Springer-Verlag, 1991.

5. J.J-R. Chen and A.P. Chen, *A blind signature scheme based on dual complexities*, International Conference on Information Security 2002 (InfoSecu02), pp.61-65, July 10-13, 2002, Shanghai, China.
6. T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inf. Theory, Vol.31, No.4, pp.469-472, 1985.
7. A. Lysyanskays and Z. Ramzan, *Group blind signatures: A scalable solution to electronic cash*, Financial Cryptography 98, LNCS 1465, pp.184-197, Springer-Verlag, 1998.
8. G. Maitland, and C. Boyd, *Fair electronic cash based on a group signature scheme*, ICICS 2001, LNCS 2229, pp.461-465, Springer-Verlag, 2001.
9. K.Q. Nguyen and J. Traoré, *An online public auction protocol protecting bidder privacy*, Proc. of ACISP 2000, LNCS 1841, pp.427-442, Springer-Verlag, 2000.
10. R.V. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystem*, Commun. ACM, Vol.21, No.2, pp.120-126, 1978.
11. K. Sakurai and S. Miyazaki, *An anonymous electronic bidding protocol based on a newcon vertible group signature scheme*, Proc. of ACISP 2000, LNCS 1841, pp.385-399, Springer-Verlag, 2000.
12. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.
13. J. Traoré, *Group signatures and their relevance to privacy protecting offline electronic cash systems*, Proc. of ACISP 99, LNCS 1587, pp.228-243, Springer-Verlag, 1999.
14. 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, 2002.
15. F. Zhang, F. Zhang, and Y. Wang, *Fair electronic cash systems with multiple banks*, SEC 2000, pp.461-470, Kluwer, 2000.