Security of A Multisignature Scheme for Specified Group of Verifiers

Jiqiang Lv[1], Xinmei Wang[1] and Kwangjo Kim[2]

[1] National Key Lab of ISN,
Xidian University,
Xi'an City, Shaanxi Province, 710071 CHINA
lvjiqiang@hotmail.com,xmwang@xidian.edu.cn
[2] International Research center for Information Security (IRIS),
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
kkj@icu.ac.kr

Abstract. A multisignature scheme for specified group of verifiers needs a group of signers' cooperation to sign a message to a specified group of verifiers that must cooperate to check the signature's validity later. Recently, Zhang *et al.* proposed a new multisignature scheme for specified group of verifiers. However, we find that Zhang *et al.*'s scheme cannot prevent a dishonest clerk of signing group from changing the signing message to another message of his choice while he is cooperating with the signers to produce a multisignature. Therefore, their scheme is insecure.

Key words: Public key cryptography; Digital signature, Multisignature scheme

1 Introduction

A digital signature provides the functions of integration, authentication and nonrepudiation for a signing message. Under some ordinary situations, one signer is sufficient to generate a signature on some message. But under other situations, it may need a group of signers' participation to produce a signature on a message. Due to the existence of the above situations, Itakura *et al.* [1] proposed a new concept of digital signature scheme, called multisignature scheme, during which a group of signers must cooperate to produce a signature on a message and any verifier can check the multisignature's validity by using the signing group's public key. later, Laih *et al.* [2] proposed a new type of multisignature scheme that is used for a specified group of verifiers. It is different from a multisignature scheme in that only under the group of verifiers' cooperation could a multisignature be verified. Unfortunately, He [3] pointed out that Laih *et al.*'s scheme has the weakness that the clerk of verifying group can verify a multisignature by himself if he once receives a signature from the same signing group. Recently, Zhang *et al.* [4] proposed a new multisignature scheme for specified group of verifiers, and

claimed that forging signatures in the proposed scheme is equivalent to forging Harn's signatures [5].

In this paper, we show that Zhang *et al.*'s scheme has the following weakness: a dishonest clerk of signing group can change the signing message to an arbitrary one while he is cooperating with the signers to produce a multisignature.

In the next section, we briefly review Zhang *et al.*'s multisignature scheme for specified group of verifiers. In Section 3, we show the weakness in Zhang *et al.*'s scheme. Concluding remarks are made in Section 4.

2 Review of Zhang *et al.*'s Multisignature Scheme for Specified Group of Verifiers [4]

Zhang *et al.*'s multisignature scheme consists of three phases: key generation, multisignature generation, and multisignature verification.

Key generation phase:

Let $G_S = \{U_{S1}, U_{S2}, \cdots, U_{Sn}\}$ be the group of n signers and $G_V = \{U_{V1}, U_{V2}, \cdots, U_{Vm}\}$ be the group of m verifiers. In each group, there is a specified user, called clerk. The clerk U_{Sc} of the signer's group is responsible for verifying all partial signatures signed by signers in G_S and combining them into a multisignature. The clerk U_{Vc} of the verifier's group is responsible for assisting all verifiers in G_V to verify the multisignature. The trusted center selects two large primes p and q such that $q|p-1$, a generator g with order q in Z_p and a public one-way hash function $H(\cdot)$. Each $U_{Si} \in G_S$ selects his private key $s_i \in Z_q$ and computes his public key $Y_{Si} = g^{s_i} \bmod p$. Each $U_{Vi} \in G_V$ selects his private key $v_i \in Z_q$ and computes his public key $Y_{Vi} = g^{v_i} \bmod p$. Then G_S and G_V respectively publish their group public key Y_S and Y_V, where $Y_S = \prod_{i=1}^{n} Y_{Si} \bmod p$ and $Y_V = \prod_{i=1}^{m} Y_{Vi} \bmod p$.

Multisignature generation phase:

All signers in G_S perform the following steps to generate the multisignature of a message m for the specified group G_V of verifiers:

Step 1: Each $U_{Si} \in G_S$ randomly selects an integer $k_i \in Z_q^*$, computes

$$r_i = g^{k_i} \bmod p,$$

$$r_i^{'} = Y_V^{k_i} \bmod p,$$

and sends $(r_i, r_i^{'})$ to U_{Sc}.

Step 2: After receiving all the $(r_i, r_i^{'}), (i = 1, 2, \cdots, n)$, U_{Sc} computes

$$r = \prod_{i=1}^{n} r_i \bmod p,$$

$$r^{'} = \prod_{i=1}^{n} r_i^{'} \bmod p,$$

and broadcasts $r^{'}$ to all signers in G_S.

Step 3: Each $U_{Si} \in G_S$ computes

$$w_i = s_i \cdot (H(m) + r^{'}) - k_i \bmod q, \tag{1}$$

and sends w_i to U_{Sc}.

Step 4: For each received w_i, U_{Sc} checks whether the following equation holds,

$$Y_{Si}^{H(m)+r^{'}} = r_i \cdot g^{w_i} \bmod p.$$

If all the $w_i, (i = 1, 2, \cdots, n)$, holds, then U_{Sc} computes $w = \sum_{i=1}^{n} w_i \bmod q$.

The multisignature of m is (r, w).

Multisignature verification phase:

All verifiers in G_V perform the following step to verify the multisignature of message m:

Step 1: Each $U_{Vj} \in G_V$ computes

$$X_j = r^{v_j} \bmod q,$$

and sends X_j to U_{Vc}.

Step 2: U_{Vc} computes

$$X = \prod_{j=1}^{m} X_j \bmod p,$$

and broadcasts X to all verifiers in G_V.

Step 3: Each U_{Vj} checks the validity of the multisignature of the message m by the following equation:

$$Y_S^{H(m)+X} = r \cdot g^{w} \bmod p.$$

If it holds, then the verifier accepts the signature is valid; Rejects, otherwise.

3 Security of Zhang *et al.*'s Multisignature Scheme

The dishonest clerk U_{Sc} can produce a valid multisignature on any message $\bar{m}$ while he is cooperating with the signers to produce a multisignature in the following way,

Step 1: After receiving all the $(r_i, r_i^{'})$ from each $U_{Si} \in G_S$,$(i = 1, 2, \cdots, n)$, U_{Sc} randomly chooses an integer $a \in Z_q^*$, computes

$$\bar{r} = g^a \cdot \prod_{i=1}^{n} r_i \bmod p,$$

$$\bar{r}^{'} = Y_V^a \cdot \prod_{i=1}^{n} r_i^{'} \bmod p,$$

$$\bar{r}^* = \bar{r}^{'} - H(m) + H(\bar{m}) \bmod p,$$

and broadcasts $\bar{r}^*$ to all signers in G_S.

Step 2: Each $U_{Si} \in G_S$ will compute

$$\bar{w}_i = s_i \cdot (H(m) + \bar{r}^*) - k_i \bmod q,$$

and send $\bar{w}_i$ to U_{Sc}.

Step 3: For all the $\bar{w}_i, (1 \le i \le n)$, U_{Sc} checks whether the following equation holds,

$$Y_{Si}^{H(\bar{m})+\bar{r}^{'}} = r_i \cdot g^{\bar{w}_i} \bmod p.$$

If all the above equalities hold, then U_{Sc} computes $\bar{w} = \sum_{i=1}^{n} \bar{w}_i - a \bmod q$.

The multisignature of $\bar{m}$ is $(\bar{r}, \bar{w})$, since

$$\bar{X} = \prod_{j=1}^{m} \bar{X}_j \bmod p = \prod_{j=1}^{m} (g^a \cdot \prod_{i=1}^{n} r_i)^{v_j} \bmod p = \prod_{j=1}^{m} (g^{a+\sum_{i=1}^{n} k_i})^{v_j} \bmod p$$

$$= (g^{a+\sum_{i=1}^{n} k_i})^{\sum_{j=1}^{m} v_j} \bmod p = (g^{\sum_{j=1}^{m} v_j})^{a+\sum_{i=1}^{n} k_i} \bmod p = \bar{r}^{'}.$$

Therefore, we have

$$\bar{w} = \sum_{i=1}^{n} \bar{w}_i - a \bmod q = \sum_{i=1}^{n} (s_i \cdot (H(m) + \bar{r}^*) - k_i) - a \bmod q$$

$$= \sum_{i=1}^{n} (s_i \cdot (H(\bar{m}) + \bar{r}^{'}) - k_i) - a \bmod q = \sum_{i=1}^{n} s_i \cdot (H(\bar{m}) + \bar{r}^{'}) - (a + \sum_{i=1}^{n} k_i) \bmod q$$

$$= \sum_{i=1}^{n} s_i \cdot (H(\bar{m}) + \bar{X}) - (a + \sum_{i=1}^{n} k_i) \bmod q.$$

Thus, the following multisignature verification equation holds:

$$Y_S^{H(\bar{m})+\bar{X}} = \bar{r} \cdot g^{\bar{w}} \bmod p.$$

The weakness is mainly caused by the linear relationship between $H(m)$ and $r^{'}$ in Eqn.(1). If Eqn.(1) is replaced with the equation $w_i = s_i \cdot H(m, r^{'}) - k_i \bmod q$, then the clerk U_{Sc} will not produce a multisignature on a message of his choice; Anyway, he can still change the parameter $r^{'}$ to another $\bar{r}^{'}$. Another way to improve Zhang *et al.*'s scheme is to broadcast $r_i^{'}$ to all the signers in G_S except just sending $(r_i, r_i^{'})$ to U_{Sc}. Then, each signer computes $r_i^{'}$ and produce an individual signature w_i. Furthermore, to prevent Li *et al.*'s attack [7], the certificated authority should require each user to prove that he knows the secret key corresponding to his public key. The disadvantage is to increase the computational complexity and communication costs, but higher security will be achieved.

4 Concluding Remarks

We show that Zhang *et al.*'s scheme cannot prevent a dishonest clerk of signing group from changing the signing message to another message of his choice while he is cooperating with the signers to produce a multisignature.

References

1. K. Itakura and K. Nakamura, A public-key cryptosystem suitable for digital multisignatures, NEC Res. Dev. 71 (1983) 1-8.
2. C.S. Laih and S.M. Yen, Multisignature for specified group of verifiers, Journal of Information Science and Engeering, 12 (1) (1996) 143-152.
3. W.H. He, Weaknesses in some multisignature schemes for specified group of verifiers, Information Processing Letters 83 (2002) 95-99.
4. Z. Zhang and G. Xiao, New Multisignature Scheme for Specified Group of Verifiers, Journal of Applied Mathematics and Computation, (2003) in press.
5. L. Harn, New digital signature scheme based on discrete logarithm, IEE Electronics Letters, 30 (5) (1994) 396-398.
6. L. Harn, Digital Multisignature with Distinguished Signing Authorities, IEE Electronics Letters, 35 (4) (1999) 294-295.
7. Z.C. Li., L.C.K. Hui., K.P. Chow., C.F. Chong., W.W. Tsang and H.W. Chan, Cryptanalysis of Harn Digital Multisignature with Distinguished Signing Authorities, IEE Electronics Letters, 36 (4) (2000) 314-315.