Security of a multisignature scheme for specified group of verifiers

Jiqiang Lv a,*, Xinmei Wang a, Kwangjo Kim b

a National Key Lab of ISN, Xidian University, Xi’an City, Shaanxi Province, 710071, China
b International Research Center for Information Security, Information and Communications University, 58-4 Hwaam-dong, Yusong-ku, Taehon, Daejeon 305732, South Korea

Received 24 February 2004; accepted 29 April 2004

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.

Keywords: 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

* Corresponding author.
E-mail address: lvjiqiang@hotmail.com (J. Lv).
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 and Nakamura [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 and Yen [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 Section 2, 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.


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

2.1. Key generation phase

Let \( G_S = \{ U_{S1}, U_{S2}, \ldots, U_{Sn} \} \) be the group of \( n \) signers and \( G_V = \{ U_{V1}, U_{V2}, \ldots, U_{Vm} \} \) 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 \( Y_{Si} = g^{s_i} \mod p \). Each \( U_{Vi} \in G_V \) selects his private key \( v_i \in Z_q \) and computes his public key \( Y_{Vi} = g^{v_i} \mod p \). Then \( G_S \) and \( G_V \)
respectively publish their group public key $Y_S$ and $Y_V$, where $Y_S = \prod_{i=1}^{n} Y_{Si} \mod p$ and $Y_V = \prod_{i=1}^{m} Y_{Vi} \mod p$.

2.2. 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:

$$r_i = g^{k_i} \mod p,$$
$$r'_i = Y_{Vi}^{k_i} \mod p,$$

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

**Step 2.** After receiving all the $(r_i, r'_i), (i = 1, 2, \ldots, n)$, $U_{Sc}$ computes:

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

and broadcasts $r'$ to all signers in $G_S$.

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

$$w_i = s_i \cdot (H(m) + r') - k_i \mod q,$$

(1)

and sends $w_i$ to $U_{Sc}$.

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

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

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

The multisignature of $m$ is $(r, w)$.

2.3. 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:

$$X_j = r_{Vj} \mod q,$$

and sends $X_j$ to $U_{Vc}$.

**Step 2.** $U_{Vc}$ computes:

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

and broadcasts $X$ to all verifiers in $G_V$. 
Step 3. Each $U_{V_j}$ checks the validity of the multisignature of the message $m$ by the following equation:

$$Y_{S}^{H(m)+X} = r \cdot g^w \mod p.$$ 

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 $U_{Si} \in G_S (i = 1, 2, \ldots, n)$, $U_{Sc}$ randomly chooses an integer $a \in Z_q^*$, computes:

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

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

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

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

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

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

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

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

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

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

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

$$X = \prod_{j=1}^{m} X_j \mod p = \prod_{j=1}^{m} \left( g^{a} \cdot \prod_{i=1}^{n} r_i \right)^{v_j} \mod p = \prod_{j=1}^{m} \left( g^{a+\sum_{i=1}^{n} k_i} \right)^{v_j} \mod p$$

$$= \left( g^{a+\sum_{i=1}^{n} k_i} \right)^{\sum_{j=1}^{m} v_j} \mod p = \left( g^{\sum_{j=1}^{m} v_j} \right)^{a+\sum_{i=1}^{n} k_i} \mod p = \bar{r}'.$$
Therefore, we have

\begin{align*}
\bar{w} &= \sum_{i=1}^{n} \bar{w}_i - a \mod q = \sum_{i=1}^{n} (s_i \cdot (H(m) + \bar{r}) - k_i) - a \mod q \\
&= \sum_{i=1}^{n} s_i \cdot (H(m) + \bar{r}) - a \mod q = \sum_{i=1}^{n} s_i \cdot (H(m) + \bar{r}) - \left(a + \sum_{i=1}^{n} k_i\right) \mod q \\
&= \sum_{i=1}^{n} s_i \cdot (H(m) + \bar{X}) - \left(a + \sum_{i=1}^{n} k_i\right) \mod q.
\end{align*}

Thus, the following multisignature verification equation holds:

\[ Y_S^{H(m) + \bar{X}} = \bar{r} \cdot g^{\bar{w}} \mod p. \]

The weakness is mainly caused by the linear relationship between \( H(m) \) and \( r' \) in Eq. (1). If Eq. (1) is replaced with the equation \( w_i = s_i \cdot H(m, r') - k_i \mod q \), 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 \( r' \) 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 [6], 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 other signers to produce a multisignature.

References

