Journal of Zhejiang University SCIENCE
ISSN 1009-3095
http://www.zju.edu.cn/jzus
E-mail: jzus@zju.edu.cn

# Improvement of Laih and Yen's multisignature scheme*

XIE Qi (谢 琪)†[1,2], YU Xiu-yuan (于秀源)[1,3]

([1]*Department of Mathematics, Zhejiang University, Hangzhou 310027, China*)

([2]*School of Information and Engineering, Hangzhou Teachers College, Hangzhou 310012, China*)

([3]*Hangzhou Teachers College, Hangzhou 310012, China*)

†E-mail: qixie@hztc.edu.cn

Received June 13, 2003; revision accepted Nov. 7, 2003

**Abstract:** A new attack is proposed to show that a specified group of verifiers can cooperate to forge the signature for any message by secret key substitution due to the leaked secret key or by the group public key adjustment because of the renewed members. This paper presents the improvement scheme which overcomes the security weakness of Laih and Yen's scheme.

**Key words:** Digital signature, Multisignature, Cryptography
**doi:**10.1631/jzus.2004.1155 **Document code:** A **CLC number:** TP309

## INTRODUCTION

In the information world, digital signatures provide similar functions as hand-written signature used to authenticate the content of a paper document and the identity of its creator. There are many applications in Internet. Since Itakura and Nakamura (1983) proposed the first multisignature scheme, many multisignature schemes have been proposed (Harn and Kiesler, 1989; Ohta and Okamoto, 1991). In the multisignature scheme, multiple signers can cooperate to sign the same message and any verifier can verify the validity of the multisignature. Specially, the size of the multisignature is independent of the number of signers.

Laih and Yen (1996) proposed a new multisignature scheme in which the group of signers should use each signer's private key and the group public key of verifiers to sign the same message; and only the specified group of verifiers can cooperate to verify the validity of the multisignature. He (2002) pointed out that Laih and Yen's multisignature scheme did not satisfy the security requirement; the clerk of a specified group of verifiers could alone verify the validity of multisignature without the help of other verifiers.

This paper presents a new attack on Laih and Yen's multisignature scheme. In this attack, a specified group of verifiers can cooperate to forge the signature for any message by secret key substitution using the leaked secret key or by the group public key adjustment because of the renewed members. The improvement scheme, which overcomes the security weakness of Laih and Yen's scheme is also presented.

## BRIEF REVIEW OF LAIH AND YEN'S SCHEME AND HE'S ATTACK

### Laih and Yen's scheme

The Laih and Yen's scheme is divided into three phases: the system initialization phase, mul-

* Project (No. 10271037) supported by the National Natural Science Foundation of China

tisignature generation phase and multisignature verification phase.

1. The system initialization phase

The trusted center selects two large primes $p$ and $q$, where $q|(p-1)$. Let $g$ be a generator of a multiplicative subgroup of $Z_p$ with order $q$; $H()$ denotes a one-way collision resistant cryptographic hash function.

Let $G_S=\{U_{S_1},U_{S_2},...,U_{S_n}\}$ be the group of $n$ signers and $G_V=\{U_{V_1},U_{V_2},...,U_{V_m}\}$ be the group of $m$ verifiers. $G_S$ and $G_V$ have their designed clerk $U_{s_c}$ and $U_{v_c}$ respectively. Each $U_{S_i}\in G_S$ selects his private key $s_i\in Z_q$ and computes his public key $y_{s_i}=g^{-s_i} \pmod p$, each $U_{V_j}\in G_V$ selects his private key $v_j\in Z_q$ and computes his public key $y_{v_j}=g^{-v_j} \pmod p$. Then $G_S$ and $G_V$ respectively publish their group public keys $y_s$ and $y_v$, where

$$y_s=\prod_{i=1}^{n}y_{s_i}=g^{-\sum_{i=1}^{n}s_i} \pmod p,$$

$$y_v=\prod_{j=1}^{m}y_{v_j}=g^{-\sum_{j=1}^{m}v_j} \pmod p.$$

2. Multisignature generation phase

All signers in $G_S$ perform the following steps to generate the multisignature of message $M$ for the specified group $G_V$ of verifiers.

(1) Each $U_{S_i}\in G_S$ randomly chooses $k_i\in_R Z_q$, computes $x_i=y_v^{k_i} \bmod p$, and sends $x_i$ to $U_{s_c}$. $U_{s_c}$ computes $x=\prod_{i=1}^{n}x_i \bmod p$, and broadcasts $x$ to all signers in $G_S$.

(2) Each $U_{S_i}\in G_S$ computes $e=h(x, M)$ and $w_i=k_i+es_i \pmod q$, then sends $w_i$ to $U_{s_c}$.

(3) Each $U_{s_c}$ computes $e=h(x, M)$ and $w=\sum_{i=1}^{n}w_i \bmod q$, then sends $(M, (e, w))$ to $G_V$.

3. Multisignature verification phase

Each $U_{V_j}\in G_V$ computes $X_j=(g^w y_s^e)^{-v_j} \bmod p$, and sends it to $U_{v_c}$, $U_{v_c}$ computes $X=\prod_{j=1}^{m}X_j$, and then broadcasts $X$ to all verifiers in $G_V$. Each $U_{V_j}\in G_V$ verifies the validity of the multisignature $(e, w)$ for message $M$ by checking if $e=h(X, M)$.

**He's attack on Laih and Yen's scheme**

He pointed out that $U_{v_c}$ could alone verify the validity of any multisignature $(\overline{e},\overline{w})$ without the help of other verifiers, if he has ever assisted all verifiers in $G_V$ to verify the validity of the multisignature $(e, w)$.

The reason is that $U_{v_c}$ could alone compute

$$y_s^{-\sum_{j=1}^{m}v_j}=(Xy_v^{-w})^{e^{-1}} \pmod p,$$

and

$$\overline{X}=y_v^{\overline{w}}((Xy_v^{-w})^{e^{-1}})^{\overline{e}}$$

for the other multisignature $(\overline{e},\overline{w})$, then he verifies the validity of the multisignature $(\overline{e},\overline{w})$ by checking if $\overline{e}=h(\overline{X},\overline{M})$.

## OUR ATTACK

In this section, we will show that Laih and Yen's multisignature scheme is insecure in the following cases:

Case 1: If the specified group of verifiers has ever verified the multisignature signed by $G_S$ and has new participant, they can cooperate to forge the signature for any message by the group public key adjustment because of the renewed members.

Case 2: If a specified group of verifiers has ever verified the multisignature signed by $G_S$, they can cooperate to forge the signature for any message by the secret key substitution due to the leaked secret key.

Now we discuss our attack under case 1. Let $\overline{G}_V=G_V\cup\{U_{m+1}\}$, where $U_{m+1}$ is a new participant.

When the specified group of verifiers $G_V$ has ever verified the multisignature $(e, w)$ of a message

$M$ signed by $G_S$, each $U_{V_j} \in G_V$ knows

$$x = \prod_{j=1}^{m} X_j = \prod_{j=1}^{m} (g^w y_s^e)^{-v_j} \mod p.$$

If $\overline{G}_V$ wants to forge the valid multisignature $(\overline{e}, \overline{w})$ of a message $\overline{M}$ which stands in $G_S$, each $U_{V_j} \in \overline{G}_V$ performs the following steps:

(1) Each $U_{V_j} \in \overline{G}_V$ computes $\overline{e} = h(x, \overline{M})$.

(2) All participants in $\overline{G}_V$ can cooperate to obtain $v_{m+1}$, from

$$-e\sum_{j=1}^{m} v_j = -\overline{e}(\sum_{j=1}^{m} v_j + v_{m+1}) \mod q.$$

(3) Each $U_{V_j} \in \overline{G}_V$ can obtain $\overline{w}$ from

$$-w\sum_{j=1}^{m} v_j = -\overline{w}(\sum_{j=1}^{m} v_j + v_{m+1}) \mod q.$$

(4) $\overline{G}_V$ computes

$$\overline{y}_v = g^{-v_{m+1}} \prod_{j=1}^{m} y_{v_j} = g^{-\sum_{j=1}^{m+1} v_j} \pmod p,$$

and then asks the trusted center to change $y_v$ to $\overline{y}_v$ because of the renewed members.

Therefore, $(\overline{e}, \overline{w})$ is the valid multisignature of a message $\overline{M}$. In fact:

$$\overline{X} = \prod_{j=1}^{m+1} \overline{X}_j = g^{\overline{w}(-\sum_{j=1}^{m+1} v_j)} y_s^{\overline{e}(-\sum_{j=1}^{m+1} v_j)} = g^{w(-\sum_{j=1}^{m} v_j)} y_s^{e(-\sum_{j=1}^{m} v_j)}$$

$$= \prod_{j=1}^{m} (g^w y_s^e)^{-v_j} = g^{\sum_{i=1}^{n} k_i (-\sum_{j=1}^{m} v_j)} = x \mod p,$$

and $\overline{e} = h(\overline{X}, \overline{M}) = h(x, \overline{M})$.

In case 2, if $G_V$ wants to forge the valid multisignature $(\overline{e}, \overline{w})$ of a message $\overline{M}$ which stands in $G_S$, they compute $\overline{e} = h(x, \overline{M})$, and obtain $\overline{V} \bmod q$ from $-e\sum_{j=1}^{m} v_j = -\overline{e}\overline{V} \bmod q$, obtain $\overline{w} \bmod q$ from $-w\sum_{j=1}^{m} v_j = -\overline{w}\overline{V} \mod q$, then compute $\overline{v}_1 = \overline{V} - \sum_{j=2}^{m} v_j \bmod q$, $\overline{y}_{v_1} = g^{-\overline{v}_1} \pmod p$.

Let one of the participants $U_{V_1}$ ask the trusted center to change $y_{v_1}$ to $\overline{y}_{v_1}$ due to the leaked secret key.

Therefore, $(\overline{e}, \overline{w})$ is the valid multisignature of a message $\overline{M}$.

## IMPROVEMENT OF LAIH AND YEN'S SCHEME

The improvement scheme can be divided into three phases: the system initialization phase, multisignature generation phase and multisignature verification phase.

1. The system initialization phase

The parameters are the same as those used in Laih and Yen's scheme.

2. Multisignature generation phase

All signers in $G_S$ perform the following steps to generate the multisignature of message $M$ for the specified group $G_V$ of verifiers.

(1) Each $U_{S_i} \in U_S$ randomly chooses $k_i \in_R Z_q$, computes $x_i = y_v^{k_i} \bmod p$, $r_i = g^{k_i} \bmod p$, and sends $x_i$ and $r_i$ to $U_{S_c}$. $U_{S_c}$ computes $x = \prod_{i=1}^{n} x_i \mod p$, $r = \prod_{i=1}^{n} r_i = g^{\sum_{i=1}^{n} k_i} \pmod p$, and broadcasts $x$ and $r$ to all signers in $G_S$.

(2) Each $U_{S_i} \in U_S$ computes

$$w_i = (r + h(x, M))k_i + s_i \pmod q, \quad (1)$$

then sends $w_i$ to $U_{S_c}$.

(3) On receiving the individual signature $w_i$ from $U_{S_i} \in U_S$, $U_{S_c}$ verifies the validity of the in-

dividual signature with the following equation:

$$y_{s_i} g^{w_i} = r_i^{r+h(x,M)} \pmod{p}, \ (i=1,2,\ldots,n) \qquad (2)$$

In fact:

$$y_{s_i} g^{w_i} = g^{-s_i+w_i} = g^{(r+h(x,M))k_i} = r_i^{r+h(x,M)} \pmod{p}, \quad (i=1,2,\ldots,n).$$

If all of the above equations hold, the multisignature can be obtained as ($r$, $w$), where $w=\sum_{i=1}^{n} w_i \bmod q$. $U_{s_c}$ sends the multisignature to $G_V$.

3. Multisignature verification phase

Each $U_{V_j} \in G_V$ computes $X_j = r^{-v_j} \bmod p$, and sends $X_j$ to $U_{v_c}$. $U_{v_c}$ computes $X=\prod_{j=1}^{m} X_j$, and broadcasts $X$ to all verifiers in $G_V$. Each $U_{V_j} \in G_V$ verifies the validity of the multisignature ($r$, $w$) for message $M$ with the following equation:

$$y_s g^w = r^{r+h(X,M)} \pmod{p}. \qquad (3)$$

In fact:

$$y_s g^w = g^{-\sum_{i=1}^{n} s_i + \sum_{i=1}^{n} w_i} = g^{(r+h(x,M))\sum_{i=1}^{n} k_i} = r^{r+h(X,M)} \pmod{p}.$$

## SECURITY DISCUSSION

To construct a signature for satisfying Eq.(3), the attacker should know ($s_i$, $k_i$) from ($y_{s_i}$, $r_i$). However, it is infeasible because of the intractability of solving the discrete logarithm problem.

The attacker knows ($s_i$, $k_i$) from Eq.(1) which is infeasible, because of the intractability of solving the bivariate simple equation.

If the attacker randomly chooses ($r$,$w$) to construct a signature for satisfying Eq.(3), that is infeasible under the assumption of one-way collision resistant cryptographic hash function and the intractability of solving the discrete logarithm problem.

Many multisignature schemes are vulnerable to substitute attack (Nyberg and Rueppel, 1994; Lin and Laih, 2000). So, we discuss the variant method of substitute attack below:

To forge a signature for a given message without the knowledge of the private key, one has to solve the signature ($r$,$w$) from the verification equation. Therefore, the security of the proposed scheme depends on the difficulty of the following problem: Given $g \in Z_p$ and $y_s \in Z_p$, find $r \in Z_p$ and $w \in Z_p$ such that the verification equation is satisfied.

Randomly choose ($u$, $v$), such that $r = y_s^u g^v \bmod p$. The attacker generates the following congruence equations from Eq.(3):

$$u(r+h(x,M))=1 \pmod{q}, \qquad (4)$$
$$v(r+h(x,M))=w \pmod{q} \qquad (5)$$

He knows $h(x, M)$ from Eq.(4), but he cannot find $\bar{M}$ such that $h(x, M)=h(x, \bar{M})$, because $H()$ is one-way collision resistant cryptographic hash function. Otherwise, if he randomly chooses $\bar{M}$, it would hardly satisfy Eq.(4).

Therefore, the variant method of substitute attack is invalid for use on the proposed scheme.

Obviously, the proposed scheme can withstand both He's and our attack.

## CONCLUSION

In this paper, we have shown a more harmful attack then He's on Laih and Yen's multisignature scheme, as a specified group of verifiers can cooperate to forge the signature for any message by secret key substitution due to the leaked secret key or by the group public key adjustment because of the renewed members. Therefore, Laih and Yen's scheme cannot be applied for generating multisignature for a specified verifier. Further, the paper presents the improvement scheme which overcomes the security weakness of Laih and Yen's scheme.

## References

Harn, L., Kiesler, T., 1989. New scheme for digital multisignature. *Electron. Lett.*, **25**(15):1002-1003.

He, W.H., 2002. Weakness in some multisignature for specified group of verifiers. *Information Processing Letters*, **83**(2002):95-99.

Itakura, K., Nakamura, K., 1983. A public-key cryptosystem suitable for digital multisignatures. *NEC Res. Development*, **71**(1983):1-8.

Laih, C.S., Yen, S.M., 1996. Multisignature for specified group of verifiers. *J. Inform. Sci. Engrg.*, **12**(1):143-152.

Lin, C.C., Laih, C.S., 2000. Cryptanalysis of Nyberg-Rueppel's message recovery scheme. *IEEE Communication Letters*, **4**(7):231-232

Nyberg, K., Rueppel, R.A., 1994. Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem. EUROCRYPT'94, p.182-193.

Ohta, K., Okamoto, T., 1991. A Digital Multisinature Scheme Based on the Fiat-Shamir Scheme. Proceedings ASIACRYPY'91, p.139-148.