ARTICLE IN PRESS

Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

The Journal of Systems and Software xxx (2004) xxx–xxx

The Journal of Systems and Software

www.elsevier.com/locate/jss

On the security of some proxy blind signature schemes

Hung-Min Sun [a,*], Bin-Tsan Hsieh [b], Shin-Mu Tseng [b]

[a] *Department of Computer Science, National Tsing Hua University, 101, Sec 2, Kuang-Fu Rd., Hsinchu 30055, Taiwan*

[b] *Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan 701, Taiwan*

Received 29 July 2003; received in revised form 29 January 2004; accepted 18 February 2004

Abstract

A proxy blind signature scheme is a digital signature scheme which combines the properties of proxy signature and blind signature schemes. Recently, Tan et al. proposed two proxy blind signature schemes based on DLP and ECDLP respectively. Later, compared with Tan et al.'s scheme, Lal and Awasthi further proposed a more efficient proxy blind signature scheme. In this paper, we show that both Tan et al.'s schemes do not satisfy the unforgeability and unlinkability properties. Moreover, we also point out that Lal and Awasthi's scheme does not possess the unlinkability property either.

Keywords: Cryptanalysis; Proxy blind signature; Elliptic curve; Cryptography

1. Introduction

The concept of blind signature scheme was first introduced by Chaum (1983). A blind signature scheme is a protocol played by two parties in which a user obtains a signer's signature for a desired message and the signer learns nothing about the message. With such properties, the blind signature scheme are useful in several applications such as e-voting and e-payment.

On the other hand, a proxy signature scheme (Mambo et al., 1996a,b; Kim et al., 1997; Petersen and Horster, 1997; Zhang, 1997) enables a proxy signer to sign messages on behalf of an original signer. Proxy signature schemes have been shown to be useful in many applications. For example, a manager can delegate his secretaries to sign documents when he is on vacation. Proxy signature schemes can also be used in electronics transaction (Kotzanikolaous et al., 2000) and mobile agent environments (Park and Lee, 2001; Sander and Tschudin, 1997; Lee et al., 2001). To categorize the delegation types, Mambo et al. (1996a) defined three levels of delegation: full delegation, partial delegation, and delegation by warrant. In full delegation, the original signer gives his secret key to the proxy signer. The proxy signer uses the key to sign documents. In partial delegation, the proxy signature signing key is generated by the original signer and proxy signer. In delegation by warrant, the original signer signs the warrant which describes the relative rights and information about the original signer and proxy signer. When verifying the proxy signature, a signature verifier should use the warrant as a part information of verification.

Recently, Tan et al. (2002) proposed two proxy blind signature schemes based on DLP and ECDLP respectively. A proxy blind signature scheme is a digital signature scheme which combines the properties of proxy signature and blind signature schemes. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. Tan et al. also defined the security properties for a good proxy blind signature scheme as follows:

Distinguish-ability: The proxy blind signature must be distinguishable from the normal signature.
Non-repudiation: Neither the original signer nor the proxy signer can sign message instead of the other party. Both the original signer and the proxy signer cannot deny their signatures against anyone.
Verifiability: The proxy blind signature can be verified by everyone.

[*] Corresponding author. Tel.: +88635742968; fax: +88635723694.
E-mail addresses: hmsun@cs.nthu.edu.tw (H.-M. Sun), tsengsm@mail.ncku.edu.tw (S.-M. Tseng).

0164-1212/$ - see front matter © 2004 Published by Elsevier Inc.
doi:10.1016/j.jss.2004.02.015

Unforgeability: Only the designated proxy signer can create the proxy blind signature.
Unlinkability: When the signature is revealed, the proxy signer cannot identify the association between the message and the blind signature he generated.

Later, Lal and Awasthi (2003) pointed out that Tan et al.'s proxy blind signature schemes suffer from a kind of forgery attack due to the signature receiver. Compared with Tan et al.'s schemes, Lal and Awasthi further proposed a more efficient and secure proxy blind signature scheme to overcome the pointed out drawback in Tan et al.'s schemes. In this paper, we show that Tan et al.'s schemes do not satisfy the unforgeability and unlinkability properties. In addition, we also point out that Lal and Awasthi's scheme does not possess the unlinkability property either.

The rest of this paper is organized as follows: In Section 2, we give the notations used throughout this paper. In Section 3, we review both Tan et al's proxy blind signature schemes, DLP and ECDLP versions, and show that these two proxy blind signature schemes are insecure against the original signer, the recipient's forgery, and the general forgery. Moreover, we also point out that these two schemes do not achieve the unlinkability property. In Section 4, we review Lal and Awasthi's proxy blind signature scheme and point out its insecurity. Section 5 concludes this paper.

2. Notations

Let E be a set of points (x, y) in finite field F_{p} satisfying the cubic equation $y^2 = x^3 + ax + b \bmod p$, where $4a^3 + 27b^2 \neq 0$.

O	the original signer
P	the proxy signer
A	the signature asker (verifier)
p, q	two large prime numbers with $q \mid (p-1)$
g	an element of order q in Z_{p}^*
$h()$	a secure one-way hash function
x_u	the secret key of user u
y_u	the public key of user u, $y_u = g^{x_u} \bmod p$
B	$B \in E$, base point with large prime order q
Y_u	the public key of user u, $Y_u = x_u B$
$x(Q)$	the x coordinate of point Q
$A \to B$	A sends message to B

3. On the security of Tan et al.'s proxy blind signature schemes

In this section, we review Tan et al.'s two proxy blind signature schemes and give the cryptanalysis on them.

3.1. Proxy blind signature scheme based on DLP

We describe Tan et al.'s DLP-based proxy blind signature scheme in the following three phases.

3.1.1. Proxy delegation phase

The original signer O computes $r_o = g^{k_o} \bmod p$ and $s_o = x_o r_o + k_o \bmod q$, where k_o is a random number. Next, O sends (r_o, s_o) to the proxy signer P in a secure manner. P accepts (r_o, s_o) if the equation $g^{s_o} = y_o^{r_o} r_o \bmod p$ does hold. Finally, the proxy signer P computes the proxy secret key $s_{\mathrm{pr}} = s_o + x_{\mathrm{p}} \bmod q$. We depict the scenario as Fig. 1.

3.1.2. Signing phase

The proxy signer P computes $t = g^k \bmod p$, where k is a random number and sends (t, r_o) to the signature asker A. A computes $r = tg^b y_{\mathrm{p}}^{-a-b} (y_o^{r_o} r_o)^{-a} \bmod p$, $e = h(r \| m) \bmod q$, $u = (y_o^{r_o} r_o)^{-e+b} y_o^{-e} \bmod p$, and $e' = e - a - b \bmod q$ where a and b are random numbers. Next, A sends e' to P. P then computes $s' = e' s_{\mathrm{pr}} + k \bmod q$ and returns s' to A. Upon receiving s', A computes $s = s' + b \bmod q$. The signature of message m is (m, u, s, e). The scenario is given in Fig. 2.

$$\begin{array}{ll}
O \text{ computes:} & k_o \in_R Z_q^*, r_o = g^{k_o} \bmod p \\
 & s_o = x_o r_o + k_o \bmod q \\
O \to P & (r_o, s_o) \\
P \text{ checks:} & g^{s_o} \overset{?}{=} y_o^{r_o} r_o \bmod p \\
P \text{ computes:} & s_{pr} = s_o + x_p \bmod q
\end{array}$$

Fig. 1. Proxy delegation phase in Tan et al.'s DLP-based scheme.

$$\begin{array}{ll}
P \text{ computes:} & k \in_R Z_q^*, t = g^k \bmod p \\
P \to A & (t, r_o) \\
A \text{ computes:} & a, b \in_R Z_q^*, r = tg^b y_p^{-a-b} (y_o^{r_o} r_o)^{-a} \bmod p \\
 & e = h(r \| m) \bmod q \\
 & u = (y_o^{r_o} r_o)^{-e+b} y_o^{-e} \bmod p \\
 & e' = e - a - b \bmod q \\
A \to P & e' \\
P \text{ computes:} & s' = e' s_{pr} + k \bmod q \\
P \to A & s' \\
A \text{ computes:} & s = s' + b \bmod q
\end{array}$$

Fig. 2. Signing phase in Tan et al.'s DLP-based scheme.

3.1.3. Verification phase

The recipient of the signature can verify the proxy blind signature by checking whether $e \overset{?}{=} h(g^s y_{\mathrm{p}}^{-e} y_o^e u \bmod p \| m)$ holds. This is because:

$$\begin{aligned} g^s y_{\mathrm{p}}^{-e} y_o^e u \bmod p &= g^{e'(s_o+x_{\mathrm{p}})+k+b} y_{\mathrm{p}}^{-e} y_o^e u \bmod p \\ &= g^k g^b g^{s_o(e-a-b)} g^{x_{\mathrm{p}}(e-a-b)} y_{\mathrm{p}}^{-e} y_o^e u \bmod p \\ &= tg^b (y_o^{r_o} r_o)^{(e-a-b)} y_{\mathrm{p}}^{(e-a-b-e)} y_o^e u \bmod p \\ &= tg^b (y_o^{r_o} r_o)^{(e-b)} (y_o^{r_o} r_o)^{-a} y_{\mathrm{p}}^{-a-b} y_o^e u \bmod p \\ &= tg^b (y_o^{r_o} r_o)^{(e-b)} \\ &\quad \times (y_o^{r_o} r_o)^{-a} y_{\mathrm{p}}^{-a-b} y_o^e (y_o^{r_o} r_o)^{-e+b} y_o^{-e} \bmod p \\ &= tg^b (y_o^{r_o} r_o)^{-a} y_{\mathrm{p}}^{-a-b} \bmod p = r \end{aligned}$$

3.2. Cryptanalysis on Tan et al's DLP-based scheme

In this subsection, we demonstrate three kinds of forgery attacks on Tan et al.'s DLP-based scheme and point out its linkability.

3.2.1. The original signer's forgery

We show that the proposed proxy blind signature is insecure against the original signer's forgery. In order to forge a proxy blind signature, a dishonest original signer computes $r'_o = y_{\mathrm{p}}^{-1} g^v \bmod p$, where v is a random number. Thus, $s'_{\mathrm{pr}} = x_o r'_o + v \bmod q$ is a valid proxy signature signing key. This is because:

$$\begin{aligned} g^s y_{\mathrm{p}}^{-e} y_o^e u \bmod p &= g^{e' s'_{\mathrm{pr}}+k+b} y_{\mathrm{p}}^{-e} y_o^e u \bmod p \\ &= tg^b g^{e'(s'_{\mathrm{pr}}-x_{\mathrm{p}})} y_{\mathrm{p}}^{e'-e} y_o^e u \bmod p \\ &= tg^b (y_o^{r'_o} r'_o)^{(e-b)} (y_o^{r'_o} r'_o)^{-a} y_{\mathrm{p}}^{-a-b} y_o^e \\ &\quad \times ((y_o^{r'_o} r'_o)^{(-e+b)} y_o^{-e}) \bmod p \\ &= tg^b (y_o^{r'_o} r'_o)^{-a} y_{\mathrm{p}}^{-a-b} \bmod p = r \end{aligned}$$

3.2.2. The recipient's universal forgery

Here we show that the recipient can perform the universal forgery for any selected message after obtaining one valid signature. Assume that (m, u, s, e) is a valid signature and $(r = tg^b y_{\mathrm{p}}^{-a-b} (y_o^{r_o} r_o)^{-a}, a, b)$ are related parameters. Therefore, $(m', u' = (y_o^{r_o} r_o)^{-e+b} y_o^{-e_{\mathrm{f}}} y_{\mathrm{p}}^{-z},\ s, e_{\mathrm{f}} = h(r\|m'))$ is a valid signature for a selected message m', where $z = e - e_{\mathrm{f}}$. This is because:

$$\begin{aligned} g^s y_{\mathrm{p}}^{-e_{\mathrm{f}}} y_o^{e_{\mathrm{f}}} u' \bmod p &= g^{k+b+(s_o+x_{\mathrm{p}})e'} y_{\mathrm{p}}^{-e_{\mathrm{f}}} y_o^{e_{\mathrm{f}}} u' \bmod p \\ &= g^k g^b g^{(s_o+x_{\mathrm{p}})e'} y_{\mathrm{p}}^{-e_{\mathrm{f}}} y_o^{e_{\mathrm{f}}} u' \bmod p \\ &= tg^b g^{s_o(e-a-b)} g^{x_{\mathrm{p}}(e-a-b)} y_{\mathrm{p}}^{-e_{\mathrm{f}}} y_o^{e_{\mathrm{f}}} u' \bmod p \\ &= tg^b (y_o^{r_o} r_o)^{(e-a-b)} y_{\mathrm{p}}^{(e-a-b-e_{\mathrm{f}})} y_o^{e_{\mathrm{f}}} \\ &\quad \times ((y_o^{r_o} r_o)^{-e+b} y_o^{-e_{\mathrm{f}}} y_{\mathrm{p}}^{-z}) \bmod p \\ &= tg^b (y_o^{r_o} r_o)^{-a} y_{\mathrm{p}}^{(e_{\mathrm{f}}+z-a-b-e_{\mathrm{f}})} y_{\mathrm{p}}^{-z} \bmod p \\ &= tg^b (y_o^{r_o} r_o)^{-a} y_{\mathrm{p}}^{-a-b} \bmod p = r \end{aligned}$$

3.2.3. The general forgery

We further propose a general forgery attack in which anyone can generate a valid signature (m, u, s, e). To forge such a valid signature, an attacker first selects a random number r for a message m and computes $e = h(r\|m)$. Next, he selects a random number s and computes u satisfying $r = g^s y_{\mathrm{p}}^{-e} y_o^e u \bmod p$. Therefore, the computed (m, u, s, e) is a valid signature for the selected message m because (m, u, s, e) will pass the signature verification equation $e \overset{?}{=} h(g^s y_{\mathrm{p}}^{-e} y_o^e u \bmod p \| m)$.

3.2.4. On the linkability

For the proxy signer, in order to identify the relationship between the revealed message and the blind information, the proxy signer records all messages he owned, such as $t(s)$, $e'(s)$, and $s'(s)$. After a signature (m, u, s, e) is revealed, the proxy signer computes $b' = s - s'$, $a' = e - b' - e'$, and $r' = tg^{b'} y_{\mathrm{p}}^{-a'-b'}$ $(y_o^{r_o}$ $r_o)^{-a'} \bmod p$ for some $s' \in s'(s)$, $t \in t(s)$ and $e' \in e'(s)$. Finally, the proxy signer checks the equation $r' = g^s y_{\mathrm{p}}^{-e} y_o^e u \bmod p$. If the equation holds, the proxy signer knows that (t, e', s') is the related blind information corresponding to the revealed message m. Namely, the proxy blind signature does not satisfy the unlinkability property.

3.3. Proxy blind signature scheme based on ECDLP

We describe Tan et al.'s ECDLP-based proxy blind signature scheme in the following three phases.

3.3.1. Proxy delegation phase

The original signer O computes $R_o = k_o B$, $r_o = x(R_o)$ and $s_o = x_o r_o + k_o \bmod q$, where k_o is a random number. Next, O sends (r_o, R_o, s_o) to the proxy signer P in a secure manner. P accepts (r_o, R_o, s_o) if the equation $R_o = s_o B - r_o Y_o$ does hold. Finally, the proxy signer P computes the proxy secret key $s_{\mathrm{pr}} = s_o + x_{\mathrm{p}} \bmod q$. We depict the scenario as Fig. 3.

O computes:	$k_o \in_R Z_q^*, R_o = k_o B, r_o = x(R_o)$
	$s_o = x_o r_o + k_o \bmod q$
$O \rightarrow P$	(r_o, R_o, s_o)
P checks:	$R_o = s_o B - r_o Y_o$
P computes:	$s_{pr} = s_o + x_p \bmod q$

Fig. 3. Proxy delegation phase in Tan et al.'s ECDLP-based scheme.

3.3.2. Signing phase

The proxy signer P computes $T = kB$, where k is a random number and sends it to the asker A. A computes $L = T + bB + (-a - b)Y_{\mathrm{p}} - aR_o - (ar_o)Y_o$, $r = x(L)$, $e = h(r\|m) \bmod q$, $U = (-e + b)R_o + (-e+ b)r_o Y_o - eY_o$, and

$$\begin{array}{ll} P \text{ computes:} & k \in_R Z_q^*, T = kB \\ P \to A & T \\ A \text{ computes:} & a, b \in_R Z_q^*, L = T + bB + (-a-b)Y_p - aR_o - (ar_o)Y_o \\ & r = x(L),\ e = h(r||m) \bmod q, \\ & U = (-e+b)R_o + (-e+b)r_oY_o - eY_o \\ & e' = e - a - b \bmod q \\ A \to P & e' \\ P \text{ computes:} & s' = e's_{pr} + k \bmod q \\ P \to A & s' \\ A \text{ computes:} & s = s' + b \bmod q \end{array}$$

Fig. 4. Signing phase in Tan et al.'s ECDLP-based scheme.

$e' = e - a - b \bmod q$ where a and b are random numbers. Next, A sends e' to P. P then computes $s' = e's_{\rm pr} + k \bmod q$ and returns s' to A. Upon receiving s', A computes $s = s' + b \bmod q$. The signature of message m is (m, U, s, e). The scenario is given in Fig. 4.

3.3.3. Verification phase

The recipient of the signature can verify the proxy blind signature by checking whether $e \overset{?}{=} h(x(sB - eY_{\rm p} + eY_o + U)\|m)$ holds.

3.4. Cryptanalysis on Tan et al's ECDLP-based scheme

In this subsection, we demonstrate three kinds of forgery attacks on Tan et al.'s ECDLP-based scheme and point out its linkability.

3.4.1. The original signer's forgery

To forge a proxy blind signature, the original signer selects point $R_o' = -Y_{\rm p} + vB$, where v is a random number, and computes $r_o' = x(R_o')$. Therefore, the original signer can obtain a valid proxy signing key $s_{\rm pr}' = x_o r_o' + v \bmod q$. This is because, according to the scheme, the proxy public key is $r_o'Y_o + R_o' + Y_{\rm p} = r_o'Y_o + vB$ which is the corresponding public key of $s_{\rm pr}'$.

3.4.2. The recipient's universal forgery

Assume that (m, U, s, e) is a valid signature and $(r = x(L), a, b)$ are related parameters. Therefore, $(m', U' = (-e+b)R_o + (-e+b)r_oY_o - e_{\rm f}Y_o - zY_{\rm p}, s, e_{\rm f} = h(r\|m'))$ is a valid signature for a selected message m', where $z = e - e_{\rm f}$. We omit the derivation here since it is similar to the recipient's universal forgery in the DLP-version.

3.4.3. The general forgery

The general forgery attack is still workable in the ECDLP-version. To forge a valid signature, an attacker first selects a point R for a message m and computes $e = h(x(R)\|m)$. Next, he selects a random number s and computes U satisfying $R = sB - eY_{\rm p} + eY_o + U$. Therefore, the computed (m, U, s, e) is a valid signature for the selected message m because (m, U, s, e) will pass the signature verification equation $e \overset{?}{=} h(x(sB - eY_{\rm p} + eY_o + U)\|m)$.

3.4.4. On the linkability

Similarly, the proxy signer can perform the similar steps as mentioned in Section 3.2.4 to identify the relationship between the revealed message and the blind information.

4. On the security of Lal and Awasthi's scheme

Lal and Awasthi proposed a proxy blind signature scheme with two modes: unprotected mode and protected mode. We review their proxy blind signature scheme as follows.

4.1. Lal and Awasthi's proxy blind signature scheme

4.1.1. Proxy delegation phase

The original signer O computes $r_o = g^{k_o} \bmod p$ and $s_o = x_o + k_o r_o \bmod q$, where k_o is a random number. Next, O sends (r_o, s_o) to the proxy signer P in a secure manner. P accepts (r_o, s_o) if the equation $g^{s_o} = y_o r_o^{r_o} \bmod p$ does hold. For unprotected mode, the proxy signer uses s_o as the proxy signature signing key. For the protected mode, the proxy signer P computes the proxy signature signing key $s_{\rm pr} = s_o + x_{\rm pr} \bmod q$. The original signer publishes the proxy public key $y_{\rm pr} = y_o r_o^{r_o} y_{\rm p} \bmod p$ or $y_{\rm pr} = y_o r_o^{r_o} \bmod p$ for unprotected or protected mode respectively. We depict the scenario as Fig. 5.

$$\begin{array}{ll}
O \text{ computes:} & k_o \in_R Z_q^*, r_o = g^{k_o} \bmod p \\
 & s_o = x_o + k_o r_o \bmod q \\
O \rightarrow P & (r_o, s_o) \\
P \text{ checks:} & g^{s_o} \overset{?}{=} y_o r_o^{r_o} \bmod p \\
P \text{ computes:} & s_{pr} = s_o + x_p \bmod q \text{ (protected)} \\
 & \text{or } (s_{pr} = s_o \bmod q) \text{ (unprotected)}
\end{array}$$

Fig. 5. Proxy delegation phase in Lal and Awasthi's scheme.

4.1.2. Signing phase

The proxy signer P computes $t = g^k \bmod p$, where k is a random number and sends t to the asker A. A computes $r = tg^{-a}y_{\mathrm{p}}^{-b} \bmod p$, $e' = h(r\|m) \bmod q$, and $e = e' + b \bmod q$ where a and b are random numbers. Next, A sends e to P. P then computes $s' = k - es_{\mathrm{pr}} \bmod q$ and returns s' to A. Upon receiving s', A computes $s = s' - a \bmod q$. The signature of message m is (m, s, e'). The scenario is given in Fig. 6.

4.1.3. Verification phase

The recipient of the signature can verify the proxy blind signature by checking whether $e' \overset{?}{=} h(g^s y_{\mathrm{pr}}^{e'} \bmod p\|m)$ holds. This is because:

$$g^s y_{\mathrm{pr}}^{e'} \bmod p = g^{k-es_{\mathrm{pr}}-a} g^{s_{\mathrm{pr}}(e-b)} \bmod p = g^{k-a-s_{\mathrm{pr}}b} \bmod p$$
$$= tg^{-a} y_{\mathrm{pr}}^{b} \bmod p = r$$

4.2. Cryptanalysis on Lal and Awasthi's scheme

Considering the original signer's forgery for Lal and Awasthi's scheme, a malicious original signer cannot perform the similar steps for Tan et al.'s schemes. This is because s_o computed in Lal and Awasthi's scheme is $s_o = x_o + k_o r_o \bmod q$, while not $s_o = x_o k_o + r_o \bmod q$. It is hard to find a r'_o such that $(r'_o)^{r'_o} = y_{\mathrm{p}}^{-1} \bmod p$. In terms of the recipient's forgery, the weakness of Tan et al.'s scheme is that u is not fresh and can be forged. However, the u does not appear in Lal and Awasthi's scheme. Therefore, the recipient's forgery are not applicable to their scheme.

$$\begin{array}{ll}
P \text{ computes:} & k \in_R Z_q^*, t = g^k \bmod p \\
P \rightarrow A & t \\
A \text{ computes:} & a, b \in_R Z_q^*, r = tg^{-a} y_{pr}^{-b} \bmod p \\
 & e' = h(r\|m) \bmod q \\
 & e = e' + b \bmod q \\
A \rightarrow P & e \\
P \text{ computes:} & s' = k - es_{pr} \bmod q \\
P \rightarrow A & s' \\
A \text{ computes:} & s = s' - a \bmod q
\end{array}$$

Fig. 6. Signing phase in Lal and Awasthi's scheme.

Although the original signer and recipient's forgery were removed from Lal and Awasthi's scheme, we still point out that Lal and Awasthi's scheme has the following weaknesses.

4.2.1. On the linkability

For the proxy signer, in order to identify the relationship between the revealed message and the blind information, the proxy signer records all messages he owned, such as $t(s)$, $e(s)$, and $s'(s)$. After a signature (m, s, e') is revealed, the proxy signer computes $a' = s' - s$, $b' = e - e'$, and $r' = tg^{-a'}y_{\mathrm{p}}^{-b'} \bmod p$ for some $s' \in s'(s)$, $t \in t(s)$, and $e \in e(s)$. Finally, the proxy signer checks the equation $r' = g^s y_{\mathrm{pr}}^{e'} \bmod p$. If the equation holds, the proxy signer knows that (t, e, s') is the related blind information corresponding to the revealed message m. Namely, Lal and Awasthi's proxy blind signature does not achieve the unlinkability property.

4.2.2. On the publishing of proxy public key

As we mentioned before, a proxy blind signature scheme can be divided into three phases: proxy delegation, signing, and verification. For practical consideration, via a successfully proxy delegation, a proxy signer can sign messages many times on behalf of the original signer. The proxy signer need not to perform the proxy delegation procedure for each signing. In general, in order to verify a proxy signature, the proxy public key is obtained by computing, while not retrieving from original signer's publishing. The computed proxy public key has the meaning of confirming the relationship between a original signer and a proxy signer. In Lal and Awasthi's scheme, such a publishing enables an adversary who obtained the proxy public key to republish it again. Finally, the adversary claims that he is the original signer. Therefore, the publishing of proxy public key suffers from the security flaw that the original signer is unable to be authenticated exactly.

The intuitive notion to solve the security flaw is to include the warrant in the signature scheme. For example, the proxy signer computes $s_{\mathrm{pr}} = s_o + x_{\mathrm{p}}h(w)$ in proxy delegation phase, where w is the warrant that describes original signer's identity and related information. On the other hand, the original signer signs the proxy public key $y_{\mathrm{pr}} = y_o r_o^{r_o} y_{\mathrm{p}}^{h(w)} \bmod p$ and w, and publishes y_{pr}, w, and the signature. Therefore, an adversary cannot republish the proxy public key again because the signed fake proxy public key $y'_{\mathrm{pr}} = y_o r_o^{r_o} y_{\mathrm{p}}^{h(w')}$ and w' cannot be used to verify the proxy signature. This method ensures the authenticity of proxy public key y_{pr}

but takes 1 or 2 exponential cost, depending on the employed signature algorithm of y_{pr}, in order to verify the signature of y_{pr}. Alternatively, a verifier should compute the $y_{\mathrm{pr}} = y_o r_o^{r_o} y_{\mathrm{p}} \bmod p$ or $y_{\mathrm{pr}} = y_o r_o^{r_o} \bmod p$ for protected or unprotected version while verifying the signature. It takes two multiplication and one exponential for protected version; and one multiplication and one exponential for unprotected version.

5. Conclusions

In this paper, we have reviewed Tan et al.'s proxy blind signature schemes based on DLP and ECDLP, and Lal and Awasthi's proxy blind signature scheme. We have shown that their schemes are insecure against some attacks and do not possess the unlinkability property which is an essential security requirement for a proxy blind signature scheme.

In terms of solving the security flaws in Lal and Awasthi's scheme, our suggestion is to employ a secure proxy key issuing protocol and a secure blind signature scheme. Through a secure proxy key issuing protocol, a proxy signer obtains a secure proxy secret key which can be used to generate a blind signature in the employed secure blind signature scheme.

Acknowledgement

This work was supported in part by the National Science Council, Taiwan, under contract NSC-92-2213-E-007-099.

References

Chaum, D., 1983. Blind signatures for untraceable payments. In: Crypto'82. Plenum Press, New York, pp. 199–203.

Kim, S., Park, S., Won, D., 1997. Proxy signatures, revisited. In: Proceedings of ICICS'97, International Conference on Information and Communications Security Lecture Notes on Computer Science, 1334. Springer-Verlag, pp. 223–232.

Kotzanikolaous, P., Burmcster, M., Chrisskopoulos, V., 2000. Secure transactions with mobile agents in hostile environments. In: Proceedings of ACISP, Lecture Notes on Computer Science, 1841. pp. 289–297.

Lal, S., Awasthi, A. K., 2003. Proxy Blind Signature Scheme, Cryptology ePrint Archive, Report 2003/072. Available from <http://eprint.iacr.org/>.

Lee, B., Kim, H., Kim, K., 2001. Secure mobile agent using strong non-designated proxy signature. In: Proceedings of ACISP Lecture Notes on Computer Science, 2119. Springer-Verlag, pp. 474–486.

Mambo, M., Usuda, K., Okamoto, E., 1996a. Proxy signature: delegation of the power to sign messages. IEICE Trans. Fundam. E79-A:9, 1338–1353.

Mambo, M., Usuda, K., Okamoto, E., 1996b. Proxy signatures for delegating signing operation. In: Proceedings of 3rd ACM Conference on Computer and Communications Security, New Delhi, India. ACM Press, New York, pp. 48–57.

Park, H.-U., Lee, I.-Y., 2001. A digital nominative proxy signature scheme for mobile communication. In: ICICS 2001. Lecture Notes on Computer Science, 2229. pp. 451–455.

Petersen, H., Horster, P., 1997. Self-certified keys—concepts and applications. In: Proceedings of Communications and Multimedia Security'97. Chapman & Hall, Athens, pp. 102–116.

Sander, T., Tschudin, C., 1997. Towards mobile cryptography. Technical Report 97-409, International Computer Science Institute, Berkeley.

Tan, Z., Liu, Z., Tang, C., 2002. Digital proxy blind signature schemes based on DLP and ECDLP. MM Research Preprints, No. 21, MMRC, AMSS, Academia, Sinica, Beijing. pp. 212–217.

Zhang, K., 1997. Threshold proxy signature schemes. Information Security Workshop. pp. 191–197.