Available online at www.sciencedirect.com
SCIENCE DIRECT®
The Journal of Systems and Software 79 (2006) 176–179
The Journal of Systems and Software
www.elsevier.com/locate/jss

Analysis of Sun et al.'s linkability attack on some proxy blind signature schemes

Lin-Chuan Wu [a,*], Yi-Shiung Yeh [a], Tsann-Shyong Liu [b]

[a] Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu 300, Taiwan, ROC
[b] Telecommunication Laboratories, Chunghwa Telecom Co., Ltd., 12 Lane 551, Min-Tsu Road Sec. 5, Yang-Mei, Taoyuan 326, Taiwan, ROC

Received 5 February 2005; received in revised form 10 May 2005; accepted 10 May 2005
Available online 29 June 2005

Abstract

The proxy blind signature scheme allows the designated proxy signer using the proxy secret key to generate a blind signature on behalf of the original signer. Tan et al. presented the DLP-based and ECDLP based blind signature schemes. Awasthi and Lal proposed a improved DLP-based scheme later. Recently, Sun et al. presented linkability attack on Tan et al.'s and Awasthi–Lal's proxy blind signature schemes respectively. In this paper, we show that Sun et al.'s attack is failed and these schemes are still satisfy the unlinkability property.

Keywords: Unlinkability; Blind signature; Proxy signature; Digital signature; Cryptography

1. Introduction

The blind signature scheme was first proposed by Chaum (1983) in Crypto'83. The security of Chaum's scheme is based on the difficulty of integer factoring. The blind signature scheme can achieve the unforgeability property for the signer and the unlinkability for the receiver. Mambo et al. (1996) presented the proxy signature scheme to allow the designated proxy signer to sign messages on behalf of the original signer. For example, when a manager is going on a vacation, (s)he can delegate her/his secretary to sign messages on behalf of her/him. Tan et al. (2002) presented two proxy blind signature schemes to allow the proxy signer to generate a blind signature on behalf of the original signer. Awasthi and Lal (2005) showed a forgery attack on Tan et al.'s schemes and proposed a more secure proxy blind signature scheme later. Recently, Sun et al. (2005) pointed out that neither Tan et al.'s schemes nor Awasthi–Lal's scheme satisfy the unlinkability property of the proxy blind signature scheme. In this paper, we show that Sun et al.'s linkability attack is failed and these schemes are still satisfy the unlinkability property.

2. Reviews of Tan et al.'s and Awasthi–Lal's proxy blind signature schemes

The system parameters in the following proxy blind signature schemes are defined as follows:

System parameters

p, q	two large prime numbers, where $q\|(p-1)$
g	element of Z_p^* of order q
x_o, y_o	secret key and public key of the original signer respectively, where $y_o = g^{x_o} \bmod p$
x_p, y_p	secret key and public key of the proxy signer respectively, where $y_p = g^{x_p} \bmod p$
$h(\,)$	a secure and public one way hash function
$\|$	the concatenation of strings

* Corresponding author. Tel.: +886 3 4244151; fax: +886 3 4244147.
E-mail address: wulc@csie.nctu.edu.tw (L.-C. Wu).

0164-1212/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2005.05.007

2.1. Tan et al.'s proxy blind signature schemes

Tan et al. (2002) presented two proxy blind signature schemes based on the discrete logarithm problem (DLP) and elliptic curve discrete logarithm problem (ECDLP) in 2002. They also defined the required security properties of proxy blind signature scheme. There are three kinds of participants: original signer, the proxy signer and the receiver in their schemes. The three phases in their schemes are (1) Proxy delegation, (2) Signing and (3) Verification. The details of Tan et al.'s DLP-based scheme are described as follows.

(1) *Proxy delegation phase*. The original signer randomly selects a number k_o, and calculates $r_o = g^{k_o} \bmod p$ and $s_o = k_o + x_o r_o \bmod q$. Then, the original signer sends (r_o, s_o) to the proxy signer in a secure way. After the proxy signer receives it, (s)he can verify it by checking the correctness of the equation $g^{s_o} = y_o^{r_o} r_o \bmod p$. Finally, the proxy signer computes her/his proxy secret key $s_{pr} = s_o + x_p \bmod q$.

(2) *Signing phase.* The proxy signer chooses a random number k, computes $t = g^k \bmod p$ and sends (r_o, t) to the receiver. After receiving it, the receiver randomly chooses two numbers a and b and calculates $r = tg^b y_p^{-a-b}(y_o^{r_o} r_o)^{-a} \bmod p$, $e = h(r \| m) \bmod q$, $u = (y_o^{r_o} r_o)^{-e+b} y_o^{-e} \bmod p$ and $e' = (e - a - b) \bmod q$. Then, the receiver sends e' to the proxy signer. Next, the proxy signer calculates the blinded signature $s' = e' s_{pr} + k \bmod q$ and sends s' back to the receiver. Finally, the receiver computes $s = s' + b \bmod q$. The signature of the message m is (m, u, s, e).

(3) *Verification phase.* Anyone can verify the correctness of the proxy blind signature (m, u, s, e) by checking that $e = h(g^s y_p^{-e} y_o^e u \bmod p \| m) \bmod q$ holds. The descriptions of Tan et al.'s ECDLP-based proxy blind signature scheme is omitted here because it is similar to DLP-based scheme except to replace discrete logarithm cryptosystem parameters by elliptic curve cryptosystem parameters.

2.2. Awasthi and Lal's proxy blind signature scheme

Awasthi and Lal (2005) showed a forgery attack on Tan et al.'s schemes and proposed a more secure and efficient proxy blind signature scheme later. Proxy-unprotected and proxy-protected are two kinds of schemes according to whether the original signer can generate the same proxy signature as the proxy signer. In proxy-protected schemes, the proxy signer and the original signer both can generate valid proxy signatures. Only the proxy signer can generate valid proxy signatures that (s)he cannot repudiate it later in proxy-protected schemes. The participants, phases and system parameters are the same as Tan et al.'s schemes. The detailed scheme is described in the following.

(1) *Proxy delegation phase.* The original signer chooses a random number k_o, and computes $r_o = g^{k_o} \bmod p$ and $s_o = x_o + k_o r_o \bmod q$. Next, the original signer sends (r_o, s_o) to the proxy signer via a secure channel. After the proxy signer receives it, (s)he can verify it by checking whether the equation $g^{s_o} = y_o r_o^{r_o} \bmod p$ holds. In proxy-unprotected case, the proxy signer uses $s_{pr} = s_o$ as her/his proxy secret key and $y_{pr} = y_o r_o^{r_o} \bmod p$ as her/his proxy public key. In proxy-protected case, the proxy signer computes $s_{pr} = s_o + x_{pr} \bmod q$ as her/his proxy secret key and $y_{pr} = y_o r_o^{r_o} y_p \bmod p$ as her/his proxy public key. (Note that the proxy public keys in Sun et al.'s paper must be exchanged each other in proxy-unprotected and proxy-protected cases.)

(2) *Signing phase.* The proxy signer randomly chooses a number k and computes $t = g^k \bmod p$ and sends (r_o, t) to the receiver. After receiving it, the receiver selects two random numbers a and b. Then (s)he calculates $r = tg^{-a} y_{pr}^{-b} \bmod p$, $e' = h(r \| m) \bmod q$, and $e = (e' + b) \bmod q$. The receiver sends e to the proxy signer. Next, the proxy signer calculates the blinded signature $s' = k - e s_{pr} \bmod q$ and sends s' back to the receiver. Finally, the receiver computes $s = s' - a \bmod q$ from the blind signature s'. The signature of the message m is (m, s, e').

(3) *Verification phase.* Anyone can verify the correctness of the proxy blind signature (m, s, e') by checking whether $e' = h(g^s y_{pr}^{e'} \bmod p \| m) \bmod q$ holds.

3. Sun et al.'s linkability attack on some proxy blind signature schemes

In Sun et al.'s (2005) linkability attack, they pointed out that the proxy signer can record all blinded messages and use them to trace back the corresponding blind signatures. Hence, Sun et al. claimed that all Tan et al.'s schemes and Awasthi–Lal's scheme cannot satisfy the unlinkability property of the blind signature. The details of Sun et al.'s attack are described as follows.

3.1. Sun et al.'s attack on Tan et al.'s schemes

We only describe the detailed Sun et al.'s attack on Tan et al.'s DLP-based proxy blind signature scheme because Tan et al.'s ECDLP-based scheme is similar to it.

1. The proxy signer can keep all set of records (t_i, e'_i, s'_i) for each instance i in Tan et al.'s DLP-based scheme, where $t_i = g^{k_i} \bmod p$.
2. When the receiver reveals (m, u, s, e) to the public, the proxy signer can compute $b'_i = s - s'_i \bmod q$ for each instance i since $s = s' + b \bmod q$.
3. The proxy signer can calculate $a'_i = (e - b'_i - e'_i) \bmod q$ for each instance i since $e' = (e - a - b) \bmod q$.

4. Then the proxy signer can compute $r'_i = t_i g^{b'_i} y_p^{-a'_i - b'_i} \times (y_o^{r_o} r_o)^{-a'_i} \bmod p$ for each instance i since $r = tg^b y_p^{-a-b} (y_o^{r_o} r_o)^{-a} \bmod p$.
5. Finally, the proxy signer can check that $r'_i = g^s y_p^{-e} y_o^e u \bmod p$ holds. If it is true, the proxy signer can trace back the blind signature.

Hence, Sun et al. claimed that Tan et al.'s schemes cannot satisfy the unlinkability property of the blind signature.

3.2. Sun et al.'s attack on Awasthi–Lal's scheme

1. The proxy signer can keep all set of records $(t_i, e'_i, \tilde{s}_i)$ for each instance i, where $t_i = g^{k_i} \bmod p$.
2. After the receiver reveals (m, s, e) to the public, the proxy signer can calculate $a'_i = \tilde{s}_i - s \bmod q$ for each instance i since $s = \tilde{s} - a \bmod q$.
3. The proxy signer can calculate $b'_i = (e'_i - e) \bmod q$ for each instance i since $e' = (e + b) \bmod q$.
4. The proxy signer then can compute $r'_i = t_i g^{-a'_i} y_{pr}^{-b'_i} \bmod p$ for each instance i since $r = tg^{-a} y_{pr}^{-b} \bmod p$.
5. Finally, the proxy signer can check whether $r'_i = g^s y_{pr}^e \bmod p$ holds. If the equation is true, the proxy signer can trace back the blind signature.

Thus, Sun et al. claimed that Awasthi–Lal's scheme cannot satisfy the unlinkability property of the blind signature.

4. Analysis of Sun et al.'s linkability attack

Harn (1995) first pointed out that Camenisch et al.'s (1994) blind signature scheme is linkable. Hoster et al. (1995) showed that Harn's claim is incorrect later. Recently, Hwang et al. (2002, 2003a,b,c) presented several papers to claim that several blind signature schemes are linkable. Unfortunately many cryptanalysts (Wu and Yeh, 2005; Lee and Wu, 2004; Lee and Sun, 2003; Fan, 2003) have showed that Hwang et al.'s papers are all failed respectively. In this section, we show that Sun et al.'s linkability attack is failed and Tan et al.'s and Awasthi–Lal's proxy blind signature schemes are still unlinkable.

4.1. Analysis of Sun et al.'s linkability attack on Tan et al.'s schemes

According to Sun et al.'s linkability attack, the proxy signer can keep all set of records (t_i, e'_i, s'_i) for each instance i in Tan et al.'s DLP-based scheme. After the receiver reveals (m, u, s, e) to the public, the proxy signer can calculate $b'_i = s - s'_i \bmod q$ for each instance i. Next, (s)he can obtain $a'_i = (e - b'_i - e'_i) \bmod q$. Then the proxy signer can calculate $r'_i = t_i g^{b'_i} y_p^{-a'_i - b'_i} (y_o^{r_o} r_o)^{-a'_i} \bmod p$. Finally, the proxy signer can check whether the equation $r'_i = g^s y_p^{-e} y_o^e u \bmod p$ holds. However, we show that the equation is always true for each instance i in the following:

$$
\begin{aligned}
& t_i g^{b'_i} y_p^{-a'_i - b'_i} (y_o^{r_o} r_o)^{-a'_i} \bmod p \\
& \equiv t_i g^{s - s'_i} y_p^{-e + b'_i + e'_i + s'_i - s} (y_o^{r_o} r_o)^{b'_i + e'_i - e} \bmod p \\
& \equiv g^s (t_i g^{-s'_i}) y_p^{-e} (y_p^{b'_i + e'_i + s'_i - s}) (y_o^{r_o} r_o)^{b'_i + e'_i - e} \bmod p \\
& \equiv g^s (t_i g^{-s'_i}) y_p^{-e} (y_p^{s - s'_i + e'_i + s'_i - s}) (y_o^{r_o} r_o)^{b'_i + e'_i - e} \bmod p \\
& \equiv g^s (t_i g^{-s'_i}) y_p^{-e} (y_p^{e'_i}) (y_o^{r_o} r_o)^{b'_i + e'_i - e} \bmod p \\
& \equiv g^s (t_i g^{-s'_i}) y_p^{-e} (y_p^{e'_i}) (y_o^{r_o} r_o)^{b'_i - e} (y_o^{r_o} r_o)^{e'_i} \bmod p \\
& \equiv g^s (t_i g^{-s'_i}) y_p^{-e} (y_p^{e'_i}) (y_o^{r_o} r_o)^{b'_i - e} (y_o^{r_o} r_o)^{e'_i} (y_o^e y_o^{-e}) \bmod p \\
& \equiv (g^s y_p^{-e} y_o^e) (t_i g^{-s'_i} y_p^{e'_i}) (y_o^{r_o} r_o)^{b'_i - e} (y_o^{r_o} r_o)^{e'_i} (y_o^{-e}) \bmod p \\
& \equiv (g^s y_p^{-e} y_o^e) (g^{k_i} g^{-e'_i s_{pr} - k_i} y_p^{e'_i}) \\
& \quad \times (y_o^{r_o} r_o)^{b'_i - e} (y_o^{r_o} r_o)^{e'_i} (y_o^{-e}) \bmod p \\
& \equiv (g^s y_p^{-e} y_o^e) (g^{k_i - k_i} g^{-e'_i (s_o + x_p)} y_p^{e'_i}) \\
& \quad \times (y_o^{r_o} r_o)^{b'_i - e} (y_o^{r_o} r_o)^{e'_i} (y_o^{-e}) \bmod p \\
& \equiv (g^s y_p^{-e} y_o^e) (g^{-e'_i (s_o + x_p)} g^{e'_i x_p}) \\
& \quad \times (y_o^{r_o} r_o)^{b'_i - e} (y_o^{r_o} r_o)^{e'_i} (y_o^{-e}) \bmod p \\
& \equiv (g^s y_p^{-e} y_o^e) (g^{-e'_i s_o}) (y_o^{r_o} r_o)^{b'_i - e} (y_o^{r_o} r_o)^{e'_i} (y_o^{-e}) \bmod p \\
& \equiv (g^s y_p^{-e} y_o^e) (y_o^{r_o} r_o)^{-e'_i} (y_o^{r_o} r_o)^{e'_i} (y_o^{r_o} r_o)^{b'_i - e} (y_o^{-e}) \bmod p \\
& \equiv (g^s y_p^{-e} y_o^e) (y_o^{r_o} r_o)^{b'_i - e} (y_o^{-e}) \bmod p \\
& \equiv g^s y_p^{-e} y_o^e u \bmod p \\
& \equiv r'_i \bmod p
\end{aligned}
$$

For a given message-signature pair (a, c, s, m), the proxy signer can derive 3-tuple (b'_i, a'_i, r'_i) such that $r'_i = g^s y_p^{-e} y_o^e u \bmod p$ is always held for each (t_i, e'_i, s'_i). Hence, Sun et al.'s claim is incorrect and Tan et al.'s DLP-based scheme is still satisfy the unlinkability property. The analysis of Sun et al.'s linkability attack on Tan et al.'s ECDLP-based scheme is similar to above description.

4.2. Analysis of Sun et al.'s linkability attack on Awasthi–Lal's scheme

Based on Sun et al.'s linkability attack, the proxy signer can record all set of (t_i, e_i, s'_i) for each instance i in Awasthi–Lal's scheme. After the receiver reveals (m, s, e') to the public, the proxy signer can compute $a'_i = (s'_i - s) \bmod q$ for each instance i. Then (s)he can calculate $b'_i = (e_i - e') \bmod q$. Next, the proxy signer

can compute $r'_i = t_i g^{-a'_i} y_{pr}^{-b'_i} \bmod p$. Finally, the proxy signer can check if the equation $e' = h(g^s y_{pr}^{-e'} \times \bmod p \| m) \bmod q$ holds. We show that the equation is always true for each instance i in the following:

$$
\begin{aligned}
& h(t_i g^{-a'_i} y_{pr}^{-b'_i} \bmod p \| m) \bmod q \\
& \quad \equiv h(t_i g^{s-s'_i} y_{pr}^{e'-e_i} \bmod p \| m) \bmod q \\
& \quad \equiv h(g^s t_i g^{-s'_i} y_{pr}^{e'-e_i} \bmod p \| m) \bmod q \\
& \quad \equiv h(g^s t_i g^{e_i s_{pr} - k_i} y_{pr}^{e'-e_i} \bmod p \| m) \bmod q \\
& \quad \equiv h(g^s g^{k_i - k_i} g^{e_i s_{pr}} y_{pr}^{e'-e_i} \bmod p \| m) \bmod q \\
& \quad \equiv h(g^s g^{e_i s_{pr}} y_{pr}^{e'-e_i} \bmod p \| m) \bmod q \\
& \quad \equiv h(g^s y_{pr}^{e_i} y_{pr}^{e'-e_i} \bmod p \| m) \bmod q \\
& \quad \equiv h(g^s y_{pr}^{e'} \bmod p \| m) \bmod q \\
& \quad \equiv e'
\end{aligned}
$$

For a given message-signature pair (m, s, e'), the proxy signer can derive 3-tuple (b'_i, a'_i, r'_i) such that $e' = h(g^s y_{pr}^{-e'} \bmod p \| m) \bmod q$ is always held for each (t_i, e_i, s'_i). Hence, Sun et al.'s linkability attack is failed again on Awasthi–Lal's scheme. Awasthi–Lal's scheme is still satisfy the unlinkability property of the proxy blind signature scheme.

5. Conclusions

Recently, Sun et al. pointed out that Tan et al.'s schemes and Awasthi–Lal's scheme cannot satisfy the unlinkability property of the proxy blind signature scheme. In this paper, we show that Sun et al.'s linkability attack is failed and these schemes are still satisfy the unlinkability property.

Acknowledgement

This work was supported in part by the Bestwise International co.

References

Awasthi, A.K., Lal, S., 2005. Proxy blind signature scheme. Transaction on Cryptology 2 (1), 5–11. Available from: <http://eprint.iacr.org/2003/072.pdf>.

Camenisch, J.L., Piveteau, J.M., Stadler, M.A., 1994. Blind signatures based on the discrete logarithm problem. In: Advances in Cryptology—EUROCRYPT'94, Rump session, 1994, 5pp.

Chaum, D., 1983. Blind signature systems. In: Advances in Cryptology—CRYPTO'83. Plenum, p. 153.

Fan, C.I., 2003. Comments on Hwang–Lee–Lai attack upon Fan–Lee partially blind signature scheme. IEICE Trans. Fundam. E86-A (7), 1900–1901.

Harn, L., 1995. Cryptanalysis of the blind signatures based on the discrete logarithm problem. Electron. Lett. 31 (14), 1136.

Hoster, P., Michels, M., Petersen, H., 1995. Comment: cryptanalysis of the blind signatures based on the discrete logarithm problem. Electron. Lett. 31 (21), 1827.

Hwang, M.S., Lee, C.C., Lai, Y.C., 2002. Traceability on low-computation partially blind signatures for electronic cash. IEICE Trans. Fundam. E85-A (5), 1181–1182.

Hwang, M.S., Lee, C.C., Lai, Y.C., 2003a. Traceability on RSA-based partially signature with low computation. Appl. Math. Comput. 145 (2–3), 465–468.

Hwang, M.S., Lee, C.C., Lai, Y.C., 2003b. An untraceable blind signature scheme. IEICE Trans. Fundam. E86-A (7), 1902–1906.

Hwang, M.S., Lee, C.C., Lai, Y.C., 2003c. Traceability on Stadler et al.'s fair blind signature scheme. IEICE Trans. Fundam. E86-A (2), 513–514.

Lee, N.Y., Sun, M.K., 2003. Analysis on traceability on Stadler et al.'s fair blind signature. IEICE Trans. Fundam. E86-A (11), 2901–2902.

Lee, N.Y., Wu, C.N., 2004. Comment on traceability analysis on chaum blind signature. IEICE Trans. Fundam. E87-A (2), 511–512.

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

Sun, H.M., Hsieh, B.T., Tseng, S.M., 2005. On the security of some proxy blind signature scheme. J. Syst. Software 74, 297–302.

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

Wu, L.C., Yeh, Y.S., 2005. Comment on Traceability on RSA-based partially signature with low computation. Appl. Math. Comput., in press.