On the Security of Some Proxy Blind Signature Schemes

Hung-Min Sun **Bin-Tsan Hsieh**[†]

Department of Computer Science
National Tsing Hua University, Hsinchu, Taiwan 300
Email: hmsun@cs.nthu.edu.tw
[†]Department of Computer Science and Information Engineering
National Cheng Kung University, Tainan, Taiwan 701
Email: bintsan@csie.ncku.edu.tw

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 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: Proxy Signature, Elliptic Curve, Cryptanalysis, Cryptography

1 Introduction

The concept of blind signature scheme was first introduced by Chaum in 1983 (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, Usuda & Okamoto 1996)(Kim, Park & Won 1997)(Petersen and Horster 1997)(Mambo, Usuda & Okamoto 1996)(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, Burmcster & Chrisskopoulos 2000) and mobile agent environments (Park and Lee 2001)(Sander and Tschudin 1997)(Lee, Kim & Kim 2001). To categorize the delegation types, Mambo *et al.* (Mambo et al. 1996) 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. (Tan, Liu & Tang 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 can not deny their signatures against anyone.

Verifiability: The proxy blind signature can be verified by everyone.

Unforgeability: Only the designated proxy signer can create the proxy blind signature.

Unlinkability: When the signature is revealed, the proxy signer can not identify the association between the message and the blind signature he generated.

Later, Lal and Awasthi (Lal & 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 Tan et al's two proxy blind signature schemes and show their weakness. 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 $4a^3 + 27b^2 \neq 0$.

Copyright ©2004, Australian Computer Society, Inc. This paper appeared at Australasian Information Security Workshop(AISW2004), Dunedin, New Zealand. Conferences in Research and Practice in Information Technology, Vol. 32. James Hogan, Paul Montague, Martin Purvis and Chris Steketee, Ed. Reproduction for academic, not-for profit purposes permitted provided this text is included.

O	the original signer
P	the proxy signer
A	the signature asker (verifier)
p, q	two large prime numbers with $q\|(p-1)$
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 the proxy blind signature scheme based on DLP in 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 $s_{pr} = s_o + x_p \bmod q$. We depict the scenario as figure 1.

O 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 checks:	$g^{s_o} \stackrel{?}{=} y_o^{r_o} r_o \bmod p$
P computes:	$s_{pr} = s_o + x_p \bmod q$

Figure 1: Tan et al.'s Proxy Delegation

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 $r = tg^b y_p^{-a-b}(y_o^{r_o} r_o)^{-a} \bmod p$, $e = h(r||m) \bmod q$, $u = (y_o^{r_o} r_o)^{-e+b} y_o^{-e} \bmod q$, and $e' = e - a - b \bmod q$ where a and b are random numbers. Next, A sends e' to P. P then computes $s' = e' s_{pr} + k \bmod q$ 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 figure 2.

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

Figure 2: Tan et al.'s Signing

3.1.3 Verification Phase

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

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

3.2 Cryptanalysis

In this subsection, we demonstrate three attacks against the proxy blind signature scheme.

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 $r'_o = y_p^{-1} g^v \bmod p$, where v is a random number. Thus, $s'_{pr} = x_o r'_o + v \bmod q$ is a valid proxy signature signing key. This is because:

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

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 $(r = tg^b y_p^{-a-b}(y_o^{r_o} r_o)^{-a}, a, b)$ are related parameters. Therefore, $(m', u' = (y_o^{r_o} r_o)^{-e+b} y_o^{-e_f} y_p^{-z}, s, e_f = h(r||m'))$ is a valid signature for a selected message m', where $z = e - e_f$. This is because:

$$\begin{aligned}
& g^s y_p^{-e_f} y_o^{e_f} u' \bmod p \\
&= g^{k+b} g^{(s_o + x_p)e'} y_p^{-e_f} y_o^{e_f} u' \bmod p \\
&= tg^b g^{s_o(e-a-b)} y_p^{e'-e_f} y_o^{e_f} u' \bmod p \\
&= tg^b (y_o^{r_o} r_o)^{(e-b)} (y_o^{r_o} r_o)^{-a} y_p^{e'-e_f} y_o^{e_f} ((y_o^{r_o} r_o)^{-e+b} y_o^{-e_f} y_p^{-z}) \bmod p \\
&= tg^b (y_o^{r_o} r_o)^{-a} y_p^{e_f + z - a - b - e_f} y_p^{-z} \bmod p \\
&= tg^b (y_o^{r_o} r_o)^{-a} y_p^{-a-b} \bmod p \\
&= r
\end{aligned}$$

3.2.3 On the Unlinkability

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 $r' = g^s y_p^{-e} y_o^e u \bmod p$ for some $s' \in s'(s)$ and $e' \in e'(s)$. Finally, the proxy signer checks the equation $r' = tg^{b'} y_p^{-a'-b'} (y_o^{r_o} r_o)^{-a'} \bmod p$ for some $t \in t(s)$. If he finds a corresponding t such that $r' = tg^{b'} y_p^{-a'-b'} (y_o^{r_o} r_o)^{-a'} \bmod p$, 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 possess the unlinkability property.

3.3 Proxy Blind Signature Scheme Based on ECDLP

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 $s_{pr} = s_o + x_p \bmod q$. We depict the scenario as figure 3.

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

Figure 3: Tan et al.'s Proxy Delegation(ECDLP)

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 $L = T + bB + (-a - b)Y_p - aR_o - (ar_o)Y_o$, $r = x(L)$, $e = h(r||m) \bmod q$, $U = (-e+b)R_o + (-e+b)r_o Y_o - eY_o$, and $e' = e - a - b \bmod q$ where a and b are random numbers. Next, A sends e' to P. P then computes $s' = e' s_{pr} + k \bmod q$ 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 figure 4.

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

Figure 4: Tan et al.'s Signing(ECDLP)

3.3.3 Verification Phase

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

3.4 Cryptanalysis

3.4.1 The Original Signer's Forgery

To forge a proxy blind signature, the original signer selects point $R'_o = -Y_p + vB$, where v is a random number, and computes $r'_o = x(R'_o)$. Therefore, the original signer computes a valid proxy signing key $s'_{pr} = x_o r'_o + v \bmod q$. This is because, according to the scheme, the proxy public key is $r'_o Y_o + R'_o + Y_p = r'_o Y_o + vB$ which is the corresponding public key of s'_{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, $(m', U' = (-e + b)R_o + (-e + b)r_o Y_o - e_f Y_o - zY_p, s, e_f = h(r||m'))$ is a valid signature for a selected message m', where $z = e - e_f$. We omit the derivation here since it is similar to the forgery in DLP-version.

3.4.3 On the Unlinkability

Similarly, the proxy signer can perform the same steps as mentioned before to identify the relationship between the revealed message and the blind information.

4 On the Security of Lal and Awasthi's Scheme

4.1 Lal and Awasthi's Proxy Blind Signature

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. Finally, for protected delegation, the proxy signer P computes the proxy secret key $s_{pr} = s_o + x_p \bmod q$. Otherwise, the proxy signer uses s_o as the proxy secret key in unprotected delegation. The original signer publishes the proxy public key $y_{pr} = y_o r_o^{r_o} y_p \bmod p$ or $y_{pr} = y_o r_o^{r_o} \bmod p$ for protected or unprotected delegation respectively. We depict the scenario as figure 5.

O 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 checks:	$g^{s_o} \stackrel{?}{=} y_o r_o^{r_o} \bmod p$
P computes:	$s_{pr} = s_o + x_p \bmod q$
	or $(s_{pr} = s_o \bmod q)$

Figure 5: Lal and Awasthi's Proxy Delegation

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 $r = tg^{-a} y_p^{-b} \bmod p$, $e' = h(r||m) \bmod q$, and $e = e' + b \bmod q$ where a and b are random numbers. Next, A sends e to P. P then computes $s' = k - es_{pr} \bmod q$ 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 figure 6.

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

Figure 6: Lal and Awasthi's Signing

4.1.3 Verification Phase

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

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

4.2 Cryptanalysis and Remarks

4.2.1 On the Unlinkability

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 $r' = g^s y_{pr}^{e'} \bmod p$ for some $s' \in s'(s)$ and $e \in e(s)$. Finally, the proxy signer checks the equation $r' = tg^{-a'} y_p^{-b'} \bmod p$ for some $t \in t(s)$. If he find a corresponding t such that $r' = tg^{-a'} y_p^{-b'} \bmod p$, therefore, 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 possess the unlinkability property.

4.2.2 On the Publishing of Proxy Public Key

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.

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.

Acknowledgments

This work was supported in part by the National Science Council, Taiwan, under contract NSC-92-2213-E-007-098.

References

Chaum, D. (1983), Blind Signatures for untraceable payments, *in* 'Crypto '82, Plenum Press', New York, pp. 199–203.

Kotzanikolaous, P., Burmcster, M. & Chrisskopoulos, V. (2000), Secure transactions with mobile agents in hostile environments, *in* 'Proc. ACISP', LNCS 1841, pp. 289–297.

Kim, S., Park, S., and Won, D. (1997), Proxy signatures, revisited, *in* 'Proc. of ICICS'97, International Conference on Information and Communications Security', LNCS 1334, Springer-Verlag, pp. 223–232.

Lal, S. and Awasthi, A. K. (2003), 'Proxy Blind Signature Scheme', to appear in Journal of Information Science and Engineering. Cryptology ePrint Archive, Report 2003/072. Available at http://eprint.iacr.org/.

Lee, B., Kim, H. & Kim, K. (2001), Secure mobile agent using strong non-designated proxy signature, *in* 'Proc. of ACISP, LNCS 2119', Springer-Verlag, pp. 474–486.

Mambo, M., Usuda, K., and Okamoto, E., (1996), 'Proxy Signature: Delegation of the Power to Sign Messages',*IEICE Trans. Fundamentals*, E79-A:9, 1338–1353.

Mambo, M., Usuda, K. & Okamoto, E. (1996), Proxy signatures for delegating signing operation, *in* 'Proc. 3rd ACM Conference on Computer and Communications Security', New Dehli, India, ACM Press New York, pp. 48–57.

Petersen, H. and Horster, P. (1997), Self-certified keys - concepts and applications, *in* 'Proc. Communications and Multimedia Security'97', Athen, Chapman & Hall, pp. 102–116.

Park, H.-U. & Lee, I.-Y. (2001), A digital nominative proxy signature scheme for mobile communication, *in* 'ICICS 2001', LNCS 2229, pp. 451–455.

Sander, T. and Tschudin, C. (1997), Towards mobile cryptography, Tech. Rep., *in* 'Intl Computer Science Inst.', Berkeley, pp 97–409.

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

Zhang, K. (1997), Threshold proxy signature schemes, *in* 'Information Security Workshop', pp. 191–197.