Available online at www.sciencedirect.com
SCIENCE DIRECT®
The Journal of Systems and Software 74 (2005) 297–302
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
Available online 19 March 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.

* 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 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2004.02.015

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 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 $q\|(p-1)$
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 $s_{pr} = s_o + x_p \bmod q$. 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 $r = tg^b y_p^{-a-b}(y_o^{r_o} r_o)^{-a} \bmod p$, $e = h(r\|m) \bmod q$, $u = (y_o^{r_o} r_o)^{-e+b} y_o^{-e} \bmod p$, and $e' = e - a - b \bmod q$ where a and b are random numbers. Next, A sends e' to P. P then computes $s' = e' s_{pr} + k \bmod q$ 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.

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:	$s_{pr} = s_o + x_p \bmod q$

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

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

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