Cryptanalysis of Lee-Hwang-Yang Blind Signature Scheme

Chun-I Fan, D. J. Guan, Chih-I Wang and Dai-Rui Lin
Department of Computer Science and Engineering
National Sun Yat-sen University, Kaohsiung 804, Taiwan
{cifan, guan}@cse.nsysu.edu.tw

Abstract

In 2005, Lee et al. proposed a blind signature scheme based on the discrete-logarithm problem to achieve the untraceability or unlinkability property. However, the scheme will be demonstrated as not being secure in this manuscript. We design an attack on the scheme such that a signature requester can obtain more than one valid signatures by performing only one round of the protocol. It violates an important security requirement of blind signatures.

Keywords : Blind Signatures, Unlinkability, Untraceability, Security & Privacy, Cryptography

1 Introduction

In 1982, Chaum proposed the concept of blind signatures [1], which makes it information theoretically impossible for a signer to derive the link between a signature and the instance of the signing operation that produced the blinded form of the signature. This is usually referred to as the *unlinkability* or *untraceability* property. Due to the unlinkability property and the unforgeabilty of the signatures, blind signatures have been widely applied to untraceable electronic cash protocols [1][3] and anonymous electronic voting systems [4][8].

Recently, several blind signature schemes based on the discrete-logarithm problem have been proposed and discussed in [2][5][6][7]. In 1994, Carmenish et al. [2] introduced a blind signature scheme based on the discrete-logarithm problem. In 1995, Harn [5] pointed out that Carmenish et al.'s scheme cannot satisfy the requirement of untraceability. However, Horster et al. [6] claimed that Harn's cryptanalysis is not correct. Later, in 2005, Lee et al. [7] show that Horster et al.'s comment on Harn's attack [5] is wrong. Thus, they proposed an improved blind signature scheme in [7] to enhance the security of Carmenish et al.'s scheme for withstanding the attack introduced in [5].

In a secure blind signature scheme, it must be guaranteed that any signature requester can acquire at most w signatures if the requester performs w rounds of the protocol with the signer where w is a positive integer [1][3][4]. In this manuscript, we will show that there exists a security flaw in the scheme of [7] such that a signature requester can obtain two valid signatures by performing only one round of the protocol with the signer. It turns out that the scheme of [7] is insecure.

The rest of this paper is organized as follows. In the next section, we briefly review Lee-Hwang-Yang scheme of [7]. The proposed attack is presented in Section 3. Finally, a concluding remark is given in Section 4.

2 Review of Lee-Hwang-Yang Blind Signature Scheme

In this section, we briefly review the blind signature scheme proposed by Lee, Hwang, and Yang [7]. There are two kinds of roles in the scheme: a signer and a group of signature requesters, where signature requesters request signatures from the signer and the signer issues blind signatures to the requesters. The details of [7] are described as follows:

Initially, the signer chooses two large primes (p, q) and an integer g where $q|(p-1)$ and g is a generator with order q in Z_p^*. The signer selects an integer x as its secret key and computes $y = g^x \bmod p$. It publishes (p, q, g, y).

The signer randomly chooses $\widetilde{k_1}$, $\widetilde{k_2}$, b_1, $b_2 \in Z_q$ and computes $\widetilde{r_1} = g^{\widetilde{k_1}} \bmod p$ and $\widetilde{r_2} = g^{\widetilde{k_2}} \bmod p$ such that $GCD(\widetilde{r_1}, q) = GCD(\widetilde{r_2}, q) = 1$. Then, the signer sends $\widetilde{r_1}$, $\widetilde{r_2}$, b_1, b_2 to a requester. After receiving $(\widetilde{r_1}, \widetilde{r_2}, b_1, b_2)$ from the signer, the reque-

Signer		Requester
Randomly choose $\widetilde{k_1}$, $\widetilde{k_2}$, b_1, $b_2 \in Z_q$.		
$\widetilde{r_1} = g^{\widetilde{k_1}} \bmod p$, $\widetilde{r_2} = g^{\widetilde{k_2}} \bmod p$	$\xrightarrow{\widetilde{r_1}, \widetilde{r_2}, b_1, b_2}$	Randomly select (a, b, c, d, e).
		$r_1 = \widetilde{r_1}^{ab_1} g^c \bmod p$, $r_2 = \widetilde{r_2}^{bb_2} g^e \bmod p$, $r = (r_1 r_2)^d \bmod p$
$\widetilde{s_1} = x\widetilde{r_1} + \widetilde{k_1} b_1 \widetilde{m_1} \bmod q$	$\xleftarrow{\widetilde{m_1}, \widetilde{m_2}}$	$\widetilde{m_1} = m\widetilde{r_1}\frac{r^{-1}}{2}ad \bmod q$, $\widetilde{m_2} = m\widetilde{r_2}\frac{r^{-1}}{2}bd \bmod q$
$\widetilde{s_2} = x\widetilde{r_2} + \widetilde{k_2} b_2 \widetilde{m_2} \bmod q$	$\xrightarrow{\widetilde{s_1}, \widetilde{s_2}}$	$s_1 = \widetilde{s_1}\widetilde{r_1}^{-1}\frac{r}{2} + cdm \bmod q, s_2 = \widetilde{s_2}\widetilde{r_2}^{-1}\frac{r}{2} + edm \bmod q$
		$s = (s_1 + s_2) \bmod q$
		$g^s \overset{?}{\equiv} y^r r^m \pmod p$

Figure 1: Lee-Hwang-Yang blind signature scheme

ster randomly chooses five integers (a, b, c, d, e) and keeps them secret. The requester computes $r = (r_1 r_2)^d \bmod p$ where $r_1 = \widetilde{r_1}^{ab_1} g^c \bmod p$ and $r_2 = \widetilde{r_2}^{bb_2} g^e \bmod p$. Then the requester blinds a message m by computing $\widetilde{m_1} = m\widetilde{r_1}\frac{r^{-1}}{2}ad \bmod q$ and $\widetilde{m_2} = m\widetilde{r_2}\frac{r^{-1}}{2}bd \bmod q$, and submits $(\widetilde{m_1}, \widetilde{m_2})$ to the signer. After receiving $(\widetilde{m_1}, \widetilde{m_2})$, the signer computes the blind signature $\widetilde{s_1} = x\widetilde{r_1} + \widetilde{k_1} b_1 \widetilde{m_1} \bmod q$ and $\widetilde{s_2} = x\widetilde{r_2} + \widetilde{k_2} b_2 \widetilde{m_2} \bmod q$ and sends $(\widetilde{s_1}, \widetilde{s_2})$ to the requester. Finally, the requester unblinds the blind signature by computing $s_1 = \widetilde{s_1}\widetilde{r_1}^{-1}\frac{r}{2} + cdm \bmod q$ and $s_2 = \widetilde{s_2}\widetilde{r_2}^{-1}\frac{r}{2} + edm \bmod q$. The requester then computes $s = (s_1 + s_2) \bmod q$ and publishes the message-signature triple (m, r, s) to the public. One can verify the triple by checking whether $g^s \overset{?}{\equiv} y^r r^m \pmod p$ is true or not. The protocol is also illustrated in Figure 1.

3 An Attack on Lee et al.'s Blind Signature Scheme

In the protocol of Session 2, if the requester is dishonest, she/he can obtain two valid signatures on two distinct messages m_α and m_β, respectively, by performing once of the protocol with the signer. The proposed attack is described below.

Instead of computing $r_1 = \widetilde{r_1}^{ab_1} g^c \bmod p$, $r_2 = \widetilde{r_2}^{bb_2} g^e \bmod p$, and $r = (r_1 r_2)^d \bmod p$ in the scheme of Section 2, the requester computes $r_1 = (\widetilde{r_1}^{ab_1} g^c)^d \bmod p$ and $r_2 = (\widetilde{r_2}^{bb_2} g^e)^d \bmod p$ where she/he does not need to compute r in the attack. The requester then forms $\widetilde{m_1} = m_\alpha \widetilde{r_1} r_1^{-1} ad \bmod q$ and $\widetilde{m_2} = m_\beta \widetilde{r_2} r_2^{-1} bd \bmod q$, instead of $\widetilde{m_1} = m\widetilde{r_1}\frac{r^{-1}}{2}ad \bmod q$ and $\widetilde{m_2} = m\widetilde{r_2}\frac{r^{-1}}{2}bd \bmod q$ in the scheme of Section 2, and she/he submits $(\widetilde{m_1}, \widetilde{m_2})$ to the signer. Then, she/he receives $(\widetilde{s_1}, \widetilde{s_2})$ from the signer where $\widetilde{s_1} = x\widetilde{r_1} + \widetilde{k_1} b_1 \widetilde{m_1} \bmod q$ and $\widetilde{s_2} = x\widetilde{r_2} + \widetilde{k_2} b_2 \widetilde{m_2} \bmod q$, which is the same as that of the scheme in Section 2. Finally, the requester derives $s_1 = \widetilde{s_1}\widetilde{r_1}^{-1} r_1 + cdm_\alpha$ $s_1 = \widetilde{s_1}\widetilde{r_1}^{-1} r_1 + cdm_\alpha \bmod q$ and $s_2 = \widetilde{s_2}\widetilde{r_2}^{-1} r_2 + edm_\beta \bmod q$, instead of $s_1 = \widetilde{s_1}\widetilde{r_1}^{-1}\frac{r}{2} + cdm \bmod q$ and $s_2 = \widetilde{s_2}\widetilde{r_2}^{-1}\frac{r}{2} + edm \bmod q$ in the scheme of Section 2. Thus, the requester acquires two different message-signature triples (m_α, r_1, s_1) and (m_β, r_2, s_2) such that $g^{s_1} \equiv y^{r_1} r_1^{m_\alpha} \pmod p$ and $g^{s_2} \equiv y^{r_2} r_2^{m_\beta} \pmod p$ in the round of the protocol because that

$$\begin{aligned}
g^{s_1} &\equiv g^{\widetilde{s_1}\widetilde{r_1}^{-1} r_1 + cdm_\alpha} \\
&\equiv g^{(x\widetilde{r_1} + \widetilde{k_1} b_1 \widetilde{m_1})\widetilde{r_1}^{-1} r_1 + cdm_\alpha} \\
&\equiv g^{x\widetilde{r_1}\widetilde{r_1}^{-1} r_1 + \widetilde{k_1} b_1 \widetilde{m_1}\widetilde{r_1}^{-1} r_1 + cdm_\alpha} \\
&\equiv g^{xr_1 + \widetilde{k_1} b_1 m_\alpha \widetilde{r_1} r_1^{-1} ad\widetilde{r_1}^{-1} r_1 + cdm_\alpha} \\
&\equiv g^{xr_1 + \widetilde{k_1} b_1 m_\alpha ad + cdm_\alpha} \\
&\equiv g^{xr_1 + (\widetilde{k_1} b_1 ad + cd)m_\alpha} \\
&\equiv y^{r_1} g^{(\widetilde{k_1} ab_1 d + cd)m_\alpha} \\
&\equiv y^{r_1} r_1^{m_\alpha} \pmod p
\end{aligned}$$

and

$$\begin{aligned}
g^{s_2} &\equiv g^{\widetilde{s_2}\widetilde{r_2}^{-1} r_2 + edm_\beta} \\
&\equiv g^{(x\widetilde{r_2} + \widetilde{k_2} b_2 \widetilde{m_2})\widetilde{r_2}^{-1} r_2 + edm_\beta} \\
&\equiv g^{x\widetilde{r_2}\widetilde{r_2}^{-1} r_2 + \widetilde{k_2} b_2 \widetilde{m_2}\widetilde{r_2}^{-1} r_2 + edm_\beta} \\
&\equiv g^{xr_2 + \widetilde{k_2} b_2 m_\beta \widetilde{r_2} r_2^{-1} bd\widetilde{r_2}^{-1} r_2 + edm_\beta} \\
&\equiv g^{xr_2 + \widetilde{k_2} b_2 m_\beta bd + edm_\beta} \\
&\equiv g^{xr_2 + (\widetilde{k_2} b_2 bd + ed)m_\beta} \\
&\equiv y^{r_2} g^{(\widetilde{k_2} bb_2 d + ed)m_\beta} \\
&\equiv y^{r_2} r_2^{m_\beta} \pmod p.
\end{aligned}$$

4 Conclusions

In this manuscript we have demonstrated that Lee et al.'s blind signature scheme is not secure. Once we apply the scheme to an untraceable electronic cash system, a customer (i.e., a signature requester in Lee et al.'s scheme) can obtain two valid electronic coins (i.e., two valid signatures) after she/he performs a withdrawing procedure for one coin with the bank (i.e., the signer). It will result in loss of the bank. Similarly, if the scheme is utilized to construct an anonymous electronic voting system, a voter (i.e., a signature requester) can acquire two valid electronic votes (i.e., two valid signatures) such that the tally result of the voting is incorrect.

References

[1] D. Chaum, "Blind signatures for untraceable payments," Advances in Cryptology-CRYPTO'82, pp. 199-203, 1983.

[2] J. Carmenisch, J. Piveteau and M. Stadler, "Blind signatures based on the discrete logorithm problem," Advances in Cryptology-EUROCRYPT'94, pp. 428-432, 1994.

[3] C.I. Fan, "Ownership-attached unblinding of blind signatures for untraceable electronic cash," Information Sciences, vol. 176. no. 3, pp. 263-284, 2006.

[4] C.I. Fan and C.L. Lei, "An unlinkably divisible and intention attachable ticket scheme for runoff elections," Journal of Network and Computer Applications, vol. 25, no. 2, pp. 93-107, 2002.

[5] L. Harn, "Cryptanalysis of the blind signatures based on the discrete logarithm problem," Electronics Letters, vol. 31, no. 14, pp. 1136-1137, 1995.

[6] P. Horster, M. Michels and H. Petersen, "Comment: cryptanalysis of the blind signatures based on the discrete logarithm problem," Electronics Letters, vol. 31, no. 21, pp. 1827, 1995.

[7] C.C. Lee, M.S. Hwang and W.P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability," Applied Mathematics and Computation, vol. 164, no. 3, pp. 837-841, 2005.

[8] H. Nurmi, A. Salomaa and L. Santean, "Secret ballot elections in computer networks," Computers & Security, vol. 10, no. 6, pp. 553-560, 1991.