Cover

Cryptanalysis of B.Lee-S.Kim-K.Kim Proxy Signature

Zheng Dong , Shengli Liu & kefei Chen

Department of Computer Science and Engineering
Shanghai Jiaotong University
Shanghai 200030, China
{zheng-dong,liu-sl,chen-kf}@cs.sjtu.edu.cn

Abstract —— Due to the security requirements of proxy signature, in 2001, B.Lee et al. proposed a strong proxy signature scheme (Lee et al.'SPSS) based on Schnorr's scheme. One major characteristic of their scheme is to avoid misusing of a proxy key pair. However, this causes some security flaw. An attack is proposed to show that the Lee et al.'s scheme is not secure.

Keywords —— Cryptanalysis, Digital signature, Proxy signature

Cryptanalysis of B.Lee-S.Kim-K.Kim Proxy Signature

Zheng Dong , Shengli Liu & kefei Chen

Abstract: Due to the security requirements of proxy signature, in 2001, B.Lee et al. proposed a strong proxy signature scheme (Lee et al.'SPSS) based on Schnorr's scheme. One major characteristic of their scheme is to avoid misusing of a proxy key pair. However, this causes some security flaw. An attack is proposed to show that the Lee et al.'s scheme is not secure.

Keywords: Cryptanalysis, Digital signature, Proxy signature

Ingtroduction: In the network environment, the digital signatures play an important role. For example, in the electronic tax report, the reporter uses his digital signature to prove that the report was actually sent by him on Internet. In the digitalized world, the digital signatures have replaced the handwritten. Digital signature can provide the cryptographic services: authentication, data integrity, and non-repudiation. There are many proposed digital signature schemes [1,2,3].

Sometimes, we have the following scenarios: a person or a company that has the capability and the necessity of signing a document does not have enough time to do so. Or perhaps this person, A, is keen to delegate his signing capability to another person, B, so B would sign documents on behalf of A if A had some (technical, logistical) problem.

This is the scenario for a proxy signature scheme: a potential signer A delegates his signing capability to a proxy signer, B (in some way, A tells B what kind of messages B can sign), and B signs a message on behalf of the original signer, A. the receiver of the message verifies the signature of B and the delegation of A together.

Since the concept of proxy signature was introduced by Mambo et al.[4] in 1996, many proxy signature schemes were proposed [4,5,6,7], all of which are based on Schnorr's signaure scheme[3]

According to the undeniability property, the proxy signature schemes may be classified into two models: strong proxy signature and weak proxy signature [7].

- Strong proxy signature: it represents both original signer's and proxy signer's signatures. Once a proxy signer creates a valid proxy signature, he cannot repudiate his signature creation against anyone.
- Weak proxy signature: it represents only original signer's signature. It does not provide non-repudiation of proxy signer.

In this letter, a new attack is proposed on Lee et al.'s strong proxy signature scheme. In Section II, the brief review of Schnorr's scheme and Lee et al.'s strong proxy signature scheme are given. Then an attack on Lee et al' scheme is proposed in Section II. The section III is our conclusion.

Brief review of related schemes and our attack:

Schnorr's scheme

In [3], Schnorr introduced the following signature scheme.

Let p and q be large primes with $q|p$-1. Let g be a generator of a multiplicative subgroup of Z_p^* with order q, $H(\ )$ denotes a collision resistant hash function.

A signer **A** has a private key $x_A \in Z_q^*$ and the corresponding public key $y_A = g^{x_A}$. To sign a message M, **A** acts as follows:

1. Choose a random $k \in Z_q^*$
2. Compute $r = g^k \bmod p$ and $s = k + x_A H(M,r) \bmod q$
3. Define the signature on M to be the pair (r, s)

The signature is verified by checking that $g^s = ry_A^{H(M,r)}$

Lee et al.'s strong proxy signature scheme

The following proxy signature scheme has been introduced in [7]. It is based on the above schnorr's scheme.

Suppose original signer **A** have the key pair (x_A, y_A), with $y_A = g^{x_A}$, whereas the (future) proxy signer **B** also has his user key pair (x_B, y_B), with $y_B = g^{x_B}$

Generation of the proxy key: the original signer **A** uses Schnorr's scheme to sign warrant information, which should specify which messages **A** will allow the proxy to sign on his behalf.

That is, **A** chooses at random $k_A \in Z_q^*$, and computes $r_A = g^{k_A}$ and $s_A = k_A + x_A H(M_\omega, r_A) \bmod q$. Signer **A** sends $(M\omega, r_A, s_A)$ to a proxy signer **B** secretly. Then **B** verifies the validity of the Schnorr's signature:

$$g^{s_A} = r_A y_A^{H(M_\omega, r_A)}$$

If the verification is M_ω correct, **B** computes his proxy key pair (x_P, y_P) as

$$x_P = x_B + s_A, \ \ y_P = g^{x_P} (= y_B r_A y_A^{H(M_\omega, r_A)})$$

Proxy signature generation: in order to create a proxy signature on a message *M* conforming to the warrant information M_ω, proxy signer **B** uses Schnorr's signture scheme with keys (x_P, y_P) and obtains a signature (r_P, s_P) for the message *M*. The valid proxy signature will be the tuple (M, r_P, s_P, M_w, r_A)

Verification: A recipient can verify the validity of the proxy signature by checking that *M* conforms to M_ω and the verification equality of Schnorr's signature scheme with public key

$$y_P \ (= y_B r_A y_A^{H(M_\omega, r_A)}):$$

Accept the proxy signature if and only if $g^{s_P} = r_P (y_B r_A y_A^{H(M_\omega, r_A)})^{H(M, r_P)}$.

The authors claim that the scheme satisfy the security requirements [7]: *Strong unfordeability, verifiability, strong identifiability, strong undeniability and prevention of misuse*. In the following, an attack on the Lee et al.' s scheme is proposed.

Our attack: if the original signer **A** is dishonest, he can forge the signature of **B** on message *M* from a proxy signature:

After obtain the proxy signature (M, r_P, s_P, M_w, r_A), the original signer **A** may forge **B**'s signature on message *M* as following:

(1) Compute $s' = x_A H(M, r_P) \bmod q$

(2) Compute $s_B = s_P - s'$, and take $r_B = r_P$

(3) Then (r_B, s_B) and *M* satisfy the following verification equality of Schnorr's signature scheme with **B**'s public key y_B:

$$g^{s_B} = r_B y_B^{H(M, r_B)}$$

Suppose $r_B = r_p = g^{k_P}$, $s_P = k_P + x_P H(M, r_P)$ where k_P is a random number selected by

B for proxy signature on *M*. Then $s_B = s_P - s' = k_P + x_B H(M, r_B)$. It is obviously that (r_B, s_B) satisfy the verification equation of Schonrr's scheme.

In other words, (M, r_B, s_B) is the forged **B**'s signature on message *M*.

Note: J. Herranz et al.[8] claim that other signature schemes (ElGamal signature or DSS) can be used in the Lee et al.'s strong proxy signature scheme. Unfortunately, our attack does also work if DSS is used.

Conclusion:

For the new secure requirement in proxy signature scheme, Lee et al. briefly modify the proposal of [5] to strong proxy signature [7]. However, The strong proxy signature scheme has a security flaw. An attack is proposed to show that the original signature of **B** can be forged from a proxy signature.

Acknowledgment: This work was partially supported by NSFC under grants 90104005, 60173032 and 60273049.

References

1. T.ElGamal, "A public key cryptosystem and a signature scheme based on discrete ,"IEEE Trans. Inform. Theory, vol. IT-31, pp. 469-472, July 1985
2. L.Harn, "New digitral signature scheme based on discrete logarithm," Electron. Lett., vol, no. 5, pp. 296-298, Mar.1994.
3. C.P. Schnorr., "Efficient signature generation by smart cards. Journal of Cryptology," vol.4, pp161-174,1991.
4. M.Mambo, K.Usuda, and E.Okamoto: "Proxy signatures: Delegation of the power to sign messages." IEICE Trans., 1996, E79-A, (9), pp. 1338-1354.
5. S.Kim, S.Park, and D.Won: 'Proxy signatures, revisited', Proc. ICICS'97, Int. Conf. Information and Communications Security, 1997,(LNCS), Vol. 1334, pp.223-23
6. W B Lee, C Y Chang, Efficient proxy-protected proxy signature scheme based on discrete logarithm, Proceedings of 10th Conference on Information Security, Hualien, Taiwan, ROC, 2000, pp 4-7
7. B.Lee, H. Kim, and K. Kim. Strong proxy signature and its applications. The 2001 Symposium on Cryptography and Information Security

   (SCIS 2001) 2001.

Authors' affiliations:

Zheng Dong , Shengli Liu & Kefei Chen(Department of Computer Science and Engineering, Shanghai Jiaotong University, 1954 Hua Shan Road, Shanghai 200030, People's Republic of China)

Email: zheng-dong@cs.sjtu.edu.cn