对一个基于离散对数代理盲签名的密码分析*

王蜀洪[1+], 王贵林[2], 鲍 丰[2], 王 杰[1]

[1](北京大学 数学科学院,北京 1000871)

[2](Cryptography Research Lab, Institute for Infocomm Research, 119613, Singapore)

Cryptananlysis of a Proxy Blind Signature Scheme Based on DLP

WANG Shu-Hong[1+], WANG Gui-Lin[2], BAO Feng[2], WANG Jie[1]

[1](School of Mathematical Science, Peking University, 100871, China)

[2](Cryptography Research Lab, Institute for Infocomm Research, 119613, Singapore)

+ Corresponding author: Phn: +65-68748274, E-mail: wshong@math.pku.edu.cn

Received 2004-02-04; Accepted 2004-06-10

Wang SH, Wang GL, Bao F, Wang J. Cryptanalysis of a proxy blind signature scheme based on DLP. *Journal of Software*, 2005,16(5):911−915. DOI: 10.1360/jos160911

Abstract: Proxy signature allows an original signer to delegate his/her signing capability to a proxy signer such that the proxy signer can sign messages on behalf of the original signer. Blind signature allows a user to have a given message signed by the signer without revealing any information about the message. By using Schnorr blind signature, Tan *et al*. recently proposed a digital proxy blind signature scheme. They claimed that it satisfies the security properties of both blind signatures and proxy signatures. However, it is not the fact. This paper shows that the proposed scheme is vulnerable to universal forgery as well as linkability attacks. It also explains why their proofs of the security are incorrect.

Key words: proxy signature; blind signature; universal forgery; linkability; cryptananlysis

摘 要: 顾名思义,代理签名让原始签名者可以将其数字签名权力委托给代理签名者,使其能够代理原始签名者签发指定的数字消息;盲签名使用户能将给定的消息让别人签发,而又不泄漏任何有关的信息给签名者.在 Schnorr 盲签名的基础上,谭作文等结合代理签名和盲签名提出了一个基于离散对数的代理盲签名方案.研究表明该方案是不安全的.它既受到广泛伪造攻击,又是可连接的.我们还进一步说明,原文安全性定理的证明是不正确的.

关键词: 代理签名;盲签名;广泛伪造;可连接性;密码分析

中图法分类号: TP309 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant No.90104004 (国家自然科学基金)

WANG Shu-Hong was born in 1977. He is a Ph.D. candidate at the School of Mathematical Sciences, Peking University. His current research areas are protocol design and analysis in information security, network security and cryptography. **WANG Gui-Lin**, born in 1968, is a Ph.D. candidate and research scientist. His main research areas are foundation and application of cryptography. **BAO Feng** is a Principal Scientist and the Head of the Cryptography Lab of the Institute for Infocomm Research in Singapore. His research areas are algorithm, authomata theory, complexity, cryptography, distributed computing, fault tolerance, and information security. **WANG Jie** was born in 1956. He is a professor at the School of Mathematical Sciences, Peking University. His current research areas are group theory, algebraic graph theory and cryptology.

1 Introduction

Proxy signatures and blind signatures are regarded as two important types of digital signatures. Precisely, proxy signatures enable one party (Original signer) to delegate his/her signing capability to another party (Proxy signer) such that the proxy signer can sign messages on behalf of the original signer. Blind signatures enable one party (User) to have a message signed by another party (Signer) in such a way that the signer can not learn any information of the signed message. The concepts of proxy signature and blind signature were firstly introduced by Mambo[1] and Chaum[2], in 1996 and 1983 respectively. Since then, many of both types of signatures were proposed[3−6]. Some of them[4,5] are illustrated to be insecure[7,8] and some of them[6] are still under study.

Due to the urgent requirements of proxy signatures as well as blind signatures in today's electronic commerce (e.g., in e-cash system, coins must be signed blindly by the bank for the anonymity of users; but to withdraw a coin from a branch of the bank, proxy signature needed. For more details, please refer to Ref.[3]), proxy blind signatures inheriting the merits of both proxy and blind signatures have emerged. Since the first proxy blind signature proposed by Lin and Jan[9] in 2000, several new schemes were proposed based on different primitives[10−12]. Fox example, Tan *et al*.'s schemes[10,11] are based on discrete logarithm problems and Zhang *et al*.'s scheme are based on bilinear pairings.

In this paper, we have a cryptanalysis on Tan *et al*.'s proxy blind signature scheme[10]. We demonstrate two effective attacks on their proposed scheme. One is called universal forgery attack, and the other is called linkability attack. Both attacks are vital to a proxy blind signature scheme. We will discuss them at length later.

The rest of the paper is organized as follows. We describe the security requirement a proxy blind signature should satisfy in Section 2 and then briefly review Tan *et al*.'s proposed scheme in Section 3. In Section 4, we present the cryptanalysis on the scheme in detail. Finally, we conclude the paper in Section 5.

2 Security Requirements of Proxy Blind Signatures

Since proxy blind signatures are combination of the proxy signatures and the blind signatures, they should certainly have the security properties of the proxy signatures[5] and blind signatures:

(1) Distinguishability: Proxy blind signatures are distinguishable from normal signatures by everyone.

(2) Verifiability: From a proxy blind signature, the verifier can be convinced of the original signer's agreement on the signed message.

(3) Undeniability: Once a proxy signer creates a valid proxy blind signature of an original signer, he/she cannot repudiate the signature creation.

(4) Identifiability: Anyone can determine the identity of the corresponding proxy signer and original signer from the proxy blind signature.

(5) Unforgeability: A designated proxy blind signer can create a valid proxy blind signature. But the original signer and any other third parties who are not designated as a proxy signer cannot create a valid proxy blind signature.

(6) Unmisusability: The proxy signer can only sign authorized messages. He/she cannot sign messages that have not been authorized by the original signer.

(7) Unlinkability: After proxy blind signature is created, the proxy signer cannot associate it with his previous signing transcripts.

3 Review of the Proxy Blind Signature Scheme

In this section we briefly recall the proxy blind signature scheme proposed in Ref.[8].

3.1 System parameters

For readers, conveniency, we adopt the same notations as in Ref.[8].

- p,q : two large prime numbers, $q|p-1$.
- g : an element of Z_p^* , its order is q.
- $x_A, x_B \in Z_p^*$, the original signer A's and the proxy signer B's secret keys, respectively.
- $y_A \equiv g^{x_A} \pmod p$: A's public key.
- $y_B \equiv g^{x_B} \pmod p$: B's public key.
- $H(\cdot)$: a public cryptographically strong hash function.
- ||: the sign of concatenation of stings.

Note that numbers will be used as exponents are the computed modulo q, others are the computed modulo p. Hereafter we do not repeat them in equations below.

3.2 Proxy delegation phase

(a) *Commission Generation*. A randomly chooses $\bar{k} \in Z_q^*$ on the condition that there exists the inverse of $\bar{r}y_A^{\bar{r}} \pmod p$, where $\bar{r} = g^{\bar{k}} \pmod p$. Then A computes $\bar{s} = x_A\bar{r} + \bar{k}$.

(b) *Proxy delivery*. A sends the pair to proxy signer B via a secure channel.

(c) *Proxy verification*. B checks $g^{\bar{s}} = \bar{r}y_A^{\bar{r}}$. If it is correct, B accepts it and computes $s' = \bar{s} + x_B$ as his proxy signature secret key.

3.3 Blind signing phase

(a) B chooses a random number $k \in Z_q^*$, computes $t = g^k$ and then sends $(\bar{r}, t)$ to the user U.

(b) *Blinding*. To obtain the blind signature of m from proxy signer B, U chooses two random numbers $a,b \in Z_q^*$, and computes $r = tg^b y_B^{-a-b}(\bar{r}y_A^{\bar{r}})^{-a}$, $e = H(r \| m)$, $e^* = e - a - b$, and

$$u = (\bar{r}y_A^{\bar{r}})^{-e+b} y_A^{-e} \tag{1}$$

If $r = 0$, U selects a,b anew. Once r, a and b are determined, the user U delivers e^* to the proxy signer B.

(c) *Signning*. After reveiving , B computes

$$s'' = e^* s' + k \tag{2}$$

using the same k as in step (a), and sends it to U.

3.4 Extraction phase

Unblinding. While reveiving , U computes

$$s = b + s'' \tag{3}$$

And then, the proxy blind signature is

$$\sigma = (m, u, s, e) \tag{4}$$

3.5 Verification

The recipient of a proxy blind signature verifies the validity of σ by checking whether or not

$$e \overset{?}{=} H(g^s y_B^{-e} y_A^e u \| m) \tag{5}$$

He accepts it if it is true, otherwise rejects.

4 Cryptanalysis of the Proposed Scheme

In this section, we demonstrate two affective attacks on Tan *et al*'s proposed scheme to show its insecurity. In the first attack, anyone can forge a proxy blind signature on any message he chooses. And the second attack says that the proxy signer can later associate a signature with corresponding signing transcripts.

4.1 Universal forgery attack

Suppose an adversary wants to forge a valid proxy blind signature on message m he chooses arbitrarily, he performs as follows.

- Choose randomly $k, s \in Z_q^*$
- Compute $r = g^{k+s} \pmod p$ and $e = H(r \| m) \pmod q$
- Set $u = y_A^{-e} y_B^e g^k \pmod p$
- Output the proxy blind signature $\sigma = (m, u, s, e)$

To see the correctness of the forgery, one only needs to check Eq.(5). In fact it is obviously true, since

$$H(g^s y_B^{-e} y_A^e u \| m) = H(g^s y_B^{-e} y_A^e y_A^{-e} y_B^e g^k \| m) = H(g^s g^k \| m) = e .$$

4.2 Linkability attack

After knowing a proxy signature 4-tuple (m,u,s,e), the proxy signer B can find its corresponding signing transcripts $(\bar{r}, e^*, s'')$ by doing.

- Compute $b = s - s'' \pmod q$
- Check whether or not $u \stackrel{?}{=} (\bar{r} y_A^{\bar{r}})^{-e+b} y_A^{-e} \pmod p$

If it is true, he can link u to $\bar{r}$ successfully. Furthermore, B can figure out the random number a. Note that a and b are random numbers secretly chosen by the user, which should not be known to others in a blind signature scheme due to the blindness requirement.

4.3 On the failure of the proofs

4.3.1 Review of the theorems

Following theorems are presented in the original paper:

Theorem 2. The proxy signer can allege his own signature a proxy signature with a success probability $1/q$.

Theorem 3. Anyone else (even the original signer) can impersonate the proxy signer and forge the proxy signature with a probability $1/q$.

Theorem 4. When the protocol has been executed, the message sent to the signer is blind for the signer and the scheme achieves the unlinkability property.

4.3.2 Why the proofs fail

To prove Theorems 2 and 3, authors of Ref,[8] make an implicit assumption that forgers have to know the right proxy secret key s' which contains the participants' secret keys x_A and x_B, thus rely the hardness on the discrete logarithm. Indeed, as in our universal forgery attack, it is completely unnecessary. The forgers only need to know y_A and y_B which are publicly known.

The failure of proving Theorem 4 is absolutely due to careless. Although finding solution to Eq.(1) itself (the random number b) is an instance of the discrete logarithm problems, it is obvious that Eq.(3) exactly gives such an solution since s and s'' are both known to the signer B.

5 Conclusion

In this paper, we show that Tan *et al*'s proxy blind signature is insecure by mounting two kinds of attacks. The universal forgery attack shows that it does not satisfy the *unforgeability* requirement and the second attack shows that it does not satisfy the *unlinkability* requirement. The attacks tell us that security proofs do not guarantee all things and also should be treated strictly and carefully.

References:

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation. In: Proc. of the 3rd ACM Conf. on Computer and Communication Security. New Delhi: ACM Press, 1996. 48−57.

[2] Chaum D. Blind signature for untraceable payments. In: Proc. of the Crypto'82. New York: Springer-Verlag, 1983. 199−203.

[3] Brands S. Untraceable off-line cash in wallets with observers. In: Douglas RS, ed. Proc. of the Crypto'93. LNCS 773, New York: Springer-Verlag, 1994. 302−318.

[4] Chen TS, Liu TP, Chung YF. A proxy-protected proxy signature scheme based on elliptic curve cryptosystem. In: Proc. of the IEEE TENCOM'02. 2002. 184−187.

[5] Lee B, Kim H, Kim K. Strong proxy signature and its applications. In: Proc. of the 2001 Symp. Cryptography and Information Security (SCIS 2001). 2001. 603−608.

[6] Kim S, Park S, Won D. Proxy signatures, revisited. In: Proc. of the Information and Communications Security-ICICS'97. LNCS 1334, 1997. 223−232.

[7] Wang GL, Bao F, Zhou JY, Deng RH. Security analysis of some proxy signatures. In: Proc. of the Information Security and Cryptology-ICISC2003. LNCS 2971, Springer-Verlag, 2004. 305−319.

[8] Wang SH, Wang GL, Bao F, Wang J. Cryptanalysis of a proxy-protected proxy signature scheme based on elliptic curve cryptosystem. In: Proc. of the 60th IEEE Vehicular Technology Conference, Session 4.6: Wireless Sensor/Network Security. IEEE Vehicular Technology Society Press. 2004.

[9] Lin WD, Jan JK. A security personal learning tools using a proxy blind signature scheme. In: Proc. of Int'l Conf. on Chinese Language Computing. 2000. 273−277.

[10] Tan ZW, Liu ZJ, Tang CM. A proxy blind signature scheme based on DLP. Journal of Software, 2003,14(11):1931−1935.

[11] Tan ZW, Liu ZJ, Tang CM. Digital proxy blind signature schemes based on DLP and ECDLP. Vol.21, Beijing: Key Laboratory of Mathematics Mechanization Research, Academy of Mathematics and Systems Science, the Chinese of Academy of Sciences, 2002. 212−217.

[12] Zhang FG, Safavi-Naini R, Lin CY. New proxy signature, proxy blind signature and proxy ring signature schemes form bilinear pairings. 2003. http://eprint.iacr.org/2003/104