Analysis of Some Attacks on Awasthi and Lal's Proxy Blind Signature Scheme *

Bennian Dou[1]#, Chungen Xu[1]

[1] School of Science, Nanjing University of Science and Technology, Nanjing 210094, China

Abstract: A proxy blind signature combines the properties of proxy signature and blind signature. Recently, Awasthi and Lal proposed a more efficient proxy blind signature based on the proxy signature scheme proposed by Mambo et al.. Later, Sun et al. and Das et al. gave some attacks on Awasthi and Lal's scheme respectively. In this paper, we analyze the two attacks and we point out that those attacks do not apply to Awasthi and Lal's scheme.

Keywords: Cryptanalysis, Digital Signature, Proxy Blind Signature

1 Introduction

Blind signature was first proposed by Chaum [1] in 1982. A blind signature allows a blinder to get a document's signature of a signer, without revealing any information about the document or its signature. Blind signature can offer anonymous which can be used in electronic cash and electronic voting. In 1996, Mambo et al. [2] proposed the concept of proxy signature. In a proxy signature, the original signer can delegate his signing power to a proxy signer and the proxy signer can sign documents on behalf of the original signer. Proxy signature has its applications in some scenarios, for example, a professor wants to go on a vacation, during his vacation, there are many documents should be signed by him, then he can delegate his signing to his secretary and the secretary can sign a document on behalf of the professor. Meanwhile, Mambo et al. gave the types of proxy signatures, i.e. full proxy signature, partial proxy signature and proxy signature with warrant. In a partial signature, the original signer generates a proxy key different with his signing key and gives the generated proxy key to the proxy signer, and then the proxy signer uses it to sign documents. There are two types of partial proxy signature: proxy unprotected scheme (both the original signer and the proxy signer can produce a valid proxy signature for a document) and proxy protected signature (only proxy signer can produce a valid proxy signature for a document). In this paper, we only consider partial proxy unprotected signature. There are some security requirements on proxy signatures which were also mentioned in [2].

In 2002, Tan et al. [3] combined proxy signature and blind signature; they proposed the first proxy blind signature. The proxy blind signature is needed in the following scenario: In e-cash system, the user makes the bank blindly sign a coin using blind signature schemes. Whenever a user wants to withdraw a coin from a branch of the bank, he needs the branch bank to produce proxy blind signature on behalf of the signee bank. Later in 2003, Awasthi and Lal [4] proposed

* The first author is supported by the Research Foundation of Nanjing University of Science & Technology and CSC (China Scholarship Council)

Corresponding author. E-mail: doubennian@yahoo.com.cn

a more efficient proxy blind signature. There are some security requirements on proxy blind signatures which are as follows [3]:

Distinguishability : The proxy signature must be distinguishable from the normal signature.

Unforgeability: Besides the original signer, only a designated proxy signer can create a valid proxy signature.

Non-repudiation: Neither the original signer nor the proxy signer can deny valid proxy signatures.

Unlinkability: Neither the original signer nor the proxy signer can link the revealed messages and signatures with the blinded messages and signatures.

On Awasthi and Lal's scheme, in 2003, Sun et al. [5] and Das et al. [6] gave some attacks respectively.

In this paper, we analyze the attacks of Sun et al.'s and Das et al.'s, we point out that both those attacks failed to Awasthi and Lal's scheme.

The rest of this paper is organized as follows. In section 2, we review Awasthi and Lal's proxy blind signature scheme. In section 3, we review the attacks of Sun et al.'s and Das et al.'s. on Awasthi and Lal's scheme. In section 4, we give our analysis of their attacks and we point out that both those attacks failed to Awasthi and Lal's scheme. We conclude the paper in section 5.

2 Awasthi and Lal's proxy unprotected blind signature

2.1 Notations and parameters

p: a large prime number

q: a large prime factor of (p -1)

g: an element of Z_p^* of order q

$x_A : x_A \in Z_q^*$, the secret key of the original signer A

y_A: the public key of the original signer A, where $y_A = g^{x_A} \bmod p$

h(.): a secure one way hash function, $h(m) \to Z_q$, for any message m

P: a proxy signer P

B: a blinder who wants to get a signature for a document from A or P

2.2 Awasthi and Lal's scheme

2.2.1 Proxy phase

1. (Proxy Generation) The original signer A randomly chooses $k \in Z_q^*$, and computes

$$r = g^k, s = (x_A + kr) \bmod q, y_p = g^s \bmod p .$$

2. (Proxy Delivery) A sends (s, r) to a proxy signer P in a secure way and makes y_p public.

3. (Proxy Verification) On receiving (s, r), P checks if $y_p = g^s = y_A r^r \bmod p$, if it holds, he

accepts it as a valid proxy and will use *s* as the proxy signing key, otherwise he rejects it.

2.2.2 Signing phase

1. *P* computes $t = g^K \bmod p$, where $K \in Z_q^*$ is a random number; *P* sends *t* to the blinder *B*.

2. *B* computes $r' = tg^{-\alpha} y_p^{-\beta} \bmod p$, $e' = h(r' \| m), e = (e' + \beta) \bmod q$, where $\alpha, \beta \in Z_p^*$ are random numbers, *m* is the document which will be signed. *B* sends *e* to *P*.

3. On receiving *e*, *P* computes $s' = (K - se) \bmod q$,and sends it to *B*.

4. On receiving s', *B* computes $s_p = (s' - \alpha) \bmod q$ .The signature of the message *m* is (m, s_p, e').

2.2.3 Verification phase

The verifier can verify the signature by checking if $e' = h(g^{s_p} y_p^{e'} \bmod p \| m)$. If it holds, it is a valid signature; otherwise it is not a valid signature.

3 Sun et al.'s and Das et al.'s attacks

3.1 Sun et al.'s attacks

3.1.1 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*, *e*, and s'. After a signature (m, s_p, e') is revealed, the proxy signer computes $\alpha' = s' - s_p, \beta' = e - e'$ and $r' = g^{s_p} y_p^{e'} \bmod p$ for some s' and *e*. finally, the proxy signer checks the equation $r' = tg^{-\alpha'} y_p^{-\beta'} \bmod p$, if he find a corresponding *t* such that $r' = tg^{-\alpha'} y_p^{-\beta'} \bmod p$, therefore, the proxy signer knows that (*t*, *e*, s') is the related blind information corresponding to the revealed message *m*. Namely, Awasthi and Lal's proxy blind signature does not possess the unlinkability property.

3.1.2 Attack 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 Awasthi and Lal'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.

3.2 Das et al.'s attacks

3.2.1 Proxy signer's forgery attack

1. *P* computes $t = g^K \bmod p$, where $K \in Z_q^*$ is a random number; *P* sends *t* to the blinder *B*.

2. *B* computes $r' = tg^{-\alpha} y_p^{-\beta} \bmod p$, $e' = h(r' \| m), e = (e' + \beta) \bmod q$, where $\alpha, \beta \in Z_p^*$ are random numbers, *m* is the document which will be signed. *B* sends *e* to *P*.

3. *P* chooses random numbers $a, b \in Z_p^*$, and computes $R = g^a (y_p)^e b^{-1}$. They assume that $t = Rb$ can holds. Then, *P* sends *a* to *B*.

4. On receiving *a*, *B* computes $s_p = (a - \alpha) \bmod q$ .The signature of the message *m* is (m, s_p, e').

Correctness:

$$h(g^{s_p} y_p^{e'} \bmod p \| m) = h(g^a g^{-\alpha} y_p^{e'} \bmod p \| m)$$
$$= h(Rby_p^{-e} g^{-\alpha} y_p^{e'} \bmod p \| m) = h(ty_p^{-\beta} y_p^{-e'} g^{-\alpha} y_p^{e'} \bmod p \| m) = h(r' \| m) = e'$$

3.2.2 Misuse of original's delegated information

As the original signer's delegation power does not contain any information about the qualification of the messages on which the proxy signer signs. The original signer cannot restrict the proxy signer for misuse of his delegation. The proxy signer can further transfer the delegation power to someone else, who also can perform the signing operation on behalf of the original signer.

4 Our analysis of Sun et al.'s and Das et al.'s attacks

4.1 Analysis of Sun et al.'s attacks

4.1.1 Awasthi and Lal's scheme possesses unlinkability

In fact, for each record (*t*, *e*, s') of the proxy signer, every revealed information (m, s_p, e') can serve as the corresponding revealed information of (*t*, *e*, s'). We now prove this property. Let (m_1, s_{p1}, e_1') be arbitrary revealed information. From the signing phase of Awasthi and Lal's scheme, we know, for a record (*t*, *e*, s'), that $t = g^K \bmod p$ and $s' = (K - se) \bmod q$, so $tg^{-s'} y_p^{-e} = g^K g^{se-K} g^{-se} = 1$. If computing $\alpha' = s' - s_{p1}$, $\beta' = e - e_1'$, $r' = g^{s_{p1}} y_p^{e_1'} \bmod p$, then, we get $tg^{-\alpha'} y_p^{-\beta'} \bmod p = tg^{-(s'-s_{p1})} y_p^{-(e-e_1')} = tg^{-s'} y_p^{-e} g^{s_{p1}} y_p^{e_1'} = r' \bmod p$. Therefore, the proxy signer cannot link (*t*, *e*, s') with any revealed information.

4.1.2 About the attack on the Publishing of Proxy Public Key

We point out if someone who is not the original or the proxy signer republish the proxy public key and then impersonate the original signer, he can be caught by the original or the proxy signer by asking him to give the corresponding secret key of the proxy public key, for, he cannot compute the secret key from the proxy public key.

4.2 Analysis of Das et al.'s attacks

4.2.1 On the proxy signer's forgery attack

We point out that Proxy signer's forgery attack cannot apply to Awasthi and Lal's scheme. In the third step of this attack, $a,b \in Z_p^*$ are random numbers, and $R = g^a (y_p)^e b^{-1}$, Das et al. assume that $t = Rb$. We claim that they cannot find such *a*, *b*. For *t* is fixed, then if we choose a random *b*, *R* must be tb^{-1}, and therefore, g^a must be $(tb^{-1})by_p^{-e} = ty_p^{-e}$, *a* cannot be random again, but the discrete logarithm of ty_p^{-e} with respect to the base *g*, on the other hand, it is hard to compute discrete logarithm, thus, *a* cannot be found and this attack fails.

4.2.2 On the misuse of original's delegated information

As far as partial proxy unprotected blind signature is concerned, we point out that Awasthi and Lal's scheme is ok, for, every proxy unprotected signature has such problem. Sometimes we need proxy signature with warrant to prevent the misuse of delegation, the warrant contains some information which restricts the delegation power of the proxy signer.

5 Conclusions

In this paper, we analyzed some attacks on Awasthi and Lal's proxy unprotected blind signature scheme, we pointed out that those attacks do not apply to Awasthi and Lal's scheme.

References

[1] D. Chaum, Blind signature for untraceable payments,*Advances in Cryptology-CRYPT'82*, Plenum Press(1982),199-203.

[2] M. Mambo, K. Usuda and K. Okamoto, Proxy signature: delegation of the power to sign messages, *IEICE Trans. Fundam.* E79-A (1996) (9), 1338–1353.

[3] Z. Tan, Z. Liu, and C. Tang, Digital proxy blind signature schemes based on DLP and ECDLP. *MM Research Preprints*, No. 21, MMRC, AMSS, Academic, Sinica, Beijing (2002), 212–217.

[4] A. K. Awasthi and S. Lal, Proxy blind signature scheme, *Transaction on Cryptology* 2 (2005) (1), 5–11, Available from: *IACR ePrint Achive*, <http://eprint.iacr.org/2003/072.pdf>.

[5] H. M. Sun, B. T. Hsieh, On the security of some proxy blind signature scheme, *IACR ePrint Achive*, <http://eprint.iacr.org/2003/068.pdf>.

[6] M. l. Das, A. Saxena and V. P. Gulati, Security Analysis of Lal and Awasthi's Proxy Signature Schemes, *IACR ePrint Achive*, <http://eprint.iacr.org/2003/263.pdf>.