http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (21): 6159-6163, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.6159.6163

A New Proxy Blind Signature Scheme with Message Recovery

[1]Lijuan Diao, [1]Junzhong Gu and [2]I-Ling Yen
[1]East China Normal University, Shang Hai, 200241, China
[2]University of Texas at Dallas, America

Abstract: This study, for the first time, presents a proxy blind signature scheme with message recovery. The proposed scheme is based on Tan et al.'s proxy blind signature scheme and Abe and Okamoto's signature scheme with message recovery.When practical hash functions are used in the place of truly random functions,the scheme is almost as efficient as the existing schemes with message recovery such as Zhang *et al.*'s scheme. And, it can be proven to be unforgeable against adaptively chosen message attacks in the random oracle model under the discrete logarithm assumption, like Abe and Okamoto scheme.

Key words: Cryptography, blind signature, proxy signature, message recovery

INTRODUCTION

The digital signature scheme with message recovery is useful for many applications in which small message (e.g., around 100 bits (Abe and Okamoto, 1999) should be signed, such as time, random dates or identifiers. And, the message recovery can be directly used in other schemes such as (Zhang *et al.*, 2005; Li *et al.*, 2005). Abe and Okamoto (1999) firstly presented a digital signature scheme with message recovery which can be proven to be secure in the random oracle model. Tseng *et al.* (2003) firstly proposed an efficient digital signature scheme with message recovery. There exists a trusted system authority in Tseng *et al.* scheme. However, the Trusted Authority (TA) is not existent in real world. Thereby, Chang *et al.* (2005) proposed a new digital signature scheme with message recovery, which provide the same function as Tseng *et al.*'s scheme without the assumption that TA is necessary to be reliable. In 2005, Zhang *et al.* (2005) gave a security analysis of Chang *et al.*'s scheme and showed that the scheme is insecure, namely, the system authority can recover the message without the private key of the recipient in Chang *et al.*'s scheme.

A blind signature (Chaum, 1982) allows a blinder to get a document's signature of a signer, without revealing any information about the document or its signature. It can offer anonymous which can be used in electronic cash and electronic voting. In 1996, Mambo *et al.* (1996) 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. Meanwhile, Mambo *et al.* gave the types of proxy signature, 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 two types of partial proxy signature: proxy unprotected scheme and proxy protected signature. In a proxy protected scheme, only the proxy signer can produce a valid proxy signature for a document. In this study, we only consider partial proxy protected signature. In 2002, Tan *et al.* (2002) combined blind signature and proxy signature and proposed the first proxy blind signature. A proxy blind signature allows the proxy signer to generate a blind signature on behalf of the original signer. For example, a professor wants to go on a vacation, during his vacation, there are many documents should be signed by him. (s) he can delegate her/his secretary to sign documents on behalf of her/him. However, in the scenario, the secretary cannot take part in the secret sharing on behalf of the professor, because she cannot produce the professor's private key in the partial proxy blind signature.

For the further research, we combine signature with message recovery and proxy blind signature, then propose the first proxy blind signature with message recovery. The proposed scheme satisfies all characteristics of strong proxy blind signature and not use secure channel in the communication between the original signer and the proxy signer.

The study is organized as follows. In section 2, we review of Tan *et al.*'s proxy blind signature scheme. Our proposed proxy blind signature scheme with message recovery is in section 3. The performance evaluation and security analysis of the proposed scheme is discussed in section 4 and 5, respectively. We conclude our scheme in section 6.

Corresponding Author: Junzhong Gu, East China Normal University, Shang Hai 200241, China

REVIEW OF TAN *ET AL.*'S SCHEME

Tan *et al*. proposed a proxy blind signature scheme based on the Discrete lLogarithm Problem (DLP) in 2002. They also defined the required security properties of proxy blind signature scheme. The scheme is consisted of three phases as following:

- Proxy delegation
- Signing
- Verification

Proxy delegation phase: The original signer randomly selects a number k_0 and calculates:

$$r_0 = g^{k0} \bmod p \text{ and } s_0 = k_0+x_{0,} r_0 \bmod q$$

Then, the original signer sends (r_0, s_0) to the proxy signer in a secure way. After the proxy signer receives it, (s)he can verify it by checking the correctness of the equation:

$$g^{s0} = y_0^{r0}.r \text{ mod} p.$$

Finally, the proxy signer computes her/his proxy secret key:

$$S_{pr} = s_0+x_p \text{ mod} q$$

Signing phase: The proxy signer chooses a random number k, computes:

$$T = g^k \text{ mod} p$$

and sends (r_0, t) to the receiver. After receiving it, the receiver randomly chooses two numbers α and b and calculates:

$$r = t.g^b.y_p^{-a-b}. (y_0^{r0}) \text{ mod} p$$

$e = h (r||m)\text{mod}q$, $e' = (e\text{-}a\text{-}b) \bmod q$, $u = (y_0^{r0}.r_0)^{-e+b}.y_0^{-e} \bmod p$

Then, the receiver sends e' to the proxy signer. Next, the proxy signer calculates the blinded signature:

$$s' = e'.s_{pr} +k \bmod q$$

And sends s′ back to the receiver. Finally, the receiver computes:

$$S = s'+b \bmod q$$

The signature of the message m is (m , u, s, e).

Verification phase: Anyone can verify the correctness of the proxy blind signature (m, u, s,e) by checking that holds.

Remark 1: Tan *et al.*'s scheme needs a secure way between the original signer and the proxy signer. However, the secure way is not existent in practical communications system. Thereby, in this study, we propose a new digital signature scheme with message recovery, which provides the same function as Tan *et al.*'s scheme and without the assumption that a secure way is necessary to be reliable.

Remark 2: If theis leaked in the communication or when it is being used. Then, anyone elsecan compute $s_A = s_0+x_A \bmod q$, where x_A is A's secret key.

And, A can impersonate a legitimate proxy signature.

PROPOSED SCHEME

This section introduces our proxy blind signature with message recovery. There are three kinds of participants: Original signer U_o, the proxy signer U_p and the receiver R

In the section. The proposed scheme is divided into four phases: system initialization phase, proxy delegation phase, signing phase and verification phase.

System initialization phase:

p: A large prime number
q: Another large prime number, where q| (p-1)
G: Element of Z_p^* of order q
x_o: Secret key of U_o
y_o: Public key of U_o, where $y_o = g^{xo} \bmod p$
x_p: Secret key of U_p
y_p: Public key of U_p, where $y_p = \bmod p$
h (.): A secure and public one way hash function
H_1 (.): A public random oracle function, $\{0, 1\}^* \rightarrow Z_q^*$
H_2(.): A public random oracle function, $Z_q^* \rightarrow \{0, 1\}^*$
||: The concatenation of strings

Proxy delegation phase: U_o randomly selects a number $k_o \in Z_q^*$ and computes $r_o = g^{ko} \bmod p$, $s_o = k_o+x_o.\ h\ (r_o) \bmod q$.

Then, U_o sends (r_o, s'_o) to U_p in a generell communication channel. After receiving it, U_p firstly computes and accepts (r_o, s'_o) if the equation holds.
Finally, U_p computes the proxy signature key.

$$s_{\mathcal{P}} = s_{\mathcal{O}} + x_{\mathcal{P}} \bmod q$$

Here, $\{r_o, y_p\}$ is proxy signature public key and $\{s_p\}$ is the proxy signature private key.

Signing phase: Suppose that R wants to get a signature of $m \in \{0, 1\}^*$ from U_p.

After finding the proxy signature public key, R randomly chooses two numbers a and b and calculates:

$$\begin{aligned}
&r = g^b \cdot y_p^{-a-b} \cdot (y_{\mathcal{O}}^{h(r_{\mathcal{O}})} \cdot r_{\mathcal{O}})^{-a} \bmod p \\
&e_1 = h(r) \| H_1(m) \bmod q,\ e_2 = H_2[h(r)] \oplus m \\
&e' = (e_1 - a - b) \bmod q, \\
&z = (y_{\mathcal{O}}^{h(r_{\mathcal{O}})} \cdot r_{\mathcal{O}})^{-e_1+b} \cdot y_{\mathcal{O}}^{-e_1} \cdot y_{\mathcal{P}}^{-1} \bmod p
\end{aligned}$$

Then, R sends:

$$\{e', H_1(m), z, e_1, e_2\}$$

to U_p.

Next, U_p calculates the blinded signature:

$$s' = e_1 \cdot s_{\mathcal{P}} + x_{\mathcal{P}} \bmod q$$

and sends s' back to R.

At last, R computes:

$$s = s' + b \bmod q$$

The resultant signature on message m is:

$$\{z, H_1(m), s, e_1, e_2\}$$

Message recovery and verification phase: Upon receiving the proxy blind signature:

$$\{z, H_1(m), s, e_1, e_2\}$$

any verifier R can recovery message m by the equation:

$$m = e_2 \oplus H_2[h(g^s \cdot y_{\mathcal{P}}^{-e_1} \cdot y_{\mathcal{O}}^{e_1} \cdot z \bmod p)]$$

And R can verify the correctness of the proxy blind signature by checking that:

$$e_1 = h(g^s \cdot y_{\mathcal{P}}^{-e_1} \cdot y_{\mathcal{O}}^{e_1} \cdot z \bmod p) \| H_1(m)$$

holds.

PROOF OF CORRESCTNESS

In this section, we will prove the correctness of the proposed scheme.

Theory 1: U_p can verify the validity of his proxy delegation from (r_o, s'_o).

Proof: From the equation:

$$r_{\mathcal{O}} = g^{k_{\mathcal{O}}} \bmod p$$

And:

$$s'_{\mathcal{O}} = s_{\mathcal{O}} \cdot (y_{\mathcal{P}}^{-x_{\mathcal{O}}} \bmod p) \bmod q$$

We have:

$$\begin{aligned}
&s'_{\mathcal{O}} \cdot (y_{\mathcal{O}}^{x_{\mathcal{P}}} \bmod p) \bmod q \\
&= s_{\mathcal{O}} \cdot (y_{\mathcal{P}}^{-x_{\mathcal{O}}} \bmod p) \cdot (y_{\mathcal{O}}^{x_{\mathcal{P}}} \bmod p) \bmod q = s_{\mathcal{O}}
\end{aligned}$$

So, using the equation:

$$s_{\mathcal{O}} = k_{\mathcal{O}} + x_{\mathcal{O}} \cdot h(r_{\mathcal{O}}) \bmod q$$

the following equation holds:

$$\begin{aligned}
&r_{\mathcal{O}} y_{\mathcal{O}}^{h(r_{\mathcal{O}})} \bmod p \\
&= g^{k_{\mathcal{O}}} \cdot y_{\mathcal{O}}^{h(r_{\mathcal{O}})} \bmod p \\
&= g^{k_{\mathcal{O}}} \cdot g^{x_{\mathcal{O}} \cdot h(r_{\mathcal{O}})} \bmod p = g^{s_{\mathcal{O}}}
\end{aligned}$$

Theory 2: The message m can be correctly recovered from proxy blind signature:

$$\{z, H_1(m), s, e_1, e_2\}$$

at the same time, the public keys y_p and y_o are also verified indirectly.

Proof: From the equation $s = s' + b \bmod q$ and:

$$z = (y_{\mathcal{O}}^{h(r_{\mathcal{O}})} \cdot r_{\mathcal{O}})^{-e_1+b} \cdot y_{\mathcal{O}}^{-e_1} \cdot y_{\mathcal{P}}^{-1} \bmod p$$

We have:

$$\begin{aligned}
&g^s \cdot y_{\mathcal{P}}^{-e_1} \cdot y_{\mathcal{O}}^{e_1} \cdot z \bmod p \\
&= g^{s'+b} \cdot y_{\mathcal{P}}^{-e_1} \cdot y_{\mathcal{O}}^{e_1} \cdot z \bmod p \\
&= g^b \cdot g^{s'} \cdot y_{\mathcal{P}}^{-e_1} \cdot y_{\mathcal{O}}^{e_1} \cdot ((y_{\mathcal{O}}^{h(r_{\mathcal{O}})} \cdot r_{\mathcal{O}})^{-e_1+b} \cdot y_{\mathcal{O}}^{-e_1} \cdot y_{\mathcal{P}}^{-1}) \bmod \\
&= g^b \cdot g^{s'} \cdot y_{\mathcal{P}}^{-e-a-b} \cdot ((y_{\mathcal{O}}^{h(r_{\mathcal{O}})} \cdot r_{\mathcal{O}})^{-e'-a} \cdot y_{\mathcal{P}}^{-1}) \bmod \\
&= r \cdot g^{s'} \cdot (y_{\mathcal{P}} \cdot y_{\mathcal{O}}^{h(r_{\mathcal{O}})} \cdot r_{\mathcal{O}})^{-e'} \cdot y_{\mathcal{P}}^{-1} \bmod p \\
&= r \cdot g^{s'} \cdot (g^{x_{\mathcal{P}}})^{-e'} \cdot y_{\mathcal{P}}^{-1} \bmod p = r
\end{aligned}$$

Then, using the equation:

$$e_2 = H_2[h(r)] \oplus m \bmod q$$

we can correctly recover the message:

$$m = e_2 \oplus H_2[h(r)] \bmod q$$

In the following, we give the detailed verification by checking:

$$\begin{aligned} & h(g^{s} \cdot y_{\mathcal{P}}^{-e_1} \cdot y_{\mathcal{O}}^{e_1} \cdot z \bmod p) \| H_1(m) \\ & = h(g^{s} \cdot y_{\mathcal{P}}^{-e_1} \cdot y_{\mathcal{O}}^{e_1} \cdot z \bmod p) \| H_1(m) \\ & = h(r) \| H_1(m) = e_1 \end{aligned}$$

Consequently, the public key y_p and y_o are also verified indirectly.

Remark 3: Li *et al.* (Li *et al.*, 2005) claim that their scheme does not use secure channel in the communication between the original signature and the proxy signature signer.

That is to say:

$$(ID_0, r_0, s_0)$$

is sended to U_p publicly. Then, everyone can be a valid proxy signer and execute proxy signature phase.

In order to avoid such attacks, we construct a secure and public channel between the original signer and the proxy signer in the above scheme. Because only they can compute $g^{xo, xp} \bmod p$, the secure is owed to CDH problem.

Security analysis: The security of the proposed scheme is based on two well-known cryptographic assumption: Discrete :ogarithm (DL) assumption and One-Way Hash Function (OWHF) assumption.

U_p cannot compute U_o's secret key x_o from:

$$s_{\mathcal{O}} = k_{\mathcal{O}} + x_{\mathcal{O}} \cdot h(r_{\mathcal{O}}) \bmod q$$

because, in the equation, k_o and x_o are all unknown. Further more, antone else cannot achieve x_o from:

$$s'_{\mathcal{O}} = s_{\mathcal{O}} \cdot (y_{\mathcal{P}}^{-x_{\mathcal{O}}} \bmod p) \bmod q$$

Which is based on the intractability of solving the DL problem and the OWHF assumption U_p's secret key from the public information is based on the intractability of solving the DL problem.

Consider the scenario that an adversary attempts generate a valid secret/public key pair (x_A, y_A) for forging proxy signer with pseudo randomly data. In such case, (x_A, y_A) should satisfy equation:

$$y_{O}^{x_A} \cdot s_{O} = y_{A}^{x_O} \cdot s'_{O}$$

Otherwise they cannot be applicable to the subsequent proxy signature scheme without being detected. Evidently, the adversary will face the intractability of solving the DL problem or reversing the OWHF problem to obtain (x_A, y_A) successfully.

As the original signer's delegation power does not contain any information about the qualification of the message on which the proxy signer signs. The original signer cannot restrict the proxy signer for misuse of his delegation. Actually, every proxy blind signature has such problem. Sometimes we need proxy blind signature with warrant to prevent the misuse of delegation, the warrant contains some information which restricts the delegation power of the proxy signer.

It can be proven security against forgery attacks and public key substitution attacks (Li *et al.*, 2005). And, it satisfies the likability property (Wu *et al.*, 2006).

PERFORMANCE EVALUATION

In the section, we evaluate our proposed scheme's: performance in terms of computational complexities and communication costs.

Firstly, denote the following notations (Hsu *et al.*, 2001) to facilitate the performance evaluation:

- T_h: The time for performing a one-way hash function h
- T_{exp}: The time for performing a modular exponentiation computation
- T_{mul}: The time for performing a modular multiplication computation
- T_{inv}: The time for performing a modular inverse computation

The analysis of the proposed scheme is stated in the following Table 1.

From the Table 1, we can see that the proposed scheme is more efficient.

Table 1: Computational complexities

	Proposed scheme
System initialize	$2T_{exp}$
Proxy delegation	$3_{exp}+3T_{mul}+T_{inv}+3T_h$
Signing phase	$2T_{exp}+7T_{mul}+4T_{inv}+2T_h$
Verification phase	$4T_{exp}+6T_{mul}+2T_{inv}+3T_h$

CONCLUSION

In this study, we propose the first proxy blind signature with message recovery. It withstands public key substitution attack, forge attack and so on. In addition, the proposed scheme satisfies all properties of strong proxy blind signature and does not use secure channel in the communication between the original signer and the proxy signature signer.

REFERENCES

Abe, M. and T. Okamoto, 1999. A signature scheme with message recovery as secure as discrete logarithm. Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, November 14-18, 1999, Singapore, pp: 378-389.

Chang, Y.F. and C.C. Chang, H.F. Huang, 2005. Digital signature with message recovery using self-certified public keys without trustworthy system authority. Applied Math. Comput., 161: 211-227.

Chaum, D., 1983. Blind Signature for Untraceable Payments. Plenum Press, New York, USA., pp: 199-203.

Hsu, C.L., T.S. Wu and T.C. Wu, 2001. New nonrepudiable thres-hold proxy signature scheme with kown signers. J. Syst. Software, 58: 119-124.

Li, J.G., Y.C. Zhang and Y.L. Zhu, 2005. A new proxy signature scheme with message recovery using self-certified public key. Wuhan Univ. J. Nat. Sci., 10: 219-222.

Mambo, M., K. Usuda and K. Okamoto, 1996. Proxy signatures: Delegation of the power to sign messages. IEICE Trans. Fundam. Electron Commun. Comput. Sci., E79-A: 1338-1354.

Tan, Z., Z. Liu and C. Tang, 2002. Digital proxy blind signature scheme based on DLP and ECDLP. MM Research Preprints, MMRC, AMSS, Academia, Sinica, Beijing, No. 21, December, 2002.

Tseng, Y.M., J.K. Jan and H.Y. Chien, 2003. Digital signature with message recovery using self-certified public keys and its variants. Applied Math. Comput., 136: 203-214.

Wu, L.C., Y.S. Yeh and T.S. Liu, 2006. Analysis of sun *et al.*'s linkability attack on some proxy blind signature schemes. J. Syst. Software, 79: 176-179.

Zhang, J.H., W. Zou, D. Chen and Y.M. Wang, 2005. On the security of a digital signature with message recovery using self-certified public key. Informatica, 29: 343-346.