A New Proxy Blind Signature Scheme with Message Recovery

1Lijuan Diao, 1Junzhong Gu and 2I-Ling Yen
1East China Normal University, Shang Hai, 200241, China
2University 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) 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.
REVIEW OF TAN ET AL.'S SCHEME

Tan et al. proposed a proxy blind signature scheme based on the Discrete Logarithm 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:

$$r_0 = g^{k_0} \mod p$$

and calculates $s_1 = k_0 \cdot x_0 \cdot r_1 \mod q$

Then, the original signer sends $(r_0, s_1)$ 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:

$$y_0^p = y_0^{s_1} \cdot r \mod p$$

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

$$S_n = s_1 + x_q \mod q$$

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

$$T = g^k \mod p$$

and sends $(r_n, t)$ to the receiver. After receiving it, the receiver randomly chooses two numbers $\alpha$ and $b$ and calculates:

$$r = \{g^\beta \cdot y_e^\alpha \cdot (y_0^\alpha) \mod p$$

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

$$s' = e' \cdot s_n + k \mod q$$

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

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

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 the is leaked in the communication or when it is being used. Then, anyone else can compute $s_n = s_1 + x_q \mod q$, where $x_q$ 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 $Z_q^*$ of order $q$
- $x_i$: Secret key of $U_i$
- $y_i$: Public key of $U_i$, where $y_i = g^{x_i} \mod p$
- $x_q$: Secret key of $U_q$
- $y_q$: Public key of $U_q$, where $y_q = \mod p$
- $h(\cdot)$: A secure and public one way hash function
- $H_1(\cdot)$: A public random oracle function, $\{0, 1\} \rightarrow Z_q^*$
- $H_2(\cdot)$: A public random oracle function, $Z_q^* \rightarrow \{0, 1\}$
- $||$: The concatenation of strings

Proxy delegation phase: $U_o$ randomly selects a number $k_0 \in Z_q^*$ and computes $r_0 = g^{k_0} \mod p$, $s_1 = k_0 \cdot x_0 \mod q$.

Then, $U_o$ sends $(r_o, s_1)$ to $U_p$ in a generell communication channel. After receiving it, $U_p$ firstly computes and accepts $(r_o, s_1)$ if the equation holds.

Finally, $U_p$ computes the proxy signature key.
Here, \( \{r_0, y'_0\} \) is proxy signature public key and \( \{s_0\} \) 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:

\[
\begin{align*}
    r &= g^a \cdot y_p^b \cdot (y_0^{b(r)} \cdot c_0)^{\alpha} \mod p \\
    e_i &= b(r) \| H_i(m) \mod q, e_j &= H_j[b(r)] \mod p \\
    e' &= (e_i - a \cdot b) \mod q \\
    z &= (y_0^{b(r)} \cdot c_0)^{\alpha} \cdot y_0^0 \cdot y_0^e \mod p
\end{align*}
\]

Then, R sends:

\[
\{e', H_i(m), z, e_i, e_j\}
\]

to \( U_p \).

Next, \( U_p \) calculates the blinded signature:

\[
s' = e_i \cdot s_p + x_p \mod q
\]

and sends \( s' \) back to R.

At last, R computes:

\[
s = s' - b \mod q
\]

The resultant signature on message \( m \) is:

\[
\{z, H_i(m), s, e_i, e_j\}
\]

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

\[
\{z, H_i(m), s, e_i, e_j\}
\]

any verifier R can recovery message \( m \) by the equation:

\[
m = e_i \| H_i[(g^a \cdot y_p^b \cdot y_0^0 \cdot z)^\| H_i(m)]
\]

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

\[
e_i = H_i[(g^a \cdot y_p^b \cdot y_0^0 \cdot z)^\| H_i(m)]
\]

holds.

**Proof of Correctness**

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 \( (r_0, s_0') \).

**Proof:** From the equation:

\[
t_0 = g^{b(r)} \mod p
\]

And:

\[
s_0' = s_0 - (y_0^{b(r)} \mod p) \mod q
\]

We have:

\[
\begin{align*}
    s_0' \cdot (y_0^{b(r)} \mod p) \mod q \\
    = s_0 \cdot (y_0^{b(r)} \mod p) - (y_0^{b(r)} \mod p) \mod q = s_0
\end{align*}
\]

So, using the equation:

\[
r_0 = k_0 + s_0 \cdot b \mod q
\]

the following equation holds:

\[
\begin{align*}
    t_0 \cdot y_0^{b(r)} \mod p \\
    = g^{b(r)} \cdot y_0^{b(r)} \mod p \\
    = g^{b(r)} - g^{b(r)} \cdot b \mod p = g^{b(r)}
\end{align*}
\]

**Theory 2**:

The message \( m \) can be correctly recovered from proxy blind signature:

\[
\{z, H_i(m), s, e_i, e_j\}
\]

at the same time, the public keys \( y_p \) and \( y_0 \) are also verified indirectly.

**Proof:** From the equation \( s = s' + b \mod q \) and:

\[
z = (y_0^{b(r)} \cdot c_0)^{\alpha} \cdot y_0^0 \cdot y_0^e \mod p
\]

We have:

\[
\begin{align*}
    g^a \cdot y_p^b \cdot y_0^0 \cdot z \mod p \\
    = g^{b(r)} \cdot y_0^0 \cdot z \mod p \\
    = g^{b(r)} \cdot y_0^0 \cdot (y_0^{b(r)} \cdot c_0)^{\alpha} \cdot y_0^0 \cdot y_0^e \mod p \\
    = g^{b(r)} \cdot y_0^0 \cdot (y_0^{b(r)} \cdot c_0)^{\alpha} \cdot y_0^e \mod p \\
    = r \cdot g^{b(r)} \cdot (y_p \cdot y_0^{b(r)} \cdot c_0)^{\alpha} \cdot y_0^e \mod p \\
    = r \cdot g^{b(r)} \cdot (y_p \cdot y_0^{b(r)} \cdot c_0)^{\alpha} \cdot y_0^e \mod p
\end{align*}
\]

Then, using the equation:

\[
e_i = H_i[b(r)] \mod q
\]

we can correctly recover the message.
In the following, we give the detailed verification by checking:

\[ h(g^{x} \cdot y_{o}^{x} \cdot z_{modp}) \cdot H_{i}(m) \]
\[ = h(g^{x} \cdot y_{2}^{x} \cdot y_{o}^{x} \cdot z_{modp}) \cdot H_{i}(m) \]
\[ = h(r) \cdot H_{i}(m) = e_{i} \]

Consequently, the public key \( y_{s} \) and \( y_{e} \) 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 signer and the proxy signature signer.

That is to say:

\[(ID_{o}, r_{o}, s_{o})\]

is sent 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 \( g^{x \cdot z_{modp}} \), the secure is owed to CDH problem.

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

\( U_{o} \) cannot compute \( U_{p} \)’s secret key \( x_{o} \) from:

\[ s_{o} = k_{o} + x_{o} \cdot h(r_{o}) \mod q \]

because, in the equation, \( k_{o} \) and \( x_{o} \) are all unknown. Further more, anyone else cannot achieve \( x_{o} \) from:

\[ s_{o} - s_{o} \cdot (y_{o}^{x_{o}} \mod p) \mod q \]

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 \((x_{o}, y_{o})\) for forging proxy signer with pseudo randomly data. In such case, \((x_{o}, y_{o})\) should satisfy equation:

\[ y_{o}^{x} \cdot s_{o} = y_{o}^{x} \cdot s_{o} \]

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 \((x_{o}, y_{o})\) 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 (Hau et al., 2001) to facilitate the performance evaluation:

- \( T_{h} \): The time for performing a one-way hash function \( h \)
- \( T_{ep} \): 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>
<thead>
<tr>
<th>Table 1: Computational complexities</th>
<th>Proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>System initialize</td>
<td>( 2T_{ep} )</td>
</tr>
<tr>
<td>Proxy delegation</td>
<td>( 3T_{ep} + 5T_{mul} + 7T_{inv} + 3T_{d} )</td>
</tr>
<tr>
<td>Signing phase</td>
<td>( 2T_{ep} + 7T_{mul} + 2T_{inv} + 3T_{d} )</td>
</tr>
<tr>
<td>Verification phase</td>
<td>( 4T_{inv} + 6T_{mul} + 2T_{inv} + 5T_{d} )</td>
</tr>
</tbody>
</table>
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


