New Efficient Proxy Blind Signature Scheme Using Verifiable Self-certified Public Key

Jiguo Li[1] and Shuhong Wang[2]

(Corresponding author: Jiguo Li)

College of Computer and Information Engineering, Hohai University[1]
Nanjing 210098, China (Email: lijiguo@hhu.edu.cn, ljg1688@163.com)
School of Information System, SMU, Singapore (Email: shwang@smu.edu.sg)[2]

(Received Nov. 8, 2005; revised and accepted Dec. 16, 2005)

Abstract

Proxy blind signature, which combines the properties of both proxy signature and blind signature, is useful in e-cash and e-commerce. In this paper, we present a verifiable self-certified public key scheme and a proxy blind signature scheme using the verifiable self-certified public key. The self-certified public key has an advantage which can withstand public key substitution attacks. As far as we know, this is the first scheme that satisfies the security properties of both the proxy blind signature and verifiable self-certified public key. Another advantage is that the proposed verifiable self-certified public key scheme overcomes the weakness of repudiability of the self-certified public key. Analysis shows that our scheme are secure and efficient.

Keywords: Blind signature, cryptography, nonrepudiation, proxy signature, self-certified public key

1 Introduction

Mambo et al. [15] proposed the concept of proxy signature in 1996, which allows a designated person, called a proxy signer, to sign on behalf of an original signer. Lee et al. [8] showed that strong proxy signature scheme should have properties of strong unforgeability, verifiability, strong identifiability, strong undeniability and prevention of misuse. The proxy signature plays the important role in many applications [6, 8, 9] and has been received great attention since it was proposed. Sometimes, a proxy signature is needed on behalf of two or more original signers. In allusion to this problem, Yi et al. [32] proposed another type proxy scheme: proxy multi-signature scheme. In some practical applications, several proxy signers may be required to cooperatively sign message for sharing the responsibility or authority. The (t, n) threshold proxy signature scheme is designed to satisfy this requirement.

Zhang and Kim et al. [4, 33] firstly proposed a threshold proxy signature schemes in 1997, respectively. Sun et al. [21] showed that Zhang's threshold proxy signatures suffered from some weaknesses and gave a modified scheme. To avoid the abuse of signing capability, a proxy signature scheme should have the nonrepudiation property that provides the ability to identify the actual proxy signers of the proxy signature. Sun [20] proposed an efficient nonrepudiable threshold proxy signature scheme with known signers to achieve above goal. However, Hwang et al. [3] showed Sun's scheme had two disadvantages and proposed a modified scheme, which remedies the weakness of the Sun's scheme. Later, Wang and Fu [26] and Tan et al. [23] proposed an anonymity-revoking blind proxy signature scheme and proxy blind signature scheme, respectively. These two schemes are very suitable for e-commerce.

In 2003, Lal et al. [7] pointed out that Tan et al.'s scheme was insecure and also proposed a new proxy blind signature scheme based on Mambo et al.'s scheme. In 2004, Wang et al. [28] showed that the scheme [23] is insecure. In 2005, Sun et al. [22] showed that Tan et al.'s schemes didn't satisfy the unforgeability and unlinkability properties. Moreover, they also pointed out that Lal and Awasthi's scheme didn't possess the unlinkability property either. In 2004, Xue and Cao [31] showed there existed one weakness in Tan et al.'s scheme[23] and Lal et al.'s scheme[7] since the proxy signer can get the link between the blind message and the signature or plaintext with great probability. Xue and Cao introduced concept of strong unlinkability and they also proposed a proxy blind signature scheme. Compared with Tan et al's scheme and Lal et al's scheme, their scheme is more efficient. However, Li et al. [13] show their scheme [31] can't satisfy unforgeability and strong unlinkability properties. Recently, Li et al. [10, 11, 12] and Wang et al. [25, 27] showed that some proxy signature schemes[1, 4, 15, 21, 32] have the drawbacks of suffering from public key substitution attack, using secure channel etc. and proposed some new proxy signature schemes to overcome the above disadvantages.

Girault [2] pointed out that most of the public key cryptosystem are vulnerable to the so-called active attacks, such as the adversary attempts to substitute or modify a genuine public key by a fake one during key distribution. In order to avoid such attacks, authenticity of the user's public key must be verified. Girault proposed a self-certified public key system to resolve the problem of public key verification. Shao [19], Wu [29], Tseng et al [24], Wu and Hsu [30] designed some cryptographic schemes using the self-certified public key, respectively. However, one disadvantage of self-certified public key is their repudiability [16]. In the certificate-based schemes, the authenticity of the public key can be verified directly after knowing a witness. In self-certified schemes, the authenticity of the public key is verified at the same time, when the key is used for encryption, signature verification, key exchange or any other cryptographic application. For example, it is uncertain whether the signature or the public key is incorrect if the verification of a digital signature fails using a self-certified public key. Kim et al. [5] first presented new concept of verifiable self-certified public key to solve the above problem. Shao [19] also proposed a self-certified public key system to resolve the problem.

As mentioned previously, most of the above signature schemes are vulnerable to the public key substitution attacks. In allusion to this problem, this paper first presents a verifiable self-certified public key scheme. And then we propose a new proxy blind signature scheme, using the verifiable self-certified public key to erase the repudiability problem and eliminate the complex public key infrastructure.

The rest of this paper is organized as follows. In Section 2, we briefly list some security properties of the scheme. And then, a verifiable self-certified public key scheme is presented in Section 3. Section 4 is dedicated to the construction of the proxy blind signature scheme using the verifiable self-certified public key. In Section 5, we analyze the security and the properties of the proposed scheme. Finally Section 6 contains the conclusions.

2 Security Properties

Our scheme is a cryptographic primitive involving four entities: a system authority SA, an original signer, a proxy signer and a verifier V of the signature. In this section, we describe the required properties of the scheme as follows. The interested readers please refer to [8, 9, 15, 23, 28].

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

2) Nonrepudiation: Neither the original signer nor the proxy signer must be able to sign in place of the other party. In other words, they cannot deny their signatures against anyone.

3) Verifiability: The receiver of the signature should be able to verify the proxy signature in a similar way to the verification of the original signature.

4) Unforgeability: Only a designated proxy signer can create a valid proxy signature for the original signer (even the original signer cannot do it).

5) Identifiability: Anyone can determine the identity of the corresponding proxy signer from a proxy signature.

6) Prevention of misuse: It should be confident that proxy key pair should be used only for creating proxy signature, which conforms to delegation information. In case of any misuse of proxy key pair, the responsibility of proxy signer should be determined explicitly.

7) Unlinkability: When the signature is verified, the signer knows neither the message nor the signature associated with the signature scheme.

However, in order to protect the proxy signer and prevent misuse of the delegation right, a delegation warrant is necessary. And this warrant has to be included in the signature. As a result, with the view of warrant m_w, the signing transcripts $(m_w, \cdots)$ automatically links to the signature $(m_w, m, \cdots)$. Therefore, the unlinkability in a proxy blind signature should be defined among signatures with the same delegation specification, as follows.

Definition 1. *Suppose more than one signatures are generated using the same information from the original signer. Then a proxy blind signature scheme is said to satisfy unlinkability requirement, if among those signatures, the proxy signer could not associate his view during the signature generation to the generated signature. Distinguishing to the (global) unlinkability of ordinary blind signature scheme, we call the unlinkability of proxy blind signature scheme local unlinkability or proxy unlinkability.*

We will show that the proposed proxy blind signature using verifiable public key satisfy all above properties. Furthermore, the scheme also provides another property called *Self-certification and verifiability.* That is, the original signer's and the proxy signer's attributes (identity, secret key, public key etc.) satisfy a computational unforgeable relationship, which is verified implicitly during the proper use of keys in proxy signature scheme. Furthermore, if necessary, there is an efficient way to verify the authenticity of the public key after knowing a witness.

3 Verifiable Self-certified Public Keys

In this section, we present a *verifiable* self-certified public key scheme based on Wu's scheme [29], which overcomes the weakness of self-certified public key.

3.1 System Setup

System authority (SA) randomly selects two prime large numbers p, q such that $q|(p-1)$, a q-ordered generator g

in group Z_p^* and a secure hash function $h(\cdot)$. SA generates a secret key $\gamma \in_R Z_q$ and computes the public key $\beta = g^\gamma \pmod p$. After that, SA publishes p, q, g, β and $h(\cdot)$, while keeping γ secret.

3.2 Self-certified Key Pair Generations

Suppose that a user U with identity ID wants to register with SA. The procedure for user verifiable self-certified key generations is stated below:

1) U randomly selects an integer $b \in_R Z_q^*$ as the master key, computes $\nu = g^{h(b||ID)} \pmod p$ and sends it to SA.

2) Upon receiving (ID, ν), SA randomly selects a time-variant integer $t \in_R Z_q^*$, computes public key $y = \nu g^t - h(ID) \pmod p$ and its witness $\omega = t + \gamma(y + h(ID)) \pmod q$ for U and sends (y, ω) to U.

3) Upon receiving (y, ω), U computes his/her secret key $x = \omega + h(b||ID) \pmod q$ and verifies the authenticity of public key y by checking that
$$g^x = (y + h(ID))\beta^{y+h(ID)} \pmod p. \qquad (1)$$

4) U randomly selects an integer $k \in_R Z_q^*$, computes $r = g^k \pmod p$ and generates $(e, \tilde{s})$ as follows:
$$\begin{aligned} e &= h(r) \pmod q \\ \tilde{s} &= k - xe \pmod q. \end{aligned}$$
Then the verifiable self-certified key of U is $(e, \tilde{s}, y, ID)$.

3.3 Authenticity Verifications

Once encryption, signature verification, key exchange or any other cryptographic application fails, given $(e, \tilde{s}, y, ID)$, any verifier can verify the authenticity of public key by checking that
$$e = h(g^{\tilde{s}} \cdot ((y + h(ID))\beta^{y+h(ID)})^e) \pmod p. \qquad (2)$$

It is obviously that the proposed self-certified public key is verifiable, thus overcomes the general weakness of repudiability.

Theorem 1. *The secret key $x = \omega + h(b||ID)$ and public key $y = \nu g^t - h(ID)$ satisfies Equation (1).*

Proof. Substituting $\omega = t + \gamma(y + h(ID))$ into $x = \omega + h(b||ID)$, we have
$$x = t + \gamma(y + h(ID)) + h(b||ID) \pmod q. \qquad (3)$$

Raising both sides of Equation (3) as exponents to base g, and from the equation $y = \nu g^t - h(ID)$, it yields
$$\begin{aligned} g^x &= g^{t+\gamma(y+h(ID))+h(b||ID)} \pmod p \\ &= \nu g^t \beta^{y+h(ID)} \pmod p \\ &= (y + h(ID))\beta^{y+h(ID)} \pmod p \end{aligned}$$
which implies that Theorem 1 holds. □

Theorem 2. *The user U's verifiable self-certified key $(e, \tilde{s}, y, ID)$ satisfies the verification Equation (2).*

Proof. Raising both sides of Equation (2) to exponents to base g, it yields
$$\begin{aligned} r &= g^k = g^{\tilde{s}+xe} \pmod p \\ &= g^{\tilde{s}}(g^x)^e \pmod p \\ &= g^{\tilde{s}} \cdot ((y + h(ID))\beta^{y+h(ID)})^e \pmod p. \end{aligned}$$

Substituting the above result into the Equation (2), it derives Equation (2), which implies that Theorem 2 also holds. □

Remark 1. Using verifiable self-certified public key, the proxy signature scheme with message recovery and proxy signcryption schemes in [14] are easy to be modified as schemes using verifiable self-certified public keys.

4 Proxy Blind Signature Scheme Using Verifiable Self-certified Public Key

In this section, we propose a new proxy blind signature scheme based on the idea of the verifiable self-certified public key. The proposed scheme is divided into seven phases: system setup, user registration, proxy key generation, blind signing, signature extraction, signature verification and authenticity verification of public key. Before describe the complete scheme, we list the notations used throughout this paper for readers convenience.

- p, q : two large prime numbers, such that $q|(p-1)$.
- g : an element of Z_p^*, its order is q.
- $h(\cdot)$: a public cryptographically strong hash function.
- $\gamma \in {}_R Z_q$: SA's secret key.
- $\beta \equiv g^\gamma \pmod p$: SA's public key.
- ID_o, ID_p : original signer U_o's and proxy signer U_p's identities.
- $x_i, (i = o, p)$: U_i's secret keys, generated as in Section 3.2.
- $(e_i, \tilde{s_i}, y_i, ID_i)$: U_i's verifiable self-certified public key.
- $||$: the sign of string concatenation.

4.1 System Setup

System setup in this subsection is same to that of Subsection 3.1.

4.2 User Registration

Suppose that the original signer U_o with identity ID_o and the proxy signer U_p with identity ID_p want to register with SA. Then the registration procedure for them is exactly the self-certified key pair generation procedure in 3.2. We depict the outline below in Figure 1, where $i = o, p$.

U_i's secret key is x_i, and his/her verifiable self-certified public key is $(e_i, \tilde{s_i}, y_i, ID_i)$. For simplicity, we define $Y_i = (y_i + h(ID_i))\beta^{y_i+h(ID_i)}$, where $i = o, p$. The authenticity of the later is verified by the equation $e_i \overset{?}{=} h(g^{\tilde{s_i}} \cdot Y_i^{e_i})$.

$$\begin{array}{rcl}
\boldsymbol{U_i\,(ID_i)} & & \textbf{SA} \\
b_i \in_R Z_q^*, \nu_i = g^{h(b_i||ID_i)} & \xrightarrow{(ID_i,\,\nu_i)} & t_i \in_R Z_q^* \\
 & & y_i = \nu_i g^{t_i} - h(ID_i) \\
x_i = \omega_i + h(b_i||ID_i) & \xleftarrow{(y_i,\,\omega_i)} & \omega_i = t_i + \gamma(y_i + h(ID_i)) \\
g^{x_i} \overset{?}{=} (y_i + h(ID_i))\beta^{y_i+h(ID_i)}(= Y_i) & & \\
\text{if true, } \tilde{k_i} \in_R Z_q^*, \tilde{r_i} = g^{\tilde{k_i}} & & \\
(e_i = h(\tilde{r_i}) \text{ and } \tilde{s_i} = \tilde{k_i} - x_i e_i) & &
\end{array}$$

Figure 1: The user registration

4.3 Proxy Key Generation

The proxy signing key pair (x', Y') is generated as follows.

1) Original signer U_o randomly chooses $k_o \in_R Z_q^*$, and computes:

$$\begin{array}{rcl} r_o & = & g^{k_o} \pmod p \\ s_o & = & x_o + k_o \cdot h(m_\omega||r_o). \end{array}$$

2) U_o sends (r_o, s_o) along with warrant m_ω to the proxy signer U_p.

3) U_p checks $g^{s_o} = Y_o r_o^{h(m_\omega||r_o)} \pmod p$.

   If it is correct, U_p accepts it and computes

$$x' = s_o + x_p \tag{4}$$

   as his proxy signature secret key. Note that the corresponding proxy public key is $Y' = Y_o Y_p r_o^{h(m_\omega||r_o)} = g^{x'} \pmod p$.

Please refer to Figure 2 for the outline of this phase and that of the following three phases as well.

4.4 Blind Signing

1) U_p chooses a random number $k_p \in {}_R Z_q^*$, computes

$$r_p = g^{k_p} \pmod p \tag{5}$$

   and then sends r_p to the user V. We assume (m_ω, r_o) be published by the original signer, V can read it whenever needed.

2) **Blinding**. To obtain the blind signature of m from proxy signer U_p. V chooses three random numbers $a, b, c, \in {}_R Z_q^*$, and computes

$$r = r_p^a g^b (Y')^{-c} \pmod p, \tag{6}$$

   where Y' computed as $Y_o Y_p r_o^{h(m_\omega||r_o)} \pmod p$. If $r = 0$, the user V should select a, b and c again. Once r, a, b and c are determined, the V computes

$$\tilde{e} = h(r||m) \tag{7}$$

   and

$$e^* = (\tilde{e} + c)/a \pmod p. \tag{8}$$

   Then V delivers e^* to the proxy signer U_p .

3) **Signing**. After receiving e^* , U_p computes

$$s' = -e^* x' + k_p \tag{9}$$

   and sends it to the user V.

4.5 Signature Extraction

While receiving s' , V computes

$$s = s'a + b \pmod q. \tag{10}$$

Then, the proxy blind signature is $(m_\omega, r_o, m, \tilde{e}, s)$ denoted by σ.

4.6 Signature Verification

The recipient of a proxy blind signature verifies the validity of $\sigma = (m_\omega, r_o, m, \tilde{e}, s)$ by checking

$$\tilde{e} \overset{?}{=} h(g^s Y'^{\tilde{e}}||m) \pmod p.$$

Where $Y' = Y_o Y_p r_o^{h(m_\omega||r_o)} \pmod p$. If it is true, the verifier accepts it as a valid proxy blind signature, otherwise rejects.

4.7 Authenticity Verification of Public Key

Once proxy blind signature verification fails, given $(e_i, \tilde{s_i}, y_i, ID_i)(i = o, p)$, any verifier can verify the authenticity of public key y_i by checking if the equation $e_i = h(g^{\tilde{s_i}} \cdot Y_i^{e_i})$holds. If the above equation don't hold,then recall $Y_i = (y_i + h(ID_i))\beta^{y_i+h(ID_i)}$.

Correctness: If every participant performs honestly as above, then σ is a valid proxy blind signature on m, and as the warrant m_ω specifying, U_o is the original signer, U_p is the proxy signer. This is because $Y' = Y_o Y_p r_o^{h(m_\omega||r_o)}$ $\pmod p$, then

$$\begin{array}{rcl}
h(g^s Y'^{\tilde{e}}||m) & = & h(g^{a(k_p - e^* \cdot x') + b} Y'^{\tilde{e}}||m) \\
 & = & h(r_p^a g^b (Y')^{-ae^*} Y'^{\tilde{e}}||m) \\
 & = & h(r_p^a g^b (Y')^{-(\tilde{e}+c)} Y'^{\tilde{e}}||m) \\
 & = & h(r_p^a g^b (Y')^{-c}||m) \\
 & = & h(r||m) \\
 & = & \widetilde{e}
\end{array}$$

Signer U_o		**Signer U_p**
$k_o \in {}_R Z_q^*, r_o = g^{k_o} \pmod p$		
$s_o = x_o + k_o \cdot h(m_\omega \Vert r_o)$	$\xrightarrow{m_\omega, r_o, s_o}$	$g^{s_o} \overset{?}{=} Y_o r_o^{h(m_\omega \Vert r_o)} \pmod p$
		If false, stop; Otherwise,
		$x' = s_o + x_p$
User V		**Signer U_p**
$a, b, c, \in {}_R Z_q^*$	$\xleftarrow{m_\omega, r_o, r_p}$	$k_p \in {}_R Z_q^*, r_p = g^{k_p} \pmod p$
$r = r_p^a g^b (Y')^{-c} \pmod p$		
$\tilde{e} = h(r \Vert m)$		
$e^* = (\tilde{e} + c)/a$	$\xrightarrow{e^*}$	$s' = -e^* x' + k_p$
$s = s'a + b$	$\xleftarrow{s'}$	

Figure 2: The message flows of the proxy blind signature scheme

5 Analysis

5.1 Security of Secret Keys

Computing SA's secret key γ from public key β is based on the intractability of solving the discrete logarithm problem (DLP). In the user registration phase, γ is protected by the time-variant integer $t_i \in_R Z_q^*$ whose security is based on the intractability of solving the DLP problem. Thus, under the DLP assumption, it is computationally infeasible to reveal γ from all available public information. As one can notice that the original signer's and the proxy signer's master key $b_i \in_R Z_q^* (i = o, p)$ are protected by DLP assumption and the one-way hash function assumption. The original signer's and the proxy signer's secret key $x_i = \omega_i + h(b_i, ID_i)$ are protected by the master key and the one-way hash function assumption. If an adversary attempts to reveal the proxy signature key x' and original signer's secret key x_o from the equations $s' = e^* x' + k_p$ and $s_o = x_o + k_o \cdot h(m_\omega || r_o)$ respectively, he/she must know the random number $k_o, k_p \in_R Z_q^*$, which is obviously impossible.

5.2 Security of the Signature Scheme

The security of our scheme is based on the security of Schnorr digital signature and Schnorr blind signature.

In fact, (r_o, s_o) of the proxy delegation phase is exact a Schnorr digital signature of message m_ω, under the public key Y_o . And obviously, (r_o, x') can also be regarded as a Schnorr signature on message m_ω, but under the public key $Y_o Y_p$. One who can forge a proxy signing key pair(x', Y') must be able to forge suitable (m_ω, r_o) to satisfy the equation $Y' = Y_o Y_p r_o^{h(m_\omega || r_o)} \pmod p$. Thus, one can succeed if and only if he can break Schnorr signature or he can obtain the discrete logarithm of $Y_o Y_p$ modulo p. Based on the security of Schnorr signature, the former is intractable. As for the latter approach, even with the knowledge of one secret, say x_o , the original signer U_o is still not able to extract $x_o + x_p \pmod q$, otherwise, U_o obtains the secret key of signer U_p, which is impossible.

On obtaining the security of the proxy signing key pair (x', Y'), the remainder signing phases is only an blind signature using this key pair. To make this clear, we note that r_o is included in the signature just for the purpose of proxy public key Y' reconstruction. And $(\tilde{e}, s)$ is similar with Schnorr blind signature on message m , using the public key $Y' = Y_o Y_p r_o^{h(m_\omega || r_o)} \pmod p$. It is proved to be secure by Pointcheval and Stern [17, 18].

However, the proof of Pointcheval et al. in [17, 18] does not consider the case of fake public keys (say, the adversary forge a public key without knowing the corresponding secret key). Note that our scheme avoids such kind of attack. This is exactly the role of verifiable self-certified public key scheme in the user registration phase (Section 4.2). In fact, if without this phase, the public key substitution attack is mountable. Suppose the adversary is original signer, he can simply impersonate as proxy signer using proxy signing key pair $(s \in_R Z_q^*, g^s)$ and substitute his public key to be $Y_o' = g^s Y_p^{-1} r_o^{-h(m_\omega || r_o)}$. Of course the adversary do not know the x_o' satisfying $g^{x_o'} = Y_o'$.

5.3 Security Properties of the Scheme

In this subsection, we show that our scheme satisfies all properties announced in Section 2.

Proxy Distinguishability: On the one hand, warrant m_ω is included in proxy blind signature $\sigma = (m_\omega, r_o, m, \tilde{e}, s)$. On the other hand, proxy signature public key $Y' = Y_o Y_p r_o^{h(m_\omega || r_o)}$ includes original signer public key Y_o and proxy signer public key Y_p. So the proxy signature is easy to be distinguishable from the normal signature.

Nonrepudiation: From Section 5.1, we know that the original signer does not obtain the proxy signer's secret key x_p and proxy signer does not obtain original signer's secret key x_o. Thus, neither the original signer nor the proxy signer can sign in place of the other party.

Verifiability: Verifiability of the scheme sees in the Sections 3.3 and 4.7.

Table 1: Computational costs comparison

Schemes	delegation	blind signing	verification	Total costs
Scheme [23]	$4T_E + 3T_M$	$7T_E + 6T_M + 1T_H$	$3T_E + 3T_M + 1T_H$	$14T_E + 12T_M + 2T_H$
Our scheme	$3T_E + 2T_M + 2T_H$	$5T_E + 6T_M + 2T_H$	$3T_E + 3T_M + 2T_H$	$11T_E + 11T_M + 6T_H$
Difference	$1T_E + 1T_M - 2T_H$	$2T_E - T_H$	$-1T_H$	$3T_E + 1T_M - 4T_H$

Unforgeability: An adversary (including the original signer) wants to impersonate the proxy signer to sign the message m. He can intercept the delegation pair (m_ω, r_o, s_o), but he cannot obtain the proxy signature secret key x' from Equation (4), since there is still an unknown x_p to the adversary in Equation (4). Because of $x_p \in_R Z_q^*$, the adversary can obtain the proper proxy signature secret key by guessing it with at most a probability $1/q$. That is, anyone else (even the original signer) can forge the proxy signature successfully with a probability $1/q$.

Identifiability: On the one hand, warrant m_ω includes original signer U_o's and proxy signer U_p's identities information ID_o, ID_p. On the other hand, proxy signature public key $Y' = Y_o Y_p r_o^{h(m_\omega || r_o)}$ includes original signer public key Y_o and proxy signer public key Y_p. Hence, anyone can determine the identity of the corresponding proxy signer from a proxy signature.

Prevention of misuse: The proposed scheme can prevent proxy key pair misuse, because the warrant m_ω includes original signer U_o's and proxy signer U_p's identities information ID_o, ID_p, message type to be signed by the proxy signer, delegation period, etc.

Proxy Unlinkability: During generation of the signature $\sigma = (m_\omega, r_o, m, \tilde{e}, s)$, the proxy signer has the view of transcripts $(m_\omega, r_o, r_p, e^*, s')$. Since (m_ω, r_o) are specified by the original signer for all the signatures under the same delegation condition. The *proxy unlinkability* holds if and only if there is no conjunction between (r_p, e^*, s') and $(m_\omega, r_o, m, \tilde{e}, s)$. This is obvious from equations Equations (5)-(10). More detailed, the value r_p is only included in Equation (6) and connected to $\tilde{e}$ through Equation (7). For this, one must be able to compute r which however is masked with three random numbers. Similarly, e^* and s' may be associated with the signature through Equation (8) and (10) respectively. They fail again due to the random numbers. Even they are combined, the number of unknowns is still one more than that of the equations. So, the proposed scheme provides indeed the proxy blindness property.

5.4 Efficiency

Our scheme is more efficient as compared to the scheme of Tan et al. [23] which was newly proposed in literature. The detailed costs in each phase are compared in Table 1. The user registration phase is a particular of our scheme, thus not be involved in the comparison.

In the table, T_E and T_M denote the once running of modulo exponential and multiplication operations, respectively. T_H denotes a one time running of hash operations. The modulo-additions are omitted due to its high performance. Also note that all the minus exponential operations can be transformed to positive exponential operations without losing almost any efficiency (modulo q).

From the table, we notice that each phase of the proposal has less computational cost than of the TLT scheme [23] except in the verification phase, in which one more hash operation is needed in our scheme. It is noteworthy that in the blind signing phase of our protocol, one modulo inverse is not counted. This is due to the typeset of our table, since only one inverse involved. With great concession, we can add one exponential operation instead. Even in this way, the improvement is still much more efficient ($2T_E + 1T_M - 4T_H$ computation less) than the TLT scheme.

6 Conclusion

In this paper, the authors show advantage and disadvantage of self-certified public key introduced by Girault and present a verifiable self-certified public key scheme, which overcomes the weakness of self-certified public key. Furthermore, on basis of the idea of proxy blind signature and verifiable self-certified public key, we present a new proxy blind signature scheme, which satisfies the given security properties. The proposed scheme has merit that the original signer and the proxy signer's public key can simultaneously be authenticated in verifying proxy blind signature process, which make the proposed scheme withstand public key substitution attack, active attacks, and forgery attacks. In addition, the proposed scheme does not use secure channel in the communication between the original signer and the proxy signature signer. Thus, it is very suitable for e-cash and e-commerce.

References

[1] W. K. Chan, and V. K. Wei, "A threshold proxy signcryption," in *Proceedings of 2002 International Conference on Security and Management (SAM'02), Monte Carlo Resort*, Las Vegas, Nevada, USA, pp. 24-27, June 2002.

[2] M. Girault, "Self-certified public keys," in *Advances in Cryptology-Eurocrypt'91*, pp. 491-497, 1991.

[3] M. S. Hwang, I. C. Lin, and E. J. L. Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers," *International Journal of Informatica*, vol. 11, no. 2, pp. 1-8, 2000.

[4] S. Kim, S. Park, and D. Won, "Proxy signatures, revisited," *in ICICS'97*, LNCS 1334, pp. 223-232, Springer-Verlage, 1997.

[5] S. Kim, S. H. Oh, S. Park, and D. Won, "Verifiable self-certified public key," in *Proceedings of INRIA Workshop on Coding and Cryptography (WCC'99)*, pp. 139-148, 1999.

[6] H. Kim, J. Baek, B. Lee, and K. Kim, "Computing with secrets for mobile agent using one-time proxy signature," in *Proceedings of SCIS'2001*, pp. 845-850, 2001.

[7] S. Lal, and A. K. Awasthi, "Proxy blind signature scheme," http:// eprint.iacr.org/2003/072.pdf.

[8] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its application," in *Proceedings of SCIS'2001*, pp. 603-608, 2001.

[9] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strong non-designated proxy signature," in *Proceedings of ACISP2001*, LNCS 2119, pp. 474-486, Springer-Verlage, 2001.

[10] J. G. Li, Z. F. Cao, and Y. C. Zhang, "Improvement of M-U-O and K-P-W proxy signature schemes," *Journal of Harbin Institute of Technology*, vol. 9, no. 2, pp. 145-148, 2002.

[11] J. G. Li, Z. F. Cao, and Y. C. Zhang, "Nonrepudiable proxy multi-signature scheme," *Journal of Computer Science and Technology*, vol. 18, no. 3, pp. 399-402, 2003.

[12] J. G. Li, J. Z. Li, Z. F. Cao, and Y. C. Zhang, "Nonrepudiable threshold proxy signcryption scheme with known signers," *Journal of Software*, vol. 14, no. 12, pp. 2021-2027, 2003.

[13] J. G. Li, Y. C. Zhang, and S. T. Yang, "Cryptanalysis of new proxy blind signature scheme with warrant," in *ICCMSE'2005*, accepted, Athens, Greece, 2005.

[14] J. G. Li, Y. C. Zhang, and Y. L. Zhu, "A new proxy signature scheme with message recovery using self-certified public key," *Wuhan University Journal of Natural Sciences*, vol. 10, no. 1, pp. 210-222, 2005.

[15] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," *IEICE Transaction on Fundamentals*, vol. E79-A, no. 9, pp. 1338-1354, 1996.

[16] H. Petersen, and P. Horster, "Self-certified keys-concepts and pplications," in *Proceedings of the 3rd Confonference on Communications and Multimedia Security. Chapman & Hall*, pp. 22-23, Sep. 1997.

[17] D. Pointcheval, and J. Stern, "Provably secure blind signature schemes," in *Proceedings of Asiacrypt'1996*, LNCS 1163, pp. 252-265, Springer-Verlage, 1996.

[18] D. Pointcheval, and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361-396, 2000.

[19] Z. Shao, "Cryptographic systems using a self-certified public key based on discrete logarithms," *IEE Proceedings-Computers and Digital Techniques*, vol. 148, no. 6, pp. 233-237, 2001.

[20] H. M. Sun, "An efficient nonrepudiable threshold proxy signature scheme with known signers," *Computer Communications*, vol. 22, no. 8, pp. 717-722, 1999.

[21] H. M. Sun, N. Y. Lee, and T. Hwang, "Threshold proxy signatures," *IEE Proceedings-Computers and Digital Techniques*, vol. 146, no. 5, pp. 259-263, 1999.

[22] H. M. Sun, B. T. Hsieh and S. M. Tseng, "On the security of some proxy signature schemes," *Journal of System and Software*, vol. 74, pp.297-302, 2005.

[23] Z. W. Tan, Z. J. Liu, and C. M. Tang, "A proxy blind signature scheme based on DLP," *Journal of Software*, vol. 14, no. 11, pp. 1931-1935, 2003.

[24] Y. M. Tseng, J. K. Jan, and H. Y. Chien, "Digital signature with message recovery using self-certified public keys and its variants," *Applied Mathematics and Computation*, vol. 136, pp. 203-214, 2003.

[25] G. L. Wang, F. Bao, J. Y. Zhou, and R. H. Deng, "Security analysis of some proxy signatures," in *Information Security and Cryptology(ICISC2003)*, LNCS 2971, pp. 305-319, Springer-Verlage, 2004.

[26] X. M. Wang, and F. W. Fu, "An anonymity-revoking blind proxy signature scheme," *Chinese Journal of Computers*, vol. 26, no. 1, pp. 51-54, 2003. (in Chinese with English abstract).

[27] S. H. Wang, G. L. Wang, F. Bao, and J. Wang, "Cryptanalysis of a proxy-protected proxy signature scheme based on elliptic curve cryptosystem," in *IEEE Vehicular Technology Conference*, Los Angeles, CA, USA, vol. 5, pp. 3240-3243, 2004.

[28] S. H. Wang, G. L. Wang, F. Bao, and J. Wang, "Cryptanalysis of a proxy blind signature scheme based on DLP," *Journal of Software*, vol. 16, no. 5, pp. 911–915, 2005.

[29] T. C. Wu, "Digital signature/multisignature schemes giving public key verification and message recovery simultaneously," *International Journal of Computer Systems Science & Engineering*, vol. 16, no. 6, pp. 329-337, 2001.

[30] T. S. Wu, and C. L. Hsu, "Threshold signature scheme using self-certified public keys," *Journal of System and Software*, vol. 67, pp. 89-97, 2003.

[31] Q. S. Xue, and Z. F. Cao, "A new proxy blind signature scheme with warrant," in *2004 IEEE Conference on Cybernetics and Intelligent Systems (CIS and RAM 2004)*, Singapore, pp. 1385-1390, 2004.

[32] L. J. Yi, G. Q. Bai, and G. Z. Xiao, "Proxy multi-signature scheme: A new type of proxy signature scheme," *Electronics Letters*, vol. 36, no. 6, pp. 527-528, 2000.

[33] K. Zhang, "Threshold proxy signature schemes," in *1997 Information Security Workshop*, pp. 191-197, 1997.

Jiguo Li is an associate professor in College of Computer & Information Engineering, Hohai University, China. He received his B.S. degree in application mathematics from Heilongjiang University, Harbin, China in 1992 and his M.S. degree in pure mathematics from Harbin Institute of Technology, Harbin, China in 2000. He received his Ph.D. degree in computer software and theory form Harbin Institute of Technology, Harbin, China in 2003. His research interests include cryptography theory and its application, secure electronic commerce and digital watermarking etc.

Shuhong Wang is a post-doctoral fellow with School of Information Systems (SIS), Singapore Management University (SMU). He received his PhD in Mathematics from Peking University, July 2005. He was a Research Assistant in the Institute for Infocomm Research and then SIS/SMU from 2003 to June 2005. His research interests include cryptography and its application in information security.