# Partial Blind Proxy Re-signature Scheme for Mobile Internet

Yanfang Lei[1], Zhijuan Jia[1(✉)], Lipeng Wang[1], Bei Gong[2], Yage Cheng[1], and Junjun Fu[1]

[1] Zhengzhou Normal University, Zhengzhou 450044, China
jzj523@163.com
[2] Beijing University of Technology, Beijing 100124, China

**Abstract.** Aiming at the problems of limited computing power and high security requirements of mobile Internet mobile terminal devices, we propose a server-assisted verification partial blind proxy re-signature scheme. Partial blind proxy re-signature algorithm protects both the trustee's privacy message and the agent's legal rights. In the server-assisted authentication protocol, the verifier transfers the complex bilinear pairing operation task to the server through the interaction, thereby reducing the amount of computation of the verifier. The numerical experiments show that the verification efficiency of the new scheme is improved by at least 71% and 74%, respectively, compared with the Yang's and Feng's schemes.

**Keywords:** Server-assisted authentication protocol · Partial blind proxy re-signature · Completeness · Unforgeability

## 1 Introduction

The development of mobile communication technology is changing with each passing day. Mobile terminals such as Ipad, smart phones, wireless sensors, and electronic keys have become an indispensable part of our lives and work. The rise of e-commerce and e-government has brought people from the real material world into a convenient electronic age. Through the network, you can conduct online shopping, stock operations, communication and access to network resources anytime and anywhere. However, due to the limitations of the mobile Internet terminal device itself, the computing power is generally weak, which makes it necessary for people to perform a large amount of time for verification in resource request and resource access. On the other hand, due to the intricate growth environment of the mobile Internet, this puts higher requirements and standards on the security of the mobile Internet. Therefore, it is necessary to design a solution that can solve terminal computing power, limited energy supply and high security to be applied in the mobile Internet environment.

A secure server-assisted verification signature scheme was given in [1]. However, this scheme does not satisfy the conditions of collusion against server and signer. Later, in [2], Niu proposed a server-assisted verification signature scheme and the scheme can resist the attack, but the scheme needs to consume large broadband expenditure. Combined with aggregation signature and server-assisted verification signatures, Yang


W. Han et al. (Eds.): CTCIS 2019, CCIS 1149, pp. 16–30, 2020.
https://doi.org/10.1007/978-981-15-3418-8_2

et al. proposed a cryptosystem to save broadband expenditure in [3], which combines different signatures corresponding to multiple messages into one signature to reduce broadband expenditure, thus saving verification time and improving verification efficiency.

Agent re-signature is an important research direction of cryptography. Domestic and foreign scholars have done a lot of work in this direction. The security model of proxy re-signature was firstly proposed in [4], and two schemes with strict security under the random oracle model are given in this paper. A general combinable proxy re-signature scheme was proposed in [5]. However, some scholars have found that this scheme does not satisfy the conditions of unforgeability. In order to overcome this problem, a modification of the above scheme was proposed in the literature [6]. In recent years, the wide practicality of proxy re-signature has attracted the attention of scholars. Some proxy re-signature schemes with special properties have been proposed successively, such as proxy-based signature scheme based on polynomial isomorphism [7], lattice-based proxy re-signature [8], identity-based proxy re-signature [9], etc. However, these identity-based or certificate-based proxy re-signature schemes have issues such as certificate management and key escrow. In order to overcome these problems, a non-certificate proxy re-signature scheme with aggregation properties was designed in [10]. Effectively reduce the computational cost and communication cost in the verification process. In addition, Mi et al. proposed a blind proxy re-signature scheme in [11] in order to avoid the proxy getting the details of the converted message. However, the verifier in this scheme is pre-designated, which has limitations and low security in practical application. In addition, in order to avoid the agent obtaining the detailed content of the converted message, Mi et al. proposed a blind proxy re-signature scheme in [11]. However, the verifier in this scheme is pre-designated, which has limitations and low security in practical application. Aiming at this problem, in [12], the authors gave a partially blind proxy re-signature scheme with security. This scheme not only realizes the conversion of the signature between the trustee and the agent when the message content is not public. Moreover, the trustee's illegal use of the re-signature is effectively prevented. However, in the signature verification algorithm of this scheme, 4 bilinear pairing operations are needed, which is time-consuming and cannot be well applied to mobile Internet. Therefore, it is necessary to design a scheme that can reduce the verification overhead in partial blind proxy re-signature.

This paper combines the server-assisted authentication protocol and the partial blind proxy re-signature algorithm, and proposes a server-assisted verification part blind proxy re-signature scheme for low-end devices, and gives the security proof of the scheme. In the process of server-assisted verification protocol, the verifier and the server transfer the complex bilinear pairing operation task to the server through the interaction protocol between them, which makes the verifier verify the signature with a small computational cost and improves the verification efficiency of the signature. The verification algorithm reduces complex double-pair operations and has lower computational time overhead, so it can be better adapted to the mobile Internet environment.

## 2 Preliminaries

### 2.1 Bilinear Pairings

Let $p$ be a large prime, $G_1$ and $G_2$ are two $p$-ordered cyclic groups, and $g$ is a generator of group $G_1$. $e : G_1 \times G_2 \rightarrow G_2$ is a bilinear map and satisfies the following conditions:

(1) Bilinear: For arbitrary $x, y \in Z_q^*$, satisfied $e(g^x, g^y) = e(g, g)^{xy}$.
(2) Non-degenerate: There exist $g_1, g_2 \in G_1$, which satisfied $e(g_1, g_2) \neq 1$.
(3) Computability: There exists a valid algorithm $e(g_1, g_2)$, where $g_1, g_2 \in G_1$.

### 2.2 CDH Hypothesis

**Definition 1 (CDH problem):** For any unknown $x, y \in Z_q^*$, when $(g, g^x, g^y) \in G_1^3$ is known, we can calculate $g^{xy} \in G_1$.

**Definition 2 (CDH Hypothesis):** The CDH problem in the group $G_1$ can be solved with a large probability in polynomial time. The algorithm that satisfies the above conditions does not exist.

## 3 Scheme Model and Security Definitions

### 3.1 Server-Assisted Verification Partial Blind Proxy Re-signature Scheme

Combined with partial blind proxy re-signature algorithm and server-assisted authentication protocol, this paper proposes a partial blind proxy re-signature scheme for mobile internet. The participating entities involved in the scheme are the principal Bob, the trustee Alice, the verifier (SV), the semi-trusted proxy (P), and the server (SS). The details are as follows:

(1) The system parameter $cp$ required by the signature algorithm is obtained through the initialization process, then disclosed the parameter $cp$.
(2) According to the disclosed system parameter $cp$, the user obtains the public and private key pairs $(pk, sk)$ of the user by running a key generation algorithm.
(3) Generate a re-signature key $rk_{A \rightarrow B}$ for the agent by running the re-signature key algorithm by the given private keys $sk_A$ , $sk_B$ of principal and trustee.
(4) According to the public parameter $cp$, the trustee and the agent output a common message $c$ by running an agreed message algorithm.
(5) The signature $\sigma$ is obtained by running the signature algorithm by public message $c$, signature message $m$ and private key $sk$.
(6) Given a blinding factor $\kappa$, Alice obtains the blinded message $x$ corresponding to the message $m$ and the blinded signature $\sigma'_A$ corresponding to the message $m, c$ by running the blinding algorithm, and sends $(x, \sigma'_A)$ to the agent.

(7) Firstly, we should judge $\sigma'_A$ whether a legal signature corresponding to the trustee's public key $pk_A$, and if it is not a legal signature, output 0; if it is a legal signature, the agent obtains a partial blind proxy re-signature $\sigma'_B$ by running a re-signature generation algorithm.
(8) The trustee uses the blinding factor $\kappa$ to process the partial blind proxy re-signature to obtain the signature $\sigma_B$ of the signed message $m$ and the public message $c$.
(9) The verifier verifies whether the signature $\sigma$ is a legal signature that corresponding to the public key $pk$ for the signed message $m$ and the public message $c$. If it is a legal signature, output 1; otherwise, it outputs 0.
(10) Generate server-assisted authentication parameters: from $cp$, generate a string $vst$ for the verifier through this process.
(11) Server-assisted authentication protocol: for string $vst$, public key $pk$ and message signature pairs $(m, \sigma)$, if the server lets the verifier determine that $\sigma$ is a valid signature, output 1; otherwise, output 0.

### 3.2 Security Definition

The security of the server-assisted verification part of the blind proxy re-signature should at least include the unforgeability of the proxy re-signature, the partial blindness and the completeness of the server-assisted authentication protocol. Unforgeability guarantees that an attacker cannot generate a legal signature for a new message. Partial blindness ensures that the agent generates a re-signature of the message without knowing the content of the converted message, and the agent cannot match the final re-signature of the message with a partial blind proxy re-signature. The completeness of the so-called server-assisted authentication protocol means that the server cannot enable the verifier to determine the legality of an illegal signature.

The unforgeability and partial blindness of proxy re-signature have been proved in [12]. In [13], the completeness of the server-assisted verification protocol under joint attack and adaptive selection message attack was defined by designing two games Game1 and Game2.

**Definition 1:** If the attacker's probability of winning in Game1 and Game2 in the literature [13] approaches, the server-assisted verification protocol in the scheme is said to be complete.

**Definition 2:** If the server-assisted verification part of the blind proxy re-signature scheme satisfies the following two conditions at the same time, it indicates that the scheme is secure under collusion attacks and selective message attacks.

(1) In the case of adaptive selection of message attacks, there is both unforgeability and partial blindness.
(2) The server-assisted verification protocol is complete.

## 4 Partial Blind Proxy Re-signature Scheme

In this part we construct a partial blind proxy re-signature scheme that is both secure and efficient and adapts to the mobile Internet environment. The bit length of the signature message is taken as $n_m bit$, and the bit length of the public message is $n_{m_1} bit$. Use the anti-collision hash function $H_1 : \{0,1\}^* \rightarrow \{0,1\}^{n_m}$ and $H_2 : \{0,1\}^* \rightarrow \{0,1\}^{n_{m_1}}$ to extend the fixed length of the message $m$ and $c$ to any length to enhance the flexibility of the solution.

(1) *Setup*: Given security parameter $\lambda$, disclose system parameter $(cp) = (e, p, G_1, G_2, g, g_1, u^*, u_1, \ldots, u_{n_m}, \mu^*, \mu_1, \ldots, \mu_{n_{m1}})$, where $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map, $G_1, G_2$ are cyclic groups which prime number is $p$, $g$ is a generator element of $G_1$, and $g_1$ is an element of the cyclic group $G_1$. $u^*, u_1, \ldots, u_{n_m}, \mu_1, \ldots, \mu_{n_{m_1}}$, which are randomly selected elements in the cyclic group $G_1$.

(2) *Keygen*: The user randomly selects $\alpha \in Z_p^*$ and obtains the corresponding public-private key pair $(pk, sk) = (g^\alpha, \alpha)$.

(3) *Rekey*: After inputting the private keys $sk_A = a$ and $sk_B = b$ of Alice and Bob, and outputting a re-signature key $rk_{A \rightarrow B} = \frac{b}{a} \bmod p$ of the agent, however, Alice and Bob's private key are not disclosed to the agent P in the process.

(4) *Agree*: Alice and Bob agree on a message $c = (c_1, c_2, \ldots, c_{m_1}) \in \{0,1\}^{n_{m_1}}$ with a bit length of $n_{m_1} bit$.

(5) *Sign*: Given the signed message $m$ and the public message $c$, Alice then randomly selects $\varepsilon_1, \varepsilon_2 \in Z_p^*$ and then uses Alice's private key $sk_A = a$ to calculate $\sigma_{A1} = g_1^a \left( u^* \prod_{i=1}^{n_m} u_i^{m_i} \right)^{\varepsilon_1} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\varepsilon_2}$, $\sigma_{A2} = g^{\varepsilon_1}$ and $\sigma_{A3} = g^{\varepsilon_2}$, finally, outputting the original signature $\sigma_A = (\sigma_{A1}, \sigma_{A2}, \sigma_{A3})$ of the message $m$ and $c$.

(6) *Blind*: For a signed message $m$ and $c$ are with bit lengths $n_m bit, n_{m_1} bit$ respectively. Alice randomly selects a blinding factor $\kappa \in Z_p^*$, calculates a blind message $x = \left( u^* \prod_{i=1}^{n_m} u_i^{m_i} \right)^{\kappa}$ of the signed message $m$, and then randomly selects $\gamma_m, \gamma_{m_1} \in Z_p^*$, calculates $\sigma'_{A1} = g_1^a x^{\gamma_m} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\gamma_{m1}}$, $\sigma'_{A2} = g^{\gamma_m}$ and $\sigma'_{A3} = g^{\gamma_{m_1}}$ finally, sends the blind message $x$, public message $c$, and blind signature $\sigma'_A = \left(\sigma'_{A1}, \sigma'_{A2}, \sigma'_{A3}\right)$ to the agent P.

(7) *Resign*: After the agent P receives the blind message $x$, the public message $c$ and the blind signature $\sigma'_A = \left(\sigma'_{A1}, \sigma'_{A2}, \sigma'_{A3}\right)$ then verifies whether the equation

$$e\left(\sigma'_{A1}, g\right) = e(g_1, pk_A) e\left(x, \sigma'_{A2}\right) e\left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, \sigma'_{A3} \right) \tag{1}$$

is established, if not, output 0; if it is established, randomly selected $\gamma'_m, \gamma'_{m_1} \in Z_p^*$, then use the re-signature key $rk_{A\to B}$ to calculate $\sigma'_{B1} = \left(\sigma'_{A1}\right)^{rk_{A\to B}} x^{\gamma'_m} \left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\gamma'_{m_1}}$, $\sigma'_{B2} = \left(\sigma'_{A2}\right)^{rk_{A\to B}} g^{\gamma'_m}$ and $\sigma'_{B3} = \left(\sigma'_{A3}\right)^{rk_{A\to B}} g^{\gamma'_{m_1}}$ then send the partial blind proxy re-signature to Alice.

(8) *Unblind*: After receiving a partial blind proxy re-signature sent by the agent P, Alice uses Bob's public key $pk_B$ to verify whether the equation

$$e\left(\sigma'_{B1}, g\right) = e(g_1, pk_B) e\left(x, \sigma'_{B2}\right) e\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, \sigma'_{B3}\right) \tag{2}$$

is established, if the equation is not established, it means that $\sigma'_B$ is an invalid signature, and Alice refuses to accept it; if the equation is established, then randomly selects $\lambda \in Z_p^*$ which satisfied $\varepsilon_1 = \kappa\gamma_m + \lambda$ and $\varepsilon_2 = \gamma_{m_1} + \kappa\lambda$. The following is a blinding of partial blind proxy re-signatures. From calculating $\sigma_{B1} = \left(\sigma'_{B1}\right) \left(\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}\right)\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\kappa}\right)^{\lambda}$, $\sigma_{B2} = \left(\sigma'_{B2}\right)^{\kappa} g^{\lambda}$ and $\sigma_{B3} = \left(\sigma'_{B3}\right) g^{\kappa\lambda}$, we can obtain a re-signature $\sigma_B = (\sigma_{B1}, \sigma_{B2}, \sigma_{B3})$ of the public message and the signed message.

(9) *Verify*: Enter the public key $pk$, signature message $m$, public message $c$ and signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$, if the equation

$$e(\sigma_1, g) = e(g_1, pk) e\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}, \sigma_2\right) e\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, \sigma_3\right) \tag{3}$$

is established, outputs 1, otherwise outputs 0.

(10) *Server-setup*: The verifier randomly selects an element $y \in Z_p^*$ and further assumes a string $vst = y$, and requires the string to be undisclosed.

(11) *Server-verify*: The server helps the verifier to verify the validity of the signature through the following interactive protocol. Specific steps are as follows:

(1) The verifier first enters the signature message $m$, the public message $c$, and computes $\sigma^* = \left(\sigma_1^*, \sigma_2^*, \sigma_3^*\right) = \left(\sigma_1^y, \sigma_2^y, \sigma_3^y\right)$ by using the string $vst = y$, and sends the information $(m, c, \sigma^*)$ to the server.

(2) After receiving the information $(m, c, \sigma^*)$ sent by the verifier, the server calculates $\eta_1 = e\left(\sigma_1^*, g\right)$, $\eta_2 = e\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}, \sigma_2^*\right)$, $\eta_3 = e\left(\mu^* \prod_{j=1}^{n_m} \mu_j^{m_{1j}}, \sigma_3^*\right)$ and $\eta_4 = e(g_1, pk)$, and then sends $(\eta_1, \eta_2, \eta_3, \eta_4)$ to the verifier.

(3) After obtaining $(\eta_1, \eta_2, \eta_3, \eta_4)$, the verifier verifies whether the equation

$$\eta_1 = (\eta_4)^y \eta_2 \eta_3 \tag{4}$$

is true, if it is true, output 1; otherwise output 0.

## 5 Safety Proof and Effectiveness Analysis

### 5.1 Correctness Analysis

**Theorem 1:** If the Eq. (1) holds, then the blind signature is correct.

**Proof:** From the natures of the bilinear pair and $\sigma'_{A1} = g_1^a x^{\gamma_m} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\gamma_{m_1}}$, we obtain

$$\begin{aligned} e(\sigma'_{A1}, g) &= e\left( g_1^a x^{\gamma_m} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\gamma_{m_1}}, g \right) \\ &= e(g_1^a, g) e(x^{\gamma_m}, g) e\left( \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\gamma_{m_1}}, g \right) \\ &= e(g_1, pk_A) e(x, \sigma'_{A2}) e\left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, \sigma'_{A3} \right). \end{aligned}$$

**Theorem 2:** If the Eq. (2) holds, then the partial blind proxy re-signature is correct.

**Proof:** From the natures of the bilinear pair and $rk_{A\to B} = \frac{b}{a} \bmod p$, $pk_B = g^b$,and $\sigma'_A = (\sigma'_{A1}, \sigma'_{A2}, \sigma'_{A3}) = \left( g_1^a x^{\gamma_m} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\gamma_{m_1}}, g^{\gamma_m}, g^{\gamma_{m_1}} \right)$, we get

$$\begin{aligned} \sigma'_{B1} &= (\sigma'_{A1})^{rk_{A\to B}} x^{\gamma'_m} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\gamma'_{m1}} \\ &= \left( g_1^a x^{\gamma_m} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\gamma_{m_1}} \right)^{\frac{b}{a}} x^{\gamma'_m} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_1 j} \right)^{\gamma'_{m_1}} \\ &= g_1^b x^{\frac{b}{a}\gamma_m + \gamma'_m} \left( \mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}} \right)^{\frac{b}{a}\gamma_{m_1} + \gamma'_{m_1}}, \end{aligned}$$

$$\sigma'_{B2} = (\sigma'_{A2})^{rk_{A\to B}} g^{\gamma'_m} = (g^{\gamma_m})^{\frac{b}{a}} g^{\gamma'_m} = g^{\frac{b}{a}\gamma_m + \gamma'_m},$$

$$\sigma'_{B3} = \left(\sigma'_{A3}\right)^{rk_{A\to B}} g^{\gamma'_{m_1}} = \left(g^{\gamma_{m_1}}\right)^{\frac{b}{a}} g^{\gamma'_{m_1}} = g^{\frac{b}{a}\gamma_{m_1}+\gamma'_{m_1}}$$

then, using the properties of the bilinear pair again, we get

$$\begin{aligned} e\left(\sigma'_{B1}, g\right) &= e\left(g_1^b x^{\frac{b}{a}\gamma_m+\gamma'_m}\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\frac{b}{a}\gamma_{m_1}+\gamma'_{m_1}}, g\right) \\ &= e\left(g_1^b, g\right) e\left(x^{\frac{b}{a}\gamma_m+\gamma'_m}, g\right) e\left(\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\frac{b}{a}\gamma_{m_1}+\gamma'_{m_1}}, g\right) \\ &= e\left(g_1, g^b\right) e\left(x, g^{\frac{b}{a}\gamma_m+\gamma'_m}\right) e\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, g^{\frac{b}{a}\gamma_{m_1}+\gamma'_{m_1}}\right) \\ &= e(g_1, pk_B) e\left(x, \sigma'_{B2}\right) e\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, \sigma'_{B3}\right). \end{aligned}$$

**Theorem 3:** If the Eq. (3) holds, then the proxy re-signature is correct.

**Proof:** For the sake of simplicity of writing, we write $\gamma_m^B = \frac{b}{a}\gamma_m + \gamma'_m$ and $\gamma_{m_1}^B = \frac{b}{a}\gamma_{m_1} + \gamma'_{m_1}$.

With Bob's public key and blind proxy re-signature, de-blinding the blind proxy re-signature in the following:

$$\begin{aligned} &\left(\sigma'_{B1}\right)\left(\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}\right)\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\kappa}\right)^{\lambda} \\ &= \left(g_1^b x^{\gamma_m^B}\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\gamma_{m_1}^B}\right)\left(\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}\right)\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\kappa}\right)^{\lambda} \\ &= g_1^b \left(\mu^* \prod_{j=1}^{n_{m1}} \mu_j^{m_{1j}}\right)^{\gamma_{m_1}^B + \kappa\lambda} \left(u^* \prod_{i=1}^{n_m} u_i^{m_i}\right)^{\kappa\gamma_m^B + \lambda} \\ &= \sigma_{B1}, \end{aligned}$$

$$\left(\sigma'_{B2}\right)^{\kappa} g^{\lambda} = g^{\kappa\gamma_m^B} g^{\lambda} = g^{\kappa\gamma_m^B + \lambda} = \sigma_{B2},$$

$$\left(\sigma'_{B3}\right) g^{\kappa\lambda} = g^{\gamma_{m_1}^B} g^{\kappa\lambda} = g^{\gamma_{m_1}^B + \kappa\lambda} = \sigma_{B3},$$

then, from the properties of the bilinear pair, we get

$$
\begin{aligned}
e(\sigma_{B1}, g) &= e\left(g_1^b\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\gamma_{m_1}^B + \kappa\lambda}\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}\right)^{\kappa\gamma_m^3 + \lambda}, g\right) \\
&= e\left(g_1^b, g\right) e\left(\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}\right)^{\kappa\gamma_m^B + \lambda}, g\right) e\left(\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\gamma_{m_1}^B + \kappa\lambda}, g\right) \\
&= e\left(g_1, g^b\right) e\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}, g^{\kappa\gamma_m^B + \lambda}\right) e\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, g^{\gamma_{m_1}^B + \kappa\lambda}\right) \\
&= e(g_1, pk_B) e\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}, \sigma_{B2}\right) e\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, \sigma_{B3}\right).
\end{aligned}
$$

**Theorem 4:** If the Eq. (4) holds, then the server-assisted verification algorithm is correct.

**Proof:** From the un-blind proxy re-signature $\sigma_B = (\sigma_{B1}, \sigma_{B2}, \sigma_{B3})$ and string $vst = y$ and using the properties of bilinear pairs, we obtain

$$
\begin{aligned}
\eta_1 &= e\left(\sigma_{B1}^*, g\right) \\
&= e\left((\sigma_{B1})^y, g\right) \\
&= e\left(\left(g_1^b\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}\right)^{\kappa\gamma_m^B + \lambda}\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}\right)^{\gamma_{m_1}^B + \kappa\lambda}\right)^y, g\right) \\
&= e\left(g_1, g^b\right)^y e\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}, \left(g^{\kappa\gamma_m^B + \lambda}\right)^y\right) e\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, \left(g^{\gamma_{m_1}^B + \kappa\lambda}\right)^y\right) \\
&= e(g_1, pk_B)^y e\left(u^* \prod_{i=1}^{n_m} u_i^{m_i}, \sigma_{B2}^y\right) e\left(\mu^* \prod_{j=1}^{n_{m_1}} \mu_j^{m_{1j}}, \sigma_{B3}^y\right) \\
&= (\eta_4)^y \eta_2 \eta_3.
\end{aligned}
$$

Through the derivation of the above four theorems, it is found that the obtained blind signature, partial blind proxy re-signature and proxy re-signature obtained after detachment processing are effective and the server-assisted verification protocol algorithm is correct. Because the original signature is indistinguishable from the proxy re-signature, this scheme satisfies transparency and versatility.

### 5.2 Security Analysis

The scheme of this paper is based on the scheme in [12]. In this scheme, the partial blindness and unforgeability have been proved under the standard model. Therefore, according to the definition of security of the scheme, in order to prove the security of the scheme, it is only necessary to prove that the server-assisted verification algorithm is complete.

**Theorem 5:** The server-assisted verification of the proposed scheme is complete.

The proof of this theorem needs to consider two aspects. Firstly, consider that the server and the trustee jointly generate an illegal signature, so that the verifier is convinced that the probability that an illegal signature is legal is negligible. Secondly, consider that the server and the agent jointly generate an illegal signature, and the probability that the signature convinced by the verifier that an illegal signature is legitimate is negligible. Next, the conclusion of Theorem 5 will be proved from the following two lemmas.

**Lemma 1:** If the server collides with Alice to become an attacker $A_1$, the attacker asks the challenger to determine that an illegal original signature is legal. The probability that the event is true is zero.

**Proof:** In this process, $A_1$ plays the role of the server and in the agreement, C plays the role of verifier. Given the illegal original signature of a message, the goal of $A_1$ is to let $C$ make sure that the illegal signature is legitimate. The interaction between them is as follows:

Establishment: Challenger $C$ performs the initialization algorithm to generate system parameter $cp$, randomly selects $y^*, \gamma \in Z_p^*$, lets $vst = y^*$ and calculates the public-private key pair $(pk_A, sk_A) = (e(g_1, g^{\gamma}), \gamma)$ of the trustee Alice and then sends $\{cp, pk_A, sk_A\}$ to the attacker $A_1$.

Query: The attacker $A_1$ can make a limited number of secondary verification queries to the server. In the process of each inquiry of $(m_i, \sigma_i)$, both the challenger $C$ and the attacker $A_1$ perform server-assisted verification to obtain the authentication protocol, and then respond to the output of the protocol and return it to the attacker $A_1$.

Output: Finally, the attacker $A_1$ outputs the forged messages $m^*$, $c^*$ and the string $\sigma^{1*} = \left(\sigma_1^{1*}, \sigma_2^{1*}, \sigma_3^{1*}\right)$, and let the set of all legal signatures that make the messages $m^*$, $c^*$ corresponding to the public key $pk_A$ is $\Gamma_{m^*}$, and satisfies $\sigma^{1^*} \notin \Gamma_{m^*}$. When the challenger $C$ receives $\left(m^*, c^*, \sigma^{1^*}\right)$, it computes $\left(\sigma^{1^*}\right)^* = \left(\left(\sigma_1^{1*}\right)^*, \left(\sigma_2^{1*}\right)^*, \left(\sigma_3^{1*}\right)^*\right) = \left(\left(\sigma_1^{1*}\right)^{y^*}, \left(\sigma_2^{1*}\right)^{y^*}, \left(\sigma_3^{1*}\right)^{y^*}\right)$ with the given string $vst$ and sends it to the attacker $A_1$. Then, $A_1$ obtains $\eta_1^* = e\left(\sigma_1^{1*}, g\right)$, $\eta_2^* = e\left(u' \prod_{i=1}^{n_m} u_i^{m_i}, \sigma_2^{1*}\right)$, $\eta_3^* = e\left(\mu^* \prod_{j=1}^{n_{m1}} \mu_j^{m_{1j}}, \sigma_3^{1*}\right)$ and $\eta_4 = e(g_1, pk_A)$ by operation and returns them to $C$. The following is a detailed derivation of the probability that the equation $\eta_1^* = (\eta_4)^{y^*} \eta_2^* \eta_3^*$ is established is $1/(p-1)$.

(1) Because of $(\sigma^{1*})^* = (\sigma^{1*})^{y^*}$ and $y^* \in Z_p^*$, the probability of attacker $A_1$ forging $(\sigma^{1*})^*$ from $\sigma^{1*}$ is $1/(p-1)$.

(2) Assuming that the attacker $A_1$ returns $\left(\eta_1^*, \eta_2^*, \eta_3^*, \eta_4\right)$, which satisfies $\eta_1^* = (\eta_4)^{y^*} \eta_2^* \eta_3^*$, then we have

$$\log_{n_4} \eta_1^* = y^* + \log_{\eta_4} \eta_2^* + \log_{n_4} \eta_3^*,$$

Because $y^*$ is an element selected arbitrarily from $Z_p^*$, the probability that the attacker tries to get $y^*$ to make the above equation true is $1/(p-1)$.

From the above analysis, it can be seen that the probability that attacker $A_1$ makes $C$ believe that message signature $(m^*, \sigma^*)$ is legitimate is $1/(p-1)$. Since $p$ is a large prime, the probability that attacker $A_1$ let $C$ decide that an illegal original signature is legitimate is zero.

**Lemma 2:** If the server collides with the proxy to become an attacker $A_2$. The probability that $A_2$ lets $C$ decide that an illegal re-signature is legal is negligible.

**Proof:** In this process, $A_2$ plays the role of the server and in the agreement, $C$ plays the role of verifier. When an illegal signature of a message is given, the goal of $A_2$ is to let $C$ make sure the illegal signature is legal. The interaction between the two is as follows:

Establishment: Challenger $C$ obtains system parameter $cp$ by running a system initialization algorithm, selects three elements $y^*$, $\alpha$, $\beta$ from $Z_p^*$, and computes $(pk_A, sk_A) = (e(g_1, g^{\alpha}), \alpha)$, $(pk_B, sk_B) = \left(e\left(g_1, g^{\beta}\right), \beta\right)$ and $rk_{A\to B} = \frac{b}{a} mod\, p$. Then Challenger $C$ sends $cp, pk_A, pk_B$ and $rk_{A\to B}$ to $A_2$.

Query: Same as the interrogation response process in Lemma 1.

Output: Finally, the attacker $A_2$ outputs the forged messages $m^*$, $c^*$, and the string $\sigma^{1*} = \left(\sigma_1^{1*}, \sigma_2^{1*}, \sigma_3^{1*}\right)$, and let the set of all legal signatures that make the messages $m^*$, $c^*$ corresponding to the public key $pk_B$ is $\Gamma_{m^*}$, and satisfies $\sigma^{1^*} \notin \Gamma_{m^*}$. Similarly, in the analysis process in Lemma 1, attacker $A_2$ let $C$ make sure that the probability that $(m^*, c^*, \sigma^{1*})$ is a legal signature is $1/(p-1)$. Therefore, the probability that attacker $A_2$ makes $C$ convinced that $(m^*, c^*, \sigma^{1*})$ is a legitimate signature is negligible.

Based on the above analysis, we know that the partial blind proxy re-signature scheme proposed in this paper is safe in the case of adaptive selection of message attacks and collusion attacks.

Next, we present a performance analysis of the server-assisted verification partial blind proxy re-signature scheme.

## 5.3 Performance Analysis

### 5.3.1 Efficiency Analysis

The computational difficulty of the server-assisted verification partial blind proxy re-signature scheme proposed in this paper is equivalent to the CDH problem. In order to compare performance with the existing blind proxy re-signature algorithm, the following symbols are defined (Table 1).

**Table 1.** The symbolic representation of the solution.

| Symbol | Description |
|---|---|
| $\lvert G_1\rvert$ | The length of the element in $G_1$ |
| $\lvert G_2\rvert$ | The length of the element in $G_2$ |
| $C_p$ | Exponential calculation |
| $C_q$ | Bilinear pairing calculation |

It should be noted that since the calculation amount of addition, multiplication, HMAC algorithm and hash function are relatively small, we only consider the computational exponential operation and the bilinear pair operation with large computational complexity when considering the computational overhead.

The following analysis will be carried out from five aspects: the calculation amount of the signature algorithm, the calculation amount of the blind algorithm, the calculation amount of the re-signature algorithm, the calculation amount of the un-blind algorithm and the calculation amount of the verifier. The calculation amount of the algorithm in the scheme of this paper is shown in Table 2 below.

**Table 2.** Calculation amount of the scheme.

| Procedure | Calculated amount |
|---|---|
| Sign algorithm | $5C_p$ |
| Blind algorithm | $6C_p$ |
| Re-signature algorithm | $7C_p + 4C_q$ |
| Un-blind algorithm | $5C_p + 4C_q$ |
| Verifier | $4C_p$ |

The literature [12, 14, 15] respectively gives three different blind proxy re-signature schemes. The signature algorithm proposed in this paper is compared with the existing three algorithms based on its computational cost and security attributes. The comparison results are shown in the following Table 3.

**Table 3.** Calculation overhead and security attributes of blind proxy re-signature algorithm.

| Scheme | The length of signature | The length of Re-signature | Re-signature algorithm | Blind algorithm | Verifier | Versatility | Partial blindness |
|---|---|---|---|---|---|---|---|
| Alg. in [12] | $\|3G_1\|$ | $\|3G_1\|$ | $7C_p + 4C_q$ | $6C_p$ | $4C_p$ | Yes | Yes |
| Alg. in [14] | $\|3G_1\|$ | $\|3G_1\|$ | $4C_q$ | $2C_p$ | $6C_q$ | Yes | No |
| Alg. in [15] | $\|3G_1\|$ | $\|2G_1\|$ | $2C_p + 7C_q$ | $5C_p$ | $3C_q$ | No | No |
| Ours | $\|3G_1\|$ | $\|3G_1\|$ | $7C_p + 4C_q$ | $6C_p$ | $4C_p$ | Yes | Yes |

It can be seen from Table 3 that on the one hand, from the perspective of storage overhead, the signature length and re-signature length of the scheme are similar to those of the literature [12, 14, 15], but the scheme in [14] does not have partial blindness. The scheme of [15] is neither versatile nor partially blind, so its practical applicability is small. On the other hand, from the calculation amount, the scheme in the literature [12] and the scheme proposed in this paper are slightly higher in the calculation of the re-signature algorithm and the blind algorithm than in the literature [12, 14, 15]. However, the scheme in this paper only needs four exponential operations in the verification process, and literature [12, 14, 15] needs six, three and four bilinear pairing operations

with high computational complexity, respectively. In summary, the scheme has partial blindness and versatility security attribute features, which can effectively protect the trustee's privacy messages and the agent's legal rights can also be maintained. Moreover, the scheme has less computational complexity when verifying the validity of signatures, thus reducing the time required for verification and improving the efficiency of verification. Therefore, the scheme can be better applied to mobile communications.

### 5.3.2 Numerical Experiments

This part is a simulation experiment of the verifier's time overhead, verification efficiency and message signatures of different orders of magnitude in the schemes of this paper, the literature [12] and [14]. The environment of the simulation experiment is CPU for Intel Core i5-8300H processor, clocked at 2.3 GHz, memory 8 GB, software environment: 64-bit Window 10 operating system, MyEclipse2015.

It can be seen from Fig. 1 that for the signature messages of the same length, the verification time overhead of the scheme is lower than that in [12, 14] and is a bit higher than that in [15], however, the scheme in [15] is neither versatile nor partially blind. In addition, in the schemes of [12] and [14], the verifier needs to perform 4 and 6 bilinear pairing operations, respectively. As the length of the signature message increases, the time overhead of the verifier in the scheme increases greatly. However, in this scheme, the computationally complex bilinear pair operation is transferred to the server through the interaction protocol between the verifier and the server. The verifier only needs to perform 4 times exponential operation, so in this scheme as the length of the signature message increases, the time cost of the verifier changes little.

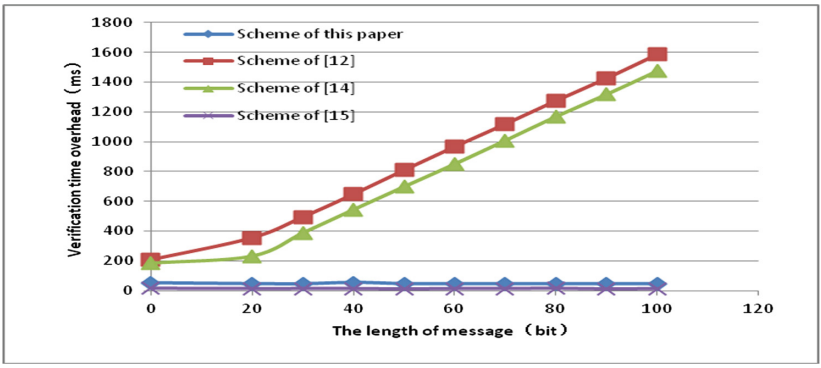


**Fig. 1.** Relationship between verification time overhead and message length.

It can be seen from Fig. 2 that the verification efficiency of the scheme is improved by at least 74% and 71%, respectively, compared with the schemes of [14] and [12], which greatly reduces the time cost of the verifier and saves the verification cost.

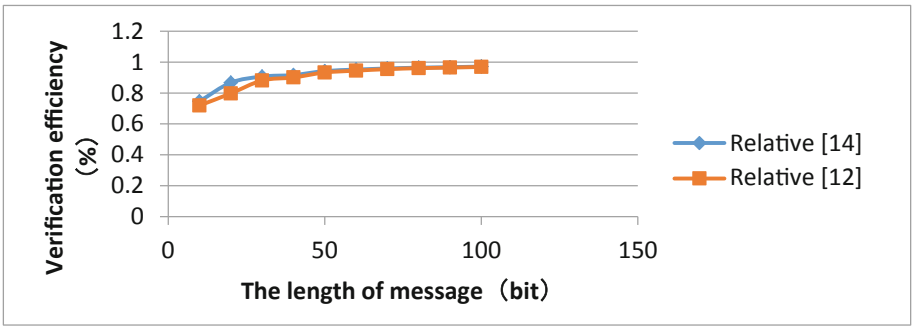


**Fig. 2.** Relationship between verification time overhead and message length.

## 6 Conclusion

This paper proposes a formal model of server-assisted verification of partial blind proxy re-signature, constructs a specific implementation scheme, and gives corresponding security proof. In this solution, on the one hand, in the process of the server-assisted authentication protocol, the verifier and the server transfer the complex bilinear pairing operation task to the server through the interaction protocol between them, so that the verifier compares the small computational cost verifies the signature and improves the verification efficiency of the signature. On the other hand, the use of partial blindness not only protects the privacy message of the trustee but also protects the legitimate rights and interests of the agent. Finally, simulation experiments show that the proposed scheme has higher verification efficiency than other existing blind proxy re-signature schemes, and satisfies the requirements of low-end computing equipment with weak computing power and limited energy supply. Therefore, it is suitable for use in the mobile Internet application environment.

## References

1. Wei, W., Yi, M., Susilo, W., et al.: Provably secure server-aided verification signatures. Comput. Math. Appl. **61**(7), 1705–1723 (2011)
2. Niu, S.F., Wang, C.F., et al.: Server-assisted verification signature scheme against collusion attacks. Appl. Res. Comput. **33**(1), 229–231 (2016)
3. Yang, X.D., Li, Y.N., Zhou, Q.X., et al.: Security analysis and improvement of a server-sided authentication aggregation signature scheme. Comput. Eng. **43**(1), 183–187 (2017)
4. Ateniese, G., Hohenberger, S.: Proxy re-signatures: new definitions, algorithms, and applications. https://doi.org/10.1145/1102120.1102161
5. Hong, X., Chen, K.F., Wan, Z.M.: Simple universally combinable proxy re-signature scheme. J. Softw. **21**(8), 2079–2088 (2010)
6. Ai, H., Liu, X.J.: Research on universal combinable re-signature scheme based on bilinear pairs. Comput. Eng. Des. **34**(11), 3748–3751 (2013)
7. Li, H.X., Shao, L., Pang, L.J.: Proxy re-signature scheme based on polynomial isomorphism. J. Commun. **38**(2), 16–24 (2017)

8. Qiao, L.: Research on Lattice-Based Proxy Signature Scheme, pp. 40–46. University of Electronic Science and Technology of China, Chengdu (2016)
9. Huang, P., Yang, X.D., Li, Y., et al.: Identity-based proxy re-signature scheme for unpaired linear pairs. Comput. Appl. **35**(6), 1678–1682 (2015)
10. Yang, X.D., Yang, P., Gao, G.J., et al.: Uncertified proxy re-signature scheme with aggregation properties. Comput. Eng. Sci. **40**(6), 71–76 (2018)
11. Mi, J.L., Zhang, J.Z., Chen, S.T., et al.: Blind proxy signature scheme for designated verifiers that can tolerate information disclosure. Comput. Eng. Appl. **52**(22), 123–126 (2016)
12. Yang, X.D., Chen, C.L., Yang, P., et al.: Partially blind proxy re-signature scheme. J. Commun. **39**(2), 67–72 (2018)
13. Yang, X.D., Li, Y.N., Gao, G.J., et al.: Sever-aided verification proxy re-signature scheme in the standard model. J. Electron. Inf. Technol. **38**(5), 1151–1157 (2016)
14. Feng, T., Liang, Y.X.: Proven secure certificateless blind proxy re-signature. J. Commun. **33** (Z1), 58–78 (2012)
15. Hu, X.M., Yang, Y.C., Liu, Y.: Security analysis and improvement of a blind proxy re-signature scheme based on standard model. Small Microcomput. Syst. **2**(10), 2008–2011 (2011)