可证安全的部分盲代理重签名方案

杨小东[1,2]，陈春霖[1]，杨平[1]，安发英[1]，麻婷春[1]，王彩芬[1]
（1. 西北师范大学计算机科学与工程学院，甘肃 兰州 730070；2. 密码科学技术国家重点实验室，北京 100878）

摘 要：针对盲代理重签名的匿名性和可控性问题，借鉴部分盲签名的设计思想，引入部分盲代理重签名的概念，并给出了部分盲代理重签名的安全性定义。基于改进的 Shao 方案，构造一种标准模型下的双向盲代理重签名方案，允许在最终的重签名中添加受托者和代理者协商的公共信息，不仅实现了签名从受托者到代理者之间的透明转换，保护重签名消息的隐私，还能防止受托者对重签名的非法使用。分析结果表明，新方案满足正确性、多用性、部分盲性和不可伪造性，其性能更适用于电子政务数据交换、跨域身份认证等系统。

关键词：部分盲代理重签名；不可伪造性；多用性；标准模型
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018014

Partially blind proxy re-signature scheme with proven security

YANG Xiaodong[1,2], CHEN Chunlin[1], YANG Ping[1], AN Faying[1], MA Tingchun[1], WANG Caifen[1]
1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China
2. State Key Laboratory of Cryptology, Beijing 100878, China

Abstract: In order to solve the problem of anonymity and controllability of blind proxy re-signature, the concept of partially blind proxy re-signature was introduced by using the idea of partially blind signature. Furthermore, the security definition of partially blind proxy re-signature was also given. Based on the improved Shao scheme, a partially blind proxy re-signature scheme in the standard model was proposed. The proposed scheme allows proxy to add some public information negotiated by delegatee and proxy to re-signature. The scheme not only can achieve the transparent signature conversion from delegatee to proxy and protect privacy of message re-signed by proxy, but also prevented illegal use of re-signature. Analysis results show that the proposed scheme is correct, multi-use, partially blind and existentially unforgeable. It is more suitable for e-government data exchange system, cross-domain authentication system and so on.

Key words: partially blind proxy re-signature, unforgeability, multi-use, standard model

1 引言

代理重签名是一种具有签名转换特性的密码体制，一个半可信的代理者利用重签名密钥可将受托者 Alice 的签名转换为委托者 Bob 对同一个消息的签名，但代理者无法代替受托者或委托者生成任意消息的合法签名[1]。代理重签名在车联网隐私保护、电子政务数据交换、数字版权管理等方面有广阔的应用前景[2,3]。

近年来，代理重签名已成为数字签名领域研究的一个热点，国内外学者提出了一系列具有特殊性质的代理重签名方案。Ateniese 等[4]定义了代理重

收稿日期：2017-05-31；**修回日期**：2017-10-30
基金项目：国家自然科学基金资助项目（No.61662069）；中国博士后科学基金资助项目（No.2017M610817）；甘肃省科技计划基金资助项目（No.1506RJZA130）；兰州市科技计划基金资助项目（No.2013-4-22）；西北师范大学青年教师科研能力提升计划基金资助项目（No.WNU-LKQN-14-7）
Foundation Items: The National Natural Science Foundation of China (No.61662069), The China Postdoctoral Science Foundation (No.2017M610817), The Science and Technology Planning Project of Gansu Province (No.1506RJZA130), The Science and Technology Project of Lanzhou (No.2013-4-22), Foundation for Excellent Young Teachers by Northwest Normal University (No.NWNU-LKQN-14-7)

签名的安全模型，并构造了 2 种安全性依赖于理想随机预言机的代理重签名方案。但在标准模型下证明安全的密码系统，其安全性只依赖于所关联的困难问题[5]。Shao 等[6]构造了一种基于标准模型的代理重签名方案，然而，Kim 等[7]发现该方案的重签名算法存在安全漏洞，并提出了一种改进方案。Tian 等[8]构造了一种基于身份的代理重签名方案，有效避免了复杂的证书管理。为了解决密钥托管问题，Chen 等[9]提出了一种无证书代理重签名方案。Yang 等[10]提出了门限代理重签名方案，防止代理者滥用签名转换的权限。Tian 等[11]构造了基于格的代理重签名方案，用于抵抗量子计算的攻击。Yang 等[12]提出了可分离的在线/离线代理重签名方案，有效改善了代理重签名的实时性。然而，目前，大部分代理重签名方案不具有消息致盲性，代理者能够获得所转换消息的具体内容。为了解决这个问题，邓宇乔等[13]提出了一种双向盲代理重签名方案，冯涛等[14]将该方案扩展为一种无证书盲代理重签名方案，但胡小明等[15]指出这类方案存在严重的安全缺陷，受托者能够伪造任意消息的重签名。针对该安全缺陷，胡小明等[15]提出了一种改进的盲代理重签名方案，但该方案是双向单用的，在实际应用中有很大的局限性。

在已有的盲代理重签名方案中，代理者不知道最终重签名的任何信息，很容易造成重签名被受托者非法使用。针对盲代理重签名的匿名性和可控性问题，本文提出了部分盲代理重签名体制，将代理者所转换的消息分为 2 个部分：一部分是受托者发送的消息，对代理者保持盲性；一部分是受托者和代理者提前协商好的公共消息。新签名体制不仅保护了受托者所发送消息的隐私，还确保了代理者的合法权益，使代理者对重签名内容是部分可控的。结合部分盲签名体制和代理重签名体制，给出了部分盲代理重签名的安全性定义，设计了一种具体的部分盲代理重签名方案，并在标准模型下证明该方案满足不可伪造性、部分盲性、多用性和正确性。通过对相关领域的文献搜索，目前还没有关于部分盲代理重签名研究的公开文献。

2 预备知识

2.1 双线性对

假设 G_1 和 G_2 是阶为素数 p 的循环群，g 是 G_1 的一个生成元，双线性对 $e: G_1 \times G_1 \to G_2$ 是一个满足以下条件的能有效计算的映射[13]。

1) 双线性：对任意的 $a,b \in Z_p^*$，满足 $e(g^a, g^b) = e(g,g)^{ab}$。

2) 非退化性：$e(g,g) \neq 1_{G_2}$。

2.2 CDH 假设

CDH（computational Diffie-Hellman）问题：给定三元组 $(g, g^a, g^b) \in G_1^3$，这里，$a,b \in Z_p^*$ 是未知的，计算 $g^{ab} \in G_1$。

定义 1 CDH 假设。若任何一个多项式时间算法解决 CDH 问题的概率是可忽略的，则称 G_1 上的 CDH 问题是困难的[16]。

3 双向部分盲代理重签名的安全性定义

定义 2 一种双向部分盲代理重签名方案 PBPRS = (Setup, KeyGen, ReKey, Agree, Sign, Blind, ReSign, Unblind, Verify)由以下 9 个算法组成。

1) Setup $(1^\eta) \to par$：给定安全参数 η，运行系统参数生成算法输出公开参数 par。

2) KeyGen $(par) \to sk$：给定系统参数 par，用户运行密钥生成算法输出一对公钥/私钥 (pk, sk)。

3) ReKey $(sk_A, sk_B) \to rk_{A\to B}$：给定受托者 Alice 的私钥 sk_A 和委托者 Bob 的私钥 sk_B，运行重签名密钥生成算法为代理者 Proxy 生成一个重签名密钥 $rk_{A\to B}$。

4) Agree $(par) \to c$：给定 par，受托者和代理者通过协商消息算法生成一个公共消息 c。

5) Sign $(c, m, sk) \to \sigma$：给定公共消息 c、签名消息 m 和私钥 sk，运行签名算法生成 m 和 c 的签名 σ。

6) Blind $(m, c, sk, t) \to (h, \sigma'_A)$：给定公共消息 c、签名消息 m、私钥 sk 和盲化因子 t，受托者运行盲化算法生成 m、c 的盲化消息 h 和盲化签名 σ'_A，并将 (h, σ'_A) 发送给代理者。

7) ReSign $(rk_{A\to B}, c, h, \sigma'_A, pk_A) \to \sigma'_B$：给定重签名密钥 $rk_{A\to B}$、公共消息 c、盲化消息 h、盲化签名 σ'_A 和受托者的公钥 pk_A，首先，判断 σ'_A 是否为对应于 pk_A 的 h 和 c 的合法签名，如果不是，输出 $\perp$；否则，代理者运行重签名生成算法生成一个对应于委托者公钥 pk_B 的部分盲代理重签名 σ'_B。

8) Unblind $(\sigma'_B, t) \to \sigma_B$：给定部分盲代理重签名 σ'_B 和盲化因子 t，受托者运行脱盲算法生成签

名消息 m 和公共消息 c 的重签名 σ_{B}。

9) Verify $(m,c,pk,\sigma)\to\{0,1\}$：对于公钥 pk、消息 m、公共消息 c 和签名 σ，如果 σ 是对应于 pk 的关于 m 和 c 的合法签名，验证者接受签名，输出 1；否则，输出 0。

方案的合理性包括 4 个部分：原始签名 σ、盲化签名 σ'_{A}、部分代理重签名 σ'_{B} 和重签名 σ_{B} 的正确性。安全性至少包括 2 个部分：存在不可伪造性和部分盲性。存在不可伪造性保证攻击者不能伪造任何一个新消息的合法签名，下面，通过挑战者 $\mathcal{C}$ 和攻击者 $\mathcal{A}$ 之间的游戏来定义部分盲代理重签名的存在不可伪造性。

系统建立。$\mathcal{C}$ 运行 Setup 算法和 KeyGen 算法分别生成系统参数 par 和目标用户的公私钥对 (pk_t,sk_t)，并将 par 和 pk_t 发送给 $\mathcal{A}$。

由于 $\mathcal{A}$ 能产生除目标用户之外其余用户的私钥，所以 $\mathcal{A}$ 不需要发起密钥询问。如果 $\mathcal{A}$ 拥有目标用户与某个用户之间的重签名密钥，则通过重签名密钥的双向性和该用户的私钥很容易计算出目标用户的私钥。因为 $\mathcal{A}$ 能计算除目标用户之外其余用户间的重签名密钥，所以不允许 $\mathcal{A}$ 进行重签名密钥询问。

询问。$\mathcal{A}$ 可以自适应地向 $\mathcal{C}$ 进行一系列如下预言机的询问。

1) 签名询问。$\mathcal{A}$ 和 $\mathcal{C}$ 运行 Agree 算法协商生成公共消息 c，对于 $\mathcal{A}$ 发起的签名询问 (m,c)，$\mathcal{C}$ 首先运行 Sign (c,m,sk_t)算法生成消息 m 和 c 的签名 σ，然后将 σ 返回给 $\mathcal{A}$。

2) 重签名询问。对于 $\mathcal{A}$ 发起的询问 (c,h,σ'_i,pk_i)，$\mathcal{C}$ 首先判断 σ'_i 是否为对应于 pk_i 的 h 和 c 的合法签名，如果不是，输出 $\perp$；否则，以 (h,c) 为输入进行签名询问，并将询问的结果 σ'_t 返回给 $\mathcal{A}$。假设 t 是攻击者 $\mathcal{A}$ 在 Blind 算法中选取的盲化因子，$\mathcal{A}$ 最后运行 Unblind (σ'_i,t)算法生成 m 和 c 的最终重签名 σ_t。

伪造。$\mathcal{A}$ 最后输出一个伪造 (m^*,c^*,σ^*)，并且 $\mathcal{A}$ 在询问阶段没有发起过 (m^*,c^*) 的签名询问以及 $(c^*,h^*,\lozenge,\square)$ 的重签名询问，这里 h^* 是 m^* 的盲化消息，$\lozenge$ 表示任何一个签名，$\square$ 表示任何一个公钥。如果 σ^* 是对应于 pk_t 的 m^* 和 c^* 的有效签名，则攻击者 $\mathcal{A}$ 赢得游戏。

定义 3　如果没有一个攻击者在多项式时间内以不可忽略的概率赢得上述游戏，则称双向部分盲代理重签名方案 PBPRS 满足存在不可伪造性。

部分盲性确保代理者在不知道转换消息内容的情况下生成消息的重签名，并且代理者无法将消息的最终重签名与部分盲代理重签名相对应。借鉴部分盲签名的安全性定义[16,17]，下面，通过挑战者 $\mathcal{B}$ 和攻击者 $\mathcal{F}$ 之间的游戏来定义部分盲代理重签名的部分盲性。

系统建立。$\mathcal{B}$ 运行 Setup 算法、KeyGen 算法和 ReKey 算法生成系统参数 par、2 个公私钥对 $(pk_{\mathrm{A}},sk_{\mathrm{A}})$ 和 $(pk_{\mathrm{B}},sk_{\mathrm{B}})$ 以及重签名密钥 $rk_{\mathrm{A}\to\mathrm{B}}$，将 par 和 $rk_{\mathrm{A}\to\mathrm{B}}$ 发送给 $\mathcal{F}$。

准备。$\mathcal{F}$ 选择 2 个等长的消息 (m_0,m_1) 以及公共消息 c，将 (m_0,m_1,c) 发送给 $\mathcal{B}$。

询问。$\mathcal{B}$ 随机选取比特 $b\in\{0,1\}$，运行 Blind 算法对 (m_b,c) 和 (m_{1-b},c) 进行盲处理，请求 $\mathcal{F}$ 对盲化消息 $(c,h_b,\sigma'_{\mathrm{A},b})$ 和 $(c,h_{1-b},\sigma'_{\mathrm{A},1-b})$ 进行重签名。$\mathcal{F}$ 运行重签名算法 ReSign，并将生成的部分盲代理重签名 $\sigma'_{\mathrm{B},b}$ 和 $\sigma'_{\mathrm{B},1-b}$ 返回给 $\mathcal{B}$。通过运行脱盲算法 Unblind，$\mathcal{B}$ 获得 (m_b,c) 和 (m_{1-b},c) 的最终重签名 $\sigma_{\mathrm{B},b}$ 与 $\sigma_{\mathrm{B},1-b}$，然后将 $(m_b,c,\sigma_{\mathrm{B},b})$ 和 $(m_{1-b},c,\sigma_{\mathrm{B},1-b})$ 发送给 $\mathcal{F}$。

应答。$\mathcal{F}$ 输出一个对 b 的猜测 b'，如果 $b=b'$，则 $\mathcal{F}$ 赢得游戏。

定义 $Adv=|2\Pr[b=b']-1|$ 为 $\mathcal{F}$ 在以上游戏中获胜的优势。

定义 4　如果没有一个攻击者在多项式时间内以不可忽略的优势赢得上述游戏，那么称双向部分盲代理重签名方案 PBPRS 具有部分盲性。

4　新的双向部分盲代理重签名方案

基于改进的 Shao 方案[7]，设计了一个具有双向多用特性的部分盲代理重签名方案。用 n_m 表示消息的比特长度，n_c 表示受托者和代理者预先协商公共消息的比特长度。为了增强方案的灵活性，利用抗碰撞的散列函数 $H_1:\{0,1\}^*\to\{0,1\}^{n_m}$ 和 $H_2:\{0,1\}^*\to\{0,1\}^{n_c}$，将签名消息和公共消息的固定长度扩展为任意长度。

1) Setup 算法

给定安全参数 η，输出系统公开参数 $par=(G_1,G_2,p,e,g,g_2,u',u_1,\cdots,u_{n_m},v',v_1,\cdots,v_{n_c})$。其中，$G_1$ 和 G_2 是阶为素数 p 的循环群，g 是 G_1 的一个生成元，$e:G_1\times G_1\to G_2$ 是一个双线性映射，g_2 是 G_1 上的一个元素，$u',u_1,\cdots,u_{n_m},v',v_1,\cdots,v_{n_c}$ 是 G_1 上随机

选取的 $n_m + n_c + 2$ 个元素。

2) KeyGen 算法

用户随机选取 $x \in Z_p^*$，计算 $pk = g^x$，则用户的公钥/私钥对 $(pk, sk) = (g^x, x)$。

3) ReKey 算法

给定受托者 Alice 的私钥 $sk_{\mathrm{A}} = \alpha$ 和委托者 Bob 的私钥 $sk_{\mathrm{B}} = \beta$，通过安全的分发协议[4]为代理者 Proxy 生成一个重签名密钥 $rk_{\mathrm{A}\to\mathrm{B}} = \dfrac{\beta}{\alpha (\mathrm{mod}\, p)}$，但代理者不知道 sk_{A} 和 sk_{B}。

4) Agree 算法

受托者 Alice 与代理者 Proxy 协商一个 n_c 比特长度的公共消息 $c = (c_1, \cdots, c_{n_c}) \in \{0,1\}^{n_c}$。

5) Sign 算法

给定 n_m 比特长度的签名消息 $m = (m_1, \cdots, m_{n_m}) \in \{0,1\}^{n_m}$ 和 n_c 比特长度的公共消息 c，受托者随机选取 $s_m, s_c \in Z_p^*$，利用私钥 $sk_{\mathrm{A}} = \alpha$ 计算 $\sigma_{\mathrm{A1}} = g_2^{\alpha} (u' \prod_{i=1}^{n_m} u_i^{m_i})^{s_m} (v' \prod_{j=1}^{n_c} v_j^{c_j})^{s_c}$，$\sigma_{\mathrm{A2}} = g^{s_m}$ 和 $\sigma_{\mathrm{A3}} = g^{s_c}$，输出 m 和 c 的原始签名 $\sigma_{\mathrm{A}} = (\sigma_{\mathrm{A1}}, \sigma_{\mathrm{A2}}, \sigma_{\mathrm{A3}})$。

6) Blind 算法

对于 n_m 比特长度的签名消息 m 和 n_c 比特长度的公共消息 c，受托者随机选取 $t \in Z_p^*$，计算 m 的盲化消息 $h = (u' \prod_{i=1}^{n_m} u_i^{m_i})^t$；然后，随机选取 $r_m, r_c \in Z_p^*$，计算 $\sigma'_{\mathrm{A1}} = g_2^{\alpha} h^{r_m} (v' \prod_{j=1}^{n_c} v_j^{c_j})^{r_c}$，$\sigma'_{\mathrm{A2}} = g^{r_m}$ 和 $\sigma'_{\mathrm{A3}} = g^{r_c}$，将公共消息 c、盲化消息 h 和盲化签名 $\sigma'_{\mathrm{A}} = (\sigma'_{\mathrm{A1}}, \sigma'_{\mathrm{A2}}, \sigma'_{\mathrm{A3}})$ 发送给代理者。

7) ReSign 算法

代理者收到 $(c, h, \sigma'_{\mathrm{A}} = (\sigma'_{\mathrm{A1}}, \sigma'_{\mathrm{A2}}, \sigma'_{\mathrm{A3}}))$ 后，若等式 $e(\sigma'_{\mathrm{A1}}, g) = e(g_2, pk_{\mathrm{A}}) e(h, \sigma'_{\mathrm{A2}}) e(v' \prod_{j=1}^{n_c} v_j^{c_j}, \sigma'_{\mathrm{A3}})$ 不成立，输出 $\perp$；否则，随机选取 $r'_m, r'_c \in Z_p^*$，利用重签名密钥 $rk_{\mathrm{A}\to\mathrm{B}}$ 计算 $\sigma'_{\mathrm{B1}} = (\sigma'_{\mathrm{A1}})^{rk_{\mathrm{A}\to\mathrm{B}}} h^{r'_m} (v' \prod_{j=1}^{n_c} v_j^{c_j})^{r'_c}$、$\sigma'_{\mathrm{B2}} = (\sigma'_{\mathrm{A2}})^{rk_{\mathrm{A}\to\mathrm{B}}} g^{r'_m}$ 和 $\sigma'_{\mathrm{B3}} = (\sigma'_{\mathrm{A3}})^{rk_{\mathrm{A}\to\mathrm{B}}} g^{r'_c}$，将部分盲代理重签名 $\sigma'_{\mathrm{B}} = (\sigma'_{\mathrm{B1}}, \sigma'_{\mathrm{B2}}, \sigma'_{\mathrm{B3}})$ 发送给受托者。

8) Unblind 算法

受托者收到 $\sigma'_{\mathrm{B}} = (\sigma'_{\mathrm{B1}}, \sigma'_{\mathrm{B2}}, \sigma'_{\mathrm{B3}})$ 后，用委托者的公钥 pk_{B} 验证 $e(\sigma'_{\mathrm{B1}}, g) = e(g_2, pk_{\mathrm{B}}) e(h, \sigma'_{\mathrm{B2}}) e(v' \prod_{j=1}^{n_c} v_j^{c_j}, \sigma'_{\mathrm{B3}})$。

如果等式不成立，受托者拒绝接受 σ'_{B}；否则，随机选取 $y \in Z_p^*$，利用盲化因子 t 对 σ'_{B} 进行脱盲处理，计算 $\sigma_{\mathrm{B1}} = (\sigma'_{\mathrm{B1}}) ((u' \prod_{i=1}^{n_m} u_i^{m_i}) (v' \prod_{j=1}^{n_c} v_j^{c_j})^t)^y$，$\sigma_{\mathrm{B2}} = (\sigma'_{\mathrm{B2}})^t g^y$ 和 $\sigma_{\mathrm{B3}} = (\sigma'_{\mathrm{B3}}) g^{yt}$，生成 m 和 c 的重签名 $\sigma_{\mathrm{B}} = (\sigma_{\mathrm{B1}}, \sigma_{\mathrm{B2}}, \sigma_{\mathrm{B3}})$。

9) Verify 算法

给定公钥 pk、n_m 比特长度的消息 m、n_c 比特长度的公共消息 c 和签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3)$，如果 $e(\sigma_1, g) = e(g_2, pk) e(u' \prod_{i=1}^{n_u} u_i^{m_i}, \sigma_2) e(v' \prod_{j=1}^{n_c} v_j^{c_j}, \sigma_3)$，则说明 σ 是 m 和 c 的有效签名，输出 1；否则，输出 0。

5 安全性证明与有效性分析

5.1 正确性分析

由于改进的 Shao 方案[7]能确保新方案中原始签名的正确性，下面仅分析盲化签名、部分代理重签名和重签名的正确性。

1) 盲化签名的正确性

给定公共消息 c、盲化消息 $h = (u' \prod_{i=1}^{n_m} u_i^{m_i})^t$、签名 $\sigma'_{\mathrm{A}} = (\sigma'_{\mathrm{A1}}, \sigma'_{\mathrm{A2}}, \sigma'_{\mathrm{A3}}) = (g_2^{\alpha} h^{r_m} (v' \prod_{j=1}^{n_c} v_j^{c_j})^{r_c}, g^{r_m}, g^{r_c})$ 和受托者的公钥 $pk_{\mathrm{A}} = g^{\alpha}$，则盲化签名 σ'_{A} 的正确性验证如下

$$\begin{aligned} e(\sigma'_{\mathrm{A1}}, g) &= e(g_2^{\alpha} h^{r_m} (v' \prod_{j=1}^{n_c} v_j^{c_j})^{r_c}, g) \\ &= e(g_2^{\alpha}, g) e(h^{r_m}, g) e((v' \prod_{j=1}^{n_c} v_j^{c_j})^{r_c}, g) \\ &= e(g_2, pk_{\mathrm{A}}) e(h, \sigma'_{\mathrm{A2}}) e(v' \prod_{j=1}^{n_c} v_j^{c_j}, \sigma'_{\mathrm{A3}}) \end{aligned}$$

2) 部分代理重签名的正确性

给定重签名密钥 $rk_{\mathrm{A}\to\mathrm{B}} = \dfrac{\beta}{\alpha} (\mathrm{mod}\, p)$、委托者的公钥 $pk_{\mathrm{B}} = g^{\beta}$ 和签名 $\sigma'_{\mathrm{A}} = (\sigma'_{\mathrm{A1}}, \sigma'_{\mathrm{A2}}, \sigma'_{\mathrm{A3}}) = (g_2^{\alpha} h^{r_m} (v' \prod_{j=1}^{n_c} v_j^{c_j})^{r_c}, g^{r_m}, g^{r_c})$，则有

$$\sigma'_{\mathrm{B1}}=(\sigma'_{\mathrm{A1}})^{rk_{\mathrm{A}\to\mathrm{B}}}h'^{r'_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r'_c}$$

$$=(g_2^{\alpha}h'^{r_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r_c})^{\frac{\beta}{\alpha}}h'^{r'_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r'_c}$$

$$=g_2^{\beta}h^{r_m\frac{\beta}{\alpha}+r'_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r_c\frac{\beta}{\alpha}+r'_c}$$

$$\sigma'_{\mathrm{B2}}=(\sigma'_{\mathrm{A2}})^{rk_{\mathrm{A}\to\mathrm{B}}}g^{r'_m}=(g^{r_m})^{\frac{\beta}{\alpha}}g^{r'_m}=g^{r_m\frac{\beta}{\alpha}+r'_m}$$

$$\sigma'_{\mathrm{B3}}=(\sigma'_{\mathrm{A3}})^{rk_{\mathrm{A}\to\mathrm{B}}}g^{r'_c}=(g^{r_c})^{\frac{\beta}{\alpha}}g^{r'_c}=g^{r_c\frac{\beta}{\alpha}+r'_c}$$

部分盲代理重签名 $\sigma'_{\mathrm{B}}=(\sigma'_{\mathrm{B1}},\sigma'_{\mathrm{B2}},\sigma'_{\mathrm{B3}})$ 的正确性验证如下

$$e(\sigma'_{\mathrm{B1}},g)=e(g_2^{\beta}h^{r_m\frac{\beta}{\alpha}+r'_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r_c\frac{\beta}{\alpha}+r'_c},g)$$

$$=e(g_2^{\beta},g)e(h^{r_m\frac{\beta}{\alpha}+r'_m},g)e((v'\prod_{j=1}^{n_c}v_j^{c_j})^{r_c\frac{\beta}{\alpha}+r'_c},g)$$

$$=e(g_2,g^{\beta})e(h,g^{r_m\frac{\beta}{\alpha}+r'_m})e(v'\prod_{j=1}^{n_c}v_j^{c_j},g^{r_c\frac{\beta}{\alpha}+r'_c})$$

$$=e(g_2,pk_{\mathrm{B}})e(h,\sigma'_{\mathrm{B2}})e(v'\prod_{j=1}^{n_c}v_j^{c_j},\sigma'_{\mathrm{B3}})$$

3) 重签名的正确性

给定部分盲代理重签名 $\sigma'_{\mathrm{B}}=(\sigma'_{\mathrm{B1}},\sigma'_{\mathrm{B2}},\sigma'_{\mathrm{B3}})=(g_2^{\beta}h'^{r^{\mathrm{B}}_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r^{\mathrm{B}}_c},g'^{r^{\mathrm{B}}_m},g'^{r^{\mathrm{B}}_c})$ 和委托者公钥 $pk_{\mathrm{B}}=g^{\beta}$，受托者进行脱盲处理可得

$$\sigma_{\mathrm{B1}}=(\sigma'_{\mathrm{B1}})((u'\prod_{i=1}^{n_m}u_i^{m_i})(v'\prod_{j=1}^{n_c}v_j^{c_j})^t)^y$$

$$=(g_2^{\beta}h'^{r^{\mathrm{B}}_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r^{\mathrm{B}}_c})((u'\prod_{i=1}^{n_m}u_i^{m_i})(v'\prod_{j=1}^{n_c}v_j^{c_j})^t)^y$$

$$=(g_2^{\beta}(u'\prod_{i=1}^{n_m}u_i^{m_i})^{tr^{\mathrm{B}}_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r^{\mathrm{B}}_c})((u'\prod_{i=1}^{n_m}u_i^{m_i})(v'\prod_{j=1}^{n_c}v_j^{c_j})^t)^y$$

$$=g_2^{\beta}(u'\prod_{i=1}^{n_m}u_i^{m_i})^{tr^{\mathrm{B}}_m+y}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r^{\mathrm{B}}_c+ty}$$

$$\sigma_{\mathrm{B2}}=(\sigma'_{\mathrm{B2}})^t g^y=(g^{r^{\mathrm{B}}_m})^t g^y=g^{r^{\mathrm{B}}_m t+y}$$

$$\sigma_{\mathrm{B3}}=(\sigma'_{\mathrm{B3}})g^{yt}=(g^{r^{\mathrm{B}}_c})g^{yt}=g^{r^{\mathrm{B}}_c+ty}$$

重签名 $\sigma_{\mathrm{B}}=(\sigma_{\mathrm{B1}},\sigma_{\mathrm{B2}},\sigma_{\mathrm{B3}})$ 的正确性验证如下

$$e(\sigma_{\mathrm{B1}},g)=e(g_2^{\beta}(u'\prod_{i=1}^{n_m}u_i^{m_i})^{tr^{\mathrm{B}}_m+y}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{r^{\mathrm{B}}_c+ty},g)$$

$$=e(g_2^{\beta},g)e((u'\prod_{i=1}^{n_m}u_i^{m_i})^{tr^{\mathrm{B}}_m+y},g)e((v'\prod_{j=1}^{n_c}v_j^{c_j})^{r^{\mathrm{B}}_c+ty},g)$$

$$=e(g_2,g^{\beta})e(u'\prod_{i=1}^{n_m}u_i^{m_i},g^{tr^{\mathrm{B}}_m+y})e(v'\prod_{j=1}^{n_c}v_j^{c_j},g^{r^{\mathrm{B}}_c+ty})$$

$$=e(g_2,pk_{\mathrm{B}})e(u'\prod_{i=1}^{n_m}u_i^{m_i},\sigma_{\mathrm{B2}})e(v'\prod_{j=1}^{n_c}v_j^{c_j},\sigma_{\mathrm{B3}})$$

5.2　双向多用性分析

代理者利用重签名密钥 $rk_{\mathrm{A}\to\mathrm{B}}=\dfrac{\beta}{\alpha}$ 将受托者的签名转换委托者的签名，但通过 $rk_{\mathrm{A}\to\mathrm{B}}$ 很容易计算出 $rk_{\mathrm{B}\to\mathrm{A}}=\dfrac{\alpha}{\beta}=\dfrac{1}{rk_{\mathrm{A}\to\mathrm{B}}}$，实现委托者与受托者的签名转换，即本文方案满足双向性。因为签名算法输出的原始签名 σ_{A} 和脱盲算法输出的重签名 σ_{B} 是计算不可区分的，所以新方案具有透明性和多用性。

5.3　部分盲性证明

定理 1　本文提出的部分盲代理重签名方案具有部分盲性。

证明　假设攻击者 $\mathcal{F}$ 能转换生成任意消息的部分盲代理重签名，即 $\mathcal{F}$ 掌握了重签名密钥，它的目标是将最终的重签名与中间的部分盲代理重签名相对应。挑战者 $\mathcal{B}$ 拥有受托者的私钥，能生成任意消息的原始签名，将与 $\mathcal{F}$ 进行如下的模拟游戏。

系统建立。$\mathcal{B}$ 运行 Setup 算法、KeyGen 算法和 ReKey 算法生成系统参数 par、2 个公私钥对 (g^{α},α) 和 (g^{β},β) 以及重签名密钥 $rk_{\mathrm{A}\to\mathrm{B}}=\dfrac{\beta}{\alpha}(\mathrm{mod}\ p)$，将 par 和 $rk_{\mathrm{A}\to\mathrm{B}}$ 发送给 $\mathcal{F}$。

准备。$\mathcal{F}$ 选择 2 个等长的消息 (m_0,m_1) 以及公共消息 c，将 (m_0,m_1,c) 发送给 $\mathcal{B}$。

询问。$\mathcal{B}$ 随机选取比特 $b\in\{0,1\}$ 和 $t_b,t_{1-b}\in Z_p^*$，运行 Blind 算法生成 m_b 的盲化消息 $h_b=(u'\prod_{i=1}^{n_m}u_i^{m_{b,i}})^{t_b}$ 和 m_{1-b} 的盲化消息 $h_{1-b}=(u'\prod_{i=1}^{n_m}u_i^{m_{1-b,i}})^{t_b}$ 以及盲化签名 $\sigma'_{\mathrm{A},b}$ 与 $\sigma'_{\mathrm{A},1-b}$，请求 $\mathcal{F}$ 对 $(c,h_b,\sigma'_{\mathrm{A},b})$ 和 $(c,h_{1-b},\sigma'_{\mathrm{A},1-b})$ 进行重签名。$\mathcal{F}$ 运行 ReSign 算法生成部分盲代理签名 $\sigma'_{\mathrm{B},b}$ 和 $\sigma'_{\mathrm{B},1-b}$，并发送给 $\mathcal{B}$。$\mathcal{B}$ 随机选取 $y_b,y_{1-b}\in Z_p^*$，运行 Unblind 算法得

$$\sigma_{\mathrm{B},k,1}=(\sigma'_{\mathrm{B},k,1})((u'\prod_{i=1}^{n_m}u_i^{m_{k,i}})(v'\prod_{j=1}^{n_c}v_j^{c_j})^{t_k})^{y_k}$$

$$\sigma_{\mathrm{B},k,2}=(\sigma'_{\mathrm{B},k,2})^{t_k}g^{y_k}$$

$$\sigma_{\mathrm{B},k,3}=(\sigma'_{\mathrm{B},k,3})g^{y_k t_k}$$

其中，$k\in\{0,1\}$，(m_b,c) 和 (m_{1-b},c) 的重签名为 $\sigma_{\mathrm{B},b}=(\sigma_{\mathrm{B},b,1},\sigma_{\mathrm{B},b,2},\sigma_{\mathrm{B},b,3})$ 与 $\sigma_{\mathrm{B},1-b}=(\sigma_{\mathrm{B},1-b,1},\sigma_{\mathrm{B},1-b,2},\sigma_{\mathrm{B},1-b,3})$，然后将 $(m_b,c,\sigma_{\mathrm{B},b})$ 和 $(m_{1-b},c,\sigma_{\mathrm{B},1-b})$ 发送给 $\mathcal{F}$。

应答。$\mathcal{F}$ 最后输出一个对 b 的猜测 b'。

下面，分析 $\mathcal{F}$ 正确猜对 b 的概率。因为盲化因子 t_b,t_{1-b},y_b,y_{1-b} 是在 Z_p^* 上随机选取的，h_b 和 $\sigma_{\mathrm{B},b}$ 完全独立于 (m_b,t_b,y_b)，h_{1-b} 和 $\sigma_{\mathrm{B},1-b}$ 完全独立于 $(m_{1-b},t_{1-b},y_{1-b})$，所以 $(m_b,c,\sigma_{\mathrm{B},b})$ 和 $(m_{1-b},c,\sigma_{\mathrm{B},1-b})$ 的分布对 $\mathcal{F}$ 来说相同的，并且完全独立于 b。由于 b 是随机选取的，并且 t_b,t_{1-b},y_b,y_{1-b} 在部分盲代理重签名的过程中一直存在且完全独立于 $\mathcal{F}$ 的视角，$(m_b,c,\sigma_{\mathrm{B},b})$ 和 $(m_{1-b},c,\sigma_{\mathrm{B},1-b})$ 在计算上具有不可区分性，因此，$\mathcal{F}$ 正确猜对 b 的概率是 $\frac{1}{2}$，即攻击者无法以不可忽略的概率猜对 b。因为攻击者 $\mathcal{F}$ 无法将部分盲代理重签名与最终的重签名相对应，所以新方案具有部分盲性。

5.4 不可伪造性证明

定理 2 本文提出的部分盲代理重签名方案在标准模型下是存在不可伪造的。

证明 假设攻击者 $\mathcal{A}$ 在多项式时间内最多进行 q_{S} 次签名询问和 q_{RS} 次重签名询问后，以一个不可忽略的概率 ε 攻破新方案的存在不可伪造性，则存在攻击者 $\mathcal{C}$ 将以 $\frac{\varepsilon}{8(q_{\mathrm{S}}+q_{\mathrm{RS}})^2(n_m+1)(n_c+1)}$ 的概率求解 CDH 问题。给定 CDH 问题实例 (g,g^a,g^b)，$\mathcal{C}$ 与 $\mathcal{A}$ 进行如下的模拟游戏。

系统建立。$\mathcal{C}$ 设置 $l_m=l_c=2(q_{\mathrm{S}}+q_{\mathrm{RS}})$，满足 $l_m(n_m+1)<p$，$l_c(n_c+1)<p$；随机选取 k_m 和 k_c，满足 $0\leqslant k_m\leqslant n_m$，$0\leqslant k_c\leqslant n_c$；在 Z_{l_m} 上随机选取 n_m+1 个元素 $y',y_i(i=1,\cdots,n_m)$，在 Z_{l_c} 上随机选取 n_c+1 个元素 $z',z_i(i=1,\cdots,n_c)$，在 Z_p^* 上随机选取 n_m+n_c+2 个元素 w'、$w_i(i=1,\cdots,n_m)$、d'、$d_j(j=1,\cdots,n_c)$。对于 n_m 比特长的签名消息 m 和 n_c 比特长的公共消息 c，定义 $F(m)=y'+\sum_{i=1}^{n_m}y_im_i-l_mk_m$，$J(m)=w'+\sum_{i=1}^{n_m}w_im_i$，$K(c)=z'+\sum_{i=1}^{n_c}z_ic_i-l_ck_c$ 和 $L(c)=d'+\sum_{j=1}^{n_c}d_jc_j$。令目标用户的公钥 $pk_t=g^a$，$g_2=g^b$，参数 $u'=g_2^{-l_mk_m+y'}g^{w'}$，$u_i=g_2^{y_i}g^{w_i}$，$v'=g_2^{-l_ck_c+z'}g^{d'}$，$v_j=g_2^{z_j}g^{d_j}$，$1\leqslant i\leqslant n_m$，$1\leqslant j\leqslant n_c$。于是，可得 $u'\prod_{i=1}^{n_m}u_i^{m_i}=g_2^{F(m)}g^{J(m)}$，$v'\prod_{j=1}^{n_c}v_j^{c_j}=g_2^{K(c)}g^{L(c)}$。最后，$\mathcal{C}$ 将参数 $par=(G_1,G_2,p,e,g,g_2,pk_t,u',u_1,\cdots,u_{n_m},v',v_1,\cdots,v_{n_c})$ 发送给 $\mathcal{A}$。

由于 $\mathcal{A}$ 已掌握除目标用户之外其余用户的私钥，目标用户的私钥 a 对挑战者 $\mathcal{B}$ 也是未知的，所以 $\mathcal{A}$ 不能发起密钥询问和重签名密钥询问。

询问。$\mathcal{A}$ 可以自适应地向 $\mathcal{C}$ 进行一系列如下签名预言机和重签名预言机的询问。

签名询问。对于 $\mathcal{A}$ 发起的签名询问 (m,c)，$\mathcal{C}$ 随机选取 $s_m,s_c\in Z_p^*$，并进行以下操作。

1) 如果 $K(c)\neq 0(\mathrm{mod}\,p)$，计算

$$\sigma_1=g_1^{-\frac{L(c)}{K(c)}}(u'\prod_{i=1}^{n_m}u_i^{m_i})^{s_m}(v'\prod_{j=1}^{n_c}v_j^{c_j})^{s_c}$$

$\sigma_2=g^{s_m}$，$\sigma_3=g_1^{-\frac{1}{K(c)}}g^{s_c}$，返回 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$ 给 $\mathcal{A}$。从攻击者 $\mathcal{A}$ 的视角来看，模拟游戏生成的 σ 与实际方案产生的签名在计算上是不可区分的。

2) 如果 $K(c)=0(\mathrm{mod}\,p)$，$\mathcal{C}$ 宣告模拟失败，退出游戏。

重签名询问。$\mathcal{A}$ 随机选取 $t\in Z_p^*$，计算 m 的盲化消息 $h=(u'\prod_{i=1}^{n_m}u_i^{m_i})^t$ 和 (m,c) 对应于公钥 pk_i 的盲化签名 $\sigma_i'=(\sigma_{i1}',\sigma_{i2}',\sigma_{i3}')$，然后向 $\mathcal{C}$ 发起重签名询问 $(c,h,\sigma_i'=(\sigma_{i1}',\sigma_{i2}',\sigma_{i3}'),pk_i)$。如果验证等式 $e(\sigma_{i1}',g)=e(g_2,pk_i)e(h,\sigma_{i2}')e(v'\prod_{j=1}^{n_c}v_j^{c_j},\sigma_{i3}')$ 不成立，$\mathcal{C}$ 输出 $\perp$；否则，$\mathcal{C}$ 以 (h,c) 为输入进行签名询问，并将询问的结果 $\sigma_t'=(\sigma_{t1}',\sigma_{t2}',\sigma_{t3}')$ 返回给 $\mathcal{A}$。$\mathcal{A}$ 随机选取 $y\in Z_p^*$，计算 (m,c) 的最终重签名 $\sigma_t=(\sigma_{t1},\sigma_{t2},\sigma_{t3})=((\sigma_{t1}')((u'\prod_{i=1}^{n_m}u_i^{m_i})(v'\prod_{j=1}^{n_c}v_j^{c_j})^t)^y,(\sigma_{t2}')^tg^y,(\sigma_{t3}')g^{ty})$。

伪造。经过有限次的询问后，$\mathcal{A}$ 最后输出一个对应于 pk_t 的 m^* 和 c^* 的伪造 σ^*。如果 $F(m^*)\neq 0(\mathrm{mod}\,p)$ 或 $K(c^*)\neq 0(\mathrm{mod}\,p)$，$\mathcal{C}$ 宣告模拟失败，终止游戏；否则，$\mathcal{C}$ 利用伪造 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$ 计算

$$\frac{\sigma_1^*}{(\sigma_2^*)^{J(m^*)}(\sigma_3^*)^{L(c^*)}}=\frac{g_2^a(u'\prod_{i=1}^{n_m}u_i^{m_i^*})^{r_m^*}(v'\prod_{j=1}^{n_c}v_j^{c_j^*})^{r_c^*}}{(g^{r_m^*})^{J(m^*)}(g^{r_c^*})^{L(c^*)}}$$

$$= \frac{g_2^a (u' \prod_{i=1}^{n_m} u_i^{m_i^*})^{r_m^*} (v' \prod_{j=1}^{n_c} v_j^{c_j^*})^{r_c^*}}{(g^{r_m^*})^{J(m^*)} (g^{r_c^*})^{L(c^*)}}$$

$$= g_2^a = (g^b)^a = g^{ab}$$

从而解决 CDH 问题实例。

下面，分析 $\mathcal{C}$ 不退出模拟游戏并成功求解 CDH 问题的概率。设 $c_1', c_2', \cdots, c_{q_Q}'$ 是签名询问和重签名询问中出现的公共消息（但不包括 c^*），这里，$q_Q \leqslant q_S + q_{RS}$。与文献[6,7]分析的过程相似，$\mathcal{C}$ 要完成整个模拟过程，在询问阶段满足 $K(c_i') \neq 0 (\mathrm{mod}\ p)$，在伪造阶段满足 $F(m^*) = 0 (\mathrm{mod}\ p)$ 且 $K(c^*) = 0 (\mathrm{mod}\ p)$。定义 4 个事件 $E_i : K(c_i') \neq 0 (\mathrm{mod}\ p)$，$E_i' : K(c_i') \neq 0 (\mathrm{mod}\ l_c)$，$E^* : K(c^*) = 0 (\mathrm{mod}\ p)$，$M^* : F(m^*) = 0 (\mathrm{mod}\ p)$。事件 $\wedge_{i=1}^{q_Q} E_i \wedge E^*$ 与事件 M^* 是独立的，因此，$\mathcal{C}$ 不退出游戏的概率为 $\Pr[\neg abort] \geqslant \Pr[\wedge_{i=1}^{q_Q} E_i \wedge E^* \wedge M^*]$。由文献[6,7]可知

$$\Pr[\wedge_{i=1}^{q_Q} E_i \wedge E^*] \geqslant \frac{1}{4(q_S + q_{RS})(n_c + 1)}$$

$$\Pr[M^*] \geqslant \frac{1}{2(q_S + q_{RS})(n_m + 1)}$$

于是有

$$\Pr[\neg abort] \geqslant \Pr[\wedge_{i=1}^{q_Q} E_i \wedge E^*] \Pr[M^*]$$

$$\geqslant \frac{1}{4(q_S + q_{RS})(n_c + 1)} \frac{1}{2(q_S + q_{RS})(n_m + 1)}$$

$$= \frac{1}{8(q_S + q_{RS})^2 (n_m + 1)(n_c + 1)}$$

如果 $\mathcal{A}$ 以概率 ε 攻破新方案的存在不可伪造性，那么 $\mathcal{C}$ 将以 $\frac{\varepsilon}{8(q_S + q_{RS})^2 (n_m + 1)(n_c + 1)}$ 的概率解决 CDH 问题。

5.5　有效性分析

下面，将本文方案与已有的盲代理重签名方案进行计算开销和安全属性的比较，结果如表 1 所示。为了便于比较，假设所有方案选取相同长度的素数 p 和 2 个群 (G_1, G_2)。因为计算开销比较大的密码学操作是双线性对与指数运算，因此，表 1 主要分析讨论这 2 类运算，用 E 表示 G_1 上的一次指数运算，P 表示一次双线对运算。

由表 1 可知，文献[6,7]方案的计算开销和存储开销都比较小，但这 2 种方案都不具备致盲性。本文方案的计算开销大于文献[13,14]方案，但文献[13,14]方案存在严重的安全缺陷，无法抵抗受托者的重签名伪造攻击。文献[15]方案的重签名算法需要进行 7 次双线性对和 2 次幂运算，并且不满足多用性，因此该方案的实用性较差。本文所提方案同时满足多用性和部分盲性，不仅能保护受托者的隐私信息，还能保障代理者的合法权益，具有更强的应用性。

6　结束语

结合代理重签名和部分盲签名的思想，提出了部分盲代理重签名体制，将受托者和代理者提前协商的公共消息加入到重签名中，实现了代理者对重签名消息的隐私性和重签名过程的可控性。基于改进的 Shao 方案[7]，构造了一种基于标准模型架构的双向部分盲代理重签名方案，其安全性依赖于 CDH 问题。下一步的工作是设计具有更低计算复杂度的部分盲代理重签名方案。

表 1　　**计算开销与安全属性比较**

方案	重签名算法开销	盲化算法开销	签名长度开销	重签名长度开销	多用性	部分盲性
文献[6]方案	3*P*+2*E*	0	2|G_1|	2|G_1|	是	否
文献[7]方案	3*P*+4*E*	0	2|G_1|	2|G_1|	是	否
文献[13]方案	3*P*+2*E*	2*E*	2|G_1|	2|G_1|	是	否
文献[14]方案	4*P*	2*E*	3|G_1|	3|G_1|	是	否
文献[15]方案	7*P*+2*E*	5*E*	3|G_1|	2|G_1|	否	否
本文方案	4*P*+7*E*	6*E*	3|G_1|	3|G_1|	是	是

参考文献：

[1] BLAZE M, BLEUMER G, STRUSS M. Divertible protocols and atomic proxy cryptography[C]// EUROCRYPT'98. 1998: 127-144.

[2] HU X, LIU Y, XU H, et al. Analysis and improvement of

certificateless signature and proxy re-signature schemes[C]//2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference.2015: 166-170.

[3] JIANG M M, HU Y P, WANG B C, et al. Lattice-based multi-use unidirectional proxy re-encryption[J]. Security and Communication Networks, 2015, 8(18): 3796-3803.

[4] ATENIESE G, HOHENBERGER S. Proxy re-signatures: new definitions, algorithms, and applications[C]//The 12th ACM CCS. 2005: 310-319.

[5] CANETTI R, GOLDREICHO O, HALEVI S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4): 557-594.

[6] SHAO J, CCAO Z, WANG L, et al. Proxy re-signature schemes without random oracles[C]// INDO-CRYPT 2007. 2007: 197-209.

[7] KIM K, YIE I, LIM S. Remark on shao et al's bidirectional proxy re-signature scheme in indocrypt'07 [J]. International Journal of Network Security, 2009, 8(3): 308-311.

[8] TIAN M. Identity-based proxy re-signatures from lattices[J]. Information Processing Letters, 2015, 115(4): 462-467.

[9] CHEN L, CHEN X, SUN Y, et al. A new certificateless proxy re-signature scheme in the standard model[C]//IEEE Computational Intelligence and Design. 2014: 202-206.

[10] YANG X, GAO G, WANG C. On-line/off-line threshold proxy re-signature scheme through the simulation approach[J]. Applied Mathematics & Information Sciences, 2015, 9(6): 3251-3261.

[11] TIAN M M. Identity-based proxy re-signatures from lattices[J]. Information Processing Letters, 2015, 115(4): 462-467.

[12] YANG X D, LI C M, LI Y, et al. Divisible on-line/off-line proxy re-signature[J]. Applied Mathematics & Information Sciences, 2015, 9(2): 759-767.

[13] 邓宇乔, 杜明辉, 尤再来, 等. 一种基于标准模型的盲代理重签名方案[J]. 电子与信息学报, 2010, 32(5): 1219-1223.
DENG Y Q, DU M H, YOU Z L, et al. A blind proxy re-signatures scheme based on standard model[J]. Journal of Electronics & Information Technology, 2010, 32(5): 1219-1223.

[14] 冯涛, 梁一鑫. 可证安全的无证书盲代理重签名[J]. 通信学报, 2012, 31(S1): 58-69.
FENG T, LIANG Y X. Provably secure certificate less blind proxy re-signatures[J]. Journal on Communications, 2012, 31(S1): 58-69.

[15] 胡小明, 杨寅春, 刘琰. 一种基于标准模型的盲代理重签名方案的安全性分析和改进[J]. 小型微型计算机系统, 2011, 32(10): 2008-2011.
HU X M, YANG Y C, LIU Y. Analysis and improvement of a blind proxy re-signature scheme based on standard model[J]. Journal of Chinese Computer Systems, 2011, 32(10): 2008-2011.

[16] 张延红, 陈明. 标准模型下增强的基于身份部分盲签名[J]. 四川大学学报: 工程科学版, 2014, 46(1): 95-101.
ZHANG Y H, CHEN M. Extended identity-based partially blind signature scheme in the standard model[J]. Journal of Sichuan University(Engineering Science Edition), 2014, 46(1): 95-101.

[17] TAHAT N, ADBALLAH E E. A proxy partially blind signature approach using elliptic curve cryptosystem[J]. International Journal of Mathematics in Operational Research, 2016, 8(1): 87-95.

[作者简介]

杨小东（1981-），男，甘肃甘谷人，西北师范大学副教授，主要研究方向为密码学及云计算安全。

陈春霖（1995-），女，甘肃兰州人，西北师范大学硕士生，主要研究方向为大数据安全。

杨平（1993-），男，甘肃灵台人，西北师范大学硕士生，主要研究方向为网络与信息安全。

安发英（1991-），男，青海民和人，西北师范大学硕士生，主要研究方向为物联网安全。

麻婷春（1992-），女，甘肃武威人，西北师范大学硕士生，主要研究方向为云计算安全。

王彩芬（1963-），女，河北安国人，博士，西北师范大学教授、博士生导师，主要研究方向为密码学、网络安全、信息安全。