

无证书公钥密码体制→传统公钥基础设施异构环境下部分盲签密方案

王彩芬^{*①②} 许钦百^① 刘超^① 成玉丹^① 赵冰^①

^①(西北师范大学 计算机科学与工程学院 兰州 730070)

^②(深圳技术大学 大数据与互联网学院 深圳 518118)

摘 要: 该文提出在无证书公钥密码体制(CLPKC)和传统公共密钥基础设施体制(TPKI)下部分盲签密方案的形式化定义, 并在此基础上提出一个在CLPKC-TPKI环境下具有双线性对的部分盲签密方案。依据随机预言模型, 计算Diffie-Hellman困难问题(CDHP)和修改逆计算Diffie-Hellman困难问题(MICDHP)假设, 使得方案在异构环境下满足不可伪造性、机密性、部分盲性、不可跟踪性、不可否认性等性质。最后和相关方案进行了比较分析, 该文方案在增加了盲性同时并未显著增加计算量的开销。

关键词: 异构签密; 部分盲签密; 修改逆计算Diffie-Hellman困难问题

中图分类号: TN918.4

文献标识码: A

文章编号: 1009-5896(2019)08-1823-08

DOI: 10.11999/JEIT180850

Partial Blind Signcryption Scheme in CLPKC-to-TPKI Heterogeneous Environment

WANG Caifen^{*①②} XU Qinbai^① LIU Chao^① CHENG Yudan^① ZHAO Bing^①

^①(College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China)

^②(College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China)

Abstract: The definition and security models of partial blind signcryption scheme in heterogeneous environment between CertificateLess Public Key Cryptography (CLPKC) and Traditional Public Key Infrastructure (TPKI) are proposed, and a construction by using the bilinear pairing is proposed. Under the random oracle model, based on the assumptions of Computational Diffie-Hellman Problem (CDHP) and Modifying Inverse Computational Diffie-Hellman (MICDHP), the scheme is proved to meet the requirement of the unforgeability, confidentiality, partial blindness, and untraceability, undeniability. Finally, compared with the related scheme, the scheme increases the blindness and does not significantly increase the computational cost.

Key words: Heterogeneous signcryption; Partial blind signcryption; Modifying Inverse Computational Diffie-Hellman Problem (MICDHP)

1 引言

部分盲签密是由盲签名发展演变而来并在一个逻辑步骤里让签密人同时对消息完成签密和加密工作, 被广泛用于电子商务、移动通信和智能卡片等^[1,2]。2010年, 邓宇桥等人^[3]提出了一种基于标准

模型的盲代理重签名方案。2015年, 刘哲等人^[4]通过对临时公钥进行盲签名完成了车载网络中分布式的假名生成。2017年, 文献^[5]提出了UC安全的自认证盲签密协议。同年傅晓红等人^[6]在基于代理的密码货币支付系统模型上给出了基于盲签名算法的实现方案。已有的文献大多是研究单一体制下的盲签密方案, 研究异构环境下部分盲签密方案相对较少。

无证书公钥密码体制(CertificateLess Public Key Cryptography, CLPKC)由可信第三方密钥产生中心(Key Generation Center, KGC)产生部分私钥。传统公钥基础设施(Traditional Public Key Infrastructure cryptosystems, TPKI)是由证书机构(Certificate Authority, CA)通过对用户颁发公钥证书为密钥提供认证。由于密码体制的具体应用场景不同, 交互使用情境越发频繁。2010年, Sun等人^[7]

收稿日期: 2018-08-31; 改回日期: 2019-02-25; 网络出版: 2019-03-04

*通信作者: 王彩芬 wangcf@nwnu.edu.cn

基金项目: 国家自然科学基金(61202395, 61562077, 61662069, 61662071), 甘肃省自然科学基金(145RJDA325), 甘肃省高等学校科研项目(2017A-003, 2018A-207)

Foundation Items: The National Natural Science Foundation of China (61202395, 61562077, 61662069, 61662071), The Natural Science Foundation of Gansu Province of China (145RJDA325), The Scientific Research Projects of Universities in Gansu Province(2017A-003, 2018A-207)

首次提出异构签密方案并构造了传统公钥密码和身份公钥密码环境下异构签密方案。2011年, Huang等人^[8]构造了身份公钥密码体制和传统公钥密码体制下异构签密方案。2016年, 张玉磊等人^[9]提出了从无证书公钥密码体制到传统公钥密码体制异构签密方案的形式化定义及其方案。

本文定义了CLPKC→TPKI异构环境下部分盲签密方案的形式化和安全模型, 并以此提出了具体方案。在已有的盲签密方案中, 消息拥有者与签密人通常是分开的。而本文方案的消息拥有者与签密人为同一人, 因此本文方案可以应用在文件等消息的审批业务流程场景中。呈递消息方既是消息发送方也是接收方。签密过程由消息被呈递方完成, 即只标记消息经手方, 签密者在不知消息具体内容的情况下仅根据协议消息辨识消息类别进行签密认证。

2 具体的CLPKC→TPKI异构环境下部分盲签密方案定义及具体方案

2.1 方案的形式化定义

CLPKC→TPKI异构环境部分盲签密需完成以下算法过程:

(1) CLPKC环境下系统建立算法。该算法由CLPKC环境系统的KGC运行。输入安全参数 k , 输出系统主密钥 s (KGC的私钥)、系统公共密钥 P_{pb} (KGC的公钥)和系统参数 ps_1 。KGC公开 P_{pb} 和 ps_1 , 保密 s ;

(2) TPKI环境下系统建立及密钥生成算法。该算法由PKI环境系统中的CA生成并发布系统参数 ps_2 。生成公钥 pk_i 和私钥 sk_i , CA对用户的公钥进行签名并输出用户证书;

(3) CLPKC环境下的KGC生成部分私钥。输入用户身份 ID_i , ps_1 和 s , 输出用户的部分私钥 D_i ;

(4) CLPKC环境下用户完成最后的密钥生成算法。用户选择秘密值 x_i , 由 D_i 和 ps_1 , 输出完整私钥 $S_i = (D_i, x_i)$ 和公钥 P_i ;

(5) 两方用户共同协商生成协商消息 c , 且过程中均可见;

(6) 承诺: CLPKC用户完成承诺过程;

(7) 部分盲化: TPKI用户输入 pk_i , P_i , 消息 m , c 及 ps_2 , 完成对 m 和 c 的盲化过程;

(8) 签密算法: CLPKC用户输入 S_i , 输出密文 δ ;

(9) 去盲: δ 送回TPKI用户去盲;

(10) 解签密算法: TPKI用户进行解签密算法, 输出 m 或者符号“ $\perp$ ”。其中, “ $\perp$ ”表示密文不合法。

算法须满足一致性约束条件: 在去盲条件下若

$\delta = \text{Signcrypt}(m, c, S_A, pk_B)$, 则 $m = \text{Unsigncrypt}(\delta, c, P_A, sk_B)$ 成立; 在盲化条件下若 $\bar{\delta} = \text{Signcrypt}(\bar{m}, c, S_A, pk_B)$, 则 $\bar{m} = \text{Unsigncrypt}(\bar{\delta}, c, P_A, sk_B)$ 同样成立。其中 m 为明文消息, $\bar{m}$ 为盲化后的消息。

2.2 具体方案

基于文献^[9,10]本文提出一个具体的CLPKC→TPKI异构环境下部分盲签密方案。

(1) TPKI系统建立及密钥生成算法: 设 k_2 为TPKI系统安全参数, q_2 为 k_2 比特的大素数, 定义阶均为 q_2 的加法群 G_{T1} 和乘法群 G_{T2} , 生成元 $P_2 \in G_{T1}$, l_2 表示 G_{T1} 元素长度, 双线性映射^[11] $e': G_{T1} \times G_{T1} \rightarrow G_{T2}$ 。发布系统参数 $Ps_2 = \{G_{T1}, G_{T2}, e', q_2, P_2\}$ 。用户产生公/私钥对, 公钥为 $pk_B = x_B P_2$, 私钥为 $sk_B = x_B$, 且 $x_B \in Z_{q_1}^*$ 。CA生成并发布用户公钥证书;

(2) CLPKC系统建立算法: 设 k_1 为CLPKC系统安全参数, q_1 为 k_1 比特的大素数, 定义阶均为 q_1 的加法群 G_1 和乘法群 G_2 , 生成元 $P_1 \in G_1$, l_1 表示 G_1 元素长度, 双线性映射^[11] $e: G_1 \times G_1 \rightarrow G_2$ 。KGC定义哈希函数: $H_1: \{0, 1\}^{k_1} \rightarrow G_1$, $H_2: G_1 \rightarrow Z_{q_1}^*$, $H_3: \{0, 1\}^* \rightarrow Z_{q_1}^*$, $H_4: \{0, 1\}^* \rightarrow \{0, 1\}^{l_1}$, $H_5: \{0, 1\}^* \rightarrow \{0, 1\}^{l_2}$ 其中, l_1 和 l_2 为函数长度。KGC选取 $s \in Z_{q_1}^*$, 计算 $P_{pb} = sP_1$, 发布系统参数 $Ps_1 = \{G_1, G_2, e, q_1, P_1, P_{pb}, H_1, H_2, H_3, H_4\}$ 并保存 s ;

(3) CLPKC部分私钥生成算法: 用户提交 ID_A , KGC计算 $Q_A = H_1(ID_A)$ 和 $D_A = sQ_A$, 发送 D_A 给用户;

(4) CLPKC密钥生成算法: 选取秘密值 $x_A \in_R Z_{q_1}^*$, 计算公钥 $P_A = x_A P_1$, $y_A = H_2(P_A)$ 生成私钥 $S_A = \frac{1}{x_A + y_A} D_A$;

(5) 签密算法:

(a) 承诺: 用户A选择 $r_1 \in_R Z_{q_1}^*$, $r_2 \in_R Z_{q_2}^*$, 计算 $Q_A = H_1(ID_A)$, $U = r_1 Q_A$ 和 $V = r_2 P_2$ 之后, 将承诺 (U, V) 发送给用户B;

(b) 盲化: 用户B选盲化参数 $\alpha \in_R Z_{q_2}^*$, $\beta \in_R Z_{q_2}^*$, 计算 $L_1 = \alpha U$, $L_2 = \beta V$, $h = H_3(m, c, U, P_A, pk_B, L_1, L_2)$ 和 $h' = h\beta^{-1}$, $\bar{m} = (m \| c) \oplus H_4(V, \alpha, \beta, sk_B)$ 之后将 $(h', \bar{m})$ 送给用户A;

(c) 签密: 用户A计算 $T = r_2 pk_B$, $W = (r_1 H_3(c) + h') S_A$ 和 $Q = \bar{m} \oplus H_5(V, pk_B, T)$, 将密文 $\delta = (Q, W)$ 送给用户B;

(6) 解签密算法: 用户B得到部分盲签密 (W, U, Q) 后执行以下过程;

(a) 去盲: 用户B计算 $T' = sk_B V$, $U' = \beta U$,

$W' = \beta W$ 和 $Q' = Q \oplus H_4(V, \alpha, \beta, sk_B)$;

(b) 解签密: 运算 $Q'' = Q' \oplus H_5(V, pk_B, T')$
 $= m \parallel c$ 。

(7) 检查等式 $e(W', P_A + y_A P_1) \stackrel{?}{=} e(U' H_3(c) + h Q_A, P_{pb})$ 是否成立。成立则返回 m , 否则返回错误符号“ $\perp$ ”;

由一致性约束条件可得, 签密密文在盲化条件下的验证结果形式上应与去盲条件下验证结果保持一致, 即 W' 与 W 均能通过验证等式 $e(W, P_A + y_A P_1) = e(U H_3(c) + h' Q_A, P_{pb})$ 。

3 CLPKC→TPKI异构环境下部分盲签密方案安全模型及安全性分析

安全模型由不可伪造性游戏和机密性游戏组成。

3.1 不可伪造性CLPKC→TPKI

CLPKC→TPKI异构环境下部分盲签密方案的不可伪造性主要考虑两类伪造者 A_I 和 A_{II} ^[12] 的攻击。 A_I 类敌手实现公钥替换攻击; A_{II} 类敌手实现部分私钥实现KGC攻击。

游戏1 (EUF-CLPKC→TPKI-HSC-CMA-I) 假定 F 为挑战者, CLPKC→TPKI异构环境下部分盲签密方案针对敌手 A_I 的适应性选择消息和身份的攻击游戏包括初始阶段、攻击阶段(部分私钥询问、秘密值提取询问、公钥询问、公钥替换询问、部分盲签密询问)和伪造阶段。

初始阶段: F 输入系统安全参数 k_2 运行“CLPKC环境系统建立算法”生成系统参数 ps_1 系统公钥 P_{pb} 和系统主密钥 s ; F 输入系统安全参数 k_1 运行“TPKI环境系统建立及密钥生成算法”生成系统参数 ps_2 和用户的公/私钥对 (pk_j, sk_j) , F 设置协商消息 c 后发送 ps_1, ps_2, P_{pb} 和 (pk_j, sk_j) 给 A_I 。 F 保密系统主密钥 s 。

攻击阶段: F 与 A_I 模拟过程中, 能够对下列预言机进行多项式有界次的适应性询问。

(1) 部分私钥询问: A_I 选择一个用户身份信息 ID_i 并提交给 F , 若列表中已存在选择的信息则返回, 否则 F 运行“CLPKC环境下的部分私钥生成算法”, 获得对应的部分私钥 D_i 并返回给 A_I ;

(2) 秘密值提取询问: A_I 输入 ID_i 并提交给 F , 若列表中已存在选择的信息则返回, 如果 ID_i 的公钥未被替换则 F 运行“CLPKC环境下的密钥生成算法”获得 ID_i 对应的完整私钥 S_i 并返回给 A_I (获得私钥前可能首先会运行秘密值设置算法)。如果 ID_i 的公钥已经被替换, 那么让 F 回答这样的询问是不合理的;

(3) 公钥询问: A_I 输入 ID_i 并提交给 F , F 运行“CLPKC环境下公钥生成算法”将获得对应 ID_i 的公钥 P_i 并返回给 A_I ;

(4) 公钥替换询问: A_I 输入 ID_i 和对应选择的公钥 P'_i 并提交给 F , F 用 P'_i 替换 P_i , 并将原来的用户秘密值 x_i 改为“ $\perp$ ”。

(5) 部分盲签密询问: A_I 将 ID_i 、公钥 P_i 、接收者公钥 pk_j 、消息 $\bar{m}_i$ 和协议消息 c 提交给 F , F 调用“CLPKC环境下的密钥生成算法”用获得的 ID_i 和设置的秘密值计算得到私钥 S_i , 然后利用得到的 S_i 运行“签密算法”并返回密文 $\delta = \text{Signcrypt}(\bar{m}_i, c, S_i, pk_j)$ 送给 A_I 。本文采用的是弱无证书签密询问^[2], 即在这种询问情况下如果敌手替换了用户的公钥, 那么要求敌手提供替换后的公钥对应的秘密值。

伪造阶段: A_I 输出消息 $(ID^*, P^*, pk^*, \bar{m}^*, \delta^*)$, 如果以下3个条件成立, 则 A_I 赢得该游戏: (1) δ^* 对于消息 $\bar{m}^*, (ID^*, P^*)$ 和 pk^* 是一个合法的密文, “解签密算法”执行后不会输出符号“ $\perp$ ”; (2) A_I 没有提交过对 ID^* 的“部分私钥询问”, 也没有提交过对 ID^* 的“替换公钥询问”和“部分私钥询问”; (3) A_I 没有执行对 $(ID^*, P^*, pk^*, \bar{m}^*)$ 的“部分盲签密询问”。

定义1 (EUF-CLPKC→TPKI-HSC-CMA-I) 如果没有任何多项式有界敌手 A_I 在 t 时间内, 经过若干次询问后以至少 ε 的优势赢得游戏1, 那么称该CLPKC→TPKI异构签密方案在适应性选择消息和身份攻击下对于 A_I 攻击是 $(\varepsilon, t, q_{pr}, q_{kr}, q_{pk}, q_{rp}, q_s)$ -EUF-CLPKC→TPKI-HSC-CMA-I 安全的。

游戏2 (EUF-CLPKC→TPKI-HSC-CMA-II) 假定 F 为挑战者, CLPKC→TPKI异构部分盲签密方案针对敌手 A_{II} 的适应性选择消息和身份的攻击游戏包括初始阶段、攻击阶段(秘密值提取询问、公钥询问、部分盲签密询问)和伪造阶段。

初始阶段: F 分别在CLPKC和TPKI环境下系统建立算法, 产生对应的系统参数 ps_1 、系统公钥 P_{pb} 、系统主密钥 s 和 ps_2 及用户公钥/私钥对 (pk_j, sk_j) , F 设置协商消息 c 后发送 ps_1, ps_2, P_{pb}, s 和 (pk_j, sk_j) 给 A_{II} 。

攻击阶段: F 与 A_{II} 模拟过程中, 能够对下列预言机进行多项式有界次的适应性询问。

(1) 秘密值提取询问: A_{II} 输入 ID_i 并提交给 F , 若列表中已存在选择的信息则返回;

(2) 公钥询问: A_{II} 输入 ID_i 并提交给 F , F 运行“CLPKC环境下公钥生成算法”获得 ID_i 对应的 P_i 并返回给 A_{II} ;

(3) 部分盲签密询问: A_{II} 将 ID_i 、公钥 P_i 、接收者公钥 pk_j 、消息 $\bar{m}_i$ 和协议消息 c 提交给 F , F 调用

“CLPKC环境下的密钥生成算法”生成 S_i 运行“签密算法”并返回密文 $\delta = \text{Signcrypt}(\bar{m}_i, c, S_i, \text{pk}_j)$ 送给 A_{II} 。

伪造阶段： A_{II} 输出消息 $(ID^*, P^*, \text{pk}^*, \bar{m}^*, \delta^*)$ ，如果以下3个条件成立，则 A_{II} 赢得该游戏：(1) δ^* 对于消息 $\bar{m}^*$ 、 (ID^*, P^*) 和 pk^* 是一个合法密文，“解签密算法”执行后不会输出“ $\perp$ ”；(2) A_{II} 没有提交过对 ID^* 的“秘密值提取询问”；(3) A_{II} 没有执行对 $(ID^*, P^*, \text{pk}^*, \bar{m}^*)$ 的“部分盲签密询问”。

定义2 (EUF-CLPKC $\rightarrow$ TPKI-HSC-CMA-II)如果没有任何多项式有界敌手 A_I 在 t 时间内，经过若干次询问后以至少 ε 的优势赢得游戏2，那么称该CLPKC $\rightarrow$ TPKI异构签密方案在适应性选择消息和身份攻击下对 A_I 攻击是 $(\varepsilon, t, q_{kr}, q_{pk}, q_s)$ -EUF-CLPKC $\rightarrow$ TPKI-HSC-CMA-II安全的。

注意：在游戏1、游戏2中，敌手被允许获得TPKI环境下用户的私钥，确保方案满足不可伪造性的内部安全性。

定义3 如果不存在敌手 A_I 和 A_{II} 能够以不可忽略的概率在游戏1和游戏2中获胜，则该方案在适应性选择消息和身份攻击下具有存在不可伪造性即方案是EUF-CLPKC $\rightarrow$ TPKI-HSC-CMA安全的。

3.2 机密性CLPKC $\rightarrow$ TPKI

CLPKC $\rightarrow$ TPKI异构环境下签密方案的机密性主要分析来自普通敌手的攻击，敌手包括来自CLPKC环境和TPKI环境中的内部攻击敌手。

游戏3 (IND-CLPKC $\rightarrow$ TPKI-HSC-CC2) CLPKC-TPKI环境下异构签密方案的机密性表现在适应性选择密文攻击游戏中， A 为敌手， F 为挑战者。

初始阶段： F 分别在CLPKC和TPKI环境下系统建立算法，生成 ps_1, P_{pb}, s 和 ps_2 及 $(\text{pk}_j, \text{sk}_j)$ ， F 设置 c 后发送 $\text{ps}_1, \text{ps}_2, P_{pb}, s$ 和 $(\text{pk}_j, \text{sk}_j)$ 给 A 。

阶段1： F 与 A 模拟过程中， A 能够对签密预言机和解签密预言机进行询问。

(1) 部分盲签密询问： A 提交 $\bar{m}_i, c, S_i$ 及 pk_j ，执行“签密算法”生成并返回 $\delta = (Q, W)$ 送给 A ；

(2) 解签密询问： A 将 P_i 和 δ 给 F ， F 输入 sk_j 后运行“解签密算法”并将结果返回给 A 。

挑战阶段： A 决定何时结束“阶段1”进入“挑战阶段”。 A 选择两个等长的消息 $\bar{m}_0$ 和 $\bar{m}_1$ ， D_i, pk_j 发送给 F 。 F 首先生成 ID_i 对应 S_i ，并随机选择 $b \in \{0, 1\}$ ，对 $\bar{m}_b$ 执行“签密算法”获得 $\delta_b^* = \text{Signcrypt}(\bar{m}_b, c, S_i, \text{pk}_j)$ 发送给 A 。

阶段2： A 进行“阶段1”中除提交关于 δ_b^* 解签密询问以外的其他询问， F 反馈给 A 。其中，攻击者不能提交关于 δ_b^* 的解签密询问。

猜测阶段： A 选择 $b' \in \{0, 1\}$ ，如果 $b' = b$ 则 A 赢得游戏优势为： $\text{Adv}(A) = |\Pr[b' = b] - 1/2|$ ， $\Pr[b' = b]$ 表示 $b' = b$ 的概率。

注意：在游戏3中，敌手被允许获得CLPKC系统主密钥和用户秘密值，使得敌手可以获得用户完整私钥，以确保方案满足机密性的内部安全性。

定义4 如果没有任何多项式有界敌手 A 在 t 时间内，经过若干次询问后以至少 ε 的优势赢得游戏3，那么称该CLPKC $\rightarrow$ TPKI异构签密方案在适应性选密文攻击下具有密文不可区分性即机密性，则该方案对于 A 的攻击是 $(\varepsilon, t, q_k, q_s, q_u)$ -IND-CLPKC $\rightarrow$ TPKI-HSC-CCA2安全。

本文方案满足一致性约束条件因此盲化后的消息在满足不可伪造性和机密性的同时对去盲后的消息同样满足。

3.3 不可伪造性证明

定理1 随机预言模型下，假设计算Diffie-Hellman困难问题^[13](Computational Diffie-Hellman Problem, CDHP)和修改逆计算Diffie-Hellman困难问题(Modification Inverse Computational Diffie-Hellman Problem, MICDHP)困难，则方案依据安全模型对于 A_I 和 A_{II} 具有不可伪造性。

引理1 随机预言模型下，若存在一个敌手 A_I 能够以 ε 优势攻破本文方案，那么存在一个算法 F 能够以 $\left(1 - \frac{1}{q_{H_1} + q_{H_2} + q_{pr} + q_{kr} + q_{pk}}\right) \left(1 - \frac{(q_s + q_{H_4} + q_{H_5})}{2^{\text{poly}(k_1)}}\right) \varepsilon$ 的优势解决CDHP困难问题。

证明 A_I 是敌手， F 是CDHP问题挑战者。 F 给定一个CDHP问题实例 (P_1, aP_1, bP_1) ， F 的目标是使用 A_I 解决CDHP问题，即计算 abP_1 。

初始阶段： F 分别在CLPKC和TPKI环境下系统建立算法，产生 ps_1, ps_2 及 $(\text{pk}_j, \text{sk}_j)$ ，设 $P_{pb} = aP_1$ (F 不知道 a ， a 扮演KGC的主密钥)发送给 A_I 。

攻击阶段： F 与 A_I 模拟过程中， A_I 对预言机 $H_1 \sim H_5$ 进行询问 F 维护列表 $L_1 \sim L_5$ ， $L = (ID_i, x_i, P_i, v)$ 和 $L' = (ID_i, D_i)$ ，其中 $L_1 \sim L_5$ 更新保存 F 对预言机 $H_1 \sim H_5$ 的询问数据， L 列表存储公钥信息， L' 列表存储部分私钥询问信息。

H_1 询问： F 保持 $L_1 = (i, ID_i, *)$ 。 A_I 对于第 i 次非重复 $H_1(ID_i)$ 询问，(1)若 $ID_i = ID^*$ ，则 F 返回 $D_i = bP_1$ ，并将 $(i, ID_i, \perp)$ 增加到 L_1 。“ $\perp$ ”表示不能确定 bP_1 的系数；(2)若 $ID_i \neq ID^*$ ，则 F 从 Z_q^* 随机选取 r_i ，并将 (i, ID_i, r_i) 填入表 L_1 中，“*”表示空。

H_2 询问： F 保持 $L_2 = (P_i, y_i)$ ， A_I 询问 H_2 若 L_2 中存在则返回，否则 F 从 Z_q^* 随机选取 y_i 返回 y_i 并将 (P_i, y_i) 增加到 L_2 中。

H_3 询问： A_I 询问 H_3 , F 保持 $L_3 = (m, c, U_i, P_i, pk_j, L_{1i}, L_{2i}, z_i)$ 。若已存在则返回结果 z_i ；否则 F 从 Z_q^* 随机选取 z_i 返回给 A_I ，并且将 $(m, c, U_i, P_i, pk_j, L_{1i}, L_{2i}, z_i)$ 增加到 L_3 。

H_4 询问： A_I 询问 H_4 , F 保持列表 $L_4 = H_4(V_i, \alpha_i, \beta_i, x_j, u_i)$ 。若存在则返回结果 u_i ；否则随机选择 $u_i \in \{0, 1\}^l$ 返回给 A_I ，并且将 $(V_i, \alpha_i, \beta_i, x_j, u_i)$ 增加到 L_4 。

H_5 询问： A_I 询问 H_5 , F 保持 $L_5 = H_5(V_i, pk_j, T_i, d_i)$ 。若存在则返回结果 d_i ；否则随机选择 $d_i \in \{0, 1\}^l$ 提交给 A_I ，并将 (V_i, pk_j, T_i, d_i) 增加到 L_5 。

公钥询问： F 保持 $L = (ID_i, x_i, P_i, v)$, A_I 输入 ID_i 若存在则直接返回 P_i ；否则 F 从 Z_q^* 随机选取 x_i ，计算 $P_i = x_i P_1$ 返回给 A_I 并将 $(ID_i, x_i, P_i, 1)$ 增加到 L 。

秘密值提取询问： F 保持 $L = (ID_i, x_i, P_i, v)$, A_I 输入 ID_i 若存在并且 $v = 1$ 则直接返回 x_i ；若 L 中存在且 $v = 0$ ，则终止询问并返回。若 L 中不存在 F 执行“公钥询问”获得并返回 x_i 。

公钥替换询问： A_I 提交 ID_i 和 P'_i , F 查找 L 若存在对应 ID_i 则令 $P_i = P'_i$, $v = 0$ ；否则先对 ID_i 进行公钥询问，然后令 $P_i = P'_i$, $x_i = \perp$ 和 $v = 0$ 修改对应元组。

部分私钥询问： F 保持 $L' = (ID_i, D_i)$, A_I 输入 ID_i , (1) 若 $ID_i = ID^*$ 则 F 失败并终止；(2) 若 $ID_i \neq ID^*$ 且 L' 中存在则返回；否则 F 检查 L_1 获得 r_i 值，计算 $D_i = r_i a P_1$ 返回 ID_i 将 (ID_i, D_i) 增加到 L' 。

部分盲签密询问： A_I 提交 ID_s, P_s, pk_s 和 $\bar{m}$ ，执行以下过程：

(1) $ID_s \neq ID^*$ ，则 F 计算 $S_s = \frac{1}{x_s + y_s} r_i a P_1$ ，后执行签密算法返回密文 $\delta = \text{Signcrypt}(\bar{m}, c, S_s, pk_s)$ ；

(2) $ID_s = ID^*$ ，则 F 生成 $(pk_s = x_s P_2, x_s)$ 。 F 从 L_1 和 L 中获得 (i, ID_i, r_i) 和 (ID_i, x_i, P_i, v) ，然后执行以下过程：

(a) 若 $v = 1$ ， F 随机选择 $\theta_1, \theta_2, z \in Z_q^*$ ，查 L_2 获得 (P_i, y_i) 。若 (P_i, y_i) 不存在，则 F 选择 $y_i \in Z_q^*$ ，并将 (P_i, y_i) 增加到 L_2 。 F 计算 $U = \theta_1 a P_1$, $V = \theta_2 P_2$, $W = \theta_1 (P_i + y_i P_1) - z Q_i$ 。对于 H_4 询问 $(V, \alpha_i, \beta_i, x_s)$ ，选择 $u_i \in \{0, 1\}^l$ ，增加 $(V, \alpha_i, \beta_i, x_s, u)$ 到 L_4 。对于 $H_5(V_i, pk_s, T)$ ，选择 $d_i \in \{0, 1\}^l$ 增加 (V, pk_s, T, d) 到 L_5 。令 $H_3(m, c, U, P_s, pk_s, L_1, L_2) = d$ 增加 $(m, c, U, P_s, pk_s, L_1, L_2, d)$ 到 L_3 。若存在则 F 将终止，这样的概率最多为 $q_s + q_{H_4} + q_{H_5}/2^{\text{poly}(k_1)}$ 。计算 $Q = \bar{m} \oplus d$ 返回 $\delta = (Q, W)$ 给 A_I ；

(b) 若 $v = 0$ ，根据弱签密攻击^[14]的定义， F 从敌手 A_I 获得秘密值 x'_i 模拟 $v = 1$ 类似的过程。

伪造阶段： A_I 输出 $\bar{m}, ID_s, P_s, (pk_s, sk_s = x_s)$ 和 $\delta^* = (Q^*, W^*)$ ：

(1) 若 $ID_s \neq ID^*$ 则 F 失败终止， F 不能解决 CDHP 困难问题；

(2) 若 $ID_s = ID^*$ ，根据文献^[14]的分叉引理可知，当 F 是仅由公开参数组成的概率多项式时间图灵机，可分别对预言模型进行 Q 次和 R 次询问。假设在 T 时间内可以利用 A_I 产生一个有效的 h^* ，则可在 T' 时间内伪造另一个图灵机获得 $\dot{h}$ ，并再次利用 A_I 获得另一个有效密文 $\dot{\delta} = (\dot{Q}, \dot{W})$ ，其中 $\dot{h} \neq h^*$ 。则有式(1)成立

$$\left. \begin{aligned} \bar{m} &= Q^* \oplus H_5(V^*, pk_s, T^*), \\ e(W^*, P_s + y_s P_1) &= e(U' H_3(c) + h^* Q_s, P_{pb}) \\ \bar{m} &= \dot{Q} \oplus H_5(\dot{V}, pk_s, \dot{T}), \\ e(\dot{W}', P_s + y_s P_1) &= e(U' H_3(c) + \dot{h} Q_s, P_{pb}) \end{aligned} \right\} \quad (1)$$

并且

$$\left. \begin{aligned} h^* &= H_3(m, c, U, P_s, pk_s, L_1, L_2^*), \\ \dot{h} &= H_3(m, c, U, P_s, pk_s, L_1, \dot{L}_2) \end{aligned} \right\} \quad (2)$$

则有式(3)成立

$$\left. \begin{aligned} e(W^* - \dot{W}', P_s + y_s P_1) &= e(h^* Q_s - \dot{h} Q_s, P_{pb}) \\ e((x_s + y_s)(W^* - \dot{W}'), P_1) & \\ &= e((h^* - \dot{h}) ab P_1, P_1) \end{aligned} \right\} \quad (3)$$

因此获得 CDHP 问题的一个解为： $ab P_1 = [(x_s + y_s) / (h^* - \dot{h})] (W^* - \dot{W}')$ 。

以下分析 F 成功解决 CDHP 问题的优势。

F 两种失败终止情况：(1) A_I 对 ID_s^* 进行过部分私钥询问则 F 终止；(2) 若部分盲签密询问的值在 L_3 中则 F 终止。

定义 E_1 为“部分私钥询问并替换相应公钥过程失败终止”事件， E_2 为“部分盲签密询问过程失败终止”事件， E_3 为“成功伪造一个合法密文”事件， E_4 为“ E_3 发生的条件下，存在 $ID_s = ID^*$ ，由分叉引理成功得到 CDHP 困难问题的一个解”事件。如果以上事件都发生则 F 成功解决 CDHP 问题优势可定义为

$$\begin{aligned} \Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] \\ = \Pr[E_1] \Pr[E_2 | E_1] \cdot \Pr[E_3 | E_2 \wedge E_1] \end{aligned} \quad (4)$$

发生 E_1 , 若 $ID_i = ID^*$ 则终止。否则 A_I 输出有助于解决身份信息 ID_s 的概率为: $1/(q_{H_1} + q_{H_2} + q_{pr} + q_{kr} + q_{pk})$, 则 $\Pr[E_1] \geq (1 - 1/(q_{H_1} + q_{H_2} + q_{pr} + q_{kr} + q_{pk}))$ 。

对于部分盲签密询问, 若 $H_3(m, c, U, P_s, pk_s, L_1, L_2, d)$ 的值已经存在, 则F终止, 概率为: $(1 - (q_s + q_{H_4} + q_{H_5})/2^{\text{poly}(k_1)})$, 则 $\Pr[E_2|E_1] \geq (1 - (q_s + q_{H_4} + q_{H_5})/2^{\text{poly}(k_1)})$ 。又因为 $\Pr[E_3 \cdot E_2 \wedge E_1] = \varepsilon$, 则有

$$\Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] = \left(1 - \frac{1}{q_{H_1} + q_{H_2} + q_{pr} + q_{kr} + q_{pk}}\right) \cdot \left(1 - \frac{(q_s + q_{H_4} + q_{H_5})}{2^{\text{poly}(k_1)}}\right) \varepsilon \quad (5)$$

其中, $q_{H_1}, q_{H_2}, q_{H_4}, q_{H_5}, q_{pr}, q_{kr}, q_{pk}$ 和 q_s 分别表示 H_1 哈希询问、 H_2 哈希询问、 H_4 哈希询问、 H_5 哈希询问、部分私钥询问、秘密值提取询问、公钥询问、公钥替换询问和部分盲签密询问的最大次数。

证毕

引理2 随机预言模型下, 如果存在一个敌手 A_{II} 能够以 ε 的优势攻破 $CLPKC \rightarrow TPKI$ 异构环境下部分盲签密方案的 A_{II} 类安全性, 那么存在一个算法F能够以 $(1 - 1/(q_{H_1} + q_{H_2} + q_{kr} + q_{pk})) \cdot (1 - (q_s + q_{H_4} + q_{H_5})/2^{\text{poly}(k_1)}) \varepsilon$ 的优势解决MICDHP困难问题。

证明 A_{II} 是敌手, F是MICDHP问题挑战者。F给定一个MICDHP问题实例 (P_1, aP_1, b) , F的目标是使用 A_{II} 解决MICDHP问题, 即计算 $(a + b)^{-1} P_1$ 。

初始阶段: F分别在CLPKC和TPKI环境下系统建立算法, 并将参数发送给 A_{II} 。

攻击阶段: F与 A_{II} 模拟过程中, A_{II} 通过对预言机 $H_1 \sim H_4$ 进行多项式有界地适应性询问, F维护对应列表 $L_1 \sim L_4$ 。 A_{II} 还需进行公钥询问、秘密值提取询问和部分盲签密询问后才能进入伪造阶段。

在部分盲签密询问过程中 A_{II} 提交 ID_s, P_s, pk_s 和 $\bar{m}$, 执行以下过程:

(1) 若 $ID_s \neq ID$, 则F计算 ID_s 的 $S_s = [1/(x_s + y_s)] sr_i P_1$, 然后执行部分盲签密算法返回 $\delta = \text{Signcrypt}(\bar{m}, c, S_s, pk_s)$;

(2) 若 $ID_s = ID$, F查表或替换秘密值计算 $Q = \bar{m} \oplus d$ 返回 $\delta = (Q, W)$ 给 A_{II} 。

伪造过程与引理1中相似, 并获得MICDHP问

题的一个解为: $\frac{1}{a+b} P_1 = v \frac{(W'^* - \dot{W}')}{(h^* - \dot{h}) sr_s}$ 。

通过证明的F成功解决MICDHP问题, 其优势为

$$\Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] = \left(1 - \frac{1}{q_{H_1} + q_{H_2} + q_{kr} + q_{pk}}\right) \cdot \left(1 - \frac{(q_s + q_{H_4} + q_{H_5})}{2^{\text{poly}(k_1)}}\right) \varepsilon \quad (6)$$

其中, $q_{H_1}, q_{H_2}, q_{H_4}, q_{H_5}, q_{kr}, q_{pk}$ 和 q_s 分别表示 H_1 哈希询问、 H_2 哈希询问、 H_4 哈希询问、 H_5 哈希询问、秘密值提取询问、公钥询问和部分盲签密询问的最大次数。

证毕

以上为方案中的盲化消息满足不可伪造性的证明, 同理可证去盲后的消息仍然满足不可伪造性。引理2的询问部分与引理1有部分相似之处, 证明对应的游戏模型已在安全模型中给出, 请读者自行证明。限于篇幅省去引理2证明中与引理1相似部分。

3.4 机密性证明

定理2 随机预言模型下, 假设CDHP问题困难, 则CLPKC-TPKI异构环境下部分盲签密方案在适应性选择密文和身份攻击下具有不可区分性, 即适应性选择密文和身份攻击对于攻击者A安全。

引理3 随机预言模型下, 如果存在一个攻击者能够以 ε 的优势攻破CLPKC-TPKI异构环境下部分盲签密方案的机密性($IND\text{-}CLPKC \rightarrow TPKI\text{-}HSC\text{-}CCA2$), 则存在一个算法F能够以 $(\varepsilon/(q_{H_4} + q_{H_5})) (1 - (q_s + q_{H_4} + q_{H_5})/2^{\text{poly}(k_1)})$ 的优势解决CDHP困难问题。

以上为方案中的盲化消息满足机密性的证明, 同理可证去盲后的消息仍然满足机密性。引理3证明相对简单, 安全模型已在前文给出, 读者可自行证明。限于篇幅省略其证明过程。

3.5 部分盲性

定理3 在签密通信过程中, 签密人始终对所签署的内容不可见, 只能看到与消息所有者协议声明的公共消息 c , 则方案满足部分盲性。

证明 对于任意给定的一个有效盲签密 (W, U, Q) 过程中, 签密人在签密算法的过程中总是存在随机选取的唯一一对盲化因子 $\alpha, \beta \in_R Z_{q_1}^*$ 。则签密人具有且满足部分盲性总需要式(7)~式(10)成立

$$L_1 = \alpha U \quad (7)$$

$$L_2 = \beta V \quad (8)$$

$$h' = h\beta^{-1} \quad (9)$$

$$\bar{m} = (m \parallel c) \oplus H_4(V, \alpha, \beta, sk_B) \quad (10)$$

当给定一个有效的 (W, U, Q) 仅存在唯一对应的密文信息 $(L_1, L_2, h, \bar{m})$, 并同时存在一个唯一合法

密文 $\delta=(Q, W)$ 可通过验证等式，即

$$e(W', P_A + y_A P_1) = e(U' H_3(c) + h Q_A, P_{pb}) \quad (11)$$

又因为 $W' = \beta W$, $W = (r_1 H_3(c) + h') S_A$, 因此有 $e(W', P_A + y_A P_1) = e(U' H_3(c) + h Q_A, P_{pb})$ 。

由以上过程得，对于有效的 (W, U, Q) 及盲签密过程，盲因子总存在于整个签密过程中。因此密文信息 $(L_1, L_1, h, \bar{m})$ 在异构交互环境中无法直观与密文 (W, U, Q) 对应。与此同时， c 的作用是，在不改变 m 和 c 的情况下，若单方篡改 m 则影响 c 使得部分盲签密过程失败，则部分盲性成立。 证毕

4 效率分析及仿真实验结果

在已公开的文献方案中还没有CLPKC→TPKI异构环境下部分盲签密方案，因此本文将类比相似异构签密方案的计算复杂性。主要考虑指数运算(E)和对运算(P)忽略其他时间开销。本文通过理论计算和仿真实验进行效率分析。在考虑方案空间复杂性上，由于算法随问题规模扩大而不需要占用更多的内存单元，其空间复杂度为 $O(1)$ 。由表1可知，对比文献[15]的异构混合盲签密方案，在具备盲性要求的同时，计算开销明显下降。

本文的仿真实验结果是由仿真平台为Myeclipse10，程序语言为Java得出。通过对比两个方案的仿真结果并统计其中10次的运行时间，图1为本文方案10次的运行结果。

5 结论

对于已知的异构方案，鲜有运用于部分盲签密方案中。本文所提的CLPKC-TPKI异构环境下部分盲签密的形式化定义及安全模型，满足以下特点：

- (1) 满足随机预言模型下CDHP和MICDHP，

证明该方案满足机密性和不可伪造性使得敌手无法通过签密人泄露的私钥从密文中恢复明文；利用部分盲性避免签密滥用；

- (2) 本方案中生成参数由CLPKC和TPKI在各自密码体制下生成，只用到2个双线性运算来减小计算量开销；

- (3) 本方案为消息既保密又具有呈递和认证过程提供具体解决方案。

参 考 文 献

[1] HU Xiaoming, LIU Yan, XU Huajie, et al. Analysis and improvement of certificateless signature and proxy re-signature schemes[C]. 2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference, Chongqing, China, 2015: 166–170. doi: 10.1109/IAEAC.2015.7428540.

[2] 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. doi: 10.1002/sec.1300.

[3] 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. doi: 10.3724/SP.J.1146.2009.00754.

DENG Yuqiao, DU Minghui, YOU Zailai, et al. A blind proxy re-signatures scheme based on standard model[J]. *Journal of Electronics & Information Technology*, 2010, 32(5): 1219–1223. doi: 10.3724/SP.J.1146.2009.00754.

[4] 刘哲, 刘建伟, 伍前红, 等. 车载网络中安全有效分布式的假名生成[J]. *通信学报*, 2015, 36(11): 33–40. doi: 10.11959/j.issn.1000-436x.2015253.

LIU Zhe, LIU Jianwei, WU Qianhong, et al. Secure and efficient distributed pseudonym generation in VANET[J]. *Journal on Communications*, 2015, 36(11): 33–40. doi: 10.11959/j.issn.1000-436x.2015253.

[5] 李建民, 俞惠芳, 赵晨. UC安全的自认证盲签密协议[J]. *计算机科学与探索*, 2017, 11(6): 932–940. doi: 10.3778/j.issn.1673-9418.1605047.

LI Jianmin, YU Huifang, and ZHAO Chen. Self-certified blind signcrypton protocol with UC security[J]. *Journal of Frontiers of Computer Science and Technology*, 2017, 11(6): 932–940. doi: 10.3778/j.issn.1673-9418.1605047.

[6] 傅晓彤, 陈思, 张宁. 基于代理的密码货币支付系统[J]. *通信学报*, 2017, 38(7): 199–206. doi: 10.11959/j.issn.1000-436x.2017121.

FU Xiaotong, CHEN Si, and ZHANG Ning. Proxy-cryptocurrency payment system[J]. *Journal on Communications*, 2017, 38(7): 199–206. doi: 10.11959/j.issn.1000-436x.2017121.

[7] SUN Yinxia and LI Hui. Efficient signcrypton between TPKC and IDPKC and its multi-receiver construction[J].

表 1 计算复杂度

方案	签密	解签密	系统参数	盲性
文献[15]	2E+P	E+3P	不同	满足
本文	0E+0P	0E+2P	不同	满足

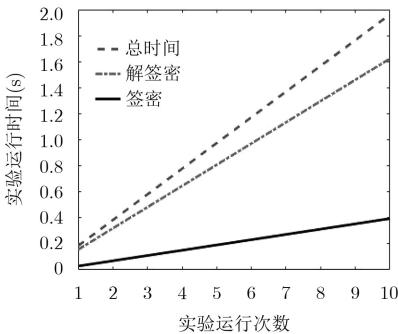


图 1 本文方案运行结果

- Science China Information Sciences*, 2010, 53(3): 557–566. doi: [10.1007/s11432-010-0061-5](#).
- [8] HUANG Qiang, WONG D S, and YANG Guomin. Heterogeneous signcryption with key privacy[J]. *The Computer Journal*, 2011, 54(4): 525–536. doi: [10.1093/comjnl/bxq095](#).
- [9] 张玉磊, 张灵刚, 张永洁, 等. 匿名CLPKC-TPKI异构签密方案[J]. 电子学报, 2016, 44(10): 2432–2439. doi: [10.3969/j.issn.0372-2112.2016.10.022](#).
- ZHANG Yulei, ZHANG Linggang, ZHANG Yongjie, *et al.* CLPKC-to-TPKI heterogeneous signcryption scheme with anonymity[J]. *Acta Electronica Sinica*, 2016, 44(10): 2432–2439. doi: [10.3969/j.issn.0372-2112.2016.10.022](#).
- [10] 冯涛, 彭伟, 马建峰. 安全的无可信PKG的部分盲签名方案[J]. 通信学报, 2010, 31(1): 128–134. doi: [10.3969/j.issn.1000-436X.2010.01.020](#).
- FENG Tao, PENG Wei, and MA Jianfeng. Provably secure partially blind signature without trusted PKG[J]. *Journal on Communications*, 2010, 31(1): 128–134. doi: [10.3969/j.issn.1000-436X.2010.01.020](#).
- [11] 杨小东, 陈春霖, 杨平, 等. 可证安全的部分盲代理重签名方案[J]. 通信学报, 2018, 39(2): 65–72. doi: [10.11959/j.issn.1000-436x.2018014](#).
- YAGN Xiaodong, CHEN Chunlin, YANG Ping, *et al.* Partially blind proxy re-signature scheme with proven security[J]. *Journal on Communications*, 2018, 39(2): 65–72. doi: [10.11959/j.issn.1000-436x.2018014](#).
- [12] BARBOSA M and FARSHIM P. Certificateless signcryption[C]. 2008 ACM Symposium on Information, Computer and Communications Security, Tokyo, Japan, 2008: 369–372. doi: [10.1145/1368310.1368364](#).
- [13] 彭巧, 田有亮. 基于多线性Diffie-Hellman问题的秘密共享方案[J]. 电子学报, 2017, 45(1): 200–205. doi: [10.3969/j.issn.0372-2112.2017.01.027](#).
- PENG Qiao and TIAN Youliang. A secret sharing scheme based on multilinear Diffie-Hellman problem[J]. *Acta Electronica Sinica*, 2017, 45(1): 200–205. doi: [10.3969/j.issn.0372-2112.2017.01.027](#).
- [14] POINTCHEVAL D and STERN J. Security arguments for digital signatures and blind signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361–396. doi: [10.1007/s001450010003](#).
- [15] 牛淑芬, 杨喜艳, 王彩芬, 等. 基于异构密码系统的混合盲签密方案[J]. 计算机工程, 2018, 44(8): 151–154, 160. doi: [10.19678/j.issn.1000-3428.0047898](#).
- NIU Shufen, YANG Xiyan, WANG Caifen, *et al.* Hybrid blind signcryption scheme based on heterogeneous cryptosystem[J]. *Computer Engineering*, 2018, 44(8): 151–154, 160. doi: [10.19678/j.issn.1000-3428.0047898](#).
- 王彩芬: 女, 1963 年生, 教授, 博士生导师, 研究方向为密码学与信息安全.
- 许钦百: 男, 1992 年生, 硕士生, 研究方向为密码学与信息安全.
- 刘 超: 男, 1989 年生, 硕士生, 研究方向为密码学与信息安全.
- 成玉丹: 女, 1992 年生, 硕士生, 研究方向为密码学与信息安全.
- 赵 冰: 男, 1994 年生, 硕士生, 研究方向为密码学与信息安全.