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 Caifen①② XU Qinbai① LIU Chao① CHENG Yudan① ZHAO Bing①
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 requirment 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$P_{\rm pb}$(KGC的公钥)和系统参数$\rm ps_1$。KGC公开$P_{\rm pb}$和$\rm ps_1$，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$\rm ps_2$。生成公钥$\rm pk_{\it i}$和私钥$\rm sk_{\it i}$, 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$\rm ID_{\it i}$, $\rm ps_1$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$\rm ps_1$，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$\rm pk_{\it i}$, P_i，消息m, c及$\rm ps_2$，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“⊥”。其中，“⊥”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$\delta=\text{Signcrypt}(m, c, S_{\rm A}, \rm pk_B)$，则$m=\text{Unsigncrypt}(\delta, c, P_{\rm A}, \rm sk_B)$成立；在盲化条件下若$\bar{\delta}=\text{Signcrypt}(\bar{m}, c, S_{\rm A}, \rm pk_B)$，则$\bar{m}=\text{Unsigncrypt}(\bar{\delta}, c, P_{\rm A}, \rm sk_B)$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$G_{\rm T1}$和乘法群$G_{\rm T2}$，生成元$P_2\in G_{\rm T1}$, l_2表示$G_{\rm T1}$元素长度，双线性映射[11] $e': G_{\rm T1}\times G_{\rm T1}\to G_{\rm T2}$。发布系统参数$\rm Ps_2=\{\it G_{\rm T1}, G_{\rm T2}, e', q_2, P_2\rm\}$。用户产生公/私钥对，公钥为$\rm pk_B=\it x_{\rm B}P_2$，私钥为$\rm sk_B=\it x_{\rm B}$，且$x_{\rm B}\in Z_{q_1}^*$。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]$e: G_1\times G_1\to G_2$。KGC定义哈希函数：$H_1:\{0,1\}^{l_{\rm id}}\to G_1$, $H_2: G_1\to Z_{q_1}^*$, $H_3:\{0,1\}^*\to Z_{q_1}^*$，$H_4:\{0,1\}^*\to\{0,1\}^{l_1}$，$H_5:\{0,1\}^*\to\{0,1\}^{l_2}$其中，$l_1$和$l_2$为函数长度。KGC选取$s\in Z_{q_1}^*$，计算$P_{\rm pb}=sP_1$，发布系统参数$\rm Ps_1=\{\it G_1, G_2, e, q_1, P_1, P_{\rm pb}, H_1, H_2, H_3, H_4\rm\}$并保存$s$；

(3) CLPKC部分私钥生成算法：用户提交$\rm ID_A$, KGC计算$Q_{\rm A}=H_1(\rm ID_A)$和$D_{\rm A}=sQ_{\rm A}$，发送$D_{\rm A}$给用户；

(4) CLPKC密钥生成算法：选取秘密值$x_{\rm A}\in_R Z_{q_1}^*$，计算公钥$P_{\rm A}=x_{\rm A}P_1$, $y_{\rm A}=H_2(P_{\rm A})$生成私钥$S_{\rm A}=\dfrac{1}{x_{\rm A}+y_{\rm A}}D_{\rm A}$；

(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$Q_{\rm A}=H_1(\rm ID_A)$, $U=r_1Q_{\rm A}$和$V=r_2P_2$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$L_1=\alpha U, L_2=\beta V, h=H_3(m, c, U, P_{\rm A}, \rm pk_B, \it L_1, L_2\rm)$和$h'=h\beta^{-1}$, $\overline{m}=(m\|c)\oplus H_4(V, \alpha, \beta, \rm sk_B)$之后将$(h', \overline{m})$送给用户A；

(c) 签密：用户A计算$T=r_2\rm pk_B$, $W=(\it r_1H_3(c)+h'\rm)S_{\rm A}$和$Q=\overline{m}\oplus H_5(V, \rm pk_B, \it T\rm)$，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$T'=\rm sk_B\it V$, $U'=\beta U$,

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

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

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

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$e(W,P_\mathrm{A}+y_\mathrm{A}P_1)=e(UH_3(c)+h'Q_\mathrm{A},P_\mathrm{pb})$。

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$\mathrm{A_I}$和$\mathrm{A_{II}}$[12]的攻击。$\mathrm{A_I}$类敌手实现公钥替换攻击；$\mathrm{A_{II}}$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$\mathrm{A_I}$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$\mathrm{ps_1}$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$\mathrm{ps_2}$和用户的公/私钥对$(\mathrm{pk}_j,\mathrm{sk}_j)$，F设置协商消息$c$后发送$\mathrm{ps_1}$, $\mathrm{ps_2}$, P_pb和$(\mathrm{pk}_j,\mathrm{sk}_j)$给$\mathrm{A_I}$。F保密系统主密钥$s$。

攻击阶段：F与$\mathrm{A_I}$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：$\mathrm{A_I}$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$\mathrm{A_I}$；

(2) 秘密值提取询问：$\mathrm{A_I}$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$\mathrm{A_I}$(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：$\mathrm{A_I}$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$\mathrm{A_I}$；

(4) 公钥替换询问：$\mathrm{A_I}$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“⊥”。

(5) 部分盲签密询问：$\mathrm{A_I}$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$\delta=\mathrm{Signcrypt}(\bar{m}_i,c,S_i,\mathrm{pk}_j)$送给$\mathrm{A_I}$。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：$\mathrm{A_I}$输出消息$(\mathrm{ID}^*,P^*,\mathrm{pk}^*,\bar{m}^*,\delta^*)$，如果以下3个条件成立，则$\mathrm{A_I}$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“⊥”；(2) $\mathrm{A_I}$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)$\mathrm{A_I}$没有执行对$(\mathrm{ID}^*,P^*,\mathrm{pk}^*,\bar{m}^*)$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$\mathrm{A_I}$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$\mathrm{A_I}$攻击是$(\varepsilon,t,q_\mathrm{pr},q_\mathrm{kr},q_\mathrm{pk},q_\mathrm{rp},q_\mathrm{s})$-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$\mathrm{A_{II}}$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$\mathrm{ps_1}$、系统公钥P_pb、系统主密钥s和$\mathrm{ps_2}$及用户公钥/私钥对$(\mathrm{pk}_j,\mathrm{sk}_j)$, F设置协商消息$c$后发送$\mathrm{ps_1}$, $\mathrm{ps_2}$, P_pb, s和$(\mathrm{pk}_j,\mathrm{sk}_j)$给$\mathrm{A_{II}}$。

攻击阶段：F与$\mathrm{A_{II}}$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：$\mathrm{A_{II}}$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：$\mathrm{A_{II}}$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$\mathrm{A_{II}}$；

(3) 部分盲签密询问：$\mathrm{A_{II}}$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$\text{A}_{\text{II}}$。

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

定义2 (EUF-CLPKC→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→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$(\varepsilon, t, q_{\text{kr}}, q_{\text{pk}}, q_s)$-EUF-CLPKC→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→TPKI-HSC-CMA安全的。

3.2 机密性CLPKC→TPKI

CLPKC→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→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$\text{ps}_1$, 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：$\text{Adv}(\text{A})=|\Pr[b'=b]-1/2|$，$\Pr[b'=b]$表示$b'=b$的概率。

注意：在游戏3中，敌手被允许获得CLPKC系统主秘钥和用户秘密值，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→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$(\varepsilon, t, q_{\text{k}}, q_{\text{s}}, q_{\text{u}})$-IND-CLPKC→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
$$\left(1-\frac{1}{q_{H_1}+q_{H_2}+q_{\text{pr}}+q_{\text{kr}}+q_{\text{pk}}}\right)\left(1-\frac{(q_s+q_{H_4}+q_{H_5})}{2^{\text{poly}(k_1)}}\right)\varepsilon$$
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$P_{\text{pb}}=aP_1$(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$L_1\sim L_5$, $L=(\text{ID}_i, x_i, P_i, v)$和$L'=(\text{ID}_i, D_i)$，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$L_1=(i, \text{ID}_i, *)$。A_{I}对于第i次非重复$H_1(\text{ID}_i)$询问，(1)若$\text{ID}_i=\text{ID}^*$，则F返回$D_i=bP_1$，并将$(i, \text{ID}_i, \perp)$增加到L_1。“$\perp$”表示不能确定bP_1的系数；(2)若$\text{ID}_i\neq\text{ID}^*$，则F从$Z_{q_1}^*$随机选取$r_i$，并将$(i, \text{ID}_i, r_i)$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$Z_{q_1}^*$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：$\mathrm{A_I}$ 询问H_3，F保持$L_3=(m, c, U_i, P_i, \mathrm{pk}_j, L_{1i}, L_{2i}, z_i)$。若已存在则返回结果$z_i$；否则F从$Z_{q_1}^*$随机选取$z_i$返回给$\mathrm{A_I}$，并且将$(m, c, U_i, P_i, \mathrm{pk}_j, L_{1i}, L_{2i}, z_i)$增加到$L_3$。

H_4询问：$\mathrm{A_I}$ 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$u_i\in\{0,1\}^{l_1}$返回给$\mathrm{A_I}$，并且将$(V_i, \alpha_i, \beta_i, x_j, u_i)$增加到$L_4$。

H_5询问：$\mathrm{A_I}$ 询问H_5，F保持$L_5=H_5(V_i, \mathrm{pk}_j, T_i, d_i)$。若存在则返回结果$d_i$；否则随机选择$d_i\in\{0,1\}^{l_2}$提交给$\mathrm{A_I}$，并将$(V_i, \mathrm{pk}_j, T_i, d_i)$增加到$L_5$。

公钥询问：F保持$L=(\mathrm{ID}_i, x_i, P_i, v)$，$\mathrm{A_I}$输入$\mathrm{ID}_i$若存在则直接返回$P_i$；否则F从$Z_{q_1}^*$随机选取$x_i$，计算$P_i=x_iP_1$返回给$\mathrm{A_I}$并将$(\mathrm{ID}_i, x_i, P_i, 1)$增加到$L$。

秘密值提取询问：F保持$L=(\mathrm{ID}_i, x_i, P_i, v)$，$\mathrm{A_I}$输入$\mathrm{ID}_i$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：$\mathrm{A_I}$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$L'=(\mathrm{ID}_i, D_i)$，$\mathrm{A_I}$输入ID_i，(1)若$\mathrm{ID}_i=\mathrm{ID}^*$则$F$失败并终止；(2)若$\mathrm{ID}_i\neq\mathrm{ID}^*$且$L'$中存在则返回；否则F检查$L_1$获得$r_i$值，计算$D_i=r_iaP_1$返回$\mathrm{ID}_i$将$(\mathrm{ID}_i, D_i)$增加到$L'$。

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

(1) $\mathrm{ID}_s\neq\mathrm{ID}^*$，则F计算$S_s=\dfrac{1}{x_s+y_s}r_iaP_1$，后执行签密算法返回密文$\delta=\mathrm{Signcrypt}(\bar{m}, c, S_s, \mathrm{pk}_s)$；

(2) $\mathrm{ID}_s=\mathrm{ID}^*$，则F生成$(\mathrm{pk}_s=x_sP_2, x_s)$。F从$L_1$和$L$中获得$(i, \mathrm{ID}_i, r_i)$和$(\mathrm{ID}_i, x_i, P_i, v)$，然后执行以下过程：

(a) 若$v=1$，F随机选择θ_1，θ_2，$z\in Z_{q_1}^*$，查L_2获得(P_i, y_i)。若(P_i, y_i)不存在，则F选择$y_i\in Z_{q_1}^*$，并将(P_i, y_i)增加到L_2。F计算$U=\theta_1aP_1$，$V=\theta_2P_2$，$W=\theta_1(P_i+y_iP_1)-zQ_i$。对于$H_4$询问$(V, \alpha, \beta, x_s)$，选择$u_i\in\{0,1\}^{l_1}$，增加$(V, \alpha_i, \beta_i, x_s, u)$到$L_4$。对于$H_5(V, \mathrm{pk}_s, T)$，选择$d_i\in\{0,1\}^{l_2}$增加$(V, \mathrm{pk}_s, T, d)$到$L_5$。令$H_3(m, c, U, P_s, \mathrm{pk}_s, L_1, L_2)=d$增加$(m, c, U, P_s, \mathrm{pk}_s, L_1, L_2, d)$到$L_3$。若存在则F将终止，这样的概率最多为$q_s+q_{H_4}+q_{H_5}/2^{\mathrm{poly}(k_1)}$。计算$Q=\overline{m}\oplus d$返回$\delta=(Q, W)$给$\mathrm{A_I}$；

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

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

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

(2) 若$\mathrm{ID}_s=\mathrm{ID}^*$，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$\mathrm{A_I}$产生一个有效的h^*，则可在T'时间内伪造另个图灵机获得$\dot{h}$，并再次利用$\mathrm{A_I}$获得另一个有效密文$\dot{\delta}=\left(\dot{Q}, \dot{W}\right)$，其中$\dot{h}\neq h^*$。则有式(1)成立

$$\left.\begin{aligned}&\bar{m}=Q^*\oplus H_5(V^*, \mathrm{pk}_s, T^*),\\&\quad e\left(W^{\prime *}, P_s+y_sP_1\right)=e\left(U'H_3(c)+h^*Q_s, P_{\mathrm{pb}}\right)\\&\bar{m}=\dot{Q}\oplus H_5\left(\dot{V}, \mathrm{pk}_s, \dot{T}\right),\\&\quad e\left(\dot{W}', P_s+y_sP_1\right)=e\left(U'H_3(c)+\dot{h}Q_s, P_{\mathrm{pb}}\right)\end{aligned}\right\}\tag{1}$$

并且

$$\begin{aligned}h^*&=H_3(m, c, U, P_s, \mathrm{pk}_s, L_1, L^*{}_2),\\\dot{h}&=H_3\left(m, c, U, P_s, \mathrm{pk}_s, L_1, \dot{L}_2\right)\end{aligned}\tag{2}$$

则有式(3)成立

$$\left.\begin{aligned}&e\left(W^{\prime *}-\dot{W}', P_s+y_sP_1\right)=e\left(h^*Q_s-\dot{h}Q_s, P_{\mathrm{pb}}\right)\\&e\left((x_s+y_s)\left(W^{\prime *}-\dot{W}'\right), P_1\right)\\&\quad=e\left(\left(h^*-\dot{h}\right)abP_1, P_1\right)\end{aligned}\right\}\tag{3}$$

因此获得CDHP问题的一个解为：$abP_1=\left[(x_s+y_s)\Big/\left(h^*-\dot{h}\right)\right]\left(W^{\prime *}-\dot{W}'\right)$。

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)$\mathrm{A_I}$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$\mathrm{ID}_s=\mathrm{ID}^*$，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

$$\begin{aligned}&\Pr[\mathrm{E}_1\wedge\mathrm{E}_2\wedge\mathrm{E}_3\wedge\mathrm{E}_4]\\&\quad=\Pr[\mathrm{E}_1]\Pr[\mathrm{E}_2|\,\mathrm{E}_1]\cdot\Pr[\mathrm{E}_3|\,\mathrm{E}_2\wedge\mathrm{E}_1]\end{aligned}\tag{4}$$

发生E_1，若$\mathrm{ID}_i=\mathrm{ID}^*$则终止。否则$\mathrm{A_I}$输出有助于解决身份信息$\mathrm{ID}_s$的概率为：$1/(q_{H_1}+q_{H_2}+q_{\mathrm{pr}}+q_{\mathrm{kr}}+q_{\mathrm{pk}})$，则$\Pr[\mathrm{E}_1]\geq(1-1/(q_{H_1}+q_{H_2}+q_{\mathrm{pr}}+q_{\mathrm{kr}}+q_{\mathrm{pk}}))$。

对于部分盲签密询问，若$H_3(m,c,U,P_s,\mathrm{pk}_s,L_1,L_2,d)$的值已经存在，则F终止，概率为：$\left(1-(q_s+q_{H_4}+q_{H_5})/2^{\mathrm{poly}(k_1)}\right)$，则$\Pr[\mathrm{E}_2|\,\mathrm{E}_1]\geq\left(1-(q_s+q_{H_4}+q_{H_5})/2^{\mathrm{poly}(k_1)}\right)$。又因为$\Pr[\mathrm{E}_3|\cdot\mathrm{E}_2\wedge\mathrm{E}_1]=\varepsilon$，则有

$$\begin{aligned}&\Pr[\mathrm{E}_1\wedge\mathrm{E}_2\wedge\mathrm{E}_3\wedge\mathrm{E}_4]\\&=\left(1-\frac{1}{q_{H_1}+q_{H_2}+q_{\mathrm{pr}}+q_{\mathrm{kr}}+q_{\mathrm{pk}}}\right)\\&\quad\cdot\left(1-\frac{(q_s+q_{H_4}+q_{H_5})}{2^{\mathrm{poly}(k_1)}}\right)\varepsilon\end{aligned}\tag{5}$$

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$\mathrm{A_{II}}$能够以ε的优势攻破CLPKC→TPKI异构环境下部分盲签密方案的$\mathrm{A_{II}}$类安全性，那么存在一个算法F能够以$(1-1/(q_{H_1}+q_{H_2}+q_{\mathrm{kr}}+q_{\mathrm{pk}}))\cdot\left(1-(q_s+q_{H_4}+q_{H_5})/2^{\mathrm{poly}(k_1)}\right)\varepsilon$的优势解决MICDHP困难问题。

证明 $\mathrm{A_{II}}$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$\mathrm{A_{II}}$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$\mathrm{A_{II}}$。

攻击阶段：F与$\mathrm{A_{II}}$模拟过程中，$\mathrm{A_{II}}$通过对预言机$H_1\sim H_4$进行多项式有界次地适应性询问，F维护对应列表$L_1\sim L_4$。$\mathrm{A_{II}}$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$\mathrm{A_{II}}$提交ID_s，P_s，pk_s和$\bar{m}$，执行以下过程：

（1）若$\mathrm{ID}_s\neq\mathrm{ID}$，则F计算$\mathrm{ID}_s$的$S_s=[1/(x_s+y_s)]\,sr_iP_1$，然后执行部分盲签密算法返回$\delta=\mathrm{Signcrypt}(\bar{m},c,S_s,\mathrm{pk}_s)$；

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

伪造过程与引理1中相似，并获得MICDHP问题的一个解为：$\dfrac{1}{a+b}P_1=v\dfrac{\left(W'^{*}-\dot{W}'\right)}{\left(h^*-\dot{h}\right)sr_s}$。

通过证明的F成功解决MICDHP问题，其优势为

$$\begin{aligned}&\Pr[\mathrm{E}_1\wedge\mathrm{E}_2\wedge\mathrm{E}_3\wedge\mathrm{E}_4]\\&=\left(1-\frac{1}{q_{H_1}+q_{H_2}+q_{\mathrm{kr}}+q_{\mathrm{pk}}}\right)\\&\quad\cdot\left(1-\frac{(q_s+q_{H_4}+q_{H_5})}{2^{\mathrm{poly}(k_1)}}\right)\varepsilon\end{aligned}\tag{6}$$

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-CLPKC→TPKI-HSC-CCA2)，则存在一个算法F能够以$\left(\varepsilon/\left(q_{H_4}+q_{H_5}\right)\right)\left(1-(q_s+q_{H_4}+q_{H_5})/2^{\mathrm{poly}(k_1)}\right)$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，只能看到与消息拥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

$$L_1=\alpha U\tag{7}$$

$$L_2=\beta V\tag{8}$$

$$h'=h\beta^{-1}\tag{9}$$

$$\overline{m}=(m\|\,c)\oplus H_4(V,\alpha,\beta,sk_{\mathrm{B}})\tag{10}$$

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

密文$\delta=(Q, W)$可通过验证等式，即

$$e(W', P_{\mathrm{A}}+y_{\mathrm{A}}P_1)=e(U'H_3(c)+hQ_{\mathrm{A}}, P_{\mathrm{pb}}) \quad (11)$$

又因为$W'=\beta W$，$W=(r_1H_3(c)+h')S_{\mathrm{A}}$，因此有$e(W', P_{\mathrm{A}}+y_{\mathrm{A}}P_1)=e(U'H_3(c)+hQ_{\mathrm{A}}, P_{\mathrm{pb}})$。

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。

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

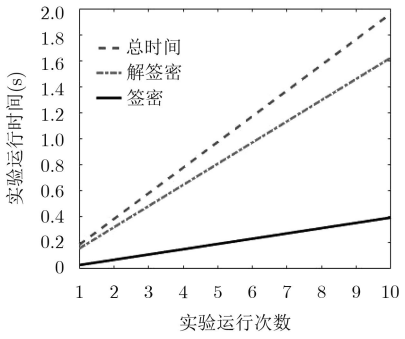

图 1 本文方案运行结果

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 signcryption 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 signcryption between TPKC and IDPKC and its multi-receiver construction[J].

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.