一种异构混合群组签密方案的安全性分析与改进

张玉磊[①] 刘祥震*[①] 郎晓丽[①] 张永洁[②] 王彩芬[①]

[①](西北师范大学计算机科学与工程学院 兰州 730070)

[②](甘肃卫生职业学院 兰州 730070)

摘 要：异构混合群组签密不仅能够解决不同密码体制下数据传输的机密性和不可伪造性，而且还能对任意长度的数据进行加密。该文首先分析了一种异构密码体制下混合群组签密方案的安全性，指出该方案不满足正确性、机密性和不可伪造性。并提出了一种新的高效异构混合群组签密方案。其次在随机预言机模型下证明了该方案是安全的。最后效率分析表明，该方案在实现原方案所有的功能的基础上同时降低了计算代价。

关键词：混合签密；异构；安全性分析；效率分析

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)11-2708-07

DOI: 10.11999/JEIT190129

Security Analysis and Improvements of Hybrid Group Signcryption Scheme Based on Heterogeneous Cryptosystem

ZHANG Yulei[①] LIU Xiangzhen[①] LANG Xiaoli[①]

ZHANG Yongjie[②] WANG Caifen[①]

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

[②](*Gansu Health Vocational College*, *Lanzhou* 730070, *China*)

Abstract: Heterogeneous hybrid group signcryption can not only solve the confidentiality and unforgeability of data transmission under different cryptosystems, but also encrypt data of any length. Firstly, the security of a hybrid group signcryption scheme under heterogeneous cryptosystem is analyzed, and it is pointed out that the scheme does not satisfy the correctness, confidentiality and unforgeability. And a new efficient heterogeneous hybrid group signcryption scheme is proposed. Secondly, it is proved that the proposed scheme is safe under the random oracle model. Finally, the efficiency analysis shows that the proposed scheme reduces the computational cost while realizing all the functions of the original scheme.

Key words: Hybrid signcryption; Heterogeneous; Security analysis; Efficiency analysis

1 引言

随着人们对数据安全要求的提高，在传输过程不仅要保证消息的机密性同时还要保证消息的不可伪造性。Zheng[1]在1997年提出了区别于传统先签名后加密的签密方案，把签名的不可伪造性与加密的机密性很好地结合起来，并且计算量小于两者总和。

公钥签密机制要求传输的数据不宜过长，这就导致该机制无法加密长消息。为了解决这个问题，文献[2]在混合加密基础上利用签密密钥封装(Key Encapsulation Mechanism, KEM)和数据封装技术(Data Encapsulation Mechanism, DEM)提出了混合签密方案[3,4]，与传统的公钥签密机制相比，混合签密灵活性较高，也更安全，因此引起了研究者们的关注[5,6]。2009年，Li等人[7]提出了无证书(CertificateLess Cryptography, CLC)混合签密方案，将混合签密技术应用到无证书密码环境下。同年，Selvi等人[8]指出文献[7]方案不满足密文的不可伪造性并对该方案进行改进。周彦伟等人[9]提出了基于身份的匿名混合签密机制，将混合签密机制运用到身份密码环境。

在实际的应用环境中，跨平台通信越来越普及，不同系统或平台使用不同的密码体制。为了保证异构密码环境下数据的机密性和不可伪造性，Sun等人[10]首次提出了异构签密方案。该方案的发送

收稿日期：2019-03-05；改回日期：2019-06-29；网络出版：2019-07-19

*通信作者： 刘祥震 woliuxiangzhen@foxmail.com

基金项目：国家自然科学基金(61163038, 61262056,61262057)，甘肃省高等学校科研项目(2017A-003, 2018A-207)

Foundation Items: The National Natural Science Foundation of China (61163038, 61262056, 61262057), The Higher Educational Scientific Research Foundation of Gansu Province (2017A-003, 2018A-207)

方来自传统公钥密码环境(Public Key Infrastructure, PKI)，接收方来自身份密码环境(Identity-Based Cryptograph, IBC)。刘景伟等人[11]提出了异构PKI → CLC签密方案，随后张玉磊等人[12]指出该方案不满足机密性。2017年，Niu等人[13]提出了具有双重隐私保护的异构签密方案，随后张玉磊等人[14]指出该方案不能抵挡恶意密钥生成中心(Key Generation Center, KGC)攻击。2017年，Niu等人[15]首次将混合签密运用到异构密码体制下。

2019年，牛淑芬等人[16]提出了基于异构密码系统的混合群组签密方案(简称牛方案)，并证明了该方案的安全性。分析牛方案，发现该方案不满足正确性、机密性与不可伪造性。恶意KGC获取签密密文后，可以解密出消息，不满足机密性；任意敌手A可以选择任意消息实现伪造攻击，不满足不可伪造性。首先，本文通过2类具体的攻击对牛方案进行了安全性分析与正确性分析。其次，为了解决牛方案中存在的安全缺陷，提出了一个改进的异构密码系统的混合群组签密方案。最后，在随机预言模型下，证明了所提方案不仅能满足异构密码体制下签密内部安全模型的机密性与不可伪造性，并减少了计算效率开销。

2　牛方案回顾及安全性分析

限于篇幅，略去对牛方案的描述，具体算法见文献[16]。本节将利用具体的攻击来展示牛方案不满足机密性、不可伪造性和正确性。

2.1　机密性

对于牛方案中的机密性，主要考虑无证书密码体制中的敌手$\mathrm{A_{II}}$，恶意KGC知道系统主密钥s_2，可以计算出$D_{B_i}=s_2{}^{-1}H_1(\mathrm{ID}_{B_i})$，具体攻击过程如下：

(1) 捕获签密密文：恶意KGC通过截获或窃听等方式获得发送者对消息m的签密密文$\sigma=(c,\phi\leftarrow(U_1,U_2,U_3,V))$。

(2) 解密密文：KGC首先计算$P_1V=P^2H_1(\mathrm{ID_A})H_1(G_{\mathrm{ID}})(U_1+PH)$，由于$P_1$，$P$，$H_1(\mathrm{ID_A})$，$H_1(G_{\mathrm{ID}})$为系统公开参数，$V$，$U_1$为发送者正确的签密密文。其次计算$T=U_1\sum_{i=1}^{n}D_{B_i}$，$K=H_2\left(U_1,U_2,U_3,T,U_1\sum_{i=1}^{n}x_{B_i},\sum_{i=1}^{n}\mathrm{ID}_{B_i},G_{\mathrm{ID}}\right)=H_2\left(U_1,U_2,U_3,T,U_1\sum_{i=1}^{n}P_{B_i},\sum_{i=1}^{n}\mathrm{ID}_{B_i},G_{\mathrm{ID}}\right)$。最后，恢复消息$m=\mathrm{DEM.DEC}(K,c)$。

当恶意KGC获取签密密文后，可根据等式$T=U_1\sum_{i=1}^{n}D_{B_i}$很容易计算出解密密钥$K$，因而牛方案针对自适应选择密文攻击下的不可区分性攻击成功。

2.2　不可伪造性

对于牛方案中的不可伪造性，主要考虑基于身份密码体制下的任意敌手A。具体攻击过程如下：

(1) 系统参数设置：生成系统参数$\{G_1,G_2,q,P,e,n,H_1,H_2,H_3,E,D\}$并发送给敌手A。

(2) 询问：A从签密询问中获取发送者对消息m_j的签密，记为$\sigma_j=(c_j,\phi_j\leftarrow(U_1,U_2,U_3,V))$。

(3) 计算：由于$V_j=V_1V_2=r_{\mathrm{A}}{}^{-1}\cdot S\cdot h_{\mathrm{A}}=r_{\mathrm{A}}{}^{-1}\cdot P(t+H)\cdot s_1\cdot R\cdot P\cdot H_1(G_{\mathrm{ID}})=P(t+H)\cdot s_1\cdot H_1(\mathrm{ID_A})P\cdot H_1(G_{\mathrm{ID}})$，所以可以得到$X=s_1P=(P(t+H)\cdot H_1(\mathrm{ID_A})\cdot H_1(G_{\mathrm{ID}}))/V_j$。

(4) 伪造：A随机选择$t_1\in Z_q^*$和消息m_1，然后计算$U_1'=t_1P$，$U_2'=t_1H_1(\mathrm{ID_A})$，$U_3'=t_1$，$T'=U_3'H_1(G_{\mathrm{ID}})\sum_{i=1}^{n}H_1(\mathrm{ID})$，$K'=H_1(U_1',U_2',U_3',T,t_1\sum_{i=1}^{n}P_{B_i},\sum_{i=1}^{n}\mathrm{ID}_{B_i},G_{\mathrm{ID}})$，$c'=\mathrm{DEM.Enc}(K,m_1)$，$H'=H_3\left(c',U_1',U_2',U_3',\mathrm{ID_A},\sum_{i=1}^{n}\mathrm{ID}_{B_i},G_{\mathrm{ID}}\right)$，$V'=P(t_1+H')s_1P\cdot H_1(\mathrm{ID_A})\cdot H_1(G_{\mathrm{ID}})$。最后，A输出对消息$m_1$的签密密文$\sigma_1=(c',\phi\leftarrow(U_1',U_2'U_3',V'))$。

(5) 验证伪造密文：根据验证等式$P_1V'=P^2H_1(\mathrm{ID_A})H_1(G_{\mathrm{ID}})(U_1'+PH)$可知：$P_1V'=s_1{}^{-1}P\cdot P(t_1+H')s_1\cdot H_1(\mathrm{ID_A})P\cdot H_1(G_{\mathrm{ID}})=P^2t_1\cdot H_1(\mathrm{ID_A})P\cdot H_1(G_{\mathrm{ID}})+P^2H'\cdot H_1(\mathrm{ID_A})P\cdot H_1(G_{\mathrm{ID}})=P^2H_1(\mathrm{ID_A})\cdot H_1(G_{\mathrm{ID}})(U_1'+PH')$。

伪造的签密通过验证等式，敌手A针对适应性选择消息攻击系的不可区分性攻击成功。

2.3　正确性

牛方案中的哈希函数构造为：$H_1:\{0,1\}^*\to G_1$，$H_2:G_2\to\{0,1\}^n\times\{0,1\}^n$，$H_3:\{0,1\}^*\times G_2\to Z_q^*$，因此，$R=r_{\mathrm{A}}H_1(\mathrm{ID_A})\in G_1$，$S=P(t+H\in Z_q^*)\in G_1$，所以，PKG无法计算出$h_{\mathrm{A}}=s_1RPH_1(G_{\mathrm{ID}})$。同时发送方也就无法计算出$V_2=Sh_{\mathrm{A}}$；对于接收方来说，无法验证$P_1V=P^2H_1(\mathrm{ID_A})H_1(G_{\mathrm{ID}})(U_1+PH)$。由于$D_{B_i}=s_2{}^{-1}H_1(\mathrm{ID}_{B_i})\in G_1$，所以，接收方也就无法计算出$T=U_1\sum_{i=1}^{n}D_{B_i}$。由于原作者笔误，牛方案无法对消息进行签密同时也无法进行解密得到正确的消息。

3　改进的异构混合群组签密方案

基于牛方案存在的问题，本文提出了一种改进的异构混合群组签密方案。对机密性而言，在本文所提解签密算法中，CLC系统下的接收群组成员需要用到自己的秘密值x_{B_i}来计算解签密密钥K。即，用户解密时，不仅要使用KGC生成的部分私钥，而且需要使用只有用户自己才知道的秘密值x_{B_i}。因此，恶意KGC无法计算出解密密钥。

具体方案构造如下：

(1) 系统建立：选择循环加群G_1和循环乘群G_2，其阶同为q, P为G_1的生成元。选择$e: G_1\times G_1 \to G_2$，定义5个Hash函数：$H_0: \{0,1\}^* \to Z_q^*$，$H_1: \{0,1\}^* \to G_1, H_2: \{0,1\}^* \times \{0,1\}^* \to Z_q^*$，$H_3: G_1 \times G_2 \times \{0,1\}^* \to \{0,1\}^n, H_4: \{0,1\}^n \to Z_q^*$，$n$为消息的长度。选择对称加密体制中的加密与解密算法$(E, D)$。PKG和KGC分别选择$s_1 \in Z_q^*$和$s_2 \in Z_q^*$作为各自系统的主密钥，分别计算各自系统主公钥$P_1 = s_1P$和$P_2 = s_2P$。公开系统参数Paras = $\{G_1, G_2, e, P, q, H_0, H_1, H_2, H_3, H_4, P_1, P_2, n\}$。

(2) IBC密钥提取：PKG利用其系统主密钥s_1为IBC系统中$\mathrm{ID_A}$的发送者，计算$S_A = s_1Q_\mathrm{A}$作为$\mathrm{ID_A}$的私钥，其中，$Q_\mathrm{A} = H_1(\mathrm{ID_A})$。

(3) CLC密钥提取。

(a) 部分私钥生成：KGC使用系统主密钥s_2为CLC系统中身份为ID_{B_i}的接收方，计算$D_{B_i} = s_2Q_{B_i}$为ID_{B_i}的部分私钥。其中，$Q_{B_i} = H_0(\mathrm{ID}_{B_i})$。

(b) 秘密值设置：用户ID_{B_i}选取任意的$x_{B_i} \in Z_q^*$作为其秘密值。

(c) 公钥设置：用户ID_{B_i}计算其公钥为$P_{B_i} = x_{B_i}P$。

(d) 私钥设置：用户ID_{B_i}设置其私钥$S_{B_i} = (x_{B_i}, D_{B_i})$。

(4) 签密：IBC系统下的发送方通过混合签密方式将消息m发送给CLC系统下的群组用户，混合签密过程如下：

(a) 发送者$\mathrm{ID_A}$随机选择$r \in \{0,1\}^*$，计算$t = H_2(r, m)$。

(b) 计算$U = tP$，$V = P_2Q_{B_i}$和$f = e(Q_\mathrm{A}, P_{B_i})^t$。

(c) 计算$K = H_3\left(U, f, V, t\sum_{i=1}^{n} P_{B_i}, G_\mathrm{ID}, \sum_{i=1}^{n} \mathrm{ID}_{B_i}\right)$。

(d) 对消息加密$c = \mathrm{DEM.Enc}(K, m)$。

(e) 计算$S = tQ_\mathrm{A} + H_4(m)S_\mathrm{A}$。

(f) 输出密文$\sigma = (c, U, S)$

(5) 解签密：当CLC系统下的接收群组成员G_ID收到$\sigma = (c, U, S)$时，计算如下：

(a) 首先计算$V = D_{B_i}P$, $f = e(Q_\mathrm{A}, x_{B_i}U)$和$K = H_3\left(U, f, V, U\sum_{i=1}^{n} x_{B_i}, G_\mathrm{ID}, \sum_{i=1}^{n} \mathrm{ID}_{B_i}\right)$。

(b) 恢复消息$m = \mathrm{DEM.Dec}(K, c)$。

(c) 验证$e(S, P) = e(U + H_4(m)P_1, Q_\mathrm{A})$是否相等。若成立，则返回消息$m$；否则返回错误符号“$\perp$”。

正确性证明

(1) 解密密钥K中的f与V的正确性分析：

(a) $f = e(Q_\mathrm{A}, P_{B_i})^t = e(Q_\mathrm{A}, x_{B_i}tP) = e(Q_\mathrm{A}, x_{B_i}U)$。

(b) $V = P_2Q_{B_i} = s_2PQ_{B_i} = D_{B_i}P$。

(2) 密文验证的正确性分析：$e(S, P) = e(tQ_\mathrm{A} + H_4(m)S_\mathrm{A}, P) = e(tQ_\mathrm{A}, P)e(H_4(m)S_\mathrm{A}, P) = e(tP, Q_\mathrm{A})e(H_4(m)P_1, Q_\mathrm{A}) = e(U + H_4(m)P_1, Q_\mathrm{A})$。

4 安全性分析

4.1 机密性

定理1 随机预言模型下的敌手$\mathrm{A_I}$能以不可忽略的概率赢得改进的异构混合群组签密方案的游戏，则存在一个挑战者C就能以不可忽略的概率解决BDH问题。

证明 C给定BDH问题的实例(P, aP, bP, cP)，目标是计算$e(P, P)^{abc}$。

系统初始化：生成系统公开参数$\{G_1, G_2, e, P, q, H_0, H_1, H_2, H_3, H_4, P_1, P_2, n\}$，其中，$P_1 = \lambda P$, $P_2 = yP$。同时，C选择选择ID^*为被挑战者身份。

阶段1 $\mathrm{A_I}$适应性的进行以下询问。

H_0询问：C维护初始为空的表L_1来应对$\mathrm{A_I}$询问CLC系统下身份为ID_i的H_0的结果，若询问的(ID_i, Q_i)存在表中，则直接返回Q_i；否则，C随机选择$\gamma_i \in Z_q^*$给A_I，同时将$(\mathrm{ID}_i, Q_i, \gamma_i)$添加到表$L_1$。

H_1询问：C维护初始为空的表L_1来应对$\mathrm{A_I}$询问身份为ID_i的H_1的结果，若询问的(ID_i, Q_i)存在表中，则直接返回Q_i；若$\mathrm{ID}_i = \mathrm{ID}^*$，C设置$Q_i = aP$给$\mathrm{A_I}$；否则，C随机选择$\chi_i \in G_1$给$\mathrm{A_I}$，同时将$(\mathrm{ID}_i, Q_i, \chi_i)$添加到表$L_1$。

H_2询问：C维护初始为空的表L_2来应对$\mathrm{A_I}$对H_2的询问结果，若$\mathrm{A_I}$询问的H_2存在表L_2中，则C直接返回相应的结果；否则，C随机选择$t \in Z_q^*$给$\mathrm{A_I}$，并将(H_2, t)保存到表L_2中。

H_3询问：C维护初始为空的表L_3来应对$\mathrm{A_I}$对H_3询问的结果，若$\mathrm{A_I}$询问的H_3存于表L_3中，C直接将结果返回给$\mathrm{A_I}$；否则，C随机选择$\kappa \in \{0,1\}^n$给$\mathrm{A_I}$，并将(H_3, κ)保存到表L_3中。

H_4询问：C维护初始为空的表L_4，当C收到$\mathrm{A_I}$对H_4的询问时，若表中存在相应的结果，C直接返回结果；否则，C随机选择$h_4 \in Z_q^*$给$\mathrm{A_I}$作为询问的结果，并将(H_4, h_4)存于表L_4中。

CLC公钥询问：C维护初始为空的表L_P，若$\mathrm{A_I}$询问ID_{B_i}的公钥时，若$\mathrm{ID}_{B_i} = \mathrm{ID}^*$,C设置$P_{B_i} = bP$,并将$P_{B_i}$给$\mathrm{A_I}$；否则，C随机选择$x_i \in Z_q^*$，计算$P_{B_i} = x_iP$给$\mathrm{A_I}$，并将$(\mathrm{ID}_{B_i}, P_{B_i}, x_i)$保存到表$L_P$中。

CLC部分私钥询问：若$\mathrm{A_I}$询问ID_{B_i}的部分私钥时，若$\mathrm{ID}_{B_i}=\mathrm{ID}^*$, C停止；否则，C检索表$L_1$，获取元组$(\mathrm{ID}_i, Q_i, \chi_i)$，计算$D_{B_i}=y\gamma_i$给$\mathrm{A_I}$。

CLC公钥替换询问：当$\mathrm{A_I}$对ID_{B_i}公钥替换询问时，若$\mathrm{ID}_{B_i}=\mathrm{ID}^*$，则C停止；否则，$\mathrm{A_I}$用新公钥$P_{B_i}'$替换原公钥$P_{B_i}$，并更新表$L_P$中的元组$(\mathrm{ID}_{B_i}, P_{B_i}', \perp)$。

IBC私钥询问：当$\mathrm{A_I}$询问身份为$\mathrm{ID_A}$的私钥时，若$\mathrm{ID_A}=\mathrm{ID}^*$, C停止；否则，计算$S_{\mathrm{A}}=\lambda\chi_i$给$\mathrm{A_I}$，并将$(\mathrm{ID_A}, S_{\mathrm{A}})$保存到表$L_S$中。

解签密询问：若对$(\mathrm{ID_A}, \mathrm{ID}_{B_i})$下的消息解签密询问时，若$\mathrm{ID_A}$或$\mathrm{ID}_{B_i}$等于$\mathrm{ID}^*$, C停止；否则，C首先计算$V=y\gamma_i P$，$f=e(\chi_A, x_{B_i}U)$与$K=H_3\left(U, f, V, U\sum_{i=1}^{n}x_{B_i}, G_{\mathrm{ID}}, \sum_{i=1}^{n}\mathrm{ID}_{B_i}\right)$；恢复消息$m=\mathrm{DEM.Dec}(K, c)$；检查等式$e(S, P)=e(U+P_1H_4(m), Q_{\mathrm{A}})$是否成立。若成立，则接收消息$m$；否则，输出“$\perp$”。

挑战　阶段1结束后，$\mathrm{A_I}$选择两个消息m_0, m_1和挑战身份$\mathrm{ID_A}^*$, $\mathrm{ID}_{B_i}{}^*$。在阶段1中不能对$\mathrm{ID}_{B_i}{}^*$执行秘密值询问。若$\mathrm{ID}_{B_i}{}^*\neq\mathrm{ID}^*$，C结束；否则，C计算挑战密文，计算过程如下：

C首先检索表L_1，得到元组(H_2, t)，设置$U^*=cP$，计算$K_b=H_3\left(U^*, f^*, V^*, t\sum_{i=1}^{n}bP, G_{\mathrm{ID}}, \sum_{i=1}^{n}\mathrm{ID}_{B_i}\right)$，随机选择消息$b\in\{0,1\}$，计算$c^*=\mathrm{DEM.Enc}(K_b, m_b)$。计算$S^*=cQ_{\mathrm{A}}{}^*+H_4(m)S_A{}^*$。返回$\sigma^*=(c^*, U^*, S^*)$给$\mathrm{A_I}$。

阶段2　与阶段1一样，但是不可对$\mathrm{ID_A}{}^*$私钥询问、对$\mathrm{ID}_{B_i}{}^*$秘密值询问，同样也不可对$\mathrm{ID_A}{}^*$、$\mathrm{ID}_{B_i}{}^*$解签密询问。

猜测　C输出$f^*=e(P_{B_i}{}^*, Q_{\mathrm{A}}{}^*)^t=e(aP, bP)^c=e(P, P)^{abc}$为BDH的实例解。　证毕

定理2　假设敌手$\mathrm{A_\Pi}$能以无法忽略的概率赢取改进方案中的游戏，则挑战者C就能以不可忽略的概率解决BDH问题。

证明　给定BDH问题的实例(P, aP, bP, cP)，C的目标是利用$\mathrm{A_\Pi}$计算$e(P, P)^{abc}$。

系统初始化　生成系统公开参数$\{G_1, G_2, e, P, q, H_0, H_1, H_2, H_3, H_4, P_1, P_2, n\}$，其中，$P_1=yP$，$\mathrm{A_\Pi}$知道$P_2=s_2P$。C选择选择$\mathrm{ID}^*$为被挑战者身份。

阶段1　$\mathrm{A_\Pi}$可以进行以下适应性的询问。

H_0, H_1, H_2, H_3, H_4询问，CLC公钥询问，IBC私钥询问：同定理1中的H_0, H_1, H_2, H_3, H_4询问，CLC公钥询问，IBC私钥询问。

解签密询问：当$\mathrm{A_\Pi}$对$(\mathrm{ID_A}, \mathrm{ID}_{B_i})$下的密文解签密询问时，C查看表$L_P$，若$\mathrm{ID}_{B_i}\neq\mathrm{ID}^*$时，C首先计算$f=e(Q_A, x_{B_i}U_1)$, $K=H_3\left(U, f, U_1\sum_{i=1}^{n}x_{B_i}, G_{\mathrm{ID}}, \sum_{i=1}^{n}\mathrm{ID}_{B_i}\right)$。其次恢复消息$m=\mathrm{DEM.Dec}(K, c)$。最后检查验证$e(S, P)=e(U+H_4(m)P_1, Q_A)$。若成立，则接收$m$，否则，输出“$\perp$”。

挑战　阶段1结束后，$\mathrm{A_\Pi}$选择了两个消息m_0、m_1和挑战身份$\mathrm{ID_A}^*$, $\mathrm{ID}_{B_i}{}^*$。在阶段1中不能获得$\mathrm{ID}_{B_i}{}^*$的部分私钥$D_{B_i}{}^*$、秘密值$x_{B_i}{}^*$。若$\mathrm{ID}_{B_i}{}^*\neq\mathrm{ID}^*$，C结束游戏；否则，C计算挑战密文，计算过程如下：

C首先检索表L_1，获得元组(H_2, t)。设置$U_1{}^*=cP$，计算$K_b=H_3\left(U^*, f^*, t\sum_{i=1}^{n}bP, G_{\mathrm{ID}}, \sum_{i=1}^{n}\mathrm{ID}_{B_i}\right)$，选取任意$b\in\{0,1\}$，计算$c^*=\mathrm{DEM.Enc}(K_b, m_b)$。计算$S^*=cQ_{\mathrm{A}}{}^*+H_4(m)S_A{}^*$。把密文$\sigma^*=(c^*, U^*, S^*)$返回给$\mathrm{A_\Pi}$。

阶段2　与阶段1相同，但是不能对$\mathrm{ID}_{B_i}{}^*$进行部分私钥询问。

猜测　C输出$f^*=e(P_{B_i}{}^*, Q_{\mathrm{A}}{}^*)^t=e(aP, bP)^c=e(P, P)^{abc}$作为BDH问题的实例解。　证毕

4.2 不可伪造性

定理3　在随机预言模型下，若敌手A能以无法忽略的概率伪造出有效的密文，则挑战者C就能以无法忽略的概率解决离散对数问题。

证明　C输入离散对数问题的一个实例(P, aP)，目标是计算a。

系统初始化　生成系统公开参数$\{G_1, G_2, e, P, q, H_0, H_1, H_2, H_3, H_4, P_1, P_2, n\}$，其中，$P_1=\lambda P$，$P_2=yP$，任意选取$\mathrm{ID}^*$为被挑战者的身份。

训练　敌手A可以进行以下询问当作训练。

C维护初始均为空的表$L_0\sim L_4$来分别回应H_0, H_1, H_2, H_3, H_4询问的结果。

H_0询问：C维护初始为空的表L_1来应对A询问CLC系统下身份为ID_i的H_0的结果，若询问的(ID_i, Q_i)存在表中，则直接返回Q_i；否则，C随机选择$\gamma_i\in Z_q^*$给A，同时将$(\mathrm{ID}_i, Q_i, \gamma_i)$添加到表$L_1$。

H_1询问：A输入(ID_i, Q_i)进行H_1询问时，若表L_1存在，则直接将Q_i返回给A；若询问的$\mathrm{ID}_i=\mathrm{ID}^*$，C设置$Q_i=aP$给A；否则，C随机选择$Q_i\in G_1$给A，并保存到表$L_1$。

H_2, H_3, H_4询问：同定理1中H_2, H_3, H_4询问。

CLC公钥询问：当C收到A对身份ID_{B_i}的公钥询问时，若该元组在表中则返回给A；否则，C选取任意$x_i\in Z_q^*$，计算$P_{B_i}=x_iP$给A。

CLC公钥替换询问：A用新公钥P_{B_i}'替代原来公钥P_{B_i}。

IBC私钥询问：若询问IBC系统下用户ID_i的私钥时，若$\mathrm{ID}_i=\mathrm{ID}^*$, C停止；否则，检索表$L_1$，得到元组$(\mathrm{ID}_i, Q_i)$，计算$S_{\mathrm{A}}=Q_iP$给A。

签密询问：当C收到A对$(\mathrm{ID}_{\mathrm{A}}, \mathrm{ID}_{B_i})$下消息$m$的签密询问时，C检索表$L_1$，若$\mathrm{ID}_i\neq\mathrm{ID}^*$，查表$L_2$和$L_4$获取$t$和$h_4$，C计算$U=tP$，$V=yP\gamma_i$和$f=e(Q_{\mathrm{A}}, P_{B_i})^t$，计算$K=H_3\left(U, f, V, t\sum_{i=1}^{n}P_{B_i}, G_{\mathrm{ID}}, \sum_{i=1}^{n}\mathrm{ID}_{B_i}\right)$和$c=\mathrm{DEM.Enc}(K, m)$。同时计算$S=tQ_{\mathrm{A}}+H_4(m)S_{\mathrm{A}}$，将签密密文$\sigma=(c, U, S)$返回给A。

伪造 A最终输出对$(m^*, \mathrm{ID}_{\mathrm{A}}^*)$下的签密密文$\sigma^*=(c^*, U^*, S^*)$。假设$\mathrm{ID}_{\mathrm{A}}\neq\mathrm{ID}^*$，则C中止游戏；否则，根据分叉引理[17]，对$H_4$进行重放之后，A可以输出另外一个有效的密文$\sigma^{*\prime}=(c^{*\prime}, U^{*\prime}, S^{*\prime})$，其中，$S^*=tQ_{\mathrm{A}}{}^*+H_4(m)S_{\mathrm{A}}{}^*$，$S^{*\prime}=tQ_{\mathrm{A}}{}^*+H_4'(m)S_{\mathrm{A}}{}^*$，根据这两个等式，可以计算出$S^*-S^{*\prime}=S_{\mathrm{A}}{}^*(H_4(m)-H_4'(m))=\lambda aP(H_4(m)-H_4'(m))$，输出$a=(\lambda P)^{-1}\left(\dfrac{S^*-S^{*\prime}}{H_4(m)-H_4'(m)}\right)$作为离散对数问题解的一个实例。 证毕

5 性能分析

5.1 计算代价比较

首先，对本文所提改进方案进行性能分析。P代表双线性对运算、M点乘运算与E指数运算，其运行时间依次为3.711 ms, 2.165 ms与4.38 ms。表1为本文方案与牛方案在通信方向、签密与解签密计算代价、安全性等方面进行的性能比较。本文方案与牛方案均为IBC→CLC的通信，在签密阶段，本文方案虽然增加了一个双线性对的运算，但是，本文方案的点乘运算比牛方案的点乘运算少。在解签密阶段，本文方案增加了3个双线性对和1个指数运算，但是，在点乘运算上本文方案的计算量低于牛方案。

当接收人数n依次为100, 200, …, 1000时，签密与解签密时间如表2、表3所示。由表2、表3可知，在签密阶段与解签密阶段，本文方案的计算代价要优于牛方案。

5.2 模拟实验

将本文方案与牛方案进行实验模拟。实验平台为Dell笔记本(I7-4700 CPU @3.20 GHz, 8 GB内存和Ubuntu Linux操作系统)，运用了密码学函数库(Pairing Based Cryptography, PBC)。采用类型为A的椭圆曲线$y^2=x^3+x \bmod n$，其生成元为$|P|=512$ bit，大素数为$|q|=1024$ bit。实验结果如图1、图2所示。

由图1、图2可知，当接收者人数越多时，本文方案的计算效率明显优于牛方案。所以，本文方案更适合多接收者的签密环境。

6 结束语

异构混合群组签密可以实现不同密码体制下的发送方对任意长度的消息利用多接收者的身份进行签密，从而保证消息的机密性与不可伪造性。本文分析了牛淑芬等人提出的异构混合群组签密方案的安全性，指出该方案不满足方案的正确性、安全模型下的机密性和不可伪造性。为了克服这些安全缺陷，本文提出了一个安全的异构混合群组签密方案，并证明了本文方案的安全性。性能分析表明，与牛方案相比，本文方案的计算效率更高。

表 1 性能分析

方案	方向	签密	解签密	机密性	不可伪造性
牛方案	IBC→CLC	$(2n+7)M$	$(2n+5)M$	×	×
本文方案	IBC→CLC	$P+(4+n)M$	$3P+E+(n+2)M$	√	√

表 2 签密计算时间(s)

N	100	200	300	400	500	600	700	800	900	1000
牛方案	0.448	0.881	1.314	1.747	2.18	2.613	3.046	3.479	3.912	4.345
本文方案	0.229	0.445	0.662	0.878	1.095	1.311	1.529	1.744	1.961	2.177

表 3 解签密计算时间(s)

N	100	200	300	400	500	600	700	800	900	1000
牛方案	0.443	0.876	1.309	1.742	2.175	2.608	3.041	3.474	3.907	4.340
本文方案	0.236	0.453	0.669	0.889	1.102	1.318	1.535	1.751	1.968	2.184

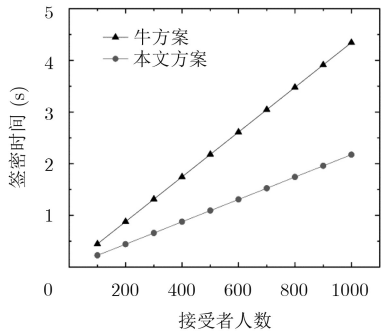

图 1 签密阶段计算效率

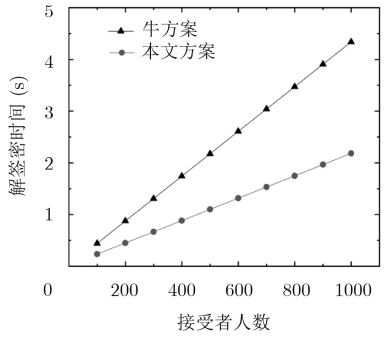

图 2 解签密阶段计算效率

参 考 文 献

[1] ZHENG Yuliang. Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption)[C]. Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 1997: 165–179. doi: 10.1007/BFb0052234.

[2] CRAMER R and SHOUP V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack[J]. *SIAM Journal on Computing*, 2004, 33(1): 167–226. doi: 10.1137/S0097539702403773.

[3] DENT A W. Hybrid signcryption schemes with outsider security[C]. Proceedings of the 8th International Conference on Information Security, Singapore, 2005: 203–217. doi: 10.1007/11556992_15.

[4] DENT A W. Hybrid signcryption schemes with insider security[C]. Proceedings of the 10th Australasian Conference on Information Security, Brisbane, Australia, 2005: 253–266. doi: 10.1007/11506157_22.

[5] SIVASUNDARI A and RAMAKRISHNAN M. Hybrid aggregated signcryption scheme using multi-constraints differential evolution algorithm for security[J]. *Cluster Computing*, 2018(2): 1–11. doi: 10.1007/s10586-018-2016-3.

[6] 周彦伟, 杨波, 王青龙. 可证安全的抗泄露无证书混合签密机制[J]. 软件学报, 2016, 27(11): 2898–2911. doi: 10.13328/j.cnki.jos.004941.

ZHOU Yanwei, YANG Bo, and WANG Qinglong. Provably secure leakage-resilient certificateless hybrid signcryption scheme[J]. *Journal of Software*, 2016, 27(11): 2898–2911. doi: 10.13328/j.cnki.jos.004941.

[7] LI Fagen, SHIRASE M, and TAKAGI T. Certificateless hybrid signcryption[C]. Proceedings of the 5th International Conference on Information Security Practice and Experience, Xi'an, China, 2008: 112–123. doi: 10.1007/978-3-642-00843-6_11.

[8] SELVI S S D, VIVEK S S, and RANGAN C P. Breaking and Re-building a Certificateless Hybrid Signcryption Scheme[M]. Berlin, Heidelberg: Springer, 2010: 294–307. doi: 10.1007/978-3-642-12827-1_22.

[9] 周彦伟, 杨波, 王青龙. 基于身份的多接收者(多消息)匿名混合签密机制[J]. 软件学报, 2018, 29(2): 442–455. doi: 10.13328/j.cnki.jos.005250.

ZHOU Yanwei, YANG Bo, and WANG Qinglong. Anonymous hybrid signcryption scheme with multi-receiver (multi-message) based on identity[J]. *Journal of Software*, 2018, 29(2): 442–455. doi: 10.13328/j.cnki.jos.005250.

[10] 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.

[11] 刘景伟, 张俐欢, 孙蓉. 异构系统下的双向签密方案[J]. 电子与信息学报, 2016, 38(11): 2948–2953. doi: 10.11999/JEIT160056.

LIU Jingwei, ZHANG Lihuan, and SUN Rong. Mutual signcryption schemes under heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2016, 38(11): 2948–2953. doi: 10.11999/JEIT160056.

[12] 张玉磊, 王欢, 刘文静, 等. 异构双向签密方案的安全性分析和改进[J]. 电子与信息学报, 2017, 39(12): 3045–3050. doi: 10.11999/JEIT170203.

ZHANG Yulei, WANG Huan, LIU Wenjing, *et al*. Security analysis and improvement of mutual signcryption schemes under heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2017, 39(12): 3045–3050. doi: 10.11999/JEIT170203.

[13] NIU Shufen, LI Zhenbin, and WANG Caifen. Privacy-preserving multi-party aggregate signcryption for heterogeneous systems[C]. Proceedings of the 3rd International Conference on Cloud Computing and Security, Nanjing, China, 2017: 216–229. doi: 10.1007/978-3-319-68542-7_18.

[14] 张玉磊, 刘祥震, 郎晓丽, 等. 新的具有隐私保护功能的异构聚合签密方案[J]. 电子与信息学报, 2018, 40(12): 3007–3012. doi: 10.11999/JEIT180249.

ZHANG Yulei, LIU Xiangzhen, LANG Xiaoli, *et al*. New privacy preserving aggregate signcryption for heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2018, 40(12): 3007–3012. doi: 10.11999/JEIT180249.

[15] NIU Shufen, NIU Ling, YANG Xiyan, *et al*. Heterogeneous hybrid signcryption for multi-message and multi-receiver[J]. *PLoS One*, 2017, 12(9): e0184407. doi: 10.1371/journal.pone.0184407.

[16] 牛淑芬, 杨喜艳, 王彩芬, 等. 基于异构密码系统的混合群组签密方案[J]. 电子与信息学报, 2019, 41(5): 1180–1186. doi: 10.11999/JEIT180554.

NIU Shufen, YANG Xiyan, WANG Caifen, *et al*. Hybrid group signcryption scheme based on heterogeneous cryptosystem[J]. *Journal of Electronics & Information Technology*, 2019, 41(5): 1180–1186. doi: 10.11999/JEIT180554.

[17] HORNG S J, TZENG S F, HUANG P H, *et al*. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. *Information Sciences*, 2015, 317: 48–66. doi: 10.1016/j.ins.2015.04.033.

张玉磊：男，1979年生，博士，副教授，研究方向为密码学与信息安全.

刘祥震：男，1991年生，硕士生，研究方向为密码学与信息安全.

郎晓丽：女，1993年生，硕士生，研究方向为密码学与信息安全.

张永洁：女，1978年生，硕士，副教授，研究方向为密码学与信息安全.

王彩芬：女，1963年生，博士，教授，博士生导师，研究方向为密码学与信息安全.