基于异构密码系统的混合群组签密方案

牛淑芬*[①] 杨喜艳[①] 王彩芬[①] 田 苗[①] 杜小妮[②]

[①](西北师范大学计算机科学与工程学院 兰州 730070)

[②](西北师范大学数学与统计学院 兰州 730070)

摘 要：群组签密既能实现群组签名，又能实现群组加密，但是现有的群组签密方案的发送者和接收者基本上在同一个密码系统中，不能满足现实环境的需求，而且基本上采用的是公钥加密技术，公钥加密技术在加密长消息时效率较低。因此该文提出由基于身份的密码体制(IBC)到无证书密码体制(CLC)的异构密码系统的混合群组签密方案。在该方案中，私钥生成器(PKG)和密钥生成中心(KGC)能够分别在IBC密码体制和CLC密码体制中产生自己的系统主密钥；而且群组成员只有协作才能解签密，提高了方案的安全性；同时在无需更换群组公钥和其他成员私钥的情况下，用户可以动态地加入该群组。所提方案采用了混合签密，具有可加密任意长消息的能力。在随机预言模型下，证明了该文方案在计算Diffie-hellman困难问题下具有保密性和不可伪造性。通过理论和数值实验分析表明该方案具有更高的效率和可行性。

关键词：无证书密码学；异构密码系统；混合签密；基于身份的密码学；群组签密

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)05-1180-07

DOI: 10.11999/JEIT180554

Hybrid Group Signcryption Scheme Based on Heterogeneous Cryptosystem

NIU Shufen[①] YANG Xiyan[①] WANG Caifen[①] TIAN Miao[①] DU Xiaoni[②]

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

[②](*College of Mathematics and Statistics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Group signcryption is a cryptosystem which can realize group signature and group encryption. However, the message sender and receiver of existing group signcryption schemes are basically in the same cryptosystem, which does not meet the needs of the real environment and the public key encryption technology is basically used, public key encryption technology in encrypted long message efficiency is too low. Therefore, this paper proposes a hybrid group signcryption scheme based on heterogeneous cryptosystem from Identity-Based Cryptosystem (IBC) to CertificateLess Cryptosystem (CLC). In the scheme, The Private Key Generator (PKG) in the IBC cryptosystem and Key Generation Center (KGC) in the CLC cryptosystem generate their own system master keys, and group members can only solve signcryption through collaboration, which improves the security of the scheme. Meanwhile, the user can dynamically join the group without changing the group public key and other members' private key. The scheme uses hybrid signcryption and has the ability to encrypt any long message. It is proved that the scheme satisfies confidentiality and unforgeability in computing the Diffie-hellman hard problem in the random oracle model. Theoretical and numerical analysis shows that the scheme is more efficient and feasible.

Key words: CertificateLess Cryptography (CLC); Heterogeneous systems; Hybrid signcryption; Identity-Based Cryptography (IBC); Group signcryption

收稿日期：2018-06-06；改回日期：2018-12-25；网络出版：2019-01-02

*通信作者： 牛淑芬 sfniu76@nwnu.edu.cn

基金项目：国家自然科学基金(61562077, 61462077, 61662071, 61662069)，甘肃省杰出青年基金(1308RJDA007)，国家留学基金

Foundation Items: The National Natural Science Foundation of China (61562077, 61462077, 61662071, 61662069), The Natural Science Foundation of Gansu Province for Distinguished Young Scholars (1308RJDA007), China Scholarship Council Project

1　引言

信息在网络通信中需要同时具备保密性和认证性，数字签密[1]使得签密密文同时具备保密性和认证性。此后很多学者研究了签密[2–4]，例如异构签密方案[5,6]。但现有的异构签密方案基本采用公钥加密技术，公钥加密技术加密长消息时速度太慢，通常只适合加密短消息。在实际的安全通信中，大多采用混合加密[7]或混合签密[8–11]的方式，混合加密分为密钥封装机制(Key Encapsulation Mechanism, KEM)和数据封装机制(Data Encapsulation Mechanism, DEM)，其中KEM使用公钥加密技术加密对称密钥，DEM使用对称加密技术加密消息。因此，混合密码学具有安全高效的特点。但是上述异构签密方案和混合签密方案均没有实现广播式地将签密密文发送给多个接收方，在某些网络通信中，需要将签密密文发送给多个接收方，若是将签密密文点对点的依次发送给不同的用户，显而易见的是效率很低，通信成本也很高。为此很多学者提出了群组签密方案[12,13]，2013年，冯君等人[14]提出了一种高安全的门限群签密方案，同年，Chen等人[15]提出了一种新的基于身份的群体签密方案。

在上述的群组签密方案中，既不具备对任意长消息签密能力，也没有实现在不同的密码体制中密钥生成中心能够产生自己的系统主密钥。针对此问题，本文提出了一个基于异构密码系统的混合群组签密方案，本文方案采取了混合签密，可对任意长消息加密，提高了方案的计算效率。PKG和KGC能够分别在IBC密码体制和CLC密码体制中产生各自的系统主密钥，提高了系统的安全性。同时，在无需更换群组公钥和其他成员私钥的情况下，用户可以动态地加入该群组。

2　形式化定义和具体方案

2.1　形式化定义

基于异构密码系统的混合群组签密方案的形式化定义由以下5个算法构成：

系统建立　输入安全参数k，输出PKG的密钥对(s_1, P_1)、KGC的密钥对(s_2, P_2)和系统参数pa。

IBC密钥提取　输入身份ID_j、群组身份$G_{\mathrm{ID}} \in \{0,1\}^*$和主密钥$s_1$, PKG输出用户私钥$S_j$。

CLC密钥提取　该提取过程分为以下3步：

(1)部分私钥提取：输入身份ID_i和群组身份G_{ID}, KGC计算该用户的部分私钥D_i。

(2)用户公钥提取：输入身份ID_i和群组身份G_{ID}，随机选取ID_i的秘密值x_i，并输出公钥P_i。

(3)私钥提取：输入系统参数pa、部分私钥D_i、秘密值x_i，输出私钥S_i。

签密　由以下2个算法构成：

(1)密钥封装：发送方A输入私钥S_j、消息m、系统参数pa、接收群组身份G_{ID}和接收群组成员身份ID_i，输出密钥封装(K, ϕ)，其中K为对称密钥，ϕ是对K进行封装的结果。

(2)加密：输入安全参数k、对称密钥K和消息m，输出密文c。

解签密　由以下2个算法构成：

(1)密钥解封装：输入发送者身份ID_j、接收群组身份G_{ID}、系统参数pa、密钥封装ϕ、接收群组成员身份ID_i、私钥S_i，输出对称密钥K或者$\perp$。

(2)解密：输入密文c、对称密钥K，输出消息m或者$\perp$。

2.2　具体方案

基于异构密码系统的混合群组签密方案的具体实现如下：

系统建立　设循环群G_1, G_2的阶均为素数q, P为G_1的生成元。定义3个安全的Hash函数：$H_1: \{0,1\}^* \to G_1$，$H_2: G_2 \to \{0,1\}^n \times \{0,1\}^n$和$H_3: \{0,1\}^* \times G_2 \to \boldsymbol{Z}_q^*$。$(E, D)$分别是对称加密体制中的加密和解密算法。输入安全参数1^k，输出主密钥s_1, s_2、参数pa。然后PKG和KGC分别保密s_1和s_2，并计算对应公钥$P_1 = s_1^{-1}P$和$P_2 = s_2^{-1}P$。公开系统参数$\mathrm{pa}=\{G_1, G_2, q, P, e, n, H_1, H_2, H_3, E, D\}$。

IBC密钥提取　PKG随机选取$r_A \in \boldsymbol{Z}_q^*$，输入发送方身份$\mathrm{ID}_A$、接收方群组身份$G_{\mathrm{ID}}$，输出发送方私钥$S_A = \left(r_A^{-1} s_1 R P H_1(G_{\mathrm{ID}}), h_A\right)$，其中$R = r_A H_1(\mathrm{ID}_A)$, $h_A = s_1 R P H_1(G_{\mathrm{ID}})$，并通过安全方式发送给发送者。

CLC密钥提取　该提取过程分为以下3步：

(1)部分私钥提取：输入用户身份$\mathrm{ID}_{B_i} \in (\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n})$、接收群组身份$G_{\mathrm{ID}}$和系统参数pa, KGC计算该用户的部分私钥$D_{B_i} = s_2^{-1} H_1(\mathrm{ID}_{B_i}) \cdot H_1(G_{\mathrm{ID}})$，并通过安全方式发送给该用户。

(2)用户公钥提取：输入用户身份ID_{B_i}、接收群组身份G_{ID}和系统参数pa，用户随机选择秘密值$x_{B_i} \in \boldsymbol{Z}_q^*$，并输出公钥$P_{B_i} = x_{B_i} P$。

(3)私钥提取：输入系统参数pa、部分私钥D_{B_i}、秘密值x_{B_i}，输出私钥$S_{B_i} = (x_{B_i}, D_{B_i}) = (x_{B_i}, s_2^{-1} H_1(\mathrm{ID}_{B_i}) H_1(G_{\mathrm{ID}}))$。

签密　若发送者需将消息m发送给接收群组的的所有成员，过程如下：

随机选取$t \in \boldsymbol{Z}_q^*$，计算$U_1 = tP$, $U_2 = tH_1(G_{\mathrm{ID}})$, $U_3 = tP_2$, $T = U_3 H_1(G_{\mathrm{ID}}) \sum_{i=1}^{n} H_1(\mathrm{ID}_{B_i})$, $K = H_2\big(U_1,$

$U_2, U_3, T, t\sum_{i=1}^{n} P_{B_i}, \sum_{i=1}^{n}\mathrm{ID}_{B_i}, G_{\mathrm{ID}}\Big)$, $c=\mathrm{DEM}$。$\mathrm{Enc}(K,m), H=H_3\Big(c, U_1, U_2, U_3, \mathrm{ID}_A, \sum_{i=1}^{n}\mathrm{ID}_{B_i}, G_{\mathrm{ID}}\Big)$, $S=P(t+H)$, $V_1=r_A^{-1}$, $V_2=Sh_A$, $V=V_1V_2$，输出密文：$\sigma=(c,\phi\leftarrow(U_1,U_2,U_3,V))$。

解签密 若接收群组成员收到密文$\big(c,\phi\leftarrow(U_1,U_2,U_3,V)\big)$时，验证$P_1V=P^2H_1(\mathrm{ID}_A)H_1(G_{\mathrm{ID}})\cdot(U_1+PH)$是否成立，若不成立，输出$\perp$；否则，则进行以下操作：计算$T=U_1\sum_{i=1}^{n}D_{B_i}$，$K=H_2\Big(U_1, U_2, U_3, T, U_1\sum_{i=1}^{n}x_{B_i}, \sum_{i=1}^{n}\mathrm{ID}_{B_i}, G_{\mathrm{ID}}\Big)$，$m=\mathrm{DEM.Dec}(K,c)$，输出$m$。

正确性证明

$$\begin{aligned}P_1V&=s_1^{-1}r_A^{-1}PSh_A=s_1^{-1}r_A^{-1}PP(t+H)r_AH_1(\mathrm{ID}_A)\\&\quad\cdot Ps_1H_1(G_{\mathrm{ID}})\\&=U_1P^2H_1(\mathrm{ID}_A)H_1(G_{\mathrm{ID}})+P^3HH_1(\mathrm{ID}_A)\\&\quad\cdot H_1(G_{\mathrm{ID}})\\&=P^2H_1(\mathrm{ID}_A)H_1(G_{\mathrm{ID}})(U_1+PH)。\end{aligned}$$

3 安全模型和安全性分析

3.1 安全模型

基于异构密码系统的混合群组签密方案(Hybrid Group Signcryption Scheme Based on Heterogeneous Cryptosystem, HGSSBHC)应该满足IND-CCA2 (INDistinguishability against Adaptive Chosen Ciphertext Attack)安全性和EUF-CMA (Existential UnForgeability against adaptive Chosen Message Attack)安全性。在安全模型中，主要考虑两种攻击者A_1和A_2: s_2对于A_1是未知的，对于A_2是已知的，但A_1能自适应地替换用户公钥，A_2不能。

3.1.1 自适应选择密文不可区分安全模型

游戏1 在IND-CCA2-1中挑战者C和A_1的交互分为以下5个阶段：

(1)系统建立：C运行系统建立算法，输出s_2和pa，保留s_2，返回pa给A_1。

(2)阶段1：C和A_1的游戏过程中，A_1能对以下预言机进行有界次询问。

(a)公钥询问：A_1输入身份ID_i和群组身份G_{ID}，C运行公钥提取算法，返回公钥P_i。

(b)部分私钥询问：A_1输入身份ID_i和群组身份G_{ID}，C运行部分私钥提取算法，返回D_i。

(c)私钥询问：A_1输入身份ID_i和群组身份G_{ID}，C运行私钥提取算法，返回$S_i\leftarrow(x_i,D_i)$。

(d)公钥替换：A_1用任何值替换用户公钥。

(e)签密询问：当C得到消息m、发送方身份ID_A时，计算$S_A=\mathrm{KeyGen}(\mathrm{ID}_A,G_{\mathrm{ID}})$, $\sigma\leftarrow\mathrm{Sig}\big(\mathrm{pa}, m, S_A, G_{\mathrm{ID}}, \mathrm{ID}_A, \mathrm{ID}_{B_i}, P_A, P_{B_i}\big)$，返回给$A_1$。

(f)解签密询问：询问发送方身份ID_A、密文σ、接收群组身份G_{ID}、接收群组成员身份ID_{B_i}下的解签密时，C在相应的列表中查询到(S_{B_i},P_A,P_{B_i})，然后返回$m/\perp\leftarrow\mathrm{U}_n\big(\mathrm{pa},\mathrm{ID}_A,\mathrm{ID}_{B_i},S_{B_i},G_{\mathrm{ID}},P_A,P_{B_i},\sigma\big)$。

(3)挑战：阶段1结束后，A_1输入等长的消息m_0,m_1和挑战身份$\mathrm{ID}_A^*,\mathrm{ID}_{B_i}^*$，阶段1中不询问$\mathrm{ID}_{B_i}^*$的$D_{B_i}^*$, $x_{B_i}^*$，及$P_{B_i}^*$替换。C在相应列表中查询到$(S_A^*,P_A^*,P_{B_i}^*)$，选择$b\in\{0,1\}$，计算$\sigma^*\leftarrow\mathrm{Sig}\big(\mathrm{pa}, m_b, S_A^*, G_{\mathrm{ID}}, \mathrm{ID}_A^*, \mathrm{ID}_{B_i}^*, P_A^*, P_{B_i}^*\big)$，返回挑战密文$\sigma^*$。

(4)阶段2：同阶段1，另外A_1不询问$\mathrm{ID}_{B_i}^*$的$S_{B_i}^*$和$P_{B_i}^*$替换，及对$\mathrm{ID}_A^*,\mathrm{ID}_{B_i}^*$下的$\sigma^*$解签密。

(5)猜测：A_1猜测出一个b'，若$b'=b$, A_1在IND-CCA2-1中获胜。

游戏2 在IND-CCA2-2中挑战者C和A_2的交互分为以下5个阶段：

(1)系统建立：C运行系统建立算法，输出参数pa、主密钥s_2，返回(s_2,pa)给A_2。

(2)阶段1：A_2不询问D_i及P_i替换，其余询问同IND-CCA2-1的阶段1。

(3)挑战：阶段1结束后，A_2输入两个等长的消息m_0,m_1和两个挑战身份$\mathrm{ID}_A^*,\mathrm{ID}_{B_i}^*$，但是在阶段1的询问过程中，不能询问$\mathrm{ID}_{B_i}^*$的秘密值。$C$从相关列表中查询到$(S_A{}^*,P_A^*,P_{B_i}^*)$，选择$b\in\{0,1\}$，计算挑战密文$\sigma^*\leftarrow\mathrm{Sig}(\mathrm{pa},m_b,S_A^*,G_{\mathrm{ID}},\mathrm{ID}_A^*,\mathrm{ID}_{B_i}^*,P_A^*,P_{B_i}^*)$，最后返回$\sigma^*$。

(4)阶段2：同阶段1，另外A_2不对$\mathrm{ID}_{B_i}^*$的秘密值及$\mathrm{ID}_A^*,\mathrm{ID}_{B_i}^*$下的$\sigma^*$解签密询问。

(5)猜测：A_2猜测出一个b'，若$b'=b$, A_2在IND-CCA2-2中获胜。

3.1.2 自适应选择消息存在性不可伪造安全模型

游戏3 在EUF-CMA中伪造者F和挑战者C的交互分为以下3个阶段：

(1)系统建立：C运行系统建立算法，输出pa和s_1，返回pa给F，保留s_1。

(2)训练：同IND-CCA2-1的阶段1，另外F的S_j询问方式不同，及不询问D_j。

私钥询问：F输入ID_j和G_{ID}, C运行私钥提取算法，返回私钥S_j。

(3)伪造：训练结束后，F输出伪造$\big(\mathrm{ID}_A^*,\mathrm{ID}_{B_i}^*,G_{\mathrm{ID}},\sigma^*\big)$，在训练中，不允许询问$\mathrm{ID}_A^*$的$S_A^*$、替换$\mathrm{ID}_A^*$的$P_A{}^*$和$\sigma^*$不可以是$\mathrm{ID}_{B_i}^*$下消息$m^*$的应答。若$\sigma^*$下的解签密$\mathrm{U}_n(\mathrm{pa},\mathrm{ID}_A^*,\mathrm{ID}_{B_i}^*,G_{\mathrm{ID}},S_{B_i}^*,P_A^*,P_{B_i}^*,\sigma^*)$输出的不是$\perp$, F赢得EUF-CMA。

3.2 安全性分析

定理1　假设在IND-CCA2-1中，A_1能攻破HGSSBHC的IND-CCA2-1安全性，则C就能够求解CDH问题。

证明　C获得CDH问题的随机实例$(P, aP, bP) \in G_1$时，需计算出$abP \in G_1$作为实例解答。

系统建立　C运行系统建立算法，同时建立4张空列表L_1, L_2, L_3, L_k，用来储存对应预言机的询问和应答。

阶段1　A_1适应性地询问。

H_1询问：A_1选择一系列身份询问相应Hash值，若询问ID_{B_i}的H_1时，L_1中含$(\mathrm{ID}_{B_i}, H_i, l_i)$时，$C$将$H_i$作为应答返回；反之，$C$随机选择$\{1,2,\cdots,n\} \subseteq \{1,2,\cdots,q_1\}$，且不泄露给$A_1$，并将$\{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$作为挑战身份。当第$\{1,2,\cdots,n\}$次询问时，$C$设置$H_i = bP$，并返回$H_i$，最后添加$(\mathrm{ID}_{B_i}, H_i, -)$到$L_1$。当不是第$\{1,2,\cdots,n\}$次询问时，随机选择$l_i \in \boldsymbol{Z}_q^*$，设置$H_i \leftarrow l_i P$，然后添加$(\mathrm{ID}_{B_i}, H_i, l_i)$到$L_1$。

H_2询问：对每次新的$H_2\Big(U_1, U_2, U_3, T, \sum_{i=1}^{n} Q_{B_i}, \sum_{i=1}^{n} \mathrm{ID}_{B_i}, G_{\mathrm{ID}}\Big)$询问，$C$执行以下步骤：

(1)检查$e(aP, bP) = e\Big(P, \sum_{i=1}^{n} Q_{B_i}\Big)$是否成立，若成立，$C$返回$\sum_{i=1}^{n} Q_{B_i}$并停止；

(2)检查列表L_2是否存在$\Big(U_1, U_2, U_3, T, -, \sum_{i=1}^{n} \mathrm{ID}_{B_i}, G_{\mathrm{ID}}, K\Big)$满足$e(U_1, aP) = e\Big(P, \sum_{i=1}^{n} Q_{B_i}\Big)$。在这种情况下，$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$，$C$返回$K$，并用$\sum_{i=1}^{n} Q_{B_i}$代替“$-$”；

(3)若C执行到这一步，随机选择$K \in \{0,1\}^n$，并将$\Big(U_1, U_2, U_3, T, \sum_{i=1}^{n} Q_{B_i}, \sum_{i=1}^{n} \mathrm{ID}_{B_i}, G_{\mathrm{ID}}, K\Big)$存入$L_2$。

H_3询问：如若询问H_3时，C查看L_3中有无元组$(c, U_1, U_2, U_3, \mathrm{ID}_A, \mathrm{ID}_{B_i}, G_{\mathrm{ID}}, H, f)$，若有，则返回$H$；否则，$C$选择随机数$f \in \boldsymbol{Z}_q^*$，返回$H = fP$，添加$(c, U_1, U_2, U_3, \mathrm{ID}_A, \mathrm{ID}_{B_i}, G_{\mathrm{ID}}, H, f)$到$L_3$。

公钥询问：如若询问ID_{B_i}的公钥时，C查看L_k中有无$(\mathrm{ID}_{B_i}, D_{B_i}, x_{B_i}, P_{B_i})$，若有，$C$返回$P_{B_i}$；否则，选择随机数$a \in \boldsymbol{Z}_q^*$，计算$P_{B_i} = aP$，返回公钥$P_{B_i}$，添加$(\mathrm{ID}_{B_i}, -, a, P_{B_i})$到$L_k$。

公钥替换询问：A_1用随机数P_B'替换P_{B_i}。如果$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$，那么$C$退出游戏；否则，$C$用$(\mathrm{ID}_{B_i}, D_{B_i}, -, P_{B_i}')$更新$L_k$。

部分私钥询问：假如询问ID_{B_i}的部分私钥时，C查看$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$是否成立。若成立，那么$C$放弃游戏；否则，$C$从$H_1$预言机得到$l_i$，并且设置$D_{B_i} = s^{-1} l_i P_{\mathrm{pub}}$，然后返回部分私钥$D_{B_i}$，最后用$(\mathrm{ID}_{B_i}, D_{B_i}, x_{B_i}, P_{B_i})$更新$L_k$。

私钥询问：收到ID_{B_i}的私钥询问时，C检查$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$是否成立。若成立，$C$放弃游戏；否则，$C$从$L_1/L_k$找到$l_i/\big(\mathrm{ID}_{B_i}, -, x_{B_i}, P_{B_i}\big)$，返回$x_{B_i}$，用$(\mathrm{ID}_{B_i}, s^{-1} l_i P_{\mathrm{pub}}, x_{B_i}, P_{B_i})$更新$L_k$。

解签密询问：若是$(\mathrm{ID}_A, \mathrm{ID}_{B_i})$下的解签密询问时，$C$检查$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$是否成立。若成立，$C$返回失败并停止；否则，$C$作出如下应答：

通过L_k得到$x_{B_i} = a$；若$\mathrm{ID}_{B_i} \notin \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$，计算$\sum_{i=1}^{n} Q_{B_i} = U_1 \sum_{i=1}^{n} x_{B_i}$；计算$K = H_2\Big(U_1, U_2, U_3, T, \sum_{i=1}^{n} Q_{B_i}, \sum_{i=1}^{n} \mathrm{ID}_{B_i}, G_{\mathrm{ID}}\Big)$，$m = \mathrm{DEM.Dec}(K, c)$；检查等式$P_1 V = P^2 H_1(\mathrm{ID}_A) \cdot H_1(G_{\mathrm{ID}})(U_1 + PH)$是否成立。若成立，接受$m$；否则，输出$\perp$。

挑战　阶段1结束后，A_1输入两个等长的消息m_0, m_1和挑战身份$\mathrm{ID}_A^*, \mathrm{ID}_{B_i}^*$。在阶段1询问期间，不能询问$\mathrm{ID}_{B_i}^*$的秘密值。若$\mathrm{ID}_{B_i} \notin \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_j}\}$，$C$结束游戏；反之，$C$计算挑战密文，过程如下：

设置$U_1^* = cP$；通过L_k可得到$\sum_{i=1}^{n} x_{B_i} = a$，计算$\sum_{i=1}^{n} Q_{B_i} = U_1 \sum_{i=1}^{n} x_{B_i}$；计算$K_1 = H_2\Big(U_1^*, U_2, U_3, T^*, U_1^* \sum_{i=1}^{n} x_{B_i}, \sum_{i=1}^{n} \mathrm{ID}_{B_i}^*, G_{\mathrm{ID}}\Big)$，添加$\Big(U_1^*, U_2, U_3, T^*, U_1^* \sum_{i=1}^{n} x_{B_i}, \sum_{i=1}^{n} \mathrm{ID}_{B_i}^*, G_{\mathrm{ID}}, K_1\Big)$到$L_2$；选择任意$K_0 \in K_{\mathrm{HGSSBHC}}$，$b \in \{0,1\}$；计算$c^* = \mathrm{DEM.Dec}(K_b, m_b)$；计算$H^* = f^* P$，添加$\Big(c^*, U_1^*, U_2, U_3, \mathrm{ID}_A^*, \sum_{i=1}^{n} \mathrm{ID}_{B_i}^*, G_{\mathrm{ID}}, H^*\Big)$到$L_3$；计算$S^* = P(t + H^*)$，$V_1^* = r_A^{-1}$，$V_2^* = S^* h_A$，$V^* = V_1^* V_2^*$；返回$\sigma^* = (c^*, \phi \leftarrow (U_1^*, U_2, U_3, V^*))$。

阶段2　同阶段1，另外A_1不对$\mathrm{ID}_{B_i}^*$的秘密值及$\mathrm{ID}_A^*, \mathrm{ID}_{B_i}^*$下$\sigma^*$的解签密询问。

猜测　C输出$Q_{B_i}^* = U_1^* x_{B_i}^* = acP$作为CDH问题的实例解答。　　证毕

定理2　在IND-CCA2-2中，假如A_2能攻破HGSSBHC的IND-CCA2-2安全性，则C可以求解CDH问题。

证明　C获得CDH问题的随机实例$(P, aP, bP) \in G_1$时，需计算出$abP \in G_1$作为实例解答。

系统建立　C运行系统建立算法，同时建立4张空列表L_1, L_2, L_3, L_k，用来储存对应预言机的询

问和应答。

阶段1 A_2适应性的询问。

H_1, H_2, H_3询问和公钥询问：与定理1相同。

私钥询问：若是ID_{B_i}的私钥询问，C检查是否$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$成立。若成立，$C$退出游戏；反之，$C$从$L_k$中检索到$(\mathrm{ID}_{B_i}, D_{B_i}, a, P_{B_i})$，返回私钥$S_{B_i} \leftarrow (a, D_{B_i})$。

解签密询问：对于身份$\mathrm{ID}_A, \mathrm{ID}_{B_i}$下的$\sigma$解签密询问，$C$作如下应答：

通过L_k得到$P_{B_i} = aP$；若$\mathrm{ID}_{B_i} \notin \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$，计算$\sum_{i=1}^{n} Q_{B_i} = t\sum_{i=1}^{n} P_{B_i}$；计算$U_2 = tH_1(G_{\mathrm{ID}})$，$m = \mathrm{DEM.Dec}(K, c)$；检查等式$P_1 V = P^2 H_1(\mathrm{ID}_A) H_1(G_{\mathrm{ID}})(U_1 + PH)$是否成立，若成立，接受$m$；否则，输出$\perp$。

挑战 阶段1结束后，A_2输入两个等长的消息m_0, m_1和挑战身份$\mathrm{ID}_A^*, \mathrm{ID}_{B_i}^*$。在阶段1中，不询问$\mathrm{ID}_{B_i}^*$的$D_{B_i}^*$，$x_{B_i}^*$，及$P_{B_i}^*$替换。若$\mathrm{ID}_{B_i}^* \in \{\mathrm{ID}_{B_1}^*, \mathrm{ID}_{B_2}^*, \cdots, \mathrm{ID}_{B_n}^*\}$，$C$放弃游戏；反之，$C$计算挑战密文，计算过程如下：

通过L_k得到$P_{B_i}^* = aP$；计算$\sum_{i=1}^{n} Q_{B_i}^* = t\sum_{i=1}^{n} P_{B_i}^*$；计算$K_1 = H_2\left(U_1, U_2, U_3, T^*, \sum_{i=1}^{n} Q_{B_i}^*, \sum_{i=1}^{n} \mathrm{ID}_{B_i}^*, G_{\mathrm{ID}}\right)$，添加$\left(U_1, U_2, U_3, T^*, \sum_{i=1}^{n} Q_{B_i}^*, \sum_{i=1}^{n} \mathrm{ID}_{B_i}^*, G_{\mathrm{ID}}, K_1\right)$到$L_2$；选择任意$K_0 \in K_{\mathrm{HGSSBHC}}$，$b \in \{0, 1\}$；计算$c^* = \mathrm{DEM.Dec}(K_b, m_b)$；计算$H^* = f^* P$，添加$\left(c^*, U_1, U_2, U_3, \mathrm{ID}_A^*, \sum_{i=1}^{n} \mathrm{ID}_{B_i}^*, G_{\mathrm{ID}}, H^*\right)$到$L_3$；计算$S^* = P(t + H^*)$，$V_1^* = r_A^{-1}$，$V_2^* = S^* h_A$，$V^* = V_1^* V_2^*$；返回$\sigma^* = (c^*, \phi \leftarrow (U_1^*, U_2, U_3, V^*))$。

阶段2 与定理1的阶段2相同，另外A_2不询问$\mathrm{ID}_{B_i}^*$的$D_{B_i}^*$和$P_{B_i}^*$替换。

猜测 C输出$Q_{B_i}^* = tP_{B_i}^* = abP$作为CDH问题的实例解答。 证毕

定理3 假设伪造者F在EUF-CMA中能够伪造HGSSBHC的密文，且获胜概率不可忽略，那么C就能求解CDH问题。

证明 C获得CDH问题的随机实例$(P, aP, bP) \in G_1$时，需计算出$abP \in G_1$作为实例解答。

系统建立 C运行系统建立算法，同时建立4张空列表L_1, L_2, L_3, L_k，用来储存对应预言机的询问和应答。

训练 F适应性地询问。

H_1, H_2, H_3询问：和定理1的H_1, H_2, H_3询问一样。

公钥询问：收到身份ID_{B_i}的公钥询问时，若$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$，$C$设置$P_{B_i} = aP$，返回公钥$P_{B_i}$；否则，选择随机数$x_{B_i} \in \boldsymbol{Z}_q^*$，计算$P_{B_i} = x_{B_i} P$，返回公钥$P_{B_i}$，添加$(\mathrm{ID}_{B_i}, -, x_{B_i}, P_{B_i})$到$L_k$。

公钥替换询问：F用随机数P_{B_i}'替换P_{B_i}。如果$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$，那么$C$退出游戏；否则，$C$用$(\mathrm{ID}_{B_i}, D_{B_i}, -, P_{B_i}')$更新$L_k$。

私钥询问：若是ID_{B_i}的私钥询问，C检查是否$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$成立。若成立，$C$退出游戏；反之，$C$从$L_k$中检索到$(\mathrm{ID}_{B_i}, D_{B_i}, x_{B_i}, P_{B_i})$，返回私钥$S_{B_i} \leftarrow (x_{B_i}, D_{B_i})$。

签密询问：收到$\mathrm{ID}_A, \mathrm{ID}_{B_i}$下$m$的签密询问时，$C$按如下方式生成密文：

(1) $\mathrm{ID}_A \neq \mathrm{ID}_\alpha$($\alpha$为目标身份)，$C$运行密钥提取算法，计算$\mathrm{ID}_A$的私钥$S_A$，用$\mathrm{Sig}\left(\mathrm{pa}, m, S_A, G_{\mathrm{ID}}, \mathrm{ID}_A, \sum_{i=1}^{n} \mathrm{ID}_{B_i}, P_A, \sum_{i=1}^{n} P_{B_i}\right)$作为应答。

(2) $\mathrm{ID}_A = \mathrm{ID}_\alpha$，$\mathrm{ID}_{B_i} \in \{\mathrm{ID}_{B_1}, \mathrm{ID}_{B_2}, \cdots, \mathrm{ID}_{B_n}\}$，$C$选择随机数$t, H \in \boldsymbol{Z}_q^*$，并计算$U_1 = tP$，$U_2 = tH_1(G_{\mathrm{ID}})$，$U_3 = tP_2$，$T = U_1 \sum_{i=1}^{n} D_{B_i}$，运行$H_2$得到$K = H_2\left(U_1, U_2, U_3, T, U_1 \sum_{i=1}^{n} x_{B_i}, \sum_{i=1}^{n} \mathrm{ID}_{B_i}, G_{\mathrm{ID}}\right)$，计算$c = \mathrm{DEM.Enc}(K, m)$，并将$\left(c, U_1, U_2, U_3, \mathrm{ID}_A, \sum_{i=1}^{n} \mathrm{ID}_{B_i}, G_{\mathrm{ID}}\right)$添加到$L_3$，若发生碰撞，$C$输出失败并停止，否则，$C$计算$S = t + H$，$V_1 = r_A^{-1} P$，$V_2 = Sh_A$，$V = V_1 V_2$，并将密文$(c, \phi \leftarrow (U_1, U_2, U_3, V))$返回给$F$。

伪造 结束训练后，输入m，输出ID_A，ID_{B_i}下的密文$\sigma = (c, \phi \leftarrow (U_1, U_2, U_3, V))$，在训练中，不允许询问$\mathrm{ID}_A$的$S_A$和替换$\mathrm{ID}_A$的$P_A$。假设$\mathrm{ID}_A \neq \mathrm{ID}_\alpha$，则$C$退出游戏；否则，运用分叉引理[16]，$F$给出一个密文$\sigma^*$，$C$选择不同的$H, H^*$和相同的随机数与$F$进行交互。已知$P_1 V = P^2 H_1(\mathrm{ID}_A) \cdot H_1(G_{\mathrm{ID}})(U_1 + PH)$和$P_1 V^* = P^2 H_1(\mathrm{ID}_A) H_1(G_{\mathrm{ID}}) \cdot (U_1 + PH^*)$均可通过验证等式，其中$P_1 = eP$，$H_1(\mathrm{ID}_A) = bP$，$H_1(G_{\mathrm{ID}}) = cP$。$C$能够计算出$\dfrac{V - V^*}{H - H^*} = e^{-1} bcP^4$，最终输出$T = U_1 \sum_{i=1}^{n} D_{B_i} = tPs_2^{-1} H_1(G_{\mathrm{ID}}) \sum_{i=1}^{n} H_1(\mathrm{ID}_{B_i})) = aPe^{-1} bcP^4 = abce^{-1} \cdot P^5$作为CDH问题的实例解答。 证毕

4　效率分析

4.1　理论分析比较

在理论分析中，对本文方案与文献[13]，文献[15]所提方案的计算效率和通信成本进行比较。

首先，与文献[13]，文献[15]的计算效率作比较，其中，P_M和P_H分别表示点乘运算和哈希运算，n表示接收者的个数。由表1可知，在签密阶段和解签密阶段，本文的哈希函数计算量和文献[13]，文献[15]相比，略逊一点。但本文的点乘运算量和接收者个数n呈线性增长关系，随着n的增大，本文的计算效率就会显著优于文献[13]，文献[15]。其次，由表1可知，本文方案比文献[13]的通信成本低，但比文献[15]略高一点。其中，$|G_1|$表示群G_1中的元素，$|\boldsymbol{Z}_q^*|$表示群$\boldsymbol{Z}_q^*$中的元素。

4.2　数值实验分析

利用双线性对包(Pairing-Based Cryptography library, PBC)，使用C语言编程对IBC到CLC的异构混合群组签密方案进行数值实验分析。群G_1, G_2的长度为1024 bit，利用的参数类型为a型椭圆曲线$y^2 = x^3 + x \bmod q$，用户身份和消息均为160 bit。

本文方案的签密和解签密时间由接收者人数决定。在数值实验分析中，接收者人数n分别取：100, 200, 300, 400, 500, 600, 700, 800, 900, 1000。签密和解签密时间如表2所示。

同时，为了比较本文方案和文献[15]在签密和解签密的计算效率，对文献[15]做了同样的数值实验分析，数值实验结果取40次的平均值，如图1和图2所示。

由图1，图2可以看出，在签密和解签密阶段，本文方案明显比文献[15]所提方案效率更高，而且随着接收者人数的增加，本文方案的效率更优。所以本文方案更适合应用于多接收者的群组签密中，具有更高的可行性。

5　结束语

现有的群组签密方案大多不具有可加密任意长消息的能力，且签密密文的发送者和接收者在同一个密码体制中。但是在大数据的现实环境中，用户是需要根据自己对密钥生成中心的信任度来选择生成密钥的方式。例如，在车载自组织网中，当信任中心及路边单元与车辆单元不属于同一个密码体制时：信任中心及路边单元属于IBC密码体制，车载单元属于CLC密码体制，此时就需要提出IBC密码体制与CLC密码体制间的异构密码方案来保证各单元间的安全通信。本文方案安全高效，可加密任意长消息，以及在不改变群组公钥和其他成员私钥的前提下用户可以动态地加入该群组，更适合应用于大数据和云计算。

表 1　效率分析

方案	签密阶段运算量	解签密阶段运算量	签密密文长度
文献[13]	$(2n^2+7n+3)P_M+3P_H$	$(n^2+n+3)P_M+3P_H$	$2\|G_1\|+3\|\boldsymbol{Z}_q^*\|$
文献[15]	$(2n^2+3n+2)P_M+3P_H$	$(n^2+n+2)P_M+3P_H$	$\|G_1\|+3\|\boldsymbol{Z}_q^*\|$
本文	$(2n+7)P_M+4P_H$	$(2n+5)P_M+3P_H$	$\|G_1\|+4\|\boldsymbol{Z}_q^*\|$

表 2　本文方案计算时间(s)

n	100	200	300	400	500	600	700	800	900	1000
签密时间	1.1861	2.3375	3.6016	4.7899	5.9708	7.1283	8.1671	9.5163	10.7285	11.8963
解签密时间	1.4792	1.5774	1.7442	1.8645	1.8991	1.9001	2.1469	2.3773	2.4658	2.5549

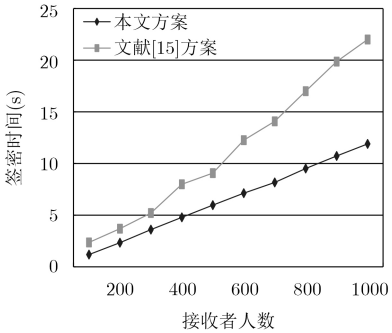

图 1 签密阶段计算效率

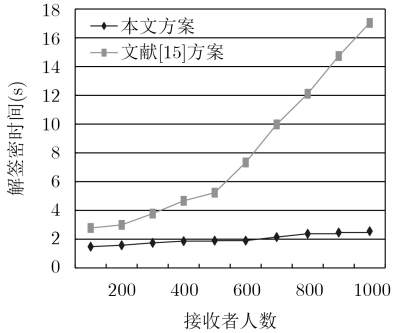

图 2 解签密阶段计算效率

参 考 文 献

[1] ZHENG Yuliang. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) +cost(encryption)[C]. Proceedings of the Cryptology-CRYPTO 1997, California, USA, 1997: 165–179. doi: 10.1007/BFb0052234.

[2] BAEK J, STEINFELD R, and ZHENG Yuliang. Formal proofs for the security of signcryption[C]. Proceedings of the Cryptology-PKC2002, Paris, France, 2002: 81–98. doi: 10.1007/3-540-45664-3_6.

[3] 张宇, 陈晶, 杜瑞颖, 等. 适于车载网安全通信的高效签密方案[J]. 电子学报, 2015, 43(3): 512–517. doi: 10.3969/j.issn.0372-2112.2015.03.015.

ZHANG Yu, CHEN Jing, DU Ruiying, *et al*. An efficient signcryption scheme for secure communication of VANET[J]. *Acta Electronica Sinica*, 2015, 43(3): 512–517. doi: 10.3969/j.issn.0372-2112.2015.03.015.

[4] 周才学. 几个签密方案的密码学分析与改进[J]. 计算机工程与科学, 2016, 38(11): 2246–2253. doi: 10.3969/j.issn.1007-130X.2016.11.014.

ZHOU Caixue. Cryptanalysis and improvement of some signcryption schemes[J]. *Computer Engineering and Science*, 2016, 38(11): 2246–2253. doi: 10.3969/j.issn.1007-130X.2016.11.014.

[5] 王彩芬, 李亚红, 张玉磊, 等. 标准模型下高效的异构签密方案[J]. 电子与信息学报, 2017, 39(4): 881–886. doi: 10.11999/JEIT160662.

WANG Caifen, LI Yahong, ZHANG Yulei, *et al*. Efficient heterogeneous signcryption scheme under standard model[J]. *Journal of Electronics & Information Technology*, 2017, 39(4): 881–886. doi: 10.11999/JEIT160662.

[6] 牛淑芬, 牛灵, 王彩芬, 等. 一种可证安全的异构聚合签密方案[J]. 电子与信息学报, 2017, 39(5): 1213–1218. doi: 10.11999/JEIT160829.

NIU Shufen, NIU Ling, WANG Caifen, *et al*. A provable aggregate signcryption for heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2017, 39(5): 1213–1218. doi: 10.11999/JEIT160829.

[7] 薛鹏. 混合加密的密钥封装算法研究与设计[D]. [博士论文], 西安电子科技大学, 2014.

XUE Peng. Research and design of hybrid encryption key encapsulation algorithm[D]. [Ph.D. dissertation], Xi'an University, 2014.

[8] YU Huifang and YANG Bo. Provably secure certificateless hybrid signcryption[J]. *Chinese Journal of Computers*, 2015, 38(4): 804–813. doi: 10.3724/SP.J.1016.2015.00804.

[9] 卢万谊, 韩益亮, 杨晓元. 前向安全的可公开验证无证书混合签密方案[C]. 中国计算机学会服务计算学术会议, 西安, 中国, 2012: 1–6.

LU Wanyi, HAN Yiliang, and YANG Xiaoyuan. Forward secure publicly verifiable hybrid certificateless signcryption scheme[C]. Academic Conference on Service Computing of China Computer Society, Xi'an, China, 2012: 1–6.

[10] 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.

[11] 徐鹏, 薛伟. 可公开验证的无证书混合签密方案[J]. 计算机应用与软件, 2017(11): 278–283. doi: 10.3969/j.issn.1000-386x.2017.11.051.

XU Peng and XUE Wei. A publicly verifiable certificateless hybrid signcryption scheme[J]. *Computer Application and Software*, 2017(11): 278–283. doi: 10.3969/j.issn.1000-386x.2017.11.051.

[12] 张波, 徐秋亮. 基于身份的面向群组签密方案[C]. 中国计算机网络与信息安全学术会议, 天津, 中国, 2009: 23–28.

ZHANG Bo and XU Qiuliang. Identity based group oriented signcryption scheme[C]. China Academic Conference on Computer Network and Information Security, Tianjin, China, 2009: 23–28.

[13] 陈尚弟, 卞广旭. 一种新的基于身份的群体签密方案[J]. 中国民航大学学报, 2013, 31(1): 93–96. doi: 10.3969/j.issn.1674-5590.2013.01.022.

CHEN Shangdi and BIAN Guangxu. A new identity based group signcryption scheme[J]. *Journal of Civil Aviation University of China*, 2013, 31(1): 93–96. doi: 10.3969/j.issn.1674-5590.2013.01.022.

[14] 冯君, 汪学明. 一种高安全的门限群签密方案[J]. 计算机应用研究, 2013, 30(2): 503–506. doi: 10.3969/j.issn.1001-3695.2013.02.051.

FENG Jun and WANG Xueming. A high security threshold group signcryption scheme[J]. *Computer Application Research*, 2013, 30(2): 503–506. doi: 10.3969/j.issn.1001-3695.2013.02.051.

[15] PENG Changgen, LI Xiang, and LUO Wenjun. A generalized group-oriented threshold signcryption schemes[J]. *Acta Electronica Sinica*, 2007, 35(1): 64–67.

[16] 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.

牛淑芬：女，1976年生，博士，副教授，研究方向为密码学.

杨喜艳：女，1992年生，硕士生，研究方向为密码学.

王彩芬：女，1963年生，博士，教授，研究方向为密码学.

田 苗：女，1993年生，硕士生，研究方向为密码学.

杜小妮：女，1972年生，博士，教授，研究方向为信息安全.