新的具有隐私保护功能的异构聚合签密方案

张玉磊 刘祥震* 郎晓丽 陈文娟 王彩芬

(西北师范大学计算机科学与工程学院 兰州 730070)

摘 要：异构聚合签密方案不仅可以保证异构密码系统之间数据的机密性和不可伪造性，而且可以提供多个密文批量验证。该文分析了一个具有隐私保护功能的异构聚合签密方案的安全性，指出该方案不能抵挡恶意密钥生成中心(KGC)攻击，恶意KGC可以伪造有效的单密文和聚合密文。为了提高原方案的安全性，该文提出一种新的具有隐私保护功能的异构聚合签密方案。该方案克服了原方案存在的安全性问题，实现了无证书密码环境到身份密码环境之间的数据安全传输，在随机预言机模型下证明新方案的安全性。效率分析表明新方案与原方案效率相当。

关键词：异构签密；聚合签密；恶意密钥生成中心；不可伪造性

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2018)12-3007-06

DOI: 10.11999/JEIT180249

New Privacy Preserving Aggregate Signcryption for Heterogeneous Systems

ZHANG Yulei LIU Xiangzhen LANG Xiaoli CHEN Wenjuan WANG Caifen

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

Abstract: The privacy preserving aggregate signcryption for heterogeneous systems can ensure the confidentiality and unforgeability of the data between heterogeneous cryptosystems, it also can provide multi-ciphertext batch verification. This paper analyzes the security of a scheme with privacy-preserving aggregate signcryption heterogeneous, and points out that the scheme can not resist the attack of malicious Key Generating Center (KGC), it can forge a valid ciphertext. In order to improve the security of the original scheme, a new heterogeneous aggregation signature scheme with privacy protection function is proposed.The new scheme overcomes the security problems existing in the original scheme and ensures the data transmission between the certificateless public key cryptography and the identity-based public key cryptographic, and the security of the new scheme is proved under the random oracle model. Efficiency analysis shows that the new program is equivalent to the original one.

Key words: Heterogeneous signcryption; Aggregation signcryption; Malicious Key Generating Center (KGC); Unforgeability

1 引言

在数据传输过程中，不仅要保护数据的机密性，而且还要保证数据的不可伪造性。1997年，Zheng[1]提出签密的概念。签密可以同时完成“签名和加密”功能，该技术与传统的先加密后签名或者先签名后加密相比具有通信成本低、安全水平高等优点，在很多实际应用场景中受到青睐[2, 3]。2009年Selvi等人[4]结合了聚合签名和签密的优势，提出了聚合签密概念。

聚合签密可以把多个签密密文聚合为单个签密密文，验证者仅需验证聚合后的密文，就可以实现对多个消息的认证。聚合签密适合于多对一的用户环境，在无线传感器[5]等领域得到了广泛的使用。随后，Han等人[6]提出了基于身份的聚合签密的方案，Eslami等人[7]提出了基于无证书的聚合签密方案。在实际应用环境中，跨平台通信越来越普及，不同系统使用不同的密码系统，为了保证异构密码系统之间数据的机密性和完整性。2010年，Sun等人[8]首次提出了异构签密方案。随后，Huang等人[9]提出了一个从传统公钥密码体制(Traditional Pub-

收稿日期：2018-03-19；改回日期：2018-08-13；网络出版：2018-08-31
*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)

lic Key Cryptography, TPKC)到身份公钥密码体制(IDentity-based Public Key Cryptographic, IDPKC) TPKI→IDPKC异构签密方案，Li等人[10]提出了IDPKC→TPKI签密方案。自此，异构签密成为当前密码学研究的一个热点[11–15]。

2017年，Niu等人[16]提出了一个具有隐私保护功能的异构聚合签密方案，经过分析，发现该方案不满足签密密文的不可伪造性。恶意密钥生成中心(Key Generating Center, KGC)可以伪造签密密文。为了解决Niu方案[16]中存在的密文可伪造攻击，本文先提出了一种新的具有系统隐私功能的保护异构聚合签密方案，随后证明了本文方案的安全性。最后对比了本文方案与Niu方案。

2 Niu方案及安全性分析

限于篇幅，略去对Niu方案的描述，具体算法见文献[16]。

Niu方案是从无证书公钥密码体制到身份公钥密码体制(CLPKC→IDPKC)的异构签密方案。对于机密性，主要考虑IDPKC密码环境；对于不可伪造性，则是CLPKC密码环境。在CLPKC中，主要存在两类敌手A_1和A_2。A_1为不诚实的用户，通过对用户原有公钥的替换实现公钥替换攻击；A_2为恶意的KGC，可以获取系统的主密钥和用户的部分私钥，实现KGC攻击。通过分析，发现Niu方案不满足密文的不可伪造性，即KGC可以伪造单个签密密文和聚合签密密文。

2.1 单个签密密文伪造

KGC通过以下过程实现单个密文的伪造：

(1)KGC在系统初始化时，选择$\overline{w}\in Z_q^*$，计算$Q=\overline{w}P$作为G_1的一个生成元。随机选择$s\in Z_q^*$为系统的主密钥，计算$P_{\rm pu}=sP$为系统公开密钥。

(2) KGC随机选择$r_j'\in Z_q^*$，计算$r_j'Q{=}R_j'\overline{w}$和$h_j'=H_4(C_j,R'_j,P_{\rm sj},{\rm ID}_{\rm sj})$，可计算出$X_{\rm sj}\overline{w}P=P_{\rm sj}\overline{w}$。

(3)伪造签密密文：$S_j{=}D_{\rm sj}+h_j'r_j'\overline{w}P+P_{\rm sj}\overline{w}$，则伪造的密文为$\sigma_j=(R_j,C_j,S_j,\Gamma_j)$。

(4)验证伪造密文的正确性：由于

$$\begin{aligned}e(S_j',P)&=e(D_{\rm sj}{+}h_j'r_j'\overline{w}P+P_{\rm sj}\overline{w},P)\\&=e(D_{\rm sj},P)e(h_j'r_j'\overline{w}P,P)e(P_{\rm sj}\overline{w},P)\\&=e(s\cdot Q_{\rm sj},P)e(h_j'r_j'P,Q)e(P_{\rm sj},Q)\\&=e(Q_{\rm sj},P_{\rm pu})e(h_j'R_j'+P_{\rm sj},Q)\end{aligned}$$

因此，KGC可以成功伪造单个签密密文。

2.2 聚合签密密文伪造

KGC通过以下过程实现聚合密文的伪造：

(1)按照2.1节步骤伪造单个密文。

(2)$S{=}\sum_{j=1}^{m}S_j{=}\sum_{j=1}^{m}(D_{\rm sj}{+}X_{\rm sj}Q+h_j'r_j'Q)$，伪造聚合签密密文为$\sigma_j=(\{R_j,C_j,\Gamma_j\}_{j=1}^m,S)$。

(3)验证伪造密文的正确性：由于

$$\begin{aligned}e(S,P)&=e\left(\sum_{j=1}^{m}(D_{\rm sj}+X_{\rm sj}Q+h_j'r_j'Q),P\right)\\&=e\left(\sum_{j=1}^{m}D_{\rm sj},P\right)e\left(\sum_{j=1}^{m}X_{\rm sj}Q,P\right)\\&\quad\cdot e\left(\sum_{j=1}^{m}h_j'r_j'Q,P\right)\\&=e\left(\sum_{j=1}^{m}Q_{\rm sj}\cdot s,P\right)e\left(\sum_{j=1}^{m}X_{\rm sj}Q,P\right)\\&\quad\cdot e\left(\sum_{j=1}^{m}h_j'R_j',Q\right)\\&=e\left(\sum_{j=1}^{m}Q_{\rm sj},P_{\rm pu}\right)e\left(\sum_{j=1}^{m}P_{\rm sj},Q\right)\\&\quad\cdot e\left(\sum_{j=1}^{m}h_j'r_j',Q\right)\\&=e\left(\sum_{j=1}^{m}Q_{\rm sj},P_{\rm pu}\right)e\left(\sum_{j=1}^{m}(P_{\rm sj}+h_j'r_j'),Q\right)\end{aligned}$$

因此，KGC可以成功伪造聚合签密密文。

3 改进的异构签密方案

Niu方案的主要问题在于签密生成环节泄漏了签密者的秘密值信息，即KGC可以容易地得到$X_{\rm sj}Q$和$r_j'Q$。

(1) **系统建立Setup**：输入安全参数k, KGC选择两个阶为q的循环群G_1和G_2, G_1为加法群，G_2为循环乘群。P为G_1的生成元。$e:G_1\times G_1\to G_2$为一个双线性映射。KGC随机地选择$s\in Z_q^*$作为系统的主密钥，保留s。计算系统公钥为$P_{\rm pu}=sP$。KGC选择4个哈希函数$H_1:\{0,1\}^*\to G_1$, $H_2:G_2\to\{0,1\}^{\rm lm}$, $H_3:\{0,1\}^*\to Z_q^*$, $H_4:\{0,1\}^{\rm lm}\to G_1$。系统参数${\rm params}=\{q,G_1,G_2,e,P,P_{\rm pu},H_1,H_2,H_3,H_4\}$。

(2) **公/私钥生成CLPKC-KG**: CLPKC系统中发送者$S_i(i\in\{1,2,\cdots,n\})$的身份为$M_j$。

(3) **密钥提取IDPKC-KG**: IDPKC系统中接收者的身份为${\rm ID}_{\rm rj}(j\in\{1,2,\cdots,n\})$。CLPKC-KG和IDPKC-KG里面包含的算法设置同2.1节。

(4) **签密Signcrypt**：输入消息M_i和接收者的身份列表$L=\{{\rm ID}_{\rm ri}\}_{i=1}^n$，发送者$S_j$执行如下步骤：

(a)随机地选择$r_i\in Z_q^*$，计算$R_i=r_iP$, $\omega_i=e(P_{\rm pu},P_i)^{r_i}$和$C_i{=}H_2(\omega_i)\oplus M_i$。

(b)对$j=1,2,\cdots,m$，计算$x_{\mathrm{rj}}=H_3(\mathrm{ID}_{\mathrm{rj}}), f_j(x)=\prod_{1\le \mathrm{j}\ne \mathrm{i}\le \mathrm{m}} \frac{x-x_i}{x_j-x_i}=a_{j,1}+a_{j,2}x+a_{j,m}x^{m-1}$，$y_{\mathrm{ji}}=r_i(P_i+Q_{\mathrm{rj}})$，其中$a_{j,1}, a_{j,2}, \cdots, a_{j,m}\in Z_q^*$。

(c)对于$j=1,2,\cdots,m$，计算$T_{ji}=\sum_{k=1}^{n} a_{k,j}\, y_{k,i}$，令$\Gamma=(T_{1i}, T_{2i}, \cdots, T_{mi})$。

(d)计算$h_i=H_3(C_i, R_i, P_{\mathrm{si}}, \mathrm{ID}_{\mathrm{si}})$和$S_i=D_{\mathrm{si}}+(X_{\mathrm{si}}+h_i r_i)H_4(P_{\mathrm{pu}})$。

(e)发送者S_i把密文$\sigma_i=(R_i, C_i, S_i, \Gamma_i)$给接收者。

(5) **单个解签密Individual De-signcrypt**：收到密文$\sigma_i=(R_i, C_i, S_i, \Gamma_i)\}_{i=1}^{m}$，接收者利用自己的身份$\mathrm{ID}_{\mathrm{rj}}(j\in\{1,2,\cdots,n\})$解密$\sigma_i$步骤如下：

(a)计算$Q_{\mathrm{si}}=H_1(\mathrm{ID}_{\mathrm{si}}), h_i=H_3(C_i, R_i, P_i, \mathrm{ID}_i)$。

(b)检查$e(S_i, P)=e(Q_{\mathrm{si}}, P_{\mathrm{pu}})e(P_{\mathrm{si}}+h_i\cdot R_i, H_4(Q))$是否成立。如果成立，密文有效；否则，拒绝该密文。

(c)计算$x_j=H_3(\mathrm{ID}_{\mathrm{rj}})$和$y'_{\mathrm{ij}}=T_{1i}+x_j T_{2i}+\cdots+x_j^{m-1}T_{mi}(i=1,2,\cdots,n)$。

(d)计算$\omega'_i=e(P_{\mathrm{pu}}, y'_{\mathrm{ij}})e(R_i, D_{\mathrm{rj}})^{-1}$。

(e)恢复消息M_i, $M_i=H_2(\omega_i)\oplus C_i(i=1,2,\cdots,m)$。

(6) **聚合签密Aggregate**：由聚合者执行产生m个用户对M个消息的聚合签密过程如下：

(a)输入$\{\mathrm{ID}_{\mathrm{si}}\}_{i=1}^{m}$签密密文$\sigma_i=(R_i, C_i, S_i, \Gamma_i)_{i=1}^{m}$。

(b)计算$S=\sum_{i=1}^{m} S_i$。

(c)输出聚合密文为$\sigma=(\{R_i, C_i, \Gamma_i\}_{i=1}^{m}, S)$。

(7)**聚合验证Aggregate de-signcrypt**：验证聚合签密是否有效，步骤如下：

(a)计算$Q_{\mathrm{si}}=H_1(\mathrm{ID}_{\mathrm{si}}), h_i=H_3(C_i, R_i, P_{\mathrm{si}}, \mathrm{ID}_{\mathrm{si}})$。

(b)检查等式

$$e(S,P)=e\left(\sum_{i=1}^{m} Q_{\mathrm{si}}, P_{\mathrm{pu}}\right)e\left(\sum_{i=1}^{m}(P_{\mathrm{si}}+h_i\cdot R_i), H_4(Q)\right)$$

是否成立。成立则接受；否则，退出算法。

4　新方案的安全性分析

新方案的机密性证明过程与原方案一致，以下对不可伪造性进行分析。

4.1 单个签密密文不可伪造性

定理 1　假定CDH问题困难，针对敌手A_1，本文异构签密方案在随机预言模型下自适应选择消息攻击下不可伪造。

以下需要引理1和引理2来证明定理1。

引理 1　在随机预言模型下，假设一个敌手A_1在t时间内能以不可忽略的优势ε攻破本文方案，则存在算法B，能以$\varepsilon'\ge(\varepsilon-q^s/2^k)(1-1/q^{\mathrm{pk}})^{q_{\mathrm{Pk}}}$优势解决 CDH 问题，其中，$H_1$-Query, H_2-Query, H_3-Query, H_4-Query, Partial-Private-Key-query, Secret-Value-query, Public-key-replave-query, Signcryption-query的访问次数分别为q_{H1}, q_{H2}, q_{H3}, q_{H4}, q_{pk}, q_{Sk}, q_{kr}, q_s。

证明　A_1为攻击者，B为CDH问题的挑战者。B给定 (P, aP, bP), B的目标是使用A_1解决 CDH问题，即计算abP。

(1) **系统建立Setup**：挑战者B设$P_{\mathrm{pu}}=aP$。返回系统参数params给A_1, B随机选择挑战的伪身份$\mathrm{ID}_{\mathrm{ai}}^*$, A_1执行以下询问：

(2)***H*$_1$-query:** B维持列表L_1=$(\mathrm{ID}_{\mathrm{si}}, Q_{\mathrm{si}}, \alpha_i, c_i)$，初始为空。当$A_1$对$H_1$进行询问时，$B$首先检查$L_1$列表，若列表$L_1$中存在$(\mathrm{ID}_{\mathrm{si}}, Q_{\mathrm{si}}, \alpha_i)$，$B$就返回相应的$Q_{\mathrm{si}}$，否则：$B$随机选择$\alpha_i\in Z_q^*$和$c_i\in\{0,1\}$(其中，$c_i=0$的概率为$\zeta=1/q_{H_1}$。$c_i=1$的概率为$1-\zeta$)。当$c_i$=0时，计算$Q_{\mathrm{si}}=\alpha_i P$。当$c_i$= 1时，计算$Q_{\mathrm{si}}=\alpha_i bP$。返回$Q_{\mathrm{si}}$给$A_1$，并增加$(\mathrm{ID}_{\mathrm{si}}, Q_{\mathrm{si}}, \alpha_i, c_i)$到$L_1$列表。

(3) ***H*$_2$-query:** B维持L_2= $(\omega_i,\omega_{2i}, H_2(\omega_i))$，当$B$收到对$H_2$的询问时，$B$随机选择$\omega_{2i}\in Z_q^*$，令$H_2(\omega_i)=\omega_{2i}$，发送给$A_1$。

(4) ***H*$_3$-query:** B维持$L_3=\{C_i, R_i, P_{\mathrm{si}}, \mathrm{ID}_{\mathrm{si}}, h_i, \gamma_i\}$，初始为空。当$A_1$询问$L_3$列表的元组时，$B$首先检查列表，若列表中有相应元组，则发送对应的$h_i$；否则$B$随机选择$\gamma_i\in Z_q^*$，令$h_i=\gamma_i$，增加$(C_i, R_i P_{\mathrm{si}}, \mathrm{ID}_{\mathrm{si}}, h_i, \gamma_i)$到列表$L_3$中，并返回$h_i$。

(5) ***H*$_4$-query:** A_1对$H_4(P_{\mathrm{pu}})$进行询问时，B随机选择$t\in Z_q^*$，令$H_4(P_{\mathrm{pu}})=tP$。

(6) **部分私钥询问Partial-Private-Key-query:** B保持列表$E=\{\mathrm{ID}_{\mathrm{si}}, D_{\mathrm{si}}, Q_{\mathrm{si}}\}$，初始为空。$A_1$询问$\mathrm{ID}_{\mathrm{si}}$的部分私钥时，若$E$中已有相应记录，则直接返回$D_{\mathrm{si}}$。否则，$A_1$执行$H_1$询问，返回$(\mathrm{ID}_{\mathrm{si}}, Q_{\mathrm{si}}, \alpha_i, c_i)$。若$c_i$= 1，则$B$终止；否则，计算$D_{\mathrm{si}}=\alpha_i P_{\mathrm{pu}}=\alpha_i aP$，返回$D_{\mathrm{si}}$给$A_1$，并将$(\mathrm{ID}_{\mathrm{si}}, D_{\mathrm{si}}, Q_{\mathrm{si}})$添加到表$E$。

(7) **公钥询问Public-key-query:** B保持列表$F=(\mathrm{ID}_{\mathrm{si}}, X_i, P_{\mathrm{si}})$，初始为空。当$A_1$询问$\mathrm{ID}_{\mathrm{si}}$的公钥时，若$F$包含询问内容，返回$P_{\mathrm{si}}$给$A_1$。否则，选择任意$X_i\in Z_q^*$，$P_{\mathrm{si}}=X_i P$，返回$P_{\mathrm{si}}$给$A_1$将$(\mathrm{ID}_{\mathrm{si}}, X_i, P_{\mathrm{si}})$加入到$F$表中。

(8) **秘密值询问Secret-Value-query**：当A_1询问$\mathrm{ID}_{\mathrm{si}}$的秘密值时，如果$c_i$= 1, B终止。否则，B查F表，若F表中有对应的$\mathrm{ID}_{\mathrm{si}}$，则返回相应秘密值；否则$B$随机选择$X_i\in Z_q^*$，作为相应的秘密值，更新列表并返回$X_i$。

(9) **公钥替换询问Public-key-replace-query:**

A_1对$\mathrm{ID_{si}}$公钥替代询问时，A_1随机选择一个公钥P'_{si}代替原公钥P_{si}。设置$P_{\mathrm{si}}=P'_{\mathrm{si}}$, $X_i=\perp$。

(10) **签密询问Signcryption-query**：当A_1对$(M_i,\mathrm{ID_{si}},L)$里的$L=\{\mathrm{ID_{R1}},\mathrm{ID_{R2}},\cdots,\mathrm{ID_{R}}n\}$进行签密询问时，若$\mathrm{ID_{si}}\neq\mathrm{ID^*_{ai}}$，则运行签密算法得到密文$\sigma$。若$\mathrm{ID_{si}}=\mathrm{ID^*_{ai}}$, B模拟算法生成一个签密。

(a)B随机选择$r_i\in Z_q^*$, $h_i\in Z_q^*$。

(b)计算$R_i=r_iP-h_i^{-1}P_{\mathrm{si}}$和$S_i=D_{\mathrm{si}}+h_ir_iH_4(Q)$, B把$\sigma_i=(R_i,C_i,S_i)$给A_1。

$$\begin{aligned}e(S_i,P)&=e(D_{\mathrm{si}}+h_ir_iH_4(Q),P)\\&=e(D_{\mathrm{si}},P)e(h_ir_iH_4(Q),P)\\&=e(\alpha_iaP,P)e(h_ir_iH_4(Q),P)\\&=e(\alpha_iP,P_{\mathrm{pu}})e(h_ir_iP,H_4(Q))\\&=e(Q_{\mathrm{si}},P_{\mathrm{pu}})e(h_i(R_i+h_i^{-1}P_{\mathrm{si}}),H_4(Q))\\&=e(Q_{\mathrm{si}},P_{\mathrm{pu}})e(h_iR_i+P_{\mathrm{si}},H_4(Q))\end{aligned}$$

(11) **输出Output**：最后，A_1输出一个元组$(M_i^*,\sigma_i^*,\mathrm{ID_{si}^*},P_{\mathrm{si}}^*)$。如果$\mathrm{ID_{si}^*}\neq\mathrm{ID_{ai}^*}$，$B$终止；否则，通过使用分叉引理，在用相同的随机带重放A_1之后的两个不同的h'_i, B在多项式时间内获得两个有效签名$\sigma_i^*=(M_i^*,h_i^*,\mathrm{ID_{si}^*},R_i^*,S_i^*)$和$\sigma^{*\prime}i=(M^{*\prime}i,h^{*\prime}i,\mathrm{ID^{*\prime}_{si}}i,R^{*\prime}i,S^{*\prime}i)$。

$$\begin{aligned}S_i^*&=D_{\mathrm{si}}^*+(X_{\mathrm{si}}^*+h_i^*r_i^*)H_4(Q)\\&=D_{\mathrm{si}}^*+(X_i^*+h_i^*r_i^*)abP\end{aligned}\tag{1}$$

$$\begin{aligned}S_i^{*\prime}&=D_{\mathrm{si}}^*+(X_{\mathrm{si}}^*+h_i^{*\prime}r_i^*)H_4(Q)\\&=D_{\mathrm{si}}^*+(X_i^*+h_i^{*\prime}r_i^*)abP\end{aligned}\tag{2}$$

根据式(1)和式(2), B通过计算输出abP作为CDH实例的解决方案$abP=(S_i^*-S_i^{*\prime})/(h_i^*r_i^*-h'^*_ir_i^*)$。

引理 2 在随机预言模型下，假设一个敌手A_2在t时间内能以不可忽略的优势ε攻破本文方案，则存在算法B，能以$\varepsilon'\geq(\varepsilon-q^s/2^k)(1-1/(q^{\mathrm{pk}}+m))^{q_{\mathrm{P}k}+m-1}$优势解决 CDH 问题的一个实例。

证明 A_2为攻击者，B为CDH问题的挑战者。B给定(P,aP,bP), B 的目标是使用A_2解决 CDH问题，即计算abP。

(1) **系统建立Setup**: B运行Setup算法，随机选择$s\in Z_q^*$作为系统的主密钥，计算$P_{\mathrm{pu}}=sP$。B随机选取$\mathrm{ID_{ai}^*}$作为挑战身份，B将params和s一起传递给A_2。A_2执行以下询问：

(2) $\boldsymbol{H_1}$**-query**: B维持列表$L_1=(\mathrm{ID_{si}},Q_i,)$，初始为空。当$A_2$对$\mathrm{ID_{si}}$进行询问时，$B$首先检测$L_1$表，若$L_1$存在$(\mathrm{ID_{si}},Q_i)$, B就返回相应Q_i，否则：B随机选择$Q_i\in G_1$，更新列表，把Q_i发送给A_2。

(3) $\boldsymbol{H_2}$**-query**: B维持列表$L_2=(\omega_i,\beta_i,H_2(\omega_i))$, B收到对ω_i的H_2询问时：

(a)如果$H_2(\omega_i)$存在L_2列表中，就把$H_2(\omega_i)$返回给A_2。

(b)否则，随机选择$\beta_i\in Z_q^*$，计算$H_2(\omega_i)=\beta_iaP$，输出$H_2(\omega_i)$，添加$(\omega_i,\beta_i,H_2(\omega_i))$到列表$L_2$中。

(4) $\boldsymbol{H_3}$**-query**: B维持$L_3=\{C_i,R_i,P_{\mathrm{si}},\mathrm{ID_{si}},h_i,\gamma_i\}$，初始为空。当$A_2$询问$L_3$时，$B$首先检测$L_3$，若$L_3$存在，则返回$h_i$；否则$B$随机选择$\gamma_i\in Z_q^*$，令$h_i=\gamma_i$，增加元组到列表$L_3$中，并返回$h_i$给$A_2$。

(5) $\boldsymbol{H_4}$**-query**: A_2对$H_4(P_{\mathrm{pu}})$进行询问时，B令$H_4(P_{\mathrm{pu}})=aP$，并返回给A_2。

(6) **公钥询问Public-key-query**: B保持列表$F=(\mathrm{ID_{si}},X_i,P_{\mathrm{si}})$，初始为空。当$A_2$询问$\mathrm{ID_{si}}$公钥时，若$F$列表中包含$P_{\mathrm{si}}$，则返回$P_{\mathrm{si}}$给$A_2$。否则，随机选择$X_i\in Z_q^*$。若$c_i=0$，计算$P_{\mathrm{si}}=X_iP$。否则计算$P_{\mathrm{si}}=X_ibP$。返回$P_{\mathrm{si}}$给$A_2$同时更新元组$(\mathrm{ID_{si}},X_i,P_{\mathrm{si}})$到$F$ 表中。

(7) **签密询问Signcryption-query**：当A_2对$(M_i,\mathrm{ID_{si}},L)$这里的$L=\{\mathrm{ID_{R1}},\mathrm{ID_{R2}},\cdots,\mathrm{ID_{R}}n\}$签密询问时，首先$B$查表。若$c_i=0$, B随机选择$h_i\in Z_q^*$，计算$R_i=-h_i^{-1}P_{\mathrm{si}}$, $S_i=D_{\mathrm{si}}$。最后，B把$\sigma_i=(R_i,C_i,S_i,T_i)$给$A_2$。

$$\begin{aligned}&e(Q_{\mathrm{si}},P_{\mathrm{pu}})e(h_i\,R_i+P_{\mathrm{si}},H_4(Q))\\&=e(Q_{\mathrm{si}},P_{\mathrm{pu}})=e(Q_{\mathrm{si}},s\cdot P)=e(s\cdot Q_{\mathrm{si}},P)\\&=e(D_{\mathrm{si}},P)=e(S_i,P)\end{aligned}$$

(8) **输出Output**: A_2输出一个元组$(M_i^*,\sigma_i^*,\mathrm{ID_{si}^*},P_{\mathrm{si}}^*)$。如果$\mathrm{ID_{si}^*}\neq\mathrm{ID_{ai}^*}$, B终止；否则，利用分叉引理，在用同样的任意带重放A_2之后得到两个不一样h'_i, B在多项式时间内获得两个有用签名$\sigma_i^*=(M_i^*,h_i^*,\mathrm{ID_{si}^*},R_i^*,S_i^*)$和$\sigma^{*\prime}i=(M^{*\prime}i,h^{*\prime}i,\mathrm{ID^{*\prime}_{si}}i,R^{*\prime}i,S^{*\prime}i)$。

$$\begin{aligned}S_i^*&=D_{\mathrm{si}}^*+(X_{\mathrm{si}}^*+h_i^*r_i^*)H_4(Q)\\&=D_{\mathrm{si}}^*+(X_i^*+h_i^*r_i^*)abP\end{aligned}\tag{3}$$

$$\begin{aligned}S_i^{*\prime}&=D_{\mathrm{si}}^*+(X_{\mathrm{si}}^*+h^{*\prime}_ir_i^*)H_4(Q)\\&=D_{\mathrm{si}}^*+(X_i^*+h^{*\prime}_ir_i^*)abP\end{aligned}\tag{4}$$

根据式(3)和式(4), B通过计算输出abP作为CDH实例的解决方案

$$abP=(S_i^*-S_i^{*'})/(h_i^*r_i^*-h'^*_ir^*_i)。$$ 证毕

4.2 聚合签密密文不可伪造性

定理2 假定CDH问题困难，本文异构聚合签密方案在随机预言模型下自适应选择消息攻击下不可伪造。

这个定理是通过结合引理3和引理4得到的。

引理 3 在随机预言模型下，假设敌手A_1在时间t内能以不可忽略的优势ε攻破本文方案，则存在

算法B，能以$\varepsilon' \geq (\varepsilon - q^s/2^k)(1-1/q^{\mathrm{pk}})^{q_{\mathrm{Pk}}}$优势解决 CDH 问题的一个实例。

证明　算法B首先设置在引理1中描述的公共参数。注意，在设置阶段，B设置$P_{\mathrm{pu}} = aP$。然后，A_1执行在引理1中描述的模拟询问。挑战者B以与引理1相同的方式回答A_1的查询。

(1)**聚合解签密询问Aggregate De-signcryption query**: A_1向B提交一个密文集合σ，发送者的伪身份$\{\mathrm{ID_{si}}\}_{i=1}^{m}$，接收者的身份集$L^* = \{\mathrm{ID_{rj}}\}_{j=1}^{n}$，$B$使用IBC-KG算法计算接收者的私钥$\{\mathrm{ID_{rj}}\}_{j=1}^{n}$。如果它是一个有效的密文，$A_1$首先检查$\sigma$的有效性。之后，$A_1$返回对密文$\sigma$运行Aggregate de-signcrypt算法的结果。

(2)**输出Output**: A_1输出$\{\mathrm{ID_{si}}\}_{i=1}^{m}$和$\{\mathrm{ID_{rj}}\}_{j=1}^{n}$且对应的公钥$\{P_{\mathrm{si}}^*\}_{i=1}^{m}$和$\{\mathrm{ID_{rj}}\}_{j=1}^{n}$，$m$个消息$\{M_i\}_{i=1}^{m}$和他们的聚合密文$\sigma^* = (R_i^*, C_i^*, S_i^*)$。伪造的聚合密文必须使用聚合解密来验证，即

$$
\begin{aligned}
e(S^*, P) &= e\left(\sum_{i=1}^{m} Q_{\mathrm{si}}^*, P_{\mathrm{pu}}\right) \\
&\quad \cdot e\left(\sum_{i=1}^{m}(D_{\mathrm{si}}^* + h_i \cdot r_i H_4(P_{\mathrm{pu}})), P_{\mathrm{pu}}\right) \\
&= e\left(\sum_{i=1}^{m} Q_{\mathrm{si}}^*, P_{\mathrm{pu}}\right) \\
&\quad \cdot e\left(\sum_{i=1}^{m}(P_{\mathrm{si}}^*, +h_i \cdot R_i), H_4(P_{\mathrm{pu}})\right)
\end{aligned}
$$

$$
P_{\mathrm{pu}} = aP,\ H_4(P_{\mathrm{pu}}) = tP,\ Q_{\mathrm{si}}^* = \alpha_i bP
$$

利用分叉引理我们得到

$$
abP = \left(S^* - t\sum_{i=1}^{m} X_i P + h_i^* R_i^*\right)\left(\sum_{i=1}^{m}\alpha_i\right)^{-1}
$$

引理 4　在随机预言模型下，假设敌手A_2在时间t内能以不可忽略的优势ε攻破本文方案，则存在算法B，能以$\varepsilon' \geq (\varepsilon - q^s/2^k)(1-1/(q^{\mathrm{pk}}+m))^{q_{\mathrm{Pk}}+m-1}$优势解决CDH问题的一个实例。

证明　B设置与引理2中描述的公共参数。挑战者B以与引理2相同的方式回答A_2的查询。

输出Output: A_2输出$\{\mathrm{ID_{si}}\}_{i=1}^{m}$和$\{\mathrm{ID_{rj}}\}_{j=1}^{n}$且对应的公钥$\{P_{\mathrm{si}}^*\}_{i=1}^{m}$和$\{Q_{\mathrm{rj}}^*\}_{j=1}^{n}$，$m$个消息$\{M_i\}_{i=1}^{m}$和它们的聚合密文$\sigma^* = (R_i^*, C_i^*, S_i^*)$。伪造的聚合密文必须使用聚合解密来验证。

利用分叉引理我们得到

$$
abP = \left(S^* - t\sum_{i=1}^{m} X_i P + h_i^* R_i^*\right)\left(\sum_{i=1}^{m}\alpha_i\right)^{-1}
$$

证毕

5　性能分析

将本文方案和Niu方案进行效率对比。用T_{add}代表点加运算耗费的时间，T_{pm}代表点乘运算耗费的时间，T_p代表双线性对运算耗费的时间，T_H代表Hash函数映射到点耗费的时间，T_h代表一次普通Hash函数耗费的时间。$|m|$代表消息的长度，$|U|$代表用户身份的长度，$|G_1|$ 代表G_1群中元素长度。

本文方案使用的基本运算耗费的时间如表1所示。实验环境为戴尔笔记本(I7-4700 CPU @3.20 GHz, 16 GB内存和Ubuntu Linux操作系统)。同时使用了密码函数库(Pairing-Based Cryptography, PBC)。

表 1　基本运算耗费的时间(ms)

T_{add}	T_{pm}	T_p	T_H	T_h
0.023	3.382	3.711	6.720	1.024

表2分析了两个方案的签密以及解签密效率。从表2可以看出，在签密阶段，本文方案效率略低于Niu[16]方案，是因为比Niu方案多了一个Hash函数，但是安全性因此略有提高。在解签密阶段，本文方案与Niu方案效率相当。

表 2　签密方案效率比较

方案	签密	解签密	安全性
Niu方案	$(2n+5)T_{\mathrm{pm}} + T_p + 2T_H + T_h + (n+3)T_{\mathrm{add}} \geq 41.849$	$nT_{\mathrm{pm}} + 5T_p + 3T_H + T_h + (n+1)T_{\mathrm{add}} \geq 42.143$	低
本文方案	$(2n+5)T_{\mathrm{pm}} + T_p + 3T_H + T_h + (n+3)T_{\mathrm{add}} \geq 48.569$	$nT_{\mathrm{pm}} + 5T_p + 3T_H + T_h + (n+1)T_{\mathrm{add}} \geq 42.143$	高

以上性能分析表明，新方案在运算效率上与Niu方案相当，这是因为本文的主要工作是提高原方案的安全性，确保方案可以抵抗不可伪造性攻击。

6　结束语

具有系统隐私保护功能的异构聚合签密方案不仅解决了不同密码系统之间多个签密密文验证困难的问题，同时还具有双重隐私保护功能。本文分析了Niu方案的安全性。指出了该方案存在KGC伪造攻击，并分析了产生KGC被动攻击的原因，描述了KGC伪造攻击的过程。随后对Niu方案进行了改造，给出了新的方案。证明了本文方案满足不可伪造性。本文方案具有较高安全性，未来会进一步地研究降低运算效率。

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: 165–179. doi: 10.1007/BFb0052234.

[2] 杜庆灵. 基于身份的动态群通信签密方案[J]. 信息网络安全, 2017(9): 42–44. doi: 10.3969/j.issn.1671-1122.2017.09.010.
DU Qingling. Identity based dynamic group communication signcryption scheme[J]. *Netinfo Security*, 2017(9): 42–44. doi: 10.3969/j.issn.1671-1122.2017.09.010.

[3] 刘明烨, 韩益亮, 杨晓元. 基于准循环低密度奇偶校验码的签密方案研究[J]. 信息网络安全, 2016(11): 66–72. doi: 10.3969/j.issn.1671-1122.2016.11.011.
LIU Mingye, HAN Yiliang, and YANG Xiaoyuan. Research of signcyption based on QC-LDC[J]. *Netinfo Security*, 2016(11): 66–72. doi: 10.3969/j.issn.1671-1122.2016.11.011.

[4] SELVI S, VIVEK S, SHRIRAM J, *et al*. Identity based aggregate signcryption schemes[C]. International Conference on Cryptology in India, New Delhi, India, 2009: 378–397. doi: 10.1007/978-3-642-10628-6_25.

[5] BABAMIR F S and EALAMI Z. Data security in unattended wireless sensor networks through aggregate signcryption[J]. *KSII Transactions on Internet & Information Systems*, 2012, 6(11): 2940–2955. doi: 10.3837/tiis.2012.10.011.

[6] HAN Yiliang, LU Wanyi, and ZHANG Jian. Identity based aggregate signcryption scheme[J]. *Lecture Notes in Electrical Engineering*, 2014, 273(7): 383–389. doi: 10.1007/978-3-642-40640-9-48.

[7] EALAMI Z snd NASROLLAH P. Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model[J]. *Journal of King Saud University Computer and Information Sciences*, 2014, 26(3): 276–286. doi: 10.1016/j.jksuci.2014.03.006.

[8] 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.

[9] HUANG Qiong, 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.

[10] LI Fagen, ZHANG Hui, and TAKAGI T. Efficient signcryption for heterogeneous systems[J]. *IEEE Systems Journal*, 2013, 7(3): 420–429. doi: 10.1109/JSYST.2012.2221897.

[11] 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.

[12] 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 in the standard model[J]. *Journal of Electronics & Information Technology*, 2017, 39(4): 881–886. doi: 10.11999/JEIT160662.

[13] 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.

[14] 张玉磊, 张灵刚, 王彩芬, 等. 可证安全的IDPKC-to-CLPKC异构签密方案[J]. 电子与信息学报, 2017, 39(9): 2127–2133. doi: 10.11999/JEIT170062.
ZHANG Yulei, ZHANG Linggang, WANG Caifen, *et al*. Provable secure IDPKC-to-CLPKC heterogeneous signcryption scheme[J]. *Journal of Electronics & Information Technology*, 2017, 39(9): 2127–2133. doi: 10.11999/JEIT170062.

[15] 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.

[16] NIU Shufen, LI Zhenbin, and WANG Caifen. Privacy-Preserving Multi-party Aggregate Signcryption for Heterogeneous Systems[C]. International Conference on Cloud Computing and Security, Nanjing, China, 2017: 216–229. doi: 10.1007/978-3-319-68542-7_18.

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.

陈文娟：女，1993年生，硕士生，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.