一种可证安全的异构聚合签密方案

牛淑芬* 牛 灵 王彩芬 杜小妮
(西北师范大学计算机科学与工程学院 兰州 730070)

摘 要：异构签密可实现不同安全域之间数据通信的机密性、认证性和不可伪造性。分析现有的异构签密方案，发现它们仅是针对单个消息而设计的，计算效率普遍较低，不适合大数据环境下的网络通信系统。该文提出一个异构的聚合签密方案，该方案不但可以实现单个消息的签密验证，而且可以实现多个消息的聚合验证，并且验证需要的双线性对个数固定，与所签密消息的个数无关。同时，在随机预言模型下，证明了方案的机密性和不可伪造性分别基于 q 双线性 Diffie-Hellman 逆问题和离散对数问题。数值结果表明，该方案与现有方案相比在计算效率和传输效率上有着极大的提高。

关键词：聚合签密；异构系统；q 双线性 Diffie-Hellman 逆问题；离散对数问题
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2017)05-1213-06
DOI: 10.11999/JEIT160829

A Provable Aggregate Signcryption for Heterogeneous Systems

NIU Shufen NIU Ling WANG Caifen DU Xiaoni
(*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Heterogeneous signcryption can ensure the confidentiality, authentication and unforgeability of information transmission of cross cryptograph environment. Through analyzing some existing heterogeneous signcryption schemes, it is found that they can only be applicable to single message of signcryption. In order to improve the efficiency of computation and transmission in heterogeneous systems, a provable multi-message aggregate signcryption is proposed. In the new scheme, the pairing numbers are constant in verification phase, it not depends on the number of signcryption message. Moreover, based on the assumption of q-bilinear Diffie-Hellman inversion issue and Discrete logarithm, in the random oracle model, it is proved that the new scheme satisfies the properties of confidentiality and unforgeability. Furthermore, theoretical analysis and experimental results demonstrate that the computation overhead efficiency of the proposed scheme is better than the existing one.

Key words: Aggregate signcryption; Heterogeneous systems; q-bilinear Diffie-Hellman inversion problem; Discrete logarithm problem

1 引言

现代的计算机通信网络是一个全球覆盖的网络，不同类型的计算机和不同类型的终端之间进行着各种访问。不同的网络系统可能采用不同的密码技术。例如，它们各自使用传统 PKI 技术、身份公钥密码技术和无证书公钥密码技术等。当网络系统采用不同的密码技术进行通信时，就需要考虑支持异构通信的密码技术。

1997 年，Zheng[1]首次提出签密的概念，签密可以同时实现加密和签名操作，保证消息的机密性、认证性和不可伪造性，其效率优于传统“先签名后加密”方法。2002 年，Baek 等人[2]首次描述了签密方案的安全模型，并对文献[1]的方案进行了严格的安全性证明。自此，研究者们对签密问题进行了一系列的研究[3−7]。但有关异构签密算法的出版文献相对比较少。2010 年，Sun 和 Li[8]首次提出了一个异构系统的签密方案，但其方案只满足外部安全性。2011 年，Huang 等人[9]提出了一个从 IBC(基于身份的密码技术)到 PKI 的隐私保护性签密方案并且满足内部安全性。2013 年，Li 等人[4]提出了两个类型的异构签密方案，分别是从 IBC 到 PKI 及 PKI 到

收稿日期：2016-08-15；改回日期：2017-01-13；网络出版：2017-03-21
*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)，西北师范大学青年教师科研提升计划(NWNU-LKQN-13-12)
Foundation Items: The National Natural Science Foundation of China (61562077, 61462077, 61662071), The Young Teacher's Scientific Research Ability Promotion Program of Northwest Normal University (NWNU-LKQN-13-12)

IBC，并证明了这两个方案都满足内部安全性。

聚合签密能够把多个消息的签密聚合生成一个签密，验证者只需验证聚合后的签密，就可以实现对多个消息的签密认证[10−14]。在当前的大数据环境下，应用聚合签密技术能够极大地提高系统的验证效率，同时也能够有效地减少系统的传输量。

本文针对 PKI 到 IBC 的异构密码系统，提出了一个可证安全的异构聚合签密方案 MHSC，与文献[4]方案相比，新方案可以对多个消息同时进行签密验证，并且验证需要的双线性对个数固定，与所签密消息的个数无关。同时，在随机预言模型下，证明了方案的机密性和不可伪造性分别基于 q 双线性 Diffie-Hellman 逆问题和离散对数问题。通过理论分析和数值分析可以看出，当签密多个消息时，本文方案在计算效率和传输效率上都优于已有的方案。

2 基础知识

定义 1(双线性映射) 设 p 是一个大素数，G_1,G_2 分别是两个有着相同素数阶 p 的循环加法群和循环乘法群，P 是 G_1 的生成元。一个双线性映射 $e:G_1\times G_1\to G_2$ 满足下列性质：

双线性 对任意的 $P,Q\in G_1$，存在 $a,b\in Z_p^*$，使得 $e(aP,bQ)=e(P,Q)^{ab}$。

非退化性 存在 $P,Q\in G_1$，使得 $e(P,Q)\neq 1$。

可计算性 对所有的 $P,Q\in G_1$，存在有效算法计算 $e(P,Q)$。

定义 2(q 双线性 Diffie-Hellman 逆问题(q-BDHIP)) G_1 和 G_2 分别是两个阶为素数 p 的循环加法群和循环乘法群，P 是 G_1 的生成元，$e:G_1\times G_1\to G_2$ 为双线性映射，q 双线性 Diffie-Hellman 逆问题是指给定 $(P,\alpha P,\alpha^2P,\cdots,\alpha^qP)$，求解 $e(P,P)^{1/\alpha}$。

定义 3(离散对数问题(DLP)) 已知有限循环群 G 及其生成元 P，离散对数问题是指给定 $P,\alpha P\in G$，求解 $\alpha\in Z_p^*$。

3 MHSC 方案形式化定义和安全模型

本文的方案是 PKI 到 IBC 的聚合签密算法。其中，签密者的公私钥颁发是基于 PKI 系统，而解签密者的公私钥生成是基于 IBC 的密码体制。

3.1 方案的形式化定义

MHSC 方案包括以下 6 个算法：

系统建立 给定安全参数 k，输出系统参数 params，系统公钥 mpk 和主密钥 msk。

密钥生成(PKI-KG) PKI 系统中的用户使用该算法生成私钥 sk 和相应的公钥 pk。CA 需要对该公钥进行签名并生成数字证书。

密钥提取(IBC-KG) IBC 系统中的用户使用该算法获得自己的私钥。给定身份 ID_U，PKG 计算用户的私钥 S_{ID_U}。用户的公钥 pk 就是身份 ID_U。

签密算法 输入系统参数和消息 m_i，一个发送者的私钥 sk_s，一个接收者的公钥 pk_r，输出一个密文 σ_i。

聚合签密算法 给定 m 个消息的密文 $\sigma_i(i=1,2,\cdots,m)$，发送者的私钥 sk_s，接收者的公钥 ID_r，输出聚合签密密文 σ。

聚合解签密算法 给定密文 σ，发送者的公钥 pk_s 和接收者的私钥 S_{ID_r}，输出明文 $m_i(i=1,2,\cdots,m)$。若聚合解签密算法验证不正确，则输出 $\perp$。

3.2 安全模型

MHSC 签密方案的安全性包括机密性和不可伪造性。即在适应性选择密文攻击下具有不可区分性(IND-MHSC-CCA2)和在适应性选择消息攻击下具有存在性不可伪造(EUF-MHSC-CMA)。本文安全性的概念是内部安全性，即如果发送者的私钥丢失了，攻击者也不能从密文中恢复出消息，如果接收者的私钥丢失了，攻击者也不能伪造一个密文。另外，由于敌手知道接收者的私钥，因此解签密询问就不再需要了。

游戏 1(机密性) 该聚合异构签密算法的适应性选择密文攻击游戏由下面 3 个阶段组成，这是一个挑战者 F 和攻击者 A 之间的游戏。

初始阶段 F 运行系统建立算法，并将产生的系统参数 params 发送给攻击者 A。F 同时运行密钥生成算法 PKI-KG 获得发送者的公私钥对 $(\mathrm{pk}_s,\mathrm{sk}_s)$ 并将其发送给 A。

阶段 1 攻击者 A 适应性地进行以下的询问：

密钥提取询问 攻击者 A 选择一个身份 ID，F 运行密钥提取算法 IBC-KG 将 ID 的私钥 S_{ID} 发送给攻击者 A。

解签密询问 A 提交一个接收者身份 ID_r 和一个密文 σ 给 F。F 首先运行密钥提取算法以便获得接收者的私钥 S_{ID_r}，然后利用私钥 S_{ID_r} 运行 σ 解签密算法并将产生的结果发送给 A。

挑战阶段 A 产生两个长度相同的明文 m_0,m_1 和接收者身份 ID_r 并将它们发送给 F。ID_r 不能是已经执行过密钥提取询问的身份。F 随机选择一个比特 $\gamma\in\{0,1\}$ 并计算 σ^*，F 发送 σ^* 给攻击者 A。

阶段 2 A 可以像阶段 1 那样执行多项式有界的适应性询问。但 A 不能询问 ID_r 的私钥，也不能提交 σ^* 进行 ID_r 的解签密询问。

猜测阶段 A 输出一个比特 γ'，如果 $\gamma'=\gamma$，那么 A 赢得了游戏。

游戏 2(不可伪造性)　聚合异构签密算法的适应性选择消息攻击游戏由下面 3 个阶段组成，这是一个挑战者 F 和攻击者 A 之间的游戏。

初始阶段　F 运行系统建立算法，并将产生的系统参数 params 和主密钥 s 发送给 A。F 运行密钥生成算法以获得发送者的公私钥对 $(\mathrm{pk}_s^*,\mathrm{sk}_s^*)$ 对并将 pk_s^* 发送给 A。

攻击阶段　A 适应性执行多项式有界的询问。在签密询问中，A 提交一个接收者的身份 ID_j 和一个消息 m_i 给 A。A 运行签密预言机并返回密文 σ_i。

伪造阶段　A 产生一个接收者的身份 ID_r 和一个密文 σ_i^*。如果 σ_i^* 对于 pk_s^* 和 ID_r 是一个合法的密文，且 A 没有询问过 m_i^*，pk_s^* 和某个接收者身份 $\mathrm{ID}_r^{'}$ 的签密询问。

4　具体方案

系统建立算法　输入安全参数 1^k, PKG：

(1)输出阶为素数 p 的循环加法群 G_1 和循环乘法群 G_2，P 为群 G_1 的生成元，$e:G_1\times G_1\to G_2$ 为一个双线性映射，$H_1:\{0,1\}^*\to Z_p^*$，$H_2:\{0,1\}^*\times G_2\to G_1$，$H_3:G_2\to\{0,1\}^n$ 为 3 个哈希函数，n 为签密消息的长度。

(2)选择一个主密钥 $s\in Z_p^*$，计算系统公钥 $P_0=sP$。

(3)计算 $K=e(P,P)$。

PKG 公开系统参数 $\{G_1,G_2,n,P,P_0,K,H_1,H_2,H_3\}$，保密主密钥 s。

密钥生成(PKI-KG)　PKI 系统中的发送者随机选择 $x_s\in Z_p^*$ 为自己的私钥，计算公钥 $\mathrm{pk}_s=x_sP$。

密钥提取(IBC-KG)　IBC 系统中的接收者向 PKG 提交一个身份 ID_r，PKG 计算 ID_r 的私钥 $S_{\mathrm{ID}_r}=\dfrac{1}{H_1(\mathrm{ID}_r)+s}P$，并以安全的方式发送给接收者。

签密算法　对要发送的消息 $m_i(i=1,2,\cdots,m)$，发送者的私钥 $\mathrm{sk}_s=x_s$，接收者的身份 ID_r，该签密算法如下：

(1)随机选取 $x_i\in Z_p^*$。

(2)计算 $r_i=K^{x_i}$，$m=(m_1\oplus r_1)\,\|\,(m_2\oplus r_2)\,\|\cdots\|\,(m_m\oplus r_m)$，$C=m\oplus H_3(r_1\,\|\,r_2\,\|\cdots\|\,r_m)$。

(3)计算 $h_i=H_2(m_i,r_i)$。

(4)计算 $S_i=h_ix_s-x_iP$。

(5)计算 $T_i=x_i(H_1(\mathrm{ID}_r)P+P_0)$。

发送者发送密文 C 和消息 m_i 的签名 $\sigma_i=(S_i,T_i)$ 给聚合者。

聚合签密算法　聚合者输入消息 m_i 对应的签密密文 $\sigma_i=(S_i,T_i)$ 及 C、接收者的身份 ID_r，计算 $S=\sum_{i=1}^m S_i$，则聚合密文为 $\sigma=(C,S,T=(T_1,T_2,\cdots,T_m))$

聚合解签密算法　接收到的密文 σ，发送者的公钥 pk_s，接收者的私钥 $S_{\mathrm{ID}_r}=\dfrac{1}{H_1(\mathrm{ID}_r)+s}P$，该聚合解签密算法如下：

(1)计算 $r_i=e(T_i,S_{\mathrm{ID}_r})$。

(2)恢复 $m=C\oplus H_3(r_1\,\|\,r_2\,\|\cdots\|\,r_m)$。

(3)恢复 $m_i=(m_i\oplus r_i)\oplus r_i$。

(4)计算 $h_i=H_2(m_i,r_i)$。

(5)计算 $R=\prod_{i=1}^m r_i$。

(6)检查等式 $R\cdot e(S,P)=e\left(\sum_{i=1}^m h_i,\mathrm{pk}_s\right)$ 是否成立，若等式成立，接受消息 m_i。

正确性证明　本文的方案是正确的，当且仅当异构签密密文 $\sigma_i=(S_i,T_i)$ 及 C 和异构聚合签密密文 $\sigma=(C,S,T=(T_1,T_2,\cdots,T_m))$ 都按照签密算法计算得到，即有以下两类验证等式成立：

(1)验证者检查等式 $r_i\cdot e(S_i,P)=e(h_i,\mathrm{pk}_s)$，可以验证签密密文 $\sigma_i=(C,S_i,T_i)$ 的正确性。

$$\begin{aligned}r_i\cdot e(S_i,P)&=r_i\cdot e(h_ix_s-x_iP,P)=r_i\cdot e(h_ix_s,P)\\&\quad\cdot e(-x_iP,P)=e(P,P)^{x_i}\cdot e(h_i,x_sP)\\&\quad\cdot e(P,P)^{-x_i}=e(h_i,x_sP)=e(h_i,\mathrm{pk}_s)\end{aligned}$$

(2)验证该异构聚合签密方案的一致性，首先：

$$\begin{aligned}e(T_i,S_{\mathrm{ID}_r})&=e(x_i(H_1(\mathrm{ID}_r)P+P_0),S_{\mathrm{ID}_r})\\&=e\left(x_i(H_1(\mathrm{ID}_r)+s)P,\ \frac{1}{H_1(\mathrm{ID}_r)+s}P\right)\\&=e(P,P)^{x_i}=K^{x_i}=r_i\end{aligned}$$

那么有

$$\begin{aligned}R\cdot e(S,P)&=\prod_{i=1}^m r_i\cdot e\left(\sum_{i=1}^m S_i,P\right)\\&=\prod_{i=1}^m r_i\cdot e\left(\sum_{i=1}^m(h_ix_s-x_iP),P\right)\\&=\prod_{i=1}^m r_i\cdot e\left(\sum_{i=1}^m h_ix_s,\ P\right)\cdot e\left(-\sum_{i=1}^m x_iP,P\right)\\&=K^{\sum_{i=1}^m x_i}\cdot e\left(\sum_{i=1}^m h_i,x_sP\right)\cdot K^{-\sum_{i=1}^m x_i}\\&=e\left(\sum_{i=1}^m h_i,x_sP\right)=e\left(\sum_{i=1}^m h_i,\mathrm{pk}_s\right)\end{aligned}$$

5　安全性分析

5.1 机密性

定理 1　随机预言模型下，假设 q-BDHIP 问题是困难的，则本文 MHSC 方案在适应性选择密文攻

击下不可区分，即 IND-MHSC-CCA2 安全。

引理 1 随机预言模型下，如果存在一个概率多项式时间攻击者 A 以不可忽略的概率赢得游戏，那么存在一个算法 F 能够解决 q-BDHIP 困难问题。

引理 1 的证明过程与文献[4]方案的机密性证明过程相似，限于篇幅，略去此部分。

5.2 不可伪造性

定理 2 随机预言模型下，假设 DLP 问题困难，则提出的 MHSC 方案在适应性选择消息攻击下是存在性不可伪造的，即 EUF-MHSC-CMA 安全。

引理 2 随机预言模型下，如果存在一个概率多项式时间攻击者 A 以不可忽略的概率赢得游戏，那么存在一个算法 F 能够解决 DLP 困难问题。

证明 我们利用分叉引理[15]来证明引理 2。A 是攻击者，F 是 DLP 问题挑战者。F 给定一个 DLP 问题实例 $(P,\alpha P)$，F 的目标是使用攻击者 A 解决 DLP 问题，即计算 α。

初始阶段 F 运行系统建立算法获得系统参数并发送系统参数 params、主密钥 msk 和发送者的公钥 $\mathrm{pk}_s^* = \alpha P$ 给攻击者 A。

攻击阶段 F 保持 3 个表 L_1, L_2, L_3 分别保存 H_1, H_2, H_3 询问中产生的数据。A 能够对以下预言机进行多项式有界次地适应性询问。

H_1 询问 对于 $H_1(\mathrm{ID}_i)$ 询问，如果以前被询问过，则返回 L_1 的值；否则 F 返回一个随机数 $h_{1,i} \in Z_p^*$，增加 $(\mathrm{ID}_i, h_{1,i})$ 到列表 L_1 中。

H_2 询问 F 保持列表 $L_2 = (m_i, r_i, h_{2,i})$，初始为空。$A$ 询问 H_2 预言机，若 L_2 存在询问则直接返回，否则，F 选择 $h_{2,i} \in G_1$ 并将 $(m_i, r_i, h_{2,i})$ 增加到列表 L_2 中。

H_3 询问 F 保持列表 $L_3 = (r_i, h_{3,i})$，初始为空。A 询问 H_3 预言机，若 L_3 存在询问则直接返回，否则，F 选择 $h_{3,i} \in \{0,1\}^n$ 并将 $(r_i, h_{3,i})$ 增加到列表 L_3 中。

签密询问 A 对明文 m_i 和接收者的身份 ID_j 进行签密询问，F 执行以下操作：

(1)随机选择 $\theta_i, t_i \in Z_p^*$。

(2)计算 $h_i = t_i P$。

(3)计算 $S_i = \theta_i S_{\mathrm{ID}_j}$。

(4)计算 $T_i = \alpha t_i (H_1(\mathrm{ID}_j)P + P_0) - \theta_i P$。

(5)计算 $r_i = e(T_i, S_{\mathrm{ID}_j})$。

(6) 计 算 $m = (m_1 \oplus r_1) \| (m_2 \oplus r_2) \| \cdots \| (m_m \oplus r_m)$ 以及 $C = m \oplus H_3(r_1 \| r_2 \| \cdots \| r_m)$。

(7)返回 $\sigma_i = (S_i, T_i)$ 及 C 给攻击者 A。

伪造阶段 从攻击者的角度看，每个序号 i 有相同的概率。不失一般性，从多个消息 $m_i (i = 1,2,\cdots,m)$ 中选择一个作为目标。由 Forking 引理，设 A 能够伪造成功，则对消息 m_i 输出两个不同的签名 (m_i^*, h_i^*, S_i^*) 和 $(m_i^*, h_i^{'*}, S_i^{'*})$，同时输出两个聚合密文 $\sigma^* = (C^*, S^*, T^*), \sigma^{'*} = (C^*, S^{'*}, T^*)$，使得满足聚合签密等式，即有

$$e\left(\sum_{j=1, j\neq i}^{m} h_j^* + h_i^*, \mathrm{pk}_s^*\right) \cdot e(S^*, P)^{-1} = e\left(\sum_{j=1, j\neq i}^{m} h_j^* + h_i^{'*}, \mathrm{pk}_s^*\right) \cdot e\left(S^{'*}, P\right)^{-1}$$

其中，$S^* = \sum_{j=1, j\neq i}^{m} S_j^* + S_i^*$，$S^{'*} = \sum_{j=1, j\neq i}^{m} S_j^{'*} + S_i^{'*}$，则可得：$\alpha = (h_i^* - h_i^{'*})^{-1}(S_i^* - S_i^{'*})$，相当于解决了 DLP 问题。 证毕

6 效率分析

本节主要讨论所提方案在签密阶段和验证阶段的计算效率，其次比较已有的异构签密方案[4]与本文方案在计算效率和传输效率上的优劣。

6.1 计算效率分析与比较

6.1.1 理论分析比较 本节首先从理论角度分析所提方案与文献[4]在计算效率上的优劣。在表 1 和表 2 中，主要比较的运算包括双线性对(T_p)、指数运算(T_e)、哈希运算(T_h)、点乘运算(T_m)和加法运算(T_a)。

表 1 签密阶段的计算量比较

方案	一个消息	m 个消息
文献[4]	$T_\mathrm{e} + 2T_\mathrm{h} + 3T_\mathrm{a} + 3T_\mathrm{m}$	$mT_\mathrm{e} + 2mT_\mathrm{h} + 3mT_\mathrm{a} + 3mT_\mathrm{m}$
本文方案	$T_\mathrm{e} + 2T_\mathrm{h} + 3T_\mathrm{a} + 4T_\mathrm{m}$	$mT_\mathrm{e} + (m+1)T_\mathrm{h} + (3m+2)T_\mathrm{a} + 4mT_\mathrm{m}$

由表 1 可以看出在签密阶段，当系统需要传送一个消息时，本文方案增加了一个乘法运算，运算负担有略微的增加；而当系统传送 m 个消息时，虽然在乘法和加法运算量上有所增加，但极大地减少了就运算耗时量大的哈希运算。

由表 2 可以看出在解签密阶段，当系统需要传送一个消息时，本文方案增加了一个对运算，而减

表 2 解签密阶段的计算量比较

方案	一个消息	m 个消息
文献[4]	$2T_\mathrm{p} + T_\mathrm{e} + 2T_\mathrm{h} + T_\mathrm{a} + T_\mathrm{m}$	$2mT_\mathrm{p} + mT_\mathrm{e} + 2mT_\mathrm{h} + mT_\mathrm{a} + mT_\mathrm{m}$
本文方案	$3T_\mathrm{p} + T_\mathrm{h} + T_\mathrm{a} + T_\mathrm{m}$	$(m+2)T_\mathrm{p} + (m+1)T_\mathrm{h} + 2mT_\mathrm{a} + mT_\mathrm{m}$

少了一个指数运算，运算负担也有略微的增加；而当系统传送 m 个消息时，同样在乘法和加法运算量上有所增加，但极大地减少了运算耗时量大的哈希运算和对运算。综上的分析可以看出，当消息的个数 m 较大时，本文方案总的计算效率优于文献[4]的方案。

6.1.2 数值分析　我们在 Linux 操作系统下利用双线性对包(pairing-based cryptography library)[16]，用 C 语言编程，在 2.9 GHz CPU, 4 GB RAM PC 机上运行。表 3 说明双线性对包参数 Type a 的性质。

表 3 对参数的主要性质

参数类型	基域(bit)	Dlog 安全(bit)	椭圆曲线次数
Type a	512	1024	2

(1)本文方案MHSC的计算效率：　本算法的签密与解签密运行效率是由签密方案中消息的个数所决定的。在数值实验中，签密消息的个数 m 分别取为：1, 10, 50, 100, 500, 1000。表 4 分别是整个算法、签密算法和解签密算法运行所花费的时间。

(2)比较分析：　为了比较本文MHSC算法与文献[4]中所提方案在签密和解签密两个阶段的计算效率，在MHSC方案中，签密消息的个数 m 分别取为：50, 100, 500, 1000。而在文献[4]中的程序中，算法运行次数分别设为：50, 100, 500, 1000。两个算法在签密阶段和解签密阶段的比较结果分别如图 1 和图 2。

由图 1和图 2可以看出，当对多个消息进行签密时，本文所提MHSC算法无论在签密阶段，还是解签密阶段，计算效率都优于文献[4]的算法。尤其当消息的个数逐渐增大时，本文的算法计算效率更优，更适用于大数据环境。

6.2 传输效率分析

本文的 MHSC 算法基于聚合签名的思想，对 m 个消息只传输一个聚合后的加密密文，系统传输量为 $|M|+(m+1)|G_1|$，而在文献[4]中，当签密 m 个消息时，系统传输量为 $m|M|+2m|G_1|$，其中，$|M|$ 为明文的长度，$|G_1|$ 为 G_1 中元素的长度。所以当对多个消息进行签密时，本文方案有效地减少了系统的传输负担。

7　结论

本文提出了一个由 PKI 密码体制到基于身份密码体制的异构签密算法，实现了跨密码体制数据传输的机密性和认证性。本算法基于聚合签密的思想，实现多个消息的同时验证，有效地减少了算法的计算量和网络系统的传输开销，更适合于大数据时代下的网络环境。

表4 本文方案MHSC的计算效率(s)

	m=1	m=10	m=50	m=100	m=500	m=1000
算法运行时间	0.0446	0.1701	0.7009	1.4073	6.8842	13.750
签密运行时间	0.0142	0.1077	0.5023	1.0295	5.1218	10.256
解签密运行时间	0.0105	0.0423	0.1796	0.3580	1.7408	3.4785

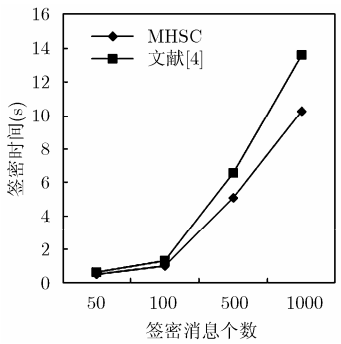

图 1 签密计算效率

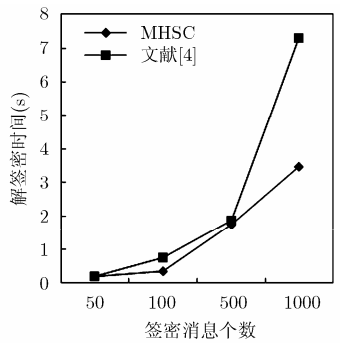

图 2 解签密计算效率

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] PANG Liaojun, GAO Lu, LI Huixian, *et al*. Anonymous multi-receiver ID-based signcryption scheme[J]. *Iet Information Security*, 2015, 9(3): 194–201. doi: 10.1049/iet-ifs.2014.0360.

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

[5] 张雪, 冀会芳, 李光松, 等. 基于身份的跨信任域签密方案[J]. 计算机科学, 2015, 42(5): 165–168. doi: 10.11896/j.issn.1002-137X.2015.5.033.

ZHANG Xue, JI Huifang, LI Guangsong, *et al*. Identity-based signcryption cross autonomous domains[J]. *Computer Science*, 2015, 42(5): 165–168. doi: 10.11896/j.issn.1002-137X.2015.5.033.

[6] ZHOU Yanwei, YANG Bo, and ZHANG Wenzheng. Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing[J]. *Discrete Applied Mathematics*, 2016, 204(C): 185–202. doi: 10.1016/j.dam.2015.10.018.

[7] LI Fagen, HAN Yanan, and JIN Chunhua. Practical signcryption for secure communication of wireless sensor networks[J]. *Wireless Personal Communications*, 2016, 89(4): 1391–1412. doi: 10.1007/s11277-016-3327-4.

[8] SUN Yinxia and LI Hui. Efficient signcryption between TPKC and IDPKC and its multi-receiver construction[J]. *Sciece 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]. *Computer Journal*, 2011, 54(4): 525–536. doi: 10.1093/comjnl/bxq095.

[10] 张玉磊, 王欢, 李臣意, 等. 可证安全的紧致无证书聚合签密方案[J]. 电子与信息学报, 2015, 37(12): 2838–2844. doi: 10.11999/JEIT150407.

ZHANG Yulei, WANG Huan, LI Chenyi, *et al*. Provable secure and compact certificateless aggregate signcryption scheme[J]. *Journal of Electronics & Information Technology*, 2015, 37(12): 2838–2844. doi: 10.11999/JEIT150407.

[11] WANG Hao, LIU Zhen, LIU Zhe, *et al*. Identity-based aggregate signcryption in the standard model from multilinear maps[J]. *Frontiers of Computer Science*, 2016, 10(4): 741–754. doi: 10.1007/s11704-015-5138-2.

[12] HAN Yiliang and CHEN Fei. The multilinear maps based certificateless aggregate signcryption scheme[C]. IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Xi'an, China, 2015: 92–99. doi: 10.1109/CyberC.2015.93.

[13] ESLAMI Z and PAKNIAT N. Certificateless aggregate signcryption[J]. *Journal of King Saud University-Computer and Information Sciences*, 2014, 26(3): 276–286. doi: 10.1016/j.jksuci.2014.03.006.

[14] CHEN Juqin and REN Xiaoxi. A privacy protection scheme based on certificateless aggregate signcryption and masking random number in smart grid[C]. International Conference on Mechanical Materials and Manufacturing Engineering, Wuhan, China, 2016: 10–13. doi: 10.2991/mmme-16.2016.3.

[15] DAVID P and JACQUES S. Security arguments for digital signatures and blind signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361–396. doi: 10.1007=s001450010003.

[16] The pairing-based cryptography library[OL]. http://crypto.stanford.edu/pbc/, 2015.

牛淑芬： 女，1976 年生，博士，副教授，研究方向为云计算和大数据网络的隐私保护.

牛 灵： 女，1991 年生，硕士生，研究方向为云计算和大数据网络的隐私保护.

王彩芬： 女，1963 年生，博士，教授，研究方向为网络安全.

杜小妮： 女，1972 年生，博士，教授，研究方向为信息安全.