标准模型下高效的异构签密方案

王彩芬*[①②] 李亚红[②] 张玉磊[①] 牛淑芬[①]
[①](西北师范大学计算机科学与工程学院 兰州 730070)
[②](西北师范大学数统学院 兰州 730070)

摘 要：异构签密方案能够为不同安全域之间的数据通信提供机密性和认证性。分析现有的异构签密方案，都是在随机预言模型下可证安全的。基于此，该文提出一个在标准模型下从基于身份的密码到传统公钥设施的签密方案，利用计算 Diffie-Hellman 问题和判定双线性 Diffie-Hellman 问题的困难性，对该方案的机密性和不可伪造性进行了证明。通过理论和实验分析，该方案在计算成本和通信成本方面具有更高的效率。

关键词：异构签密；标准模型；基于身份的密码；传统公钥设施
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2017)04-0881-06
DOI: 10.11999/JEIT160662

Efficient Heterogeneous Signcryption Scheme in the Standard Model

WANG Caifen[①②] LI Yahong[②] ZHANG Yulei[①] NIU Shufen[①]
[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: Heterogeneous signcryption scheme can ensure the confidentiality and the authentication for data communication between different security domains. Some existing heterogeneous signcryption schemes are analyzed to be secure in the random oracle model. Based on this problem, an Identity-Based Cryptography (IBC) to Public Key Infrastructure (PKI) signcryption scheme is proposed. The proposed scheme has the confidentiality and the unforgeability under the Computational Diffie-Hellman (CDH) problem and the Decisional Bilinear Diffie-HellmanB (DBDH) problem. Through the theoretical and experimental analysis, both the computational costs and the communication overheads of the proposed scheme are more efficient.

Key words: Heterogeneous signcryption; Standard model; Identity-Based Cryptography (IBC); Public Key Infrastructure (PKI)

1 引言

签密[1]能够在一个逻辑步骤内实现加密和签名，因此在通信过程中能够同时实现保密性和认证性，并且效率优于传统的先签名再加密的方法。同时，传统公钥设施(PKI)和基于身份的密码(IBC)作为信息安全领域的关键技术，在实际应用中起着非常重要的作用。因此，研究者对基于传统公钥设施和基于身份的签密进行了一系列的研究[2–7]。然而，以上方案都是在随机预言模型下证明了安全性，但并不能够保证在实际的环境中也是安全的。因此，文献[8–11]分别提出在标准模型下的签密方案。

分析上述的签密方案，发送者和接收者在同一个公钥密码环境中。现在考虑这样两种情形：PKI 系统的用户发送消息给 IBC 系统的用户(类型 I: PKI→IBC); IBC 系统的用户传送消息给 PKI 系统的用户(类型 II: IBC→PKI)，那么上述的签密方案显然不能满足这样的需求。因此，Sun 等人[12]首次提出两个类型 I 的签密方案和多接收者签密方案，而此方案仅满足外部安全性。Huang 等人[13]提出一个类型 II 的签密方案，证明了此方案满足内部安全性；Li 等人[14]提出两个高效的类型 I 和类型 II 的签密方案，并给出了具体的形式化定义及安全模型。

分析以上的异构签密方案都是在随机预言模型证明了安全性。然而，目前仍缺乏在标准模型下有效的的异构签密方案。因此设计一个在标准模型下可证安全的异构签密方案是很有必要的，也是十分有意义的。基于此，本文提出一个在标准模型下的异构签密方案。同时，基于 DBDH 问题和 CDH 问题的困难性证明了方案的安全性。

收稿日期：2016-06-24；改回日期：2016-12-13；网络出版：2017-02-09
*通信作者：王彩芬 wangcf@nwnu.edu.cn
基金项目：国家自然科学基金(61163038, 61562077, 61662069)，甘肃省高等学校科研项目(2014-A011)，西北师范大学青年教师科研能力提升计划(NWNU-LKQN-14-7)
Foundation Items: The National Natural Science Foundation of China (61163038, 61562077, 61662069), Research Fund of Higher Education of Gansu Province (2014-A011), The Foundation for Excellent Young Teachers by Northwest Normal University (NWNU-LKQN-14-7)

2 预备知识

2.1 相关困难问题

定义 1 (计算 Diffie-Hellman(CDH)问题) 给定(g,g^a,g^b)，其中$a,b\in Z_p^*$，求g^{ab}。

定义 2 (判定双线性 Diffie-Hellman(DBDH)问题) 给定(g,g^a,g^b,g^c,T)，其中$a,b,c\in Z_p^*$，$T\in G_T$，判断$T=e(g,g)^{abc}$是否成立。算法$\mathcal{A}$解决DBDH问题的概率优势至少是ε的定义为$\mathrm{Adv}(\mathcal{A})=\left|\Pr\left[1\leftarrow\mathcal{A}\left(g^a,g^b,g^c,T\right)\right]-\Pr\left[1\leftarrow\mathcal{A}(g^a,g^b,g^c,e(g,g)^{abc}\right]\right|\geq 2\varepsilon$。

定义 3 ($(\varepsilon_{\mathrm{dbdh}},t)$-DBDH 假定成立) 如果不存在概率多项式时间算法$\mathcal{A}$在时间t内，以至少$\varepsilon_{\mathrm{dbdh}}$的概率解决DBDH问题。

定义 4 (Hash 函数是(ε_H,t)-抗碰撞的) 如果不存在任意概率多项式时间算法$\mathcal{A}$以至少ε_H的概率找到两个不同的消息m_0和m_1，使得$H(m_0)=H(m_1)$。

2.2 IBC→PKI 异构签案形式化定义

IBC→PKI 的签密方案由以下 5 个算法组成：

(1)系统建立算法(Setup)：给定安全参数λ，输出系统参数Pa。

(2)IBC 密钥生成算法(IBC-KG)：IBC 系统的用户用该算法生成私钥，给定身份u，PKG 计算u的私钥d。

(3)PKI 密钥生成算法(PKI-KG)：PKI 系统中的用户用该算法生成私钥 sk 和公钥 pk，CA 对 pk 进行签名并产生数字证书。

(4)签密算法(Signcrypt)：输入消息m，系统参数Pa，IBC 系统中发送者的私钥d_A和 PKI 系统中接收者的公钥pk_B，输出签密密文σ。

(5)解签密算法(Unsigncrypt)：输入密文σ，系统参数Pa，IBC 系统中发送者的身份u_A和 PKI 系统中接收者的私钥sk_B，输出消息m或符号“⊥”，其中“⊥”表示密文不合法。

以上算法必须满足

$$m=\mathrm{Unsigncrypt}\left(\mathrm{Signcrypt}\left(m,d_A,\mathrm{pk}_B\right),u_A,\mathrm{sk}_B\right)$$

2.3 IBC→PKI 的安全模型

IBC→PKI 的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-IBC→PKI-CCA2)和在适应性选择消息攻击下具有存在不可伪造性(EUF-IBC→PKI-CMA)。本文安全性的定义可参考文献[14]。

3 具体的 IBC→PKI 异构签密方案

(1)Setup：设安全参数为λ，群G和G_T的阶为q，且$G=\langle g\rangle$，$e:G\times G\to G_T$是双线性对。PKG 随机选取$\alpha\in Z_p,g_2,v',u'\in G$，计算$g_1=g^\alpha$；定义哈希函数$H_1:\{0,1\}^*\to\{0,1\}^n$；随机选取$n_u$和$n$维的向量$\boldsymbol{U}=(u_i)$和$\boldsymbol{V}=(v_i)$，且$u_i,v_i\in G$。PKG 发布系统参数$Pa=\{G,G_T,e,g,g_1,g_2,v',u',\boldsymbol{V},\boldsymbol{U},H_1\}$，保存主密钥${g_2}^\alpha$。

(2)IBC-KG：设 IBC 系统中用户的身份为$u_A\in\{0,1\}^{n_u}$，$\mathcal{U}_A=\{i\mid u[i]=1,1\le i\le n_u\}$，其中$u[i]$为$u_A$的第$i$个比特。PKG 随机选取$r_A\in Z_p$，计算$u_A$的钥$d_A=(d_{A1},d_{A2})=\left(g_2^\alpha\left(u'\prod_{i\in\mathcal{U}_A}u_i\right)^{r_A},g^{r_A}\right)$。

(3)PKI-KG: PKI 系统中的用户选择$r_B\in Z_p$，则用户的公钥为$\mathrm{pk}_B=(h_1,Z)$，私钥为$\mathrm{sk}_B=g_2^{r_B}$，其中$h_1=g^{r_B},Z=e(h_1,g_2)$。

(4)Signcrypt：当 Alice 发送消息m给 Bob 时，Alice 执行如下：

(a)随机选取$r\in Z_p$，计算$\sigma_1=mZ^r$，$\sigma_2=g^r$。

(b)计算$\sigma_3=d_{A2}$。

(c)计算$\tau=H_1\left(\sigma_1,\sigma_2,\sigma_3,u'\prod_{i\in\mathcal{U}_A}u_i,\mathrm{pk}_B\right)$，且$\tau=\tau_1\tau_2\cdots\tau_n\in\{0,1\}^n$。

(d)计算$\sigma_4=d_{A1}\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^r$。

输出消息m的签密密文$\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$。

(5)Unsigncrypt：Bob 收到密文$\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$，执行以下步骤：

(a)计算$\tau=H_1\left(\sigma_1,\sigma_2,\sigma_3,u'\prod_{i\in\mathcal{U}_A}u_i,\mathrm{pk}_B\right)$，且$\tau=\tau_1\tau_2\cdots\tau_n\in\{0,1\}^n$。

(b)验证$e(\sigma_4,\ g)=e(g_1,g_2)e\left(u'\prod_{i\in\mathcal{U}_A}u_i,\sigma_3\right)\cdot e\left(v'\prod_{i=1}^n v_i^{\tau_i},\sigma_2\right)$是否成立；若成立，返回$m=\dfrac{\sigma_1}{e(\sigma_2,\mathrm{sk}_B)}$；否则，输出错误符号“⊥”。

4 安全性分析

4.1 正确性分析

(1)验证等式成立：

$$\begin{aligned}e(\sigma_4,g)&=e\left(d_{A1}\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^r,g\right)\\&=e\left(g_2^\alpha\left(u'\prod_{i\in\mathcal{U}_A}u_i\right)^{r_A}\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^r,g\right)\\&=e(g_2^\alpha,g)e\left(\left(u'\prod_{i\in\mathcal{U}_A}u_i\right)^{r_A},g\right)e\left(\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^r,g\right)\\&=e(g_1,g_2)e\left(u'\prod_{i\in\mathcal{U}_A}u_i,g^{r_A}\right)e\left(v'\prod_{i=1}^n v_i^{\tau_i},g^r\right)\\&=e(g_1,g_2)e\left(u'\prod_{i\in\mathcal{U}_A}u_i,\sigma_3\right)e\left(v'\prod_{i=1}^n v_i^{\tau_i},\sigma_2\right)\end{aligned}$$

(2) 恢复消息：

$$\frac{\sigma_1}{e(\sigma_2,\mathrm{sk}_B)}=\frac{mZ}{e(g^r,g_2^{r_B})}=\frac{me(h_1,g_2)^r}{e(h_1,g_2^r)}=m$$

4.2 安全性分析

为了证明本方案的安全性，首先我们引用由 Shoup[15]定义的“区分引理”，定义如下：

引理 1　若 E,E' 和 F 是概率空间上的事件，且 $\Pr[E\wedge\neg F]=\Pr[E'\wedge\neg F]$，则

$$|\Pr[E]-\Pr[E']|\leq\Pr[F]$$

定理 1　标准模型下，若 $(\varepsilon_{\mathrm{dbdh}},t)$-DBDH 假定成立，且 H_1 是 (ε_{H_1},t) 抗碰撞的 Hash 函数，则提出的异构签密方案是 (ε,t,q_u)-IND-IBC→PKI-CCA2 安全的，且 $\varepsilon\leq\varepsilon_{\mathrm{dbdh}}+\varepsilon_{H_1}+\dfrac{2q_u+1}{p}$，其中 t 是运行时间，q_u 是解签密询问的次数。

证明　首先 $\mathcal{B}$ 得到一个 DBDH 实例 (g,g^a,g^b,g^c,T)，$\mathcal{B}$ 利用 $\mathcal{A}$ 判断 $T=e(g,g)^{abc}$ 是否成立。

初始阶段　令 $l_u=2q_u$，且 $l_u(n+1)<p$，$\mathcal{B}$ 进行如下过程：

(1)随机选取整数 k_u，且 $0\leq k_u\leq n$；

(2)随机选取 $x',x_i\in Z_{l_u}$，$y',y_i\in Z_p,1\leq i\leq n$；

(3)计算 $v'=g_2^{-l_uk_u+x'}g^{y'}$，$v_i=g_2^{x_i}g^{y_i},1\leq i\leq n$；

(4)设置 $g_1=g^b,h_1^*=g^a$，计算 $Z^*=e(h_1^*,g_2)$，则接收者的公钥为 $\mathrm{pk}_B^*=(h_1^*,Z^*)$。

(5)定义 $\tau=\tau_1\tau_2\cdots\tau_n\in\{0,1\}^n$ 的函数：$F(\tau)=x'+\sum_{i=1}^n x_i\tau_i-l_uk_u$ 和 $J(\tau)=y'+\sum_{i=1}^n y_i\tau_i$，则 $v'\prod_{i=1}^n v_i^{\tau_i}=g_2^{F(\tau)}g^{J(\tau)}$。

$\mathcal{B}$ 将 $Pa=\{G,G_T,e,g,g_1,g_2,v',u',\boldsymbol{V},\boldsymbol{U},H_1\}$ 和 pk_B^* 发送给 $\mathcal{A}$。上述的公共参数与现实的公共参数具有相同的分布。

阶段 1　$\mathcal{A}$ 对 $\mathcal{B}$ 进行签密询问和解签密询问。

签密询问　$\mathcal{A}$ 提交消息 m 和一个接收者公钥 pk_w 进行签密询问。如果 pk_w 等于 pk_r 或者不合法，则返回错误符号“⊥”，否则执行正常签密操作。

解签密询问　$\mathcal{A}$ 对密文 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 进行解签密询问，$\mathcal{B}$ 首先检查 $\sigma_2=\sigma_2^*$ 是否成立。如果成立，$\mathcal{B}$ 终止；否则，$\mathcal{B}$ 执行以下步骤：

(1)计算 $\tau=H_1\left(\sigma_1,\sigma_2,\sigma_3,u'\prod_{i\in\mathcal{U}_A}u_i,\mathrm{pk}_B\right)$，$\tau=\tau_1\tau_2\cdots\tau_n\in\{0,1\}^n$；

(2) 验证 $e(\sigma_4,g)=e(g_1,g_2)e\left(u'\prod_{i\in\mathcal{U}_A}u_i,\sigma_3\right)\cdot e\left(v'\prod_{i=1}^n v_i^{\tau_i},\sigma_2\right)$ 是否成立；若不成立，$\mathcal{B}$ 拒绝并返回⊥；否则，$\mathcal{B}$ 执行下列步骤：

(a)若 $F(\tau)\neq 0\bmod p$，$\mathcal{B}$ 选取 $\beta\in Z_p$，计算 $d_1=h_1^{*\frac{-J(\tau)}{F(\tau)}}\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^{\beta}$，$d_2=h_1^{*\frac{-1}{F(\tau)}}g^{\beta}$，返回 $m=\dfrac{\sigma_1e(\sigma_4,d_2)}{e(\sigma_2,d_1)e(\mathrm{sk}_B,d_2)}$。设 $\overline{\beta}=\beta-\dfrac{a}{F(\tau)}$，因为

$$d_1=h_1^{*\frac{-J(\tau)}{F(\tau)}}\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^{\beta}=g_2^{x}\left(g_2^{F(\tau)}g^{J(\tau)}\right)^{\frac{-x}{F(\tau)}}\left(g_2^{F(\tau)}g^{J(\tau)}\right)^{\beta}$$

$$=g_2^{x}\left(g_2^{F(\tau)}g^{J(\tau)}\right)^{\beta-\frac{x}{F(\tau)}}=g_2^{x}\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^{\overline{\beta}}$$

$$d_2=h_1^{*\frac{-1}{F(\tau)}}g^{\beta}=g^{\beta-\frac{x}{F(\tau)}}=g^{\overline{\beta}}$$

所以

$$\frac{\sigma_1e(\sigma_4,d_2)}{e(\sigma_2,d_1)e(\mathrm{sk}_s,d_2)}=\frac{me(h_1^*,g_2)^re\left(d_1\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^r,g^{\overline{\beta}}\right)}{e\left(g^r,g_2^x\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^{\overline{\beta}}\right)e\left(d_1,g^{\overline{\beta}}\right)}$$

$$=\frac{me(g^x,g_2)^re\left(d_1,g^{\overline{\beta}}\right)e\left(\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^r,g^{\overline{\beta}}\right)}{e(g^r,g_2^x)e\left(g^r,\left(v'\prod_{i=1}^n v_i^{\tau_i}\right)^{\overline{\beta}}\right)e\left(d_1,g^{\overline{\beta}}\right)}=m$$

(b)若 $F(\tau)=0\bmod p$，模拟终止。

挑战阶段　$\mathcal{A}$ 输出两个消息 m_0，m_1 及挑战的身份 u_A^*。$\mathcal{B}$ 随机选择 $\delta\in\{0,1\}$ 对挑战密文做如下回应：$\mathcal{B}$ 首先运行 IBC-KG 计算 u_A^* 的私钥 $d_A^*=(d_{A1}^*,d_{A2}^*)$，然后计算 $\sigma_1^*=m_\delta T^*$，$\sigma_2^*=g^c,\sigma_3^*=d_{A2}^*$，$\tau^*=H_1\left(\sigma_1^*,\sigma_2^*,\sigma_3^*,u'\prod_{i\in\mathcal{U}_A^*}u_i,\mathrm{pk}_B^*\right)$，且 $\tau^*=\tau_1^*\tau_2^*\cdots\tau_n^*\in\{0,1\}^n$。若 $F(\tau)\neq 0\bmod l_u$，$\mathcal{B}$ 失败并停止；否则，计算 $\sigma_4^*=d_{A1}^*g^{cJ(\tau^*)}$。

阶段 2　$\mathcal{A}$ 进行同阶段 1 一样的签密询问和解签密询问，但不能对 σ^* 解签密询问。

猜测阶段　$\mathcal{A}$ 输出一个比特 $\delta'\in\{0,1\}$。若 $\delta=\delta'$，$\mathcal{B}$ 返回 1 表示 $T=e(g,g)^{abc}$；否则，返回 0 表示 $T\neq e(g,g)^{abc}$。

下面运用序列游戏的方法来分析 $\mathcal{B}$ 成功的概率。定义游戏 0 到游戏 5 的游戏，其中游戏 0 是最开始的攻击游戏。设 $E_i=\{\delta=\delta'|\text{游戏}i,0\leq i\leq 5\}$，因此，由 $\mathcal{A}$ 在游戏中成功的概率优势定义可知，$\mathrm{Adv}(\mathcal{A})=|\Pr[E_0]-1/2|$。

游戏 1　(在阶段 1 排除对 σ_2 正确的猜测) 在此游戏中，模拟游戏 0 在阶段 1 拒绝密文 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 的解签密询问。若 $\sigma_2=\sigma_2^*$，$\mathcal{B}$ 失败并停止。

由于 $\mathcal{A}$ 在挑战密文 σ^* 中没有 $\sigma_2=\sigma_2^*$ 的信息，因此给敌手 $\mathcal{A}$ 提交这种类型密文的概率是 q_u/p。从而由引理 1: $\left|\Pr[E_1]-\Pr[E_0]\right|\le q_u/p$。

游戏 2 (排除 H_1 的碰撞) 在此游戏中，模拟游戏 1 拒绝密文 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 及发送者身份 u_A^* 的解签密询问。若 $\sigma_4{=}\sigma_4^*,(\sigma_1,\sigma_2,\sigma_3)\ne(\sigma_1^*,\sigma_2^*,\sigma_3^*)$, $\tau=\tau^*$，其中 $\tau=H_1\left(\sigma_1,\sigma_2,\sigma_3,u'\prod_{i\in\mathcal{U}_A^*}u_i,\mathrm{pk}_B^*\right)$，$\mathcal{B}$ 失败并停止。拒绝的概率是可忽略的，ε_{H_1} 为 $\left(\sigma_1,\sigma_2,\sigma_3,u'\prod_{i\in\mathcal{U}_A^*}u_i,\mathrm{pk}_B^*\right)\ne\left(\sigma_1^*,\sigma_2^*,\sigma_3^*,u'\prod_{i\in\mathcal{U}_A^*}u_i,\mathrm{pk}_B^*\right)$ 时 $\tau=\tau^*$ 的概率。从而由引理 1：

$$\left|\Pr[E_2]-\Pr[E_1]\right|\le\varepsilon_{H_1}$$

游戏 3 (在阶段 1 排除 $F(\tau)=0\bmod p$)在此游戏中，模拟游戏 2 拒绝密文 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 在阶段 1 的解签密询问。若 $F(\tau)=0\bmod p$，$\mathcal{B}$ 失败并停止。因为给敌手 $\mathcal{A}$ 提交这一类型的密文概率是 q_u/p。从而由引理 1: $\left|\Pr[E_3]-\Pr[E_2]\right|\le q_u/p$。

游戏 4 (在挑战阶段排除 $F(\tau^*)\ne0\bmod l_u$) 在此游戏中，模拟游戏 3 在挑战阶段对消息 m_0，m_1 及发送者的身份 u_A^* 拒绝挑战。若 $F(\tau^*)=0\bmod l_u$，$\mathcal{B}$ 失败并停止。因为给敌手 $\mathcal{A}$ 提交 m_0，m_1 及发送者身份 u_A^* 的概率至多是 $1/p$。从而由引理 1：

$$\left|\Pr[E_4]-\Pr[E_3]\right|\le1/p$$

游戏 5 (模拟挑战密文) 在此游戏中，模拟游戏 4 在挑战阶段用 σ_1^* 代替 $m_\delta T$ $(T\in G_T)$。由于 $m_\delta T$ 与 δ 是独立的，敌手 $\mathcal{A}$ 没有 δ 的信息，因此 $\left|\Pr[E_5]\right|{=}1/2$。除非敌手 $\mathcal{A}$ 能够区分 $e(g,g)^{abc}$ 和 T，否则游戏 4 和游戏 5 是相同的。从而由引理 1：

$$\left|\Pr[E_5]-\Pr[E_4]\right|\le\varepsilon_{\mathrm{dbdh}}$$

综上：$\varepsilon\le\varepsilon_{\mathrm{dbdh}}+\varepsilon_{H_1}+(2q_u+1)/p$。 证毕

定理 2 标准模型下，若敌手 $\mathcal{F}$ 能以不可忽略的优势 ε 攻破 EUF-IBC→PKI-CMA 的安全性，则存在算法 $\mathcal{B}$ 能够以 $\varepsilon'>\dfrac{\varepsilon}{4l_ul_m(n_u+1)(n+1)}$ 的优势解决 CDH 问题，其中 q_k,q_s 表示至多进行 q_k 次密钥提取询问和 q_s 次签密询问。

证明 首先，$\mathcal{B}$ 得到一个 CDH 问题的实例 (g,g^a,g^b)，$\mathcal{B}$ 将利用 $\mathcal{F}$ 计算出 g^{ab}。

初始阶段 令 $l_u=2q_s,l_m=2(q_s+q_k)$，且 $l_u(n+1)<p,l_m(n_m+1)<p$。$\mathcal{B}$ 进行如下过程：

(1)随机选取整数 k_m,k_u，满足 $0\le k_u\le n,\ 0\le k_m\le n_u$；

(2)随机选取 $x',x_i\in Z_{l_u},1\le i\le n$，$z',z_i\in Z_{l_m}$, $1\le i\le n_m$；

(3)随机选取 $y',c',y_i,c_j\in Z_p,\ 1\le i\le n,\ 1\le j\le n_m$；

(4)设置 $g_1=g^a,\ g_2=g^b,\ u'=g_2^{-l_mk_m+z'}g^{c'},\ v'=g_2^{-l_uk_u+x'}g^{y'}$；

(5)计算 $v_i=g_2^{x_i}g^{y_i},\ 1\le i\le n$ 和 $u_j=g_2^{z_j}g^{c_j}$, $1\le j\le n_m$；

(6)定义函数：

$F(\tau)=x'+\sum_{i=1}^n x_i\tau_i-l_uk_u$，$J(\tau)=y'+\sum_{i=1}^n y_i\tau_i$，$K(u)=z'+\sum_{j\in\mathcal{U}}z_j-l_mk_m$ 和 $L(u)=c'+\sum_{j\in\mathcal{U}}c_j$，则 $u'\prod_{i\in\mathcal{U}}u_i=g_2^{K(u)}g^{L(u)}$ 和 $v'\prod_{i=1}^n v_i^{\tau_i}=g_2^{F(\tau)}g^{J(\tau)}$。

$\mathcal{B}$ 运行 PKI-KG 生成发送者的公私钥对 $(\mathrm{pk}_B^*,\mathrm{sk}_B^*)$，并将系统参数 $Pa=\{G,G_T,e,g,g_2,v',u',\boldsymbol{V},\boldsymbol{U},H_1\}$ 和 $(\mathrm{pk}_B^*,\mathrm{sk}_B^*)$ 给 $\mathcal{F}$。

密钥提取询问 $\mathcal{F}$ 对身份 u 进行密钥询问，$\mathcal{B}$ 执行以下过程：

(1)若 $K(u)=0\bmod l_m$，$\mathcal{B}$ 终止；

(2)若 $K(u_A)\ne0\bmod l_m$，$\mathcal{B}$ 选取 $r_u\in Z_p$，计算

$$d_u=(d_{u1},d_{u2})=\left(g_2^{\frac{-L(u)}{K(u)}}\left(u'\prod_{i\in\mathcal{U}}u_i\right)^{r_u},g_2^{\frac{-1}{K(u)}}g^{r_u}\right)$$

返回 $d_u=(d_{u1},d_{u2})$ 给 $\mathcal{F}$。设 $\tilde{r}_u=r_u-a/K_u$，则 d_u 是 u 有效的私钥。因为

$$\begin{aligned}d_{u1}&=g_1^{\frac{-L(u)}{K(u)}}\left(u'\prod_{i\in\mathcal{U}}u_i\right)^{r_u}\\&=g_2^a\left(g_2^{K(u)}g^{L(u)}\right)^{\frac{-a}{K(u)}}\left(g_2^{K(u)}g^{L(u)}\right)^{r_u}\\&=g_2^a\left(g_2^{K(u)}g^{L(u)}\right)^{r_u-\frac{a}{K(u)}}=g_2^a\left(u'\prod_{i\in\mathcal{U}}u_i\right)^{\tilde{r}_u},\\d_{u2}&=g_1^{\frac{-1}{K(u)}}g^{r_u}=g^{r_u-\frac{a}{K(u)}}=g^{\tilde{r}_u}\end{aligned}$$

签密询问 $\mathcal{F}$ 对 (m,u_A,pk_B) 进行签密询问。若 $K(u_A)\ne0\bmod l_m$，$\mathcal{B}$ 首先运行 IBC-KG 计算 u_A 的私钥 d_A，然后随机选取 $r\in Z_p$，计算 $\sigma_1=m.Z^r$, $\sigma_2=g^r,\sigma_3=d_{A2}$，$\tau=H_1(\sigma_1,\sigma_2,\sigma_3,u'\prod_{i\in\mathcal{U}_A}u_i,\mathrm{pk}_B)$，$\sigma_4=d_{A1}g^{rJ(\tau)}$。$\mathcal{B}$ 将 $\sigma{=}(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 给 $\mathcal{F}$。否则，$\mathcal{B}$ 终止。

解签密询问 $\mathcal{F}$ 对 $(\sigma,u_A,\mathrm{pk}_B)$ 进行解签密询问。$\mathcal{B}$ 判定 $F(\tau)\ne0\bmod p$ 是否成立，若成立，$\mathcal{B}$ 选择接收者身份 u_B，计算 u_B 的私钥 sk_B，然后执行解签密算法的验证部分，若验证不成立，输出符号 $\perp$；否则返回消息 m。

伪造阶段 $\mathcal{F}$ 提交消息 m^*，发送者的身份 u_A^*，接收者公钥 pk_B^* 及伪造的有效签名 $(\sigma_2^*,\sigma_3^*,\sigma_4^*)$，其中 $\tau^*=H_1\left(\sigma_1^*,\ \sigma_2^*,\ \sigma_3^*,\ u'\prod_{i\in\mathcal{U}_A^*}u_i,\ \mathrm{pk}_B^*\right)$。若 $K(u_A^*)\ne0\bmod l_m,F(\tau^*)\ne0\bmod p$，$\mathcal{B}$ 失败并停止；若

$K(u_A^*)=0 \bmod l_m, F(\tau^*)=0 \bmod p$ ， $\mathcal{B}$ 得出 CDH 问题的解：

$$\frac{\sigma_4^*}{\sigma_3^{*L(u_A^*)}\sigma_2^{*J(\tau^*)}}=\frac{g_2^a\left(u'\prod_{i\in\mathcal{U}_A^*}u_i\right)^{r_A^*}\left(v'\prod_{i=1}^{n}v_i^{\tau_i^*}\right)^{r*}}{g^{r_A^*L(u_A^*)}g^{r^*J(\tau^*)}}=g^{ab}$$

以下分析 $\mathcal{F}$ 不终止的概率。$\mathcal{F}$ 模拟不终止的情况有 3 种：在对身份 u 进行密钥提取询问时 $K(u)\neq 0 \bmod l_m$；在对 (u_A, pk_B, m) 进行签密询问时 $K(u_A)\neq 0 \bmod l_m$；在对消息 m^* 进行伪造时 $K(u_A^*)=0 \bmod l_m, F(\tau^*)=0 \bmod p$。因此， $\mathcal{B}$ 解决 CDH 问题的优势为：$\varepsilon'>\dfrac{\varepsilon}{4l_u l_m(n_u+1)(n+1)}$。证毕

4.3 效率分析

根据已有文献，目前没有在标准模型下 IBC→PKI 的异构签密方案。因此，本文方案与已有标准模型下的签密方案进行比较。表 1 从理论上分析文献[9]、文献[10]和本文方案的计算成本和通信成本(密文长度)，其中， P, M, E 分别表示对运算、乘法运算和指数运算，$|\Delta|$表示 Δ 中元素的长度。

其次，本文通过实验仿真分析了方案具体的计算成本和通信成本。本次仿真是在LINUX平台上进行，使用PBC函数库，用C语言编程，主机CPU主频2.9 GHz，内存4 G。采用类型A的配对，其构造在有限域 F_q 中椭圆曲线 $y^2=x^3+x$ 上，基域$|q|=512$ bit，素数$|p|=1024$ bit。由于文献[9]和文献[10]在签密和解签密阶段所需的对运算一样，所以表2仅给出文献[9]和本文所提方案的具体计算成本。根据仿真的结果，在签密和解签密阶段，本方案需要8.404 ms 和18.655 ms，文献[9]需要14.608 ms和21.039 ms。表 3 给出文献[9]、文献[10]和本文方案的具体通信成本，其中文献[9]的密文长度为660 Byte，文献[10]的密文长度为640 Byte，本方案的密文长度为512 Byte。因此，本文方案在计算成本和密文长度上具有更大的优势。

表 1 方案的性能分析

方案	签密	解签密	密文长度
文献[9]	$6M+6E+1P$	$8M+3E+6P$	$\|G_T\|+4\|G\|+\|p\|$
文献[10]	$3M+5E+1P$	$6M+3E+5P$	$\|G_T\|+4\|G\|$
本文方案	$4M+3E$	$7M+3E+5P$	$\|G_T\|+3\|G\|$

表 2 方案的计算成本(ms)

方案	签密运行时间	解签密运行时间	算法运行时间
文献[9]	14.608	21.039	84.375
本文方案	8.404	18.665	74.127

表 3 方案的通信成本(Byte)

方案	文献[9]	文献[10]	本文方案
密文长度	660	640	512

5 结束语

随着 5G 网络的发展，异构网络通信将变得越来越重要。针对跨域通信的安全需求，本文提出一个在标准模型下异构签密方案，并在困难问题下证明了本文方案的安全性。该方案与已有的方案相比较，密文长度较短，在签密阶段不需要对运算。本文所提的异构签密方案以更低的开销达到较高的安全性。

参 考 文 献

[1] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption)<<cost(signature)+cost (encryption)[C]. Proceedings of the Cryptology-CRYPTO1997, California, USA, 1997: 165–179. doi: 10.1007/BFb0052234.

[2] PAN Chunhua, LI Shunpeng, ZHU Qihui, *et al*. Notes on proxy signcryption and multi-proxy signature schemes[J]. *International Journal of Network Security*, 2015, 17(1): 29–33.

[3] 项顺伯, 徐兵, 柯文德. 基于身份的在线/离线广播签密方案[J]. 四川大学学报(工程科学版), 2016, 48(2): 156–161. doi: 10.1007/BFb0052234.10.15961/j.jsuese.2016.02.023.
XIANG Shunbo, XU Bing, and KE Wende. Identity-based online /offline broadcast signcryption scheme[J]. *Journal of Sichuan University* (*Engineer Science*), 2016, 48(2): 156–161. doi: 10.1007/BFb0052234.10.15961/j.jsuese.2016.02.023.

[4] 李慧贤, 巨龙飞. 对一个匿名多接收者签密方案的安全性分析与改进[J]. 电子学报, 2015, 43(11): 2187–2193. doi:10.3969/j. issn.0372-2112.2015.11.008.
LI Huixian and JU Longfei. Security analysis and improvement of an anonymous multi-receiver signcryption scheme[J]. *Acta Electronica Sinica*, 2015, 43(11): 2187–2193. doi: 10.3969/j.issn.0372-2112.2015.11.008.

[5] 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.

[6] 刘雪峰, 张玉清, 王鹤, 等. 一种后向撤销隐私安全的车载自组织网络快速匿名消息认证协议[J]. 电子与信息学报, 2014, 36(1): 94–100. doi: 10.3724/SP.J.1146.2013.00342.
LIU Xuefeng, ZHANG Yuqing, WANG He, *et al*. An efficient anonymity message authentication with backward secure revocation for vehicular Ad hoc networks[J]. *Journal of Electronics & Information Technology*, 2014, 36(1): 94–100. doi: 10.3724/SP.J.1146.2013.00342.

[7] 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.

[8] TAN C. Signcryption scheme in multi-user setting without random oracles[C]. Proceedings of the 3rd International Workshop on Security, Kagawa, Japan, 2008: 64–82. doi: 10.1007/978-3-540-89598-5_5.

[9] LI Fageng and TAKAGI T. Secure identity-based signcryption in the standard model[J]. *Mathematical & Computer Modelling*, 2013, 57(11/12): 2685–2694. doi: 10.1016/j.mcm.2011.06.043.

[10] LI Xiangxue, QIAN Haifeng, WENG Jian, *et al*. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model[J]. *Mathematical & Computer Modelling*, 2013, 57(3/4): 503–511. doi: 10.1016/j.mcm.2012.06.030.

[11] LI Fageng, ZHANG Mingwu, and TSUYOSHI T. Efficient signcryption in the standard model[J]. *Concurrency & Computation Practice & Experience*, 2012, 24(17): 1977–1989. doi: 10.1002/cpe.1823.

[12] 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.

[13] HUANG Qiong, DUN C, and YAN Guomin. Heterogeneous signcryption with key privacy[J]. *Computer Journal*, 2011, 54(4): 525–536. doi: 10.1093/comjnl/bxq095.

[14] LI Fageng, 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.

[15] SHOUP V. OAEP Reconsidered[J]. *Journal of Cryptology*, 2000, 15(4): 223–249. doi: 10.1007/3-540-44647-8_15.

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.

李亚红： 女， 1984 年生，博士生，研究方向为密码学与信息安全.

张玉磊： 男， 1979 年生，副教授，硕士生导师，研究方向为密码学与信息安全.

牛淑芬： 女， 1976 年生，副教授，硕士生导师，研究方向为密码学与信息安全.