可证安全的无证书混合签密

俞惠芳[1),2)] 杨 波[1)]

[1)](陕西师范大学计算机科学学院 西安 710062)

[2)](青海师范大学计算机学院 西宁 810008)

摘 要 混合签密能够处理任意长度的消息,而公钥签密则不能.文中将混合签密技术扩展到无证书环境,构建了一个可证明安全的无证书混合签密方案.随机预言模型下,作者证明,所提方案在双线性Diffie-Hellman问题和计算性Diffie-Hellman问题的难解性下,满足自适应选择密文攻击下的不可区分性和自适应选择消息攻击下的不可伪造性.文中方案计算复杂度低,适合于实际应用.

关键词 无证书密码学;混合签密;可证安全性;双线性对;密码学

中图法分类号 TP309 **DOI号** 10.3724/SP.J.1016.2015.00804

Provably Secure Certificateless Hybrid Signcryption

YU Hui-Fang[1),2)] YANG Bo[1)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710062)

[2)](*School of Computer, Qinghai Normal University, Xining* 810008)

Abstract Hybrid signcryption can process the messages of arbitrary length, while public key signcryption cannot. In this paper, we extend hybrid signcryption technique to the certificateless setting, and construct a provably secure certificateless hybrid signcryption (PS-CLHS) scheme. In the random oracle model, we prove that the proposed scheme satisfies the indistinguishability against adaptive chosen-ciphertext attacks and unforgeability against adaptive chosen-message attacks under the hardness of the bilinear Diffie-Hellman problem and computational Diffie-Hellman problem. In addition, this scheme has lower computational complexity and is appropriate to applications in practice.

Keywords certificateless cryptography; hybrid signcryption; provable security; bilinear pairing; cryptography

1 引 言

公钥密码是一种实现网络和信息安全的重要技术.传统公钥密码要求认证机构颁发证书来绑定用户的身份和公钥,这样就带来了证书管理问题.一旦用户量剧增,证书管理问题就会极大地影响系统性能.为了简化证书的管理,降低额外的计算开销,Shamir[1]提出了基于身份的公钥密码学概念.按照Shamir思想,用户不是自己生成公钥和私钥,而是选择其公开身份信息作为公钥,私钥生成中心用这些公开身份信息为用户计算出相应私钥.为了解决身份密码学中的密钥托管问题和传统公钥基础设施中的证书管理问题,2003年的亚密会上Al-Riyami

收稿日期:2013-11-26;最终修改稿收到日期:2014-11-15.本课题得到国家自然科学基金(61363080,61272436)、教育部春晖计划项目(Z2012094)、广东省自然科学基金项目(10351806001000000)资助.**俞惠芳**,女,1972年生,博士研究生,副教授,硕士生导师,中国计算机学会(CCF)高级会员,主要研究领域为密码学、信息安全.E-mail:yuhuifang@qhnu.edu.cn.**杨 波**,男,1963年生,博士,教授,博士生导师,主要研究领域为密码学、信息安全.

和 Paterson[2] 提出无证书密码学，减少了对密钥生成中心（Key Generation Center，KGC）的信任，KGC 生成用户的部分私钥，用户的完整私钥由这个部分私钥和用户自己随机选取的秘密值构成，而用户公钥由用户自己计算得出. 构造无证书的密码方案[3-5]一直是密码学界感兴趣的研究方向.

加密任意长度的消息时，通常的公钥加密限制了其消息空间. Cramer 等人[6]构造的混合加密能够实现大消息的保密通信. 一个混合加密方案包含两部分：密钥封装机制（Key Encapsulation Mechanism，KEM）和数据封装机制（Data Encapsulation Mechanism，DEM），KEM 运用非对称技术加密一个对称密钥，而 DEM 利用对称技术和这个对称密钥加密任意长度的消息. KEM 和 DEM 是完全独立的两个模块，因而可以被分别研究. 混合密码学[7-10]能够顾及到密码学应用中的安全性和高效性，是 IND-CCA2 安全的公钥密码机制的通用解决方法. 2005 年，Dent[11-12]将 KEM-DEM 混合结构扩展到签密环境，提出混合签密的概念. 后来，Tan[13]构造了标准模型下的签密 KEM 和签密 tag-KEM. 2011 年，Sun 等人[14]提出了基于身份的多接收者签密 KEM. 2013 年，Li 等人[15]给出了一个内部安全的无证书混合签密方案. 可以说，设计安全高效的无证书混合签密方案是值得研究的重要问题.

本文构造出随机预言模型下可证安全的无证书混合签密（PS-CLHS），PS-CLHS 包含一个无证书签密 KEM（Certificateless Signcryption KEM，CLS-KEM）和一个 DEM. PS-CLHS 的 IND-CCA2 安全性和 sUF-CMA 安全性可规约为双线性 Diffie-Hellman 问题和计算性 Diffie-Hellman 问题的难解性. PS-CLHS 方案不仅计算复杂度低，而且安全实用.

本文第 2 节介绍双线性映射和一些密码学假设，描述 CLS-KEM、DEM 和 PS-CLHS 的定义以及 PS-CLHS 的安全模型；第 3 节具体描述本文方案；第 4 节分析本文方案的安全结果；第 5 节对本文方案与同类方案进行性能比较；最后一节总结全文.

2　预备知识

2.1　双线性映射

G_1 是一个阶为素数 q 的加法群，G_2 为相同阶的乘法群. P 是 G_1 的本原根. $e: G_1 \times G_1 \to G_2$ 是具有以下性质的双线性映射.

（1）双线性. $\forall a, b \in Z_q^*$，$e(aP, bP) = e(P, P)^{ab}$.

（2）非退化性. $e(P, P) \neq 1_{G_2}$.

（3）可计算性. $\forall P, Q \in G_1$，存在一个有效算法计算 $e(P, Q)$.

2.2　复杂性假设

Bilinear Diffie-Hellman（BDH）问题. 已知 $(P, aP, bP, cP) \in G_1$，对于任意未知的 $a, b, c \in Z_q^*$，计算 $e(P, P)^{abc} \in G_2$.

Decisional Bilinear Diffie-Hellman（DBDH）问题. 已知 $(P, aP, bP, cP) \in G_1$ 和 $z \in G_2$，对于任意未知的 $a, b, c \in Z_q^*$，判定 $e(P, P)^{abc} = z$ 是否成立？若成立，O_{DBDH} 返回 1；否则，O_{DBDH} 返回 0.

Computational Diffie-Hellman（CDH）问题. 已知 $(P, aP, bP) \in G_1$，对于任意未知的 $a, b \in Z_q^*$，计算 $abP \in G_1$.

2.3　CLS-KEM[14]

一个 CLS-KEM 方案可以通过下面 6 个概率多项式时间算法来定义.

Setup：这个算法输入安全参数 k，输出系统参数 $params$ 以及主密钥 x.

Extract-Partial-Private-Key：这个算法输入系统参数 $params$、主控钥 x 和用户身份 $u_i \in \{0,1\}^*$，输出该用户部分私钥 d_i.

Generate-User-Key：这个算法输入用户身份 $u_i \in \{0,1\}^*$，输出秘密值 x_i 和用户公钥 P_i.

Extract-Private-Key：这个算法输入部分私钥 d_i 和秘密值 x_i，输出完整私钥 $s_i = (x_i, d_i)$.

Encap：这个算法输入系统参数 $params$、发送者的身份 u_A 和公私钥对 (P_A, s_A)、接收者的身份 u_B 和公钥 P_B，输出对称密钥 κ 和密钥封装 ϕ.

Decap：这个算法输入系统参数 $params$、密钥封装 ϕ、发送者的身份 u_A 和公钥 P_A、接收者的身份 u_B 和公私钥对 (P_B, s_B)，输出对称密钥 κ 或表示解封装失败的标志 $\perp$.

2.4　DEM[15]

DEM 包含下面两个概率多项式时间算法.

Enc：这个算法输入安全参数 k、消息 m 和对称密钥 κ，输出密文 c.

Dec：这个算法输入对称密钥 κ 和密文 c，输出明文 m 或符号 $\perp$.

2.5　PS-CLHS

PS-CLHS 由 CLS-KEM 和 DEM 两个方案组成，算法细节如下所述.

Setup：与 CLS-KEM 方案相同.

Extract-Partial-Private-Key：与 CLS-KEM 方案相同.

Generate-User-Key：与 CLS-KEM 方案相同.

Extract-Private-Key：与 CLS-KEM 方案相同.

Signcrypt：已知($params$, u_A, u_B, m, s_A, P_A, P_B)，发送者通过以下步骤生成密文 σ.

(1) 利用 2.3 节 Encap 算法计算(κ,ϕ).

(2) 利用 2.4 节 Enc 算法计算密文 c.

(3) 输出 $\sigma \leftarrow (c,\phi)$.

Unsigncrypt：已知($params$, u_A, u_B, σ, s_B, P_A, P_B)，接收者执行如下步骤.

(1) 利用 2.3 节 Decap 算法计算 κ.

(2) 利用 2.4 节 Dec 算法恢复消息 m.

(3) 检查验证等式是否成立？若成立，接受明文 m；否则，输出符号 $\perp$.

2.6 PS-CLHS 的安全模型

PS-CLHS 方案应该满足 IND-CCA2 安全性和 sUF-CMA 安全性. PS-CLHS 的安全模型中，我们考虑两类攻击者. 第 1 类攻击者 $\mathcal{A}_{\mathrm{I}}$ 或 $\mathcal{F}_{\mathrm{I}}$ 不知道 KGC 的主控钥，但能够自适应地替换任意用户的公钥. 第 2 类攻击者 $\mathcal{A}_{\mathrm{II}}$ 或 $\mathcal{F}_{\mathrm{II}}$ 知道 KGC 的主控钥，但不具备替换任意用户公钥的能力.

定义 1. 如果任何多项式有界的敌手 $\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$ 赢得 IND-CCA2-I 和 IND-CCA2-II 的优势是可忽略的，则称一个 PS-CLHS 方案具有自适应选择密文攻击下的不可区分性.

IND-CCA2-I：这是一个挑战者 Γ 和敌手 $\mathcal{A}_{\mathrm{I}}$ 之间进行的交互游戏.

初始化. Γ 运行系统初始化算法产生系统参数 $params$ 和主控钥 x，返回 $params$ 给 $\mathcal{A}_{\mathrm{I}}$，保留 x.

阶段 1. $\mathcal{A}_{\mathrm{I}}$ 在这个阶段进行如下多项式有界次适应性询问.

公钥询问：收到任意身份的公钥询问时，Γ 运行用户钥生成算法，返回公钥 P_i.

部分私钥询问：收到任意身份的部分私钥询问时，Γ 运行部分私钥提取算法，返回部分私钥 d_i.

私钥询问：收到任意身份的私钥询问时，Γ 从相关“询问与应答”表中找到含有完整私钥的条目，返回完整私钥 $s_i \leftarrow (x_i, d_i)$. 如果公钥已被替换，不允许 $\mathcal{A}_{\mathrm{I}}$ 询问秘密值.

公钥替换：$\mathcal{A}_{\mathrm{I}}$ 可以在指定范围内选择任意值，替换任何用户的公钥.

签密询问：收到消息 m 在发送者身份 u_A 和接收者身份 u_B 下的签密询问时，Γ 从相关“询问与应答”表中检索到(s_A, P_A, P_B)，并返回

$\sigma \leftarrow Signcrypt(params, u_A, u_B, m, s_A, P_A, P_B)$.

解签密询问：收到密文 σ 在发送者身份 u_A 和接收者身份 u_B 下的解签密询问时，Γ 从相关“询问与应答”表中检索到(s_B, P_A, P_B)，并返回

$m/\perp \leftarrow Unsigncrypt(params, u_A, u_B, \sigma, s_B, P_A, P_B)$.

挑战. 阶段 1 结束后，$\mathcal{A}_{\mathrm{I}}$ 生成两个相同长度的明文 m_0, m_1 以及希望挑战的两个身份(u_A^*, u_B^*)，这里 u_A^* 和 u_B^* 分别是发送者和接收者的身份. 阶段 1 期间，u_B^* 的秘密值和部分私钥不能被询问，并且 u_B^* 不能是公钥已被替换的那个身份. Γ 从相关“询问与应答”表中找到(s_A^*, P_A^*, P_B^*)，选择 $\gamma \in_R \{0,1\}$，计算 $\sigma^* \leftarrow Signcrypt(params, u_A^*, u_B^*, m_\gamma, s_A^*, P_A^*, P_B^*)$，返回挑战密文 σ^*.

阶段 2. $\mathcal{A}_{\mathrm{I}}$ 像阶段 1 那样进行多项式有界次适应性询问. 约束条件是：(1) u_B^* 的完整私钥不能被询问；(2) u_B^* 不能是公钥已被替换的那个身份；(3) 不能对 u_A^* 和 u_B^* 下的 σ^* 进行解签密询问.

猜测. $\mathcal{A}_{\mathrm{I}}$ 输出一个猜测 γ^*. 若 $\gamma^* = \gamma$，$\mathcal{A}_{\mathrm{I}}$ 赢得 IND-CCA2-I. 我们定义 $\mathcal{A}_{\mathrm{I}}$ 的获胜优势为

$$Adv_{\mathcal{A}_{\mathrm{I}}}^{\text{IND-CCA2-I}} = |2Pr[\gamma^* = \gamma] - 1|.$$

IND-CCA2-II：这是一个挑战者 Γ 和敌手 $\mathcal{A}_{\mathrm{II}}$ 之间进行的交互游戏.

初始化. Γ 运行系统初始化算法产生系统参数 $params$ 以及主控钥 x，返回($params$, x)给 $\mathcal{A}_{\mathrm{II}}$.

阶段 1. $\mathcal{A}_{\mathrm{II}}$ 在这个阶段进行多项式有界次适应性询问. 除了不需要进行部分私钥询问和公钥替换询问之外，公钥询问、私钥询问、签密询问和解签密询问类似于 IND-CCA2-I 的阶段 1. 需要注意的是，由于 $\mathcal{A}_{\mathrm{II}}$ 知道主控钥 x，自己能够计算出用户的部分私钥.

挑战. 阶段 1 结束以后，$\mathcal{A}_{\mathrm{II}}$ 生成两个相同长度的明文 m_0, m_1 以及希望挑战的两个身份(u_A^*, u_B^*)，这里 u_A^* 和 u_B^* 分别是发送者和接收者的身份. 阶段 1 期间，u_B^* 的秘密值不能被询问. Γ 从相关“询问与应答”表中找到(s_A^*, P_A^*, P_B^*)，选择 $\gamma \in_R \{0,1\}$，计算 $\sigma^* \leftarrow Signcrypt(params, u_A^*, u_B^*, m_\gamma, s_A^*, P_A^*, P_B^*)$，返回挑战密文 σ^*.

阶段 2. $\mathcal{A}_{\mathrm{II}}$ 像阶段 1 那样进行多项式有界次适应性询问. 约束条件是：(1) u_B^* 的秘密值不能被询问；(2) 不能对 u_A^* 和 u_B^* 下的 σ^* 进行解签密询问.

猜测. $\mathcal{A}_{\mathrm{II}}$ 输出一个猜测 γ^*. 若 $\gamma^* = \gamma$，$\mathcal{A}_{\mathrm{II}}$ 赢得 IND-CCA2-II. 我们定义 $\mathcal{A}_{\mathrm{II}}$ 的获胜优势为

$$Adv_{\mathcal{A}_{\mathrm{II}}}^{\text{IND-CCA2-II}}=|2Pr[\gamma^*=\gamma]-1|.$$

定义 2. 如果任何多项式有界的伪造者$\mathcal{F}_{\mathrm{I}}$和$\mathcal{F}_{\mathrm{II}}$赢得 sUF-CMA-I 和 sUF-CMA-II 的优势是可忽略的，则称一个 PS-CLHS 方案在自适应选择明文攻击下是不可伪造的.

sUF-CMA-I：这是一个挑战者 Γ 和伪造者$\mathcal{F}_{\mathrm{I}}$之间进行的交互游戏.

初始化. Γ 运行系统初始化算法产生系统参数 $params$ 和主控钥 x，返回 $params$ 给$\mathcal{F}_{\mathrm{I}}$，保留 x.

训练. $\mathcal{F}_{\mathrm{I}}$进行适应性多项式有界次询问. 进行的询问与 IND-CCA2-I 的阶段 1 相同.

伪造. 训练阶段结束的时候，$\mathcal{F}_{\mathrm{I}}$输出一个伪造(σ^*,u_A^*,u_B^*). 训练期间，$\mathcal{F}_{\mathrm{I}}$不能询问 u_A^* 的部分私钥和秘密值，u_A^* 不能是公钥已被替换的那个身份. 此外，σ^* 不能是来自伪造者对 u_A^* 和 u_B^* 下的某个消息 m^* 的签密询问的应答. 如果

$$Unsigncrypt(params,u_A^*,u_B^*,\sigma^*,s_B^*,P_A^*,P_B^*)$$

不是符号$\perp$，$\mathcal{F}_{\mathrm{I}}$赢得 sUF-CMA-I.

$\mathcal{F}_{\mathrm{I}}$获胜的优势定义为

$$Adv_{\mathcal{F}_{\mathrm{I}}}^{\text{sUF-CMA-I}}=Pr[win].$$

sUF-CMA-II：这是一个挑战者 Γ 和伪造者$\mathcal{F}_{\mathrm{II}}$之间进行的交互游戏.

初始化. Γ 运行系统初始化算法产生系统参数 $params$ 以及主控钥 x，返回$(params,x)$给$\mathcal{F}_{\mathrm{II}}$.

训练. $\mathcal{F}_{\mathrm{II}}$自适应地进行多项式有界次询问. 进行的询问类似于 IND-CCA2-II 的阶段 1.

伪造. 训练阶段结束的时候，$\mathcal{F}_{\mathrm{II}}$输出一个伪造$(\sigma^*,u_A^*,u_B^*)$. 训练期间，$\mathcal{F}_{\mathrm{II}}$不能询问 u_A^* 的秘密值，并且 σ^* 不能是来自伪造者对 u_A^* 和 u_B^* 下的某个消息 m^* 的签密询问的应答. 如果

$$Unsigncrypt(params,u_A^*,u_B^*,\sigma^*,s_B^*,P_A^*,P_B^*)$$

不是符号$\perp$，$\mathcal{F}_{\mathrm{II}}$赢得 sUF-CMA-II.

$\mathcal{F}_{\mathrm{II}}$获胜的优势定义为

$$Adv_{\mathcal{F}_{\mathrm{II}}}^{\text{sUF-CMA-II}}=Pr[win].$$

3　具体方案

3.1　Setup

令 G_1 和 G_2 分别是素数阶 $q\geq 2^k$（k 是安全参数）的加法群和乘法群，P 是 G_1 的一个生成元，$e:G_1\times G_1\rightarrow G_2$ 是个双线性映射. KGC 定义 3 个密码学 Hash 函数：$h_1:\{0,1\}^*\rightarrow G_1$，$h_2:G_2^2\times G_1\rightarrow\{0,1\}^n$和 $h_3:\{0,1\}^{*2}\times\{0,1\}^n\times G_1^3\rightarrow G_1$，这里 n 是 DEM 的密钥长度. 然后，KGC 选择 $x\in_R Z_q^*$ 作为主控钥，计算系统公钥 $P_{\mathrm{pub}}=xP$. 最后，KGC 保密主控钥 x，公布系统参数

$$params=(G_1,G_2,e,P,P_{\mathrm{pub}},n,h_1,h_2,h_3).$$

3.2　Extract-Partial-Private-Key

给定 $params$、系统主控钥 x 和用户身份 u_i，KGC 计算 $H_i=h_1(u_i)$，设置用户的部分私钥 $d_i=xH_i$，并发送(u_i,d_i)给用户.

3.3　Generate-User-Key

给定用户身份 u_i，该用户随机选择一个秘密值 $x_i\in Z_q^*$，计算公钥 $P_i=x_iP$.

3.4　Generate-User-Key

给定部分私钥 d_i和秘密值 x_i，这个算法设置完整私钥 $s_i\leftarrow(x_i,d_i)$.

3.5　Signcrypt

给定$(params,u_A,u_B,m,s_A,P_A,P_B)$，发送者通过以下步骤生成密文.

(1) 选择 $r\in_R Z_q^*$. 计算 $R=rP$.

(2) 计算 $y=e(P_{\mathrm{pub}},H_B)^r$.

(3) 计算 $z=e(P_B,H_B)^r$.

(4) 计算 $\kappa=h_2(y,z,R)$.

(5) 计算 $c=\mathrm{DEM.Enc}(\kappa,m)$.

(6) 计算 $f=h_3(u_A,u_B,m,R,P_A,P_B)$.

(7) 计算 $S=rH_A+x_Af+d_A$.

(8) 输出 $\sigma=(c,\phi\leftarrow(R,S))$.

3.6　Unsigncrypt

给定$(params,u_A,u_B,\sigma,s_B,P_A,P_B)$，接收者执行以下步骤.

(1) 计算 $y=e(R,d_B)$.

(2) 计算 $z=e(R,H_B)^{x_B}$.

(3) 计算 $\kappa=h_2(y,z,R)$.

(4) 计算 $m=\mathrm{DEM.Dec}(\kappa,c)$.

(5) 计算 $f=h_3(u_A,u_B,m,R,P_A,P_B)$.

(6) 验证 $e(P,S)=e(R,H_A)e(P_A,f)e(P_{\mathrm{pub}},H_A)$是否成立？若成立，接受 m；否则，输出$\perp$.

4　安全性分析

定理 1. 假如存在一个 IND-CCA2-I 敌手$\mathcal{A}_{\mathrm{I}}$经过 q_i次 h_i 询问（$i=1,2,3$）、q_{e_1} 次部分私钥询问、q_{e_2} 次私钥询问和 q_r 次公钥替换询问后，能以一个不可忽略的优势 ε 攻破 PS-CLHS 方案的 IND-CCA2-I 安全性，则存在一个算法 Γ 能以优势ε'解决 BDH 问题，这里 ε'为

$$\varepsilon\left(1-\frac{q_{e_1}}{q_1}\right)\left(1-\frac{q_{e_2}}{q_1}\right)\left(1-\frac{q_r}{q_1}\right)\left(\frac{1}{q_1-q_{e_1}-q_{e_2}-q_r}\right)\frac{1}{q_2}.$$

证明. 假设 Γ 收到一个 BDH 问题的随机实例 $(P,aP,bP,cP)\in G_1$，目标是计算出 $e(P,P)^{abc}\in G_2$. 为了达到这个目标，Γ 将 $\mathcal{A}_{\mathrm{I}}$ 作为子程序并扮演其挑战者在 IND-CCA2-I 中与之交互. 假设游戏中 $\mathcal{A}_{\mathrm{I}}$ 询问以身份 u_i 作为输入的其它预言机之前都先用身份 u_i 询问 h_1 预言机.

初始化. Γ 运行系统初始化算法，返回系统参数 $(G_1,G_2,e,P,P_{\mathrm{pub}}=aP,n,h_1,h_2,h_3)$ 给 $\mathcal{A}_{\mathrm{I}}$. 为了避免对 $\mathcal{A}_{\mathrm{I}}$ 的询问的非连续应答，Γ 维护起初为空的 4 张列表 $L_1\sim L_3$ 与 L_k.

阶段 1. $\mathcal{A}_{\mathrm{I}}$ 进行多项式有界次适应性询问.

h_1 询问：$\mathcal{A}_{\mathrm{I}}$ 选择一系列身份询问相应 Hash 值. 接收到身份 u_i 的 h_1 询问时，若 L_1 中含有 (u_i,H_i,l_i)，Γ 返回 H_i 作为应答；否则，Γ 随机选择一个整数 $\alpha\in[1..q_1]$，将 u_α 作为挑战身份但不会泄露 α 的值给 $\mathcal{A}_{\mathrm{I}}$. 如果接收到的是第 α 次询问，Γ 设置 $H_i=bP$，返回 H_i，添加 $(u_i,H_i,-)$ 到 L_1. 如果接收到的不是第 α 次询问，选择一个随机数 $l_i\in Z_q^*$，返回 $H_i\leftarrow l_iP$，添加 (u_i,H_i,l_i) 到 L_1.

h_2 询问：接收到 h_2 询问时，Γ 检查 L_2 中是否含有元组 (y,z,R,κ). 若有，返回对称密钥 κ；否则，返回任意的 $\kappa\in\{0,1\}^n$，添加 (y,z,R,κ) 到 L_2.

h_3 询问：接收到 h_3 询问时，Γ 检查 L_3 中是否含有元组 $(u_A,u_B,m,R,P_A,P_B,\upsilon,f)$. 若有，返回 f；否则，Γ 选择一个随机数 $\upsilon\in Z_q^*$，返回 $f\leftarrow\upsilon P$，添加 $(u_A,u_B,m,R,P_A,P_B,\upsilon,f)$ 到 L_3.

公钥询问：收到身份 u_i 的公钥询问时，Γ 检查 L_k 中是否含有条目 (u_i,d_i,x_i,P_i). 若有，Γ 返回公钥 P_i；否则，选择一个随机数 $x_i\in Z_q^*$，计算 $P_i=x_iP$，返回公钥 P_i，添加 $(u_i,-,x_i,P_i)$ 到 L_k.

部分私钥询问：收到身份 u_i 的部分私钥询问时，Γ 检查是否 $u_i=u_\alpha$. 若相等，Γ 放弃游戏；否则，Γ 调用 h_1 预言机得到 l_i，设置 $d_i=l_iaP$，返回部分私钥 d_i，以 (u_i,d_i,x_i,P_i) 更新 L_k.

私钥询问：收到身份 u_i 的私钥询问时，Γ 检查是否 $u_i=u_\alpha$. 若相等，Γ 放弃游戏；否则，Γ 从 L_k 中获得 (u_i,d_i,x_i,P_i)，返回完整私钥 $s_i\leftarrow(d_i,x_i)$.

公钥替换：$\mathcal{A}_{\mathrm{I}}$ 在指定范围内选择一个随机数 P_i' 替换身份 u_i 的公钥 P_i. 若 $u_i=u_\alpha$，Γ 放弃游戏；否则，Γ 以 $(u_i,d_i,-,P_i')$ 更新 L_k.

签密：收到消息 m 在发送者身份 u_A 和接收者身份 u_B 下的签密询问时，Γ 检查是否 $u_A\neq u_\alpha$. 若是，Γ 正常执行签密算法，返回运行结果；否则，Γ 从 L_k 检索到 (x_B,d_B,P_A)，并按下面方式生成密文.

(1) 选择 $r,\upsilon\in_R Z_q^*$，设置 $R=rP-aP$.

(2) 计算 $y=e(R,d_B)$.

(3) 通过 L_1 得到 l_B，计算 $z=e(R,l_BP)^{x_B}$.

(4) 计算 $\kappa=h_2(y,z,R)$，添加 (y,z,R,κ) 到 L_2.

(5) 计算 $c=\mathrm{DEM.Enc}(\kappa,m)$.

(6) 计算 $f=\upsilon P$，添加 $(u_A,u_B,m,R,P_A,P_B,\upsilon,f)$ 到 L_3.

(7) 通过 L_1 得到 $H_A=bP$，计算 $S=rH_A+\upsilon P_A$.

(8) 返回 $\sigma=(c,\phi\leftarrow(R,S))$.

正确性：

$$\begin{aligned}&e(R,H_A)e(P_A,f)e(P_{\mathrm{pub}},H_A)\\&=e(rP-aP,bP)e(x_AP_A,\upsilon P)e(aP,bP)\\&=e(P,rbP-abP)e(P,\upsilon P_A)e(P,abP)\\&=e(P,rH_A+\upsilon P_A)\\&=e(P,S).\end{aligned}$$

解签密：收到密文 σ 在发送者身份 u_A 和接收者身份 u_B 下的解签密询问时，Γ 检查是否 $u_B\neq u_\alpha$. 若是，Γ 正常运行解签密算法，返回运行结果；否则，Γ 从 L_k 检索到 (x_B,P_A)，并做出如下应答.

(1) 通过 L_1 得到 $H_B=bP$，计算 $z=e(R,H_B)^{x_B}$.

(2) 寻找不同 y 值的元组 (y,z,R,κ)，使得询问 $(P_{\mathrm{pub}},H_B,R,y)$ 时 O_{DBDH} 返回 1. 如果这种情况发生，计算 $\kappa=h_2(y,z,R)$.

(3) 计算 $m=\mathrm{DEM.Dec}(\kappa,c)$.

(4) 通过调用 h_3 预言机获得 f，然后检查等式 $e(P,S)=e(R,H_A)e(P_A,f)e(P_{\mathrm{pub}},H_A)$ 是否成立？若成立，接受 m；否则，输出 $\perp$.

挑战. 阶段 1 结束后，$\mathcal{A}_{\mathrm{I}}$ 生成两个相同长度的明文 m_0,m_1 以及希望挑战的两个身份 (u_A^*,u_B^*)，这里 u_A^* 和 u_B^* 分别是发送者和接收者的身份. 阶段 1 期间，u_B^* 的秘密值和部分私钥不能被询问，并且 u_B^* 不能是公钥已被替换的那个身份. 若 $u_B^*\neq u_\alpha$，Γ 放弃游戏；否则，Γ 从 L_k 找到 $(P_A^*,x_A^*,d_A^*,x_B^*)$，并按下面方式计算挑战密文.

(1) 设置 $R^*=cP$，选择 $\upsilon^*\in_R Z_q^*$，$y^*\in_R G_2$.

(2) 通过 L_1 得到 $H_B^*=bP$，计算 $z=e(R^*,H_B^*)^{x_B^*}$.

(3) 计算 $\kappa_1=h_2(y^*,z^*,R^*)$，添加 (y^*,z^*,R^*,κ_1) 到 L_2.

(4) 选择任意的 $\kappa_0\in\kappa_{\mathrm{PS\text{-}CLHS}}$ 与 $\gamma\in\{0,1\}$.

(5) 计算 $c^*=\mathrm{DEM.Dec}(\kappa_\gamma,m_\gamma)$.

(6) 计算 $f^*=\upsilon^*P$，添加 $(u_A^*,u_B^*,m_\gamma,R^*,P_A^*,$

P_B^*, υ^*, f^*)到 L_3.

(7)通过L_1得到l_A^*,计算$S^*=l_A^*cP+x_A^*f^*+d_A^*$.

(8)返回 $\sigma^*=(c^*,\phi^*\leftarrow(R^*,S^*))$.

阶段 2. $\mathcal{A}_{\mathrm{I}}$像阶段 1 那样进行多项式有界次适应性询问. 询问期间,u_B^* 的秘密值和部分私钥不能被询问,u_B^* 不能是公钥已被替换的那个身份,并且不能对 u_A^* 和 u_B^* 下的 σ^* 进行解签密询问.

猜测. L_2中储存了 q_2 个 Hash 值,Γ 从 L_2 中随机均匀地选择 y^*,输出

$$y^*=e(P_{\mathrm{pub}},H_B^*)^r=e(aP,bP)^c=e(P,P)^{abc}$$

作为 BDH 问题实例的解答.

概率分析. 现在来分析 Γ 得到 BDH 问题实例解答 $e(P,P)^{abc}$ 的成功概率. Γ 在不放弃游戏的情况下才能解决 BDH 问题,而它放弃游戏是由于下面 4 个事件.

事件 1. $\mathcal{A}_{\mathrm{I}}$询问了挑战身份 u_α 的部分私钥,这个事件发生的概率为 q_{e_1}/q_1.

事件 2. $\mathcal{A}_{\mathrm{I}}$询问了挑战身份 u_α 的秘密值,这个事件发生的概率为 q_{e_2}/q_1.

事件 3. $\mathcal{A}_{\mathrm{I}}$替换了挑战身份 u_α 的公钥,这个事件发生的概率为 q_r/q_1.

事件 4. $\mathcal{A}_{\mathrm{I}}$在挑战阶段所选择的接收者身份不是挑战身份 u_α,这个事件发生的概率为

$$1-\frac{1}{q_1-q_{e_1}-q_{e_2}-q_r}.$$

于是,Γ 不放弃游戏的概率为

$$\left(1-\frac{q_{e_1}}{q_1}\right)\left(1-\frac{q_{e_2}}{q_1}\right)\left(1-\frac{q_r}{q_1}\right)\left(\frac{1}{q_1-q_{e_1}-q_{e_2}-q_r}\right).$$

Γ 均匀随机地从 L_2 中选择 y^* 的概率是 $1/q_2$. 因此,Γ 解决 BDH 问题的优势 ε' 为

$$\varepsilon\left(1-\frac{q_{e_1}}{q_1}\right)\left(1-\frac{q_{e_2}}{q_1}\right)\left(1-\frac{q_r}{q_1}\right)\left(\frac{1}{q_1-q_{e_1}-q_{e_2}-q_r}\right)\frac{1}{q_2}.$$

证毕.

定理 2.　假如存在一个 IND-CCA2-II 敌手$\mathcal{A}_{\mathrm{II}}$经过 q_i次 h_i询问($i=1,2,3$)和 q_{e_2}次私钥询问后,能以一个不可忽略的优势 ε 攻破 PS-CLHS 方案的 IND-CCA2-II 安全性,则存在一个算法 Γ 能以优势 ε'解决 BDH 问题,这里 ε'为

$$\varepsilon\left(1-\frac{q_{e_2}}{q_1}\right)\left(\frac{1}{q_1-q_{e_2}}\right)\frac{1}{q_2}.$$

证明.　假设 Γ 收到一个 BDH 问题的随机实例$(P,aP,bP,cP)\in G_1$,目标是计算出 $e(P,P)^{abc}\in G_2$. 为了能够得到 BDH 问题实例的解答,Γ 扮演$\mathcal{A}_{\mathrm{II}}$的挑战者并把$\mathcal{A}_{\mathrm{II}}$作为子程序与之在 IND-CCA2-II 中进行交互. 假设游戏中$\mathcal{A}_{\mathrm{II}}$询问以身份 u_i作为输入的其它预言机之前都先用身份 u_i询问 h_1预言机.

初始化. Γ 运行系统初始化算法,发送主控密钥 x 和系统参数$(G_1,G_2,e,P,P_{\mathrm{pub}},n,h_1,h_2,h_3)$给$\mathcal{A}_{\mathrm{II}}$. 为了记录相关预言机的询问与应答,$\Gamma$ 维护起初为空的 4 张列表 $L_1\sim L_3$与 L_k.

阶段 1. $\mathcal{A}_{\mathrm{II}}$自适应地进行多项式有界次询问.

h_1询问:$\mathcal{A}_{\mathrm{II}}$选择一系列身份询问相应 Hash 值. 接收到身份 u_i的 h_1询问时,若 L_1中含有(u_i,H_i,l_i),Γ返回 H_i;否则,Γ 随机选择整数$\alpha\in[1..q_1]$,将 u_α作为挑战身份但不会泄露α 的值给$\mathcal{A}_{\mathrm{II}}$. 若接收到的是第 α 次询问,Γ 设置 $H_i=bP$,返回 H_i,添加$(u_i,H_i,-)$到 L_1. 若接收到的不是第 α 次询问,选择 $l_i\in_R Z_q^*$,返回 $H_i\leftarrow l_iP$,添加(u_i,H_i,l_i)到 L_1.

h_2询问:接收到 h_2询问时,Γ 检查 L_2中是否含有元组(y,z,R,κ). 若有,返回对称密钥 κ;否则,返回任意的$\kappa\in\{0,1\}^n$,添加(y,z,R,κ)到 L_2.

h_3询问:接收到 h_3询问时,Γ 检查 L_3中是否含有元组(u_A,u_B,m,R,P_A,P_B,f). 若有,返回 f;否则,Γ 选择一个随机数$\upsilon\in Z_q^*$,返回 $f=\upsilon P$,添加(u_A,u_B,m,R,P_A,P_B,f)到 L_3.

公钥询问:$\mathcal{A}_{\mathrm{II}}$选择一个身份 u_i并询问这个身份的公钥. 若 $u_i=u_\alpha$,Γ 设置 $P_i=aP$,返回公钥 P_i,添加$(u_i,-,-,P_i)$到 L_k;否则,Γ 选择 $x_i\in_R Z_q^*$,计算 $P_i=x_iP$,添加$(u_i,-,x_i,P_i)$到 L_k,返回公钥 P_i.

私钥询问:接收到身份 u_i的私钥询问时,Γ 检查是否 $u_i=u_\alpha$. 若相等,Γ 放弃游戏;否则,Γ 从 L_1/L_k找到 $l_i/(u_i,-,x_i,P_i)$,返回秘密值 x_i,以(u_i,xl_iP,x_i,P_i)更新 L_k. $\mathcal{A}_{\mathrm{II}}$知道主密钥 x,自己能计算出用户的部分私钥.

签密:收到消息 m 在发送者身份 u_A和接收者身份 u_B下的签密询问时,Γ 检查是否 $u_A\neq u_\alpha$. 若是,Γ 正常执行签密算法,返回运行结果;否则,Γ 从 L_k检索到(x_B,d_B,P_A),接着按下面方式生成密文.

(1)选择 $r,\upsilon\in_R Z_q^*$,计算 $R=rP$.

(2)计算 $y=e(R,d_B)$.

(3)通过 L_1检索到 l_B,计算 $z=e(R,l_BP)^{x_B}$.

(4)计算 $\kappa=h_2(y,z,R)$,添加(y,z,R,κ)到 L_2.

(5)计算 $c=\mathrm{DEM.Enc}(\kappa,m)$.

(6)计算 $f=\upsilon P$,添加$(u_A,u_B,m,R,P_A,P_B,\upsilon,f)$到 L_3.

(7)通过调用 h_1预言机得到 $H_A=bP$,计算 $S=$

$rH_A+\upsilon P_A+xH_A$.

(8) 返回 $\sigma=(c,\phi\leftarrow(R,S))$.

正确性:

$$\begin{aligned}&e(R,H_A)e(P_A,f)e(P_{\text{pub}},H_A)\\&=e(rP,bP)e(P_A,\upsilon P)e(xP,bP)\\&=e(P,rbP)e(P,\upsilon P_A)e(P,xbP)\\&=e(P,rH_A+\upsilon P_A+xH_A)\\&=e(P,S).\end{aligned}$$

解签密:收到密文 σ 在发送者身份 u_A 和接收者 u_B 下的解签密询问时,Γ 检查是否 $u_B\neq u_\alpha$. 如果是,Γ 正常运行解签密算法,返回运行结果;否则,Γ 从 L_k 检索到 (P_B,P_A),按下面方式做出响应.

(1) 通过 L_k 调用 h_1 预言机得到 $H_B=bP$,计算 $y=e(R,bP)^x$.

(2) 寻找不同 z 值的元组 (y,z,R,κ),使得询问 (P_B,H_B,R,z) 时 O_{DBDH} 返回 1. 如果存在这样一个元组,计算 $\kappa=h_2(y,z,R)$.

(3) 计算 $m=\text{DEM.Dec}(\kappa,c)$.

(4) 通过 h_3 预言机得到 f,然后检查等式 $e(P,S)=e(R,H_A)e(P_A,f)e(P_{\text{pub}},H_A)$ 是否成立?若成立,接受 m;否则,输出 $\perp$.

挑战. 阶段 1 结束后,$\mathcal{A}_{\text{II}}$ 生成两个相同长度的明文 m_0,m_1 以及希望挑战的两个身份 (u_A^*,u_B^*),这里 u_A^* 和 u_B^* 分别是发送者和接收者的身份. 阶段 1 期间,u_B^* 的秘密值不能被询问. 如果 $u_B^*\neq u_\alpha$,Γ 放弃游戏;否则,Γ 从 L_k 检索到 (x_A^*,d_A^*),并按下面方式计算挑战密文.

(1) 设置 $R^*=cP$,随机选择 $\upsilon^*\in Z_q^*$,$z^*\in G_2$.

(2) 通过 L_1 得到 $H_B^*=bP$,计算 $y^*=e(R^*,H_B^*)^x$.

(3) 计算 $\kappa_1=h_2(y^*,z^*,R^*)$,添加 (y^*,z^*,R^*,κ_1) 到 L_2.

(4) 选择任意的 $\kappa_0\in\kappa_{\text{PS-CLHS}}$ 与 $\gamma\in\{0,1\}$.

(5) 计算 $c^*=\text{DEM.Enc}(\kappa_\gamma,m_\gamma)$.

(6) 计算 $f^*=\upsilon^*P$,添加 $(u_A^*,u_B^*,m_\gamma,R^*,P_A^*,P_B^*,\upsilon^*,f^*)$ 到 L_3.

(7) 通过 L_1 得到 l_A^*,计算 $S^*=l_A^*cP+x_A^*f^*+d_A^*$.

(8) 计算 $S^*=l_A^*cP+\upsilon x_A^*P+d_A^*$.

(9) 返回 $\sigma^*=(c^*,\phi^*\leftarrow(R^*,S^*))$.

阶段 2. $\mathcal{A}_{\text{II}}$ 像阶段 1 那样进行多项式有界次适应性询问. 询问期间,u_B^* 的秘密值不能被询问,并且不能对 u_A^* 和 u_B^* 下的 σ^* 进行解签密询问.

猜测. L_2 中储存了 q_2 个 Hash 值,Γ 从 L_2 中随机均匀地选择 z^*,输出

$$z^*=e(P_B^*,H_B^*)^r=e(aP,bP)^c=e(P,P)^{abc}$$

作为 BDH 问题实例的解答.

概率分析. 现在来分析 Γ 得到 BDH 问题实例解答 $e(P,P)^{abc}$ 的成功概率. Γ 在不放弃游戏的情况下才能得到 DBH 问题实例的解答,而放弃游戏是由于下面两个事件.

事件 1. $\mathcal{A}_{\text{II}}$ 询问了挑战身份 u_α 的秘密值,这个事件发生的概率为 q_{e_2}/q_1.

事件 2. 挑战阶段,$\mathcal{A}_{\text{II}}$ 所选择的接收者身份不是挑战身份 u_α,这个事件发生的概率为

$$1-\frac{1}{q_1-q_{e_2}}.$$

于是,Γ 不放弃游戏的概率为 $\left(1-\frac{q_{e_2}}{q_1}\right)\left(\frac{1}{q_1-q_{e_2}}\right)$.

Γ 随机均匀地从列表 L_2 中选择 z^* 的概率是 $1/q_2$. 因此,Γ 解决 BDH 问题的概率为

$$\varepsilon\left(1-\frac{q_{e_2}}{q_1}\right)\left(\frac{1}{q_1-q_{e_2}}\right)\frac{1}{q_2}.$$

证毕.

定理 3. 假如存在一个 sUF-CMA-I 伪造者 $\mathcal{F}_1$ 经过 q_i 次 h_i 询问 $(i=1,2,3)$、q_{e_1} 次部分私钥询问、q_{e_2} 次私钥询问和 q_r 次公钥替换询问后,能以不可忽略的优势 ε 伪造 PS-CLHS 方案的一个密文,则存在一个算法 Γ 能以优势 ε' 解决 CDH 问题,这里 ε' 为

$$\left(\varepsilon-\frac{1}{2^k}\right)\left(1-\frac{q_{e_1}}{q_1}\right)\left(1-\frac{q_{e_2}}{q_1}\right)\left(1-\frac{q_r}{q_1}\right)\left(\frac{1}{q_1-q_{e_1}-q_{e_2}-q_r}\right).$$

证明. 假设 Γ 收到一个 CDH 问题的随机实例 $(P,aP,bP)\in G_1$,目的是计算 $abP\in G_1$. 为了得到 CDH 问题实例的解答,Γ 扮演 $\mathcal{F}_1$ 的挑战者并将它作为子程序与之在 sUF-CMA-I 中进行交互. 假设游戏中 $\mathcal{F}_1$ 询问以身份 u_i 作为输入的其它预言机之前都先用身份 u_i 询问 h_1 预言机.

初始化. Γ 运行系统初始化算法,将系统参数 $(G_1,G_2,e,P,P_{\text{pub}}=aP,n,h_1,h_2,h_3)$ 发送给 $\mathcal{F}_1$. 为了保证对各个预言机询问的连续应答,Γ 维护起初为空的 4 张列表 $L_1\sim L_3$ 与 L_k.

训练. $\mathcal{F}_1$ 进行适应性多项式有界次询问. 进行的询问与 IND-CCA2-I 中的阶段 1 相同.

伪造. 训练结束的时候,$\mathcal{F}_1$ 输出一个伪造 (σ^*,u_A^*,u_B^*),这里 $R^*=P_{\text{pub}}$. 训练期间,u_A^* 的完整私钥不能被询问,u_A^* 不能是公钥已被替换的那个身份,并且 σ^* 不能是来自伪造者对 u_A^* 和 u_B^* 下的某个消息 m^* 的签密询问的应答. 若 $u_A^*\neq u_\alpha$,Γ 放弃游戏;否则,Γ 通过 L_k 得到 P_A^*,调用 h_1 预言机和 h_3 预言机得

到 $H_A^*=bP$ 和 υ^*，输出 $abP=(S^*-\upsilon^* P_A^*)/2$ 作为 CDH 问题实例的解答. 原因如下：

$$\begin{aligned}e(P,S^*)&=e(R^*,H_A^*)e(P_A^*,f^*)e(P_{\text{pub}},H_A^*)\\&=e(P_{\text{pub}},bP)e(P_A^*,\upsilon^* P))e(aP,bP)\\&=e(P,abP)e(P,\upsilon^* P_A^*)e(P,abP).\end{aligned}$$

概率分析. 现在我们来评估 Γ 解决 CDH 问题的成功概率. 参考定理 1，可得：(1) $\mathcal{F}_{\text{I}}$ 询问了挑战身份 u_α 的部分私钥的概率为 q_{e_1}/q_1；(2) $\mathcal{F}_{\text{I}}$ 询问了挑战身份 u_α 的秘密值的概率为 q_{e_2}/q_1；(3) $\mathcal{F}_{\text{I}}$ 替换了挑战身份 u_α 的公钥，这个事件发生的概率为 q_r/q_1；(4) $\mathcal{F}_{\text{I}}$ 在训练阶段所选择的接收者身份不是挑战身份 u_α 的概率为

$$1-\frac{1}{q_1-q_{e_1}-q_{e_2}-q_r}.$$

于是，Γ 不放弃游戏的概率为

$$\left(1-\frac{q_{e_1}}{q_1}\right)\left(1-\frac{q_{e_2}}{q_1}\right)\left(1-\frac{q_r}{q_1}\right)\left(\frac{1}{q_1-q_{e_1}-q_{e_2}-q_r}\right).$$

$\mathcal{F}_{\text{I}}$ 猜测相关 h_3 预言机的相应 Hash 值的概率是 $1/2^k$. 因此，Γ 解决 CDH 问题的概率是

$$\left(\varepsilon-\frac{1}{2^k}\right)\left(1-\frac{q_{e_1}}{q_1}\right)\left(1-\frac{q_{e_2}}{q_1}\right)\left(1-\frac{q_r}{q_1}\right)\left(\frac{1}{q_1-q_{e_1}-q_{e_2}-q_r}\right).$$

证毕.

定理 4.　如果存在一个 sUF-CMA-II 伪造者 $\mathcal{F}_{\text{II}}$ 经过 q_i 次 h_i 询问 $(i=1,2,3)$ 以及 q_{e_2} 次私钥提取询问后，能以一个不可忽略的优势 ε 伪造 PS-CLHS 方案的一个密文，则存在一个算法 Γ 能以概率 ε' 解决 CDH 问题，这里 ε' 为

$$\left(\varepsilon-\frac{1}{2^k}\right)\left(1-\frac{q_{e_2}}{q_1}\right)\left(\frac{1}{q_1-q_{e_2}}\right).$$

证明.　假设 Γ 收到一个 CDH 问题的随机实例 $(P,aP,bP)\in G_1$，其目标是得到 CDH 问题实例的解答 $abP\in G_1$. 为此，Γ 将 $\mathcal{F}_{\text{II}}$ 作为子程序并扮演其挑战者在 sUF-CMA-II 中与之进行交互. 假设在游戏中 $\mathcal{F}_{\text{II}}$ 询问以身份 u_i 作为输入的其它预言机之前都先用身份 u_i 询问 h_1 预言机.

初始化. Γ 运行系统初始化算法，将系统参数 $(G_1,G_2,e,P,P_{\text{pub}},n,h_1,h_2,h_3)$ 和主控钥 x 发送给 $\mathcal{F}_{\text{II}}$. 为了避免对各个预言机询问的非连续应答，Γ 维护起初为空的 4 张列表 $L_1\sim L_3$ 与 L_k.

训练. $\mathcal{F}_{\text{II}}$ 在这个阶段进行适应性多项式有界次询问. 除了 h_1 询问和 h_3 询问之外，其余询问与 IND-CCA2-II 的阶段 1 相同.

h_1 询问：收到身份 u_i 的 h_1 询问时，Γ 检查 L_1 中是否存有 (u_i,H_i,l_i). 若有，Γ 返回 H_i；否则，Γ 选择 $l_i\in_R Z_q^*$，返回 $H_i\leftarrow l_iP$，以 (u_i,H_i,l_i) 更新 L_1.

h_3 询问：接收到 h_3 询问时，Γ 检查 L_3 中是否含有元组 $(u_A,u_B,m,R,P_A,P_B,\upsilon,f)$. 若有，返回 f；否则，Γ 选择一个随机数 $\upsilon\in Z_q^*$，返回 $f\leftarrow\upsilon aP$，添加 $(u_A,u_B,m,R,P_A,P_B,\upsilon,f)$ 到 L_3.

伪造. 训练结束的时候，$\mathcal{F}_{\text{II}}$ 输出一个伪造 (σ^*,u_A^*,u_B^*). 训练期间，u_A^* 的秘密值不能被询问，并且 σ^* 不能是来自伪造者对 u_A^* 和 u_B^* 下的某个消息 m^* 的签密询问的应答. 若 $u_A^*\neq u_\alpha$，Γ 放弃游戏；否则，Γ 调用 h_1 预言机和 h_3 预言机得到 l_A^* 和 υ^*，通过 L_k 获得 d_A^*，输出 $abP=(S^*-l_A^* R^*-d_A^*)/\upsilon^*$ 作为 CDH 问题实例的解答. 原因如下：

$$\begin{aligned}e(P,S^*)&=e(R^*,H_A^*)e(P_A^*,f^*)e(P_{\text{pub}},H_A^*)\\&=e(R^*,l_A^*P)e(aP,\upsilon^* bP)e(P,d_A^*)\\&=e(P,l_A^*R^*)e(P,\upsilon^* abP)e(P,d_A^*).\end{aligned}$$

概率分析. 现在我们来评估 Γ 得到 CDH 问题实例解答的成功概率. 参考定理 2，可得：(1) $\mathcal{F}_{\text{II}}$ 询问了挑战身份 u_α 的秘密值的概率是 q_{e_2}/q_1；(2) $\mathcal{F}_{\text{II}}$ 在训练阶段所选择的接收者身份不是挑战身份 u_α 的概率是

$$1-\frac{1}{q_1-q_{e_2}}.$$

于是，Γ 不放弃游戏的概率为

$$\left(1-\frac{q_{e_2}}{q_1}\right)\left(\frac{1}{q_1-q_{e_2}}\right).$$

$\mathcal{F}_{\text{II}}$ 猜测相关 h_3 预言机的相应 Hash 值的概率是 $1/2^k$. 因此，Γ 解决 CDH 问题的概率是

$$\left(\varepsilon-\frac{1}{2^k}\right)\left(1-\frac{q_{e_2}}{q_1}\right)\left(\frac{1}{q_1-q_{e_2}}\right).$$

证毕.

5　效率分析

本节通过计算开销和通信开销对 PS-CLHS 方案和同类方案[15-16]的计算复杂性进行比较. 比较中主要考虑 3 种运算：G_2 上的双线性对运算 x_1、G_1 上的点乘运算 x_2 以及 G_1 上的指数运算 x_3. $|r|$ 表示有限域 z_q^* 中一个元素的长度，$|G_1|$ 表示 G_1 上一个元素的长度，密文长度表示通信开销. 表 1 中没有考虑双线性对预运算.

表 1　无证书混合签密之间的比较

方案	签密			解签密			密文长度
	x_1	x_2	x_3	x_1	x_2	x_3	
文献[15]方案	0	4	0	1	1	0	$n+2\|G_1\|$
文献[16]方案	1	1	0	1	1	0	$n+\|r\|+\|G_1\|$
PS-CLHS	0	3	0	1	0	0	$n+2\|G_1\|$

相对于点乘运算来说,对运算和指数运算比较耗时[17].从表 1 可以看出,除了密文长度与同类方案大致得当外,PS-CLHS 方案在签密阶段执行了 3 次 G_1 上的标量乘操作,在解签密阶段执行了 1 次 G_2 上的对操作.总体来说,PS-CLHS 方案具有较低的计算复杂性.

6 结 语

本文给出了一个可证明安全的无证书混合签密方案.在随机预言模型下以及 BDH 问题和 CDH 问题的困难性假设下,我们证明该方案是 IND-CCA2 安全的和 sUF-CMA 安全的.所提方案计算效率高、通信成本低,适合应用于电子支付、移动通信、密钥管理、EDI、防火墙、电子商务等领域.

参 考 文 献

[1] Shamir A. Identity-based cryptosystem and signature scheme//Proceedings of the CRYPT 1984. California, USA, 1984: 47-53

[2] Al-Riyami S, Paterson K G. Certificateless public key cryptography//Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China, 2003: 452-474

[3] Yu Gang, Han Wen-Bao. Certificateless signcryption scheme with proxy unsigncryption. Chinese Journal of Computers, 2011, 34(7): 1291-1299(in Chinese)
(于刚,韩文报.具有代理解签密功能的无证书签密方案.计算机学报,2011,34(7):1291-1299)

[4] Liu Z, Hu Y, Zhang X, et al. Certificateless signcryption scheme in the standard model. Information Sciences, 2010, 180(3): 452-464

[5] Li Hui-Xian, Chen Xu-Bao, Pang Liao-Jun, Wang Yu-Min. Certificateless multi-receiver signcryption scheme based on multivariate public key cryptography. Chinese Journal of Computers, 2012, 35(9): 1881-1889(in Chinese)
(李慧贤,陈绪宝,庞辽军,王育民.基于多变量公钥密码体制的无证书多接收者签密体制.计算机学报,2012,35(9):1881-1889)

[6] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 2003, 33(1): 167-226

[7] Abe M, Gennaro R, Kurosawa K. Tag-KEM/DEM: A new framework for hybrid encryption. Journal of Cryptology, 2008, 21(1): 97-130

[8] Kurosawa K, Desmedt Y. A new paradigm of hybrid encryption scheme//Proceedings of the 24th Annual International Cryptology Conference. Santa Barbara, USA, 2004: 426-442

[9] Bentahar K, Farshim P, Malone-Lee J, Smart N P. Generic constructions of identity-based and certificateless KEMs. Journal of Cryptology, 2008, 21(2): 178-199

[10] Huang Q, Wong D. Generic certificateless encryption secure against malicious-but-passive KGC attacks in the standard model. Journal of Computer Science and Technology, 2010, 25(4): 807-826

[11] Dent A. Hybrid signcryption schemes with insider security//Proceedings of the 10th Australasian Conference on Information Security and Privacy. Brisbane, Australia, 2005: 253-266

[12] Dent A. Hybrid signcryption schemes with outsider security//Proceedings of the 8th International Information Security Conference. Singapore, Singapore, 2005: 203-217

[13] Tan C. Insider-secure signcryption KEM/tag-KEM schemes without random oracles//Proceedings of the 3rd International Conference on Availability, Reliability and Security-ARES 2008. Barcelona, Spain, 2008: 1275-1281

[14] Sun Y, Li H. ID-based signcryption KEM to multiple recipients. Chinese Journal of Electronics, 2011, 20(2): 317-322

[15] Li F, Shirase M, Takagi T. Certificateless hybrid signcryption. Mathematical and Computer Modelling, 2013, 57(3-4): 324-343

[16] Sun Yin-Xia, Li Hui. Efficient certificateless hybrid signcryption. Journal of Software, 2011, 22(7): 1690-1698 (in Chinese)
(孙银霞,李晖.高效的无证书混合签密.软件学报,2011,22(7):1690-1698)

[17] Cao X, Kou W, Dang L, Zhao B. IMBAS: Identity-based multiuser broadcast authentication in wireless sensor network. Computer Communications, 2008, 31(4-5): 659-671

YU Hui-Fang, born in 1972, Ph. D. candidate, associate professor, M. S. supervisor. Her main research interests include information security and cryptography.

YANG Bo, born in 1963, professor, Ph. D. supervisor. His main research interests include information security and cryptography.

Background

This research is supported by the National Natural Science Foundation of China under Grant Nos. 61363080 and 61272436; the Chunhui Project of Ministry of Education of China under Grant No. Z2012094 and the Natural Science Foundation of Guangdong Province under Grant No. 10351806001000000.

The practical way to perform secrecy communication for large message is to use hybrid encryption that separates the encryption into two parts: one part uses public key technique to encrypt a one-time symmetric key; the other uses the symmetric key to encrypt the actual message. In such a hybrid construction, the asymmetric part of the algorithm is known as the key encapsulation mechanism (KEM) while the symmetric part is known as the data encapsulation mechanism (DEM).

Public key signcryption often limits the message space when one wants to signcrypt the message of arbitrary length. For this reason, Dent proposed hybrid signcryption in 2005. In the formal security model for a hybrid signcryption scheme, signcryption KEM uses the public key technique to encapsulate a symmetric key; DEM employs the symmetric technique and the symmetric key to encrypt the message of arbitrary length. Signcryption KEM and DEM are completely separated, each part has its own security criteria, independent of operation of the other. If a message is very large, a hybrid signcryption scheme is more efficient than a public key signcryption scheme.

Certificateless cryptosystem (CLC) is conceived as an intermediate between traditional public key cryptosystem and ID-based cryptosystem. CLC eliminates the problem of key escrow in ID-based setting and avoids the use of certificates in traditional public key infrastructure.

In this paper, we extend hybrid signcryption technique to the certificateless setting, and construct a new and provably secure certificateless hybrid signcryption scheme. In the random oracle model, this scheme is proven IND-CCA2 secure and sUF-CMA secure under the hard assumptions of the bilinear Diffie-Hellman problem and computational Diffie-Hellman problem.