软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(12):3174−3182 [doi: 10.13328/j.cnki.jos.004819]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

使用 ECC 的身份混合签密方案*

俞惠芳[1,2], 杨 波[1]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](青海师范大学 计算机学院,青海 西宁 810008)

通讯作者: 俞惠芳, E-mail: yuhuifang@qhnu.edu.cn

摘 要: 身份混合签密能够高效封装对称密钥和安全传输数据.针对现有身份混合签密方案计算复杂度高的问题,集成身份混合签密和椭圆曲线密码学(ECC)中的双线性映射,构造了一种使用 ECC 的身份混合签密方案.证明了所构造的方案在随机预言模型下满足 co-BDH 假设下的保密性和 co-CDH 假设下的不可伪造性.由于该方案通信成本低且计算效率高,因而能够更好地满足密码学应用需求.

关键词: 身份密码学;混合签密;预言机重放技术;co-BDH 假设;co-CDH 假设

中图法分类号: TP309

中文引用格式: 俞惠芳,杨波.使用 ECC 的身份混合签密方案.软件学报,2015,26(12):3174−3182. http://www.jos.org.cn/1000-9825/4819.htm

英文引用格式: Yu HF, Yang B. Identity-Based hybrid signcryption scheme using ECC. Ruan Jian Xue Bao/Journal of Software, 2015,26(12):3174−3182 (in Chinese). http://www.jos.org.cn/1000-9825/4819.htm

Identity-Based Hybrid Signcryption Scheme Using ECC

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

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

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

Abstract: Identity-Based hybrid signcryption can efficiently encapsulate symmetric key and securely transmit data. Aiming at high computational complexity problem that exists in the existing identity-based hybrid signcryption schemes, this article integrates identity-based hybrid signcryption and bilinear maps in elliptic curve cryptography (ECC), and constructs a novel identity-based hybrid signcryption (IBHS) scheme using ECC. In the random oracle model, the paper proves that the constructed scheme satisfies the confidentiality under the co-bilinear Diffie-Hellman assumption and unforgeability under the co-computational Diffie-Hellman assumption. Since this scheme has low communication cost and high computational efficiency, it can be more practical in cryptography.

Key words: identity-based cryptography; hybrid signcryption; oracle replay technique; co-bilinear Diffie-Hellman assumption; co-computational Diffie-Hellman assumption

1997 年,郑玉良教授[1]提出的签密能够在一个合理的逻辑步骤内同时实现公钥加密和数字签名两项功能,且其计算量和通信成本远远低于传统的先签名后加密的方法.此后,签密[2−8]得到了快速发展,成为密码学研究领域的重要研究方向.2010 年,刘振华等人[3]提出的标准模型下的无证书签密方案是不安全的,具体攻击见文献

* 基金项目: 国家自然科学基金(61363080, 61272436, 61572303); 教育部春晖计划合作科研项目(Z2012094); 中国科学院信息工程研究所信息安全国家重点实验室开放课题(2015-MS-10); 保密通信重点实验室基金(9140C110206140C11050)

Foundation item: National Natural Science Foundation of China (61363080, 61272436, 61572303); Chunhui Project of Ministry of Education (Z2012094); Foundation of State Key Laboratory of Information Security (2015-MS-10); Foundation of Science and Technology on Communication Security Laboratory (9140C110206140C11050)

收稿时间: 2014-04-04; 修改时间: 2014-12-01; 定稿时间: 2015-01-21

[9,10].同年,朱辉等人[8]设计的没有对的无证书签密方案的描述中,将密文σ看作消息是错误的,而且安全性证明中的区分者选择的标志位c和发送者为接收者计算的密文中一个参数同名,使得整个证明过程的可读性受到影响.另外,定理 1 中的部分私钥和私钥提取询问中没有考虑标志位的值,实际上,标志位的值为 1 的情况下,区分者只能放弃游戏的执行而不是计算出相应的部分私钥和秘密值.

公钥环境中的签密使用公钥技术实现公钥加密和数字签名的过程,但公钥签密通常要求被传输的消息取自某个特定的集合,这样就限制了其应用范围.为了解决这个问题,Dent 使用 KEM-DEM 结构给出了混合签密方案[11,12].混合签密的组成部分中,签密密钥封装机制(KEM)运用公钥技术封装一个对称密钥,而数据封装机制(DEM)使用对称技术和来自 KEM 的对称密钥加密任意长度的消息.由于签密 KEM 和 DEM 完全独立,因而可以分别研究.与公钥签密相比,混合签密有着更高的灵活性和安全性.作为公钥密码技术的一个分支,混合签密近 10 年受到了许多密码研究者们的关注[13−16].为了更好地构造签密方案,Bjϕorsted 等人[17]使用了 tag-KEM,他们用一个随机标签作为输入因子,避免了接收者直接通过密钥封装来恢复对称密钥,从而接收者不可能任意伪造所选消息的密文.后来,学者们将身份密码学和混合签密结合在一起,构建了身份混合签密方案[18,19].如何很好地利用椭圆曲线上的双线性映射构建安全高效的身份混合签密方案,是一个重要有趣的研究问题.

本文将身份混合签密和双线性映射结合在一起,设计了一个新颖的使用 ECC 的身份混合签密(IBHS)方案.我们也证明了该方案在随机预言模型以及 co-CDH 问题和 co-BDH 问题的难解性下是语义安全的.通过分析发现,这是一个算法简单并安全实用的身份混合签密方案.

1 相关知识

本节首先回顾椭圆曲线上的双线性对和一些复杂性假设,然后给出使用 ECC 的身份签密 tag-KEM 和使用 ECC 的 IBHS 方案的形式化定义,以及使用 ECC 的 IBHS 方案的安全模型.

1.1 安全假设

令$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3$是 3 个阶为素数 p 的乘法循环群,g_1,g_2分别是$\mathbb{G}_1$与$\mathbb{G}_2$的生成元.存在从$\mathbb{G}_2$到$\mathbb{G}_1$的同构并且$\psi(g_2)=g_1$.映射 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_3$是满足以下条件的双线性映射:

(1) 双线性:对任意的$P\in\mathbb{G}_1,Q\in\mathbb{G}_2$和$a,b\in\mathbb{Z}_p$,$e(P^a,Q^b)=e(P,Q)^{ab}$;

(2) 非退化性:$e(g_1,g_2)\neq 1$.

Co-bilinear Diffie-Hellman (co-BDH) problem: 给定$P,P^a,P^b\in\mathbb{G}_1,Q\in\mathbb{G}_2$,对任意未知的$a,b\in\mathbb{Z}_p$,co-BDH 问题是计算$e(P,Q)^{ab}\in\mathbb{G}_3$.如果:

$$\Pr[\mathcal{A}(P,P^a,P^b,Q)=e(P,Q)^{ab}|a,b\in\mathbb{Z}_p]\geqslant\varepsilon,$$

则有一个概率多项式时间的敌手$\mathcal{A}$至少以概率ε解决 co-BDH 问题.

定义 1(Co-BDH 假设). 如果没有任何概率多项式时间的敌手$\mathcal{A}$以一个至少是ε的概率解决 co-BDH 问题,我们就说 co-BDH 假设是成立的.

Co-decisional bilinear Diffie-Hellman (co-DBDH) problem: 给定$P,P^a,P^b\in\mathbb{G}_1,Q\in\mathbb{G}_2$和$u\in\mathbb{G}_3$,对任意未知的$a,b\in\mathbb{Z}_p$,co-DBDH 问题是判断是否$e(P,Q)^{ab}=u$.如果:

$$\Pr[\mathcal{A}(P,P^a,P^b,Q,u)=1|a,b\in\mathbb{Z}_p]-\Pr[\mathcal{A}(P,P^a,P^b,Q,e(P,Q)^{ab})=1|a,b\in\mathbb{Z}_p]\geqslant\varepsilon,$$

则有一个概率多项式时间的敌手$\mathcal{A}$至少以概率ε解决 co-DBDH 问题.

定义 2(Co-DBDH 假设). 如果没有任何概率多项式时间的敌手$\mathcal{A}$以一个至少是ε的概率解决 co-DBDH 问题,我们就说 co-DBDH 假设是成立的.

Co-computational Diffie-Hellman (co-CDH) problem: 给定$P,P^a\in\mathbb{G}_1,Q\in\mathbb{G}_2$,对任意未知的$a\in\mathbb{Z}_p$,co-CDH 问

题是计算 $Q^a \in \mathbb{G}_2$.如果:

$$\Pr[\mathcal{A}(P,P^a,Q)=Q^a | a \in \mathbb{Z}_p] \geqslant \varepsilon,$$

则有一个概率多项式时间的敌手$\mathcal{A}$至少以概率ε解决 co-CDH 问题.

定义 3(Co-CDH 假设). 如果没有任何概率多项式时间的敌手$\mathcal{A}$以一个至少是ε的概率解决 co-CDH 问题,我们就说 co-CDH 假设是成立的.

1.2 使用ECC的身份签密tag-KEM

本节给出了一种使用 ECC 身份签密 tag-KEM 方案的算法模型,包括设置算法 Setup、密钥产生算法 KeyGen、对称密钥产生算法 Sym、密钥封装算法 Encap 和解封装算法 Decap.使用 ECC 的身份签密 tag-KEM 有 3 个参与方:私钥生成器(PKG)、身份为 id_a 的发送者和身份为 id_b 的接收者.每个算法模块的设计和实现描述如下:

- Setup:输入安全参数 k,PKG 执行这个设置算法并产生系统参数 pm 以及主密钥 x.最后,PKG 公布系统参数并保留主密钥;
- KeyGen:输入 pm,x 和某实体的身份 id_i,PKG 执行这个密钥生成算法并输出该实体的私钥 s_i 和公钥 y_i;
- Sym:输入 pm、发送者的公私钥对(y_a,s_a)以及接收者的身份 id_b 和公钥 y_b,身份为 id_a 的发送者执行这个对称密钥生成算法并输出对称密钥κ和内部状态信息ω;
- Encap:输入标签 c 和状态信息ω,身份为 id_a 的发送者执行这个密钥封装算法并输出对称密钥封装ϕ;
- Decap:输入 pm、标签 c、对称密钥封装ϕ、发送者的身份 id_a 和公钥 y_a 以及接收者的公私钥对(y_b,s_b),身份为 id_b 的接收者执行这个解封装算法并输出对称密钥κ或表示解封装失败的符号$\perp$.

1.3 使用ECC的IBHS方案

一个使用 ECC 的 IBHS 方案由使用 ECC 的身份签密 tag-KEM 和 DEM[18]两个方案组成.使用 ECC 的 IBHS 方案的 4 个概率多项式算法的细节描述如下:

- Setup:与使用 ECC 的身份签密 tag-KEM 方案相同;
- KeyGen:与使用 ECC 的身份签密 tag-KEM 方案相同;
- Signcrypt:给定$(pm,id_a,id_b,m,s_a,y_a,y_b)$,发送者按照下列步骤执行这种签密算法:
  (1) 计算$(\kappa,\omega)\leftarrow Sym(pm,id_a,id_b,s_a,y_a,y_b)$;
  (2) 计算 $c\leftarrow DEM.Enc(\kappa,m)$;
  (3) 计算$\phi\leftarrow Encap(c,\omega)$;
  (4) 输出密文$\sigma\leftarrow(c,\phi)$;
- Unsigncrypt:给定$(pm,id_a,id_b,\sigma,s_b,y_a,y_b)$,接收者按照下列步骤执行这种解签密算法:
  (1) 计算$\kappa\leftarrow Decap(pm,\phi,id_a,id_b,s_b,y_a,y_b)$.
  (2) 输出 $m\leftarrow DEM.Dec(\kappa,c)$.
  (3) 如果验证等式成立,接收消息 m;否则,输出符号$\perp$.

1.4 使用ECC的IBHS方案的安全模型

本文基于下面的安全模型对使用ECC的IBHS方案的安全性给出随机预言模型下的安全证明.我们的模型中不允许发送者和接收者身份相同的询问.

1.4.1 保密性

保密性是指攻击者从一个密文中获取任何明文信息在计算上是不可行的.对于使用ECC的IBHS方案的保密性,我们采用适应性选择密文攻击下的不可区分性(IND-CCA2)安全模型.这个模型是由文献[18]中的安全模型修改得到.具体描述中,需考虑下面挑战者$\mathcal{C}$和敌手$\mathcal{A}$之间进行的一个交互游戏:

初始化. $\mathcal{C}$运行设置算法得到系统参数和主密钥,并发送系统参数给敌手$\mathcal{A}$但保留主密钥.

阶段 1. $\mathcal{A}$在这个阶段执行多项式有界次适应性询问,适应性是指每次询问都依赖于以前询问的应答:

- 私钥询问:$\mathcal{A}$选择一个身份 id_i 并询问这个身份的私钥,$\mathcal{C}$运行相关算法并将作为结果的私钥 s_i 发送给$\mathcal{A}$;
- 签密询问:当接收到关于(m,id_a,id_b)的签密询问时,$\mathcal{C}$计算密文σ并将这个密文发送给$\mathcal{A}$;
- 解签密询问:当接收到关于(σ,id_a,id_b)的解签密询问时,$\mathcal{C}$运行解签密算法并将结果发送给$\mathcal{A}$.

挑战. 当阶段 1 结束时,$\mathcal{A}$生成两个等长的消息 m_0 与 m_1 以及希望挑战的两个身份 id_a^* 与 id_b^*,这里,id_a^*,id_b^* 分别是发送者和接收者的身份.在阶段 1,身份 id_b^* 的私钥不能被询问.挑战者$\mathcal{C}$从{0,1}中选择一个随机位 t,计算:

$$\sigma^* \leftarrow Signcrypt(pm,id_a^*,id_b^*,m_t,s_a^*,y_a^*,y_b^*),$$

并发送挑战密文σ^*给$\mathcal{A}$.

阶段 2. $\mathcal{A}$在这个阶段,像阶段 1 那样自适应地执行多项式有界次询问.$\mathcal{C}$像阶段 1 那样做出应答,但是$\mathcal{A}$不能询问身份 id_b^* 的私钥,也不能对关于 id_a^* 与 id_b^* 的σ^*进行解签密询问.

当游戏结束的时候,敌手$\mathcal{A}$输出 t 的一个猜测值 t^*.假如 $t^*=t$,那么敌手$\mathcal{A}$赢得上述游戏.$\mathcal{A}$赢得游戏的优势定义为 $Adv(\mathcal{A})=|2\Pr[t^*=t]-1|$,这里,$\Pr[t^*=t]$表示 $t^*=t$ 的概率.

定义 4. 如果任意多项式有界的敌手$\mathcal{A}$赢得上面游戏的优势是可忽略的,则称一个使用 ECC 的 IBHS 方案在适应性选择密文攻击下具有不可区分性.

1.4.2 不可伪造性

不可伪造性是指发送者不能否认对消息签名的事实.对于所提方案的不可伪造性,我们采用适应性选择明文攻击下的不可伪造性(sUF-CMA)安全模型.具体描述中,需考虑挑战者$\mathcal{C}$和伪造者$\mathcal{F}$之间执行的一个交互游戏:

初始化. $\mathcal{C}$运行设置算法得到系统参数和主密钥,并返回系统参数但保留主密钥.

训练. $\mathcal{F}$在这个阶段像定义 4 中的阶段 1 那样执行多项式有界次的适应性询问,所涉及到的询问与应答和定义 4 中的阶段 1 完全相同.

伪造. 当训练阶段结束的时候,$\mathcal{F}$输出伪造的三元组 (id_a^*,id_b^*,σ^*),这里,id_a^*,id_b^* 分别是发送者和接收者的身份.在训练阶段,身份 id_a^* 的私钥不能被询问,并且σ^*不能是来自$\mathcal{F}$的任何签密询问的应答.

如果解签密的结果不是符号$\perp$,则伪造者$\mathcal{F}$就赢得上述游戏.$\mathcal{F}$赢得游戏的优势定义为 $Adv(\mathcal{F})=\Pr[win]$.

定义 5. 如果任意多项式有界的伪造者$\mathcal{F}$赢得上面游戏的优势是可忽略的,则称一个使用 ECC 的 IBHS 方案在适应性选择消息攻击下具有不可伪造性.

2 方案描述

本节给出具体的使用 ECC 的身份混合签密(IBHS)方案.这个方案由 4 个概率多项式算法模块组成,每个算法模块的细节描述如下:

2.1 Setup

给定安全参数 k,PKG 按以下步骤执行这种算法:

(1) 选择一个 k 比特的大素数 p,定义与第 1.1 节中相同的$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3,e,P\in\mathbb{G}_1$ 是循环群$\mathbb{G}_1$ 的生成元;

(2) 选择一个随机数 $x\in\mathbb{Z}_p$ 作为主密钥,计算系统公钥 $y=P^x\in\mathbb{G}_1$;

(3) 选择如下密码学安全的哈希函数:$H_1:\{0,1\}^*\to\mathbb{G}_2,H_2:\mathbb{G}_1\times\mathbb{G}_3\to\{0,1\}^n$, $H_3:\{0,1\}^n\times\mathbb{G}_1\times\mathbb{G}_2^2\times\mathbb{G}_3\to\mathbb{Z}_p$ 和 $H_4:\{0,1\}^n\times\mathbb{G}_1\times\mathbb{G}_2^2\times\mathbb{G}_3\to\mathbb{G}_2$.这里,$n$ 是 DEM 的密钥长度;

(4) 保密主密钥 x,并公布系统参数 $pm=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3,P,y,n,H_1,H_2,H_3,H_4)$.

2.2 KeyGen

给定(pm,x),PKG 计算身份为 id_i 的实体的公钥 $y_i=H_1(id_i)\in\mathbb{G}_2$ 和私钥 $s_i=y_i^x\in\mathbb{G}_2$.显而易见,发送者和接收者的公私钥对分别是(y_a,s_a)和(y_b,s_b).

2.3 Signcrypt

给定(pm,id_a,id_b,m,s_b,y_a,y_b),发送者选择随机数 $u\in\mathbb{Z}_p$,并通过以下步骤为接收者生成密文σ.

(1) 计算 $r=P^u\in\mathbb{G}_1$;

(2) 计算$\upsilon=e(y^u,y_b)\in\mathbb{G}_3$;

(3) 计算$\kappa=H_2(r,\upsilon)\in\{0,1\}^n$;

(4) 计算 $c=DEM.Enc(\kappa,m)$;

(5) 计算 $h=H_3((m,r,y_a,y_b,\upsilon)\in\mathbb{Z}_p$;

(6) 计算$\rho=H_4(m,r,y_a,y_b,\upsilon)\in\mathbb{G}_2$;

(7) 计算 $s=s_a^h\rho^u\in\mathbb{G}_2$;

(8) 输出$\sigma=(r,c,s)$.

2.4 Unsigncrypt

给定(pm,id_a,id_b,σ,s_b,y_a,y_b),接收者按如下步骤执行这种算法.

(1) 计算$\upsilon=e(r,s_b)$;

(2) 计算$\kappa=H_2(r,\upsilon)$;

(3) 计算 $m=DEM.Dec(\kappa,c)$;

(4) 计算 $h=H_3(m,r,y_a,y_b,\upsilon)$;

(5) 计算$\rho=H_4(m,r,y_a,y_b,\upsilon)$;

(6) 如果 $e(P,s)=e(y^h,y_a)e(r,\rho)$成立,接收消息 m;否则,输出符号⊥.

上述方案的解密算法和签密算法的一致性可以通过以下等式验证:

$$\upsilon=e(r,s_b)=e(P^u,y_b^x)=e(y^u,y_b),$$
$$e(P,s)=e(P,s_a^h\rho^r)=e(P,s_a^h)e(P,\rho^r)=e(y^h,y_a)e(r,\rho).$$

3 安全性分析

定理 1. 在随机预言模型下,如果存在一个 IND-CCA2 敌手$\mathcal{A}$经过最多 q_i 次对 H_i 的询问(i=1~4)以及 q_k 次私钥询问后,能够以不可忽略的优势ε赢得定义 4 中的游戏,那么就存在一种算法$\mathcal{C}$,能够至少以优势ε/eq_2q_k 解决 co-BDH 问题.

证明:设$\mathcal{C}$得到一个 co-BDH 问题的随机实例(P,P^a,P^b,Q).为了利用$\mathcal{A}$的能力得到 co-BDH 问题实例的解答 $e(P,Q)^{ab}\in\mathbb{G}_3$,$\mathcal{C}$运行设置算法后,将生成的系统参数($p$,$\mathbb{G}_1$,$\mathbb{G}_2$,$\mathbb{G}_3$,$P$,$y=P^a$,$H_1$~$H_4$)发送给$\mathcal{A}$.$\mathcal{C}$将$\mathcal{A}$作为子程序并扮演其挑战者,与之在游戏中进行交互.$\mathcal{C}$从 q_1 个身份中选择第 t 个身份作为挑战身份 id_t,但是不会泄露 id_t 给$\mathcal{A}$.假设某个δ是 $id_i=id_t$ 的概率,这个δ的值后面确定.为了避免发生对子程序$\mathcal{A}$的适应性询问的非连续性应答,$\mathcal{C}$维护 5 张列表 L_1~L_4 和 L_k,这些列表初始化为空.L_1~L_4 和 L_k 分别用于跟踪 H_1~H_4 预言机和私钥提取预言机.

阶段 1.在这个阶段,$\mathcal{A}$执行下面多项式有界次适应性询问.

- H_1 询问.

当收到关于身份 id_i 的 H_1 询问时,$\mathcal{C}$先检查列表 L_1 中是否含有元组(id_i,y_i,l_i).

- 如果含有,返回公钥 y_i;

- 否则,$\mathcal{C}$做出如下反应:(1) 如果 $id_i \neq id_t$,$\mathcal{C}$选择一个随机值 $y_i \in \mathbb{G}_2$,返回公钥 $y_i = P^{l_i}$ 并且储存(id_i, y_i, l_i)到列表 L_1 中;(2) 如果 $id_i = id_t$,$\mathcal{C}$设置 $y_i = Q$,返回公钥 y_i 并且储存$(id_i, y_i, -)$到列表 L_1 中.

- H_2 询问.

当收到$\mathcal{A}$的 H_2 询问时,$\mathcal{C}$先检查列表 L_2 中是否存在元组(z, υ, κ):若存在,返回对称密钥κ;否则,$\mathcal{C}$返回任意选择的$\kappa \in \{0,1\}^n$ 并且储存(z, υ, κ)到列表 L_2 中.

- H_3 询问.

当收到$\mathcal{A}$的 H_3 询问时,$\mathcal{C}$先检查列表 L_3 中是否存在匹配元组:若存在,$\mathcal{C}$返回相关值;否则,$\mathcal{C}$返回任意选择的 $h \in \mathbb{Z}_p$ 并且储存$(m, r, y_a, y_b, \upsilon, h)$到列表 L_3 中.

- H_4 询问.

当收到$\mathcal{A}$的 H_4 询问时,$\mathcal{C}$先检查列表 L_4 中是否存在匹配元组.

- 若存在,$\mathcal{C}$返回相关值;
- 否则,假设进行 H_4 询问之前已经询问过 H_1 预言机,$\mathcal{C}$做出如下反应:(1) 如果 $id_a \neq id_t$,$\mathcal{C}$设置$\rho = y_a$,返回ρ并且储存$(m, r, y_a, y_b, \upsilon, \rho)$到列表 L_1 中;(2) 如果 $id_a = id_t$,$\mathcal{C}$设置$\rho = Q$,返回ρ并且储存$(m, r, y_a, y_b, \upsilon, \rho)$到列表 L_4 中.

- 私钥询问.

$\mathcal{A}$可以请求一系列身份所对应的私钥(根据 H_1 询问可知,最多有 q_1 个身份).当收到身份 id_i 的私钥询问时,$\mathcal{C}$先检查列表 L_k 中是否存在条目(id_i, s_i).

- 如果存在,返回私钥 s_i;
- 否则,$\mathcal{C}$做出如下反应:(1) 如果 $id_i \neq id_t$,$\mathcal{C}$询问 H_1 预言机得到 l_i,计算 $s_i = (P^a)^{l_i}$,返回私钥 s_i 并且储存(id_i, s_i)到列表 L_k 中;(2) 如果 $id_i = id_t$,$\mathcal{C}$放弃模拟.

- 签密询问.

设在签密询问之前$\mathcal{C}$已经询问过 H_1 预言机和私钥提取预言机,当收到关于(m, id_a, id_b)的签密询问时,$\mathcal{C}$做出如下反应:如果 $id_a \neq id_t$,$\mathcal{C}$正常运行签密算法生成密文σ并将此结果发送给$\mathcal{A}$;否则,它通过下列方式生成密文σ.

- 选择 $u, \beta \in_R \mathbb{Z}_p$,计算 $r = P^u y_a^{-\beta}$;
- 计算$\upsilon = e(r, s_b)$;
- 计算$\kappa = H_2(r, \upsilon)$,储存$(r, \upsilon, \kappa)$到列表 L_2 中;
- 计算 $c = DEM.Enc(\kappa, m)$;
- 设置 $h = \beta \in \mathbb{Z}_p$,储存$(m, r, y_a, y_b, \upsilon, h)$到列表 L_3 中;
- 设置$\rho = Q \in \mathbb{G}_2$,储存$(m, r, y_a, y_b, \upsilon, \rho)$到列表 L_4 中;
- 计算 $s = P^u \in \mathbb{G}_1$;
- 输出$\sigma = (r, c, s)$.

此密文的有效性能够通过敌手$\mathcal{A}$的验证,因为验证等式是成立的.

$$e(y^h, y_a)e(r, \rho) = e(y^h, y_a)e(P^u y_a^{-\beta}, \rho) = e(y^h, Q)e(P, \rho^u)e((P^a)^{-h}, \rho) = e(y^h, Q)e(P, \rho^u)e(y^{-h}, \rho) = e(P, s).$$

- 解签密询问.

当收到关于(σ, id_a, id_b)的解签密询问时,$\mathcal{C}$做出如下反应:如果 $id_b \neq id_t$,$\mathcal{C}$正常运行解签密算法并将运行结果发送给$\mathcal{A}$;否则,$\mathcal{C}$做出如下反应.

- 检索列表 L_2 寻找针对不同υ值的元组(r, υ, κ),当询问(y, r, Q, υ)时,使得 co-DBDH 预言机返回 1.如果有这种情况,则挑战者使用来自(r, υ, κ)的对称密钥κ恢复 $m = DEM.Dec(\kappa, c)$;
- 调用 H_1, H_3 和 H_4 预言机分别得到 h, ρ与 y_a;
- 如果 $e(P, s) = e(y^h, y_a)e(r, \rho)$成立,接收 m;否则,输出$\perp$.

挑战. 当阶段 1 结束时,$\mathcal{A}$生成两个等长度的消息 m_0 与 m_1,以及希望被挑战的两个身份 id_a^* 与 id_b^*,这里,id_a^*,id_b^* 分别是发送者和接收者的身份.在阶段 1,身份 id_b^* 的私钥不能被询问.如果 $id_b^* \neq id_t$,$\mathcal{C}$放弃模拟;否则,$\mathcal{C}$通过调用 H_1 预言机和私钥提取预言机分别获得 (y_a^*,y_b^*) 与 s_a^*,然后通过下列步骤计算挑战密文 σ^*.

- 设置 $r^*=P^b\in\mathbb{G}_1$,随机选择 $\upsilon^*\in\mathbb{G}_3$;
- 计算 $\kappa_1=H_2(r^*,\upsilon^*)$,将 $(r^*,\upsilon^*,\kappa_1)$ 储存到列表 L_2 中;
- 从使用 ECC 的 IBHS 方案的密钥空间中选择任意的对称密钥 κ_0,并且从{0,1}中选择一个随机位 t;
- 计算 $c^*=DEM.Dec(\kappa_t,m_t)$;
- 计算 $h^*=H_3(m_t,r^*,y_a^*,y_b^*,\upsilon^*)$,储存 $(m_t,r^*,y_a^*,y_b^*,\upsilon^*,h^*)$ 到列表 L_3 中;
- 设置 $\rho^*=y_a^*\in\mathbb{G}_2$,储存 $(m_t,r^*,y_a^*,y_b^*,\upsilon^*,\rho^*)$ 到列表 L_4 中;
- 计算 $s^*=(s_a^*)^{h^*}(P^b)^{l_a^*}$;
- 输出 $\sigma^*=(r^*,c^*,s^*)$.

阶段 2. $\mathcal{A}$在这个阶段像在阶段 1 一样自适应地进行多项式有界次询问,$\mathcal{C}$也像在阶段 1 一样做出应答.但是敌手不能询问身份 id_b^* 的私钥,也不能对关于 id_a^* 与 id_b^* 的 σ^* 进行解签密询问.

猜测. 根据上述证明过程,敌手一定以 (r^*,υ^*) 询问过 H_2 预言机,列表 L_2 中也必然存在 q_2 个相关的询问与应答值.这也意味着:列表 L_2 中,存储有 q_2 个相关元组中的其中一个元组中必含有 co-BDH 问题实例的解答 υ^*.$\mathcal{C}$从列表 L_2 中随机选择 υ^*,输出:

$$\upsilon^*=e(y^{u^*},y_b^*)=e(y,Q)^b=e(P,Q)^{ab}.$$

下面我们分析$\mathcal{C}$在上面游戏中得到 co-BDH 问题实例解答的成功概率.

已知敌手最多进行 q_k 次私钥询问,那么$\mathcal{C}$在阶段 1 或阶段 2 不放弃仿真的概率是 δ^{q_k}.$\mathcal{C}$在挑战阶段不放弃仿真的概率是 $1-\delta$.于是,$\mathcal{C}$不放弃游戏执行的概率是 $\delta^{q_k}(1-\delta)$,这个值在 $\delta=1-\left(\frac{1}{1+q_k}\right)$ 时达到最大.因而,$\mathcal{C}$不放弃这个游戏的执行的概率至少是 $1/eq_k$,即:

$$\begin{aligned}\delta^{q_k}(1-\delta)&=\left(1-\frac{1}{1+q_k}\right)^{q_k}\left(\frac{1}{1+q_k}\right)\\&=\left(1-\frac{1}{1+q_k}\right)^{(1+q_k)}\left(\frac{1}{q_k}\right)\\&\geqslant\left(\frac{1}{e}\right)\left(\frac{1}{q_k}\right).\end{aligned}$$

$\mathcal{C}$从列表 L_2 中均匀随机地选择 υ^* 作为 co-BDH 问题实例解答的概率至少是 $1/q_2$,因此,$\mathcal{C}$解决 co-BDH 问题的概率至少为 ε/eq_2q_k. □

定理 2. 在随机预言模型下,如果存在一个 sUF-CMA 伪造者 $\mathcal{F}$ 经过最多 q_i 次对 H_i 的询问(i=1~4)以及 q_k 次私钥询问后,能够以不可忽略的优势 ε 赢得定义 5 中的游戏,那么就存在一个算法 $\mathcal{C}$,能够至少以优势 ε/eq_k 解决 co-CDH 问题.

证明:设$\mathcal{C}$得到一个 co-CDH 问题的随机实例 (P,P^a,Q).为了利用敌手 $\mathcal{F}$ 的能力得到 co-CDH 问题实例的解答 $Q^a\in\mathbb{G}_2$,$\mathcal{C}$运行设置算法后,将生成的系统参数 $(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3,P,y=P^a,H_1\sim H_4)$ 发送给 $\mathcal{F}$.$\mathcal{C}$将 $\mathcal{F}$ 作为子程序并扮演其挑战者与之在游戏中进行交互.$\mathcal{C}$从 q_1 个身份中选择第 t 个身份作为挑战身份 id_t,但是不会泄露 id_t 给 $\mathcal{F}$.假设 $id_i=id_t$ 的概率为某个 δ,这个 δ 的值后面确定.为了避免发生对子程序 $\mathcal{F}$ 的适应性询问的非连续性应答,$\mathcal{C}$维护 5 张列表 $L_1\sim L_4$ 和 L_k,这些列表起初为空.$L_1\sim L_4$ 和 L_k 分别用于跟踪 $H_1\sim H_4$ 预言机和私钥提取预言机.

训练. $\mathcal{F}$在这个阶段自适应地发起多项式有界次询问,所涉及到的询问与应答和定理 1 的阶段 1 完全相同.

伪造. 当$\mathcal{F}$决定训练阶段结束的时候,$\mathcal{F}$发送给$\mathcal{C}$关于发送者身份id_a^*和接收者身份id_b^*的伪造密文σ^*.训练阶段,身份id_a^*的私钥不能被询问,并且σ^*不能是来自$\mathcal{F}$的任何签密询问的应答.$\mathcal{C}$检查是否$id_a^* \neq id_t$:如果是,$\mathcal{C}$放弃对游戏的执行;相反,$\mathcal{C}$利用预言重放技术输出另一密文$\sigma^{**}=(r^*,c^{**},s^{**})$.$\mathcal{C}$调用 H_4 预言机得到$\rho=Q$,故有$s^* = (s_a^*)^{h^*} Q^u$和$s^{**} = (s_a^*)^{h^{**}} Q^u$.通过调用$H_1$预言机可得$y_a=Q$,故可推导出 co-CDH 问题实例的解答,即:

$$Q^a = s_a^* = \left(\frac{s^{**}}{s^*}\right)^{(h^{**}-h^*)^{-1}}.$$

下面我们分析$\mathcal{C}$在上述游戏中得到 co-CDH 问题实例解答的成功概率.

已知伪造者最多进行q_k次私钥询问,则$\mathcal{C}$在阶段 1 或阶段 2 不放弃模拟的的概率是δ^{q_k},$\mathcal{C}$在挑战阶段不放弃仿真的概率是 $1-\delta$.于是,$\mathcal{C}$不放弃这个游戏的概率是$\delta^{q_k}(1-\delta)$,这个值在$\delta=1-1/(1+q_k)$时达到最大.由此可得,$\mathcal{C}$不放弃游戏执行的概率至少是$\delta=1/eq_k$.这说明$\mathcal{C}$解决 co-CDH 问题的概率至少为ε/eq_k. □

4 性能分析

本节通过计算开销和通信开销两个方面对我们提出的使用 ECC 的 IBHS 方案与已有同类方案[18,19]进行性能比较,在比较中主要考虑 3 种运算:双线性对运算y_p、加法群G上的点乘运算y_m,以及乘法群G_1,G_2与G_3上的指数运算y_e.表 1 中没有考虑双线性对的预运算,计算开销包括签密和解签密两部分:密文长度表示通信开销,$|p|$表示有限域Z_p上一个元素的长度.

Table 1 Comparison of computation and communication overhead

表 1 计算开销和通信开销比较

方案	签密			解签密			密文长度
	y_p	y_m	y_e	y_p	y_m	y_e	
文献[18]中方案	0	1	4	2	1	1	$\|m\|+2\|G\|$
文献[19]中方案	1	1	4	5	0	1	$\|m\|+\|p\|$
本文方案	0	0	4	1	0	1	$\|m\|+\|G_1\|+\|G_2\|$

从表 1 可以看出:在密文长度与其他方案相当的情况下,本文方案在签密阶段执行了 4 个指数运算,在解签密阶段执行了 1 个对运算和 1 个指数运算.一般来说,双线性对运算最耗时,其次是指数运算和点乘运算.由此可知,本文方案的总计算开销明显低于已有方案[18,19].

5 结 语

混合签密的安全性以及计算复杂度直接影响着其实用性.本文提出了一种使用 ECC 的身份混合签密方案,该方案基于随机预言模型以及 co-BDH 假设和 co-CDH 假设被证明具有 IND-CCA2 安全性和 sUF-CMA 安全性.所提方案用较小的计算开销实现了较高的安全性,在密码学领域具有良好的应用前景.

References:

[1] Zheng YL. Digital signcryption or how to achieve *cost*(signature & encryption)<<*cost*(signature)+*cost*(encryption). In: Kaliski BS, ed. Proc. of the Cryptology (CRYPYO'97). Berlin: Springer-Verlag, 1997. 165−179. [doi:10.1007/BFb0052234]

[2] Li FG, Liao YJ, Qin ZG, Tsuyoshi T. Further improvement of an identity-based signcryption scheme in the standard model. Computers and Electrical Engineering, 2012,38(2):413−421. [doi: 10.1016/j.compeleceng.2011.11.001]

[3] Liu ZH, Hu YP, Zhang XS, Ma H. Certificateless signcryption scheme in the standard model. Information Science, 2010,180(3): 452−464. [doi: 10.1016/j.ins.2009.10.011]

[4] Liu WH, Xu CX. Certificateless signcryption scheme without bilinear pairing. Ruan Jian Xue Bao/Journal of Software, 2011,22(8): 1918−1926 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3891.htm [doi: 10.3724/SP.J.1001.2011.03891]

[5] Pang LJ, Cui JJ, Li HX, Pei QQ, Jiang ZT, Wang YM. A new multi-receiver ID-based anonymous signcryption. Chinese Journal of Computers, 2012,34(11):2104−2113 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.02104]

[6] Zhang B, Xu QL. Identity-Based multi-signcryption scheme without random oracles. Chinese Journal of Computers, 2010,33(1): 103−110. [doi: 10.3724/SP.J.1016.2010.00103]

[7] Youn TY, Hong D. Signcryption with fast online signing and short signcryptext for secure and private communication. Science China, (E: Information Science), 2012,55(11):2530−2541. [doi: 10.1007/s11432-012-4635-2]

[8] Zhu H, Li H, Wang YM. Certificateless signcryption scheme without pairing. Journal of Computer Research and Development, 2010,47(9):1587−1594 (in Chinese with English abstract).

[9] Miao S, Zhang FT, Li SJ, Mu Y. On security of a certificateless signcryption scheme. Information Science, 2013,232:475−481. [doi: 10.1016/j.ins.2011.11.045]

[10] Weng J, Yao G, Deng RH, Chen MR, Li X. Cryptanalysis of a certificateless signcryption scheme in the standard model. Information Sciences, 2011,181(3):661−667. [doi: 10.1016/j.ins.2010.09.037]

[11] Dent AW. Hybrid signcryption schemes with insider security. In: Boyd C, Nieto JMG, eds. Proc. of the ACISP 2005. LNCS 3574, Berlin: Springer-Verlag, 2005. 253−266. [doi: 10.1007/11506157_22]

[12] Dent AW. Hybrid signcryption schemes with outside security. In: Zhou JY, Lopez J, Deng RH, Bao F, eds. Proc. of the ISC 2005. LNCS 3650, Berlin: Springer-Verlag, 2005. 203−217. [doi: 10.1007/11556992_15]

[13] Sun YX, Li H. ID-Based signcryption KEM to multiple recipients. Chinese Journal of Electronics, 2011,20(2):317−322.

[14] Selvi S, Vivek S, Rangan C. Certificateless KEM and hybrid signcryption schemes revisited. In: Kwak J, *et al*., eds. Proc. of the Information Security, Practice and Experience 2010. LNCS 6047, Berlin: Springer-Verlag, 2010. 294−307. [doi: 10.1007/978-3-642-12827-1_22]

[15] Li FG, Shirase M, Takagi T. Certificateless hybrid signcryption. Mathematical and Computer Modelling, 2013,57(3-4):324−343. [doi: 10.1016/j.mcm.2012.06.011]

[16] Wang FH, Hu YP, Wang CX. Post-Quantum secure hybrid signcryption from lattice assumption. Applied Mathematics & Information Sciences, 2012,6(1):23−28.

[17] Bjϕorsted TE, Dent AW. Building better signcryption schemes with tag-KEMs. In: Proc. of the Public Key Cryptography (PKC 2006). 2006. 491−507. [doi: 10.1007/11745853_32]

[18] Li FG, Masaaki S, Tsuyushi T. Identity-Based hybrid signcryption. In: Proc. of the 2009 Int'l Conf. on Availability, Reliability and Security. 2009. 534−539. [doi: 10.1109/ARES.2009.44]

[19] Singh K. Identity-Based hybrid signcryption revisited. In: Proc. of the 2012 Int'l Conf. on Information Technology and e-Services. Washington, 2012. 34−39. [doi: 10.1109/ICITeS.2012.6216646]

附中文参考文献:

[4] 刘文浩,许春香.无双线性配对的无证书签密机制.软件学报,2011,22(8):1918−1926. http://www.jos.org.cn/1000-9825/3891.htm [doi: 10.3724/SP.J.1001.2011.03891]

[5] 庞辽军,崔静静,李慧贤,裴庆祺,姜正涛,王育民.新的基于身份的多接收者匿名签密方案.计算机学报,2011,34(11):2104−2112. [doi: 10.3724/SP.J.1016.2011.02104]

[8] 朱辉,李晖,王育民.不使用双线性对的无证书签密方案.计算机研究与发展,2010,47(9):1587−1594.

俞惠芳(1972－),女,青海乐都人,博士,副教授,CCF 高级会员,主要研究领域为密码学与信息安全.

杨波(1963－),男,博士,教授,博士生导师,主要研究领域为密码学与信息安全.