

标准模型下基于身份的分等级加密方案

陈 宇, 祁正华, 王 翔

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘 要:给出了一种新的基于身份的分等级加密(HIBE)方案,允许用户对设置在层次结构中的多个接收者进行加密,同时支持授权密钥,以减轻密钥生成器的重要管理负担。提出方案基于标准模型,利用椭圆曲线上的双线性对和 3 个安全素数,对不同素数中的元素构造私钥,生成短的固定密文,并证明了该方案具有抗适应性选择身份向量集和选择明文攻击安全。另外,基于 Lewko 的双系统的新技术,证明了该方案的安全性。实验结果表明,加密算法只需 2 个指数运算和 2 个乘法运算;解密算法需要 1 个指数运算、1 个乘法运算和 2 个双线性对运算。与现有的 HIBE 相比,该方案具有较短的私钥长度和密文长度,减少了双线性对计算的次数,具有一定的高效性。

关键词:分等级加密;标准模型;双线性对;安全素数;抗适应性选择明文攻击

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2018)06-0110-05

doi:10.3969/j.issn.1673-629X.2018.06.025

A Hierarchical Identity-based Encryption in Standard Model

CHEN Yu, QI Zheng-hua, WANG Xiang

(School of Computer Science and Technology, Nanjing University of Posts and
Telecommunications, Nanjing 210003, China)

Abstract: We propose a new hierarchical identity-based encryption scheme which allows users to encrypt to multiple receivers organized in hierarchy, while supporting delegation of secret keys to relieve the private key generator from heavy key management burden. The scheme uses bilinear pairing on elliptic curves and three secure primes based on the standard model, constructs the private key of the elements in distinct primes and generates short fixed ciphertext, and achieves a secure against adaptively chosen-identity-vector-set and chosen-plaintext attack. In addition, its security is provable on the new technology of Lewko's dual system. The experiment shows that the encryption algorithm has only two exponent operations and two multiplication operations; and the decryption algorithm requires one exponent operation, one multiplication operation and two bilinear pairings. Compared with the existing HIBE, the improved scheme has short private key length and ciphertext length, which is efficient and reduces the number of computations of bilinear pairing.

Key words: hierarchical encryption; standard model; bilinear pairing; secure prime; against adaptive chosen-plaintext attack

0 引 言

基于身份的密码体制是由 Shamir^[1]于 1984 年提出的。在该密码体制中,用户的身份标识符可以看作公钥,而私钥由可信中心产生,目的是简化密钥管理。2001 年, Boneh 和 Franklin^[2]提出了一个实用的基于身份的加密方案(identity-based encryption, IBE),该方案使用双线性映射并基于随机预言机模型证明了安全性,但安全性较弱。在 Boneh 和 Boyen^[3]的方案中,第一次提出无随机的构造方案,给出了基于 BDH 假设的高效 IBE,但其为较弱模型(selective-ID 模型)。2005 年, Waters^[4]提出了一个更高效的 IBE,使方案的安全

性规约降低,这是对 Boyen 方案的极大改进。2006 年, Gentry^[5]根据 Waters 的方案,提出一个更高效的 IBE。此后,基于身份的密码体制得到了快速发展。如签密技术,文献[6-8]给出了有关新的签密方案。2002 年, Horwitz 和 Lynn^[9]提出了 IBE 的概念,将用户身份分配在层次结构中,密钥生成器(PKG)可以将私钥生成和身份认证委托给子机构。第一个功能齐全的 HIBE 方案由 Gentry 和 Silverberg^[10]提出并证明是自适应身份安全的。

数据共享系统中的用户数可能很大^[11],随着用户数的增加,PKG 可能负担不起, HIBE^[12]以树状结构组

收稿日期:2017-07-09

修回日期:2017-11-22

网络出版时间:2018-02-24

基金项目:国家自然科学基金(61073188)

作者简介:陈 宇(1991-),男,硕士研究生,研究方向为网络与信息安全;祁正华,副教授,博士,研究方向为网络与信息安全。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20180224.1510.012.html>

织用户^[9-10,13-19]来解决 PKG 的负担。Seo^[12]提出了短密文匿名 HIBE,其方案中的密文由 4 个群元素组成,不依赖方案的等级深度,具有较高的实用性;但是 Seo 的方案是基于弱模型^[20]证明的,所以文中采用 3 个安全素数,对不同素数中的元素构造私钥,生成短的固定密文,并正确解密。

1 预备知识

1.1 双线性对

输入安全参数 λ , 输出双线性组 (N, G, G_T, e) , 阶为 $N = p_1 p_2 p_3$, p_1, p_2, p_3 是 3 个安全素数。设 G, G_T 是一个阶为 N 的循环群, g 是群 G 的生成元, 称 $e: G \times G \rightarrow G_T$ 是一个双线性映射, 当且仅当其满足以下性质。

(1) 双线性: 对于 $\forall g, g_1 \in G, a, b \in \mathbb{Z}_p^*, \mathbb{Z}_p^*$ 为模 p 的整数乘法群, 有: $e(g^a, g_1^b) = e(g, g_1)^{ab}$;

(2) 非退化性: 存在一个元素 $g \in G$, 使得 $e(g, g)$ 在 G_T 中具有 N 阶;

(3) 可计算性: 对于任意的 $u, v \in G$, 存在一个有效的多项式时间算法来计算 $e(u, v)$ 。

1.2 复杂性假设

通过 Katz^[21] 方案框架证明假设的安全性, 通过 Lewko^[17] 的新技术找出 N 的非平凡因子的困难性。

假设 1: g 是 G_{p_1} 中的生成元, 令 $X_3 \in G_{p_3}, E_1 = (g, X_3), T_1 \in G_{p_1 p_2}, T_2 \in G_{p_1}$, 定义敌手 Λ 打破假设 1 的优势为: $\text{Adv}_{1,\Lambda}(\lambda) = |\Pr[\Lambda(E_1, T_1) = 1] - \Pr[\Lambda(E_1, T_2) = 1]|$ 。

定义 1: 若 Λ 的优势 $\text{Adv}_{1,\Lambda}(\lambda)$ 是可忽略的, 则假设 1 成立。

假设 2: 令 $X_1 \in G_{p_1}, X_2, Y_2 \in G_{p_2}, X_3, Y_3 \in G_{p_3}$, 令 $E_2 = (g, X_1 X_2, X_3, Y_2 Y_3), T_1 \in G_{p_1 p_2 p_3}, T_2 \in G_{p_1 p_3}$, 定义 Λ 打破假设 2 优势为: $\text{Adv}_{2,\Lambda}(\lambda) = |\Pr[\Lambda(E_2, T_1) = 1] - \Pr[\Lambda(E_2, T_2) = 1]|$ 。

定义 2: 若 Λ 的优势 $\text{Adv}_{2,\Lambda}(\lambda)$ 是可忽略的, 则假设 2 成立。

假设 3: 令 $X_2, Y_2, Z_2 \in G_{p_2}, X_3 \in G_{p_3}, \alpha, s \in \mathbb{Z}_p^*$, 令 $E_3 = (g, Z_2, X_3, g^\alpha X_2, g^s Y_2), T_1 = e(g, g)^\alpha, T_2 \in G_T$ 。定义 Λ 打破假设 3 的优势为: $\text{Adv}_{3,\Lambda}(\lambda) = |\Pr[\Lambda(E_3, T_1) = 1] - \Pr[\Lambda(E_3, T_2) = 1]|$ 。

定义 3: 若 Λ 的优势 $\text{Adv}_{3,\Lambda}(\lambda)$ 是可忽略的, 则假设 3 成立。

1.3 基于身份的分等级加密方案的架构

一个 HIBE 由四种算法构成^[22]: 系统建立、密钥提取、加密和解密。

系统建立 (setup): 输入安全参数 λ , 输出主密钥 g^α 和公共参数 PK。

密钥提取 (extract): 输入用户身份向量 I 及其对应的私钥 SK_I , 输出对应私钥 SK_I 。

加密 (encrypt): 输入 PK、 I 和消息 M , 输出密文。

解密 (decrypt): 输入 PK、 I 的密文和私钥 SK_I , 输出明文或不合法判定。

1.4 基于身份的分等级加密方案的安全模型

文中的安全模型具有抗适应性选择身份 (向量集) 和选择明文攻击 (IND - CIVS - CPA) 的密文不可区分性, 具体定义如下:

系统建立。挑战者 ζ 运行建立算法, 将 PK 给 Λ 并初始化集合 S 。

阶段 1: Λ 进行两种适应性询问。

密钥提取。 ζ 生成用户身份 I_{id_i} 的私钥 SK_{id_i} 并将其给 Λ 。

解密。 ζ 运行密钥提取算法得到身份 I_{id_i} 的私钥 SK_{id_i} , 用 SK_{id_i} 解密 Λ 提交的密文, 并将解密后的消息发给 Λ 。

挑战。当阶段 1 结束, Λ 输出两个等长明文消息 M_0, M_1 , 同时输出一个挑战身份 T^* 。 ζ 随机选取一个比特 $b \in \{0, 1\}$, 记 M_0, M_1 中要加密的明文为 M_b , 将挑战密文 CT 发送给 Λ 。

阶段 2: 敌手继续进行以下询问。

密钥提取。设询问的身份为 $I_{\text{id}_i}, I_{\text{id}_i} \neq T^*$ 且不能是 T^* 的前一级。

解密。询问的密文 $\text{CT} \neq \text{CT}^*$ 。

猜想。 Λ 输出一个猜测 $b' \in \{0, 1\}$, 如果 $b = b'$, 则 Λ 赢得游戏。

此游戏中, 敌手的优势定义为:

$$\text{Adv}_{\Lambda}^{\text{IND-CIVS-CPA}}(\lambda) = |\Pr[b = b'] - 1/2|$$

定义 4: 若多项式时间 t 内, Λ 在以上游戏中进行了至多 q_{id_i} 次密钥询问, 其优势 $\text{Adv}_{\Lambda}^{\text{IND-CIVS-CPA}}(\lambda)$ 是可忽略的, 则称一个 HIBE 是 (t, q_{id_i}) 安全的。

Canetti^[23] 提出将具有抗适应性选择明文攻击转化为抗适应性选择密文攻击的方案。Gentry^[24] 提出一种半静态安全, 在此概念中, Λ 在系统建立前必须先提交一个身份集合 S , Λ 无法查询 S 中任何用户的私钥, 但可以攻击任何目标集 $S' \subseteq S$ 。

2 基于身份的分等级加密方案

选择 Hash 函数 $H: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$, 设用户身份的最大深度为 ℓ , 用户最大数为 ι 。令 $I_{\text{id}_i} = (\text{id}_1, \text{id}_2, \dots, \text{id}_\ell) \in (\mathbb{Z}_p^*)^\ell$, 选择一个双线性循环群 G , 其阶为 $N = p_1 p_2 p_3$, 双线性映射 $e: G \times G \rightarrow G_T$, 安全参数 k 决定群的规模。算法具体构造如下:

系统建立: 设 g 为 G_{p_1} 的任一生成元, 并随机选择

$g_1 \in G_{p_1}, X_3 \in G_{p_3}, \alpha \in Z_p^*$ 。随机选取 $h_i \in G_{p_1} (i \in [1, \iota])$, 令 $\omega = e(g, g)^\alpha$, 则 $PK = \{G, G_T, e, N, g, g_1, h_1, \dots, h_i, X_3, \omega\}$, 主密钥为 g^α 。

密钥提取: 身份向量 $I_{ID_i} = (ID_1, ID_2, \dots, ID_i), i \leq \iota$, 随机选取 $r \in Z_p^*, N_0, N_1, H_j \in G_{p_3} (j \in [1, \iota])$, 输出 $SK_{ID_i} = (g^\alpha (g_1 \prod_{i \in I_{ID_i}} h_i^{ID_i})^r N_0, g^r N_1, \{h_j^r H_j\}_{j \in [1, \iota]})$ 。则得出一个私钥 $SK_{ID_i} = (g^\alpha (g_1 \prod_{i \in I_{ID_i}} h_i^{ID_i})^r N_0, g^r N_1, \{h_j^r H_j\}_{j \in [1, \iota]}) = (d_0, d_1, \{u_j\}_{j \in [1, \iota]})$, 使 $I_{ID} = (I_{ID_i}, I_{ID_i})$, 随机选取指数 $\delta \in Z_p^*, \tilde{N}_0, \tilde{N}_1, \tilde{H}_j \in G_{p_3} (j \in [1, \iota])$, 然后再输出 $SK_{ID} = (d_0 u_i (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^\delta \tilde{N}_0, d_1 g^\delta \tilde{N}_1, \{u_j h_j^\delta \tilde{H}_j\}_{j \in [1, \iota]})$, 其中 $r = (r' + \delta) \in Z_p^*, N_0 = (N_0' H_i' \tilde{N}_0) \in G_{p_3}, N_1 = (N_1' \tilde{N}_1) \in G_{p_3}, H_j = (H_j' \tilde{H}_j) \in G_{p_3}$, 得出新的私钥: $SK_{ID} = (g^\alpha (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^r N_0, g^r N_1, \{h_j^r H_j\}_{j \in [1, \iota]})$ 。

加密: 选取 $s \in Z_p^*$, 输出密文: $CT = (C_0, C_1, C_2)$, 其中 $C_0 = M \cdot \omega^{\alpha s}, C_1 = g^s, C_2 = (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^s$ 。

解密: 得到密文 $CT = (C_0, C_1, C_2)$, 计算 $C^* = d_0 \prod_{j \in I_{ID}} u_j^{ID_j} = g^\alpha (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^r (N_0 \prod_{j \in I_{ID}} H_j)$, 则计算并返回 $M = C_0 \cdot e(d_1, C_2) \cdot (e(C_1, C^*))^{-1}$ 。

3 安全性分析

3.1 正确性

正确性证明如下:

$$C_0 \cdot e(d_1, C_2) \cdot (e(C_1, C^*))^{-1} =$$

$$\begin{aligned} & M \cdot \omega^{\alpha s} \frac{e(g^r N_1, (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^s)}{e(g^s, g^\alpha (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^r (N_0 \prod_{j \in I_{ID}} H_j))} = \\ & M \cdot \omega^{\alpha s} \frac{e(g^r, (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^s)}{e(g^\alpha, g^s) \cdot e(g^s, (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^r)} = M \end{aligned}$$

3.2 安全性

文中遵循 Lewko^[17] 方案中的证明框架。

定理 1: 若定义 1~3 成立, 则文中的 HIBE 具有抗适应性选择明文攻击安全。

半功能密文: 令 g_2 是 G_{p_2} 的生成元, 得到一组标准密文 $CT = (C_0', C_1', C_2')$, 随机选取 $x, y_c \in Z_p^*$, 设置: $C_0 = C_0', C_1 = C_1' g_2^{y_c}, C_2 = C_2' g_2^x$ 。

半功能密钥: 用户身份 I_{ID_i} 调用密钥提取算法, 生成标准密钥 $SK_{ID_i} = (d_0', d_1', \{u_j\}_{j \in [1, \iota]})$; 随机选取 $\psi, y_k, z_j \in Z_p^* (j \in [1, \iota])$, 设置半功能密钥为: $d_0 =$

$$d_0' g_2^\psi, a_1 = d_1' g_2^{\psi y_k}, \{u_j = u_j' g_2^{\psi z_j}\}_{j \in [1, \iota]} \circ$$

解密: 当使用标准密钥或半功能密钥解密半功能密文时, 解密算法将正确输出明文消息 M , 因为 G_{p_2} 中添加的元素将由于正交性而被取消。当使用半功能密钥尝试解密半功能密文时, 盲化因子中将出现附加元素 $e(g_2, g_2)^{x\psi(y_k - y_c)}$, 除非 $y_k = y_c$ 概率为 $1/N$ 。

下面通过一些游戏来证明方案的安全性。

Game_R: 真实的游戏。

Game_{RT}: $\exists I_{ID^*} = (ID_1^*, ID_2^*, \dots, ID_n^*)_{n \leq n} \in T^*, \Lambda$ 不能询问用户身份 $I_{ID} = (ID_1, ID_2, \dots, ID_n)$, 如 $V_{i \in [1, n]}, I_{ID} = I_{ID} \cdot \text{mod}_{p_2} \circ$

Game_k: 假设 Λ 在阶段 1 和阶段 2 中能进行最大 q 次密钥的查询, 则挑战密文是半功能的, 且返回给敌手 Λ 的前 k 个密钥也是半功能的, 而其他密钥都是标准的。在 Game₀ 中, 只有返回的挑战密文是半功能的; 在 Game_q 中, 返回的挑战密文以及所有的密钥都是半功能的。

Game_F: 相同于 Game_q, 挑战密文是随机消息进行加密所得的半功能密文。

令 $\text{Adv}_R^{\text{CPA}}(\lambda), \text{Adv}_{\text{RT}}^{\text{CPA}}(\lambda), \text{Adv}_K^{\text{CPA}}(\lambda), \text{Adv}_0^{\text{CPA}}(\lambda), \text{Adv}_q^{\text{CPA}}(\lambda), \text{Adv}_F^{\text{CPA}}(\lambda)$ 分别代表 Game_R, Game_{RT}, Game_K, Game₀, Game_q, Game_F 的优势。

引理 1: 若假设 2 成立, 则多项式时间算法无法以不可忽略的优势将 Game_R 和 Game_{RT} 区分开来。

证明: 若 Λ 能以 ε 的优势区分 Game_R 和 Game_{RT}, 根据 Game_{RT} 的定义, Λ 可以从用户身份 $I_{ID} = (ID_1, ID_2, \dots, ID_n)$ 中进行密钥询问, 满足 $\exists I_{ID^*} = (ID_1^*, ID_2^*, \dots, ID_n^*)_{n \leq n} \in T^*$, 如果 $V_{i \in [1, n]}, I_{ID} = I_{ID} \cdot \text{mod}_{p_2}$, 然后计算 $\gcd(ID_i - ID_i^*, N)$ 来提取 N 因子。在这个引理 5^[25] 的证明中, 建立了一个相似的算法, 以验证假设 2 的优势为 $\text{Adv}_{2,r}(\lambda) \geq \varepsilon/2$ 。

引理 2: 若假设 1 成立, 则多项式时间算法无法以不可忽略的优势将 Game_{RT} 和 Game₀ 区分开来。

证明: 构造算法 Γ 并输入 g, X_3, T , 随机选择 $\alpha \in Z_p^*, \psi_i \in Z_p^* (i \in [0, \iota]), g_1 = g^{\psi_0}, h_i = g^{\psi_i} (i \in [1, \iota])$, 设置 $\omega = e(g, g)^\alpha$, 则公共参数 $PK = (g, g_1, h_1, \dots, h_i, X_3, \omega)$, Γ 把 PK 给 Λ , 并设置主密钥为 g^α 。每当 Γ 被询问身份 ID_i 对应的密钥时, 随机选取 $r, w_0, w_1, v_j \in Z_p^* (j \in [1, \iota])$, 然后 Γ 返回一个标准密钥: $SK_{ID} = (g^\alpha (g_1 \prod_{i \in I_{ID}} h_i^{ID_i})^r X_3^{w_0}, g^r X_3^{w_1}, \{h_j^r X_3^{v_j}\}_{j \in [1, \iota]})$ 。

Λ 给 Γ 发送两个明文消息 $M_0, M_1 \in G_T$ 和 T^*, Γ 选择一个随机比特 $b \in \{0, 1\}$, 返回密文如下: $CT = (C_0', C_1', C_2') = (M_b \cdot e(g, T)^\alpha, T, T^{\psi_0 + \sum_{i=1}^{\iota} ID_i \cdot \psi_i})$ 。若 $T \in G_{p_1}$, 则这是一个标准密文; 如果 $T \in G_{p_2}$, 则这是一个半功能密文。

引理3:若假设2成立,则多项式时间算法无法以不可忽略的优势将 Game_{k-1} 和 Game_k 区分开来。

证明: Γ 输入 $g, X_1X_2, X_3, Y_2X_3, T$, 且运行系统建立算法, $\text{PK} = (g, g_1, h_1, \dots, h_\iota, X_3, \omega)$, 随机选取 r , $w_0, w_1, v_j \in Z_p^* (j \in [1, \iota])$, 返回密钥为:

$$\text{SK}_{\text{ID}} = (g^\alpha (g_1 \prod_{i \in I_{\text{ID}}} h_j^{\text{ID}_i})^r (Y_2Y_3)^{w_0}, g^r (Y_2Y_3)^{w_1}, \{h_j^r (Y_2Y_3)^{v_j}\}_{j \in [1, \iota]}).$$
 这是一个半功能密文, 设 $g_2^\psi = Y_2^{w_0}, y_k = \frac{w_1}{w_0}$ 。

若 Λ 询问密钥 $\ell (\ell \in [k, q])$ 次, Γ 运行密钥生成一组标准的密钥, 并返回给 Λ 。若 Λ 询问密钥 k 次, Γ 随机选择一个 $w_0, v_j \in Z_p^* (j \in [1, \iota])$, 输出密钥 $\text{SK}_{\text{ID}} = (g^\alpha T^{\psi_0 + \sum_{i \in I_{\text{ID}}} \text{ID}_i \cdot \psi_i} X_3^{w_0}, T, \{T^{\psi_j} X_3^{v_j}\}_{j \in [1, \iota]}).$ 若 $T \in G_{p, p_3}$, 其密钥都在 G_{p, p_3} 中, 则密钥是一个标准密钥, 否则为半功能密钥, 设 $y_k = \psi_0 + \sum_{i \in I_{\text{ID}}} \text{ID}_i \cdot \psi_i$ 。

挑战: Γ 从 Λ 中输出两个等长的消息 $M_0, M_1 \in G_T$ 和一个挑战者的身份 ID' 。 Γ 随机选取 $b \in \{0, 1\}$, 并返回 $\text{CT}' = (C'_0, C'_1, C'_2) = (M_b \cdot e(g, X_1X_2)^\alpha, X_1X_2, (X_1X_2)^{\psi_0 + \sum_{i \in I_{\text{ID}}} \text{ID}_i \cdot \psi_i})$ 给 Λ 。设 $y_c = \psi_0 + \sum_{i \in I_{\text{ID}}} \text{ID}_i \cdot \psi_i$ 。在 Game_{RT} 中, $\text{ID}_k \neq \text{ID}'_{\psi} \bmod p_2$, Λ 可将 y_c 和 y_k 看作是随机分布的。所以 y_c 和 y_k 的关系是有助于 Λ 区分 Game_{k-1} 和 Game_k 的。

虽然 y_c 和 y_k 的关系对 Λ 是隐藏的, 但是它们阻止了算法 Γ 测试用户 $I_{\text{ID}_i} \in T^*$ 的私钥 SK_{ID_i} 是否为半功能, 并尝试用私钥 SK_{ID_i} 来解密。设 $y_c = y_k + \sum_{i \in I_{\text{ID}}} \text{ID}_i \cdot \psi_i (I_{\text{ID}_i} = \{i: \text{ID}_i \in S_{I_{\text{ID}}}\}, I_{\text{ID}_i} = \{i: \text{ID}_i \in S_{T^*}\})$ 。若 $T \in G_{p, p_3}$, 即 Γ 生成私钥 $\text{SK}_{I_{\text{ID}}} \subset G_{p, p_3}$, 那么它是一个标准密钥, Γ 正确模拟了 Game_{k-1} ; 若 $T \in G_{p, p_2 p_3}$, 则密钥是半

功能的, Γ 正确模拟了 Game_k 。若 Λ 能够以 ε 的优势区分这两个游戏, 那么 Γ 能利用 Λ 以 ε 的优势区分 T 的两种可能。

引理4:若假设3成立,则多项式时间算法无法以不可忽略的优势将 Game_q 和 Game_F 区分开来。

证明: Γ 输入 $(g, Z_2, X_3, g^\alpha X_2, g^\alpha Y_2, T)$, 判断 $T = e(g, g)^\alpha$ 或者 $T \in G_T$ 的随机元素。随机选取 $\psi_i \in Z_p^* (i \in [1, \iota])$, 设 $g_1 = g^{\psi_0}, h_1 = g^{\psi_1}, \dots, h_\iota = g^{\psi_\iota}, \omega = e(g, g)^\alpha = e(g^\alpha X_2, g)$, 那么 $\text{PK} = (g, g_1, h_1, \dots, h_\iota, X_3, \omega)$ 。当 Λ 询问身份 I_{ID_i} 的私钥时, Γ 随机选取 $w_0, w_1, a_0, a_1, v_j, z_j \in Z_p^* (j \in [1, \iota])$, 输出: $\text{SK}_{\text{ID}_i} = (g^\alpha X_2 (g_1 \prod_{i \in I_{\text{ID}}} h_j^{\text{ID}_i})^r Z_2^{a_0} X_3^{w_0}, g^r Z_2^{a_1} X_3^{w_1}, \{h_j^r Z_2^{z_j} X_3^{v_j}\}_{j \in [1, \iota] \cup I_{\text{ID}}})$ 。这里设 $g_2^\psi = Z_2^{a_0}, y_k = \frac{a_1}{a_0}$ 。

挑战: Γ 从 Λ 中输出两个等长的消息 $M_0, M_1 \in G_T$ 和一个挑战者的身份 ID' 。 Γ 随机选取 $b \in \{0, 1\}$, 并返回 $\text{CT}' = (C'_0, C'_1, C'_2) = (M_b \cdot T, g^\alpha Y_2, (gY_2)^{\psi_0 + \sum_{i \in I_{\text{ID}}} \text{ID}_i \cdot \psi_i})$ 给 Λ 。

猜测:若在 Game_q 中模拟正确, 则 CT' 是消息 M_b 对应的半功能密文, Γ 输出 $T = e(g, g)^\alpha$; 如果在 Game_F 中模拟正确, 则 CT' 是一个随机加密的半功能密文, Γ 输出 $T \in G_T$ 。因此, 若 Λ 以 ε 的优势区分 Game_q 和 Game_F , 那么 Γ 以 $\text{Adv}_F(\lambda) \geq \varepsilon$ 区分 T 的不同可能。

因此, 若三个假设成立, 文中的 HIBE 是抗选择明文攻击安全的。

4 性能分析

效率对比如表1所示。

表1 HIBE 方案效率对比

方案	公共参数长度	私钥长度	密文长度	解密中双线性对运算个数	安全模型	复杂性假设
文献[2]	$\ell + 3$	$\ell + 2$	$\ell + 3$	$\ell + 2$	Selective-ID	DBDH
文献[3]	$\ell + 3$	ℓ	ℓ	$\ell + 3$	Selective-ID	BDH
文献[17]	$\iota + 5$	$\ell + 2$	3	ℓ	Adaptive-ID	静态
文献[18]	$\iota + 5$	ℓ	5ℓ	5ℓ	Adaptive-ID	静态
文献[19]	$\iota + 4$	$3(\iota - \ell + 3)$	4	3	Selective-ID	静态
文中	$\iota + 4$	$\iota - \ell + 2$	3	2	Adaptive-ID	静态

5 结束语

给出了一种基于身份的分等级加密方案, 该方案中密文的长度和计算量都比较低, 且密文的大小不依赖等级的深度, 在标准模型中的3个静态假设都是有效的, 满足抗选择明文攻击安全。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proceedings of CRYPTO 84 on advances in cryptology. New York:Springer-Verlag,1985:47-53.
[2] BONEH D,FRANKLIN M. Identity-based encryption from the Weil pairing [C]//Advances in cryptology - CRYPTO

2001. Berlin; Springer, 2001; 213–229.
- [3] BONEH D, BOYEN X. Efficient selective-ID secure identity-based encryption without random oracles [C]//International conference on the theory and applications of cryptographic techniques. Berlin; Springer, 2004; 223–238.
 - [4] WATERS B. Efficient identity-based encryption without random oracles [C]//Advances in cryptology – EUROCRYPT 2005. Aarhus, Denmark; [s. n.], 2005; 114–127.
 - [5] GENTRY C. Practical identity-based encryption without random oracles [C]//Proceedings of the 24th annual international conference on theory and applications of cryptographic techniques. [s. l.]: [s. n.], 2006; 445–464.
 - [6] QI Zhenghua, YANG Geng, REN Xunyi. Provably secure certificateless ring signcryption scheme [J]. China Communications, 2011, 8(3): 99–106.
 - [7] QI Zhenghua, REN Xunyi, YANG Geng. Provably secure general aggregate signcryption scheme in the random oracle model [J]. China Communications, 2012, 9(11): 107–116.
 - [8] REN Xunyi, QI Zhenghua, YANG Geng. Provably secure aggregate signcryption scheme [J]. ETRI Journal, 2012, 34(3): 421–428.
 - [9] HORWITZ J, LYNN B. Toward hierarchical identity-based encryption [C]//Advances in Cryptology – EUROCRYPT 2002. Amsterdam, The Netherlands; [s. n.], 2002; 466–481.
 - [10] GENTRY C, SILVERBERG A. Hierarchical ID-based cryptography [C]//Advances in cryptology – ASIACRYPT. New Zealand; [s. n.], 2002; 548–566.
 - [11] HUANG Xinyi, LIU J K, TANG Shaohua, et al. Cost-effective authentic and anonymous data sharing with forward security [J]. IEEE Transactions on Computers, 2015, 64(4): 971–983.
 - [12] SEO J H, EMURA K. Revocable identity-based encryption revisited; security model and construction [C]//16th international conference on practice and theory in public-key cryptography. Nara, Japan; [s. n.], 2013; 216–234.
 - [13] HU Chengyu, LIU Pengtao, GUO Shanqing, et al. Anonymous hierarchical identity-based encryption with bounded leakage resilience and its application [J]. International Journal of High Performance Computing and Networking, 2017, 10(3): 226–239.
 - [14] LIU Weiran, LIU Jianwei, WU Qianhong, et al. Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption [J]. International Journal of Information Security, 2016, 15(1): 35–50.
 - [15] XING Qianqian, WANG Baosheng, WANG Xiaofeng, et al. Unbounded revocable hierarchical identity-based encryption with adaptive-ID security [C]//IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems. [s. l.]: IEEE, 2016; 430–437.
 - [16] LIANG Kaitai, SUSILO W, LIU J K, et al. Efficient and fully CCA secure conditional proxy re-encryption from hierarchical identity-based encryption [J]. The Computer Journal, 2015, 58(10): 2778–2792.
 - [17] LEWKO A, WATERS B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts [C]//Proceedings of the 7th international conference on theory of cryptography. Zurich, Switzerland; Springer-Verlag, 2010; 455–479.
 - [18] TSAI T T, TSENG Y M, WU T Y. RHIBE: constructing revocable hierarchical ID-based encryption from HIBE [J]. Informatica, 2014, 25(2): 299–326.
 - [19] SEO J H, KOBAYASHI T, OHKUBO M, et al. Anonymous hierarchical identity-based encryption with constant size ciphertexts [C]//Proceedings of the 12th international conference on practice and theory in public key cryptography. CA; Springer-Verlag, 2009; 215–234.
 - [20] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme [C]//Advances in cryptology – EUROCRYPT 2003. Warsaw, Poland; Springer-Verlag, 2003; 255–271.
 - [21] KATZ J, SAHAI A, WATERS B. Predicate encryption supporting disjunctions, polynomial equations, and inner products [C]//Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on advances in cryptology. [s. l.]: [s. n.], 2008; 146–162.
 - [22] 王 皓. 基于身份密码体制的研究 [D]. 济南: 山东大学, 2012.
 - [23] CANETTI R, HALEVI S, KATZ J. Chosen-ciphertext security from identity-based encryption [C]//Advances in cryptology – EUROCRYPT 2004. Berlin; Springer, 2004; 207–222.
 - [24] GENTRY C, WATERS B. Adaptive security in broadcast encryption systems (with short ciphertexts) [C]//Proceedings of the 28th annual international conference on advances in cryptology: the theory and applications of cryptographic techniques. [s. l.]: [s. n.], 2009; 171–188.
 - [25] CHOW S S M, YIU S M, HUI L C K, et al. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity [C]//International conference on information security and cryptology. Berlin; Springer, 2003; 352–369.