中国科学: 信息科学 2023 年 第 53 卷 第 5 期: 918–930
SCIENTIA SINICA Informationis
论文

基于商用密码 SM9 的高效分层标识加密

赖建昌[1], 黄欣沂[2*], 何德彪[3], 郭福春[4]

1. 东南大学网络空间安全学院, 南京 211189, 中国
2. 福建师范大学计算机与网络空间安全学院, 福建省网络安全与密码技术重点实验室, 福州 350117, 中国
3. 武汉大学国家网络安全学院, 空天信息安全与可信计算教育部重点实验室, 武汉 430072, 中国
4. School of Computing and Information Technology, University of Wollongong, Wollongong 2522, Australia
* 通信作者. E-mail: xyhuang81@gmail.com

收稿日期: 2022–04–25; 修回日期: 2022–06–12; 接受日期: 2022–07–13; 网络出版日期: 2023–05–04

国家自然科学基金 (批准号: 62032005, 61902191, U21A20466)、湖北省自然科学基金 (批准号: 2020CFA052)、湖北省重点研发计划 (批准号: 2020AEA013, 2021BAA025) 和武汉市科技计划 (批准号: 2020010601012187) 资助项目

摘要 分层标识加密能有效减轻标识密码体制中密钥生成中心生成用户私钥和分发私钥的工作量. SM9 标识密码作为我国商用密码行业标准和国家标准, 在金融、政务等方面起着重要的作用, 但 SM9 标识加密算法不具备分层加密的功能, 不适合大规模网络的应用场景, 阻碍了 SM9 加密算法的部署. 本文基于商用密码 SM9 标识加密算法提出一个高效的分层标识加密方案 SM9-HIBE. 相比 SM9 标识加密算法, 方案的密文只增加一个群元素, 解密开销只增加一个双线性对运算, 与接收者标识的长度无关. 方案的安全性基于判定性 BDHI 困难问题, 在随机谕言模型中可证明方案满足静态选择明文攻击模型下的不可区分性. 最后, 对方案进行比较分析, 结果表明 SM9-HIBE 在计算开销和通信代价方面与现有 HIBE 方案是可比的.

关键词 分层加密, 标识密码, SM9, 密钥封装, 选择明文安全

1 引言

在标识密码 (identity-based cryptography, IBC)[1] 系统中, 不需要通过证书保证用户公钥的有效性, 用户的公钥可以是能唯一标识用户的任意字符串, 比如电话号码、邮箱地址等, 有效消除了传统公钥体制中证书的管理、验证等问题. 2001 年, Boneh 和 Franklin[2] 在 International Cryptology Conference (CRYPTO) 上提出首个实用且可证明安全的标识加密方案, 方案的设计巧妙地应用了椭圆曲线上的双线性对技术. 此后, 标识密码在学术界和工业界得到大量的研究与应用. 标识密码体制无需证书绑定用户的公钥, 但用户的私钥不再由自己生成, 而是通过第三方可信机构 – 密钥生成中心 (private key generator, PKG) 生成. PKG 首先通过物理方法验证用户身份的有效性, 然后利用自身的主私钥和用

引用格式: 赖建昌, 黄欣沂, 何德彪, 等. 基于商用密码 SM9 的高效分层标识加密. 中国科学: 信息科学, 2023, 53: 918–930, doi: 10.1360/SSI-2022-0163
Lain J C, Huang X Y, He D B, et al. Efficient hierarchical identity-based encryption based on SM9 (in Chinese). Sci Sin Inform, 2023, 53: 918–930, doi: 10.1360/SSI-2022-0163

户的标识计算相应的私钥并通过安全信道发送给用户, 用户的私钥与 PKG 的主私钥绑在一起. 由于每个用户的私钥必须通过 PKG 生成和发送, 当系统中用户数量很大时, PKG 对标识的验证, 私钥的计算和传输等工作负荷激增, 极易造成网络拥堵, 无法提供实时性服务, 导致整个系统的效率下降. 标识密码中单个 PKG 的体系在大型网络中已成为应用的瓶颈.

为有效减少单个 PKG 的工作负荷, Horwitz 和 Lynn [3] 在 2002 年的欧密会上提出分层标识加密 (hierarchical identity-based encryption, HIBE) 的概念, 并给出了 HIBE 的形式化定义和安全模型. 在 HIBE 系统中, 根据标识的长度把用户分为不同层级用户, 上一层用户 (称为节点 PKG) 可以利用自己的私钥和系统公共参数为下一层用户生成私钥, 该私钥与 IBC 系统中单个 PKG 生成的私钥具有相同的有效性, 即该私钥可用于解密密文恢复出正确的明文. HIBE 的安全性要求用户即使合谋也无法生成其上一层节点 PKG 的有效私钥. IBC 系统中的 PKG 在该系统中属于顶层 PKG 或称为根节点 PKG, 可以把用户标识认证, 私钥生成和发送工作分配给下层节点 PKG, 顶层 PKG 只负责给下一层 PKG 生成私钥. 通过层级间用户私钥向下代理生成的方式, 极大地减轻了顶层 PKG 的工作量, 有效提高了整个系统的效率. 此外, HIBE 能有效解决 IBC 系统中单个 PKG 主私钥泄露导致的安全问题. 如果某个节点 PKG 的主私钥泄露或者被腐化了, 只影响该 PKG 下层用户私钥的安全性, 对其他节点的私钥没有影响, 进一步提升了系统的健壮性. 当系统的总层数为 1 时, HIBE 与 IBE 是等价的. 因此, HIBE 中的层数通常默认大于 1.

由于标识密码体制能有效消除证书, 自标识密码概念被提出后得到广泛的研究与应用, 特别是在椭圆曲线双线性对技术可用于构造高效的标识密码方案后, 但主要围绕国外设计的算法展开. 为实现我国核心技术自主可控的战略需求, 我国密码管理局于 2006 年开始组织我国商用密码行业标准的制定, 并自主设计了我国商用密码 SM9 标识密码算法 [4], 包括数字签名、密钥交换、密钥封装和公钥加密. SM9 标识密码于 2020 年成为国家标准, 2021 年成为 ISO/IEC 国际标准, 在国内外的影响日益突出. 然而, SM9 密码算法属于标识密码, 系统中用户的私钥只能由 PKG 生成, 当用户数量很大时, 同样存在单个 PKG 工作负荷较大导致系统效率低下的问题. 虽然国内学者对 SM9 展开了积极的研究并取得了优秀的成果, 包括算法的安全性分析 [5,6]、椭圆曲线计算的算法优化 [7,8]、数字签名的扩展 [9,10]、多用户的实现 [11] 等, 但目前尚未在密码学国际主流期刊和学术会议上发现有关 SM9 分层加密的研究.

本文基于商用密码 SM9 标识加密算法, 提出一个高效的分层标识加密方案记为 SM9-HIBE. 方案的设计基于素数阶群, 为更好地融合 SM9 系列密码算法, 本文只给出 SM9-HIBE 密钥封装, 生成封装密钥后, 可根据 SM9 加密算法完成数据的加密和解密. 在 SM9-HIBE 中, 用户的私钥可由上层 PKG 直接生成, 顶层 PKG 无需为每个用户生成私钥, 只需为其下一层节点 PKG 生成私钥, 极大地减轻了 IBC 系统中单个 PKG 的工作负荷. 方案中密文的长度是固定的, 由两个群元素组成, 解密算法只包括两个双线性对运算, 与系统支持的最大层数或用户的标识长度无关, 效率较高. 代价是系统的公钥长度和用户的私钥长度都是线性的. 基于非对称群上判定性 (q,n)-BDHI 问题的难解性, 我们在随机谕言模型中证明 SM9-HIBE 方案满足静态选择明文攻击模型下的不可区分安全性. 最后, 比较分析表明方案在计算效率和通信效率方面与现有 HIBE 方案是可比的.

2 相关工作

1984 年, Shamir [1] 提出了标识密码的概念, 目的是消除传统公钥体制中的证书问题. 在该系统中, 用户的公钥不再由证书给出, 而是任意一个可唯一标识用户的字符串, 用户的私钥通过密钥生成中心

PKG 生成, 密码学的研究从此进入一个新阶段. 直到 2001 年, Boneh 和 Franklin [2] 才给出第一个实用且可证明安全的标识加密方案, 方案的设计巧妙地利用了椭圆曲线上的双线性配对技术, 并在随机谕言模型中分析了方案的安全性. 随后, Boneh 和 Boyen [12] 给出了非随机谕言模型 (也称为标准模型) 下可证明安全的标识加密方案, 但方案只满足静态选择明文攻击 (indistinguishability against selective identity chosen-plaintext attacks, IND-sID-CPA) 的安全性. Waters [13] 提出在标准模型中具有自适应性 (adaptive) 选择明文安全的加密方案. 相比于静态安全性, 适应性安全性不要求攻击者在获知系统公开参数之前给出挑战目标, 攻击者允许在结束询问后根据获得的询问回复自由的选取挑战目标, 给予攻击者更多的选择. 因此, 适应性安全性的安全强度高于静态安全性. 由于挑战目标的不确定性, 模拟者无法在生成系统公开参数时嵌入挑战目标, 一定程度上增加了安全规约的难度. Gentry [14] 进一步提升标准模型中加密方案的安全性, 提出标准模型下可证明满足选择密文攻击安全 (indistinguishability against chosen-ciphertext attacks, IND-CCA) 的实用标识加密方案, 攻击者可询问非挑战密文的解密. 上述方案都只有单个 PKG 为系统中的每个用户生成私钥, 不适用于大规模网络.

为解决上述问题, Horwitz 和 Lynn [3] 于 2002 年首次提出分层标识加密 (HIBE) 的概念. HIBE 允许顶层 PKG 把用户的私钥生成和身份认证工作量分配给低层 PKG, 顶层 PKG 只为其范围内的下一层 PKG 生成私钥即可, 低层 PKG 为其范围内更低层的 PKG 或者用户生成私钥. 文献 [3] 提出了一个两层的 HIBE 方案, 该方案中第一层是完全抗合谋的, 但第二层只满足部分坑合谋. 当属于某个一层 PKG 范围内的第二层用户的数量达到某一门限值时, 这些用户就可以通过合谋获取该 PKG 的私钥. Gentry 和 Silverberg [15] 基于 BF-IBE [2] 提出一个完全抗合谋的 HIBE 方案, 方案满足任意层数抗合谋攻击, 并在随机谕言模型下证明方案具有选择密文的安全性. Boneh 和 Boyen [12] 给出了一个标准模型下可证明安全的 HIBE 方案, 方案的安全性基于 BDH 问题的困难性.

以上所述方案密文的长度、用户的私钥长度、加密开销和解密开销都与系统支持的最大层数线性相关. Boneh 等 [16] 提出了具有短密文的 IND-sID-CPA 安全分层标识加密方案, 密文的长度和解密开销与系统的最大层数无关, 其中密文由 3 个群元素组成, 解密只要求两个双线性对运算. 系统的公钥长度和用户的私钥长度都是线性的, 方案的安全性不依赖于随机谕言器. Waters [17] 通过引入对偶加密技术 (dual system encryption), 基于 2-LIN 困难假设提出具有适应性安全的 HIBE 方案. 文献 [18] 基于合数阶群, 采用对偶加密技术提出了首个在标准模型下具有适应性安全且没有系统最大层数限制的分层标识加密算法. Boyen 和 Waters [19] 提出了首个具有匿名性的 HIBE 方案, 并在标准模型下证明方案具有 IND-sID-CPA 的安全性, 密文长度依赖于系统最大层数. 文献 [20] 基于合数阶双线性阶群提出了具有定长密文的匿名 HIBE 方案, 方案在标准模型下具有 IND-sID-CPA 的安全性. Langrehr 和 Pan [21] 给出了首个在标准模型中具有紧归约的分层标识加密方案. 随后, 在文献 [22] 中基于 k-LIN 假设给出了在多挑战安全模型下具有紧归约的 HIBE 方案. 文献 [23~25] 进一步研究了分层标识加密中的紧归约问题.

SM9 标识密码作为我国商用密码自提出后得到了国内学者积极的研究. 文献 [7] 研究如何快速计算 SM9 中的 R-ate 双线性对, 文献 [8] 给出了优化 R-ate 双线性对计算方法. Wang 等 [10] 提出了加速 SM9 数字签名及验证的方法. 文献 [9] 提出一种基于 SM9 的盲签名方案. Yang 等 [26] 给出了基于 SM9 的区块链隐私保护方案. 文献 [27] 提出基于 SM9 的安全密钥分发方案. 基于 SM9 的广播加密方案在文献 [11] 得到研究. SM9 标识密码只公布了算法的描述, 并未公布算法的安全性分析. Cheng [5] 于 2018 年给出了密钥交换协议、密钥封装机制和加密算法的安全性分析, 但 3 个算法的安全性分析都基于 Gap 类困难问题. 文献 [6] 基于 q-SDH 困难问题首先证明了 SM9 数字签名算法满足 EUF-CMIA (existential unforgeability against chosen-message and identity attacks) 的安全性. 接着,

采用 Twin-Hash-ElGamal 技术提出了具有 IND-CCA 安全的 Twin-SM9 密钥封装机制, 安全性基于 q-BDHI 假设, 消除了文献 [5] 的 Gap 类困难假设. 文献 [28] 基于 SM9 加密算法提出面向调度控制云 (dispatching and control cloud) 的高效属性基加密方案. Ren 等 [29] 基于 SM9 提出具有可追踪和可问责性质的面向云存储的多用户访问控制系统. Zhang 等 [30] 基于 SM9 密码算法提出了一种在随机谕言模型中满足密文不可区分和限门不可区分安全的可搜索加密方案. 文献 [31] 提出一种基于仲裁的 SM9 标识加密算法, 通过可信第三方可快速实现对用户访问权限的撤销和更新操作. 目前尚未在国际主流的密码学期刊和会议上发现基于 SM9 的分层标识加密研究.

3 分层标识加密

分层标识加密通过以下 4 个多项式时间算法描述. 为有效融合 SM9 系列密码算法, 本文给出分层标识加密的密钥封装, 其形式化定义如下:

• $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathbf{Setup}\,(\lambda, n)$. 输入安全参数 λ 和最大层数 n, 由 PKG 执行的系统建立算法 **Setup** 输出系统主公钥 mpk 和主私钥 msk, 其中系统主公钥 mpk 是系统的公开参数, 所有参与者均可获取. msk 由 PKG 秘密保存.

• $d_{\mathrm{ID}|_k} \leftarrow \mathbf{KeyGen}\left(\mathrm{mpk}, d_{\mathrm{ID}|_{k-1}}, \mathrm{ID}\right)$. 输入系统主公钥 mpk, 第 k 层用户的标识 $\mathrm{ID}|_k = (\mathrm{ID}_1, \ldots, \mathrm{ID}_k)$ 和第 $k-1$ 层用户的私钥 $d_{\mathrm{ID}|_{k-1}}$, 由第 $k-1$ 层用户执行的用户私钥生成算法 **KeyGen** 输出第 k 层用户的私钥 $d_{\mathrm{ID}|_k}$, 其中 $1 < k \leqslant n$. $k-1$ 层用户的私钥可由其上一层用户或者根 PKG (顶层 PKG) 生成.

• $(K, \mathrm{CT}) \leftarrow \mathbf{Encrypt}\,(\mathrm{mpk}, \mathrm{ID}|_k)$. 输入系统主公钥 mpk 和接收者标识 $\mathrm{ID}|_k$, 由加密者运行的加密算法 **Encrypt** 输出封装的会话密钥 (又称封装密钥) K 和封装密文 CT. 若需加密的数据为 M, 加密者生成封装密钥 K 后, 选取安全的对称加密系统以 M 和 K 为输入运行对称加密算法生成最终的数据密文 CT_M.

• $K/\perp \leftarrow \mathbf{Decrypt}\left(\mathrm{mpk}, \mathrm{CT}, \mathrm{ID}|_k, d_{\mathrm{ID}|_k}\right)$. 输入系统主公钥 mpk, 封装密文 CT, 解密者标识 $\mathrm{ID}|_k$ 及其私钥 $d_{\mathrm{ID}|_k}$, 由解密者运行的解密算法 **Decrypt** 输出封装密钥 K 或者解密失败符号 $\perp$. 当解密者恢复出正确的封装密钥 K 后, 以 K 和 CT_M 为输入运行对称加密系统的解密算法恢复出数据 M. 本文只给出密钥封装形式, 不再描述数据加密的具体步骤.

分层标识加密方案的正确性要求对任意的 $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathbf{Setup}\,(\lambda, n)$, $d_{\mathrm{ID}|_k} \leftarrow \mathbf{KeyGen}(\mathrm{mpk}, d_{\mathrm{ID}|_{k-1}}, \mathrm{ID}|_k)$ 和 $(K, \mathrm{CT}) \leftarrow \mathbf{Encrypt}\,(\mathrm{mpk}, \mathrm{ID}|_k)$, 有 $\mathbf{Decrypt}\left(\mathrm{mpk}, \mathrm{CT}, \mathrm{ID}|_k, d_{\mathrm{ID}|_k}\right) = K$.

安全模型. 本文给出分层标识加密在静态选择明文攻击下的不可区分 (IND-sID-CPA) 安全模型. 该安全模型通过挑战者和攻击者之间的游戏定义. 不妨设挑战者和攻击者都以最大层数 n 为输入.

• **初始化.** 攻击者输出挑战标识 $\mathrm{ID}^* = (\mathrm{ID}_1^*, \mathrm{ID}_2^*, \ldots, \mathrm{ID}_m^*)$, 其中 $1 < m \leqslant n$.

• **系统建立.** 已知安全参数 λ, 挑战者运行系统建立算法 **Setup**, 生成系统主公私钥对 $(\mathrm{mpk}, \mathrm{msk})$, 并将 mpk 发送给攻击者.

• **询问 1.** 攻击者允许适应性地询问标识 ID_i 的解密私钥, 要求 $\mathrm{ID}_i \neq \mathrm{ID}^*$ 且 ID_i 不是 ID^* 的前缀. 挑战者运行用户私钥生成算法 **KeyGen** 生成私钥 d_{ID_i}, 并将 d_{ID_i} 发送给攻击者.

• **挑战.** 询问 1 结束后, 挑战者运行加密算法 $\mathbf{Encrypt}(\mathrm{mpk}, \mathrm{ID}^*)$ 生成挑战的封装密钥和封装密文 (K^*, CT^*), 并选择随机比特 $b \in \{0, 1\}$. 设 $K_b = K^*$, 从封装密钥空间中随机选择一个会话密钥设为 K_{1-b}. 最后返回 $(\mathrm{CT}^*, K_0, K_1)$ 给攻击者.

• **询问 2.** 攻击者可继续适应性地向挑战者询问标识 ID_i 的私钥, 要求 $\mathrm{ID}_i \neq \mathrm{ID}^*$ 且 ID_i 不是 ID^* 的前缀, 挑战者的回复与询问 1 相同.

• **猜测.** 攻击者输出对 b 的猜测 $b' \in \{0,1\}$. 如果 $b'=b$, 则攻击者获胜.

定义攻击者 $\mathcal{A}$ 获胜的优势为

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sID\text{-}CPA}}(\lambda) = \left|\Pr[b'=b] - \frac{1}{2}\right|.$$

定义1 如果不存在多项式时间攻击者 $\mathcal{A}$ 能以不可忽略的优势 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}sID\text{-}CPA}}(\lambda)$ 赢得 IND-sID-CPA 游戏, 则称方案是 IND-sID-CPA 安全的.

4 SM9 分层标识加密方案

设 λ 为安全参数, p 是与 λ 相关的大素数. $\mathbb{G}_1$, $\mathbb{G}_2$ 和 $\mathbb{G}_T$ 都是通过 λ 生成的循环群, 且阶为 p. 映射 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ 称为双线性映射如果对任意群元素 $P\in\mathbb{G}_1$, $Q\in\mathbb{G}_2$ 和整数 $a,b\in\mathbb{Z}_p$, $e(P,Q)$ 都能高效的计算, 且等式 $e\left(aP,bQ\right)=e\left(P,Q\right)^{ab}$ 成立. 此外, 至少存在群元素 $P\in\mathbb{G}_1$, $Q\in\mathbb{G}_2$, 满足 $e(P,Q)\neq 1$. 记双线性群为 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$. 为便于理解本文, 首先根据文献 [4] 给出 SM9 密钥封装机制的简单描述.

4.1 SM9 密钥封装机制

PKG 首先根据安全参数 λ 生成系统主公钥 $\mathrm{mpk}=(\mathcal{BP},P_1,P_2,P_{\mathrm{pub}}=\alpha P_1,H,\mathrm{KDF},\mathrm{hid},\ell)$ 和主私钥 $\mathrm{msk}=\alpha$, 其中 P_1, P_2 分别为群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的生成元, $H:\mathbb{Z}_p^*\to\mathbb{Z}_p^*$ 为密码函数和 $\mathrm{KDF}:\{0,1\}^*\to\{0,1\}^\ell$ 为密钥派生函数, ℓ 为封装密钥的长度, hid 为私钥生成函数识别符. 给定用户标识 ID, PKG 计算用户的私钥为 $\mathrm{sk}_{\mathrm{ID}}=\frac{\alpha}{H(\mathrm{ID}||\mathrm{hid},p)+\alpha}P_2$. 为生成封装密文 C 和封装密钥 K 给用户 ID, 加密者首先选取随机数 $r\in\mathbb{Z}_p$, 计算 $C=r(H(\mathrm{ID}||\mathrm{hid},p)P_1+P_{\mathrm{pub}})$, $w=e\left(P_{\mathrm{pub}},P_2\right)^r$, $K=\mathrm{KDF}(C||w||\mathrm{ID},\ell)$. 为解密封装密文 C, 解密者 (拥有标识 ID) 首先利用私钥 $\mathrm{sk}_{\mathrm{ID}}$ 计算 $w'=e\left(C,\mathrm{sk}_{\mathrm{ID}}\right)$, 然后计算封装密钥 $K'=\mathrm{KDF}(C||w'||\mathrm{ID},\ell)$.

4.2 SM9 分层标识加密

为描述方便, 本文用 $H(\mathrm{ID})$ 代替 $H(\mathrm{ID}||\mathrm{hid},p)$, SM9 分层标识加密 (SM9-HIBE) 算法描述如下.

• **Setup.** 已知安全参数 λ 和分层加密系统中层数的最大值 n, 即用户标识长度的最大值. 首先利用安全参数 λ 生成非对称双线群 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$, 其中 p 为大素数且 $p>2^\lambda$, 并随机选择生成元 $P\in\mathbb{G}_1$, $Q,Q_1,Q_2,\ldots,Q_n\in\mathbb{G}_2$. 选择随机数 $\alpha\in\mathbb{Z}_p^*$, 密码函数 $H:\mathbb{Z}_p^*\to\mathbb{Z}_p^*$ 和密钥派生函数 $\mathrm{KDF}:\{0,1\}^*\to\{0,1\}^\ell$, 其中 ℓ 为封装密钥的长度 (与 SM9 密钥封装机制描述一致). 计算 $P_{\mathrm{pub}}=\alpha P$, $v=e\left(P_{\mathrm{pub}},Q\right)$. 系统的主公钥 mpk 和主私钥 msk 为

$$\mathrm{mpk}=\left(\mathcal{BP},P,P_{\mathrm{pub}},Q,Q_1,Q_2,\ldots,Q_n,v,H,\mathrm{KDF},n,\ell\right),\ \mathrm{msk}=\alpha.$$

• **KeyGen.** 已知第 k 层用户标识为 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_k)\in\left(\mathbb{Z}_p^*\right)^k$, 其中 $1<k\leqslant n$, 为生成第 k 层用户的私钥 $d_{\mathrm{ID}|_k}$, 选取随机数 $r\in\mathbb{Z}_p^*$ 并计算

$$d_{\mathrm{ID}|_k}=\left(\frac{\alpha}{\alpha+H(\mathrm{ID}_1)}Q+r\cdot\left(Q_1+H(\mathrm{ID}_2)Q_2+\cdots+H(\mathrm{ID}_k)Q_k\right),\ r\cdot\left(\alpha+H(\mathrm{ID}_1)\right)P,\right.$$

$$
\begin{aligned}
& r\cdot Q_{k+1},\ r\cdot Q_{k+2},\ldots,\ r\cdot Q_n\Big)\\
=\ & (d_1,\ d_2,\ u_{k+1},\ u_{k+2},\ \ldots,\ u_n)\,.
\end{aligned}
$$

第 k 层用户的私钥 $d_{\mathrm{ID}|_k}$ 同样可以通过第 $k-1$ 层用户的私钥生成. 假设第 $k-1$ 层用户 $\mathrm{ID}|_{k-1}=(\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_{k-1})\in\left(\mathbb{Z}_p^*\right)^{k-1}$ 的私钥为

$$
\begin{aligned}
d_{\mathrm{ID}|_{k-1}} =\ & \Big(\frac{\alpha}{\alpha+H(\mathrm{ID}_1)}Q+r'\cdot\left(Q_1+H(\mathrm{ID}_2)Q_2+\cdots+H(\mathrm{ID}_{k-1})Q_{k-1}\right),\ r'\cdot(\alpha+H(\mathrm{ID}_1))\,P,\\
& r'\cdot Q_k,\ r'\cdot Q_{k+1},\ldots,\ r'\cdot Q_n\Big)\\
=\ & \left(d_1',\ d_2',\ u_k',\ u_{k+1}',\ \ldots,\ u_n'\right).
\end{aligned}
$$

为生成 $d_{\mathrm{ID}|_k}$, 选择随机数 $t\in\mathbb{Z}_p^*$, 计算

$$
\begin{aligned}
& d_1=(d_1'+H(\mathrm{ID}_k)\cdot u_k'+t\cdot(Q_1+H(\mathrm{ID}_2)Q_2+\cdots+H(\mathrm{ID}_k)Q_k))\,,\\
& d_2=d_2'+t\cdot(P_{\mathrm{pub}}+H(\mathrm{ID}_1)P)\,,\\
& u_{k+1}=u_{k+1}'+t\cdot Q_{k+1},\\
& \quad\vdots\\
& u_n=u_n'+t\cdot Q_n.
\end{aligned}
$$

最后输出第 k 层用户的私钥 $d_{\mathrm{ID}|_k}=(d_1,\ d_2,\ u_{k+1},\ u_{k+2},\ \ldots,\ u_n)$. 容易验证该私钥是第 k 层用户 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_k)$ 的正确私钥, 且生成私钥用的随机数为 $r=r'+t\in\mathbb{Z}_p^*$. 注意到, 层数越大, 用户的私钥长度越短.

• **Encrypt.** 设接收者为第 k 层用户 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_k)$, 加密者选取随机数 $s\in\mathbb{Z}_p^*$, 计算

$$
C_1=s\cdot(P_{\mathrm{pub}}+H(\mathrm{ID}_1)P)\,,\quad C_2=s\cdot(Q_1+H(\mathrm{ID}_2)Q_2+\cdots+H(\mathrm{ID}_k)Q_k)\,,\quad w=v^s.
$$

计算 $K=\mathrm{KDF}\left(C_1||C_2||w||\mathrm{ID}|_k,\ell\right)$, 若 K 为全 0 的比特, 则重新选择随机数. 最后输出 (K,CT), 其中 K 是被封装的密钥, $\mathrm{CT}=(C_1,C_2)$ 是封装密文.

• **Decrypt.** 设待解密的封装密文为 $\mathrm{CT}=(C_1,C_2)$ 且接收者为第 k 层用户, 标识为 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_k)$, 对应的私钥为 $d_{\mathrm{ID}|_k}=(d_1,\ d_2,\ u_{k+1},\ u_{k+2},\ \ldots,\ u_n)$. 解密者计算 $A=e\left(C_1,d_1\right),B=e\left(d_2,C_2\right)$. 接着计算群 $\mathbb{G}_T$ 中的元素 $w'=A/B$, 封装密钥 $K'=\mathrm{KDF}\left(C_1||C_2||w'||\mathrm{ID}|_k,\ell\right)$, 若 K' 为全 0 比特串, 则报错并退出, 否则, 输出密钥 K'.

注意到随着层数的增加, 用户标识 ID 的长度越来越长, 导致 KDF 的输入也越来越长. 为实现 KDF 的固定长度输入, 可设 KDF 输入的 $\mathrm{ID}|_k$ 为其各层标识哈希值的乘积. 即, 若 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_k)$, 则 $\mathrm{KDF}\left(C_1||C_2||w||\mathrm{ID}|_k,\ell\right)$ 可改为 $\mathrm{KDF}(C_1||C_2||w||\prod_{i=1}^k H(\mathrm{ID}_i)\mod p,\ell)$.

4.3 正确性分析

假设 $\mathrm{CT}=(C_1,C_2)$ 为正确的封装密文, 对应接收者的标识为 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\ldots,\mathrm{ID}_k)$ 且其私钥为 $d_{\mathrm{ID}|_k}=(d_1,\ d_2,\ u_{k+1},\ u_{k+2},\ \ldots,\ u_n)$, 则有

$$
w'=\frac{e\left(C_1,d_1\right)}{e\left(d_2,C_2\right)}
$$

$$
\begin{aligned}
&= \frac{e\big(s\cdot(P_{\mathrm{pub}}+H(\mathrm{ID}_1)P)\,,\frac{\alpha}{\alpha+H(\mathrm{ID}_1)}Q+r\cdot(Q_1+H(\mathrm{ID}_2)Q_2+H(\mathrm{ID}_3)Q_3+\cdots+H(\mathrm{ID}_k)Q_k)\big)}{e\left(r\cdot(\alpha+H(\mathrm{ID}_1))\,P,s\cdot(Q_1+H(\mathrm{ID}_2)Q_2+\cdots+H(\mathrm{ID}_k)Q_k)\right)}\\
&= e\left(sP,\alpha Q\right)\\
&= w.
\end{aligned}
$$

因此, 若 $\mathrm{CT}=(C_1,C_2)$ 为正确的封装密文, 则 $w'=w$, $K'=\mathrm{KDF}\left(C_1||C_2||w'||\mathrm{ID}|_k,\ell\right)=\mathrm{KDF}(C_1||C_2||w||\mathrm{ID}|_k,\ell)=K$, 满足分层加密的正确性要求.

4.4 安全性分析

SM9-HIBE 方案的安全性基于判定性 BDHI 问题的困难性, 记为 (q,n)-DBDHI. 我们在随机谕言模型中给出方案的安全性证明. 首先给出非对称群上的 (q,n)-DBDHI 问题的定义.

定义2 ((q,n)-DBDHI 问题) 已知双线性群 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$, 元素 $(c,P_1,bP_1,aP_1,a^2P_1,\ldots,a^{n+1}P_1,P_2,bP_2,aP_2,a^2P_2,\ldots,a^qP_2,\frac{1}{(a+c)^2}P_2,\frac{1}{(a+c)^3}P_2,\ldots,\frac{1}{(a+c)^n}P_2)$ 和元素 $T\in\mathbb{G}_T$, 判断 T 等于 $e(P_1,P_2)^{\frac{b}{a+c}}$ 还是群 $\mathbb{G}_T$ 中的一个随机元素, 其中 a,b,c 都是随机数, 且 a,b 未知.

定理1 令方案中的密码函数 H 为随机谕言器. 如果 (q,n)-DBDHI 问题是难解的, 则本文提出的 SM9-HIBE 方案满足 IND-sID-CPA 的安全性.

证明 假定存在攻击算法 $\mathcal{A}$ 能以不可忽略的优势 (概率) ϵ 攻破方案, 则可构造一个模拟算法 $\mathcal{B}$ 通过与 $\mathcal{A}$ 交互, 以不可忽略的优势求解 (q,n)-DBDHI 问题. 在证明中 $\mathcal{B}$ 扮演 IND-sID-CPA 安全模型中挑战者的角色. $\mathcal{B}$ 输入 (q,n)-DBDHI 问题实例

$$
\left(c,P_1,bP_1,aP_1,a^2P_1,\ldots,a^{n+1}P_1,P_2,bP_2,aP_2,a^2P_2,\ldots,a^qP_2,\frac{1}{(a+c)^2}P_2,\frac{1}{(a+c)^3}P_2,\ldots,\frac{1}{(a+c)^n}P_2,T\right),
$$

目标是判断 T 是否等于 $e(P_1,P_2)^{\frac{b}{a+c}}$. 此外, 假设 $\mathcal{B}$ 和 $\mathcal{A}$ 都以 q 和 n 为输入, 其中 q 表示第一层标识的个数, n 表示系统的最大层数.

初始化. $\mathcal{A}$ 输出挑战用户标识 $\mathrm{ID}^*=(\mathrm{ID}_1^*,\mathrm{ID}_2^*,\ldots,\mathrm{ID}_m^*)$, 其中 $1<m\leqslant n$.

系统建立. $\mathcal{B}$ 首先设 $x^*=c$ (设为 $H(\mathrm{ID}_1^*)$ 的值), 选取两两不同的随机数 $x_2^*,x_3^*,\ldots,x_m^*\in\mathbb{Z}_p^*$ (将设为 $H(\mathrm{ID}_i^*)$ 的值, $i=2,3,\ldots,m$), 随机选取 $w_1,w_2,\ldots,w_q\in\mathbb{Z}_p^*$ (设为第一层除 ID_1^* 外标识的哈希值), 随机选取 $x_1,x_2,\ldots,x_n,y_2,y_3,\ldots,y_n\in\mathbb{Z}_p^*$, 不妨设选取的随机数都两两不同. 接着, 在不知道 a 的情况下隐试设 $\alpha=a$, $\beta=(a+w_1)(a+w_2)\cdots(a+w_q)\mod p$, 并通过已知问题实例计算

$$
P=P_1,\quad P_{\mathrm{pub}}=aP_1,\quad Q=\beta\cdot P_2.
$$

对任意 $i\in[2,n]$, 计算

$$
Q_i=x_iP_2+\frac{y_i}{(a+x^*)^{n+2-i}}P_2.
$$

接着计算

$$
Q_1=x_1(a+x^*)P_2-\sum_{i=2}^{m}x_i^*Q_i=x_1(aP_2+x^*P_2)-\sum_{i=2}^{m}x_i^*Q_i,\quad v=e(P_{\mathrm{pub}},Q).
$$

最后选取恰当的密钥派生函数KDF, 并输出系统主公钥

$$
\mathrm{mpk}=\Big(P,P_{\mathrm{pub}},Q,Q_1,\ldots,Q_n,v,\mathrm{KDF},n,\ell\Big),
$$

其中哈希函数 H 被看成是由 $\mathcal{B}$ 控制的随机谕言器. mpk 中的元素都可通过已知问题实例计算得到.

Hash – 询问. 设询问的标识为 ID_i. $\mathcal{B}$ 首先建立哈希列表 $\mathcal{L}_H$, 表中元素为二元组 (ID_i, h_i), 并设初值为空. 若 ID_i 在列表 $\mathcal{L}_H$ 中, 则 $\mathcal{B}$ 返回相应的 h_i. 否则, 根据以下步骤回复 $\mathcal{A}$.

• ID_i 为第一层标识:

- 若 $\mathrm{ID}_i = \mathrm{ID}_1^*$, 设 $h_i = H(\mathrm{ID}_1^*) = x^* = c$, 将 h_i 发送给 $\mathcal{A}$ 并把新的二元组 (ID_i, h_i) 添加到列表 $\mathcal{L}_H$ 中. 由问题实例中 a, b, c 的随机性可知, 该设置满足哈希函数随机性的要求.

- 若 $\mathrm{ID}_i \neq \mathrm{ID}_1^*$, 设 $h_i = H(\mathrm{ID}_i) = w_i$, 将 h_i 发送给 $\mathcal{A}$ 并把新的二元组 (ID_i, h_i) 添加到列表 $\mathcal{L}_H$ 中.

• ID_i 不是第一层标识:

- 若 $\mathrm{ID}_i = \mathrm{ID}_j^*$, $j \in [2, m]$, 设 $h_i = H(\mathrm{ID}_j^*) = x_j^*$, 将 h_i 发送给 $\mathcal{A}$ 并把新的二元组 (ID_i, h_i) 添加到列表 $\mathcal{L}_H$ 中.

- 若 $\mathrm{ID}_i \neq \mathrm{ID}_j^*$, $j \in [2, m]$, 随机选取 $z_i \in \mathbb{Z}_p^*$, 设 $h_i = H(\mathrm{ID}_i) = z_i$, 将 h_i 发送给 $\mathcal{A}$ 并把新的二元组 (ID_i, h_i) 添加到列表 $\mathcal{L}_H$ 中.

询问 1. 在该阶段, $\mathcal{A}$ 允许适应性地询问标识 $\mathrm{ID} = (\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_j)$ 的私钥, 其中 $j \leqslant n$. 我们要求 ID 不等于 ID^*, 且不是 ID^* 的前缀. $\mathcal{B}$ 根据以下步骤回复.

• 情况 1. $\mathrm{ID}_1 \neq \mathrm{ID}_1^*$. 在该情况中, $H(\mathrm{ID}_1)$ 的值为某个 w_i, 根据参数设置, $\frac{\alpha}{\alpha + H(\mathrm{ID}_1)} Q = \frac{a\beta}{a + w_i} P_2$. 又 $\beta = (a + w_1)(a + w_2) \cdots (a + w_q) \mod p$, 则 $\frac{\alpha}{\alpha + H(\mathrm{ID}_1)} Q$ 的值很容易通过已知困难问题实例计算得到. 最后根据私钥生成算法很容易计算出正确的私钥.

• 情况 2. $\mathrm{ID}_1 = \mathrm{ID}_1^*$. 因为 ID 不等于 ID^*, 且不是 ID^* 的前缀, 则至少存在一个 $k \in [2, j]$ 使得 $\mathrm{ID}_k \neq \mathrm{ID}_k^*$. 不妨设第一个不相等标识的下标为 k, 则有

$$\frac{\alpha}{\alpha + H(\mathrm{ID}_1^*)} Q = \frac{a\beta}{a + x^*} P_2 = f(a) P_2 + \frac{W}{a + x^*} P_2,$$

其中 $f(a)$ 为 q 次多项式, $W \neq 0$ 且可求. 又 $(\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_{k-1}) = \left(\mathrm{ID}_1^*, \mathrm{ID}_2^*, \ldots, \mathrm{ID}_{k-1}^*\right)$, 对 $i \in [2, n]$, $Q_i = x_i P_2 + \frac{y_i}{(a+c)^{n+2-i}} P_2$, 有

$$\begin{aligned}
&Q_1 + H(\mathrm{ID}_2) Q_2 + H(\mathrm{ID}_3) Q_3 + \cdots + H(\mathrm{ID}_j) Q_j \\
&= x_1 (a P_2 + x^* P_2) - \sum_{i=2}^{m} x_i^* Q_i + z_2 Q_2 + z_3 Q_3 + \cdots + z_j Q_j \\
&= x_1 (a P_2 + x^* P_2) - \sum_{i=2}^{m} x_i^* Q_i + x_2^* Q_2 + x_3^* Q_3 + \cdots + x_{k-1}^* Q_{k-1} + z_k Q_k + \cdots + z_j Q_j \\
&= x_1 (a P_2 + x^* P_2) - \sum_{i=k}^{m} x_i^* Q_i + z_k Q_k + \cdots + z_j Q_j \\
&= x_1 (a + x^*) P_2 + X P_2 + \frac{Y_k}{(a+c)^{2+n-k}} P_2 + \cdots + \frac{Y_{\max(m,j)}}{(a+c)^{2+n-\max(m,j)}} P_2.
\end{aligned}$$

该值可通过问题实例计算, 其中 X 为可求系数, $Y_i, i = k, k+1, \ldots, \max(m, j)$ 为非 0 的可求系数. 接着, $\mathcal{B}$ 选取随机数 $Z \in \mathbb{Z}_p^*$, 设 $r = Z - \frac{W}{Y_k} (a + x^*)^{(2+n-k)-1}$, 计算

$$\begin{aligned}
d_1 =& \frac{\alpha}{\alpha + H(\mathrm{ID}_1^*)} Q + r \cdot (Q_1 + H(\mathrm{ID}_2) Q_2 + H(\mathrm{ID}_3) Q_3 + \cdots + H(\mathrm{ID}_j) Q_j) \\
=& f(a) P_2 + \frac{W}{a + x^*} P_2 + \left(Z - \frac{W}{Y_k} (a + x^*)^{(2+n-k)-1} \right)
\end{aligned}$$

$$\cdot\left(x_1(a+x^*)P_2+XP_2+\frac{Y_k}{(a+c)^{2+n-k}}P_2+\cdots+\frac{Y_{\max(m,j)}}{(a+c)^{2+n-\max(m,j)}}P_2\right)$$
$$=f(a)P_2+Z\cdot\left(x_1(a+x^*)P_2+XP_2+\frac{Y_k}{(a+c)^{2+n-k}}P_2+\cdots+\frac{Y_{\max(m,j)}}{(a+c)^{2+n-\max(m,j)}}P_2\right)$$
$$-\frac{x_1W}{Y_k}(a+x^*)^{(2+n-k)}P_2-\frac{XW}{Y_k}(a+x^*)^{(2+n-k)-1}P_2-\frac{Y_{k+1}W}{Y_k}P_2-\frac{Y_{k+2}W}{Y_k}(a+x^*)P_2$$
$$-\cdots-\frac{Y_{\max(m,j)}W}{Y_k}(a+x^*)^{(\max(m,j)-k-1)}P_2,$$
$$d_2=r\cdot(\alpha+H(\mathrm{ID}_1^*))\,P$$
$$=\left(Z-\frac{W}{Y_k}(a+x^*)^{(2+n-k)-1}\right)\cdot(a+x^*)\,P_1$$
$$=Z\cdot(a+x^*)\,P_1-\frac{W}{Y_k}(a+x^*)^{(2+n-k)}P_1.$$

对任意 $i\in[j+1,n]$, 计算

$$u_i=r\cdot Q_i$$
$$=\left(Z-\frac{W}{Y_k}(a+x^*)^{(2+n-k)-1}\right)\cdot\left(x_iP_2+\frac{y_i}{(a+x^*)^{n+2-i}}P_2\right)$$
$$=Z\cdot\left(x_iP_2+\frac{y_i}{(a+x^*)^{n+2-i}}P_2\right)-\frac{x_iW}{Y_k}(a+x^*)^{(2+n-k)-1}P_2-\frac{y_iW}{Y_k}(a+x^*)^{i-k-1}P_2.$$

最后, $\mathcal{B}$ 发送私钥 $d_{\mathrm{ID}}=(d_1,\ d_2,\ u_{j+1},\ u_{j+2},\ \ldots,\ u_n)$ 给 $\mathcal{A}$. 从上面的设置可知, d_{ID} 为正确的私钥, d_{ID} 中的元素可以通过给定的困难问题计算得到.

挑战. 询问 1 结束后, $\mathcal{B}$ 计算 $C_1^*=bP_1$, $C_2^*=x_1bP_2$, $w^*=e\,(bP_1,f(a)P_2)\cdot T^W$, $K^*=\mathrm{KDF}(C_1^*||C_2^*||w^*||\mathrm{ID}^*,\ell)$. 随机选择比特 $\mu\in\{0,1\}$, 设 $K_\mu=K^*$. 接着, 从密钥空间中选取一个随机值设为 $K_{1-\mu}$, 并发送挑战密文 (C_1^*,C_2^*,K_0,K_1) 给 $\mathcal{A}$. 下面分析挑战密文的正确性.

设生成挑战密文的随机数为 $s^*=\frac{b}{a+x^*}$, 则有

$$C_1^*=s^*\cdot(P_{\mathrm{pub}}+H(\mathrm{ID}_1^*)P)$$
$$=\frac{b}{a+x^*}\cdot(a+x^*)P_1$$
$$=bP_1,$$
$$C_2^*=s^*\cdot(Q_1+H(\mathrm{ID}_2^*)Q_2+\cdots+H(\mathrm{ID}_m^*)Q_m)$$
$$=\frac{b}{a+x^*}\cdot\left(x_1(aP_2+x^*P_2)-\sum_{i=2}^{m}x_i^*Q_i+x_2^*Q_2+\cdots+x_m^*Q_m\right)$$
$$=x_1bP_2.$$

若 $T=e(P_1,P_2)^{\frac{b}{a+c}}=e(P_1,P_2)^{\frac{b}{a+x^*}}$, 则有

$$w^*=e\,(bP_1,f(a)P_2)\cdot T^W$$
$$=e\,(bP_1,f(a)P_2)\cdot\left(e(P_1,P_2)^{\frac{b}{a+x^*}}\right)^W$$
$$=\left(e(P_1,P_2)^{f(a)+\frac{W}{a+x^*}}\right)^b$$

$$
\begin{aligned}
&= \left(e(P_1,P_2)^{\frac{a\beta}{a+x^*}}\right)^b \\
&= e(aP_1,\beta P_2)^{\frac{b}{a+x^*}} \\
&= e(P_{\text{pub}},Q)^{s^*}.
\end{aligned}
$$

因此, 当 $T=e(P_1,P_2)^{\frac{b}{a+c}}$ 时, (C_1^*,C_2^*) 是正确的挑战密文.

询问 2. $\mathcal{A}$ 允许继续适应性地询问私钥, $\mathcal{B}$ 的回复与询问 1 相同.

猜测. 最后, $\mathcal{A}$ 输出对 μ 的猜测 $\mu'\in\{0,1\}$. 若 $\mu=\mu'$, $\mathcal{B}$ 输出 "1", $\mathcal{B}$ 认为困难问题实例中 $T=e(P_1,P_2)^{\frac{b}{a+c}}$. 否则输出 "0", 认为困难问题实例中 T 是群 $\mathbb{G}_T$ 中不等于 $e(P_1,P_2)^{\frac{b}{a+c}}$ 的随机元素.

以上完成了模拟步骤. 从证明的设置可知, 模拟和真实攻击环境同分布, 是不可区分的, 且模拟过程没有终止事件发生. 接下来, 分析 $\mathcal{B}$ 解决困难问题的优势. 若 $T=e(P_1,P_2)^{\frac{b}{a+c}}$, 模拟和真实攻击环境不可区分. 根据假设 $\mathcal{A}$ 有不可忽略的优势 ϵ 攻破方案, 则有

$$
\Pr\left[\mu=\mu'|T=e(P_1,P_2)^{\frac{b}{a+c}}\right]=\epsilon+\frac{1}{2}.
$$

若 T 是群 $\mathbb{G}_T$ 中不等于 $e(P_1,P_2)^{\frac{b}{a+c}}$ 的随机元素, 我们有 $e\left(bP_1,f(a)P_2\right)\cdot T^W$ 是随机的, 即 w^* 随机. 对 $\mathcal{A}$ 而言, w^* 与 C_1^*,C_2^* 独立无关, 则有

$$
\Pr\left[\mu=\mu'|T\neq e(P_1,P_2)^{\frac{b}{a+c}}\right]=\frac{1}{2}.
$$

综上, $\mathcal{B}$ 正确解决 (q,n)-DBDHI 问题的概率为

$$
\begin{aligned}
\mathsf{Adv}^{(\mathsf{q},\mathsf{n})-\mathsf{DBDHI}}(\lambda) &= \left|\Pr\left[\mu=\mu'|T=e(P_1,P_2)^{\frac{b}{a+c}}\right]-\Pr\left[\mu=\mu'|T\neq e(P_1,P_2)^{\frac{b}{a+c}}\right]\right| \\
&= \left|\epsilon+\frac{1}{2}-\frac{1}{2}\right| \\
&= \epsilon.
\end{aligned}
$$

注意到本文方案具有 CPA 的安全性且方案的安全性分析依赖于随机谕言器, 因此, 我们可以采用 FO 转换技术 [32] 实现 CCA 的安全性.

4.5 方案性能分析

本小节将分析 SM9-HIBE 方案的计算效率和存储效率, 并与现有基于素数阶群设计的分层标识加密方案进行比较. 首先比较用户私钥生成算法、加密算法和解密算法的计算开销, 结果如表 1 所示. 接着比较方案的存储开销和安全性, 结果如表 2 所示. 在比较中作如下假设: 系统最大层数为 n, 私钥生成算法为根 PKG 生成第 k 层用户的私钥, 第 $k-1$ 层用户为第 k 层用户生成私钥记为 $(k-1\to k)$, 加密数据接收者为第 k 层用户. 在比较中只考虑密钥封装形式, 即不考虑封装密钥加密数据的开销. 符号说明: $\mathcal{P}$ 表示双线性运算, SM_i $(i=1,2)$ 表示非对称群 $\mathbb{G}_i$ 中的标量乘运算 (等价乘法群中的指数运算), SM 表示对称群 $\mathbb{G}$ 中的标量乘运算, E_t 表示群 $\mathbb{G}_T$ 中的指数运算, $|\mathbb{G}_i|$ $(i=1,2)$ 表示非对称群 $\mathbb{G}_i$ 中元素的大小, $|\mathbb{G}|$ 表示对称群 $\mathbb{G}$ 中元素的大小.

从表 1 可知, 本文方案 SM9-HIBE 的加密效率与现有素数阶标识加密方案是可比的, 都与接收者标识长度线性增长, 但解密开销与文献 [16] 都是固定的, 只包含两个双线性对运算, 其他比较方案中的解密要求线性个双线性对运算. 从表 2 可知, 虽然文献 [15] 的公钥长度只包含两个群元素, 但其具有线性长的密文. SM9-HIBE 与文献 [16] 具有定长的密文, 密文由两个群元素组成, 与接收者标识长

表 1　计算开销比较

Table 1　Comparison of computational overhead

Schemes	Key generation	Key generation($k-1 \to k$)	Encryption	Decryption
[15]	–	2SM	$\mathcal{P}+k\mathrm{SM}+E_t$	$k\mathcal{P}$
[12]	$(3k+1)$SM	3SM	$(2k+1)\mathrm{SM}+E_t$	$(k+1)\mathcal{P}$
[16]	$(n+2)$SM	$(n+2)$SM	$(k+1)\mathrm{SM}+E_t$	$2\mathcal{P}$
[17]	$(4k+11)$SM	$(4k+9)$SM	$(3k+11)\mathrm{SM}+E_t$	$(2k+7)\mathcal{P}+kE_t$
SM9-HIBE	$2\mathrm{SM}_1+(n+1)\mathrm{SM}_2$	$2\mathrm{SM}_1+(n+1)\mathrm{SM}_2$	$2\mathrm{SM}_1+k\mathrm{SM}_2+E_t$	$2\mathcal{P}$

表 2　存储开销和安全性比较

Table 2　Comparison of storage overhead and security

Schemes	Public key size	Private key size	Ciphertext overhead	Assumption	Security
[15]	$2\lvert\mathbb{G}\rvert$	$k\lvert\mathbb{G}\rvert$	$k\lvert\mathbb{G}\rvert$	BDH	CPA
[12]	$(n+3)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$(k+1)\lvert\mathbb{G}\rvert$	$(k+1)\lvert\mathbb{G}\rvert$	DBDH	sCPA
[16]	$(n+4)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$(n-k+2)\lvert\mathbb{G}\rvert$	$2\lvert\mathbb{G}\rvert$	DBDHE	sCPA
[17]	$(2n+13)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$(2k+7)\lvert\mathbb{G}\rvert+k\lvert\mathbb{Z}_p\rvert$	$(k+8)\lvert\mathbb{G}\rvert+k\lvert\mathbb{Z}_p\rvert$	2-LIN	CPA
SM9-HIBE	$\lvert\mathbb{G}_T\rvert+(n+1)\lvert\mathbb{G}_2\rvert+2\lvert\mathbb{G}_1\rvert$	$(n-k+1)\lvert\mathbb{G}_2\rvert+\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	DBDHI	sCPA

度无关. 此外, 当接收者标识的层数越大时, 本文方案和文献 [16] 中的私钥长度越短, 而其他比较方案的私钥长度随着用户标识长度的增加而增加.

5　结论

基于我国商用密码 SM9 标识密码无法高效处理大规模网络应用中用户私钥的生成和分发问题, 本文提出了一种高效的 SM9 分层标识加密方案的设计 SM9-HIBE. 用户的私钥生成和分发可实现分布式处理, 极大减轻密钥生成中心的工作负担. 方案中用户的私钥长度随着层数的增加而减少, 密文长度由两个群元素组成, 解密只包含两个配对运算. 在随机谕言模型中证明若判定性 BDHI 问题是难解的, 则 SM9-HIBE 具有 CPA 的安全性. 最后, 与现有方案比较, 结果表明 SM9-HIBE 方案在计算效率和通信效率方面与现有基于素数阶群的高效分层标识加密方案是可比的.

参考文献

1 Shamir A. Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO 84 on Advances in Cryptology, Santa Barbara, 1984. 47–53

2 Boneh D, Franklin M K. Identity-based encryption from the weil pairing. In: Proceedings of the 21st Annual International Cryptology Conference, Santa Barbara, 2001. 213–229

3 Horwitz J, Lynn B. Toward hierarchical identity-based encryption. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, 2002. 466–481

4 GM/T0044-2016. Identity-based cryptographic algorithm SM9. 2016 [GM/T0044-2016. SM9标识密码算法. 2016]

5 Cheng Z H. Security analysis of SM9 key agreement and encryption. In: Proceedings of the 14th International Conference on Information Security and Cryptology, Fuzhou, 2018. 3–25

6 Lai J C, Huang X Y, He D B, et al. Security analysis of SM9 digital signature and key encapsulation. Sci Sin Inform, 2021, 51: 1900–1913 [赖建昌, 黄欣沂, 何德彪, 等. 国密SM9数字签名和密钥封装算法的安全性分析. 中国科学: 信息科学, 2021, 51: 1900–1913]

7 Gan Z W, Liao F Y. Rapid calculation of R-ate bilinear pairing in China state cryptography standard SM9. Comput Eng, 2019, 45: 171–174 [甘植旺, 廖方圆. 国密SM9中R-ate 双线性对快速计算. 计算机工程, 2019, 45: 171–174]

8 Wang M D, He W G, Li J, et al. Optimal design of R-ate pair in SM9 algorithm. Commun Technol, 2020, 53: 2241–2244 [王明东, 何卫国, 李军, 等. 国密 SM9 算法R-ate 对计算的优化设计. 通信技术, 2020, 53: 2241–2244]

9 Zhang X F, Peng H. Blind signature scheme based on SM9 algorithm. Netinfo Secur, 2019, 19: 61–67 [张雪锋, 彭华. 一种基于SM9算法的盲签名方案研究. 信息网络安全, 2019, 19: 61–67]

10 Wang S, Fang L G, Han L B, et al. Fast implementation of SM9 digital signature and verification algorithms. Commun Technol, 2019, 52: 2524–2527 [王松, 房利国, 韩炼冰, 等. 一种SM9数字签名及验证算法的快速实现方法. 通信技术, 2019, 52: 2524–2527]

11 Lai J C, Huang X Y, He D B. An efficient identity-based broadcast encryption scheme based on SM9. Chinese J Comput, 2021, 44: 897–907 [赖建昌, 黄欣沂, 何德彪. 一种基于SM9的高效标识广播加密方案. 计算机学报, 2021, 44: 897–907]

12 Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, 2004. 223–238

13 Waters B. Efficient identity-based encryption without random oracles. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 114–127

14 Gentry C. Practical identity-based encryption without random oracles. In: Proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, 2006. 445–464

15 Gentry G, Silverberg A. Hierarchical ID-based cryptography. In: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, 2002. 548–566

16 Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 440–456

17 Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Proceedings of the 29th Annual International Cryptology Conference, Santa Barbara, 2009. 619–636

18 Lewko A B, Waters B. Unbounded HIBE and attribute-based encryption. In: Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, 2011. 547–567

19 Boyen X, Waters B. Anonymous hierarchical identity-based encryption (without random oracles). In: Proceedings of the 26th Annual International Cryptology Conference, Santa Barbara, 2006. 290–307

20 Seo J H, Kobayashi T, Ohkubo M, et al. Anonymous hierarchical identity-based encryption with constant size ciphertexts. In: Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, 2009. 215–234

21 Langrehr R, Pan J X. Tightly secure hierarchical identity-based encryption. In: Proceedings of the 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, 2019. 436–465

22 Langrehr R, Pan J X. Hierarchical identity-based encryption with tight multi-challenge security. In: Proceedings of the 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, 2020. 153–183

23 Blazy O, Kiltz E, Pan J X. (Hierarchical) identity-based encryption from affine message authentication. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 408–425

24 Gong J, Cao Z, Tang S, et al. Extended dual system group and shorter unbounded hierarchical identity based encryption. Des Codes Cryptogr, 2016, 80: 525–559

25 Langrehr R, Pan J. Tightly secure hierarchical identity-based encryption. J Cryptol, 2020, 33: 1787–1821

26 Yang Y T, Cai J L, Zhang X W, et al. Privacy preserving scheme in blockchain with provably secure based on SM9 algorithm. Ruan Jian Xue Bao/J Softw, 2019, 30: 1692–1704 [杨亚涛, 蔡居良, 张筱薇, 等. 基于SM9算法可证明安全的区块链隐私保护方案. 软件学报, 2019, 30: 1692–1704]

27 Xu S W, Ren X P, Yuan F, et al. A secure key issuing scheme of SM9. Comput Appl Softw, 2020, 37: 314–319 [许盛伟, 任雄鹏, 袁峰, 等. 一种关于SM9的安全私钥分发方案. 计算机应用与软件, 2020, 37: 314–319]

28 Ji H, Zhang H, Shao L, et al. An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud. Connection Sci, 2021, 33: 1094–1115

29 Ren K, Jiang P, Gai K K, et al. SM9-based traceable and accountable access control for secure multi-user cloud storage. In: Proceedings of the 6th IEEE International Conference on Smart Cloud, Newark, 2021. 13–18

30 Zhang C, Peng C G, Ding H F, et al. SM9-based searchable encryption scheme. Comput Eng, 2022, 7: 159–167 [张超, 彭长根, 丁红发, 等. 基于国密 SM9 的可搜索加密方案. 计算机工程, 2022, 7: 159–167]
31 Qin B D, Zhang B X, Bai X. Mediated SM9 identity-based encryption algorithm. Chinese J Comput, 2022, 45: 412–426 [秦宝东, 张博鑫, 白雪. 基于仲裁的 SM9 标识加密算法. 计算机学报, 2022, 45: 412–426]
32 Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes. In: Proceedings of the 19th Annual International Cryptology Conference, Santa Barbara, 1999. 537–554

An efficient hierarchical identity-based encryption based on SM9

Jianchang LAI[1], Xinyi HUANG[2*], Debiao HE[3] & Fuchun GUO[4]

1. *School of Cyber Science and Engineering, Southeast University, Nanjing* 211189*, China*;
2. *Fujian Provincial Key Lab of Network Security and Cryptology, College of Computer and Cyber Security, Fujian Normal University, Fuzhou* 350117*, China*;
3. *Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072*, China*;
4. *School of Computing and Information Technology, University of Wollongong, Wollongong* 2522*, Australia*
* Corresponding author. E-mail: xyhuang81@gmail.com

Abstract Hierarchical identity-based encryption can efficiently reduce the workload of private key generation and key distribution of the private key generator in the identity-based cryptography. SM9 is an identity-based cryptosystem and has become a Chinese cryptographic standard and national standard. It plays a significant role in many applications, such as finance and government affairs. However, SM9 encryption algorithm does not support hierarchical encryption, which is undesirable for the large network and becomes a bottleneck for its deployments. In this paper, we proposed an efficient hierarchical identity-based encryption scheme SM9-HIBE based on SM9. Compared to SM9 encryption algorithm, the ciphertext in SM9-HIBE only requires an additional group element and the decryption overhead increases one pairing operation only, which is independent of the length of receiver's identity. We prove that if the DBDHI assumption holds, our scheme is proved to be IND-sCPA secure in the random oracle model. Finally, we theoretically analyze our scheme and make a comparison. The result shows that the SM9-HIBE is comparable to the existing HIBE schemes in terms of computational cost and communication overhead.

Keywords hierarchical encryption, identity-based cryptography, SM9, key encapsulation, chosen-plaintext attack (CPA)