中国科学: 信息科学 2024 年 第 54 卷 第 6 期: 1400–1418
SCIENTIA SINICA Informationis
论文

基于 SM9 的分层标识广播内积函数加密

李聪[1,3,4], 梁俊凯[1,3,4], 丁煜甲[2,4], 沈晴霓[2,3,4*], 吴中海[2,3,4*]

1. 北京大学计算机学院, 北京 100871
2. 北京大学软件与微电子学院, 北京 102600
3. 软件工程国家工程研究中心 (北京大学), 北京 100871
4. 北京大学 – 八分量区块链与隐私计算联合实验室 (北京大学), 北京 100871
* 通信作者. E-mail: qingnishen@ss.pku.edu.cn, wuzh@pku.edu.cn

收稿日期: 2023–07–31; 修回日期: 2023–10–14; 接受日期: 2023–12–13; 网络出版日期: 2024–06–13

国家重点研发计划 (批准号: 2022YFB2703301) 和国家自然科学基金 (批准号: 61672062, 61232005) 资助项目

摘要 内积函数加密支持当使用一个与向量 $\boldsymbol{y}$ 相关的私钥解密一份与向量 $\boldsymbol{x}$ 相关的密文时, 解密者仅能获得内积值 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ 而无法获取任何其他信息. 分层广播内积函数加密, 则进一步具有密文向指定用户广播与密钥授权的性质. SM9 标识加密是我国自主设计的一个商用密码标准, 已被应用于物联网、医疗协同服务与电子政务等领域, 但 SM9 标识加密算法及现有扩展算法均无法同时实现内积函数的功能与密文广播、密钥授权的性质, 限制了 SM9 标识加密算法的适用场景. 本文基于 SM9 标识加密算法设计了一个分层标识广播内积函数加密方案 HIBB-IPFE-SM9. 方案构造借鉴了 Abdalla 等的内积函数加密 (PKC'15) 与 Liu 等的分层广播加密 (ACISP'14) 的设计思想, 解密算法仅包含两个双线性配对运算. 本文还在随机谕言机模型中证明了方案满足选择明文安全性. 最后, 对提出方案与现有相关方案进行了对比分析, 结果显示 HIBB-IPFE-SM9 方案在计算和通信开销上与相关方案是可比的.

关键词 内积函数加密, 分层广播加密, 标识密码, SM9, 选择明文安全

1 引言

在传统的公钥加密方案中, 接收方要么能够恢复整个明文消息 m, 要么无法获得任何有效的信息, 缺乏在解密时, 对于暴露给接收方信息量的控制机制. 为了解决该问题, Abdalla 等 [1] 在 2015 年 PKC (Public-Key Cryptography) 会议中引入了公钥内积函数加密 (public-key inner product functional encryption, PK-IPFE) 这一概念. PK-IPFE 是一种特殊的函数加密, 接收方使用与向量 $\boldsymbol{y}$ 相关的私钥解密加密了向量 $\boldsymbol{x}$ 的密文时, 其仅能恢复内积值 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$, 而无法获得向量 $\boldsymbol{x}$ 的值. 由于具有上述特点, PK-IPFE

引用格式: 李聪, 梁俊凯, 丁煜甲, 等. 基于 SM9 的分层标识广播内积函数加密. 中国科学: 信息科学, 2024, 54: 1400–1418, doi: 10.1360/SSI-2023-0232
Li C, Liang J K, Ding Y J, et al. Hierarchical identity-based broadcast inner product functional encryption based on SM9 (in Chinese). Sci Sin Inform, 2024, 54: 1400–1418, doi: 10.1360/SSI-2023-0232

有着许多实际的应用场景, 包括隐私保护描述性统计分析、隐私保护机器学习等. 例如, 在一家银行中, 所有储蓄用户的资金信息均以向量 $\boldsymbol{x}$ 的形式记录, 并使用信息部门 A 的公钥 PK 加密后存储. 其中, 资金信息包括资金总额、理财产品金额、存款金额与贷款金额. 该银行的信用卡部门 B, 为了处理用户 U 的信用卡申请, 需要对其信用情况进行评估. 用户 U 的资金情况为 $\boldsymbol{x} = (10000, 4000, 6000, 3000)$. 此时, 部门 B 向部门 A 申请用户 U 密文形式的资金数据, 并提交向量 $\boldsymbol{y} = (1, 1, 0.5, -5)$ 形式的评级权重信息 (即资金总额的权重为 1, 理财产品金额的权重为 1, 存款金额的权重为 0.5, 贷款金额的权重为 -5). 经审批并通过后, 部门 A 首先为部门 B 生成一个与向量 $\boldsymbol{y}$ 相关的私钥 $\mathrm{SK}_{\boldsymbol{y}}$. 接着, 将密文 $\mathrm{CT}_{\boldsymbol{x}}$ 与私钥 $\mathrm{SK}_{\boldsymbol{y}}$ 发送给部门 B. 至此, 部门 B 可运行解密算法, 计算得到内积值 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 10000 \times 1 + 4000 \times 1 + 6000 \times 0.5 + 3000 \times (-5) = 2000$. 此时, 部门 B 获得了用户 U 的信用评估值 2000, 但无法得到关于向量 $\boldsymbol{x}$ (即用户 U 的资金信息) 的任何一点信息.

考虑到公钥密码体系中的公钥往往是一个 “无意义” 的随机串, 需要借助于证书完成认证, 但证书的管理是一项繁琐的工作, 1984 年, Shamir [2] 首次提出了标识加密的概念, 它采用了标识作为用户公钥, 故能够很好地解决证书管理问题. 2001 年, Boneh 与 Franklin [3] 定义了标识加密的安全模型, 并基于双线性配对设计了首个可证明安全的标识加密方案. 之后, 关于标识加密方案的研究受到了学术界的广泛关注, 一系列工作 [4~11] 从安全性与性能等方面对标识加密进行了提升. Lai 等 [12] 首次将标识加密体系扩展到了内积函数加密领域, 提出了标识广播内积函数加密的概念, 并设计了一个具有固定密文长度性质的方案. 随后, 文献 [13,14] 对标识内积函数加密进行了进一步的探索.

为了保障国家的网络与信息安全, 实现密码算法的自主可控, 我国设计了一个商用标识密码算法标准 SM9 [15], 并于 2016 年正式发布成为行业标准, 2020 年确立为国家标准, 2021 年被纳入 ISO/IEC 国际标准. 近年来, 国内的学者们基于 SM9 标识加密算法设计了一系列扩展方案, 它们能够支持同态加密 [16]、仲裁 [17]、密文检索 [18]、密文广播 [19~21] 以及机构分层 [22] 等功能. 然而, 现有的标识内积函数加密方案均基于国外提出的算法设计, 尚未见国际, 国内主流期刊和会议上发表基于 SM9 的内积函数加密的相关设计方案.

因此, 本文基于 SM9 标识加密算法的特点, 结合 Abdalla 等 [1] 的内积函数加密方案和 Liu 等 [23] 的分层标识广播加密方案的设计思路, 将向量 $\boldsymbol{y}$ 有机地与私钥结构中的主密钥部分进行绑定, 同时将向量 $\boldsymbol{x}$ 嵌入至密文结构中, 提出了一个基于 SM9 的分层标识广播内积函数加密方案 HIBB-IPFE-SM9 (hierarchical identity-based broadcast inner product functional encryption based on SM9). 该方案能够同时支持内积运算、密文广播与密钥授权功能. 其密文仅占用 $(n+2)$ 个群元素长度, 与方案 [23] 相当, 解密算法也仅包含两次双线性配对运算. 本文还定义了分层标识广播内积函数加密的安全模型, 并基于 DBDHI (decisional bilinear Diffie-Hellman inversion) 困难性假设在随机谕言机模型下, 证明了 HIBB-IPFE-SM9 方案满足选择标识集合及向量和选择明文攻击模型中的不可区分性 (indistinguishability against selective identity set and vector, and chosen plaintext attacks, IND-sIDSV-CPA). 最后, 本文从理论和实验两方面将 HIBB-IPFE-SM9 方案与现有主要标识内积函数加密方案进行了对比. 结果表明 HIBB-IPFE-SM9 方案无论在计算开销还是通信开销上, 均与现有相关方案是可比的.

本文余下部分的内容为, 第 2 节介绍了分层标识加密、标识广播加密、标识内积函数加密以及基于 SM9 的标识加密的研究进展. 第 3 节对本文使用的符号、数学基础、困难性假设、分层标识广播内积函数加密的系统模型和安全模型、SM9 标识加密方案进行了简介. 第 4 节重点阐述了 HIBB-IPFE-SM9 的方案构造、正确性分析与安全性证明. 第 5 节将 HIBB-IPFE-SM9 方案与相关方案的性能表现进行了对比与分析. 第 6 节则概要性地对全文进行了总结, 并对未来工作进行了展望.

2 相关工作

分层标识加密. 考虑到标识加密系统往往仅支持单一密钥生成中心 (private key generator, PKG), 无法处理大规模用户的场景, Horwitz 与 Lynn[24] 首次引入了分层标识加密 (hierarchical identity-based encryption, HIBE) 的概念并提出了一个两层 HIBE 方案. Gentry 与 Silverberg[25] 提出了首个具有完全功能性的 HIBE 方案, 并在随机谕言机模型下证明了其具有选择密文 (chosen ciphertext attack, CCA) 安全性. Boneh 与 Boyen[5] 设计了首个标准模型下的 HIBE 方案, 该方案具有选择标识 (selective-ID) 安全性. Boneh 等[26] 进一步提出了一个具有固定密文长度的 HIBE 方案, 该方案同样具有选择标识安全性. Gentry 与 Halevi[27] 提出了首个具有自适应标识 (full/adaptive-ID) 安全性的 HIBE 方案. 该方案还解决了过去方案中的系统最大深度为某一固定值的不足, 能够支持多项式级的最大深度. Waters[9] 引入了 "双系统" 加密这一新工具, 以构造具有自适应标识安全性的 HIBE 方案. 随后, 基于该工具, 文献 [28, 29] 相继提出了两个新的具有自适应标识安全性的 HIBE 方案, 它们分别具有短密文长度与不限制系统最大深度的特点. Boyen 与 Waters[30] 提出了首个匿名化 HIBE 方案. 该方案的密文不会泄露接收方的标识信息. Seo 等[31] 则设计了一个新的匿名化 HIBE 方案, 其具有固定密文长度的性质. Langrehr 与 Pan[32] 构造了首个满足紧安全的 HIBE 方案. 该方案的安全性基于标准困难性假设 (standard assumption), 且安全规约中的损失不再是用户私钥查询次数的倍数, 而仅与安全参数 λ 相关. 文献 [33] 进一步提出了一个满足紧安全且不限制系统最大深度的 HIBE 方案.

标识广播加密. 标识广播加密 (identity-based broadcast encryption, IBBE) 的概念分别由 Delerablée[34] 与 Sakai 和 Furukawa[35] 在同一时期独立提出. 文献 [34] 提出了一个具有固定密文与密钥长度的 IBBE 方案, 并在随机谕言机模型下证明了其具有选择标识集合与选择明文攻击模型中的不可区分性 (indistinguishability against selective identity set and chosen plaintext attacks, IND-sIDS-CPA). 考虑到方案[34] 仅满足选择安全性, Gentry 和 Waters[36] 提出了首个自适应安全的 IBBE 方案. 他们首先构造了一个半静态 (semi-static) 安全的 IBBE 方案, 接着设计了一个将半静态安全的 IBBE 转换为自适应安全的 IBBE 的通用方法, 从而完成了自适应安全 IBBE 的构建. Ren 和 Gu[37] 提出了一个同时具有 CCA 安全性与自适应安全性的 IBBE 方案, 该方案具有固定的公共参数与密文长度. Kim 等[38] 提出了一个新的具有选择安全性的 IBBE 方案. 相较于文献 [36] 中提出的同类方案, 它移除了 "标签" 并简化了安全性证明, 具有更好的性能表现. Kim 等[39] 基于合数阶双线性群提出了一个标准模型下自适应安全的 IBBE 方案. 该方案基于 "双系统" 加密技术设计, 具有固定密文长度的性质. 文献 [23, 40] 分别提出了一个 CCA 安全的分层标识广播加密 (hierarchical identity-based broadcast encryption, HIBBE) 方案与一个自适应安全的 HIBBE 方案, 它们同时支持密钥授权与密文广播功能. 此后, 一系列工作在功能性上对 IBBE 进行了增强, 包括用户吊销[41, 42]、匿名性[43, 44] 以及部分外包解密[45] 等.

标识内积函数加密. Abdalla 等[1] 首次引入了公钥内积函数加密 (PK-IPFE) 这一概念. 在 PK-IPFE 中, 当使用一个与向量 $\boldsymbol{y}$ 相关的私钥解密一份加密了向量 $\boldsymbol{x}$ 的密文时, 接收方仅能获得 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ 这一内积值, 而无法获取其他有效的信息. 他们还给出了一个 PK-IPFE 具体构造与一个构建 PK-IPFE 的通用方法. Lai 等[12] 首次将 PK-IPFE 与 IBBE 结合, 提出了一个新的概念, 即标识广播内积函数加密 (IBB-IPFE). 在 IBB-IPFE 中, 当且仅当接收方的标识 ID 属于密文中的标识集合 S 时, 接收方才能顺利地获得内积值 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$. 他们还提出了一个 IBB-IPFE 具体构造, 具有固定密文长度的性质, 并能在随机谕言机模型下被证明满足 IND-sIDSV-CPA 安全性. 之后, Song 等[13] 将 PK-IPFE 与 HIBE 结合, 提出了首个分层标识内积函数加密 (HIB-IPFE) 方案. 该方案既能够支持密钥授权, 还实现了内积函

数功能. 此外, 他们还在标准模型下证明了 HIB-IPFE 方案满足选择标识及向量和选择明文攻击模型中的不可区分性 (indistinguishability against selective identity and vector, and chosen plaintext attacks, IND-sIDV-CPA). Zhang 等 [14] 探索了自适应安全的标识内积函数加密 (IB-IPFE) 方案的设计, 并在此基础上, 提出了一个抗泄露的 IB-IPFE 方案.

基于 SM9 的标识加密. SM9 作为一款国内自主设计的商用密码, 包括数字签名、密钥交换协议、密钥封装与公钥加密 4 个部分. 在密钥封装与公钥加密方面, 近些年来一系列工作 [16~22, 46, 47] 相继被提出. 文献 [46] 提出了一个新型密钥封装机制 Twin-SM9, 它优化了原有 SM9 密钥封装算法 [48], 消除了其对于 Gap 类困难性问题的依赖. 文献 [47] 提出了首个基于 SM9 的标识签密方案, 相较于先使用 SM9 签名, 后采用 SM9 加密的数据保护方式, 该方案在计算性能与密文长度上优势明显. Tang 等 [16] 提出了一个基于 SM9 的同态加密方案, 该方案支持加法同态运算与门限解密. 为了解决 SM9 标识加密算法中的密钥撤销与更新问题, Qin 等 [17] 提出了一个基于仲裁的 SM9 标识加密方案 SM9-mIBE, 该方案引入了一个仲裁者以便快速处理用户权限变更操作, 且该仲裁者无法通过密文获取任何有用的信息. Pu 等 [18] 设计了一个基于 SM9 的公钥可搜索加密方案 SM9-PEKS. 相较于经典的公钥可搜索加密方案, 该方案在陷门生成算法与测试算法上表现更优. Lai 等 [19] 提出了首个基于 SM9 的标识广播加密方案, 它支持一份密文可由一组指定的用户解密, 并能在随机谕言机模型下被证明满足 CPA 安全性. 文献 [20] 则进一步增强了方案 [19] 的安全性, 提出了一个基于 SM9 的 CCA 安全广播加密方案. 该方案的 CCA 安全性并不借助于 FO 通用转换, 而是通过引入一个虚拟标识实现. Ji 等 [21] 提出了一个基于 SM9 的属性基加密方案, 并在随机谕言机模型下, 证明了其满足 CPA 安全性. 文献 [22] 提出了首个基于 SM9 的分层标识加密方案 SM9-HIBE, 该方案的解密算法仅需两个双线性配对运算, 密文也只占用两个群元素大小, 有着良好的计算与通信开销表现. 综上, 目前尚未见国际、国内主流密码学期刊与会议上发表基于 SM9 的分层标识广播内积函数加密的相关研究成果.

3 预备知识

3.1 符号及其描述

对于 $n \in \mathbb{N}$, 定义 $[n] \stackrel{\text{def}}{=} \{1, 2, \ldots, n\}$. 对于整数 a, b 且 $a \leqslant b$, 定义 $[a, b] \stackrel{\text{def}}{=} \{a, a+1, \ldots, b-1, b\}$. 倘若 A 是一个算法, $A \to a$ 或 $a \leftarrow A$ 表示 A 被调用并输出 a. 对于一个向量 $\boldsymbol{v}$, $S_{\boldsymbol{v}}$ 表示包含向量 $\boldsymbol{v}$ 中各分量的集合, $\mathrm{Pref}(\boldsymbol{v})$ 表示向量 $\boldsymbol{v}$ 的前缀, $|\boldsymbol{v}|$ 表示向量 $\boldsymbol{v}$ 的长度. 对于一个向量集合 $\boldsymbol{\Gamma}$, $S_{\boldsymbol{\Gamma}}$ 表示包含向量集合 $\boldsymbol{\Gamma}$ 中各向量中的每一个分量的集合 (对于不同向量中具有相同值的分量, 仅记录一次), $\mathrm{Pref}(\boldsymbol{\Gamma})$ 则表示 $\bigcup_{\boldsymbol{v} \in \boldsymbol{\Gamma}} \mathrm{Pref}(\boldsymbol{v})$.

3.2 双线性配对

定义1 (双线性配对) 设 $\mathbb{G}_1, \mathbb{G}_2$ 与 $\mathbb{G}_T$ 是 3 个阶为素数 p 的乘法循环群, g 与 g_2 分别为 $\mathbb{G}_1$ 与 $\mathbb{G}_2$ 的一个生成元. 若存在一个映射 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 满足下述性质, 则称 e 是一个双线性映射: (1) 双线性: 对于任意 $u \in \mathbb{G}_1, v \in \mathbb{G}_2$ 以及 $a, b \in \mathbb{Z}_p$, 均有 $e(u^a, v^b) = e(u, v)^{ab}$. (2) 非退化性: $e(g, g_2) \neq 1$, 其中 1 表示 $\mathbb{G}_T$ 中的单位元. (3) 可计算性: 对于所有的 $u \in \mathbb{G}_1, v \in \mathbb{G}_2$, 均存在一个有效的算法计算 $e(u, v)$.

3.3 困难性假设

假设1 (l-DBDHI 假设[22]1)) 挑战者首先运行群生成算法, 该算法以安全参数 λ 作为输入. 接着, 挑战者随机地选择生成元 $g \in \mathbb{G}_1$, 生成元 $\hat{g} \in \mathbb{G}_2$ 与 $a, b, c \in \mathbb{Z}_p$, 并将群描述信息 $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ 以及下列项发送给攻击者:

$$c, g, g^b, g^a, g^{a^2}, \ldots, g^{a^l}, \hat{g}, \hat{g}^b, \hat{g}^a, \hat{g}^{a^2}, \ldots, \hat{g}^{a^l}, \hat{g}^{\frac{1}{(a+c)^2}}, \hat{g}^{\frac{1}{(a+c)^3}}, \ldots, \hat{g}^{\frac{1}{(a+c)^l}}.$$

随后, 挑战者随机地抛掷一枚硬币 $\zeta \in \{0,1\}$. 倘若 $\zeta = 0$, 则挑战者将项 $T = T_0 = e(g,\hat{g})^{\frac{b}{a+c}} \in \mathbb{G}_T$ 发送给攻击者; 否则, 挑战者将一个随机项 $T = T_1 = R \in \mathbb{G}_T$ 发送给攻击者. 最后, 攻击者输出一个关于 ζ 的猜想值 $\zeta' \in \{0,1\}$.

定义2 倘若不存在任何多项式时间敌手 $\mathcal{A}$ 能以一个不可忽略的优势赢得上述游戏的胜利, 则 l-DBDHI 假设成立. 敌手 $\mathcal{A}$ 的优势可被定义为 $\mathrm{Adv}_{\mathcal{A}}^{l\text{-DBDHI}} = |\Pr[\zeta' = \zeta] - 1/2|$.

3.4 分层标识广播内积函数加密的定义及安全模型

分层标识广播内积函数加密包括 Setup, KeyGen, Delegate, Encrypt 与 Decrypt 5 个算法, 其形式化定义如下:

• $\mathsf{Setup}(1^\lambda, d, l, n) \to (\mathrm{PP}, \mathrm{MSK})$. 初始化算法接收一个安全参数 $\lambda \in \mathbb{N}$, 系统最大层次数 (即深度) d, 系统支持的最大用户数量 l 与向量长度 n 作为输入. 输出系统公共参数 PP 与主密钥 MSK.

• $\mathsf{KeyGen}(\mathrm{PP}, \mathrm{MSK}, \mathbf{ID}, \boldsymbol{y}) \to \mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$. 私钥生成算法接收系统公共参数 PP, 主密钥 MSK, 一个长度为 $j \leqslant d$ 的标识向量 $\mathbf{ID}$ 与一个向量 $\boldsymbol{y}$ 作为输入. 输出一个与二元组 $(\mathbf{ID}, \boldsymbol{y})$ 相关的私钥 $\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$.

• $\mathsf{Delegate}(\mathrm{PP}, \mathrm{SK}_{(\mathbf{ID}',\boldsymbol{y})}, I_j) \to \mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$. 委托算法接收系统公共参数 PP, 一个与二元组 $(\mathbf{ID}', \boldsymbol{y})$ 相关的私钥 $\mathrm{SK}_{(\mathbf{ID}',\boldsymbol{y})}$, 其中 $|\mathbf{ID}'| = j - 1 < d$, 和一个标识 I_j 作为输入. 输出一个与二元组 $(\mathbf{ID}, \boldsymbol{y})$ 相关的私钥 $\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$, 其中 $\mathbf{ID} = (\mathbf{ID}', I_j)$ 且 $|\mathbf{ID}| = j \leqslant d$.

• $\mathsf{Encrypt}(\mathrm{PP}, \boldsymbol{V}, \boldsymbol{x}) \to \mathrm{CT}_{\boldsymbol{V}}$. 加密算法接收系统公共参数 PP, 一个广播标识向量集合 $\boldsymbol{V}$ 与一个向量 $\boldsymbol{x}$ 作为输入. 输出一个与广播标识集合 $\boldsymbol{V}$ 相关的密文 $\mathrm{CT}_{\boldsymbol{V}}$.

• $\mathsf{Decrypt}(\mathrm{PP}, \mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}, \mathrm{CT}_{\boldsymbol{V}}) \to \langle \boldsymbol{x}, \boldsymbol{y} \rangle$ or $\perp$. 解密算法接收系统公共参数 PP, 一个与二元组 $(\mathbf{ID}, \boldsymbol{y})$ 相关的私钥 $\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$, 和一个与广播标识集合 $\boldsymbol{V}$ 相关的密文 $\mathrm{CT}_{\boldsymbol{V}}$ 作为输入. 倘若 $\mathbf{ID} \in \mathrm{Pref}(\boldsymbol{V})$ ($\mathrm{Pref}(\cdot)$ 的定义参见 3.1 小节), 则算法执行 (有限范围内) 离散对数求解运算 T_d 后, 输出 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$; 否则, 算法输出 $\perp$.

$$\Pr\left[\langle \boldsymbol{x}, \boldsymbol{y} \rangle \leftarrow \mathsf{Decrypt}(\mathrm{PP}, \mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}, \mathrm{CT}_{\boldsymbol{V}}) : \begin{array}{l} (\mathrm{PP}, \mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda, d, l, n) \\ \mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})} \leftarrow \mathsf{KeyGen}(\mathrm{PP}, \mathrm{MSK}, \mathbf{ID}, \boldsymbol{y}) \\ \mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})} \leftarrow \mathsf{Delegate}(\mathrm{PP}, \mathrm{SK}_{(\mathbf{ID}',\boldsymbol{y})}, I_j) \\ \mathrm{CT}_{\boldsymbol{V}} \leftarrow \mathsf{Encrypt}(\mathrm{PP}, \boldsymbol{V}, \boldsymbol{x}) \end{array}\right] = 1.$$

定义3 (IND-sIDSV-CPA) 倘若对于任意多项式时间敌手 $\mathcal{A}$, 其在下列游戏中的优势均可忽略不计, 则 HIBB-IPFE-SM9 方案是 IND-sIDSV-CPA 安全的.

1) 本文使用的 l-DBDHI 假设基本即是文献 [22] 中使用的 (q,n)-DBDHI 假设 (乘法群版本) 在 $q = n = l$ 设定下的形式, 即 (l,l)-DBDHI 假设. 唯一的不同是本文使用的假设减少了 $g^{a^{l+1}}$ 这一项. 显然易证, 倘若存在一个敌手能以不可忽略的优势 ϵ 解决 l-DBDHI 问题, 则可构建一个模拟器以不可忽略的优势 ϵ 解决 (l,l)-DBDHI 问题[22]. 因此, 上述项的减少并不会破坏假设的困难性.

声明. 敌手 $\mathcal{A}$ 声明一个挑战广播标识向量集合 $\boldsymbol{V}^*$ 和两个挑战向量 $\boldsymbol{x}_0^*, \boldsymbol{x}_1^*$ ($\boldsymbol{x}_0^* \neq \boldsymbol{x}_1^*$), 并将它们发送给挑战者 $\mathcal{C}$.

初始化. 挑战者 $\mathcal{C}$ 运行 $\mathsf{Setup}(1^\lambda, d, l, n)$ 算法, 并将生成的系统公共参数 PP 返回给敌手 $\mathcal{A}$.

阶段 1. 敌手 $\mathcal{A}$ 在该阶段可以提交多项式次私钥查询, 具体为

• **私钥查询 $(\mathbf{ID}, \boldsymbol{y})$.** 敌手 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 提交私钥查询. 对于任意一次私钥查询 $(\mathbf{ID}, \boldsymbol{y})$, $\mathcal{C}$ 均运行 $\mathsf{KeyGen}(\mathrm{PP}, \mathrm{MSK}, \mathbf{ID}, \boldsymbol{y}) \to \mathrm{SK}_{(\mathbf{ID}, \boldsymbol{y})}$, 并将 $\mathrm{SK}_{(\mathbf{ID}, \boldsymbol{y})}$ 返回给 $\mathcal{A}$. 唯一的限制条件为若 $\langle \boldsymbol{x}_0^* - \boldsymbol{x}_1^*, \boldsymbol{y} \rangle \neq 0$ 时, $\mathbf{ID} \notin \mathrm{Pref}(\boldsymbol{V}^*)$.

挑战. 挑战者 $\mathcal{C}$ 选择一个随机比特 $b \in \{0,1\}$, 并运行 $\mathsf{Encrypt}(\mathrm{PP}, \boldsymbol{V}^*, \boldsymbol{x}_b^*) \to \mathrm{CT}_{\boldsymbol{V}^*}$. 随后, $\mathcal{C}$ 将挑战密文 $\mathrm{CT}_{\boldsymbol{V}^*}$ 返回给 $\mathcal{A}$.

阶段 2. 该阶段与**阶段 1** 相同.

猜测. 敌手 $\mathcal{A}$ 输出关于 b 的猜测值 b'. 倘若 $b' = b$, 则敌手 $\mathcal{A}$ 赢得该游戏的胜利. 敌手 $\mathcal{A}$ 的优势定义如下:

$$\mathrm{Adv}^{\text{IND-sIDSV-CPA}}_{\mathcal{A},\text{HIBB-IPFE-SM9}} = |\Pr[b' = b] - 1/2|.$$

3.5 SM9 标识加密方案

为了便于描述, 本小节仅介绍 SM9 密钥封装机制 [15], 该构造使用乘法群, 具体描述如下:

• $\mathsf{Setup}(1^\lambda) \to (\mathrm{PP}, \mathrm{MSK})$: 初始化算法首先调用群生成算法 $\mathcal{G}(1^\lambda)$ 得到非对称双线性群 $D = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, 其中 $p > 2^\lambda$. 随后, 它随机地选择 $\mathbb{G}_1$ 群的生成元 g, $\mathbb{G}_2$ 群的生成元 g_2 和 $\alpha \in \mathbb{Z}_p^*$. 接着, 该算法选择一个抗碰撞哈希 (hash) 函数 $H : \{0,1\}^* \times \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, 一个合适的私钥生成函数识别符 hid[2)]以及一个密钥派生函数 $\mathrm{KDF} : \{0,1\}^* \times \mathbb{Z}_{\mathrm{p}}^* \to \{0,1\}^\ell$, 其中 ℓ 是封装密钥的长度. 最后, 它计算 $g_1 = g^\alpha, v = e(g_1, g_2)$, 并输出系统公共参数/主密钥对 $(\mathrm{PP}, \mathrm{MSK})$ 为

$$\mathrm{PP} = (D, g, g_1, g_2, v, H, \mathrm{KDF}, \mathrm{hid}, \ell), \mathrm{MSK} = \alpha.$$

• $\mathsf{KeyGen}(\mathrm{PP}, \mathrm{MSK}, \mathrm{ID}) \to \mathrm{SK}_{\mathrm{ID}}$: 私钥生成算法解析系统公共参数 PP 为 $(D, g, g_1, g_2, v, H, \mathrm{KDF}, \mathrm{hid}, \ell)$, 主密钥 MSK 为 α 与标识 $\mathrm{ID} \in \{0,1\}^*$. 接着, 它计算

$$K = g_2^{\frac{\alpha}{\alpha + H(\mathrm{ID}||\mathrm{hid}, p)}}.$$

算法输出一个与标识 ID 相关的私钥为 $\mathrm{SK}_{\mathrm{ID}} = (\mathrm{ID}, K)$.

• $\mathsf{Encrypt}(\mathrm{PP}, \mathrm{ID}) \to \mathrm{CT}_{\mathrm{ID}}$: 加密算法解析系统公共参数 PP 为 $(D, g, g_1, g_2, v, H, \mathrm{KDF}, \mathrm{hid}, \ell)$ 与标识 $\mathrm{ID} \in \{0,1\}^*$. 随后, 它随机地选择 $s \in \mathbb{Z}_p^*$, 并计算

$$C_1 = g_1^s g^{H(\mathrm{ID}||\mathrm{hid}, p)s}, C_2 = v^s.$$

接着, 它计算封装密钥 $\mathrm{EK} = \mathrm{KDF}(C_1||C_2||\mathrm{ID}, \ell)$. 算法输出一个封装密钥/封装密文对为 $(\mathrm{EK}, \mathrm{CT}_{\mathrm{ID}} = (\mathrm{ID}, C_1))$.

• $\mathsf{Decrypt}(\mathrm{PP}, \mathrm{SK}_{\mathrm{ID}}, \mathrm{CT}_{\mathrm{ID}'}) \to \mathrm{EK}'$ or $\perp$: 解密算法解析系统公共参数 PP 为 $(D, g, g_1, g_2, v, H, \mathrm{KDF}, \mathrm{hid}, \ell)$, 私钥 $\mathrm{SK}_{\mathrm{ID}}$ 为 (ID, K) 以及封装密文 $\mathrm{CT}_{\mathrm{ID}'}$ 为 (ID', C_1). 接着, 它计算 $C_2' = e(C_1, K), \mathrm{EK}' = \mathrm{KDF}(C_1||C_2'||\mathrm{ID}, \ell)$. 若 EK' 为全 0 比特串, 则输出 $\perp$; 否则, 输出 EK' 为封装密钥.

2) hid: 其长度为一个字节, 由 PKG 选择并公开. 它与身份标识一同作为哈希函数 H 的输入, 以区分使用的 SM9 商用密码中的不同原语. 例如, 根据 SM9 标准 [15] 中的描述, 在 SM9 数字签名中, hid 被设置为 0x01; 而在 SM9 加密算法中, 其则被设置为 0x03.

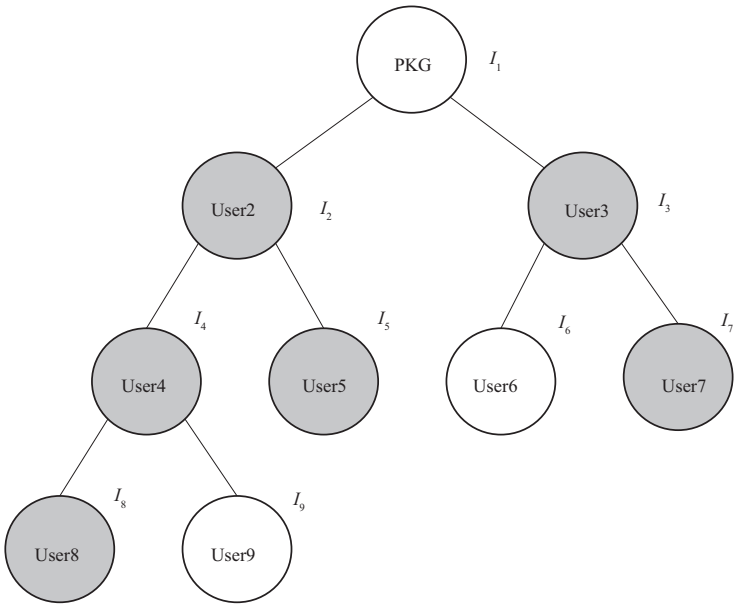

图 1　一个 HIBB-IPFE-SM9 系统中用户组织形式的例子

Figure 1　An example of the organization of users in the HIBB-IPFE-SM9 system

4　HIBB-IPFE-SM9 方案

4.1　具体构造

本小节将描述基于 SM9 的分层标识广播内积函数加密的具体构造. 该构造使用乘法群, 为了描述简洁, 将哈希函数 $H(\cdot||\mathrm{hid},p)$ 简写为 $H(\cdot)$. 例如, $H(I_1||\mathrm{hid},p)$ 表示为 $H(I_1)$. 在 HIBB-IPFE-SM9 系统中, 用户被组织为树形结构, 其中根节点表示 PKG, 使用标识 I_1 标记, 树中其他节点表示用户 i, 使用标识 I_i $(i\in[2,l])$ 标记. 用户的标识向量为从根节点至用户节点路径上标识组成的向量. 例如, 在图 1 中, 用户 5 的标识向量为 $\boldsymbol{I}=(I_1,I_2,I_5)$. 加密者在加密时会指定一个标识向量集合, 其中包含一个或多个能够解密该份密文的用户标识向量. 例如, 图 1 中的灰色节点表示标识向量集合 $\boldsymbol{V}=\{(I_1,I_2,I_5),(I_1,I_3,I_7),(I_1,I_2,I_4,I_8)\}$ 包含的用户节点, 此时集合 $S_{\boldsymbol{V}}=\{I_1,I_2,I_3,I_4,I_5,I_7,I_8\}$. 当灰色节点用户 (如用户 5) 想要解密该份与 $\boldsymbol{V}$ 相关的密文时, 可使用其私钥 (如与 $\boldsymbol{I}$ 相关) 派生出一个与标识向量 $(I_1,I_2,I_3,I_4,I_5,I_7,I_8)$ 相关的 "临时" 私钥, 便能够顺利地解密该密文. 而白色节点用户 (如用户 6) 无法利用其私钥派生出上述 "临时" 私钥, 故不能解密该密文.

令 $\mathcal{X}\subset\mathbb{Z}_p^n$ 与 $\mathcal{Y}\subset\mathbb{Z}_p^n$ 分别是密文中向量 $\boldsymbol{x}$ 与私钥中向量 $\boldsymbol{y}$ 的取值空间. 集合 $\mathcal{V}\subset\mathbb{Z}_p$ 是内积 $\langle\boldsymbol{x},\boldsymbol{y}\rangle$ 的取值空间, 其大小 $|\mathcal{V}|$ 是多项式级的.

• $\mathsf{Setup}(1^\lambda,d,l,n)\to(\mathrm{PP},\mathrm{MSK})$: 初始化算法首先调用群生成算法 $\mathcal{G}(1^\lambda)$ 得到非对称双线性群 $D=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e)$, 其中 $p>2^\lambda$. 随后, 它随机选择 $\mathbb{G}_1$ 群的生成元 g, $\mathbb{G}_2$ 群的生成元 $g_2,g_3,u_2,\ldots,u_l\in\mathbb{G}_2$, $\alpha,\beta_1,\ldots,\beta_n\in\mathbb{Z}_p^*$. 接着, 该算法选择一个抗碰撞哈希函数 $H:\{0,1\}^*\times\mathbb{Z}_p^*\to\mathbb{Z}_p^*$. 最后, 它计算 $g_1=g^\alpha, v=e(g_1,g_2), v'=e(g,g_2), \{g_2^{\beta_i}\}_{i\in[n]}$, 并输出系统公共参数/主密钥对 $(\mathrm{PP},\mathrm{MSK})$ 为

$$\mathrm{PP}=(D,g,g_1,g_2,g_3,\{u_i\}_{i\in[2,l]},\{g_2^{\beta_i}\}_{i\in[n]},v,v',H,d,l,n),\quad \mathrm{MSK}=(\alpha,\{\beta_i\}_{i\in[n]}).$$

• $\mathsf{KeyGen}(\mathrm{PP},\mathrm{MSK},\mathbf{ID},\boldsymbol{y})\to\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$: 私钥生成算法解析系统公共参数 PP 为 $(D,g,g_1,g_2,g_3,$

$\{u_i\}_{i\in[2,l]}, \{g_2^{\beta_i}\}_{i\in[n]}, v, v', H, d, l, n)$, 主密钥 MSK 为 $(\alpha, \{\beta_i\}_{i\in[n]})$, 标识向量 $\mathbf{ID}$ 为 $(I_1, \ldots, I_j)$, 向量 $\boldsymbol{y}$ 为 $(y_1, \ldots, y_n)$. 接着, 它令 $\mathcal{I} = \{i | I_i \in S_{\mathbf{ID}}\}$, 随机地选择 $r \in \mathbb{Z}_p^*$, 并计算

$$K_1 = g_2^{\frac{\alpha\langle\boldsymbol{\beta},\boldsymbol{y}\rangle}{\alpha+H(I_1)}} \left(g_3 \prod_{i\in\mathcal{I}\setminus\{1\}} u_i^{H(I_i)}\right)^r, \quad K_2 = g^{(\alpha+H(I_1))r}, \quad \{\mathcal{K}_i = u_i^r\}_{i\in[l]\setminus\mathcal{I}},$$

其中, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$. 最后, 算法输出一个与二元组 $(\mathbf{ID}, \boldsymbol{y})$ 相关的私钥为

$$\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})} = ((\mathbf{ID}, \boldsymbol{y}), K_1, K_2, \{\mathcal{K}_i\}_{i\in[l]\setminus\mathcal{I}}).$$

• $\mathsf{Delegate}(\mathrm{PP}, \mathrm{SK}_{(\mathbf{ID}',\boldsymbol{y})}, I_j) \to \mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$: 委托算法解析系统公共参数 PP 为 $(D, g, g_1, g_2, g_3, \{u_i\}_{i\in[2,l]}, \{g_2^{\beta_i}\}_{i\in[n]}, v, v', H, d, l, n)$, 私钥 $\mathrm{SK}_{(\mathbf{ID}',\boldsymbol{y})}$ 为 $((\mathbf{ID}', \boldsymbol{y}), K_1', K_2', \{\mathcal{K}_i'\}_{i\in[l]\setminus\mathcal{I}'})$, 其中, $\mathbf{ID} = (\mathbf{ID}', I_j)$. 随后, 它令 $\mathcal{I} = \{i | I_i \in S_{\mathbf{ID}}\}$ 并随机地选择 $\overline{r} \in \mathbb{Z}_p^*$. 接着, 计算

$$K_1 = K_1'(\mathcal{K}_j')^{H(I_j)} \left(g_3 \prod_{i\in\mathcal{I}\setminus\{1\}} u_i^{H(I_i)}\right)^{\overline{r}}, \quad K_2 = K_2'(g_1 g^{H(I_1)})^{\overline{r}}, \quad \{\mathcal{K}_i = \mathcal{K}_i' u_i^{\overline{r}}\}_{i\in[l]\setminus\mathcal{I}}.$$

算法输出一个与二元组 $(\mathbf{ID}, \boldsymbol{y})$ 相关的私钥为

$$\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})} = ((\mathbf{ID}, \boldsymbol{y}), K_1, K_2, \{\mathcal{K}_i\}_{i\in[l]\setminus\mathcal{I}}).$$

容易验证, 该私钥是与二元组 $(\mathbf{ID}, \boldsymbol{y})$ 相关的合法私钥, 且随机数 $r = r' + \overline{r}$, 其中 r' 是私钥 $\mathrm{SK}_{(\mathbf{ID}',\boldsymbol{y})}$ 中使用的随机数.

• $\mathsf{Encrypt}(\mathrm{PP}, \boldsymbol{V}, \boldsymbol{x}) \to \mathrm{CT}_{\boldsymbol{V}}$: 加密算法解析系统公共参数 PP 为 $(D, g, g_1, g_2, g_3, \{u_i\}_{i\in[2,l]}, \{g_2^{\beta_i}\}_{i\in[n]}, v, v', H, d, l, n)$ 与向量 $\boldsymbol{x}$ 为 $(x_1, \ldots, x_n)$. 随后, 它令集合 $\mathbb{I} = \{i : I_i \in S_{\boldsymbol{V}}\}$ 并随机地选择 $s \in \mathbb{Z}_p^*$. 接着, 计算

$$C_1 = g_1^s g^{H(I_1)s}, \quad C_2 = \left(g_3 \prod_{i\in\mathbb{I}\setminus\{1\}} u_i^{H(I_i)}\right)^s, \quad \{C_{x,i} = e(g, g_2)^{x_i} e(g_1, g_2^{\beta_i})^s\}_{i\in[n]}.$$

算法输出一个与广播标识集合 $\boldsymbol{V}$ 相关的密文为

$$\mathrm{CT}_{\boldsymbol{V}} = (\boldsymbol{V}, C_1, C_2, \{C_{x,i}\}_{i\in[n]}).$$

• $\mathsf{Decrypt}(\mathrm{PP}, \mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}, \mathrm{CT}_{\boldsymbol{V}}) \to \langle\boldsymbol{x}, \boldsymbol{y}\rangle$ or $\perp$: 解密算法解析系统公共参数 PP 为 $(D, g, g_1, g_2, g_3, \{u_i\}_{i\in[2,l]}, \{g_2^{\beta_i}\}_{i\in[n]}, v, v', H, d, l, n)$, 私钥 $\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$ 为 $((\mathbf{ID}, \boldsymbol{y}), K_1, K_2, \{\mathcal{K}_i\}_{i\in[l]\setminus\mathcal{I}})$ 以及密文 $\mathrm{CT}_{\boldsymbol{V}}$ 为 $(\boldsymbol{V}, C_1, C_2, \{C_{x,i}\}_{i\in[n]})$. 倘若 $\mathbf{ID} \notin \mathrm{Pref}(\boldsymbol{V})$, 算法输出 $\perp$; 否则, 算法进行如下计算:

$$\mathsf{W} = \frac{\prod_{i\in[n]} C_{x,i}^{y_i} \cdot e(K_2, C_2)}{e(C_1, K_1 \prod_{i\in\mathbb{I}\cap\neg\mathcal{I}} \mathcal{K}_i^{H(I_i)})}.$$

算法接着在内积空间 $\mathcal{V}$ 中查找 ϑ, 使得 $e(g, g_2)^\vartheta = \mathsf{W}$ 成立. 倘若 ϑ 存在, 则算法输出 ϑ; 否则, 它输出 $\perp$. 注意到, 由于 $|\mathcal{V}|$ 是多项式级的, 故该算法是可计算的.

4.2 正确性分析

倘若 $(\mathrm{PP},\mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda,d,l,n)$, $\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})} \leftarrow \mathsf{KeyGen}(\mathrm{PP},\mathrm{MSK},\mathbf{ID},\boldsymbol{y})$ (或 $\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})} \leftarrow \mathsf{Delegate}(\mathrm{PP},\mathrm{SK}_{(\mathbf{ID}',\boldsymbol{y})},I_j)$), $\mathrm{CT}_{\boldsymbol{V}} \leftarrow \mathsf{Encrypt}(\mathrm{PP},\boldsymbol{V},\boldsymbol{x})$, 则有

$$
\begin{aligned}
\mathsf{W} &= \frac{\prod_{i\in[n]} C_{x,i}^{y_i}\cdot e(K_2,C_2)}{e(C_1,K_1\cdot\prod_{i\in\mathbb{I}\cap\neg\mathcal{I}}\mathcal{K}_i^{H(I_i)})}\\
&= \frac{\prod_{i\in[n]} e(g,g_2)^{x_iy_i}e(g,g_2)^{\alpha\beta_iy_is}\cdot e(g^{r(\alpha+H(I_1))},(g_3\prod_{i\in\mathbb{I}\setminus\{1\}}u_i^{H(I_i)})^s)}{e((g_1g^{H(I_1)})^s,g_2^{\frac{\alpha\langle\boldsymbol{\beta},\boldsymbol{y}\rangle}{\alpha+H(I_1)}}(g_3\prod_{i\in\mathcal{I}\setminus\{1\}}u_i^{H(I_i)})^r\prod_{i\in\mathbb{I}\cap\neg\mathcal{I}}((u_i)^r)^{H(I_i)})}\\
&= \frac{e(g,g_2)^{\langle\boldsymbol{x},\boldsymbol{y}\rangle}\cdot e(g,g_2)^{\alpha\langle\boldsymbol{\beta},\boldsymbol{y}\rangle s}\cdot e(g^{\alpha+H(I_1)},g_3\prod_{i\in\mathbb{I}\setminus\{1\}}u_i^{H(I_i)})^{rs}}{e(g^{(\alpha+H(I_1))s},g_2^{\frac{\alpha\langle\boldsymbol{\beta},\boldsymbol{y}\rangle}{\alpha+H(I_1)}})\cdot e(g^{(\alpha+H(I_1))s},(g_3\prod_{i\in(\mathcal{I}\cup(\mathbb{I}\cap\neg\mathcal{I}))\setminus\{1\}}u_i^{H(I_i)})^r)}\\
&= \frac{e(g,g_2)^{\langle\boldsymbol{x},\boldsymbol{y}\rangle}\cdot e(g,g_2)^{s\alpha\langle\boldsymbol{\beta},\boldsymbol{y}\rangle}\cdot e(g^{\alpha+H(I_1)},g_3\prod_{i\in\mathbb{I}\setminus\{1\}}u_i^{H(I_i)})^{rs}}{e(g,g_2)^{s\alpha\langle\boldsymbol{\beta},\boldsymbol{y}\rangle}\cdot e(g^{\alpha+H(I_1)},g_3\prod_{i\in\mathbb{I}\setminus\{1\}}u_i^{H(I_i)})^{sr}} \quad (\text{由于 } \mathcal{I}\subseteq\mathbb{I},\mathcal{I}\cup(\mathbb{I}\cap\neg\mathcal{I})=\mathbb{I})\\
&= \frac{e(g,g_2)^{\langle\boldsymbol{x},\boldsymbol{y}\rangle}\cdot e(g,g_2)^{s\alpha\langle\boldsymbol{\beta},\boldsymbol{y}\rangle}}{e(g,g_2)^{s\alpha\langle\boldsymbol{\beta},\boldsymbol{y}\rangle}} = e(g,g_2)^{\langle\boldsymbol{x},\boldsymbol{y}\rangle}.
\end{aligned}
$$

4.3 安全性证明

本小节将对定理 1 进行证明, 该定理保证了 HIBB-IPFE-SM9 方案满足 IND-sIDSV-CPA 安全性.

定理1 令方案中的哈希函数 H 为随机谕言机. 倘若 l-DBDHI 假设成立, 则 HIBB-IPFE-SM9 方案满足 IND-sIDSV-CPA 安全性.

证明 假设存在一个敌手 $\mathcal{A}$ 能够以不可忽略的优势 $\mathcal{E}$ 攻破 HIBB-IPFE-SM9 方案, 则可构造一个模拟器 $\mathcal{B}$, 它能以不可忽略的优势攻击 l-DBDHI 假设. 模拟器 $\mathcal{B}$ 输入 l-DBDHI 问题实例 $(c,g,g^b,g^a,g^{a^2},\ldots,g^{a^l},\hat{g},\hat{g}^b,\hat{g}^a,\hat{g}^{a^2},\ldots,\hat{g}^{a^l},\hat{g}^{\frac{1}{(a+c)^2}},\hat{g}^{\frac{1}{(a+c)^3}},\ldots,\hat{g}^{\frac{1}{(a+c)^l}},T)$, 其中 $T=e(g,\hat{g})^{\frac{b}{a+c}}$ 或 $T=R\in\mathbb{G}_T$, l 为系统支持的最大用户数量. 模拟器 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 的交互如下.

初始化. 敌手 $\mathcal{A}$ 输出一个挑战广播标识集合 $\boldsymbol{V}^*$ (其对应的索引集合 $\mathbb{I}^*=\{i:I_i^*\in S_{\boldsymbol{V}^*}\}$), 其中 $|S_{\boldsymbol{V}^*}|\leqslant l$, 以及两个挑战向量 $\boldsymbol{x}_0^*=(x_{0,1}^*,x_{0,2}^*,\ldots,x_{0,n}^*)$, $\boldsymbol{x}_1^*=(x_{1,1}^*,x_{1,2}^*,\ldots,x_{1,n}^*)$.

系统建立. 模拟器 $\mathcal{B}$ 令 $x^*=c$ (设为 $H(I_1^*)$ 的值), 选取两两不同的随机数 $x_i^*\in\mathbb{Z}_p^*$ (设为 $H(I_i^*)$ 的值), 其中 $i\in\mathbb{I}^*$. 接着, $\mathcal{B}$ 选择随机数 $w,x_1,x_2,\ldots,x_l,y_2,y_3,\ldots,y_l,\phi_1,\ldots,\phi_n\in\mathbb{Z}_p^*$, 并隐式地令 $\alpha=a,\beta=(a+w)\bmod p$ 以及对于任意 $i\in[n]$, $\beta_i=\phi_i(a+x^*)+(x_{0,i}^*-x_{1,i}^*)\bmod p$. 随后, $\mathcal{B}$ 计算

$$
\begin{aligned}
&g_1=g^a,\ g_2=\hat{g}^\beta=\hat{g}^a\cdot\hat{g}^w,\ v=e(g_1,g_2),\ v'=e(g,g_2),\\
&\left\{u_i=\hat{g}^{x_i+\frac{y_i}{(a+x^*)^{l+2-i}}}=\hat{g}^{x_i}\cdot(\hat{g}^{\frac{1}{(a+x^*)^{l+2-i}}})^{y_i}\right\}_{i\in[2,l]},\\
&g_3=\hat{g}^{x_1(a+x^*)}\Big/\prod_{i\in\mathbb{I}^*\setminus\{1\}}u_i^{x_i^*}=(\hat{g}^a)^{x_1}\cdot\hat{g}^{x_1x^*}\Big/\prod_{i\in\mathbb{I}^*\setminus\{1\}}u_i^{x_i^*},\\
&\left\{g_2^{\beta_i}=g_2^{\phi_i(a+x^*)+(x_{0,i}^*-x_{1,i}^*)}=(\hat{g}^{a^2})^{\phi_i}\cdot(\hat{g}^a)^{\phi_i(x^*+w)}\cdot\hat{g}^{\phi_ix^*w}\cdot g_2^{(x_{0,i}^*-x_{1,i}^*)}\right\}_{i\in[n]}.
\end{aligned}
$$

最后, $\mathcal{B}$ 将公共参数 $\mathrm{PP}=(D,g,g_1,g_2,g_3,\{u_i\}_{i\in[2,l]},\{g_2^{\beta_i}\}_{i\in[n]},v,v',H,d,l,n)$ 返回给 $\mathcal{A}$. 需要注意的是, $\mathcal{B}$ 不知道 α 的值, 故也不知道 MSK 完整的值.

哈希询问. 敌手 $\mathcal{A}$ 提交查询标识 I_i. 此时, 模拟器 $\mathcal{B}$ 维护一个哈希列表 L_h, 记录标识/哈希值二元组 (I_i,h_i), 其初始值为空. 若 I_i 在 L_h 中, $\mathcal{B}$ 将对应的 h_i 返回给 $\mathcal{A}$; 否则, $\mathcal{B}$ 执行如下操作:

• 若 I_i 为首层标识时, $\mathcal{B}$ 将 $h_i = H(I_1^*) = x^* = c$ 返回给 $\mathcal{A}$, 并将新二元组 (I_i, h_i) 添加至 L_h 中.

• 若 I_i 为非首层标识且 $I_i \in S_{\boldsymbol{V}^*}$ 时, $\mathcal{B}$ 将 $h_i = H(I_i^*) = x_i^*$ 返回给 $\mathcal{A}$, 并将新二元组 (I_i, h_i) 添加至 L_h 中.

• 若 I_i 为非首层标识且 $I_i \notin S_{\boldsymbol{V}^*}$ 时, $\mathcal{B}$ 随机地选取 $z_i \in \mathbb{Z}_p^*$, 将 $h_i = H(I_i) = z_i$ 返回给 $\mathcal{A}$, 并将新二元组 (I_i, h_i) 添加至 L_h 中.

询问阶段 1. 在该阶段, 敌手 $\mathcal{A}$ 可以提交多项式次私钥查询. 对于任意一次私钥查询 **ID**, 模拟器 $\mathcal{B}$ 均执行如下操作:

• 情况 1. 若 $\langle \boldsymbol{x}_0, \boldsymbol{y}\rangle \neq \langle \boldsymbol{x}_1, \boldsymbol{y}\rangle$, 此时 $\mathbf{ID} \notin \mathrm{Pref}(\boldsymbol{V}^*)$, 即至少存在一个索引值 k, 使得 $I_k \in S_{\mathbf{ID}}, I_k \notin S_{\boldsymbol{V}^*}$ 成立. 令 k 为满足该条件的最小下标, $\mathbf{ID}_k = (I_1, \ldots, I_k), \mathcal{I} = \{i | I_i \in S_{\mathbf{ID}}\}$ 以及 $\mathcal{I}_k = \{i | I_i \in S_{\mathbf{ID}_k}\}$. $\mathcal{B}$ 首先计算 K_1. 此时

$$
\begin{aligned}
g_2^{\frac{\alpha\langle \boldsymbol{\beta}, \boldsymbol{y}\rangle}{\alpha + H(I_1^*)}} &= \hat{g}^{\frac{\alpha\beta}{\alpha + H(I_1^*)} \sum_{i=1}^n (\phi_i (a + x^*) y_i + (x_{0,i}^* - x_{1,i}^*) y_i)} \\
&= (\hat{g}^{a^2})^{\sum_{i=1}^n \phi_i y_i} \cdot (\hat{g}^a)^{w \sum_{i=1}^n \phi_i y_i} \cdot \hat{g}^{(\tau(a) + \frac{W}{a + x^*}) \sum_{i=1}^n (x_{0,i}^* - x_{1,i}^*) y_i}, \\
g_3 \prod_{i \in \mathcal{I} \setminus \{1\}} u_i^{H(i)} &= \hat{g}^{x_1 (a + x^*)} \Big/ \prod_{i \in \mathbb{I}^* \setminus \{1\}} u_i^{x_i^*} \cdot \prod_{i \in \mathcal{I} \setminus \{1\}} u_i^{H(I_i)} \\
&= \hat{g}^{x_1 (a + x^*)} \cdot \prod_{i \in \mathbb{I}^* \setminus \{1, k\}} u_i^{-x_i^*} \cdot \prod_{i \in \mathcal{I} \setminus \{1, k\}} u_i^{H(I_i)} \cdot u_k^{H(I_k) - x_k^*} \\
&= \hat{g}^{x_1 (a + x^*)} \cdot \prod_{i \in (\mathbb{I}^* \cup \mathcal{I}) \setminus ((\mathbb{I}^* \cap \mathcal{I}) \cup \{k\})} u_i^{\Delta_i} \cdot u_k^{\Delta_k},
\end{aligned}
$$

其中, $\tau(a)$ 是一次多项式, Δ_i 是可求指数 $(i \in (\mathbb{I}^* \cup \mathcal{I}) \setminus (\mathbb{I}^* \cap \mathcal{I}))$, W 是一个常数. 模拟器 $\mathcal{B}$ 隐式地令 $r = \hat{r} - \frac{W}{\Delta_k y_k} (a + x^*)^{(2 + l - k) - 1} \sum_{i=1}^n (x_{0,i}^* - x_{1,i}^*) y_i$, 并计算

$$
K_1 = g_2^{\frac{\alpha\langle \boldsymbol{\beta}, \boldsymbol{y}\rangle}{\alpha + H(I_1^*)}} \cdot (\hat{g}^{x_1 (a + x^*)})^r \cdot \left(\prod_{i \in (\mathbb{I}^* \cup \mathcal{I}) \setminus ((\mathbb{I}^* \cap \mathcal{I}) \cup \{k\})} u_i^{\Delta_i} \right)^r \cdot (u_k^{\Delta_k})^r.
$$

其中,

$$
\begin{aligned}
(\hat{g}^{x_1 (a + x^*)})^r &= (\hat{g}^{x_1 (a + x^*)})^{\hat{r}} \cdot (\hat{g}^{x_1 (a + x^*)})^{-\frac{W}{\Delta_k y_k} (a + x^*)^{(2 + l - k) - 1} \sum_{i=1}^n (x_{0,i}^* - x_{1,i}^*) y_i} \\
&= (\hat{g}^{x_1 (a + x^*)})^{\hat{r}} \cdot \hat{g}^{-\frac{x_1 W}{\Delta_k y_k} (a + x^*)^{(2 + l - k)} \sum_{i=1}^n (x_{0,i}^* - x_{1,i}^*) y_i} \\
&= (\hat{g}^a)^{x_1 \hat{r}} \cdot \hat{g}^{x_1 x^* \hat{r}} \cdot (\hat{g}^{(a + x^*)^{(2 + l - k)}})^{-\frac{x_1 W}{\Delta_k y_k} \sum_{i=1}^n (x_{0,i}^* - x_{1,i}^*) y_i},
\end{aligned}
$$

$$\begin{aligned}\left(\prod_{i\in(\mathbb{I}^*\cup\mathcal{I})\backslash((\mathbb{I}^*\cap\mathcal{I})\cup\{k\})} u_i^{\Delta_i}\right)^r &= \prod_{i\in(\mathbb{I}^*\cup\mathcal{I})\backslash((\mathbb{I}^*\cap\mathcal{I})\cup\{k\})} (u_i)^{\Delta_i r}\\ &= \prod_{i\in(\mathbb{I}^*\cup\mathcal{I})\backslash((\mathbb{I}^*\cap\mathcal{I})\cup\{k\})} u_i^{\Delta_i\hat{r}-\frac{\Delta_i W}{\Delta_k y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= \prod_{i\in(\mathbb{I}^*\cup\mathcal{I})\backslash((\mathbb{I}^*\cap\mathcal{I})\cup\{k\})} u_i^{\Delta_i\hat{r}}\\ &\quad\cdot \prod_{i\in(\mathbb{I}^*\cup\mathcal{I})\backslash((\mathbb{I}^*\cap\mathcal{I})\cup\{k\})} (\hat{g}^{x_i+\frac{y_i}{(a+x^*)^{l+2-i}}})^{-\frac{\Delta_i W}{\Delta_k y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= \prod_{i\in(\mathbb{I}^*\cup\mathcal{I})\backslash((\mathbb{I}^*\cap\mathcal{I})\cup\{k\})} u_i^{\Delta_i\hat{r}}\\ &\quad\cdot \prod_{i\in(\mathbb{I}^*\cup\mathcal{I})\backslash((\mathbb{I}^*\cap\mathcal{I})\cup\{k\})} (\hat{g}^{(a+x^*)^{(1+l-k)}})^{-\frac{x_i\Delta_i W}{\Delta_k y_k}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &\quad\cdot \prod_{i\in(\mathbb{I}^*\cup\mathcal{I})\backslash((\mathbb{I}^*\cap\mathcal{I})\cup\{k\})} (\hat{g}^{(a+x^*)^{(i-k-1)}})^{-\frac{y_i\Delta_i W}{\Delta_k y_k}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i},\end{aligned}$$

$$\begin{aligned}(u_k^{\Delta_k})^r &= (u_k^{\Delta_k})^{\hat{r}-\frac{W}{\Delta_k y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= u_k^{\Delta_k\hat{r}}\cdot(\hat{g}^{x_k+\frac{y_k}{(a+x^*)^{l+2-k}}})^{-\frac{\Delta_k W}{\Delta_k y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= u_k^{\Delta_k\hat{r}}\cdot\hat{g}^{-\frac{x_k W}{y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &\quad\cdot(\hat{g}^{\frac{y_k}{(a+x^*)^{l+2-k}}})^{-\frac{W}{y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= u_k^{\Delta_k\hat{r}}\cdot\hat{g}^{-\frac{x_k W}{y_k}(a+x^*)^{(1+l-k)}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\cdot(\hat{g}^{\frac{W}{a+x^*}})^{-\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= u_k^{\Delta_k\hat{r}}\cdot(\hat{g}^{(a+x^*)^{(1+l-k)}})^{-\frac{x_k W}{y_k}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\cdot(\hat{g}^{\frac{W}{a+x^*}})^{-\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}.\end{aligned}$$

由于 $\hat{g}^{(\tau(a)+\frac{W}{a+x^*})\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\cdot(\hat{g}^{\frac{W}{a+x^*}})^{-\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}=(\hat{g}^{\tau(a)})^{\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}$, $2+l-k\in[2,l]$, $1+l-k\in[1,l-1]$, $i-k-1\in[0,l-3]$, 其中 $k\in[2,l], i\in\mathcal{I}\backslash\mathcal{I}_k$ (易知 $k<i\leqslant l$), 因此, $\mathcal{B}$ 能够使用假设中的项顺利地计算出 K_1.

接着, $\mathcal{B}$ 计算 $K_2,\{\mathcal{K}_i\}_{i\in[l]\backslash\mathcal{I}}$ 为

$$\begin{aligned}K_2 &= g^{(\alpha+H(I_1))r}\\ &= g^{(a+x^*)(\hat{r}-\frac{W}{\Delta_k y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*))y_i}\\ &= g^{(a+x^*)\hat{r}}\cdot g^{-\frac{W}{\Delta_k y_k}(a+x^*)^{(2+l-k)}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= (g^a)^{\hat{r}}\cdot g^{x^*\hat{r}}\cdot(g^{(a+x^*)^{(2+l-k)}})^{-\frac{W}{\Delta_k y_k}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i},\end{aligned}$$

对于任意$i\in[l]\backslash\mathcal{I}$,

$$\begin{aligned}\mathcal{K}_i &= u_i^r\\ &= u_i^{\hat{r}}\cdot(\hat{g}^{x_i+\frac{y_i}{(a+x^*)^{l+2-i}}})^{-\frac{W}{\Delta_k y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= u_i^{\hat{r}}\cdot\hat{g}^{-\frac{x_i W}{\Delta_k y_k}(a+x^*)^{(2+l-k)-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\cdot\hat{g}^{-\frac{y_i W}{\Delta_k y_k}(a+x^*)^{i-k-1}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\\ &= u_i^{\hat{r}}\cdot(\hat{g}^{(a+x^*)^{(1+l-k)}})^{-\frac{x_i W}{\Delta_k y_k}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}\cdot(\hat{g}^{(a+x^*)^{i-k-1}})^{-\frac{y_i W}{\Delta_k y_k}\sum_{i=1}^n(x_{0,i}^*-x_{1,i}^*)y_i}.\end{aligned}$$

显然, $\mathcal{B}$ 也能够利用假设中的项计算出 $K_2,\{\mathcal{K}_i\}_{i\in[l]\backslash\mathcal{I}}$.

• 情况 2. 若 $\langle \boldsymbol{x}_0, \boldsymbol{y}\rangle = \langle \boldsymbol{x}_1, \boldsymbol{y}\rangle$, 此时 $g_2^{\frac{\alpha\langle \boldsymbol{\beta}, \boldsymbol{y}\rangle}{\alpha+H(I_1^*)}} = (\hat{g}^{a^2})^{\sum_{i=1}^n \phi_i y_i} (\hat{g}^a)^{w\sum_{i=1}^n \phi_i y_i} \hat{g}^{(\tau(a)+\frac{W}{a+x^*})\sum_{i=1}^n (x_{0,i}^* - x_{1,i}^*) y_i}$ $= (\hat{g}^{a^2})^{\sum_{i=1}^n \phi_i y_i} (\hat{g}^a)^{w\sum_{i=1}^n \phi_i y_i}$, 故未知项 $\hat{g}^{\frac{1}{a+x^*}}$ 未出现. 在该情况下, $\mathcal{B}$ 可选择随机数 $r \in \mathbb{Z}_p^*$, 并计算

$$K_1 = g_2^{\frac{\alpha\langle \boldsymbol{\beta}, \boldsymbol{y}\rangle}{\alpha+H(I_1^*)}} \left(g_3 \prod_{i\in\mathcal{I}\setminus\{1\}} u_i^{H(I_i)} \right)^r = (\hat{g}^{a^2})^{\sum_{i=1}^n \phi_i y_i} (\hat{g}^a)^{w\sum_{i=1}^n \phi_i y_i} \cdot \left(g_3 \prod_{i\in\mathcal{I}\setminus\{1\}} u_i^{H(I_i)} \right)^r,$$

$$K_2 = g^{(\alpha+H(I_1))r} = (g^a)^r \cdot g^{x^* r},$$

$$\{\mathcal{K}_i = u_i^r\}_{i\in[l]\setminus\mathcal{I}}.$$

至此, 在上述两种情况下, $\mathcal{B}$ 均可计算出私钥 $\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})} = ((\mathbf{ID}, \boldsymbol{y}), K_1, K_2, \{\mathcal{K}_i\}_{i\in[l]\setminus\mathcal{I}})$. 最后, $\mathcal{B}$ 将私钥 $\mathrm{SK}_{(\mathbf{ID},\boldsymbol{y})}$ 返回给 $\mathcal{A}$.

挑战. 模拟器 $\mathcal{B}$ 隐式地令 $s = \frac{b}{a+x^*}$, 并随机地抛掷一枚硬币, 得到结果 $\zeta \in \{0,1\}$. 接着, 对于任意 $i \in [n]$, 构建 $C_{x,i}^*$ 为

$$C_{x,i}^* = e(g, g_2)^{x_{\zeta,i}^*} e(g^b, \hat{g}^{a^2}(\hat{g}^a)^w)^{\phi_i} \cdot e(g^b, \hat{g}^{\tau(a)})^{(x_{0,i}^* - x_{1,i}^*)} \cdot T^{W(x_{0,i}^* - x_{1,i}^*)}.$$

随后, $\mathcal{B}$ 计算 C_1^*, C_2^* 为

$$\begin{aligned} C_1^* &= g_1^s g^{H(I_1^*)s} = (g^{a+x^*})^{\frac{b}{a+x^*}} = g^b, \\ C_2^* &= \left(g_3 \prod_{i\in\mathbb{I}^*\setminus\{1\}} u_i^{H(I_i^*)} \right)^s \\ &= \left(\hat{g}^{x_1(a+x^*)} \Big/ \prod_{i\in\mathbb{I}^*\setminus\{1\}} u_i^{x_i^*} \cdot \prod_{i\in\mathbb{I}^*\setminus\{1\}} u_i^{x_i^*} \right)^s \\ &= \hat{g}^{x_1(a+x^*)\frac{b}{a+x^*}} = (\hat{g}^b)^{x_1}. \end{aligned}$$

最后, $\mathcal{B}$ 将挑战密文 $CT_{\boldsymbol{V}^*}^* = (\boldsymbol{V}^*, C_1^*, C_2^*, \{C_{x,i}^*\}_{i\in[n]})$ 返回给 $\mathcal{A}$.

询问阶段 2. 该阶段与**询问阶段 1** 相同.

猜测阶段. 敌手 $\mathcal{A}$ 输出一个关于 ζ 的猜测值 $\zeta' \in \{0,1\}$, 并发送给模拟器 $\mathcal{B}$. 倘若 $\zeta = \zeta'$, 则 $\mathcal{B}$ 输出 0, 表示猜测 $T = T_0 = e(g,\hat{g})^{\frac{b}{a+c}} \in \mathbb{G}_T$. 否则, $\mathcal{B}$ 将输出 1, 表示猜测 $T = T_1 = R \in \mathbb{G}_T$.

模拟器 $\mathcal{B}$ 的优势分析. 模拟器 $\mathcal{B}$ 的优势 $\mathrm{Adv}_{\mathcal{B}}^{l\text{-DBDHI}}$ 计算如下:

$$\begin{aligned} \mathrm{Adv}_{\mathcal{B}}^{l\text{-DBDHI}} &= \Pr[T = T_0]\Pr[\zeta = \zeta' | T = T_0] + \Pr[T = T_1]\Pr[\zeta \neq \zeta' | T = T_1] - \frac{1}{2} \\ &= \frac{1}{2} \cdot \left(\frac{1}{2} + \mathcal{E} \right) + \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \\ &= \frac{1}{4} + \frac{\mathcal{E}}{2} + \frac{1}{4} - \frac{1}{2} \\ &= \frac{\mathcal{E}}{2}. \end{aligned}$$

注意, 上述表达式成立的原因为

(1) $\Pr[T = T_0] = \Pr[T = T_1] = \frac{1}{2}$.

(2) 当 $T = T_0 = e(g,\hat{g})^{\frac{b}{a+c}}$ 时, 对于任意 $i \in [n]$,

$$C_{x,i}^* = e(g, g_2)^{x_{\zeta,i}^*} \cdot e(g^b, \hat{g}^{a^2}(\hat{g}^a)^w)^{\phi_i} \cdot e(g^b, \hat{g}^{\tau(a)})^{(x_{0,i}^* - x_{1,i}^*)} \cdot T^{W(x_{0,i}^* - x_{1,i}^*)}$$

$$
\begin{aligned}
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g^b, \hat{g}^{a(a+w)})^{\phi_i} \cdot e(g^b, \hat{g}^{\tau(a)})^{(x^*_{0,i}-x^*_{1,i})} \cdot e(g,\hat{g})^{\frac{b}{a+c}W(x^*_{0,i}-x^*_{1,i})} \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g^a, \hat{g}^{\beta})^{\phi_i b} \cdot e(g,\hat{g})^{(\tau(a)+\frac{W}{a+c})b(x^*_{0,i}-x^*_{1,i})} \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g^a, \hat{g}^{\beta})^{\phi_i(a+x^*)\frac{b}{a+x^*}} \cdot e(g,\hat{g})^{\frac{a\beta}{a+x^*}b(x^*_{0,i}-x^*_{1,i})} \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g_1,g_2)^{s\phi_i(a+x^*)} \cdot e(g^a, \hat{g}^{\beta})^{\frac{b}{a+x^*}(x^*_{0,i}-x^*_{1,i})} \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g_1,g_2)^{s(\phi_i(a+x^*)+(x^*_{0,i}-x^*_{1,i}))} \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g_1,g_2)^{s\beta_i} \\
&= e(g,g_2)^{x^*_{\zeta,i}} e(g_1,g_2^{\beta_i})^s.
\end{aligned}
$$

显然, 在该情况下, $CT^*_{\boldsymbol{V}^*}$ 是 $\boldsymbol{x}_b$ 在 HIBB-IPFE-SM9 方案中的合法密文且模拟过程是完美的. 因此, $\Pr[\zeta=\zeta'|T=T_0] = 1/2 + \mathrm{Adv}^{\text{IND-sIDSV-CPA}}_{\mathcal{A},\text{HIBB-IPFE-SM9}} = 1/2+\mathcal{E}$.

(3) 当 $T = T_1 = R \in \mathbb{G}_T$ 时, T 可被表示为 $T = e(g,\hat{g})^{\frac{b}{a+c}} e(g,\hat{g})^{\widetilde{r}}$, 其中 $\widetilde{r} \in \mathbb{Z}^*_p$. 此时, 对于任意 $i \in [n]$,

$$
\begin{aligned}
C^*_{x,i} &= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g^b, \hat{g}^{a^2}(\hat{g}^a)^w)^{\phi_i} \cdot e(g^b, \hat{g}^{\tau(a)})^{(x^*_{0,i}-x^*_{1,i})} \cdot T^{W(x^*_{0,i}-x^*_{1,i})} \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g^b, \hat{g}^{a^2}(\hat{g}^a)^w)^{\phi_i} \cdot e(g^b, \hat{g}^{\tau(a)})^{(x^*_{0,i}-x^*_{1,i})} \cdot e(g,\hat{g})^{\frac{b}{a+c}W(x^*_{0,i}-x^*_{1,i})} \cdot e(g,\hat{g})^{\widetilde{r}W(x^*_{0,i}-x^*_{1,i})} \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g_1,g_2)^{s(\phi_i(a+x^*)+(x^*_{0,i}-x^*_{1,i}))} \cdot e(g,\hat{g})^{\widetilde{r}W(x^*_{0,i}-x^*_{1,i})} \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g,\hat{g})^{\widetilde{r}W(x^*_{0,i}-x^*_{1,i})} \cdot e(g_1,g_2^{\beta_i})^s \\
&= e(g,g_2)^{x^*_{\zeta,i}} \cdot e(g,g_2)^{\frac{\widetilde{r}W(x^*_{0,i}-x^*_{1,i})}{\beta}} \cdot e(g_1,g_2^{\beta_i})^s \\
&= e(g,g_2)^{x^*_{\zeta,i}+\frac{\widetilde{r}W(x^*_{0,i}-x^*_{1,i})}{a+w}} e(g_1,g_2^{\beta_i})^s.
\end{aligned}
$$

根据上式可知, 此时加密的向量为 $\widetilde{\boldsymbol{x}} = (x^*_{\zeta,1}+\frac{\widetilde{r}W}{a+w}(x^*_{0,1}-x^*_{1,1}), \ldots, x^*_{\zeta,n}+\frac{\widetilde{r}W}{a+w}(x^*_{0,n}-x^*_{1,n}))$. 由于 $\widetilde{r}$ 是一个均匀分布的随机指数, 故 $\widetilde{\boldsymbol{x}}$ 不等于 $\boldsymbol{x}^*_\zeta$, 即关于 ζ 的信息均被隐藏. 因此, $\Pr[\zeta \neq \zeta'|T=T_1] = 1/2$.

5 方案性能分析

本节从理论和实验两方面对 HIBB-IPFE-SM9 方案与相关方案的性能表现进行了对比分析.

5.1 理论分析

本小节从理论方面将本文方案的特性、安全性、计算开销和通信开销同方案 [12, 13, 23] 进行了对比. 表 1 给出了特性和安全性的对比结果, 其中, ROM (random oracle model) 表示随机谕言机模型, Standard 表示标准模型, IND-sIDS-CCA 即选择标识集合与选择密文攻击模型中的不可区分性. 由表 1 可知, 方案-1 [23] 和方案-2 [23] 不支持内积函数功能, 方案 [12] 无法实现密钥授权, 方案 [13] 不支持密文广播. 相比之下, 本文方案是目前唯一同时支持上述 3 个功能的方案. 在安全性方面, 本文方案同支持密文广播与内积函数功能的方案 [12] 一样, 均可在随机谕言机模型下被证明满足 CPA 安全性.

表 2 展示了计算开销的对比结果, 其中考虑到双线性配对运算与循环群 $\mathbb{G}, \mathbb{G}_i$ ($i \in \{1,2,T\}$) 中的指数运算较为耗时, 因此主要统计各算法中上述运算的执行次数. E 表示循环群 $\mathbb{G}$ 中的指数运算, E_i 表示循环群 $\mathbb{G}_i$ ($i \in \{1,2,T\}$) 中的指数运算, P 表示双线性配对运算, T_d 表示 (有限范围内) 离散对数求解运算, T_{sig} 表示一次签名 (one-time signature) 的签名运算, T_{ver} 表示一次签名的验证运算, l 表示系统支持的最大用户数量, d 表示系统支持的最大深度, n 表示向量长度, $|S_{\boldsymbol{V}}|$ 表示广播标识集合中标

表 1 特性和安全性对比

Table 1 Comparison of features and security

Schemes	Inner product functionality	Ciphertext broadcast	Key delegation	Security	Model	Assumption	Order of group
[23]-1	×	✓	✓	IND-sIDS-CPA	Standard	DBDHI	Prime
[23]-2	×	✓	✓	IND-sIDS-CCA	Standard	DBDHI	Prime
[12]	✓	✓	×	IND-sIDSV-CPA	ROM	AGDDHE*	Prime
[13]	✓	×	✓	IND-sIDV-CPA	Standard	DBDHE	Prime
Ours	✓	✓	✓	IND-sIDSV-CPA	ROM	DBDHI	Prime

* Both of the AGDDHE and l-DBDHI assumptions are the variants of the general Diffie-Hellman exponent assumption defined in [26]. This type of assumptions has a common lower bound on the computational complexity in the generic group model [26].

表 2 计算开销对比

Table 2 Comparison of computational overhead

Schemes	KeyGen	Delegate ($j-1 \to j$)	Encrypt	Decrypt
[23]-1	$(l+2)E$	$(l+3)E$	$(\|S_{\boldsymbol{V}}\|+2)E+E_T+P$	$(\|S_{\boldsymbol{V}}\|-j)E+2P$
[23]-2	$(l+2)E$	$(l+3)E$	$(\|S_{\boldsymbol{V}}\|+3)E+E_T+P+T_{\text{sig}}$	$(\|S_{\boldsymbol{V}}\|-j+1)E+2P+T_{\text{ver}}$
[12]	E	–	$(\|S_{\boldsymbol{V}}\|+n+2)E+(2n+1)E_T$ $+(n+1)P$	$(\|S_{\boldsymbol{V}}\|+n-1)E+(n+1)E_T$ $+3P+T_d$
[13]	$(n+d+2)E$	$(d+3)E$	$(j+2)E+2nE_T+(n+1)P$	nE_T+2P+T_d
Ours	$E_1+(l+1)E_2$	$2E_1+(l+1)E_2$	$2E_1+\|S_{\boldsymbol{V}}\|E_2+2nE_T$	$(\|S_{\boldsymbol{V}}\|-j)E_2+nE_T+2P+T_d$

识的数量, j 表示参与运算的标识向量的长度. 根据表 2 可知, 在私钥生成算法与委托算法上, 本文方案与同样支持分层及密文广播的方案-1 [23] 和方案-2 [23] 间的计算开销关系, 取决于 E, E_1, E_2 的大小关系. 不妨设 E_1 与 E_2 大致相等. 此时, 当 $E<E_2$ 时, 本文方案要弱于方案-1 [23] 和方案-2 [23]; 而当 $E>E_2$ 时, 本文方案则好于它们. 在加密与解密算法上, 本文方案优于支持密文广播及内积函数功能的方案 [12]. 同时, 当 $|S_{\boldsymbol{V}}|=j$ 时, 本文方案解密算法的计算效率与方案 [13] 基本相同.

表 3 展示了存储开销的对比结果, 其中, l, d, n, j 的意义与表 2 中相同, 而 $|\mathbb{G}|$ 表示群 $\mathbb{G}$ 中元素的大小, $|\mathbb{G}_i|$ 表示群 $\mathbb{G}_i$ 中元素的大小, $|\mathbb{Z}_p|$ 表示群 $\mathbb{Z}_p$ 中元素的大小, $|vk|$ 表示一次签名的验证密钥大小, $|\sigma|$ 表示一次签名的签名大小. 由表 3 可知, 在公钥与密文长度方面, 方案-1 [23] 由于不支持内积函数功能且未使用一次签名技术, 表现最优. 而在支持内积函数功能的方案中, 本文方案的密文长度优于方案 [12], 且与方案 [13] 是可比的. 在私钥长度方面, 由于不支持分层或密文广播功能, 方案 [12,13] 具有一定的优势, 而本文方案则与方案-1 [23] 和方案-2 [23] 相近.

5.2 实验仿真

本小节从实验角度将本文 HIBB-IPFE-SM9 方案中各算法的运行时间同方案 [12,13,23] 进行了对比. 本文使用 Java 语言, 基于 jPBC (Java pairing based cryptography) 密码库与 Type D 双线性配对对各方案进行了原型实现, 其中 Type D 双线性配对基于域 $\mathbb{F}_q$ 中的椭圆曲线 $y^2=x^3+ax+b$ 构造, 其安全强度约为 100 比特 [49,50]3). 接着, 使用一台台式机进行了一系列仿真实验, 该台式机的处

3) 具体参数使用的是 jPBC 密码库自带的 d224.properties 文件中的参数, 其与 Charm 密码库 [49] 中 MNT224 椭圆曲线的参数设置相同. 而根据文献 [50] 中附录 C 给出的结论, MNT224 椭圆曲线的安全强度约为 100 比特, 因此, 本文使用的椭圆曲线的安全强度也约为 100 比特.

表 3　存储开销对比

Table 3　Comparison of storage overhead

Schemes	Public key size	Secret key size	Ciphertext size
[23]-1	$(l+4)\|\mathbb{G}\|$	$(l-j+2)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$
[23]-2	$(l+4)\|\mathbb{G}\|$	$(l-j+2)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|+\|vk\|+\|\sigma\|$
[12]	$(3n+4)\|\mathbb{G}\|$	$\|\mathbb{G}\|+\|\mathbb{Z}_p\|$	$(n+2)\|\mathbb{G}\|+(n+1)\|\mathbb{G}_T\|$
[13]	$(d+n+3)\|\mathbb{G}\|$	$(d-j+2)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+n\|\mathbb{G}_T\|$
Ours	$2\|\mathbb{G}_1\|+(n+l+1)\|\mathbb{G}_2\|+2\|\mathbb{G}_T\|$	$\|\mathbb{G}_1\|+(l-j+1)\|\mathbb{G}_2\|$	$\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+n\|\mathbb{G}_T\|$

理器为 Intel Core(TM) i7-3770 (3.4 GHz * 4), 内存大小为 16 G, 操作系统为 Windows 10 Pro 64-bit (Version 10.0.17134.407), 软件开发工具包为 JDK 16.0.1. 对于每一组实验, 均采用运行 30 次取平均的方式作为算法的运行时间. 此外, 对于有限范围内离散对数求解的实现, 均使用预先建立内积值与群元素关系表的优化方式, 使得相关方案的解密算法仅需完成一次查表操作.

图 2(a)∼(e) 展示了 IBBIPFE [12], HIBIPFE [13] 和 HIBB-IPFE-SM9 方案中各算法的运行时间随着向量长度 n 增长的变化情况, 其中参数设定为 n 从 2 增长至 20, 步长为 2, 系统最大深度 $d=4$, 系统支持的最大用户数量 $l=8$, 内积值 $\langle \boldsymbol{x}, \boldsymbol{y}\rangle$ 的范围为 $[0, 10000]$, 用户标识向量的长度 $j=1$, 密文中的标识向量长度 j' 与广播标识集合包含的标识数量 $|S_{\boldsymbol{V}}|$ 均为 2. 图 2(f)∼(h) 展示了 HIBBE [23] (CPA 安全版本)、HIBIPFE [12] 和 HIBB-IPFE-SM9 方案中 KeyGen, Encrypt 与 Decrypt 算法的运行时间随着标识向量长度或参与运算的标识数量增加的变化情况, 其中参数设定为标识向量长度 j 与参与运算的标识数量 (即 j' 或 $|S_{\boldsymbol{V}}|$) 均从 5 增长至 14, 步长为 1, 系统最大深度 $d=15$, 系统支持的最大用户数量 $l=j+1$, 向量长度 $n=1$, 内积值 $\langle \boldsymbol{x}, \boldsymbol{y}\rangle$ 的范围为 $[0, 1]$[4].

根据图 2 中的实验结果可知, 当 n 增长时, 本文 HIBB-IPFE-SM9 方案在 Encrypt 与 Decrypt 算法上表现最优, 在 $n=20$ 时的运行时间分别约为 1708 与 98 ms. 同时, 它在 Setup 与 KeyGen 算法上表现较弱, 但考虑到这两个算法往往是一次性的且运行于 PKG 端, 故这一运行时间上的差距是可接受的. 当 n 为 1 且标识向量的长度或参与运算的标识数量增长时, HIBB-IPFE-SM9 方案在 KeyGen 算法上表现较好 (j 不大的情况下), 同时在 Encrypt 算法上与 HIBBE 方案 [23] 相当, 且优于 HIBIPFE 方案 [13]. 而 HIBB-IPFE-SM9 方案在 Decrypt 算法上弱于其他两个参与对比的方案, 但差距较小, 平均差距仅约为 2.9 ms. 综上, 实验分析与理论分析的结果一致, 均表明本文 HIBB-IPFE-SM9 方案在性能表现上与现有相关方案是可比的.

6　结论

针对现有 SM9 标识加密算法无法同时支持内积函数功能、一对多密文访问控制与密钥授权的问题, 本文提出了首个基于 SM9 的分层标识广播内积函数加密方案, 即 HIBB-IPFE-SM9. 通过向密文和密钥引入实现内积函数功能的结构, 使得接收方解密密文后仅能恢复内积值, 有效地控制了信息的泄露量. 引入分层结构并改造 HIBE 的单一解密路径, 在实现密钥授权的同时还支持针对同一份密文下的多用户解密功能. 方案的解密算法仅包含两个双线性配对运算, 且方案可在随机谕言机模型下被证明能够抵御选择明文攻击. 最后, 理论和实验分析表明相较于目前国际上最新的标识内积函数加密

4) 为了便于在解密算法上将 HIBIPFE 方案、HIBB-IPFE-SM9 方案与不支持内积函数功能的 HIBBE 方案进行比较, 将内积值的范围设定为 $[0, 1]$, 以消除求解离散对数时间的影响.

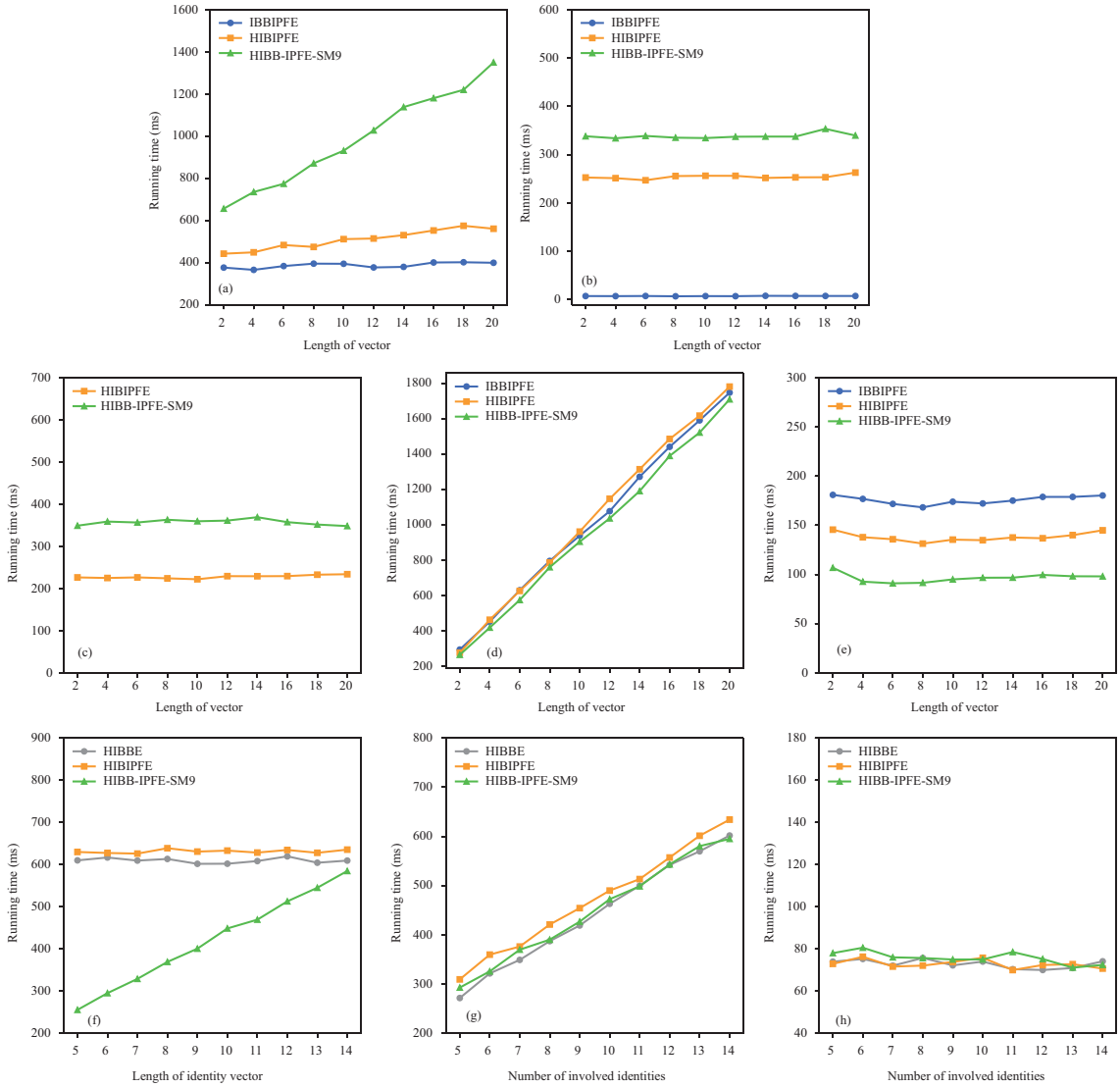

图 2 (网络版彩图) 相关方案中各算法在不同向量长度与不同参与运算的标识数量下的运行时间

Figure 2 (Color online) Running time of various algorithms under different lengths of the vector and numbers of involved identities. (a) Setup algorithm; (b) KeyGen algorithm; (c) delegate algorithm; (d) encrypt algorithm; (e) decrypt algorithm; (f) KeyGen algorithm (ID); (g) encrypt algorithm (ID); (h) decrypt algorithm (ID)

方案, HIBB-IPFE-SM9 方案不仅具有支持密钥授权或密文广播的优势, 在计算与通信开销上也是可比的.

当前, 构建一个自适应安全且基于 SM9 的分层标识广播内积函数加密方案仍是一个尚未解决的问题, 它包括两部分挑战: 一是如何实现挑战标识集合 $\boldsymbol{V}^*$ 的自适应性选择, 并保证方案的紧规约安全; 二是如何实现挑战向量 $\boldsymbol{x}_0^*, \boldsymbol{x}_1^*$ 的自适应性选择, 解决现有自适应安全的 IB-IPFE 方案的密钥结构无法直接与 SM9 标识加密方案兼容的问题. 在后续工作中, 将进一步对上述问题进行探索.

参考文献

1 Abdalla M, Bourse F, Caro A D, et al. Simple functional encryption schemes for inner products. In: Proceedings of the

18th IACR International Conference on Practice and Theory in Public-Key Cryptography (PKC'15), Gaithersburg, 2015. 733–751
2 Shamir A. Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO 84 on Advances in Cryptology, California, 1984. 47–53
3 Boneh D, Franklin M K. Identity-based encryption from the weil pairing. In: Proceedings of the 21st Annual International Cryptology Conference (CRYPTO'01), Santa Barbara, 2001. 213–229
4 Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption. In: Proceedings of the 23rd International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04), Interlaken, 2004. 207–222
5 Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In: Proceedings of the 23rd International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04), Interlaken, 2004. 223–238
6 Boneh D, Boyen X. Secure identity based encryption without random oracles. In: Proceedings of the 24th Annual International Cryptology Conference (CRYPTO'04), Santa Barbara, 2004. 443–459
7 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 (EUROCRYPT'05), Aarhus, 2005. 114–127
8 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 (EUROCRYPT'06), St. Petersburg, 2006. 445–464
9 Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Proceedings of the 29th Annual International Cryptology Conference (CRYPTO'09), Santa Barbara, 2009. 619–636
10 Lai J, Deng R H, Liu S, et al. Identity-based encryption secure against selective opening chosen-ciphertext attack. In: Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'14), Copenhagen, 2014. 77–92
11 Döttling N, Garg S. Identity-based encryption from the diffie-hellman assumption. In: Proceedings of the 37th Annual International Cryptology Conference (CRYPTO'17), Santa Barbara, 2017. 537–569
12 Lai J, Mu Y, Guo F, et al. Identity-based broadcast encryption for inner products. Comput J, 2018, 61: 1240–1251
13 Song G, Deng Y, Huang Q, et al. Hierarchical identity-based inner product functional encryption. Inf Sci, 2021, 573: 332–344
14 Zhang L, Wang X, Chen Y, et al. Adaptive-secure identity-based inner-product functional encryption and its leakage-resilience. In: Proceedings of the 21st International Conference on Cryptology in India (INDOCRYPT'20), Bangalore, 2020. 666–690
15 GM/T0044-2016. Identity-based cryptographic algorithm SM9. 2016 [GM/T0044-2016. SM9 标识密码算法. 2016] http://www.gmbz.org.cn/main/postDetail.html?id=20180322410400
16 Tang F, Ling G W, Shan J Y. Additive homomorphic encryption schemes based on SM2 and SM9. J Cryptol Res, 2022, 9: 535–549 [唐飞, 凌国玮, 单进勇. 基于国密 SM2 和 SM9 的加法同态加密方案. 密码学报, 2022, 9: 535–549]
17 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]
18 Pu L, Lin C, Wu W, et al. A public-key encryption with keyword search scheme from SM9. J Cyber Secur, 2023, 8: 108–118 [蒲浪, 林超, 伍玮, 等. 基于 SM9 的公钥可搜索加密方案. 信息安全学报, 2023, 8: 108–118]
19 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]
20 Lai J C, Huang X Y, He D B, et al. CCA secure broadcast encryption based on SM9. J Softw, 2023, 34: 3354–3364 [赖建昌, 黄欣沂, 何德彪, 等. 基于 SM9 的 CCA 安全广播加密方案. 软件学报, 2023, 34: 3354–3364]
21 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
22 Lai J C, Huang X Y, He D B, et al. An efficient hierarchical identity-based encryption based on SM9. Sci Sin Inform, 2023, 53: 918–930 [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]

23 Liu W, Liu J, Wu Q, et al. Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption. Int J Inf Secur, 2016, 15: 35–50

24 Horwitz J, Lynn B. Toward hierarchical identity-based encryption. In: Proceedings of the 21st International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02), Amsterdam, 2002. 466–481

25 Gentry C, Silverberg A. Hierarchical ID-based cryptography. In: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'02), Queenstown, 2002. 548–566

26 Boneh D, Boyen X, Goh E. Hierarchical identity based encryption with constant size ciphertext. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, 2005. 440–456

27 Gentry C, Halevi S. Hierarchical identity based encryption with polynomially many levels. In: Proceedings of the 6th Theory of Cryptography Conference (TCC'09), San Francisco, 2009. 437–456

28 Lewko A B, Waters B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Proceedings of the 7th Theory of Cryptography Conference (TCC'10), Zurich, 2010. 455–479

29 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 (EUROCRYPT'11), Tallinn, 2011. 547–567

30 Boyen X, Waters B. Anonymous hierarchical identity-based encryption (without random oracles). In: Proceedings of the 26th Annual International Cryptology Conference (CRYPTO'06), Santa Barbara, 2006. 290–307

31 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 (PKC'09), Irvine, 2009. 215–234

32 Langrehr R, Pan J. Tightly secure hierarchical identity-based encryption. In: Proceedings of the 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'19), Beijing, 2019. 436–465

33 Langrehr R, Pan J. 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 (PKC'20), Edinburgh, 2020. 153–183

34 Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'07), Kuching, 2007. 200–215

35 Sakai R, Furukawa J. Identity-based broadcast encryption. Cryptol ePrint Arch, 2007, 2007: 217

36 Gentry C, Waters B. Adaptive security in broadcast encryption systems (with short ciphertexts). In: Proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'09), Cologne, 2009. 171–188

37 Ren Y, Gu D. Fully CCA2 secure identity based broadcast encryption without random oracles. Inf Process Lett, 2009, 109: 527–533

38 Kim J, Susilo W, Au M H, et al. Efficient semi-static secure broadcast encryption scheme. In: Proceedings of the 6th International Conference on Pairing-Based Cryptography (Pairing'13), Beijing, 2013. 62–76

39 Kim J, Susilo W, Au M H, et al. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. IEEE Trans Inform Forensic Secur, 2015, 10: 679–693

40 Liu W, Liu J, Wu Q, et al. Hierarchical identity-based broadcast encryption. In: Proceedings of the 19th Australasian Conference on Information Security and Privacy (ACISP'14), Wollongong, 2014. 242–257

41 Susilo W, Chen R, Guo F, et al. Recipient revocable identity-based broadcast encryption: how to revoke some recipients in IBBE without knowledge of the plaintext. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (AsiaCCS'16), Xi'an, 2016. 201–210

42 Ge A, Wei P. Identity-based broadcast encryption with efficient revocation. In: Proceedings of the 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'19), Beijing, 2019. 405–435

43 Xu P, Li J, Wang W, et al. Anonymous identity-based broadcast encryption with constant decryption complexity and strong security. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (AsiaCCS'16), Xi'an, 2016. 223–233

44 He K, Weng J, Liu J, et al. Anonymous identity-based broadcast encryption with chosen-ciphertext security.

In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (AsiaCCS'16), Xi'an, 2016. 247–255

45 Kim J, Camtepe S, Susilo W, et al. Identity-based broadcast encryption with outsourced partial decryption for hybrid security models in edge computing. In: Proceedings of the ACM Asia Conference on Computer and Communications Security (AsiaCCS'19), Auckland, 2019. 55–66

46 Lai J C, Huang X Y, He D B, et al. Security analysis of uppercaseSM9 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]

47 Lai J C, Huang X Y, He D B, et al. An efficient identity-based signcryption scheme based on SM9. J Cryptol Res, 2021, 8: 314–329 [赖建昌, 黄欣沂, 何德彪, 等. 基于商密 SM9 的高效标识签密. 密码学报, 2021, 8: 314–329]

48 Cheng Z. Security analysis of SM9 key agreement and encryption. In: Proceedings of the 14th International Conference on Information Security and Cryptology (Inscrypt'18), Fuzhou, 2018. 3–25

49 Akinyele J, Green M, Rubin A. Charm: a framework for rapidly prototyping cryptosystems. In: Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS'12), San Diego, 2012

50 Rouselakis Y, Waters B. Efficient statically-secure large-universe multi-authority attribute-based encryption. Cryptol ePrint Arch, 2015, 2015: 16

Hierarchical identity-based broadcast inner product functional encryption based on SM9

Cong LI[1,3,4], Junkai LIANG[1,3,4], Yujia DING[2,4], Qingni SHEN[2,3,4*] & Zhonghai WU[2,3,4*]

1. *School of Computer Science, Peking University, Beijing* 100871*, China*;
2. *School of Software and Microelectronics, Peking University, Beijing* 102600*, China*;
3. *National Engineering Research Center for Software Engineering, Peking University, Beijing* 100871*, China*;
4. *PKU-OCTA Laboratory for Blockchain and Privacy Computing, Peking University, Beijing* 100871*, China*

* Corresponding author. E-mail: qingnishen@ss.pku.edu.cn, wuzh@pku.edu.cn

Abstract In the inner product functional encryption, when decrypting a ciphertext corresponding with the vector $\boldsymbol{x}$ leveraging a secret key related with the vector $\boldsymbol{y}$, the decryptor can merely obtain $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ and nothing else. The hierarchical broadcast inner product encryption further achieves the features of ciphertext broadcasting to target users and key delegation. The SM9 identity-based encryption as a Chinese cryptographic standard designed by China, has been applied in Internet of Things, medical collaboration services and e-government affairs. Nevertheless, the SM9 encryption and its current extension algorithms cannot achieve the inner product functionality, and the ciphertext broadcast and key delegation features simultaneously, which restricts its application scenarios. In this paper, we design a hierarchical identity-based broadcast inner product functional encryption scheme based on SM9, dubbed HIBB-IPFE-SM9, which borrows the design ideas of Abdalla et al.'s inner product functional encryption scheme (PKC'15) and Liu et al.'s hierarchical broadcast encryption scheme (ACISP'14). Its decryption algorithm only contains two pairing operations. We also formally prove the HIBB-IPFE-SM9 scheme chosen-plaintext secure in the random oracle model. Eventually, we compare our HIBB-IPFE-SM9 scheme with the related schemes. The results demonstrate that ours has comparable computation and communication costs to them.

Keywords inner product functional encryption, hierarchical broadcast encryption, identity-based cryptography, SM9, CPA