中国科学:信息科学 2026 年 第 56 卷 第 6 期: 1407–1419
SCIENTIA SINICA Informationis
论文

# 基于 SM9 的密文策略属性基加密

刘晓红[1], 林超[2*], 伍玮[3], 黄欣沂[4]

1. 运城学院数学与信息技术学院, 运城 044000
2. 福建师范大学计算机与网络空间安全学院, 福州 350117
3. 香港科技大学 (广州) 教育学院, 广州 511455
4. 暨南大学网络空间安全学院, 广州 510632
* 通信作者. E-mail: chaolin@nuaa.edu.cn

收稿日期: 2025–04–03; 修回日期: 2025–06–07; 接受日期: 2025–07–25; 网络出版日期: 2026–05–20

国家自然科学基金 (批准号: 62425205, 62572216, 62372108) 和山西省基础研究计划青年项目 (批准号: 202403021222303) 资助

**摘要** 密文策略属性基加密作为属性基加密的重要分支, 通过在加密数据时设置访问策略, 实现对数据的细粒度访问控制. 相较于传统基于身份的加密技术, 密文策略属性基加密支持 “单发多收” 的动态加密模式, 特别适用于多用户协作场景下的数据精准安全访问控制. 当前, 该技术已被广泛应用于云计算、物联网、区块链等新一代信息技术领域. SM9 标识加密是我国自主设计的商用标识密码算法, 现已成为国家标准和国际标准. 目前由 SM9 标识加密衍生的属性基加密算法较少, 尚不能满足国产信息系统对多用户数据安全灵活共享的需求. 本文在 SM9 标识加密的基础上, 结合经典密文策略属性基加密的构造思路, 提出了一种基于 SM9 的密文策略属性基加密方案, 并证明方案在 $(q, k{+}1)$-DBDHI 安全假设下具有抗选择明文攻击安全性, 且可通过 FO 转换技术实现抗选择密文攻击安全性. 理论分析和实验结果表明, 与国外经典的密文策略属性基加密方案相比, 本文提出方案的通信代价和计算开销均与之相当. 与现有基于 SM9 的密文策略属性基加密方案中使用的访问树相比, 本文提出的方案采用了数学性质良好的线性秘密共享方案表示访问策略, 具有很好的扩展性和安全性, 且方案在密钥生成阶段所需要的时间至少缩短了 27%. 因此, 本文提出的方案可促进属性基加密在国产信息系统中的应用发展.

**关键词** 密文策略, 属性基加密, 线性秘密共享, SM9

## 1 引言

随着数字经济的蓬勃发展, 数据规模呈指数级增长, 其价值在经济和社会活动中日益凸显. 然而, 数据安全风险也随之加剧, 数据泄露、篡改和滥用等问题频发, 严重威胁着个人隐私和商业机密. 特别是在云计算等新兴数字技术的推动下, 各行业产生了海量数据及多元化的处理需求, 用户和企业普遍倾向于将数据托管至第三方云服务器, 以实现高效存储和计算资源共享. 然而, 这些服务器通常由 “诚实但好奇” 的云服务提供商管理, 他们可能出于利益动机访问、泄露或共享用户的敏感数据. 这一现状对云环境中数据的机密性保护与访问控制技术提出了严峻挑战. 传统的广播加密 (broadcast encryption, BE) 技术虽然可以为数据提供机密性保护和 “一对多” 的

**引用格式:** 刘晓红, 林超, 伍玮, 等. 基于 SM9 的密文策略属性基加密. 中国科学: 信息科学, 2026, 56: 1407–1419, doi: 10.1360/SSI-2025-0132
Liu X H, Lin C, Wu W, et al. Ciphertext-policy attribute-based encryption based on SM9. Sci Sin Inform, 2026, 56: 1407–1419, doi: 10.1360/SSI-2025-0132

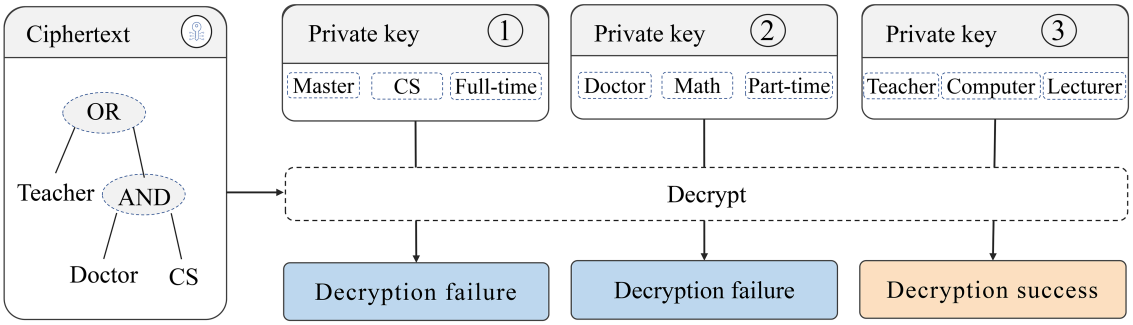


**图 1　(网络版彩图) 密文策略属性基加密系统图.**

**Figure 1**　(Color online) System diagram of CP-ABE.

数据共享模式, 但其加密过程需要依赖预定义的接收者的公钥集合完成数据加密, 仅授权的接收者可以解密并正确恢复明文数据. 然而, 在动态开放的分布式计算环境下, 加密者往往难以在初始化阶段精准预判接收群体的规模与成员, 导致该方案在动态成员管理方面存在不足. 属性基加密 (attribute-based encryption, ABE) 是一种基于属性的公钥密码算法, 可以实现多用户数据的精准灵活安全访问控制. 依据数据访问策略嵌入的载体不同, 属性基加密分为密文策略属性基加密 (ciphertext-policy ABE, CP-ABE) 和密钥策略属性基加密 (key-policy ABE, KP-ABE) 两类. 在 KP-ABE 中, 加密者将数据与属性集合 (例如: 数据的种类、产生的时间、日期等) 相关联, 权威机构根据用户的访问权限设置其对应的解密密钥, 解密时, 当且仅当解密者的访问权限被数据的属性集合所满足时, 就可以正确解密; 在 CP-ABE 中, 加密者为数据定义访问策略 (例如 “Teacher” 或 (“Doctor” 与 “CS”)), 并将访问策略嵌入密文中, 只有满足该访问策略的用户属性集合 (如 {Teacher, Computer, Lecturer}) 才能成功解密并访问数据, 而不满足访问策略的用户属性集合 (如 {Master, CS, Full-time} 或 {Doctor, Math, Part-time}) 则无法解密 (如图 1 所示). 得益于其灵活的访问控制能力和高效的数据共享特性, CP-ABE 已被广泛应用于云计算、物联网、区块链等新一代信息技术领域, 特别是在医疗数据共享以及智能电网等需要复杂权限管理的场景中具有显著优势. 目前, 大多数 CP-ABE 方案都是基于国外密码算法设计的, 难以满足我国信息技术安全可控的需求. SM9 是我国自主研发的标识密码算法, 包括标识加密、数字签名、密钥交换协议和密钥封装机制. SM9 的设计为密码技术的自主可控提供了重要支撑, 并于 2021 年陆续成为国家和国际标准 [1]. 现阶段, 基于 SM9 标识密码的功能型加密方案已取得一定进展, 主要包括标识签密、广播加密、可搜索加密、半同态加密、模糊标识加密以及密钥策略属性基加密等. 然而, 在国内外核心学术期刊及重要学术会议中, 基于 SM9 的 CP-ABE 研究仍较为匮乏. 在现有研究成果中, 文献 [2] 的方案仅能实现最简单的 AND 门数据访问控制. 文献 [3] 的方案是基于访问树结构构造的. 基于 LSSS 构造的 CP-ABE 方案能够支持更细粒度的多用户数据安全访问控制, 且在策略表达的灵活性与系统的可扩展性方面具有一定优势. 因此, 论文在文献 [2,3] 的基础上, 研究基于 LSSS 的 SM9 密文策略属性基加密具有理论价值和实际意义.

### 1.1　本文贡献

本文借鉴国外经典 CP-ABE 算法的构造思路, 在 SM9 标识加密算法的基础上, 提出了第一个基于线性秘密共享方案 (linear secret sharing scheme, LSSS) 的 CP-ABE 方案, 简称为 SM9-CP-ABE. 具体贡献如下:

(1) 本文提出的方案充分保留了 SM9 标识加密的结构特性, 能够与现有基于 SM9 的信息系统实现无缝兼容;

(2) 与国外经典的密文策略属性基加密方案相比, 本文提出的方案具有相当的计算开销和通信代价;

(3) 与现有基于 SM9 的密文策略属性基加密方案中使用的访问树和 AND 门相比, 本文提出的方案采用了数学性质良好的线性秘密共享方案表示访问结构, 具有良好的可扩展性. 此外与访问树结构的 CP-ABE 方案相比, 本文方案可将系统建立时间至少缩短 27%.

### 1.2　技术路线

虽然基于 LSSS 的 CP-ABE 方案相比基于访问树或 AND 门的方案具有一定优势, 但其技术实现却面临双重挑战. 首先, 在方案构造中, 基于 LSSS 的 CP-ABE 方案需要将主秘密值 $s$ 通过 LSSS 结构分割成与属性相关的秘密份额, 并嵌入 SM9 结构的密文中, 此外方案的构造还需兼顾方案的安全性和效率, 这将是困难的. 其次, 在方案安全性证明中, 基于 LSSS 结构的 CP-ABE 方案中的挑战密文可能与一个很大的访问结构 $\boldsymbol{M}^*$ 相关联, 且一个访问结构可能多次包含同一属性. 因此, 如何针对 SM9 的结构特点选择合适的数学困难问题将挑战访问结构编程到系统参数中, 并在该难题和随机谕言模型下证明方案的选择性或适应性安全, 是极具挑战性的. 具体的构造思路和安全性证明如下.

本文首先通过 SM9 标识加密算法的 **Setup** 算法以及借鉴经典 CP-ABE 方案的构造技巧, 在 SM9 标识加密的基础上, 引入属性空间, 生成基于 SM9 的 CP-ABE 方案的公共参数; 其次, 在密钥生成阶段, 引入属性集合 $S$, 根据 SM9 标识加密中的指数逆密钥结构 $\mathrm{sk}_{\mathrm{ID}} = \frac{\alpha}{H_1(\mathrm{ID}||\mathrm{hid},N)+\alpha}P_2$, 生成本文方案中的主要解密密钥 $K = \frac{\alpha}{H_1(N||\mathrm{hid},N)+\alpha}P_2 + tP_2$ 以及与属性相关的部分解密密钥 $\forall x \in S, K_x = t(H_1(N||\mathrm{hid})+\alpha)h_x$; 在加密阶段, 引入线性秘密共享方案表示访问策略. 首先, 产生加密时选择的随机数 $s$ 针对所有属性的秘密份额 $\lambda_i$ $(i \in [1,l])$, 其中 $l$ 是线性秘密生成矩阵的行数. 其次, 结合 SM9 标识加密的密文结构 $Q_{\mathrm{ID}} = H_1(\mathrm{ID}||\mathrm{hid},N)P_1 + P_{\mathrm{pub}}$, 产生方案的主密文 $C' = s(H_1(\mathrm{ID}||\mathrm{hid},N)P_1 + P_{\mathrm{pub}})$, 以及与该访问结构相关联的部分密文 $C_i = \lambda_i P_2 - r_i h_{\rho(i)}$, $D_i = r_i P_1$. 综上所述, 本文所构造的方案最大化地保留了 SM9 标识加密的密钥和密文结构. 在方案的安全性证明中, 本文结合 SM9 的指数逆密钥结构以及 LSSS 结构, 选择 $(q,k+1)$-DBDHI 困难问题, 并在该难题假设下证明方案的安全性.

### 1.3　相关工作

**属性基加密.** 为了减轻证书管理产生的负担, Shamir [4] 于 1984 年使用标识作为用户公钥, 提出了标识加密 (identity-based encryption, IBE) 算法. 在 IBE 的基础上, Sahai 和 Waters [5] 于 2005 年构建了模糊标识加密 (fuzzy IBE, FIBE) 机制, 并首次引入了属性基加密 (attribute-based encryption, ABE) 的核心思想, 即用户在加密数据时可以表达他想怎样分享加密数据. 随后, Goyal 等 [6] 对这一思想进行了进一步的扩展和完善, 提出了首个 KP-ABE 系统. 2007 年, Bethencourt 等 [7] 基于一般的群假设理论, 提出了基于访问树的 CP-ABE 系统. 同年, Cheung 等 [8] 在标准模型下提出了具有抗选择明文攻击安全的 CP-ABE 方案. 2010 年, Lewko 等 [9] 基于合数阶群上的数学困难问题假设, 提出了具有适应性安全的 CP-ABE 系统. 同年, Waters [10] 在标准模型下提出了可证明安全的、高效的和表达力强的 CP-ABE 系统. 2012 年, Liu 等 [11] 提出了支持白盒追踪的 CP-ABE 方案. 2013 年, Rouselakis 等 [12] 提出了支持大属性集合的属性基加密构造新思路和证明方法. 2015 年, Liu 等 [13] 又提出了支持黑盒追踪的 CP-ABE 方案. 2016 年, Ning 等 [14] 提出了支持黑盒追踪且具有短密文的 CP-ABE 方案. 2018 年, Jiang 等 [15] 提出了可抵抗密钥滥用攻击的 CP-ABE 方案. 同年, Ning 等 [16] 提出了具有用户撤销的 CP-ABE. 2019 年, Liu 等 [17] 提出了支持白盒追踪和用户撤销的 CP-ABE. 2020 年, Xu 等 [18] 提出了支持黑盒追踪的 CP-ABE. 2022 年, Ning 等 [19] 提出了同时支持白盒和黑盒可追踪的 CP-ABE. 2023 年, Guo 等 [20] 提出了可撤销的区块链辅助的 CP-ABE. 2024 年, Chen 等 [21] 提出了具有可验证数据完整性的可撤销 CP-ABE.

**SM9 标识加密.** 为实现信息技术的安全自主可控, 我国于 2008 年自主研发了 SM9 系列密码算法 [22], 并于 2021 年推动其成为国际标准 (ISO/IEC18033-5:2015/ADM1:2021), 标志着我国密码技术在国际标准化领域取得了重大突破. 随后, 文献 [23,24] 分别对 SM9 系列算法进行了安全性证明. 2021 年, Lai 等 [25] 在 SM9 标识加密的基础上, 构造了一种高效广播加密方案. 2022 年, Qin 等 [26] 构建了基于 SM9 可裁决的标识加密机制. 2023 年, Lai 等 [27] 提出了基于 SM9 的高效分层标识方案. 2024 年, Chen 等 [28] 提出了高效且 RCCA 安全的 SM9-IBE 变体. 同年, Li 等 [29] 提出了基于 SM9 的分层标识广播内积函数加密. 为了探索 SM9 在属性基加密领域的应用, 2019 年, Shi 等 [2] 提出了基于 SM9 的 CP-ABE 方案, 该方案首先将解密密钥中的属性转换成标识, 加密时将访问策略转换成集合形式, 然后使用基于 SM9 的分层标识加密方案对其进行加密. 因此, 该方案仅能实现最简单

的 AND 门数据访问控制. Ji 等 [3] 也于 2021 年提出了基于 SM9 的 CP-ABE 方案, 该方案是基于访问树结构构造的. Zhou 等 [30] 于 2023 年提出了基于 SM9 的属性基加密的区块链访问控制机制. Liu 等 [31] 于 2024 年提出了基于 SM9 的模糊标识加密系统. 同年, Liu 等 [32] 也提出了基于 SM9 的 KP-ABE 系统. 综上所述, 目前针对 SM9 密码体系的属性基加密研究在学术界尚未形成完整的研究体系, 其理论框架的构建与实践应用的探索仍存在明显不足, 难以充分满足国产信息系统对属性基加密技术日益增长的多样化需求.

### 1.4　组织机构

第 2 节重点梳理与研究工作相关的基础理论与技术支撑; 第 3 节构建基于 SM9 的密文策略属性基加密 (SM9-CP-ABE) 方案, 并证明其安全性; 第 4 节从理论分析与实验验证两个维度, 对所提方案进行性能评估与实现验证; 第 5 节总结全文研究成果并展望未来研究方向.

## 2　预备知识

### 2.1　双线性映射

设存在与安全参数 $\lambda$ 相关的大素数 $N$; $G_1, G_2$ 是以加法为运算的循环群, 其阶为 $N$; $G_T$ 是以乘法为运算的循环群, 其阶也为 $N$; $e: G_1 \times G_2 \to G_T$ 是双线性映射, 如果满足如下性质:

(1) 可计算性 (computability): 对任意 $P \in G_1, Q \in G_2$, $e(P,Q)$ 可以在多项式时间内计算得到;

(2) 双线性 (bilinearity): 对任意的 $P \in G_1, Q \in G_2$ 和 $a, b \in Z_N^*$, 满足 $e(aP, bQ) = e(P,Q)^{ab}$;

(3) 非退化性 (non-degeneracy): 存在 $P \in G_1, Q \in G_2$, 满足 $e(P,Q) \neq 1$.

则称五元组 $\mathrm{BP} = (G_1, G_2, G_T, e, N)$ 是双线性映射群.

### 2.2　困难问题

**定义1** ($(q,k)$-decisional bilinear Diffie-Hellman inverse ($(q,k)$-DBDHI) 数学问题 [33])　设存在双线性映射群 $\mathrm{BP} = (G_1, G_2, G_T, e, N)$, 选择 $P \in G_1, Q \in G_2$. 已知

$$I = \begin{pmatrix} c, & P, & bP & aP, & a^2P, & \ldots, & a^{k+1}P \\ Q, & bQ, & aQ, & a^2Q, & a^3Q, & \ldots, & a^qQ \end{pmatrix},$$

给定随机的群元素 $T \in G_T$, 判断是否有 $T = e(P,Q)^{\frac{b}{a+c}}$.

**定理1**　若所有算法 $\mathcal{B}$ 都不能以不可忽略的优势在多项式时间内解决 $(q,k)$-DBDHI 问题, 则称 $(q,k)$-DBDHI 假设成立. 其中算法 $\mathcal{B}$ 解决该问题的优势定义为

$$\mathrm{Adv}(\mathcal{B}) = \left| \Pr[\mathcal{B}(I, e(P,Q)^{\frac{b}{a+c}}) = 1] - \Pr[\mathcal{B}(I,T) = 1] \right|.$$

### 2.3　线性秘密共享方案 (LSSS)

线性秘密共享方案 (LSSS) 是一类数学性质良好的单调访问结构. 与访问树结构相比, 基于 LSSS 构造的 CP-ABE 方案在支持更加精准的多用户数据安全访问的同时更具灵活性和扩展性.

**定义2**　线性秘密共享方案 (LSSS) [34] $Z_N^*$ ($N$ 是大素数) 上的线性秘密共享方案 $\Pi$ 主要包含以下两个条件:

(1) 秘密值 $s \in Z_N$ 分配到属性集合 $U$ 中的每个属性上的秘密份额形成一个向量;

(2) $U$ 上任意访问策略 $A$, 都对应 $\Pi$ 上的一个秘密生成矩阵 $\boldsymbol{M}_{l\times n}$ 和映射 $\rho(i)$. 其中, 映射 $\rho(i)$ 将 $\boldsymbol{M}$ 中的第 $i$ ($i = 1, 2, \ldots, l$) 行映射到属性 $\rho(i)$ 上. 定义向量 $\boldsymbol{v} = (s, r_2, r_3, \ldots, r_n)$, 其中 $s \in Z_N$ 是被分享的秘密值, $r_2, r_3, \ldots, r_n \in Z_N$ 是用于隐藏 $s$ 的随机数, 则 $\boldsymbol{M} \cdot \boldsymbol{v} \in \boldsymbol{Z}_N^{l\times 1}$ 就是 $s$ 通过 $\Pi$ 所产生的 $l$ 个秘密份额所形成的向量, 其中分量 $\lambda_i = (\boldsymbol{M} \cdot \boldsymbol{v})_i, i \in [1, l]$ 对应属性 $\rho(i)$ 的秘密份额.

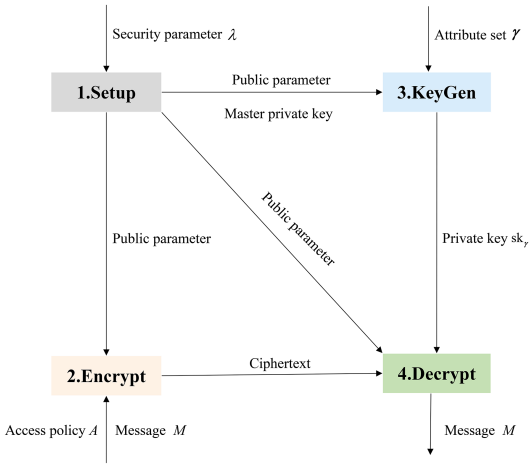


**图 2　(网络版彩图) CP-ABE 的工作流程图.**

**Figure 2**　(Color online) Workflow of CP-ABE.

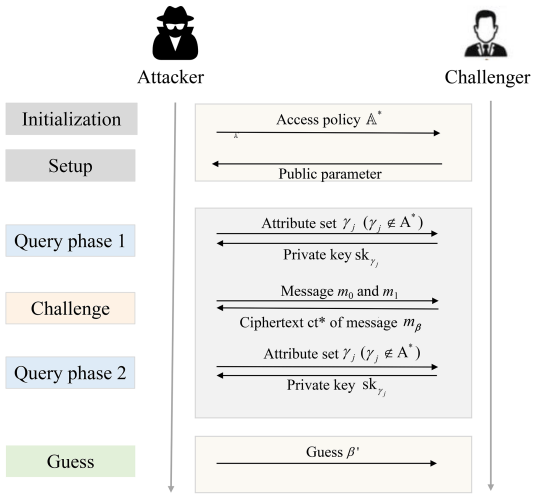


**图 3　(网络版彩图) CP-ABE 的安全模型.**

**Figure 3**　(Color online) Security model of CP-ABE.

线性秘密共享方案具有线性秘密重构的特性: 对任意的授权集合 $S \subset U$, 即 $S$ 满足访问策略 $A$, 定义 $I \subset \{1,2,\ldots,l\}$ 且 $I = \{i \in [l] \cap \rho(i) \in S\}$. 如果 $\{\lambda_i = (\boldsymbol{M} \cdot \boldsymbol{v})_i\}_{i\in I}$ 是 $s$ 通过 $\Pi$ 的有效秘密份额, 则存在一组常数集合 $\{\omega_i \in Z_N\}_{i\in I}$, 它们可以在多项式时间内被计算出来, 且满足 $\sum_{i\in I} \omega_i \cdot \lambda_i = s$. 对任意未授权集合 $S' \subset U$, 即 $S'$ 不满足访问策略 $A$, 则不存在多项式时间内被计算出来的 $\{\omega_i\}_{i\in I}$.

### 2.4　CP-ABE 的形式化定义和安全模型

CP-ABE 系统的核心架构通常由以下 4 个多项式时间算法构成 (如图 2).

- **Setup** $(\lambda) \to$ (mpk, msk). 系统建立阶段, 输入安全参数 $\lambda$, 生成系统的主私钥 msk 和公共参数 mpk.
- **Encrypt**(mpk, $m, A$) $\to$ ct. 加密阶段, 输入 mpk, 明文 $m$ 和访问策略 $A$, 生成与 $A$ 相关的密文 ct.
- **KeyGen** (mpk, msk,$\gamma$) $\to$ $\mathrm{sk}_\gamma$. 密钥生成阶段, 输入 mpk, msk 和属性集合 $\gamma$, 生成与该 $\gamma$ 相关的解密密钥 $\mathrm{sk}_\gamma$.
- **Decrypt**(mpk, $\mathrm{sk}_\gamma$, ct) $\to m$ 或者 $\perp$. 解密阶段, 输入 mpk, 与属性集合 $\gamma$ 相关的解密密钥 $\mathrm{sk}_\gamma$ 和与访问策略 $A$ 相关的密文 ct. 如果解密密钥中的属性集合 $\gamma$ 满足密文中嵌入的访问策略 $A$, 即 $\gamma \in A$, 则该算法恢复明文消息 $m$, 否则输出 $\perp$.

若对任意的安全参数 $\lambda$, 任意的 (mpk, msk)$\leftarrow$ **Setup**$(\lambda)$, 任意的属性集 $\gamma$ 和访问策略 $A$, 任意的明文 $m$, 当且仅当 $\gamma \in A$ 时, 下面的等式成立:

$$\textbf{Decrypt}\,(\mathrm{mpk}, \textbf{KeyGen}(\mathrm{mpk}, \mathrm{msk}, \gamma), \textbf{Encrypt}(\mathrm{mpk}, m, A)) \to m.$$

则称该 CP-ABE 算法是正确的.

CP-ABE 的选择策略安全模型定义如下: 设有挑战者 $C$ 和敌手 $\mathcal{A}$, 在进行如下交互游戏 (如图 3).

**初始化阶段.** 敌手 $\mathcal{A}$ 首先声明其意图挑战的目标访问策略 $A^*$.

**系统建立阶段.** $C$ 运行算法 **Setup** $(\lambda)$, 产生系统的公共参数 mpk 和主密钥 msk, 将 mpk 发送给 $\mathcal{A}$.

**询问阶段 1.** $\mathcal{A}$ 可以适应性地向 $C$ 发起解密密钥询问, 对每个查询的属性集合 $\gamma_j (\gamma_j \notin A^*)$, $C$ 运行 **KeyGen**(mpk, msk, $\gamma_j$) 算法, 将生成的解密密钥 $\mathrm{sk}_{\gamma_j}$ 发送给 $\mathcal{A}$.

**挑战阶段. 询问阶段 1** 结束后, $\mathcal{A}$ 提交两个等长消息 $m_0$ 和 $m_1$, $C$ 随机选择一个比特 $\beta \in \{0,1\}$, 运行 **Encrypt**(mpk, $m_\beta, A^*$) 算法, 生成挑战密文 $\mathrm{ct}^*$, 并将 $\mathrm{ct}^*$ 发送给 $\mathcal{A}$.

**询问阶段 2.** 重复**询问阶段 1**.

**猜测阶段.** $\mathcal{A}$ 输出一个比特 $\beta'$ 作为猜测结果. 若 $\beta'=\beta$, 则判断 $\mathcal{A}$ 在上述游戏中获胜, 定义获胜优势为 $\mathrm{Adv}_{\mathcal{A}}=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$.

**定义3** 若对于任意多项式时间的敌手 $\mathcal{A}$, 在上述游戏中获胜的优势均为可忽略函数, 则称该 CP-ABE 方案在选择访问策略和明文攻击下是 IND-SAP-CPA (indistinguishability against selective access policy, chosen plaintext attack) 安全的.

### 2.5 SM9 标识加密算法

SM9 标识加密算法是由中国国家密码管理局发布的商用密码标准 (GM/T00 44-2016 SM9), 其核心思想是通过用户唯一标识 (如邮箱、身份证号等) 直接生成系统主公钥, 消除传统公钥基础设施 (public key infrastructure, PKI) 中复杂的证书管理需求, 适用于大规模、跨域协作场景的安全通信与数据保护. SM9 标识加密是基于椭圆曲线建立的, 由以下 4 个多项式时间算法构成 [22].

**Setup** ($\lambda$). 该算法输入安全参数 $\lambda$, 双线性群 BP=$(G_1,G_2,G_T,e,N)$, 哈希函数 $H_1:\{0,1\}^*\to Z_N^*$, 一字节表示的私钥生成函数标识符 hid, 选择随机生成元 $P_1\in G_1,P_2\in G_2$ 和随机数 $\alpha\in Z_N$, 计算 $P_{\mathrm{pub}}=\alpha P_1$ 和 $g=e(P_{\mathrm{pub}},P_2)$. 输出公共参数 mpk=$\{\mathrm{BP},P_1,P_2,P_{\mathrm{pub}},g,H_1,\mathrm{hid}\}$ 和主密钥 msk=$\alpha$.

**KeyGen** (mpk, msk, ID). 该算法输入标识 ID, 公共参数 mpk 和主密钥 msk, 计算 $t_1=H_1(\mathrm{ID}||\mathrm{hid},N)+\alpha(\mathrm{mod}N)$. 若 $t_1=0$, 权威机构 KGC 更新主密钥 $\alpha\in Z_N$, 据此生成新的公共参数 $P_{\mathrm{pub}}$ 和 $g$, 并将其公开, 然后为现有用户重新计算解密密钥 sk. 否则, 计算 $t_2=\alpha t_1^{-1}$ 和 $\mathrm{sk}_{\mathrm{ID}}=t_2P_2=\frac{\alpha}{H_1(\mathrm{ID}||\mathrm{hid},N)+\alpha}P_2$.

**Encrypt** (mpk, $m$, ID). 该算法输入标识 ID, 明文消息 $m$ 和公共参数 mpk, 选择随机数 $s\in Z_N$, 并计算 $Q_{\mathrm{ID}}=H_1(\mathrm{ID}||\mathrm{hid},N)P_1+P_{\mathrm{pub}}$. 其次, 计算密文 ct=$(C_1=mg^s,C_2=sQ_{\mathrm{ID}})$.

**Decrypt** (mpk, ct, $\mathrm{sk}_{\mathrm{ID}}$). 该算法输入密文 ct 和解密密钥 $\mathrm{sk}_{\mathrm{ID}}$, 计算 $w=e(C_2,\mathrm{sk}_{\mathrm{ID}})$, 然后恢复明文消息 $m=C_1/w$.

## 3 基于 SM9 的 CP-ABE

### 3.1 方案描述

设 BP=$(G_1,G_2,G_T,e,N)$ 是双线性群, $H_1:\{0,1\}^*\to Z_N^*$ 是抗碰撞的哈希函数, hid 是一字节表示的私钥生成函数标识符. 为表述简单, 方案中使用 $H_1(N)$ 表示 $H_1(\mathrm{N}||\mathrm{hid})$.

**Setup** ($\lambda$). 该算法输入安全参数 $\lambda$, 首先选择生成元 $P_1\in G_1,P_2\in G_2$, 随机数 $\alpha\in Z_N^*$ 和随机群元素 $h_1,h_2,\ldots,h_{|U|}\in G_2$, 其对应系统中的 $|U|$ 个属性. 其次计算 $P_{\mathrm{pub}}=\alpha P_1,g=e(P_{\mathrm{pub}},P_2)$.

最后, 定义系统公共参数为 mpk=$\{P_1,P_2,P_{\mathrm{pub}},g,h_1,h_2,\ldots,h_{|U|}\}$, 主密钥为 msk=$\alpha$.

**Encrypt** (mpk, $m,A$). 该算法输入公共参数 mpk, 明文消息 $m\in G_T$ 以及与访问策略 $A$ 对应的访问控制矩阵和映射 $(\boldsymbol{M},\rho)$. 算法首先选择随机数 $s\in Z_N$, 构造向量 $\boldsymbol{v}=(s,y_2,y_3,\ldots,y_n)\in\boldsymbol{Z}_N^n$. 其次, 计算 $\lambda_i=\boldsymbol{v}\cdot\boldsymbol{M}_i(i\in[1,l])$, 其中 $\boldsymbol{M}_i$ 是矩阵 $\boldsymbol{M}$ 中第 $i$ 行元素组成的向量. 最后, 该算法随机选择 $r_1,r_2,\ldots,r_l\in Z_N$, 计算密文 ct=$(A,C,C',(C_i,D_i)_{i\in[1,l]})$, 其中

$$C=mg^s,C'=s(H_1(N)P_1+P_{\mathrm{pub}}),$$

$$\left(C_1=\lambda_1P_2-r_1h_{\rho(1)},D_1=r_1P_1\right),\ldots,\left(C_l=\lambda_lP_2-r_lh_{\rho(l)},D_l=r_lP_1\right).$$

**KeyGen** (mpk, msk, $S$). 该算法输入公共参数 mpk, 主密钥 msk 和属性集 $S$, 随机选择 $t\in Z_N^*$, 计算解密密钥 sk=$(K,L,(K_x)_{x\in S})$, 其中

$$K=\frac{\alpha}{H_1(N)+\alpha}P_2+tP_2,L=t(H_1(N)+\alpha)P_1,\forall x\in S,K_x=t(H_1(N)+\alpha)h_x.$$

**Decrypt** (mpk, sk, ct). 该算法输入嵌入属性集 $S$ 的解密密钥 $\mathrm{sk}=(K,L,(K_x)_{x\in S})$ 和包含访问策略 $A$ 的密文 $\mathrm{ct}=(A,C,C',(C_i,D_i)_{i\in[1,l]})$. 算法首先判断 $S$ 是否满足访问策略 $A$, 若不满足则输出 $\perp$; 否则, 定义 $I\subset\{1,2,\ldots,l\}$, 且 $I=\{i:\rho(i)\in S\}$. 令 $\{w_i\in Z_N|i\in I\}$ 是满足 $\sum_{i\in I}w_iW_i=(1,0,0,\ldots,0)$ 的常数集合. 该算法计算

$$
\begin{aligned}
&\frac{e(C',K)}{\prod\limits_{i\in I}(e(L,C_i)\cdot e(D_i,K_x))^{w_i}}\\
&=\frac{e(s(H_1(N)P_1+P_{\mathrm{pub}}),\frac{\alpha}{H_1(N)+\alpha}P_2+tP_2)}{\prod\limits_{i\in I}(e(t(H_1(N)+\alpha)P_1,\lambda_iP_2-r_ih_{\rho(i)})\cdot e(r_iP_1,t(H_1(N)+\alpha)h_x))^{w_i}}\\
&=\frac{e(P_1,P_2)^{\alpha s}\cdot e(s(H_1(N)+\alpha)P_1,tP_2)}{\prod\limits_{i\in I}e(t(H_1(N)+\alpha)P_1,\lambda_iP_2)^{w_i}}\\
&=\frac{e(P_1,P_2)^{\alpha s}\cdot e(s(H_1(N)+\alpha)P_1,tP_2)}{e((H_1(N)+\alpha)P_1,tP_2)^{\sum\limits_{i\in I}w_i\lambda_i}}\\
&=\frac{e(P_1,P_2)^{\alpha s}\cdot e(s(H_1(N)+\alpha)P_1,tP_2)}{e((H_1(N)+\alpha)P_1,tP_2)^{s}}\\
&=e(P_1,P_2)^{\alpha s}=g^s.
\end{aligned}
$$

最后, 该算法计算 $C/g^s$ 恢复消息 $m$.

### 3.2　安全性证明

**定理2**　若 ($q$, $k$ +1)-DBDHI 假设成立, 则上述方案是 IND-SAP-CPA 安全的.

**证明**　若存在多项式时间算法的敌手 $\mathcal{A}$, 以不可忽略的优势 $\epsilon$, 在 IND-SAP-CPA 安全游戏中获胜, 则可以构造模拟者 $\mathcal{B}$, 利用敌手 $\mathcal{A}$ 的能力解决 ($q$, $k$ + 1)-DBDHI 问题.

给定 ($q$, $k$ + 1)-DBDHI 问题实例

$$
I=\begin{pmatrix}c,\ \ P,\ \ bP\ \ \ aP,\ \ a^2P,\ \ldots,\ a^{k+2}P\\ Q,\ bQ,\ aQ,\ a^2Q,\ a^3Q,\ \ldots,\ \ \ a^qQ\end{pmatrix}
$$

和随机的群元素 $T\in G_T$, $\mathcal{B}$ 判断 $T=e(P,Q)^{\frac{b}{a+c}}$ 是否成立.

**系统建立阶段.** 敌手 $\mathcal{A}$ 首先声明其意图挑战的目标访问策略 $A^*$, 以及与之对应的矩阵和映射 $(\boldsymbol{M}^*,\rho^*)$, 其中 $\boldsymbol{M}^*$ 有 $l^*$ 行 $n^*$ 列. 模拟者 $\mathcal{B}$ 根据目标访问策略 $A^*$, 按照以下方式构建系统参数.

- 多项式构造. 从 $Z_N^*$ 中选择不同的随机数 $w_1,w_2,\ldots,w_q$, 生成多项式 $f(x)=\prod_{i=1}^q(x+w_i)=\sum_{i=0}^q c_ix^i \bmod N$. 其中, $w_1=H_1(N)=c$, 且 $f_1(x)=\prod_{i=2}^q(x+w_i)=\sum_{i=0}^{q-1}d_ix^i \bmod N$.
- 参数设置. 根据已知问题的实例计算群 $G_1$ 的生成元 $P_1=P$, 群 $G_2$ 的生成元 $P_2=f(a)Q$, 以及 $P_{\mathrm{pub}}=aP_1=aP$ 和 $g=e(P_{\mathrm{pub}},P_2)$, 注意 $a$ 未知. $\mathcal{B}$ 按照以下方式构造 $h_1,h_2,\ldots,h_{|U|}\in G_2$.

针对每个属性 $x$, 选择对应的随机数 $z_x\in Z_N^*$. 当挑战的访问策略 $A^*$ 中存在 $i\in[1,l]$, 使得 $\rho^*(i)=x$, 则令 $X$ 是所有使得 $\rho^*(i)=x$ 的指标 $i$ 的集合, 即 $X=\{i|\rho^*(i)=x\}$, 设置

$$
h_x=z_x\sum_{i\in X}\left(\frac{f(a)}{a+c}M_{i,1}^*Q+\frac{f(a)}{a+c}M_{i,2}^*Q+\cdots+\frac{f(a)}{a+c}M_{i,n^*}^*Q\right)=z_x\sum_{i\in X}\left(\sum_{j=1}^{n^*}\frac{f(a)}{a+c}M_{i,j}^*Q\right).
$$

当挑战的访问策略 $A^*$ 中不存在 $i\in[1,l]$, 使得 $\rho^*(i)=x$, 即 $X=\Phi$ 时, 设置 $h_x=z_x(aQ+cQ)$.

由于 $z_x\in Z_N^*$ 的随机性, 使得 $h_x$ 的设置也是随机的. 且 $\frac{f(a)}{a+c}Q=f_1(a)Q=\sum_{i=0}^{q-1}d_ia^iQ$ 可以通过问题实例计算得到.

最后模拟者 $\mathcal{B}$ 输出系统的公共参数 mpk=$\{P_1,P_2,P_{\mathrm{pub}},g,h_1,h_2,\ldots,h_{|U|}\}$, 主私钥 msk=$a$ 保密.

**询问阶段 1.** $\mathcal{A}$ 允许询问与属性集合 $S$ 相关的解密密钥, 其中 $S$ 不满足挑战访问策略 $A^*$.

$\mathcal{B}$ 随机选择 $t' \in Z_N^*$, 计算

$$\begin{aligned} K =& \sum_{i=0}^{q-1} d_i a^{i+1} Q + t' \sum_{i=0}^{q-1} d_i a^i Q \\ =& a f_1(a) Q + t' f_1(a) Q \\ =& \frac{a}{a+c} f(a) Q + \frac{t'}{a+c} f(a) Q \\ =& \frac{a}{a+c} P_2 + t P_2, \end{aligned}$$

$$L = t'P = \frac{t'}{a+c}(a+c)P = t(a+c)P_1,$$

其中, 隐含的有 $t = \frac{t'}{a+c}$.

$\forall x \in S$, 当 $A^*$ 中存在 $i \in [1, l]$, 使得 $\rho^*(i) = x$ 时, 计算

$$K_x = t' z_x \sum_{i \in X} \left( \sum_{j=1}^{n^*} \frac{f(a)}{a+c} M_{i,j}^* Q \right) = \frac{t'}{a+c}(a+c) z_x \sum_{i \in X} \left( \sum_{j=1}^{n^*} \frac{f(a)}{a+c} M_{i,j}^* Q \right) = t(a+c) h_x.$$

否则, 计算

$$K_x = t' z_x (aQ + cQ) = \frac{t'}{a+c} z_x (a+c)^2 Q = t(a+c) z_x (a+c) Q = t(a+c) h_x.$$

**挑战阶段.** 敌手 $\mathcal{A}$ 选择两个等长的消息 $m_0$ 和 $m_1$, 并将其发送给 $\mathcal{B}$. $\mathcal{B}$ 随机选择 $v \in \{0, 1\}$, 首先计算

$$\frac{x f(x)}{x+c} = f'(x) + \frac{E}{x+c},$$

其中 $f'(x)$ 是 $q$ 次多项式, $E \neq 0$ 且可求. 其次, 计算

$$C = m_v e(bP, f'(a) Q) T^E,$$

$$C' = bP.$$

最后, 选择随机数 $v_2, v_3, \ldots, v_n \in Z_N^*$, 隐含地设置向量 $\boldsymbol{v} = (\frac{b}{a+c}, v_2 + \frac{b}{a+c}, v_3 + \frac{b}{a+c}, \ldots, v_n + \frac{b}{a+c})$.

选择随机数 $r_i' \in Z_N$, 隐含的有 $r_i = r_i' + \frac{b}{z_x}$, 计算

$$\begin{aligned} \lambda_i = \boldsymbol{v} \cdot \boldsymbol{M}_i^* =& \left( \frac{b}{a+c}, v_2 + \frac{b}{a+c}, v_3 + \frac{b}{a+c}, \ldots, v_n + \frac{b}{a+c} \right) \cdot \left( M_{i,1}^*, M_{i,2}^*, \ldots, M_{i,n^*}^* \right) \\ =& \frac{b}{a+c} \sum_{j=1}^{n^*} M_{i,j}^* + \sum_{j=2}^{n^*} v_j \cdot M_{i,j}^*, \end{aligned}$$

$$C_i = \sum_{j=2}^{n^*} v_j M_{i,j}^* f(a) Q - r_i' h_x,$$

$$D_i = r_i' P + \frac{1}{z_x} bP.$$

设随机数 $s = \frac{b}{a+c}$, 则有关于消息 $m_v$ 的密文:

$$D_i = r_i' P + \frac{1}{z_x} bP = \left( r_i - \frac{b}{z_x} \right) P + \frac{1}{z_x} bP = r_i P = r_i P_1,$$

$$
\begin{aligned}
C_i &= \sum_{j=2}^{n^*} v_j M_{i,j}^* f(a) Q - r_i' h_x = \sum_{j=2}^{n^*} v_j M_{i,j}^* f(a) Q - \left(r_i - \frac{b}{z_x}\right) h_x \\
&= \sum_{j=2}^{n^*} v_j M_{i,j}^* f(a) Q - r_i h_{\rho(i)} + \frac{b}{z_x} h_x \\
&= \sum_{j=2}^{n^*} v_j M_{i,j}^* f(a) Q - r_i h_{\rho(i)} + \frac{b}{a+c} \sum_{j=1}^{n^*} M_{i,j}^* f(a) Q \\
&= \frac{b}{a+c} \sum_{j=1}^{n^*} M_{i,j}^* f(a) Q + \sum_{j=2}^{n^*} v_j M_{i,j}^* f(a) Q - r_i h_{\rho(i)} \\
&= \lambda_i P_2 - r_i h_{\rho(i)},
\end{aligned}
$$

$$
C' = bP = \frac{b}{a+c}(a+c)P = s(aP_1 + cP_1).
$$

如果 $T = e(P,Q)^{\frac{b}{a+c}}$, 则有

$$
\begin{aligned}
C &= m_v e(bP, f'(a)Q) T^E = m_v e(bP, f'(a)Q) e(P,Q)^{\frac{Eb}{a+c}} \\
&= m_v \left[e(P,Q)^{f'(a)+\frac{E}{a+c}}\right]^b = m_v \left[e(P,Q)^{\frac{af(a)}{a+c}}\right]^b \\
&= m_v \left[e(P_1, f(a)Q)^a\right]^{\frac{b}{a+c}} = m_v e(P_1, P_2)^{as} \\
&= m_v g^s.
\end{aligned}
$$

故该密文是在挑战访问策略 $A^*$ 下对消息 $M_v$ 加密的合法密文.

当 $T \neq e(P,Q)^{\frac{b}{a+c}}$ 时, 挑战密文 $C = m_v e(bP, f'(a)Q) T^E$ 并非消息 $m_v$ 的有效密文, 而是 $G_T$ 中的随机数, 故敌手 $\mathcal{A}$ 不能根据此密文推断出消息 $m_v$, 从而说明该密文没有泄露 $m_v$ 的任何信息.

**询问阶段 2.** 重复 "**询问阶段 1**".

**猜测阶段.** $\mathcal{A}$ 发送 $v$ 的猜测 $v'$, 当 $v' = v$ 时, $\mathcal{B}$ 判断 $T = e(P,Q)^{\frac{b}{a+c}}$, 当 $v' \neq v$ 时, $\mathcal{B}$ 判断 $T \neq e(P,Q)^{\frac{b}{a+c}}$.

计算 $\mathcal{B}$ 解决 $(q, k+1)$-DBDHI 问题的优势.

- 若 $T = e(P,Q)^{\frac{b}{a+c}}$, 则 $\mathcal{A}$ 至少可以以不可忽略的优势 $\epsilon$ 攻破上述方案. 即当 $\mathcal{A}$ 发送 $v' = v$ 时, $\mathcal{B}$ 判断 $T = e(P,Q)^{\frac{b}{a+c}}$ 的概率至少是 $\epsilon + \frac{1}{2}$.
- 否则, $\mathcal{A}$ 不知道 $m_v$ 的任何信息. 即当 $\mathcal{A}$ 发送 $v' \neq v$ 时, $\mathcal{B}$ 判断 $T = e(P,Q)^{\frac{b}{a+c}}$ 的概率是 $\frac{1}{2}$.

综上, $\mathcal{B}$ 解决 $(q, k+1)$-DBDHI 问题的优势至少是 $\frac{1}{2}(\frac{1}{2} + \epsilon) + \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} = \frac{1}{2}\epsilon$.

## 4　性能分析

### 4.1　理论分析

本小节针对所提方案进行理论上的性能评估, 定义以下关键参数: $|G_i|$ $(i = 1, 2, T)$ 表示群 $G_i$ $(i = 1, 2, T)$ 中元素的比特长度, $|U|$ 表示属性空间大小, $|S|$ 表示与解密密钥关联的属性集合大小, $l$ 表示线性秘密生成矩阵 $\boldsymbol{M}$ 的行数, $|I|$ 代表解密时使用的线性秘密生成矩阵 $\boldsymbol{M}$ 中的行数. 表 1 从通信开销角度对本文提出的方案与文献 [10] 中经典的 CP-ABE 方案以及文献 [3] 中基于 SM9 的 CP-ABE 方案进行比较. 结果显示, 与文献 [10] 相比, 本文方案的公共参数大小、私钥长度和密文长度分别与文献 [10] 中的公共参数大小、私钥长度和密文长度相当. 与文献 [3] 相比, 本文使用了更具表达力的线性秘密共享方案表示访问结构, 而且本文方案的密文长度相比文献 [3] 中的密文长度更短. 私钥长度相当, 公钥长度更长. 文献 [2] 中的方案构造并不属于严格意义上的属性基加密方案. 因此, 本文不做比较.

表 1　通信开销比较.

**Table 1**　Comparison of communication cost.

| Scheme | Size of params | Size of private key | Size of ciphertext | Access policy |
|---|---|---|---|---|
| SM9-CP-ABE | $2\|G_1\|+(\|U\|+1)\|G_2\|+\|G_T\|$ | $\|G_1\|+(\|S\|+1)\|G_2\|$ | $\|G_T\|+(1+l)\|G_1\|+l\|G_2\|$ | LSSS |
| [10] | $(\|U\|+2)\|G\|+\|G_T\|$ | $(\|S\|+2)\|G\|$ | $\|G_T\|+(1+2l)\|G\|$ | LSSS |
| [3] | $3\|G_1\|+\|G_2\|+\|G_T\|$ | $\|G_1\|+(\|S\|+1)\|G_2\|$ | $\|G_T\|+\|G_1\|+2l\|G_2\|$ | Access tress |

表 2　计算开销比较.

**Table 2**　Comparison of computational cost.

| Scheme | Cost of extract | Cost of encrypt | Cost of decrypt |
|---|---|---|---|
| SM9-CP-ABE | $T_{\mathrm{sm1}}+(\|S\|+2)T_{\mathrm{sm2}}$ | $T_e+(l+1)T_{\mathrm{sm1}}+2lT_{\mathrm{sm2}}$ | $(2\|I\|+1)T_p+\|I\|T_e+T_i$ |
| [10] | $(\|S\|+3)T_{\mathrm{sm1}}$ | $T_e+(3l+1)T_{\mathrm{sm1}}$ | $(2\|I\|+1)T_p+\|I\|T_e+T_i$ |
| [3] | $\|S\|T_{\mathrm{sm1}}+(2\|S\|+1)T_{\mathrm{sm2}}$ | $T_e+2T_{\mathrm{sm1}}+2lT_{\mathrm{sm2}}$ | $(2\|I\|+1)T_p+\|I\|T_e+T_i$ |

表 2 从计算代价角度对本文提出的方案与文献 [10] 中经典的 CP-ABE 方案以及文献 [3] 中基于 SM9 的 CP-ABE 方案进行比较. 其中, $T_{\mathrm{sm}i}$ $(i=1,2)$ 表示群 $G_i$ $(i=1,2)$ 中的乘法运算, $T_p$ 表示配对运算, $T_i, T_e$ 分别表示群 $G_T$ 中的逆运算和指数运算. 比较显示, 与文献 [10] 相比, 本文提出方案的密钥生成时间、加密时间和解密时间均与之相当. 与文献 [3] 相比, 本文方案的密钥生成时间更短, 加密时间更长, 解密时间相当. 同样, 本文与文献 [2] 不做比较.

### 4.2　实验分析

本小节在 256 比特安全强度下对所提方案与文献 [3] 中的方案开展效率对比研究. 实验采用的 R-ate 双线性配对运算和 BN 曲线均与 SM9 标识加密相同, 其中, $|G_1|=256$ 比特, $|G_2|=512$ 比特, 嵌入次数 $k=12$. 使用的设备是一台笔记本电脑 (Intel$^R$ Core$^{\mathrm{TM}}$ i5, Windows 10 操作系统, 16.0 GB 内存), 使用的编程软件是 C++, 使用的密码学库是 Miracl. 为模拟实际应用场景中的最坏情况, 实验采用 "$'S_1'$ AND $'S_2'$ AND $\cdots$ AND $'S_n'$" 作为加密时使用的访问策略, 其中 $S_i$ 表示属性. 为确保测试数据的准确性和适用性, 实验设置 $n=10$, 20, 30, 40, 50 等 5 个梯度属性规模的访问控制结构. 每个访问结构关联 10 组随机化属性配置, 最终获得 50 组异构访问策略样本空间. 对于每种情况, 实验均执行 30 次重复测试, 并计算这 30 次测试结果的平均值. 图 4 通过实验数据对比了本文方案与文献 [3] 中各子算法的运行时间. 结果显示, 与文献 [3] 相比, 由于本文方案在系统建立阶段需要选取 $|U|$ 个群 $G_2$ 中的元素, 故系统建立阶段的时间与访问策略数量即属性数量成正比. 另外本文方案在加密阶段多了 $l$ 个群 $G_1$ 中的乘法运算, 故加密开销较大. 解密算法一样, 故解密时间相当. 由于本文方案在密钥生成阶段减少了大约 $|S|$ 个群 $G_1$ 上的乘法运算和 $|S|$ 个群 $G_2$ 上的乘法运算, 故密钥生成时间更短, 可以将密钥生成时间至少缩短 27%, 而且随着属性数量的增加, 缩短的比例将更大. 此外本文方案使用了数学性质良好的线性秘密共享方案表示访问结构, 具有很强的扩展性, 可以通过算法优化实现快速解密等性能提升和功能扩展. 实验结果与理论分析相吻合.

## 5　总结与展望

针对现有基于 SM9 的密文策略属性基加密方案尚不能满足国产信息系统对多用户数据的安全灵活共享需求, 本文利用线性秘密共享方案提出了一种基于 SM9 的 CP-ABE 方案, 并证明方案在 $(q, k+1)$-DBDHI 安全假设下具有 IND-SAP-CPA 安全性. 理论分析和实验结果表明, 与国外经典的属性基加密方案以及现有基于 SM9 的属性基加密方案相比, 本文提出的方案具有相当的通信代价和计算开销. 另外, 本文采用数学性质良好的线性秘密共享方案表示访问控制策略, 其更具灵活性和扩展性, 可为后续基于 SM9 的多功能属性基加密研究奠定基础. 因此, 本研究未来的工作将围绕基于 SM9 的 CP-ABE 方案的性能优化与功能拓展展开. 例如, 在该方案的

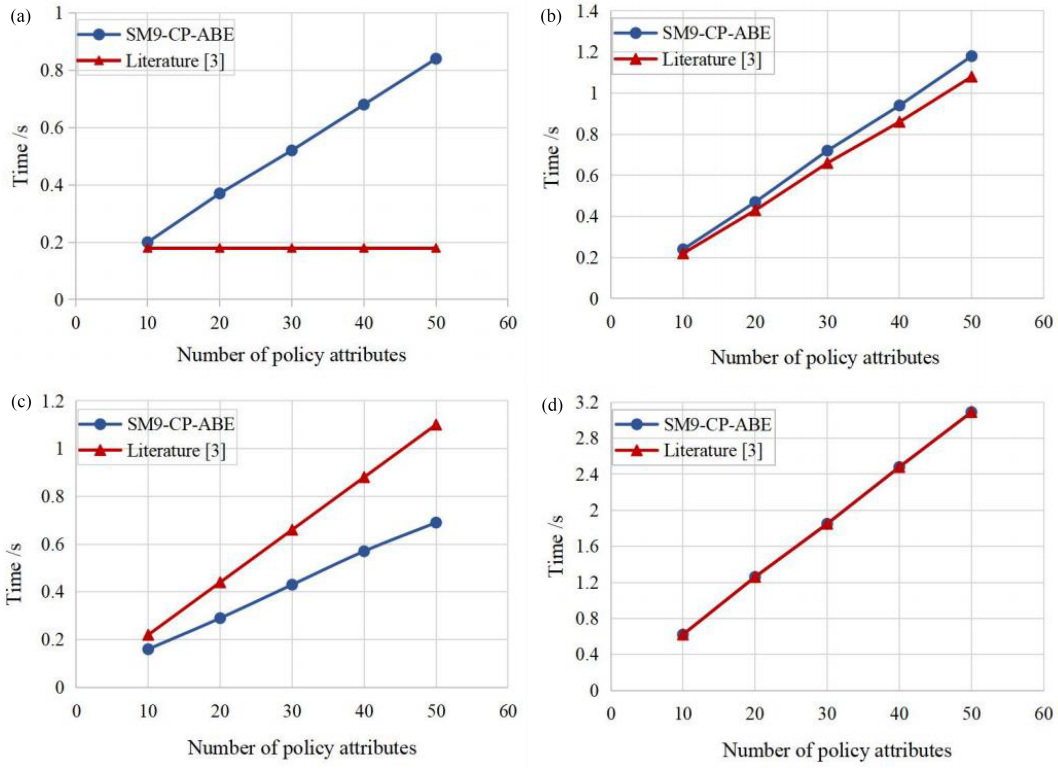


**图 4　(网络版彩图) 运行时间比较. (a) Setup; (b) Encrypt; (c) KeyGen; (d) Decrypt.**

**Figure 4**　(Color online) Comparison of running time. (a) Setup; (b) Encrypt; (c) KeyGen; (d) Decrypt.

基础上, 进一步缩短方案的加密时间和解密时间, 研究支持大属性域、密钥可追踪性和可撤销性等功能的基于 SM9 的 CP-ABE 方案, 进一步推动属性基加密技术在国产信息系统中的广泛应用与发展.

## 参考文献


1　国家密码管理局. 我国 SM9 标识加密算法正式成为 ISO/IEC 国际标准. 2021. https://www.sca.gov.cn/sca/xwdt/2021-03/01/content_1060851.shtml

2　Shi Y, Ma Z Y, Qin R F, et al. Implementation of an attribute-based encryption scheme based on SM9. Appl Sci, 2019, 9: 3074–3093

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

4　Shamir A. Identity-based cryptosystems and signature schemes. In: Proceedings of the 3th International Conference on the Theory and Application of Cryptographic Techniques, 1985. 47–53

5　Sahai A, Waters B. Fuzzy identity-based encryption. In: Proceedings of the 24th International Conference on the Theory and Application of Cryptographic Techniques, 2005. 457–473

6　Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006. 89–98

7　Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE Symposium on Security and Privacy (SP'07), 2007. 321–334

8　Cheung L, Newport C. Provably secure ciphertext policy ABE. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, 2007. 456–465

9　Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Proceedings of the 29th International Conference on the Theory and Application of Cryptographic Techniques, 2010. 62–91

10　Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography, 2011. 53–70

11 Liu Z, Cao Z F, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Trans Inform Forensic Secur, 2013, 8: 76–88

12 Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2013. 463–474

13 Liu Z, Cao Z F, Wong D S. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2013. 475–486

14 Ning J T, Cao Z F, Dong X L, et al. Traceable CP-ABE with short ciphertexts: how to catch people selling decryption devices on ebay efficiently. In: Proceedings of the European Symposium on Research in Computer Security, 2016. 551–569

15 Jiang Y H, Susilo W, Mu Y, et al. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. Future Generation Comput Syst, 2018, 78: 720–729

16 Ning J T, Cao Z F, Dong X L, et al. Auditable $\sigma$-time outsourced attribute-based encryption for access control in cloud computing. IEEE Trans Inform Forensic Secur, 2017, 13: 94–105

17 Liu Z H, Duan S H, Zhou P L, et al. Traceable-then-revocable ciphertext-policy attribute-based encryption scheme. Future Generation Comput Syst, 2019, 93: 903–913

18 Xu S M, Yuan J M, Xu G W, et al. Efficient ciphertext-policy attribute-based encryption with blackbox traceability. Inf Sci, 2020, 538: 19–38

19 Ning J T, Huang X Y, Wei L F, et al. An attribute-based cloud data sharing scheme supporting malicious user tracing. Chinese J Comput, 2022, 45: 1431–1445 [宁建廷, 黄欣沂, 魏立斐, 等. 支持恶意用户追踪的属性基云数据共享方案. 计算机学报, 2022, 45: 1431–1445]

20 Guo Y Y, Lu Z H, Ge H, et al. Revocable blockchain-aided attribute-based encryption with escrow-free in cloud storage. IEEE Trans Comput, 2023, 72: 1901–1912

21 Chen S B, Li J G, Zhang Y C, et al. Efficient revocable attribute-based encryption with verifiable data integrity. IEEE Int Things J, 2023, 11: 10441–10451

22 Cheng Z H. The SM9 cryptographic schemes. Cryptology ePrint Archive, 2017. https://eprint.iacr.org/2017/117.pdf

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

24 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]

25 Lai J C, Huang X Y, He D B, et al. 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, 等. 一种基于商密 SM9 的高效标识广播加密方案. 计算机学报, 2021, 44: 897–907]

26 Qin B D, Zhang B X, Bai X, et al. 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]

27 Lai J C, Huang X Y, He D B, et al. 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]

28 Chen R M, Chen J R, Huang X Y, et al. RCCA-SM9: securing SM9 on corrupted machines. Sci China Inf Sci, 2024, 67: 212103

29 Li C, Liang J K, Ding Y J, et al. Hierarchical identity-based broadcast inner product functional encryption based on SM9. Sci Sin Inform, 2024, 54: 1400–1418 [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]

30 Zhou Q, Chen M H, Wei K J, et al. A blockchain access control scheme based on SM9 attribute-based encryption. Netinfo Secur, 2023, 23: 37–46 [周权, 陈民辉, 卫凯俊, 等. 基于 SM9 的属性加密的区块链访问控制方案. 信息网络安全, 2023, 23: 37–46]

31 Liu X H, Huang X Y, Cheng Z H, et al. Fault-tolerant identity-based encryption from SM9. Sci China Inf Sci, 2024, 67: 122101

32 Liu X H, Huang X Y, Cheng Z H, et al. Key-policy attribute-based encryption based on SM9 and its fast decryption. Chinese J Comput, 2024, 47: 971–986 [刘晓红, 黄欣沂, 程朝辉, 等. 基于 SM9 的密钥策略属性基加密及快速解密. 计算机学报, 2024, 47: 971–986]

33 Chen L Q, Cheng Z H. Security proof of sakai-kasahara's identity-based encryption scheme. In: Proceedings of IMA International Conference on Cryptography and Coding, 2005. 442–459

34 Beimel A. Secure schemes for secret sharing and key distribution. Dissertation for Ph.D. Degree. Haifa: Technion-Israel Institute of Technology, 1996

# Ciphertext-policy attribute-based encryption based on SM9

Xiaohong LIU[1], Chao LIN[2*], Wei WU[3] & Xinyi HUANG[4]

1. *Maths and Information Technology School, Yuncheng University, Yuncheng 044000, China*
2. *College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China*
3. *College of Education Sciences, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 511455, China*
4. *College of Cyber Security, Jinan University, Guangzhou 510632, China*

* Corresponding author. E-mail: chaolin@nuaa.edu.cn

**Abstract** Ciphertext-policy attribute-based encryption (CP-ABE), as a critical branch of attribute-based encryption, achieves fine-grained access control over data by designing access policies during encryption. Compared with traditional identity-based encryption, CP-ABE supports a dynamic "one-to-many" encryption paradigm, making it particularly suitable for precise secure access control in multi-user collaborative scenarios. Currently, this technology has been widely adopted in next-generation information technology domains such as cloud computing, IoT, and blockchain. SM9 identity-based encryption, a commercial identity-based cryptographic algorithm independently designed in China, has become both a national and international standard. However, existing SM9-derived attribute-based encryption schemes remain limited and insufficient to meet the demand for flexible and secure multi-user data sharing in domestic information systems. On the basis of SM9, this paper proposes a ciphertext-policy attribute-based encryption scheme based on SM9, combined with the construction idea of classical ciphertext-policy attribute-based encryption. It is proved that the scheme has chosen-plaintext attack security under the assumption of $(q, k+1)$-decisional bilinear Diffie-Hellman inversion (DBDHI) and can achieve chosen-ciphertext attack security through FO conversion technology. Theoretical analysis and experimental results indicate that the proposed scheme achieves comparable communication overhead and computational costs to classical international CP-ABE schemes. Compared with the access tree used in existing CP-ABE schemes based on SM9, the scheme proposed in this paper adopts a mathematically sound linear secret sharing scheme (LSSS) to represent the access policy, which has good scalability and security. Moreover, the scheme can reduce the time required in the key generation stage by at least 27%. Therefore, this scheme can facilitate the application of attribute-based encryption in domestic information systems.

**Keywords** ciphertext policy, attribute-based encryption, linear secret sharing scheme, SM9