

基于 SM9 的公钥可搜索加密方案

蒲浪¹, 林超¹, 伍玮², 何德彪³

¹ 福建师范大学 计算机与网络空间安全学院 福州 中国 350117

² 福建师范大学 数学与统计学院 福州 中国 350117

³ 武汉大学 国家网络安全学院 武汉 中国 430072

摘要 云存储技术因其使用便捷、性价比高等优势得以迅速发展,越来越多用户将个人数据外包至第三方云服务器存储。虽然数据加密存储可有效保护数据安全和用户隐私,但传统的对称/非对称加密技术会影响数据检索和使用。可搜索加密是一种特殊的加密技术,一经提出便备受关注,在保障数据机密性的同时可提供数据检索功能。目前,国内外学者提出了大量可搜索加密方案,但现有方案都基于国外密码算法设计,尚未见基于国产商用密码算法的可搜索加密方案在国内外刊物上公开发表,不符合我国密码核心技术自主可控的要求。为了丰富国产商用密码算法在可搜索加密方面的研究,满足云存储领域的数据安全检索需求,本文以 SM9 标识加密算法为基础,构造了一种公钥可搜索加密方案 (SM9-PEKS)。在 q -ABDHE 安全假设和随机谕言模型下,本文首先证明 SM9 标识加密算法的匿名性,进而证明 SM9-PEKS 方案的安全性。理论分析和编程实现结果表明,与常用经典的公钥可搜索加密方案相比,本文方案在增加 64 字节通信代价的情况下,可至少降低 31.31% 的计算开销。最后,提出了未来可能的研究方向。

关键词 SM9 算法; 公钥可搜索加密; 标识密码; 匿名性

中图分类号 TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2023.01.08

A Public-key Encryption with Keyword Search Scheme from SM9

PU Lang¹, LIN Chao¹, WU Wei², HE Debiao³

¹ College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China

² School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China

³ School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Abstract Cloud storage technology has developed rapidly due to its flexible use and high cost performance, more and more users outsource their personal data to third-party cloud servers in order to save local storage resources and use data more conveniently. A large number of security risks appear while storing data, the data that usually need to be encrypted then stored to effectively protect data security and user privacy, but traditional symmetric/asymmetric encryption technology affects data efficient retrieval and use. Searchable encryption is a special cryptographic technology that not only guarantees data confidentiality but also provides convenient and secure data retrieval service. Searchable encryption has attracted widespread attention of scholars as soon as it was proposed. At present, domestic and foreign scholars have proposed a large number of searchable encryption schemes, but the existing schemes are based on foreign cryptographic algorithms. After our extensive research, there is no searchable encryption schemes based on domestic commercial cryptography algorithm has been published in domestic and foreign academic journals, which does not meet the requirements of security and independent control of cryptography core technology. In order to enrich the research of domestic commercial cryptographic algorithms in searchable encryption, and meet the security retrieval needs of data stored in the cloud servers, this article firstly adapts the SM9 identity-based encryption algorithm to construct a public key searchable encryption scheme (SM9-PEKS). Then, we prove the anonymity of SM9 identity-based encryption algorithm in the random oracle model based on the security assumption of q -ABDHE, followed by the security of the proposed SM9-PEKS. Theoretical analysis and programming implementation results show that, this scheme has a good balance between safety and efficiency. Compared with the classic commonly used PEKS schemes, the SM9-PEKS can reduce the computational overhead by at least 31.31% under extra communication cost of 64 bytes. Finally, the possible future research directions are proposed.

Key words SM9 algorithm; public key encryption with keyword search; identity-based cryptography; anonymity

通讯作者: 林超, 博士, 讲师, Email: linchao91@fjnu.edu.cn.

本课题得到国家自然科学基金(No. 62102089, No. 62032005, No. 61872089, No. 61972294), 中央高校基本科研业务费专项资金(No. 2042021kf1030), 湖北省自然科学基金 (No. 2017CFA007), 福建省自然科学基金(No. 2020J02016)资助。

收稿日期: 2021-10-04; 修改日期: 2021-12-08; 定稿日期: 2022-11-08

1 引言

伴随云存储市场规模的持续扩大, 越来越多用户将数据存储在云端。用户使用云端数据更灵活便捷, 同时可降低本地存储和计算开销, 但也意味着用户失去数据的监管权, 存在隐私泄露风险。为保障数据安全和用户隐私, 安全云存储系统中数据常以密文形式存储在云端服务器^[1-3]。然而, 传统的对称/非对称加密技术增加了数据检索和使用的难度。虽然用户可从服务器端下载全部密文至本地, 先解密再检索, 但易造成网络拥塞并占用大量本地计算和存储资源^[4]。为避免上述问题, 用户可直接将密钥发送给服务器, 由服务器进行解密后检索。但这种方式面临密钥传输易泄露、数据机密性难保障等新问题^[5]。2000 年, Song 等^[6]提出了可搜索加密(Searchable Encryption, SE)的概念。SE 是一种特殊的加密技术, 提供数据检索服务的同时保障数据安全, 有助于解决上述云存储面临的数据检索困难、隐私泄露等问题, 推动云存储的应用与推广^[7-8]。

SE 分为对称可搜索加密(Symmetric Searchable Encryption, SSE)和公钥可搜索加密(Public-key Encryption with Keyword Search, PEKS)两类, 本文重点研究 PEKS。Boneh 等^[9]2004 年提出 PEKS 的概念和首个 PEKS 方案后, 国内外学者围绕 PEKS 搜索模式(模糊搜索^[10-11]、多关键词搜索^[12-13]、布尔搜索^[14]等)和安全性(增强安全模型^[15-16]、抗外部关键词猜测攻击^[17-20]、抗内部关键词猜测攻击^[21-22]、抗文件注入攻击^[21-23]等)展开大量研究。然而, 这些 PEKS 方案都是基于国外密码算法设计, 目前未见基于国产商用密码算法的可搜索加密方案在国内外刊物上公开发表。为丰富国产商用密码算法在可搜索加密方面的研究, 满足云存储领域的安全检索需求, 促进国内云存储服务的快速发展, 亟需研究基于国产商用密码算法的 PEKS, 保障数据安全与高效检索, 满足国产密码核心技术自主、安全可控的需求。

1.1 本文贡献

本文利用 Abdalla 等^[24]在 2005 年美密会上提出的 new-ibe-2-peks 方法, 基于 SM9 标识加密算法, 提出公钥可搜索加密方案 SM9-PEKS。SM9-PEKS 方案的安全性要求 SM9 标识加密算法同时满足

IBE-IND-CPA 安全和 IBE-ANO-CPA 安全。国内学者已经证得 SM9 标识加密算法的 IBE-IND-CPA 安全^[25], 但尚未有 IBE-ANO-CPA 安全的相关证明在国内外刊物上公开发表。本文先在 q -ABDHE 安全假设下证得 SM9 标识加密算法满足 IBE-ANO-CPA 安全, 再结合文献[24]的定理证得 SM9-PEKS 满足 PEKS-IND-CPA 安全。最后性能分析与对比表明, 与经典 PEKS 方案^[9,16,21]相比, 本文 SM9-PEKS 方案在增加 64 字节通信代价的情况下, 至少降低 31.31% 的计算开销。

1.2 相关工作

本节从搜索模式和安全性方面回顾 PEKS 的研究进展。

搜索模式: 2004 年, Boneh 等^[9]提出首个支持单关键词搜索的 PEKS。为提高加密文件定位的精度, Park 等^[26]提出支持连接关键词查询的 PEKS 方案, 并在随机谕言模型下证明其安全性。2007 年, Boneh 等^[27]提出了支持加密数据连接、交集和范围查询的方案。2010 年, Wang 等^[28-29]针对存储在云端服务器的数据, 首次提出支持单关键词的排序 PEKS 方案。2012 年, Xu 等^[10]提出支持模糊关键词查询的 PEKS 方案, 该方案中关键词对应精确关键词搜索陷门和模糊关键词搜索陷门, 多个关键词共用同一个模糊关键词陷门, 搜索时只需发送模糊关键词陷门给第三方服务器, 可保障关键词隐私; Hu 等^[12]提出支持多关键词搜索的 PEKS 方案。2013 年, Cao 等^[30]提出支持多关键词的排序 PEKS 方案。2014 年, Zheng 等^[31]提出基于用户属性检索的 PEKS 方案。2019 年, Zeng 等^[14]提出云环境下支持布尔查询的 PEKS 方案。

安全性: 2006 年, Byun 等^[20]提出抗外部离线关键词猜测攻击(Resist External Keyword Guessing Attack, REKGA)的概念, 并对文献[9,26]中方案进行外部离线关键词猜测攻击。2008 年, Baek 等^[15]提出的 PEKS 方案传输关键词陷门时无需建立安全信道, 并在随机谕言模型下证得方案安全性。然而, 随机谕言模型下安全不能保证真实世界安全。2009 年, Fang 等^[32]提出了既不需要随机谕言机, 也不需要安全信道的 PEKS 方案; Rhee 等^[16]增强了 Baek 方案中的安全模型, 允许攻击者获得除挑战关键词外的陷门与

密文间的关系; Tang 等^[17]提出抗外部关键词猜测攻击的 PEKS 方案; Jeong 等^[33]指出, 关键词数量较小时, 满足一致性的 PEKS 方案无法抵抗关键词猜测攻击。2013 年, Yau 等^[34]提出在线关键词猜测攻击 (Online Keyword Guessing Attack, OKGA) 的概念, 外部敌手监听服务端和用户间的通信, 可获取陷门包含关键词内容。2017 年, Huang 等^[21]提出抗内部关键词猜测攻击的 PEKS 方案, 可解决诚实但好奇服务端引起的隐私泄露问题。2018 年, Wu 等^[22]提出既可抗文件注入攻击又可抗内部关键词猜测攻击的 PEKS 方案。

综上所述, 国内外学者在丰富和增强 PEKS 的搜索模式 and 安全性方面取得了大量的研究成果, 但目前未见基于国产商用密码算法的 PEKS 方案在国内外刊物上公开发表。根据 Abdalla 等^[24]在 2005 年美密会上提出的 new-ibe-2-peks 方法, 可将标识加密算法转换为 PEKS。因此, 本文主要关注 SM9 标识密码算法到 PEKS 方案的转换设计。国内学者在 SM9 功能型密码扩展设计方面已取得一系列研究成果, 包括标识广播加密^[35]、属性基加密^[36]、标识签密^[37]、匿名分布式密钥分发^[38]等, 这些成果为 SM9 到 PEKS 的转换设计提供了有益借鉴。

1.3 本文结构

第 2 节简要回顾本文涉及的双线性对群、相关安全假设、SM9 标识密码算法、公钥可搜索加密等预备知识; 第 3 节介绍基于 SM9 标识加密算法的公钥可搜索加密方案 (SM9-PEKS) 的具体构造和一致性分析; 第 4 节先证明 SM9 标识加密算法的匿名性, 再证明 SM9-PEKS 的安全性; 第 5 节对 SM9-PEKS 方案和现有经典 PEKS 方案进行性能分析对比和编程实现; 第 6 节总结了本文的工作。

2 预备知识

本节简要回顾双线性对群 (Bilinear Pairing Group)、SM9 标识密码、公钥可搜索加密等预备知识。

2.1 双线性对群

设 λ 为系统安全参数, N 是长度与 λ 相关的大素数。 \mathbb{G}_1 、 \mathbb{G}_2 和 \mathbb{G}_T 均是 N 阶循环群, 双线性映射 $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ 满足下列 3 个性:

1) 双线性: 对任意 $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2$ 和 $a, b \in \mathbb{Z}_p$, 等式 $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$ 成立;

2) 非退化: 存在 $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2$, 满足 $e(P_1, P_2) \neq 1$;

3) 可计算: 对于任意的 $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2$, 存在概率多项式时间 (Probabilistic Polynomial-time, PPT) 算法能够高效计算 $e(P_1, P_2)$ 。

双线性对群 $\mathcal{BP} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N)$ 。若 $\mathbb{G}_1 = \mathbb{G}_2$, 则称为对称双线性对群, 否则为非对称双线性对群。

2.2 安全假设

定义 1. (Decisional q -Augmented Bilinear Diffie-Hellman Exponent (判定 q -ABDHE) 问题^[40]) 已知 $(P', P, \alpha P, \dots, \alpha^{2q} P, Z)$, $P' \in \mathbb{G}_1, P \in \mathbb{G}_2, Z \in \mathbb{G}_T$, 判断 $Z = e(P', \alpha^{2q+1} P)$ 或 $Z = g_r$, 其中 g_r 是 \mathbb{G}_T 中的随机元素。

定义 PPT 算法 \mathcal{D} 成功解决判定 q -ABDHE 问题的优势为:

$$\text{Adv}(\lambda) = |\Pr[\mathcal{D}(P', P, \alpha P, \dots, \alpha^{2q} P, e(P', \alpha^{2q+1} P)) = 1] - \Pr[\mathcal{D}(P', P, \alpha P, \dots, \alpha^{2q} P, g_r) = 1]|.$$

判定 q -ABDHE 安全假设: 对任意 PPT 算法 \mathcal{D} , 成功解决判定 q -ABDHE 问题的优势 $\text{Adv}(\lambda)$ 可忽略。

2.3 SM9 标识密码

标识密码 (Identity-based Cryptography, IBC) 因避免了繁琐的数字证书管理, 在物联网等轻量级领域具有广泛的应用前景。我国政府十分重视标识密码算法的发展和应用, 从国家标准层面大力支持标识密码体系建设。SM9 标识密码算法是我国自主研发的第一个标识密码算法, 其发展历程如图 1 所示。

SM9 标识密码算法是基于有限域椭圆曲线上双线性对构造的密码算法, 包括数字签名、密钥交换协议、密钥封装协议以及标识加密算法四个部分。其中, SM9 标识加密方案包括以下四个多项式算法:

Setup. 算法输入安全参数 λ , 密钥生成中心 (Key generation Center, KGC) 选取双线性对群 $\mathcal{BP} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N)$, 其中 $N > 2^\lambda$, e 为双线性对 $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ 。然后随机选取群 \mathbb{G}_1 和群 \mathbb{G}_2 的生成元 P_1 和 P_2 , 哈希函数 $H_1: \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$, 密钥派生函

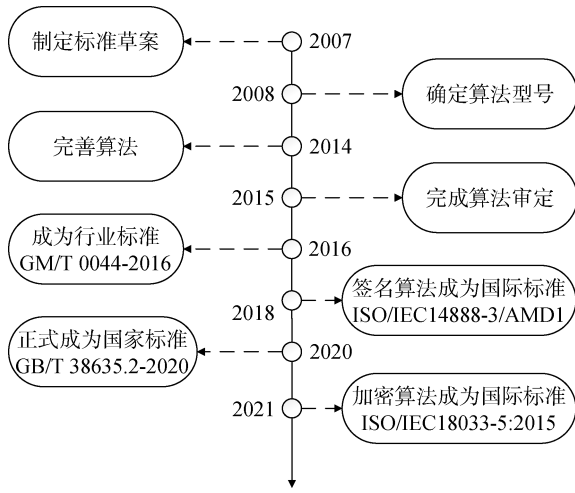


图 1 SM9 算法发展历程

Figure 1 The development history of SM9 algorithm

数 KDF , 消息认证码函数 MAC , 私钥生成函数识别符 hid 。随机选取 $s \in [1, N-1]$, 计算 $P_{pub} = [s]P_1$ 和 $g = e(P_{pub}, P_2)$ 。输出公开参数 $pp = (\mathcal{BP}, g, P_1, P_2, H_1, P_{pub}, KDF, MAC, hid)$ 、主公钥 $mpk = P_{pub}$ 和主私钥 $msk = s$ 。

Ext. 算法输入用户标识 $ID \in \{0,1\}^*$, 主私钥 msk 。首先计算 $t_1 = H_1(ID \parallel hid, N) + s \pmod{N}$, 若 $t_1 = 0$, 则重新产生并公开主公钥, 同时更新已有用户的私钥; 否则计算 $t_2 = s \cdot t_1^{-1}$, 输出用户私钥 $sk_{ID} = [t_2]P_2$ 。

Encrypt. 算法输入用户标识 $ID \in \{0,1\}^*$ 、明文 m 和系统主公钥 mpk 。随机选取 $r \in [1, N-1]$, 计算 $Q_{ID} = [H_1(ID \parallel hid, N)]P_1 + P_{pub}$, $C_1 = [r]Q_{ID}$, $u = g^r$, $K = KDF(C_1 \parallel u \parallel ID, klen) = (K_1, K_2)$, $C_2 = K_1 \oplus m$, $C_3 = MAC(K_2, C_2)$, 输出 m 的密文 $C = (C_1, C_3, C_2)$ 。

Decrypt. 算法输入用户标识 ID 、密文 C 和用户私钥 sk_{ID} , 计算 $ID, u' = e(C_1, sk_{ID}), K' = KDF(C_1 \parallel u' \parallel klen) = (K'_1, K'_2), m = C_2 \oplus K'_1, C'_3 = MAC(K'_2, C_2)$ 。若 $C'_3 = C_3$, 输出明文 m , 否则输出 \perp 。

定义 2. (IBE-IND-CPA) 已知系统安全参数 λ 和 $IBE = (Setup, Ext, Encrypt, Decrypt)$, \mathcal{PPT} 攻击者 \mathcal{A} 与挑战者进行 IBE-IND-CPA 游戏。如果 \mathcal{A} 在游戏中获胜的优势 $\text{Adv}_{\mathcal{A}}^{\text{IBE-IND-CPA}}(\lambda)$ 是可忽略的, 则该标

识加密方案在选择明文攻击下是不可区分的。

IBE-IND-CPA 游戏过程如下:

系统建立阶段. 挑战者使用安全参数 λ , 运行 $Setup(\lambda)$ 算法生成系统主公私钥对 (mpk, msk) , 并发送 mpk 给攻击者。

询问阶段 1. 在此阶段, 攻击者可以适应性地向挑战者询问任意标识 $id \in \{0,1\}^*$ 对应的私钥 usk_{id} 。

挑战阶段. 攻击者结束询问后, 发送两个长度相等的挑战明文 m_0^*, m_1^* 及挑战标识 id^* 给挑战者, 要求攻击者没有询问过挑战标识对应的私钥 usk_{id^*} 。挑战者随机选取 $b \in \{0,1\}$, 并运行标识加密算法 $Encrypt(id^*, mpk, m_b^*)$ 生成挑战密文 C 发送给攻击者。

询问阶段 2. 在此阶段, 攻击者可以继续适应性地向挑战者询问除挑战标识外任意标识 $id \in \{0,1\}^*$ 对应的私钥 usk_{id} 。

猜测阶段. 最终, 攻击者输出 $b' \in \{0,1\}$ 作为对 b 的猜测。若 $b' = b$, 则攻击者在上述游戏中获胜。

定义攻击者 \mathcal{A} 在上述游戏中获胜的优势为:

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

定义 3. (IBE-ANO-CPA) 已知系统安全参数 λ 和 $IBE = (Setup, Ext, Encrypt, Decrypt)$, \mathcal{PPT} 攻击者 \mathcal{A} 与挑战者执行 IBE-ANO-CPA 游戏。如果 \mathcal{A} 在上述游戏中获胜的优势 $\text{Adv}_{\mathcal{A}}^{\text{IBE-ANO-CPA}}(\lambda)$ 是可忽略的, 则该标识加密方案在选择明文攻击下具备匿名性。

IBE-ANO-CPA 游戏过程如下:

系统建立阶段. 已知安全参数 λ , 挑战者运行 $Setup(\lambda)$ 算法生成系统主公私钥对 (mpk, msk) , 并发送 mpk 给攻击者。

询问阶段 1. 在此阶段, 攻击者可以适应性地向挑战者询问任意标识 $id \in \{0,1\}^*$ 对应的私钥 usk_{id} 。

挑战阶段. 攻击者结束询问后, 由其发送两个长度相等的挑战标识 id_0^*, id_1^* 及明文消息 m^* 给挑战者, 唯一的限制是攻击者没有询问过挑战标识对应的私钥 $usk_{id_0^*}, usk_{id_1^*}$ 。挑战者随机选取 $b \in \{0,1\}$, 并运行标识加密算法 $Encrypt(id_b^*, mpk, m^*)$ 生成挑战密文 $C_{id_b^*}$ 发送给攻击者。

询问阶段 2. 在此阶段, 攻击者可以继续适应性地向挑战者询问除挑战标识外任意标识 $id \in \{0,1\}^*$ 对应的私钥 usk_{id} 。

猜测阶段. 最终攻击者输出 $b' \in \{0,1\}$ 作为对 b 的猜测。若 $b' = b$, 则攻击者获胜。

定义攻击者 \mathcal{A} 在 IBE-ANO-CPA 游戏中获胜的优势为:

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

2.4 公钥可搜索加密

公钥可搜索加密方案一般由以下四个多项式时间算法组成:

KeyGen(λ). 算法输入系统安全参数 λ , 输出公私钥对 (A_{pub}, A_{priv}) 。

PEKS(w, A_{pub}). 算法输入关键词 w 和接收者公钥 A_{pub} , 输出关键词密文 C_w 。

Trapdoor(w', A_{priv}). 算法输入关键词 w' 和接收者私钥 A_{priv} , 输出关键词陷门 $T_{w'}$ 。

Test($C_w, T_{w'}$). 算法输入关键词陷门 $T_{w'}$ 和关键词密文 C_w , 若两者对应关键词相匹配即 $w = w'$ 则输出 1, 否则对应关键词不匹配输出 0。

公钥可搜索加密方案中各算法间关系及执行流程如图 2 所示。

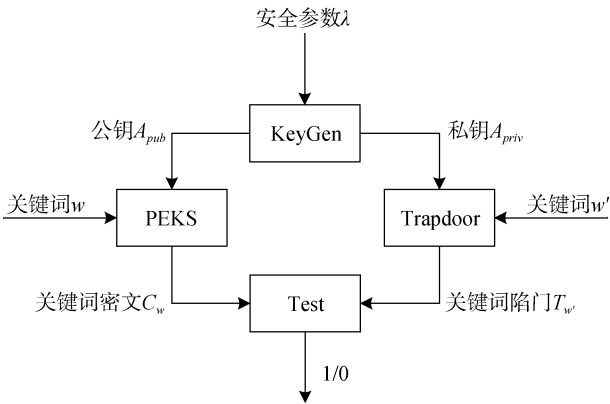


图 2 PEKS 算法流程

Figure 2 Flow chart of PEKS algorithm

公钥可搜索加密方案的一致性要求对于任意的 $(A_{pub}, A_{priv}) \leftarrow \text{KeyGen}(\lambda), C_w \leftarrow \text{PEKS}(w, A_{pub}), T_{w'} \leftarrow \text{Trapdoor}(w', A_{priv})$, 当且仅当 $w = w'$ 时, $\text{Test}(C_w, T_{w'})$ 输出为 1。

安全的公钥可搜索加密方案能够在适应性选择明文攻击下, 满足密文不可区分性 (PEKS-IND-CPA)^[4], 该安全模型可通过攻击者和挑战者之间的游戏定义。即使攻击者能够查询挑战关键词外的其他关键词陷门也无法区分挑战关键词密文, PEKS-IND-CPA 游戏包含下列几个阶段:

系统建立阶段. 挑战者利用安全参数 λ 运行 **KeyGen(λ)** 算法生成公私钥对 (A_{pub}, A_{priv}) , 并发送 A_{pub} 给攻击者。

询问阶段 1. 在此阶段, 攻击者可以适应性地向挑战者询问任意关键词 $w \in \{0,1\}^*$ 的陷门 T_w 。

挑战阶段. 攻击者结束询问后, 发送两个长度相等的挑战关键词 w_0^*, w_1^* 给挑战者, 要求攻击者没有询问过挑战关键词的陷门。挑战者随机选取 $b \in \{0,1\}$, 运行 **PEKS(A_{pub}, w_b^*)** 算法生成挑战密文 $C_{w_b^*}$, 并将其发送给攻击者。

询问阶段 2. 在此阶段, 攻击者可以继续适应性地向挑战者询问除挑战关键词外任意关键词 $w \in \{0,1\}^*$ 的陷门 T_w 。

猜测阶段. 最终攻击者输出 $b' \in \{0,1\}$ 作为对 b 的猜测。若 $b' = b$, 则攻击者获胜, 否则失败。

定义攻击者 \mathcal{A} 获胜的优势为:

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

定义 4. (PEKS-IND-CPA) 在上述游戏中, 如果对于任意 PPT 攻击者 \mathcal{A} , 优势 $\text{Adv}_{\mathcal{A}}^{\text{PEKS-IND-CPA}}(\lambda)$ 是可忽略的, 则称方案是 PEKS-IND-CPA 安全的。

3 方案构造

本节基于 SM9 标识加密算法设计一种公钥可搜索加密方案 (SM9-PEKS)。方案采用前文 2.3 小节中 SM9 标识加密算法使用的符号, 具体构造如下:

3.1 方案描述

KeyGen. 算法输入安全参数 λ , 选取双线性对 $\mathcal{BP} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N)$, 其中 $N > 2^\lambda$, e 为双线性对 $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, 随机选取群 \mathbb{G}_1 和群 \mathbb{G}_2 的生成元 P_1 和 P_2 , 选取安全哈希函数 $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_N^*$ 、密钥派生函数 KDF 、消息认证码函数 MAC , 接着选择一

字节表示的私钥生成函数识别符 hid 。随机选取 $s \in [1, N-1]$, 计算 $P_{pub} = [s]P_1$ 和 $g = e(P_{pub}, P_2)$ 。输出用户公钥 $pk = P_{pub}$, 公开参数 $pp = (\mathcal{BP}, g, P_1, P_2, P_{pub}, H_1, KDF, hid, MAC)$, 用户私钥 $sk = s$ 。

PEKS. 算法输入用户公钥 pk , 关键词 $w \in \{0,1\}^*$, 随机比特串 $m \in \{0,1\}^*$ 。执行如下运算:

A.1 计算 $Q_w = [H_1(w \parallel hid, N)]P_1 + P_{pub}$;

A.2 选取随机数 $r \in [1, N-1]$, 并计算 $C_1 = [r]Q_w$;

A.3 计算 $u = g^r$, $klen = K_1len + K_2len$, 其中 K_1len 为分组加密的密钥长度, K_2len 为 MAC 中密钥 K_2 的长度;

A.4 计算 $K = KDF(C_1 \parallel u, klen)$, 令 K_1 为 K 的最左边的 K_1len 位, K_2 为 K 剩下的 K_2len 位, 若 K_1 全为 0, 退回至随机数 r 的选取, 否则计算 $C_2 = Enc(K_1, m)$;

A.5 计算 $C_3 = MAC(K_2, C_2)$, 输出关键词 w 的密文 $C = C_1 \parallel C_3 \parallel C_2$, 将密文 C 和 m 发送给云端服务器。

Trapdoor. 算法输入关键词 $w' \in \{0,1\}^*$ 、用户私钥 sk 和系统公开参数 pp , 执行如下运算:

$t_1 = H_1(w' \parallel hid, N) + s$, 若 $t_1 = 0$ 则需要重新执行 **KeyGen** 并更新所有关键词陷门, 否则计算 $t_2 = s \cdot t_1^{-1}$, 计算并输出关键词陷门 $T_{w'} = [t_2]P_2$ 。

Test. 算法输入关键词陷门 $T_{w'}$ 、关键词密文 C 及比特串 m 。执行如下运算:

B.1 首先从 C 中提取 C_1 , 若 $C_1 \notin \mathbb{G}_1$ 则终止并返回 $b = 0$, 表示该关键词密文不包含该陷门对应的关键词, 否则进入下一步;

B.2 计算 $u' = e(C_1, T_{w'})$;

B.3 计算 $K = KDF(C_1 \parallel u', klen)$, 令 K'_1 为 K 的最左边的 K_1len 位, K'_2 为 K 剩下的 K_2len 位, 若 K'_2 全为 0, 退出并返回 $b = 0$, 表示不包含该陷门对应的关键词, 否则计算 $m' = Dec(K'_1, C_2)$, 若 $m' \neq m$ 则退出并返回 $b = 0$, 否则进入下一步;

B.4 计算 $C'_3 = MAC(K'_2, C_2)$;

B.5 若 $C_3 = C'_3$ 返回 $b = 1$, 表示包含该陷门对应的关键词, 否则返回 $b = 0$, 表示不含该陷门对应的

关键词。

本方案在云存储中的应用主要包括数据拥有者、云端服务器和数据使用者三种实体, 系统模型如图 3 所示, 使用流程如下: 数据拥有者可调用对称密码算法加密数据, 调用 **PEKS** 算法加密关键词, 然后将密文数据和关键词密文存储至云端服务器; 数据拥有者调用 **Trapdoor** 算法生成关键词陷门发送给数据使用者, 后续使用者可发送关键词陷门至云端服务器; 云端服务器收到关键词陷门后, 调用 **Test** 算法, 将关键词陷门与数据库中关键词密文进行匹配, 最后将所有匹配成功的密文数据返回给数据使用者。

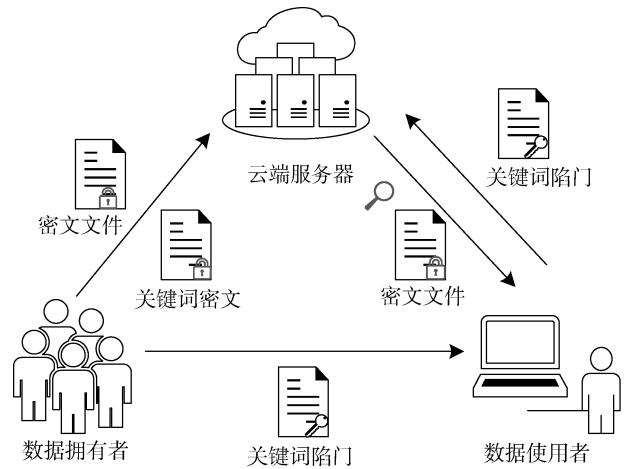


图 3 系统模型

Figure 3 System model

3.2 一致性分析

假设 **KeyGen** 输出系统主公私钥对 (mpk, msk) , **PEKS** 输出关键词 w 密文 $C = C_1 \parallel C_3 \parallel C_2$, **Trapdoor** 输出关键词 w' 的陷门 $T_{w'}$, 方案的一致性验证如下:

$$\begin{aligned}
 u' &= e([r]Q_w, [t_2]P_2) \\
 &= e([r \cdot (H_1(w \parallel hid) + s)]P_1, [s \cdot t_1^{-1}]P_2) \\
 &= e([r \cdot t_1]P_1, [s \cdot t_1^{-1}]P_2) \\
 &= e(P_1, P_2)^{rs} \\
 &= e(C_1, T_{w'}) \\
 &= g^r \\
 &= u.
 \end{aligned}$$

由于 $K = KDF(C_1 \parallel u', klen)$, 令 K'_1 为 K 的最左边的 K_1len 位, K'_2 为 K 剩下的 K_2len 位, 则

$t' = \text{Dec}(K'_1, C_2)$, $C'_3 = \text{MAC}(K'_2, C_2)$ 。因为 $u = u'$, 所以等式 $C_3 = C'_3$ 成立, **Test** 输出 $b = 1$ 。综上所述, 本方案满足公钥可搜索加密的一致性要求。

4 安全性分析

根据文献[24], 利用 new-ibe-2-peks 方法可以由 IBE 方案转换得到 PEKS 方案, 并且通过证明 IBE 方案满足 IBE-IND-CPA 安全, 可进一步证明 PEKS 方案的一致性。若 IBE 方案还满足 IBE-ANO-CPA 安全, 则 PEKS 方案满足 PEKS-IND-CPA 安全。

由于文献[25]已证明 SM9 标识加密算法的 IBE-IND-CPA 安全, 所以 SM9-PEKS 满足一致性。本文仅需证明 SM9 标识加密算法满足 IBE-ANO-CPA 安全, 即可由文献[24]的引理证得 SM9-PEKS 满足 PEKS-IND-CPA 安全。

定理 1. 在判定 (t, ϵ, q) -ABDHE 安全假设下, SM9 加密方案具有 (t', ϵ', q_{ID}) -匿名性, 其中 $t = t' + \mathcal{O}(t_{exp} \cdot q^2)$, $\epsilon = \epsilon' - 2/N$, $q = q_{ID} + 2$, q_{ID} 是询问谕言机的 ID 数量, t_{exp} 是群 \mathbb{G}_2 的单次指数运算耗时。

证明: 假设算法 \mathcal{A} 能够破坏 SM9 的匿名性, 则存在算法 \mathcal{B} 可利用 \mathcal{A} 求解判定 q -ABDHE 问题。算法 \mathcal{B} 以 q -ABDHE 问题的实例 $(P', P, \alpha P, \dots, \alpha^{2q} P, Z)$ 为输入, 其中 $P' \in \mathbb{G}_1, P \in \mathbb{G}_2, Z \in \mathbb{G}_T$, 目标是判断 $Z = e(P', \alpha^{2q+1} P)$ 或 $Z = g_r$ (其中 g_r 为 \mathbb{G}_T 中的随机元素)。 \mathcal{B} 与 \mathcal{A} 执行以下步骤:

Setup. \mathcal{B} 选取 q 阶的多项式 $f(x) = \prod_{i=1}^q (x + h_i)$ ($h_i \in \mathbb{Z}_N, \forall i \in [1, q]$), 计算 $P_2 = f(\alpha)P = \prod_{i=1}^q (\alpha + h_i)P = \sum_{i=0}^q a_i \alpha^i P$ ($a_i \in \mathbb{Z}_N$ 为多项式 $f(x)$ 第 i 项系数)、 $P_1 = \psi(P_2) = f(\alpha)P'$ 和 $P_{pub} = \alpha P_1 = \psi(\alpha P_2) = \psi(\sum_{i=0}^q a_i \alpha^{i+1} P)$, 其中 $\psi: \mathbb{G}_2 \rightarrow \mathbb{G}_1$ 是群 \mathbb{G}_2 到群 \mathbb{G}_1 的同构映射, 且 $\psi(P) = P'$ 。同时, \mathcal{B} 维护哈希值列表 $HList = \{h_i\}_{i=1}^q$ 。最后, \mathcal{B} 将 P_1, P_2, P_{pub} 返回给 \mathcal{A} 。

Phase1. \mathcal{A} 可以向 \mathcal{B} 询问 \mathcal{O}_{Hash} 和 \mathcal{O}_{Ext} 。

\mathcal{O}_{Hash} : 假设 \mathcal{A} 询问 ID_i 的哈希值, \mathcal{B} 判断 $ID_i \parallel hid$ 是否在已有询问列表 $L_H = \langle (ID_i \parallel hid, N), h_i \rangle$ 中, 若存在, 则直接返回 ID_i 对应的 h_i , 否则从 $HList$ 中随机选取一个 $hash$ 返回给 \mathcal{A} , 同时将

$((ID_i \parallel hid, N), hash)$ 记录到 L_H , 在 $HList$ 中删除 $hash$ 。

\mathcal{O}_{Ext} : 假设 \mathcal{A} 询问 ID_i 的私钥, \mathcal{B} 从 L_H 检索 ID_i 对应的 h_i (若 ID_i 未询问过 \mathcal{O}_{Hash} , 则 \mathcal{B} 先执行 \mathcal{O}_{Hash}), 确定多项式 $F_{ID}(x) = \frac{xf(x)}{x + h_i}$, 计算 $sk_i = F_{ID}(\alpha)P = \alpha \prod_{j=1, j \neq i}^q (\alpha + h_j)P = \sum_{i=0}^{q-1} (b_i \alpha^{i+1} P)$, 其中 $b_i \in \mathbb{Z}_N$ 是 $F_{ID}(x)$ 的第 i 项系数。 \mathcal{B} 将 sk_i 返回给 \mathcal{A} , 由于 $sk_i = F_{ID}(\alpha)P = \frac{\alpha f(\alpha)}{\alpha + h_i} P = \frac{\alpha}{\alpha + h_i} P_2$, 所以 sk_i 是 ID_i 的有效私钥。

Challenge. 假设 \mathcal{A} 发起挑战 (ID_0^*, ID_1^*, m^*) , 则 \mathcal{B} 随机选取比特 $b \in \{0, 1\}$, 按照 **Phase1** 的方式生成 ID_b^* 的哈希值 $h_{ID_b^*}$ 和私钥 $sk_{ID_b^*}$, 然后确定多项式 $f_2(x) = xf(x) * f(x) = \sum_{i=0}^{2q} (c_i x^{i+1})$ (其中, $c_i \in \mathbb{Z}_N$ 为 $f_2(x)$ 的第 i 项系数), 计算 $C_1 = c_{2q}^{-1} (h_{ID_b^*} P_1 + P_{pub})$, $u = Z \cdot e(P', \sum_{i=0}^{2q-1} (c_i c_{2q}^{-1} \alpha^{i+1} P))$, $K = \text{KDF}(C_1 \parallel u \parallel ID_b)$, $klen = (K_1, K_2), C_2 = K_1 \oplus m^*, C_3 = \text{MAC}(K_2, C_2)$ 。 \mathcal{B} 将 $C = (C_1, C_3, C_2)$ 返回给 \mathcal{A} 。设 $r = c_{2q}^{-1} \pmod{N}$, 若 $Z = e(P', \alpha^{2q+1} P)$, 则 $C_1 = rh_{ID_b^*} P_1 + rP_{pub}, u = e(P_{pub}, P_2)^r$ 。因此, (C_1, C_3, C_2) 是 (ID_b^*, m^*) 的有效密文。

Phase2. \mathcal{A} 继续询问 \mathcal{O}_{Hash} 和 \mathcal{O}_{Ext} , 但不可询问 (ID_0^*, ID_1^*) 的私钥。 \mathcal{B} 按照 **Phase1** 的方式进行响应。

Guess. 敌手 \mathcal{A} 输出猜测值 b' , 若 $b' = b$, 则 \mathcal{B} 输出 1 表示 $Z = e(P', \alpha^{2q+1} P)$; 否则 \mathcal{B} 输出 0。

模拟完备性分析: 当 $Z = e(P', \alpha^{2q+1} P)$ 时, 敌手 \mathcal{B} 返回的主公钥和挑战密文与实际构造具有相同的分布。假设 \mathcal{I} 是包含 ID_b 和敌手 \mathcal{A} 询问过身份的集合 ($|\mathcal{I}| \leq q + 1$)。从敌手 \mathcal{A} 的视角, $\{f(a) : a \in \mathcal{I}\}$ 是均匀随机且独立分布, 所以 \mathcal{B} 返回的私钥与实际构造也具有相同分布。

概率分析: 若 $Z = e(P', \alpha^{2q+1} P)$, 则前述模拟过程是完备的, 并且 \mathcal{A} 成功猜测 b 的概率为 $1/2 + \epsilon'$ 。否则, Z 是均匀随机的, (C_1, u) 也是均匀随机且独立于 $\mathbb{G}_1 \times \mathbb{G}_T$ 。此时, 不等式 $u \neq e(C_1, sk_{ID_0})$ 和

$u \neq e(C_1, sk_{ID_1})$ 同时成立的概率为 $1 - 2/N$ 。若上述不等式成立, 则 (C_1, C_3, C_2) 在 \mathcal{A} 的视角是均匀随机分布的, 所以不会泄露 b 的信息。

若判定 q -ABDHE 问题中的 Z 是 \mathbb{G}_T 的随机元素, 则 $|\Pr[\mathcal{B}(P', P, \alpha P, \dots, \alpha^{2q} P, Z) = 0] - 1/2| \leq 2/N$; 否则, $|\Pr[\mathcal{B}(P', P, \alpha P, \dots, \alpha^{2q} P, Z) = 0] - 1/2| \geq \epsilon'$ 。因此, 对于均匀分布的 P', P, α 和 Z , 以下式子成立:

$$|\Pr[\mathcal{B}(P', \alpha^{q+2} P', P, \alpha P, \dots, \alpha^{2q} P, Z) = 1] - \Pr[\mathcal{B}(P', \alpha^{q+2} P', P, \alpha P, \dots, \alpha^{2q} P, e(\alpha^{2q+1} P, P')) = 1]| \geq \epsilon' - 2/N。$$

耗时分析: 在上述模拟过程中, \mathcal{B} 的主要耗时是响应 \mathcal{O}_{Ext} 时计算 $F_{ID}(\alpha)P$, 其中 $F_{ID}(x)$ 是 q 阶多项式。这说明每次响应 \mathcal{O}_{Ext} 需要 $\mathcal{O}(q)$ 次的群 \mathbb{G}_2 指数运算。由于 \mathcal{A} 最多询问 $q-2$ 次 \mathcal{O}_{Ext} , 所以 $t = t' + \mathcal{O}(t_{exp} \cdot q^2)$ 。

5 性能分析

本节主要分析并对比 SM9-PEKS 方案与经典 PEKS 方案[9]、[16]、[21]的计算开销、通信代价和安全性。这些方案都基于双线性对构造, 方案[9]、[16]、[21]分别共需要 2、10、3 次高耗时的双线性对运算, SM9-PEKS 仅需 1 次双线性对运算。其中方案[9]是首个 PEKS 方案, 由 BF-IBE^[41]转换得到; 方案[16]基于 dPEKS^[15]方案构造, 增强了原方案安全性; 方案[21]的构造与签密相似, 但其安全目标不同于签密, 主要在生成关键词密文和关键词陷门过程中增加公钥和私钥信息, 保证服务器在测试时无法独自生成关键词密文, 从而可抵抗关键词猜测攻击。

为了清晰描述理论分析结果, 后文令 T_{bp} 表示单次双线性对运算用时, T_{m1} 、 T_{m2} 分别表示 \mathbb{G}_1 、 \mathbb{G}_2 上的标量乘运算时间, T_{exp1} 、 T_{expT} 分别表示 \mathbb{G}_1 、 \mathbb{G}_T 上的模幂运算用时, T_h 表示哈希函数平均运算时间, T_{h2p} 表示将比特串哈希映射到椭圆曲线点的运算时间。 $|\lambda|$ 表示安全参数 λ 的长度, $|\mathbb{G}_1|$ 、 $|\mathbb{G}_2|$ 、 $|\mathbb{G}_T|$ 分别表示群 \mathbb{G}_1 、 \mathbb{G}_2 、 \mathbb{G}_T 中的元素大小。由于四个方案都基于双线性对群设计, 而双线性对群初始化操作可预先执行, 故本文统计效率时忽略该部分的开销。

在计算开销方面(表 1), 对于 PEKS 算法, SM9-PEKS 方案需要 2 次 \mathbb{G}_1 上的点乘运算及 1 次 \mathbb{G}_T 上的模幂运算, 方案[9]需要 2 次 \mathbb{G}_1 上的模幂运算、1 次双线性对运算及 1 次哈希映射到椭圆曲线点的运算, 方案[16]需要 9 次双线性对运算、2 次模幂运算及 1 次哈希映射到椭圆曲线点的运算, 方案[21]需要 3 次 \mathbb{G}_1 上的模幂运算和 1 次哈希映射到椭圆曲线点的运算。对于 Trapdoor 算法, SM9-PEKS 方案需要 1 次 \mathbb{G}_2 上的标量乘运算, 方案[9]和[16]均需要 1 次 \mathbb{G}_1 上的模幂运算及 1 次哈希映射到椭圆曲线点的运算, 方案[21]需要 1 次 \mathbb{G}_1 上的模幂运算、1 次哈希映射到椭圆曲线点的运算及 1 次双线性对运算。对于 Test 算法, SM9-PEKS 方案和方案[9]均只需 1 次双线性对运算, 方案[16]需要 1 次双线性对运算、1 次 \mathbb{G}_1 上的模幂运算, 方案[21]需要 2 次双线性对运算。可见, 与经典 PEKS 方案相比, SM9-PEKS 方案的计算开销较低, 在实际应用中有明显优势。

表 1 公钥可搜索方案加密性能比较

Table 1 Performance comparison of PEKS schemes

方案	计算开销			通信代价			安全性	困难问题
	PEKS	Trapdoor	Test	公钥长度	密文长度	陷门长度		
方案[9]	$2T_{exp1} + T_{bp} + T_{h2p}$	$T_{exp1} + T_{h2p}$	T_{bp}	$ \mathbb{G}_1 $	$ \mathbb{G}_1 + \lambda $	$ \mathbb{G}_1 $	PEKS-IND-CPA	BDH
方案[16]	$9T_{bp} + 2T_{exp1} + T_{h2p}$	$T_{exp1} + T_{h2p}$	$T_{bp} + T_{exp1}$	$2 \mathbb{G}_1 $	$ \mathbb{G}_1 + \lambda $	$ \mathbb{G}_1 $	PEKS-IND-CPA	BDH, BDHI
方案[21]	$3T_{exp1} + T_{h2p}$	$T_{exp1} + T_{bp} + T_{h2p}$	$2T_{bp}$	$ \mathbb{G}_1 $	$2 \mathbb{G}_1 $	$ \mathbb{G}_T $	IKGA	DBDH, mDLIN
SM9-PEKS	$2T_{m1} + T_{expT}$	T_{m2}	T_{bp}	$ \mathbb{G}_1 $	$ \mathbb{G}_1 + \lambda $	$ \mathbb{G}_2 $	PEKS-IND-CPA	q -ABDHE

在通信代价方面(表 1), 对于公钥长度, SM9-PEKS 方案、方案[9]和[21]中公钥均只包含 1 个 \mathbb{G}_1 中

的元素, 方案[16]公钥包含 2 个 \mathbb{G}_1 中的元素。对于密文长度, SM9-PEKS 方案、方案[9]和[16]的关键词密

文均包含 1 个 \mathbb{G}_1 中的元素及长度为 $|\lambda|$ 的元素, 方案[21]的关键词密文包括 2 个 \mathbb{G}_1 中的元素。对于关键词陷门长度, SM9-PEKS 方案的关键词陷门包含 1 个 \mathbb{G}_2 中的元素, 方案[9]和[16]的关键词陷门均包含 1 个 \mathbb{G}_1 中的元素, 方案[21]中的陷门包括 1 个 \mathbb{G}_T 中的元素。可见, SM9-PEKS 方案的通信代价也比部分现有方案低。

在安全性方面(表 1), SM9-PEKS 和所有对比方案的安全性证明都依赖随机谕言机。本文方案安全性可规约至 q -ABDHE 困难问题, 方案[9]安全性可规约至 BDH 困难问题, 方案[16]安全性可规约至 BDH 和 BDHI 困难问题, 方案[21]安全性可规约至 DBDH 和 mDLIN 困难问题。方案[21]可抗内部关键词猜测攻击(Inside Keyword Guessing Attack, IKGA)安全性优于 SM9-PEKS, 但该方案使用了多次高耗时的双线性对运算, 且陷门长度和密文长度较大; 其余方案均可达 PEKS-IND-CPA 安全, 但在计算开销和通信代价方面的性能均比 SM9-PEKS 差。

为了得到实际的比较结果, 在相同测试环境下, 对 SM9-PEKS 方案和其他方案进行编程实现。具体的测试设备为个人笔记本电脑, 配置为: 16GB 内存、64 位 Windows 10 操作系统、Inter(R) Core(TM) i7-9750@2.59 GHz 的 CPU、Miracl 密码库和 C++编程语言。编程实现过程使用 256 比特 BN 曲线, 所以 $|\mathbb{G}_1|=64$ bytes, $|\mathbb{G}_2|=128$ bytes, $|\mathbb{G}_T|=384$ bytes, $|\lambda|=32$ bytes, 嵌入次数 $k=12$, 安全性满足 128 比特。

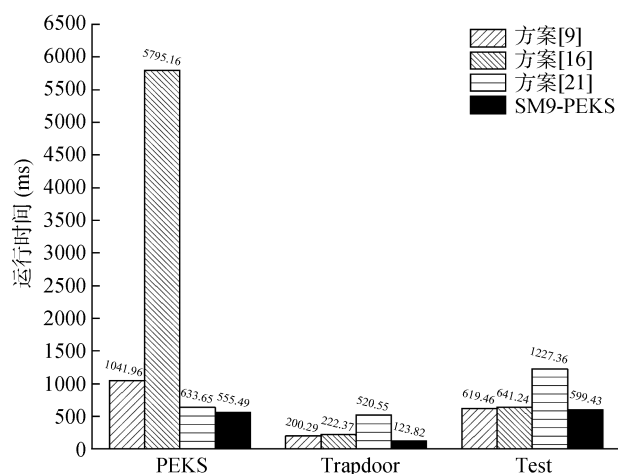


图 4 方案运行时间比较

Figure 4 Comparison on the running time of schemes

实验结果如图 4 所示, 其中横坐标表示各方案中对应算法, 纵坐标表示算法运行时间(单位为 ms)。SM9-PEKS 方案的 PEKS 算法、Trapdoor 算法、Test 算法的用时分别为 555.49 ms、123.82 ms、599.43 ms, 公钥长度、密文长度、陷门长度分别为 64 字节、96 字节、128 字节; 方案[9]的 PEKS 算法、Trapdoor 算法、Test 算法的用时分别为 1041.96 ms、200.29 ms、619.46 ms, 公钥长度、密文长度、陷门长度分别为 64 字节、96 字节、64 字节; 方案[16]的 PEKS 算法、Trapdoor 算法、Test 算法的用时分别为 5795.16 ms、222.37 ms、641.24 ms, 公钥长度、密文长度、陷门长度分别为 128 字节、96 字节、64 字节; 方案[21]的 PEKS 算法、Trapdoor 算法、Test 算法的用时分别为 633.65 ms、520.55 ms、1227.36 ms, 公钥长度、密文长度、陷门长度分别为 64 字节、128 字节、384 字节。可见, 与对比方案中用时最少、带宽最低的方案[9]相比, SM9-PEKS 方案的用时降低 31.31%、带宽增加 64 字节, 其中, 二者的总体用时分别为 1278.74 ms 和 1861.71 ms, 带宽分别为 288 字节和 224 字节。综上所述, SM9-PEKS 方案保证安全性的同时, 增加 64 字节通信代价的情况下, 可以至少降低 31.31%的计算开销。

6 总结

可搜索加密技术在保护数据机密性的同时, 提供数据检索功能, 大幅提升云存储场景下数据外包的检索效率。然而, 现有的可搜索加密方案都是基于国外算法所设计, 不符合国产自主化的发展需求。本文利用 Abdalla 等在 2005 年美密会上提出的 new-ibe-2-peks 方法, 基于 SM9 标识加密算法提出公钥可搜索加密方案 SM9-PEKS。为了证明 SM9-PEKS 方案满足 PEKS-IND-CPA 安全, 本文先在 q -ABDHE 安全假设下证明 SM9 标识加密算法满足 IBE-IND-CPA 安全, 再结合 Abdalla 等提出的引理证得 SM9-PEKS 具备 PEKS-IND-CPA 安全。最后, 通过性能评估与仿真实验对比验证 SM9-PEKS 的实用性, 可为国产商用密码在公钥可搜索加密方面的扩展提供理论参考。

未来工作将围绕安全性、场景应用等方面展开。在安全性方面, 从增强安全性的角度提出可抵抗内

部关键词猜测攻击的方案, 或者提出标准模型下安全的方案。在场景应用方面, 结合区块链、云存储、边缘计算等场景, 增强 SM9-PEKS 在多样化网络背景下的实际效能。

参考文献

- [1] Fu Y X, Luo S M, Shu J W. Survey of Secure Cloud Storage System and Key Technologies[J]. *Journal of Computer Research and Development*, 2013, 50(1): 136-145.
(傅颖勋, 罗圣美, 舒继武. 安全云存储系统与关键技术综述[J]. *计算机研究与发展*, 2013, 50(1): 136-145.)
- [2] Chuka-Maduji N, Anu V. Cloud Computing Security Challenges and Related Defensive Measures: A Survey and Taxonomy[J]. *SN Computer Science*, 2021, 2(4): 331.
- [3] Feng C S, Qin Z G, Yuan D. Techniques of Secure Storage for Cloud Data[J]. *Chinese Journal of Computers*, 2015, 38(1): 150-163.
(冯朝胜, 秦志光, 袁丁. 云数据安全存储技术[J]. *计算机学报*, 2015, 38(1): 150-163.)
- [4] Yang P, Xiong N X, Ren J L. Data Security and Privacy Protection for Cloud Storage: A Survey[J]. *IEEE Access*, 8: 131723-131740.
- [5] Li J W, Jia C F, Liu Z L, et al. Survey on the Searchable Encryption[J]. *Journal of Software*, 2015, 26(1): 109-128.
(李经纬, 贾春福, 刘哲理, 等. 可搜索加密技术研究综述[J]. *软件学报*, 2015, 26(1): 109-128.)
- [6] Song D X, Wagner D, Perrig A, et al. Practical techniques for searches on encrypted data[C]. *Proceeding 2000 IEEE Symposium on Security and Privacy. S&P*, 2002: 44-55.
- [7] Shen Z R, Xue W, Shu J W. Survey on the Research and Development of Searchable Encryption Schemes[J]. *Journal of Software*, 2014, 25(4): 880-895.
(沈志荣, 薛巍, 舒继武. 可搜索加密机制研究与进展[J]. *软件学报*, 2014, 25(4): 880-895.)
- [8] Varri U, Pasupuleti S, Kadambari K V. A Scoping Review of Searchable Encryption Schemes in Cloud Computing: Taxonomy, Methods, and Recent Developments[J]. *The Journal of Supercomputing*, 2020, 76(4): 3013-3042.
- [9] Boneh D, di Crescenzo G, Ostrovsky R, et al. Public Key Encryption with Keyword Search[M]. *Advances in Cryptology - EUROCRYPT 2004*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 506-522.
- [10] Xu P, Jin H, Wu Q H, et al. Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack[J]. *IEEE Transactions on Computers*, 2013, 62(11): 2266-2277.
- [11] Dong Q X, Guan Z, Wu L, et al. Fuzzy Keyword Search over Encrypted Data in the Public Key Setting[C]. *The 14th international conference on Web-Age Information Management*, 2013: 729-740.
- [12] Hu C Y, He P, Liu P T. Public Key Encryption with Multi-Keyword Search[M]. *Communications in Computer and Information Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012: 568-576.
- [13] Hu C Y, Liu P T, Communication N A B T, et al. Public key encryption with ranked multi-keyword search[C]. *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, 2013: 109-113.
- [14] Zeng M, Zhang K, Qian H F, et al. A Searchable Asymmetric Encryption Scheme with Support for Boolean Queries for Cloud Applications[J]. *The Computer Journal*, 2019, 62(4): 563-578.
- [15] Baek J, Safavi-Naini R, Susilo W. Public Key Encryption with Keyword Search Revisited[C]. *ICCSA '08: Proceeding sof the international conference on Computational Science and Its Applications, Part I*, 2008: 1249-1259.
- [16] Rhee H S, Park J H, Susilo W, et al. Improved Searchable Public Key Encryption with Designated Tester[C]. *The 4th International Symposium on Information, Computer, and Communications Security*, 2009: 376-379.
- [17] Tang Q, Chen L Q. Public-Key Encryption with Registered Keyword Search[C]. *The 6th European conference on Public key infrastructures, services and applications*, 2009: 163-178.
- [18] Zhang B, Zhang F G. An Efficient Public Key Encryption with Conjunctive-Subset Keywords Search[J]. *Journal of Network and Computer Applications*, 2011, 34(1): 262-267.
- [19] Hu C Y, Liu P T. An Enhanced Searchable Public Key Encryption Scheme with a Designated Tester and Its Extensions[J]. *Journal of Computers*, 2012, 7(3): 716-723.
- [20] Byun J W, Rhee H S, Park H A, et al. Off-Line Keyword Guessing Attacks on Recent Keyword Search Schemes over Encrypted Data[C]. *The Third VLDB international conference on Secure Data Management*, 2006: 75-83.
- [21] Huang Q, Li H B. An Efficient Public-Key Searchable Encryption Scheme Secure Against Inside Keyword Guessing Attacks[J]. *Information Sciences*, 2017, 403/404: 1-14.
- [22] Wu L B, Chen B W, Zeadally S, et al. An Efficient and Secure Searchable Public Key Encryption Scheme with Privacy Protection for Cloud Storage[J]. *Soft Computing*, 2018, 22(23): 7685-7696.
- [23] Zhang Y P, Katz J, Papamanthou C. All your Queries are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption[C]. *The 25th USENIX Conference on Security Symposium*, 2016: 707-720.
- [24] Abdalla M, Bellare M, Catalano D, et al. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions[J]. *Journal of Cryptology*, 2008, 21(3): 350-391.
- [25] Cheng Z H. Security Analysis of SM9 Key Agreement and Encryption[M]. *Information Security and Cryptology*. Cham: Springer International Publishing, 2019: 3-25.
- [26] Park D J, Kim K, Lee P J. Public Key Encryption with Conjunctive Field Keyword Search[C]. *The 5th international conference on Information Security Applications*, 2004: 73-86.
- [27] Boneh D, Waters B. Conjunctive, Subset, and Range Queries on Encrypted Data[C]. *The 4th conference on Theory of cryptography*, 2007: 535-554.
- [28] Wang C, Cao N, Li J, et al. Secure Ranked Keyword Search over Encrypted Cloud Data[C]. *The 2010 IEEE 30th International Conference on Distributed Computing Systems*, 2010: 253-262.
- [29] Wang C, Cao N, Ren K, et al. Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data[J]. *IEEE*

- Transactions on Parallel and Distributed Systems*, 2012, 23(8): 1467-1479.
- [30] Cao N, Wang C, Li M, et al. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2014, 25(1): 222-233.
- [31] Zheng Q J, Xu S H, Ateniese G, et al. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data[C]. *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, 2014: 522-530.
- [32] Fang L M, Susilo W, Ge C P, et al. A Secure Channel Free Public Key Encryption with Keyword Search Scheme without Random Oracle[C]. *The 8th International Conference on Cryptology and Network Security*, 2009: 248-258.
- [33] Jeong I R, Kwon J O, Hong D, et al. Constructing PEKS Schemes Secure Against Keyword Guessing Attacks is Possible? [J]. *Computer Communications*, 2009, 32(2): 394-396.
- [34] Yau W C, Phan R C W, Heng S H, et al. Keyword Guessing Attacks on Secure Searchable Public Key Encryption Schemes with a Designated Tester[J]. *International Journal of Computer Mathematics*, 2013, 90(12): 2581-2587.
- [35] Lai J C, Huang X Y, He D B. An Efficient Identity-Based Broadcast Encryption Scheme Based on SM9[J]. *Chinese Journal of Computers*, 2021, 44(5): 897-907.
(赖建昌, 黄欣沂, 何德彪. 一种基于商密 SM9 的高效标识广播加密方案[J]. *计算机学报*, 2021, 44(5): 897-907.)
- [36] Shi Y, Ma Z Y, Qin R F, et al. Implementation of an Attribute-Based Encryption Scheme Based on SM9[J]. *Applied Sciences*, 2019, 9(15): 3074.
- [37] Lai J C, Huang X Y, He D B, et al. An Efficient Identity-Based Signcryption Scheme Based on SM9[J]. *Journal of Cryptologic Research*, 2021, 8(2): 314-329.
(赖建昌, 黄欣沂, 何德彪, 等. 基于商密 SM9 的高效标识签密[J]. *密码学报*, 2021, 8(2): 314-329.)
- [38] Xu S W, Ren X P, Yuan F, et al. A Secure Key Issuing Scheme of SM9[J]. *Computer Applications and Software*, 2020, 37(1): 314-319.
(许盛伟, 任雄鹏, 袁峰, 等. 一种关于 SM9 的安全密钥分发方案[J]. *计算机应用与软件*, 2020, 37(1): 314-319.)
- [39] Yang Y T, Cai J L, Zhang X W, et al. Privacy Preserving Scheme in Block Chain with Provably Secure Based on SM9 Algorithm[J]. *Journal of Software*, 2019, 30(6): 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[J]. *软件学报*, 2019, 30(6): 1692-1704.)
- [40] Gentry C. Practical Identity-Based Encryption without Random Oracles[M]. *Advances in Cryptology - EUROCRYPT 2006*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 445-464.
- [41] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing[M]. *Advances in Cryptology — CRYPTO 2001*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 213-229.



蒲浪 于 2020 年在成都信息工程大学信息安全专业获得学士学位。现在福建师范大学网络空间安全专业攻读硕士学位。研究领域为公钥可搜索加密、区块链公平交易。Email: pulang516@163.com



林超 于 2020 年在武汉大学网络空间安全专业获得博士学位。现任福建师范大学计算机与网络空间安全学院讲师。研究领域为应用密码学、区块链隐私保护。Email: linchao91@fjnu.edu.cn



伍玮 于 2011 年在澳大利亚伍伦贡大学信息安全专业获得博士学位。现任福建师范大学数学与统计学院教授。研究领域为密码学、信息安全。Email: weiwu@fjnu.edu.cn



何德彪 于 2009 年在武汉大学应用数学专业获得博士学位。现任武汉大学国家网络安全学院教授。研究领域为公钥密码学、网络与信息安全。Email: hedebiao@whu.edu.cn