软件学报 ISSN 1000-9825, CODEN RUXUEW
[doi: 10.13328/j.cnki.jos.007271] [CSTR: 32375.14.jos.007271]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于国密 SM9 的公钥认证可搜索加密方案*

蒲 浪[1], 林 超[2], 伍 玮[3], 顾晶晶[1], 何德彪[4]

[1](南京航空航天大学 计算机科学与技术学院, 江苏 南京 211106)

[2](福建师范大学 计算机与网络空间安全学院, 福建 福州 350117)

[3](福建师范大学 数学与统计学院, 福建 福州 350117)

[4](武汉大学 国家网络安全学院, 湖北 武汉 430072)

通信作者: 林超, E-mail: linchao91@fjnu.edu.cn

摘 要: 云存储为用户的数据管理带来了极大便捷, 已成为数字经济的重要组成部分. 然而, 复杂多样的网络环境和不完全可信的第三方对用户隐私造成极大威胁. 为保护用户隐私, 通常先加密数据后存储, 但传统加密技术生成的密文阻碍了后续数据检索. 公钥可搜索加密 (public-key encryption with keyword search, PEKS) 技术在保障数据加密的同时, 可提供保密检索功能, 但由于常用关键词数量较少, 传统 PEKS 方案易遭受关键词猜测攻击. 公钥认证可搜索加密 (public-key authenticated encryption with keyword search, PAEKS) 在 PEKS 的基础上引入认证技术, 可进一步提高安全性. 然而, 现有 PAEKS 方案大多基于国外密码算法设计, 不符合我国密码技术自主创新的发展需求. 基于国密 SM9 提出 SM9-PAEKS 方案, 通过重新设计算法结构, 将耗时运算转移至资源丰富的云端服务器, 有效提升用户端检索效率. 并在随机谕言模型下基于 q-BDHI 和 Gap-q-BCAA1 安全假设证明所提方案的安全性. 最后理论分析和实验结果表明, 与同类方案中通信代价最优的方案相比, SM9-PAEKS 在仅增加 96 字节通信代价的情况下, 总计算开销可至少降低约 59.34%, 其中关键词陷门生成的计算开销降低尤其显著, 约为 77.55%. 有助于丰富国密算法的应用, 同时可为云存储中数据加密与检索提供理论与技术支撑.

关键词: 公钥认证可搜索加密; SM9 加密算法; 隐私保护; 数据安全; 云存储

中图法分类号: TP309

中文引用格式: 蒲浪, 林超, 伍玮, 顾晶晶, 何德彪. 基于国密SM9的公钥认证可搜索加密方案. 软件学报. http://www.jos.org.cn/1000-9825/7271.htm

英文引用格式: Pu L, Lin C, Wu W, Gu JJ, He DB. Public-key Authenticated Encryption Scheme with Keyword Search from Chinese Cryptographic SM9. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7271.htm

Public-key Authenticated Encryption Scheme with Keyword Search from Chinese Cryptographic SM9

PU Lang[1], LIN Chao[2], WU Wei[3], GU Jing-Jing[1], HE De-Biao[4]

[1](College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)

[2](College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China)

[3](School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China)

[4](School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China)

Abstract: Cloud storage has become an important part of the digital economy as it brings great convenience to users' data management. However, complex and diverse network environments and third parties that are not fully trusted pose great threats to users' privacy. To

* 基金项目: 国家自然科学基金 (62032005, 62102089, U21A20466, 62102050, 61972094, 62202226, 62272103, 62272104); 中国博士后科学基金 (BX2021399); 福建省科技厅科学基金 (2020J02016); 福建省高等教育协会专项基金 (22FISYZD002); 江苏省自然科学基金 (BK20220935); 中央高校基本科研业务费专项资金 (30922010917)
收稿时间: 2023-07-13; 修改时间: 2023-11-22; 采用时间: 2024-08-14; jos 在线出版时间: 2024-12-11

protect users' privacy, data is usually encrypted before storage, but the ciphertext generated by traditional encryption techniques hinders subsequent data retrieval. Public-key encryption with keyword search (PEKS) technology can provide a confidential retrieval function while guaranteeing data encryption, but the traditional PEKS scheme is vulnerable to keyword guessing attacks due to the small number of common keywords. Public-key authenticated encryption with keyword search (PAEKS) introduces authentication technology based on PEKS, which can further improve security. However, most of the existing PAEKS schemes are designed based on foreign cryptographic algorithms, which do not meet the development needs of independent innovation of cryptography in China. This study proposes an SM9-PAEKS scheme, which can effectively improve user-side retrieval efficiency by redesigning algorithm structure and transferring time-consuming operations to a resource-rich cloud server. Scheme security is also proved under the random oracle model based on q-BDHI and Gap-q-BCCA1 security assumptions. Finally, theoretical analysis and experimental results show that compared with the optimal communication cost among similar schemes, SM9-PAEKS can reduce the total computational overhead by at least 59.34% with only 96 bytes of additional communication cost, and the computational overhead reduction of keyword trapdoor generation is particularly significant, about 77.55%. This study not only helps to enrich national security algorithm applications but also provides theoretical and technical support for data encryption and retrieval in cloud storage.

Key words: public-key authenticated encryption with keyword search (PAEKS); SM9 encryption algorithm; privacy protection; data security; cloud storage

近年来, 互联网技术发展迅速, 网络中的数据呈现规模大、种类多和增速快的特征. 为缓解本地海量数据带来的存储压力, 越来越多的用户选择将个人数据上传至云端存储. 然而, 数据一旦存储至云端, 意味着用户失去对自己数据的控制权. 此外, 由于网络环境的复杂多样性和第三方云存储提供商的不完全可信, 用户个人数据和隐私面临泄露的威胁与挑战. 这将阻碍云存储的发展和应用, 云存储服务提供商需采取相应的安全措施以保护用户隐私[1].

为确保数据安全, 用户通常先加密数据后存储, 但传统对称/非对称加密技术生成的密文不利于后续数据的检索与使用. 为此, 用户可将全部数据下载至本地, 先解密后检索, 但往往用户数据量较大, 该方式面临占用大量网络带宽、消耗计算与存储资源的困境. 此外, 用户也可以将密钥发送给云端服务器, 由资源丰富的云端完成解密与检索, 但这面临密钥如何安全传输和云端是否足够可信等问题. 探寻加密数据的同时, 提供便捷检索功能的技术已成为一大研究热点. 公钥可搜索加密 (public-key encryption with keyword search, PEKS) 技术因有效平衡了功能性、效率与实用性, 成为最有效解决方式之一.

目前, 围绕 PEKS 技术的相关研究取得了一系列优秀的成果[2]. 然而, 由于日常生活中使用的关键词数量较少, 以英语为例, 常用单词仅 3 000 个. 因此, 传统 PEKS 方案易遭受恶意云服务器发起的内部关键词猜测攻击, 从而泄露用户数据中包含的关键词, 对用户的隐私造成极大威胁[3,4]. 公钥认证可搜索加密 (public-key authenticated encryption with keyword search, PAEKS) 在 PEKS 的基础上引入发送方公私钥, 分别用于关键词陷门和关键词密文生成. 由于缺少发送方私钥, 云服务器无法生成合理关键词密文, 从而可有效抵抗内部关键词猜测攻击, 为用户隐私提供更强保障. 现有 PAEKS 方案大多基于国外密码算法设计, 不符合我国密码技术自主可控的发展需求. 此外, 现有多数 PAEKS 方案中用户端涉及较多高耗时运算, 不利于物联网等领域的轻量级设备使用. 为了进一步保障用户隐私同时促进国产密码算法的扩展与应用, 亟需基于国产密码算法设计安全实用的 PAEKS 方案.

针对上述发展瓶颈, 本文提出基于国密 SM9 的公钥认证可搜索加密方案, 填补了现有研究中缺乏基于国密算法所设计 PAEKS 方案的空缺, 可有效保障云存储系统的安全性与实用性, 本文主要贡献如下.

(1) 扩展国产商用密码的功能性, 提出了首个基于国密 SM9 的公钥认证可搜索加密方案 (SM9-PAEKS), 该方案采用 SM9 密码算法的椭圆曲线参数, 可与使用 SM9 系列密码的系统实现完美兼容, 有助于国密算法的推广与应用, 增强公钥可搜索加密技术的自主可控能力.

(2) 抵抗关键词猜测攻击, SM9-PAEKS 通过引入共享密钥的方式, 在关键词密文和陷门生成阶段分别引入发送方私钥和接收方私钥, 实现抗关键词猜测攻击的特性, 即便内部诚实但好奇的云服务器也无法发起关键词猜测攻击, 从而提高了安全性.

(3) 提升用户端检索效率, 现有大部分 PAEKS 方案都是基于高耗时双线性配对运算设计的, 用户端通常涉及多次耗时操作, 这导致检索效率不佳. SM9-PAEKS 方案通过重新设计算法结构, 将耗时运算转移至算力充足的云

端服务器, 大幅提升了用户端的检索效率, 更适用于物联网等领域的轻量级设备使用. 同时, 这也可为同类型方案的性能优化提供新思路.

(4) 证明了 SM9-PAEKS 的安全性, 本文基于随机谕言模型给出了方案安全性的详细证明. 同时, 为模拟真实环境中方案的应用效率, 本文开展了大量仿真测试, 理论结合实践地对方案进行评估. 实验结果表明, 与同类方案中通信代价最优的方案相比, SM9-PAEKS 在仅增加 96 字节通信代价的情况下, 总计算开销可至少降低约 59.34%, 其中关键词陷门生成的计算开销降低约为 77.55%.

本文第 1 节对 PEKS 和 SM9 密码算法的相关工作进行介绍. 第 2 节对后文涉及的双线性对、安全假设、系统模型、安全模型等预备知识进行介绍. 第 3 节详细介绍 SM9-PAEKS 的具体构造, 并对其正确性与安全性进行分析. 第 4 节从理论分析和仿真实验测试两个角度对 SM9-PAEKS 进行评估. 最后, 第 5 节对全文工作进行总结, 并展望未来可继续开展的工作.

1 相关工作

2000 年, Song 等人[5]最早提出可搜索加密的概念, 并给出首个对称可搜索加密方案. 随后, 大量研究围绕可搜索加密开展. 2004 年, Boneh 等人[6]结合可搜索加密与公钥密码学的特点, 最早提出了 PEKS 的概念并给出了首个 PEKS 方案. 本节参考 PEKS 的重要研究成果, 从安全性和搜索模式两个角度论述 PEKS 的研究现状, 然后介绍本文研究所基于国产 SM9 密码算法的研究现状.

安全性: 2003 年, Goh 等人[7]最早给出了可搜索加密的安全性定义. 2005 年, Abdalla 等人[8]出于隐私的考虑定义了 PEKS 的搜索和访问模式, 并建议后续的研究中应确保两种模式的安全与隐私. 2006 年, Byun 等人[9]提出抵抗外部离线关键词猜测攻击的概念, 并对文献 [6,10] 的方案进行了攻击. 2010 年, Tang 等人[11]提出的方案可抵抗此类攻击. 2008 年, Baek 等人[12]在不需要建立安全信道的前提下, 构建 PEKS 方案, 并在随机谕言模型下证明其方案的安全性, 然而该模型下安全并不能保证真实世界中的安全. 2009 年, Fang 等人[13]提出的方案在无需安全信道的同时, 安全性证明也不需借助随机谕言模型. Jeong 等人[4]指出由于常用关键词空间较小, 传统 PEKS 方案无法抵抗关键词猜测攻击. 2016 年, 为抵抗关键词猜测攻击, Chen 等人[14] 利用双服务器模式, 匹配测试需由两个服务器完成. 2017 年, Huang 等人[15] 提出 PAEKS 方案, 通过为数据发送者分配密钥对的方式, 在关键词密文生成时不仅需要接收方公钥还需发送方私钥, 在单服务器模式下就可抵抗关键词猜测攻击. 2019 年, Chen 等人[16] 提出基于双服务器的 PAEKS 方案, 关键词匹配算法由两个服务器执行, 避免了单服务器权力集中导致的关键词猜测攻击, 方案可达更高的安全性. 2020 年, Qin 等人[17] 对 PAEKS 进行了安全性加强, 提出了多密文不可区分和多陷门不可区分, 并给出了满足定义的方案. 2022 年, Li 等人[18] 在电子医疗记录场景中提出公钥认证密文更新可搜索加密, 引入可信代理将来自不同发送者的密文转换为同一形式, 从而支持常量关键词陷门检索, 降低系统通信开销. 2023 年, Liu 等人[19] 基于无证书体系设计的方案避免了较高开销的双线性对映射, 提升效率的同时在陷门生成过程中引入随机数, 可提升方案中关键词陷门的安全性. Cheng 等人[20] 提出 PAEKS 没有考虑频率分析攻击, 易造成用户关键词陷门中包含关键词信息泄露, 并在此基础上给出了可抵抗频率分析攻击的 PAEKS 方案.

检索模式: 2004 年, Boneh 等人[6]提出首个支持单关键词检索的 PEKS 方案, 这是最基础的检索模式. 但由于其检索时的精度不够高, 使用场景非常受限. 2005 年, Park 等人[10]提出支撑连接关键词的 PEKS 方案, 有效提升了检索精度. 2007 年, Boneh 等人[21] 提出支持范围查询的方案, Shi 等人[22] 进一步地提出了支持多维度进行范围检索的方案. 2013 年, Xu 等人[23] 提出了支持模糊关键词查询的方案, 该模式下可检索无法精准确定的关键词. 2014 年, 李双等人[24] 提出基于属性的 PEKS 方可适应群组, 扩大信息共享范围的同时节省云端存储空间. 2023 年, Chen 等人[25] 利用区块链、哈希证明链等技术实现检索结果可验证和数据动态更新.

SM9 密码算法: SM9 密码算法是我国政府高度重视密码算法发展和应用的产物, 得到了国家标准层面的大力支持, 是我国自主研发的首个标识密码算法. 该算法基于有限域椭圆曲线上的双线性对构建, 共包括数字签名、密钥交换协议、密钥封装协议以及标识加密算法这 4 个重要部分. 目前, SM9 密码算法的相关研究也取得了诸多成

果. 2019 年, Cheng[26] 基于 Gap 类困难问题分析了 SM9 加密算法的安全性. 2021 年, 赖建昌等人[27]证明了 SM9 签名算法的安全性, 并改进了密钥封装算法同时给出了安全性证明. 2022 年, 秦宝东等人[28] 提出了基于仲裁的 SM9 标识加密方案, 该方案可实现对用户访问权限的快速管理. 2023 年, 朱留富等人[29] 提出基于 SM9 的属性基签名, 离线时完成高耗时操作, 在线时进行耗时较低的运算, 同时实现了细粒度访问控制. 彭聪等人[30] 凝练环签名和 SM9 签名算法的核心技术, 提出基于身份的环签名方案, 方案的通信开销与现有方案相比降低显著. 蒲浪等人[31] 和张超等人[32] 分别使用不同的方法设计了基于 SM9 的 PEKS 方案, 但均为传统公钥可搜索加密方案, 无法抵抗关键词猜测攻击[14]. 综上所述, 尚未见基于 SM9 的 PAEKS 方案的研究成果在国内外刊物上公开发表.

综上可知, PEKS/PAEKS 的相关研究已经取得了系列优秀成果, 但现有大部分 PAEKS 方案都基于国外的密码算法设计, 不符合我国密码技术自主可控的发展需求. SM9 标识加密是我国自主研发的一系列基于标识的密码算法, 其具有良好的可扩展性可与 PAEKS 技术结合, 以填补缺乏基于国密算法 PAEKS 方案的空缺.

2 预备知识

2.1 双线性对

设 N 为大素数, 群 $\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$ 均为 N 阶循环群, $\mathbf{1}_T$ 表示 $\mathbb{G}_T$ 的生成元, 双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ 需满足如下 3 条性质.

(1) 双线性: 对于任意的元素 $P_1\in\mathbb{G}_1,P_2\in\mathbb{G}_2$, $a,b\in\mathbb{Z}_N^*$, 等式 $e(aP_1,bP_2)=e(P_1,P_2)^{ab}$ 恒成立.

(2) 非退化性: 至少存在元素 $P_1\in\mathbb{G}_1,P_2\in\mathbb{G}_2$, 使等式 $e(P_1,P_2)\neq\mathbf{1}_T$ 成立.

(3) 可计算性: 对于 $\forall P_1\in\mathbb{G}_1,\forall P_2\in\mathbb{G}_2$, 恒存在多项式时间算法计算 $e(P_1,P_2)$ 的值.

若 $\mathbb{G}_1=\mathbb{G}_2$, 则此类双线性群称为对称双线性群, 否则为非对称双线性群, SM9 系列算法中使用非对称双线性群, 且当 P_1 和 P_2 为生成元时, 存在有效同构映射 $\psi(P_2)=P_1$.

2.2 安全假设

本节介绍后文安全性证明涉及的安全假设. 令 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,N,e,P,Q)$, 其中 P, Q 分别为 $\mathbb{G}_1$, $\mathbb{G}_2$ 的生成元. 令 λ 为系统安全参数, $\mathrm{negl}(\lambda)$ 为关于 λ 的可忽略函数.

定义 1. q-BDHI 安全假设[33]. 已知 $q+2$ 个元素 $(P,Q,aQ,a^2Q,\ldots,a^qQ)$, 计算群 $\mathbb{G}_T$ 中的元素 $e(P,Q)^{\frac{1}{a}}$, 其中 $a\in\mathbb{Z}_N^*$. 对于任意概率多项式时间 (probabilistic polynomial-time, $\mathcal{PPT}$) 敌手 $\mathcal{A}$ 求解出 $e(P,Q)^{\frac{1}{a}}$ 的概率是可忽略的, 即:

$$\Pr[\mathcal{A}(P,aQ,a^2Q,\ldots,a^qQ)=e(P,Q)^{\frac{1}{a}}]\leqslant\mathrm{negl}(\lambda) \tag{1}$$

定义 2. DBIDH 安全假设[34]. 已知如下两个元组 $\mathcal{V}_1=<P_1,P_2,[a]P_i,[b]P_j,e(P_1,P_2)^{\frac{b}{a}}>$ 和 $\mathcal{V}_2=<P_1,P_2,[a]P_i,[b]P_j,e(P_1,P_2)^{r}>$, 其中 $a,b,r\in\mathbb{Z}_N^*,i,j\in\{1,2\}$. 区分 $\mathcal{V}_1$ 和 $\mathcal{V}_2$ 是困难的. 对于任意 $\mathcal{PPT}$ 敌手 $\mathcal{A}$ 成功区分 $\mathcal{V}_1$ 和 $\mathcal{V}_2$ 的概率是可忽略的, 即:

$$|\Pr[\mathcal{A}(\mathcal{V}_1)=0]-\Pr[\mathcal{A}(\mathcal{V}_2)=0]|\leqslant\mathrm{negl}(\lambda) \tag{2}$$

定义 3. Gap-q-BCAA1 安全假设[34]. 已知如下元组 $\mathcal{V}_3=\left(P_1,P_2,[x]P_j,t_0,\left(t_1,\frac{x}{x+t_1}P_j\right),\ldots,\left(t_q,\frac{x}{x+t_q}P_j\right)\right)$, 其中 $x,q,t_i\in\mathbb{Z}_N^*,j\in\{1,2\}$. 可查询 DBIDH 谕言机的情况下, 计算 $e(P_1,P_2)^{\frac{x}{x+t_0}}$ 是困难的. 对于任意 $\mathcal{PPT}$ 敌手 $\mathcal{A}$ 成功解决上述问题的概率是可忽略的, 即:

$$\Pr[\mathcal{A}(\mathcal{V}_3)=e(P_1,P_2)^{\frac{x}{x+t_0}}]\leqslant\mathrm{negl}(\lambda) \tag{3}$$

2.3 PAEKS 方案定义与系统模型

PAEKS 基于 PEKS 设计, 在关键词密文和关键词陷门生成阶段分别引入发送方私钥和发送方公钥, 限制了关键词密文生成, 从而有效避免了内部关键词猜测攻击. 云存储中应用 PAEKS 方案, 通常包含发送方, 即数据拥有者 (data owner, DO); 数据接收方, 即数据使用者 (data user, DU); 可信中心和云端服务器这 4 个实体. 云存储下应用 PAEKS 时典型的系统模型如图 1 所示.

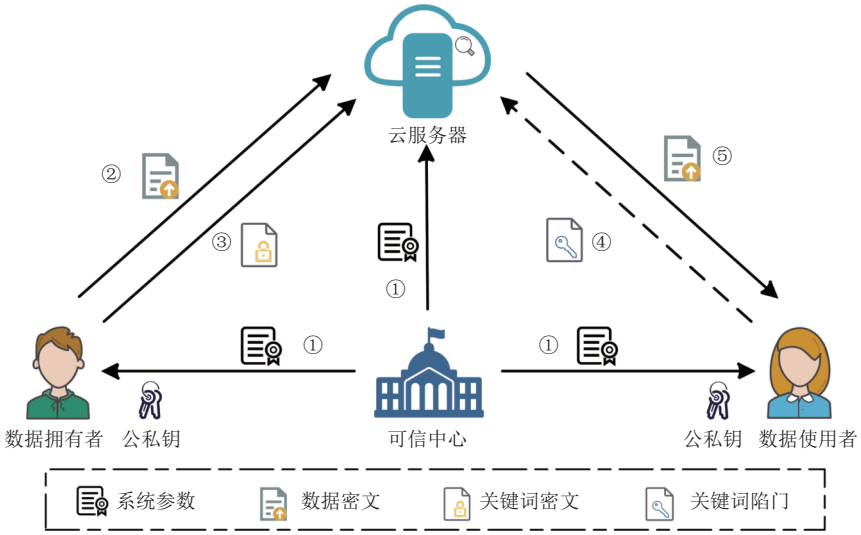

图 1　系统模型

系统运行流程如下: ① 可信中心为所有实体分发系统参数. ② DO 首先加密明文数据, 并将其中包含的关键词提取出来. ③ DO 使用关键词密文算法, 用自己的私钥和 DU 的公钥加密关键词, 随后将关键词密文数据与数据密文共同上传至云服务器存储. ④ DU 需要检索包含某一关键词数据时, 使用关键词陷门生成算法, 用自己的私钥和 DO 的公钥生成关键词陷门, 随后将关键词陷门上传至云服务器. ⑤ 云服务器收到关键词陷门后, 使用匹配测试算法, 若通过匹配测试, 则表明该关键词密文对应的数据为使用者欲检索的内容. 最终, 云服务器将所有通过匹配测试的数据密文返回给 DU.

PAEKS 方案包括如下 6 个多项式时间算法, 具体每个算法定义如下.

(1) 系统初始化 $params \leftarrow Setup(1^{\lambda})$. 此算法以系统安全参数 λ 为输入, 生成系统公开参数 $params$.

(2) 接收方密钥生成 $(sk_R, pk_R) \leftarrow KeyGen_R(params)$. 此算法以 $params$ 为输入, 生成接收方密钥对 (sk_R, pk_R).

(3) 发送方密钥生成 $(sk_S, pk_S) \leftarrow KeyGen_S(params)$. 此算法以 $params$ 为输入, 生成发送方密钥对 (sk_S, pk_S).

(4) 关键词加密 $C_w \leftarrow PAEKS(w, sk_S, pk_R, params)$. 此算法以关键词 $w \in \{0,1\}^*$、发送方私钥 sk_S、接收方公钥 pk_R 和参数 $params$ 为输入, 生成关键词密文 C_w.

(5) 关键词陷门生成 $T_{w'} \leftarrow Trapdoor(w', sk_R, pk_R, params)$. 此算法以关键词 $w' \in \{0,1\}^*$、接收方私钥 sk_R、发送方公钥 pk_S 和系统参数 $params$ 为输入, 输出关键词陷门 $T_{w'}$.

(6) 匹配测试 $\{0/1\} \leftarrow Test(C_w, T_{w'}, params)$. 此算法以关键词密文 C_w、关键词陷门 $T_{w'}$ 和系统参数 $params$ 为输入, 若 C_w 和 $T_{w'}$ 包含的关键词一致, 则输出 1, 否则输出 0.

2.4　安全模型

本节介绍后文方案安全性证明中使用的安全模型. 设 PAEKS 方案为 $PAEKS = (Setup, KeyGen_R, KeyGen_S, PAEKS, Trapdoor, Test)$, 由敌手 $\mathcal{A}$ 与挑战者 C 之间进行的两个游戏刻画 PAEKS 方案的语义安全, 其中 CI-CKA 游戏定义了关键词密文不可区分性, TI-CKA 游戏定义了关键词陷门隐私性.

CI-CKA 游戏: 即适应性选择关键词攻击下的关键词密文不可区分性 (ciphertext indistinguishability under the adaptive chosen keyword attack, CI-CKA), 保证敌手获取合理关键词密文后, 无法获取其中包含的关键词信息, 具体的游戏定义如下.

(1) 初始化阶段. C 首先运行 $Setup(1^{\lambda})$ 算法, 生成系统中的公开参数 $params$, 然后运行密钥生成算法 $KeyGen_R(params)$ 和 $KeyGen_S(params)$, 分别生成接收方公私钥对 (sk_R, pk_R) 和发送方公私钥对 (sk_S, pk_S), 最终将生成的 $(params, pk_R, pk_S)$ 发送给 $\mathcal{A}$.

(2) 询问阶段 1. 此阶段, $\mathcal{A}$ 可适应性地选取关键词 $w \in \{0,1\}^*$, 并向 C 进行如下两种询问.

1) 关键词密文询问 O_{C_w}. $\mathcal{A}$ 发送关键词给 C, C 运行 $PAEKS(sk_S, pk_R, w, params)$ 算法生成关键词 w 的密文 C_w 并发送给 $\mathcal{A}$.

2) 关键词陷门询问 O_{T_w}. $\mathcal{A}$ 发送 $w \in \{0,1\}^*$ 给 C, 然后 C 运行 $Trapdoor(sk_R, pk_s, w, params)$ 算法生成关键词 w 的陷门 T_w 并发送给 $\mathcal{A}$.

(3) 挑战阶段. $\mathcal{A}$ 可以决定何时结束上述询问阶段 1, 随后选取两个挑战关键词 $w_0^*, w_1^* \in \{0,1\}^*$, 此处限制条件为 $|w_0^*| = |w_1^*|$ 且挑战关键词没有在询问阶段 1 中被询问过. C 收到挑战关键词后, 随机选取 $b \in \{0,1\}$, 然后运行加密算法 $PAEKS(w_b^*, sk_S, pk_R, params)$ 生成挑战关键词密文 $C_{w_b^*}$, 最后发送给 $\mathcal{A}$.

(4) 询问阶段 2. 此阶段, $\mathcal{A}$ 可继续向 C 进行同询问阶段 1 的询问, 但是此处限制其询问的关键词 $w \in \{0,1\}^*$ 不能为挑战关键词, 即 $w \notin \{w_0^*, w_1^*\}$.

(5) 猜测. 最终, $\mathcal{A}$ 输出 $b' \in \{0,1\}$ 作为对 b 的猜测. 若 $b' = b$, 则 $\mathcal{A}$ 赢得 CI-CKA 游戏, 否则失败.

定义上述游戏中, $\mathcal{A}$ 赢得游戏的优势为:

$$Adv_{\mathcal{A},\mathrm{PAEKS}}^{\text{CI-CKA}}(\lambda) = \left|\Pr[b' = b] - \frac{1}{2}\right| \tag{4}$$

定义 4. 若任意 $\mathcal{PPT}$ 敌手 $\mathcal{A}$ 赢得上述游戏的优势是可忽略的, 即 $Adv_{\mathcal{A},\mathrm{PAEKS}}^{\text{CI-CKA}}(\lambda) \leqslant \mathrm{negl}(\lambda)$, 则该 PAEKS 方案满足关键词密文不可区分性.

TI-CKA 游戏: 即适应性选择关键词攻击下的关键词陷门不可区分性 (trapdoor indistinguishability under the adaptive chosen keyword attack, TI-CKA), 满足此安全性可保证在 PAEKS 方案中, 即便是内部敌手 $\mathcal{A}$ (通常为诚实但好奇的云端服务器) 获取合理关键词陷门后, 也无法获取其中包含的关键词信息, 具体游戏定义如下.

初始化阶段: 此阶段与 CKA-CI 游戏中的初始化阶段一致.

询问阶段 1: 此阶段与 CKA-CI 游戏中的询问阶段 1 一致.

挑战阶段: $\mathcal{A}$ 决定结束上述询问阶段 1 后, 随即选取挑战关键词 $w_0^*, w_1^* \in \{0,1\}^*$, 此处 $|w_0^*| = |w_1^*|$ 并且挑战关键词没有在询问阶段 1 中被询问过. C 收到挑战关键词后, 随机选取 $b \in \{0,1\}$, 然后运行陷门生成算法 $Trapdoor(w_b^*, sk_R, pk_S, params)$ 生成挑战关键词陷门 $T_{w_b^*}$ 并发送给 $\mathcal{A}$.

询问阶段 2: 与 CKA-CI 游戏中的询问阶段 2 一致, 但此处限制其询问的关键词 $w \in \{0,1\}^*$ 不能为挑战关键词, 即 $w \notin \{w_0^*, w_1^*\}$.

猜测: 最终, $\mathcal{A}$ 输出 $b' \in \{0,1\}$ 作为对 b 的猜测. 若 $b' = b$, 则 $\mathcal{A}$ 赢得此 TI-CKA 游戏, 否则失败.

定义上述游戏中, $\mathcal{A}$ 赢得游戏的优势为:

$$Adv_{\mathcal{A},\mathrm{PAEKS}}^{\text{TI-CKA}}(\lambda) = \left|\Pr[b' = b] - \frac{1}{2}\right| \tag{5}$$

定义 5. 若任意 $\mathcal{PPT}$ 敌手 $\mathcal{A}$ 赢得上述游戏的优势是可忽略的, 即 $Adv_{\mathcal{A},\mathrm{PAEKS}}^{\text{TI-CKA}}(\lambda) \leqslant \mathrm{negl}(\lambda)$, 则该 PAEKS 方案满足关键词陷门不可区分性.

3 基于 SM9 的公钥认证可搜索加密方案

3.1 方案描述

基于 SM9 的公钥认证可搜索加密方案具体构造如下.

(1) $Setup(1^\lambda)$. 本算法以安全参数 λ 为输入, 生成系统中的公开参数. 首先选取双线性对群 $\mathcal{BP} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, N, e, P_1, P_2)$, 其中 $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ 为素 N 阶循环群, e 为双线性映射, P_1, P_2 分别为群 $\mathbb{G}_1, \mathbb{G}_2$ 的生成元, 且存在从 $\mathbb{G}_2$ 到 $\mathbb{G}_1$ 的同态映射 ψ 使得 $\psi(P_2) = P_1$. 随后选取哈希函数 $H_1 : \{0,1\}^* \to \mathbb{Z}_N^*$, 密钥派生函数 $H_2 : \{0,1\}^* \to \{0,1\}^{klen}$, 其中 $klen$ 为 SM9 中使用对称加密的密钥长度. 然后确定消息认证码函数 MAC. 此外, 选取 8 比特表示的私钥生成函数标识符 hid. 最终, 该算法输出系统参数 $params = (\mathcal{BP}, hid, H_1, H_2, MAC)$.

(2) $KeyGen_R(params)$. 本算法以 $params$ 为输入, 生成接收方公私钥对. 首先随机选取 $x \in \mathbb{Z}_N^*$, 然后计算 xP_1.

设接收方私钥为 $sk_R = x$, 公钥为 $pk_R = (xP_1, g)$, 其中 $g = e(pk_R, P_2)$. 最终, 算法将公钥公开, 秘密存储私钥.

(3) $KeyGen_S(params)$. 本算法以 $params$ 为输入, 生成发送方公私钥对. 首先随机选取 $y \in \mathbb{Z}_N^*$, 然后计算 yP_1. 设接收方私钥为 $sk_S = y$, 公钥为 $pk_S = yP_1$. 最终, 该算法公开公钥, 秘密存储私钥.

(4) $PAEKS(w, pk_R, sk_S, m)$. 本算法以关键词 $w \in \{0,1\}^*$、接收方公钥 pk_R、发送方私钥 sk_S、随机比特 $m \in \{0,1\}^*$ 和系统参数 $params$ 为输入, 生成关键词密文. 具体计算过程如下.

1) 计算 $Q_w = [H_1(w\|hid\|V,N)]P_1 + pk_R$, 其中 $V = [y]pk_R$.

2) 选取随机数 $r \in \mathbb{Z}_N^*$, 然后计算 $C_1 = [r]Q_w$.

3) 计算 $u = g^r, klen = k_1 + k_2$, 其中 k_1 为分组加密中密钥的长度, k_2 为消息认证码中密钥长度.

4) 计算 $K = H_2(C_1\|u, klen)$, 令 K_1 为 K 的前 k_1 位, K_2 为剩下的 k_2 位. 若 K_1 全为 0, 则重新选取随机数 r; 否则计算 $C_2 = Enc(K_1, m)$.

5) 计算 $C_3 = MAC(K_2, C_2)$, 输出关键词密文 $C_w = C_1\|C_3\|C_2$. 最后将 C_w 和随机比特 m 发送至云端服务器.

(5) $Trapdoor(w', pk_S, sk_R, params)$. 本算法以关键词 $w' \in \{0,1\}^*$、发送方公钥 pk_S、接收方私钥 sk_R 和系统参数 $params$ 为输入, 生成关键词陷门. 具体计算过程如下.

1) 首先, 计算 $t_1 = H_1(w'\|hid\|V', N) + x$, 其中 $V' = [x]pk_S$. 若 $t_1 = 0$, 则重新执行 $KeyGen_R$ 算法生成公私钥对, 并更新所有关键词陷门; 否则下一步.

2) 计算 $t_2 = x \cdot t_1^{-1}$, 最终计算并输出关键词陷门 $T_{w'} = t_2 P_2$.

(6) $Test(C_w, T_{w'}, params)$. 本算法以关键词密文 C_w、关键词陷门 $T_{w'}$ 和系统参数 $params$ 为输入, 对二者所含关键词是否一致进行匹配测试. 具体算法如下.

1) 若 $C_1 \notin \mathbb{G}_1$, 则终止算法并返回 $b = 0$ 表示匹配测试不通过, 否则计算 $u' = e(T_{w'}, C_1)$.

2) 计算 $K = H_2(C_1\|u', klen)$, $klen = k_1 + k_2$, 其中 k_1 为分组加密中密钥的长度, k_2 为消息认证码中密钥长度. 令 K_1' 表示 K 的前 k_1 位, K_2' 为剩下的 k_2 位, 若 K_1' 全为 0, 则终止算法并返回 $b = 0$; 否则, 下一步.

3) 计算 $m' = Dec(K_1', C_2)$, 若 $m \neq m'$, 则终止算法返回 $b = 0$.

4) 计算 $C_3' = MAC(K_2', C_2)$, 若 $C_3' = C_3$, 则返回 $b = 1$, 表示 $w = w'$, 否则返回 $b = 0$.

正确性分析: 若接收方可生成合法关键词陷门, 并且关键词密文是有效的且二者所含关键词相同, 那么一定可通过匹配测试算法. 假设接收方、发送方的公私钥分别为 (pk_R, sk_R) 和 (pk_S, sk_S), 关键词密文为 $C_w = C_1\|C_3\|C_2$, 关键词陷门为 $T_{w'}$, 方案的正确性验证如下:

$$\begin{aligned} u' &= e(C_1, T_{w'}) \\ &= e(rQ_w, t_2 P_2) \\ &= e([r \cdot (H_1(w\|hid, N) + x)]P_1, [x \cdot t_1^{-1}]P_2) \end{aligned} \tag{6}$$

分析可知, 因 $t_1^{-1} = (H_1(w'\|hid, N) + x)^{-1}$, 当且仅当 $w = w'$ 时, 有 $u' = e(P_1, P_2)^{rx} = g^r = u$ 成立, 由于 $K = H_2(C_1\|u', klen), klen = k_1 + k_2$, 令 K_1' 表示 K 的前 k_1 位, K_2' 为剩下的 k_2 位, 有 $m' = Dec(K_1', C_2)$ 及 $C_3' = MAC(K_2', C_2)$. 当且仅当 $w = w'$ 时, $m' = m$, $C_3' = C_3$, 则匹配算法 $Test$ 输出 1. 综上, 本方案满足 PAEKS 方案的正确性要求.

3.2 安全性分析

本节对 SM9-PAEKS 进行安全性分析与证明, 通过证明如下定理 1, 证得方案具备关键词密文不可区分性和关键词陷门不可区分性.

定理 1. 若 q-BDHI 和 Gap-q-BCAA1 安全假设成立, 则 SM9-PAEKS 方案具备密文不可分性和陷门隐私性.

上述定理 1 可通过如下两条引理证得, 其中引理 1 证明方案的关键词密文不可区分性, 引理 2 证明方案的关键词陷门不可区分性.

引理 1. 若 q-BDHI 安全假设成立, 那么 SM9-PAEKS 是 CKA-CI 安全的.

证明: 假设存在 $\mathcal{PPT}$ 敌手 $\mathcal{A}$ 询问 q_{H_1} 次谕言机后能以不可忽略的优势攻破 SM9-PAEKS 方案的 CKA-CI 安全性. 则挑战者 $\mathcal{C}$ 可通过与 $\mathcal{A}$ 交互, 以不可忽略的优势解决 q-BDHI 问题. $\mathcal{C}$ 输入 q-BDHI 困难问题实例 $(P, Q, aQ, \ldots,$

$a^qQ)$, 其目标是计算 $e(P,Q)^{1/a}$, $\mathcal{C}$ 与 $\mathcal{A}$ 的具体交互过程如下.

● 初始化阶段. $\mathcal{C}$ 随机选取 $k\in[1,q], B_k\in\mathbb{Z}_N^*$, 然后选取 $q-1$ 个不同的随机数 $t_1,t_2,...,t_{k-1}, t_{k+1},\ldots,t_q\in\mathbb{Z}_N^*$ 对于 $\forall i\in[1,q]\backslash\{k\}$, 计算 $B_i=B_k-t_i$, 同时生成如下多项式 $f(x)=\prod_{i=1,i\neq k}^{q}(x+t_i)=\sum_{i=0}^{q-1}c_ix^i$, 随后根据困难问题实例设置 SM9-PAEKS 方案中的系统参数, $P_2=f(a)Q=\sum_{i=0}^{q-1}c_i(a^iQ), P_1=\psi(P_2)=f(a)P$, 设置发送方的公钥为 $pk_S=\sum_{i=1}^{q}c_{i-1}(a^iQ)=aP_2$, 上述过程中的 a 是未知的, 并且 $\psi(Q)=P$. 对于任意 $i\in[1,q]\backslash\{k\}$, 令 $f_i(x)=\frac{f(x)}{a+t_i}=\sum_{i=0}^{q-2}d_ix^i$, 可计算 $U_i=\sum_{i=0}^{q-2}d_i(a^iQ)=f_i(a)Q=\frac{f(a)}{a+t_i}Q=\frac{P_2}{a+t_i}$, 即对于任意的二元组 $(t_i,U_i), i\in[1,q]\backslash\{k\}$ 都是可计算的. 随后计算 $pk_R=-pk_S-B_kP_1=-(a+B_k)P_1$, 上述过程中隐式地设置了 $sk_S=y=a, sk_R=x=-(a+B_k)$. 然后, 选取一字节表示的私钥生成函数标识符 hid. 最后, 返回系统参数 $params=(P_1,P_2,g,N,hid)$.

● 哈希询问阶段. 此阶段, $\mathcal{A}$ 可适应性地选取关键词 $w_i\in\{0,1\}^*$ 向 $\mathcal{C}$ 进行如下两类哈希询问.

(1) H_1 询问: 为响应 $\mathcal{A}$ 的询问, $\mathcal{C}$ 维持列表 $L_1=<w_i,V_i,B_i>$, 如果询问项 $<w_i,V_i>$ 存在列表 L_1 中, 则按照列表中记录的 B_i 响应. 否则, 记 w_i 是第 i 个新关键词的询问. 设 $H_1(w_i\|hid\|V_i,N)=B_i$, 最终返回 B_i 并更新列表.

(2) H_2 询问: 针对 $\mathcal{A}$ 发起的二元组 $<C_i,u_i>$ 询问, $\mathcal{C}$ 维持列表 $L_2=<C_i,u_i,K_i>$, 如果询问项 $<C_i,u_i>$ 存在列表 L_2 中, 则按照列表中记录的 K_i 响应. 否则, $\mathcal{C}$ 随机选取 K_i, 设 $H_1(C_i\|u_i,klen)=K_i$ 同时更新 L_2.

● 询问阶段 1. 此阶段, $\mathcal{A}$ 可适应性地选取关键词 $w_i\in\{0,1\}^*$ 并向 $\mathcal{C}$ 进行如下两种询问.

(1) 关键词密文询问 O_{C_w}: 首先 $\mathcal{C}$ 查询 $\mathcal{A}$ 询问的关键词 w_i 是否在列表 L_1 中, 如果不存在, 则按照 H_1 询问阶段生成关键词对应的表项, 由于是 $\mathcal{C}$ 生成的表项, 其无法计算出 $V_i=[xy]P_1$, 因此记 $V_i=\star$. 如果 $i=k$, 输出失败. 否则 $\mathcal{C}$ 选取随机数 $r_i\in\mathbb{Z}_N^*$, 计算 $Q_{w_i}=[t_i]P_1+pk_R, C_1=r_iQ_{w_i}$, 随后按照 $PAEKS$ 算法生成关键词密文 $C_{w_i}=C_1\|C_3\|C_2$ 并返回给 $\mathcal{A}$. 与 SM9-PAEKS 方案中的关键词密文相比可知, O_{C_w} 响应的关键词密文与真实方案中的关键词密文是不可区分的.

(2) 关键词陷门询问 O_{T_w}: 首先 $\mathcal{C}$ 查询 $\mathcal{A}$ 询问的关键词是否在列表 L_1 中, 如果不存在, 则按照 H_1 询问阶段生成关键词对应的表项, 由于是 $\mathcal{C}$ 生成的表项, 因此其无法计算出 $V_i=[xy]P_2$, 故记 $V_i=\star$. 如果 $i=k$, 输出失败. 否则 $\mathcal{C}$ 可根据初始化阶段的 $B_i=B_k-t_i$, 计算 $\left(B_i,\frac{1}{x+B_i}P_2\right)$, 进而 $\mathcal{C}$ 可计算元组 $(B_i,P_2-B_iU_i)=\left(B_i,P_2-\frac{B_i}{x+B_i}P_2\right)=\left(B_i,\frac{x}{x+B_i}P_2\right)$. 最终, $\mathcal{C}$ 返回关键词陷门 $T_{w_i}=\frac{x}{B_i+x}P_2$. 分析 SM9-PAEKS 方案中的关键词陷门形式和谕言机 O_{T_w} 响应的形式可知, 从 $\mathcal{A}$ 的角度而言, 是不可区分的.

● 挑战阶段. $\mathcal{A}$ 决定结束上述询问后, 选取挑战关键词 $w_0^*,w_1^*\in\{0,1\}^*, |w_0^*|=|w_1^*|$, $\mathcal{C}$ 随机选取 $b\in\{0,1\}$, 如果 $w_b^*\neq w_k$, $\mathcal{C}$ 终止此次模拟, 否则选取随机数 $t^*\in\mathbb{Z}_N^*, K^*\in\{0,1\}^{klen}$, 计算 $C_1^*=-t^*P_1$, 若设 $r^*=\frac{t^*}{a}$, 由于系统设置阶段隐式地设置了 $x=-a-B_k$, 有 $C_1^*=-t^*P_1=-r^*aP_1=r^*(B_kP_1+pk_R)$. 随后, 按照 SM9-PAEKS 方案中的 PAEKS 算法生成 C_2^*,C_3^*. 最后返回关键词密文 $C_1^*\|C_3^*\|C_2^*$. 从 $\mathcal{A}$ 的角度而言, 挑战密文和真实密文是不可区分的, 即上述模拟过程和真正的方案攻击不可区分. 除非 $\mathcal{A}$ 询问过关于 $u^*=e(pk_R,P_2)^{r^*}$ 的值.

● 询问阶段 2. 在此阶段, $\mathcal{A}$ 可继续进行同询问阶段 1 的询问, 但是此处限制 $\mathcal{A}$ 询问的关键词 $w_i\notin\{w_0,w_1\}$.

● 猜测阶段. $\mathcal{A}$ 输出对挑战关键词密文中关键词的猜测, 若猜测正确 $\mathcal{A}$ 赢得上述游戏, 否则失败. $\mathcal{C}$ 可忽略 $\mathcal{A}$ 的猜测, 从 L_2 中选择元组 $<C_1,u,K_i>$, 选择的元组包含 u^* 的概率为 $1/q_{H_2}$. 由于 $\mathcal{A}$ 不可区分上述模拟与真实方案, 那么其将以不可忽略的优势询问 H_2 关于 u^* 的值.

根据上述分析, $\mathcal{C}$ 可通过如下方式解决困难问题实例:

$$\begin{aligned}u^*&=e(pk_R,P_2)^{r^*}=e(f(a)(-a-B_k)P,f(a)Q)^{\frac{t^*}{a}}\\&=e(P,Q)^{\frac{-f^2(a)at^*-f^2(a)t^*B_k}{a}}\\&=e(P,Q)^{-f^2(a)t^*-\frac{f^2(a)t^*B_k}{a}}\end{aligned}\tag{7}$$

由于其中 $f(a),t^*,B_k$ 都是已知的, 则有:

$$\begin{cases} f^2(a)t^* = \left(\sum_{i=0}^{q-1} c_i a^i\right) f(a)t^* \\ \dfrac{f^2(a)t^*}{a} = \left(\sum_{i=0}^{q-2} c_{i+1}a^i + \dfrac{c_0}{a}\right) f(a)t^* \\ \qquad\qquad = f(a)t^* \cdot \sum_{i=0}^{q-2} c_{i+1}a^i + \left(c_0 t^* \sum_{i=0}^{q-2} c_{i+1}a^i + \dfrac{{c_0}^2 t^*}{a}\right) \end{cases} \tag{8}$$

因此, 上述 u^* 可进一步表示为:

$$\begin{aligned} u^* &= e(-t^*P_1, f(a)Q)\cdot e(P,Q)^{-B_k\cdot(f(a)t^*\cdot\sum_{i=0}^{q-2}c_{i+1}a^i + c_0t^*\sum_{i=0}^{q-2}c_{i+1}a^i + \frac{{c_0}^2t^*}{a})} \\ &= e(t^*P_1, f(a)Q)^{-1}\cdot e(B_kt^*(P_1+c_0P), \sum_{i=0}^{q-2}c_{i+1}a^iQ)^{-1}\cdot e(P,Q)^{-\frac{B_k{c_0}^2t^*}{a}} \end{aligned} \tag{9}$$

可计算 q-BDHI 问题的解为:

$$e(P,Q)^{\frac{1}{a}} = (u^*\cdot e(t^*P_1, f(a)Q)\cdot e(B_kt^*(P_1+c_0P), \sum_{i=0}^{q-2}c_{i+1}a^iQ))^{\frac{-1}{B_k{c_0}^2t^*}} \tag{10}$$

概率分析: 根据上述证明过程有 $w_b^* = w_k$, 即 $\mathcal{A}$ 选择 w_k 作为挑战关键词的概率为 $1/q_{H_1}$. 若 $\mathcal{A}$ 能以不可忽略的优势 ϵ_1 攻破 SM9-PAEKS 方案的 CKA-CI 安全性, 则 C 解决 q-BDHI 困难问题的优势为:

$$Adv_C^{q\text{-BDHI}} \geqslant \epsilon_1 \cdot \frac{1}{q_{H_1}} \cdot \frac{1}{q_{H_2}} = \frac{\epsilon_1}{q_{H_1}q_{H_2}} \tag{11}$$

引理 1 证毕.

引理 2. 若 Gap-q-BCAA1 安全假设成立, 那么 SM9-PAEKS 具备 CKA-TI 安全性.

证明: 假设存在 $\mathcal{PPT}$ 敌手 $\mathcal{A}$ 能以不可忽略的优势攻破 SM9-PAEKS 方案的 CKA-TI 安全性. 则挑战者 C 可通过与 $\mathcal{A}$ 交互, 以不可忽略的优势解决 Gap-q-BCAA1 困难问题实例. C 输入困难问题实例 $\left(P_1, P_2, [x]P_1, t_0, \left(t_1, \left[\frac{x}{x+t_1}\right]P_2\right), \ldots, \left(t_q, \left[\frac{x}{x+t_q}\right]P_2\right)\right)$, 其中 $t_i \in \mathbb{Z}_N^*, i \in [0,q]$. C 可查询 DBIDH 谕言机 O_{DBIDH}, 其目标是计算 $e(P_1,P_2)^{\frac{x}{x+t_0}}$, C 与 $\mathcal{A}$ 的具体交互过程如下.

● 初始化阶段. C 根据 SM9-PAEKS 及困难问题实例设置系统参数 $(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,P_1,P_2)$, 令接收方公钥为 $pk_R = [x]P_1$, 随机选取 $y \in \mathbb{Z}_N^*$, 计算发送方公钥为 $pk_S = [y]P_1$. 然后, 选取一字节表示的私钥生成函数标识符为 hid. 最后, 返回系统公开参数.

● 哈希询问阶段. 此阶段, $\mathcal{A}$ 可适应性地选取关键词 $w_i \in \{0,1\}^*$ 向 C 进行如下两类哈希询问.

(1) H_1 询问. 为响应 $\mathcal{A}$ 的询问, C 维持列表 $L_1 =< w_i, V_i, t_i, T_i >$, 如果询问项 $< w_i, V_i >$ 存在列表 L_1 中, 则按照列表中记录的 h_i 响应. 否则, 记 w_i 是第 i 个新关键词的询问. 设 $H_1(w_i||hid||V_i,N) = t_i$, 最终返回 t_i 并更新 L_1. 令 $k \in [1,q+1]$, 若为 w_k 则记录 $T_k = \perp$, 否则记录每次的 $T_i = \left[\frac{x}{x+t_i}\right]P_2$.

(2) H_2 询问. 针对 $\mathcal{A}$ 发起的关于元组 $< C_i, u_i >$ 的询问, C 维持列表 $L_2 =< C_i, u_i, K_i >$, 如果询问项 $< C_i, u_i >$ 存在列表 L_2 中, 则按照列表中记录的 K_i 响应. 否则, C 随机选取 K_i, 并设 $H_2(C_i||u_i,\ klen) = K_i$, 同时更新 L_2.

● 询问阶段 1. 此阶段, $\mathcal{A}$ 可适应性地选取关键词 $w_i \in \{0,1\}^*$ 并向 C 进行如下两种询问.

(1) 关键词密文询问 O_{C_w}. 首先 C 查询 $\mathcal{A}$ 询问的关键词 w_i 是否在列表 L_1 中, 如果不存在, 则按照 H_1 询问阶段生成关键词对应的表项. 如果 $i = k$, 终止游戏. 否则 C 选取随机数 $r_i \in \mathbb{Z}_N^*$, 计算 $Q_{w_i} = [t_i]P_1 + pk_R, C_1 = r_iQ_{w_i}$, 并按照 PAEKS 算法生成关键词密文 $C_{w_i} = C_1||C_3||C_2$ 并返回给 $\mathcal{A}$. 与 SM9-PAEKS 方案中的关键词密文相比可知, O_{C_w} 响应的关键词密文与真实方案中的关键词密文是不可区分的.

(2) 关键词陷门询问 O_{T_w}. 首先 C 查询 $\mathcal{A}$ 询问的关键词是否在列表 L_1 中, 如果不存在, 则按照 H_1 询问阶段生

成关键词对应的表项. 如果 $i=k$, 输出失败 (记作事件 E_1). 否则, C 可将 L_1 中记录的 $T_i=\left[\frac{x}{x+t_i}\right]P_2$ 作为关键词陷门返回给 $\mathcal{A}$. 分析真实方案中的陷门和 O_{T_w} 响应的陷门, 从敌手的角度这是不可区分的.

● 挑战阶段. $\mathcal{A}$ 决定结束上述询问后, 选取挑战关键词 $w_0^*, w_1^* \in \{0,1\}^*, |w_0^*|=|w_1^*|$, 挑战者 C 随机选取 $b\in\{0,1\}$, 如果 w_b^* 未曾被询问过谕言机且 $T_i\neq\perp$, C 终止此次模拟 (记作事件 E_2). 否则选取随机数 $r^*\in\mathbb{Z}_N^*$, 计算 $T_{w_b^*}=r^*P_2$. 从 $\mathcal{A}$ 的角度而言, 挑战关键词密文和真实密文是不可区分的, 即上述模拟过程和真正的方案攻击不可区分的.

● 询问阶段 2. 在此阶段, $\mathcal{A}$ 可继续进行同询问阶段 1 的询问, 但是此处限制 $w_i\notin\{w_0,w_1\}$.

● 猜测阶段. $\mathcal{A}$ 输出对挑战关键词密文中关键词的猜测. 若猜测正确, 则 $\mathcal{A}$ 赢得上述游戏, 否则失败. 若对于 L_2 中的每个元组 $<C_i,u_i,K_i>$, C 可向谕言机 O_{DBIDH} 查询 $<[x]P_1,P_2,[t_0+x]P_1,r^*P_1,u_i>$. 如果 O_{DBIDH} 返回 1, 那么 C 输出 u_i^{1/r^*} 作为 Gap-q-BCAA1 困难问题实例的解. 如果不存在这样的元组 (记作事件 E_3), 那么 C 输出 $\mathbb{G}_T$ 中的随机元素作为解.

概率分析: 令 $\mathcal{A}$ 赢得上述游戏为事件 E_4, 根据上述分析有 $\Pr[E_4|E_3]=\frac{1}{2}$, 公式 (12) 成立:

$$\begin{cases}\Pr[E_4]=\Pr[E_4|E_3]\Pr[E_3]+\Pr[E_4|\overline{E_3}]\Pr[\overline{E_3}]\\ \qquad\leqslant\frac{1}{2}(1-\Pr[\overline{E_3}])+\Pr[\overline{E_3}]\\ \qquad=\frac{1}{2}+\frac{1}{2}\Pr[\overline{E_3}]\\ \Pr[E_4]\geqslant\Pr[E_4|E_3]\Pr[E_3]\\ \qquad=\frac{1}{2}\Pr[E_3]\\ \qquad=\frac{1}{2}-\frac{1}{2}\Pr[\overline{E_3}]\end{cases}\tag{12}$$

若 $\mathcal{A}$ 能以不可忽略的优势 ϵ_2 攻破 SM9-PAEKS 方案的 CKA-TI 安全性, 有 $\epsilon_2\leqslant|\Pr[E_4-\frac{1}{2}|\leqslant\frac{1}{2}\Pr[\overline{E_3}]$, 且根据上述游戏, 若 $\overline{E_2}$ 则有 $\overline{E_1}$. C 解决 Gap-q-BCAA1 困难问题实例的优势为

$$Adv_C^{\text{Gap-}q\text{-BCAA1}}\geqslant\epsilon_2\cdot\frac{1}{q+1}\tag{13}$$

引理 2 证毕.

综上, 通过引理 1 与引理 2 完成了对定理 1 的证明. SM9-PAEKS 具备 CI-CKA 和 TI-CKA 安全性.

4 性能分析

本节从理论分析和实验仿真测试两个角度对 SM9-PAEKS 与同类型经典方案进行比较, 所有方案均仅支持单关键词检索. 统计各方案时仅考虑耗时较高的运算. 为便于后文清晰地描述各方案性能, 令 $|C_w|$ 和 $|T_w|$ 分别表示关键词密文长度和关键词陷门长度, $|\mathbb{G}_i|(i\in\{1,2,T\})$ 表示群 $\mathbb{G}_i$ 中单个元素的长度, $|\mathbb{Z}_N^*|$ 表示单个 $\mathbb{Z}_N^*$ 元素的长度, $|PK|$ 表示用户公钥长度. T_{m1} 表示 $\mathbb{G}_1$ 中的单次标量乘运算, T_{m2} 表示 $\mathbb{G}_2$ 中的单次标量乘运算, T_b 表示单次双线性对运算, T_e 表示 $\mathbb{G}_T$ 上的单次模幂运算, T_{h2p} 表示哈希至椭圆曲线上的一点.

4.1 理论分析

各方案的计算开销 (如表 1 所示), 关键词密文生成阶段 SM9-PAEKS 仅需 3 次 T_{m1} 和 1 次 T_e, Huang 等人[15]的方案需要 1 次 T_{h2p} 和 3 次 T_{m1}, 而 Qin 等人[17]的方案需要 2 次 T_b 、2 次 T_{m1} 及 2 次 T_{h2p}; 关键词陷门生成阶段 SM9-PAEKS 仅需 1 次 T_{m1} 和 1 次 T_{m2}, 避免了高耗时的 T_b 运算, 而 Huang 等人[15]和 Qin 等人[17]的方案不仅需要 T_{m1} 还需 1 次 T_b; 对于匹配测试算法, SM9-PAEKS 仅需 1 次 T_b 运算, Huang 等人[15]的方案在此基础上增加 1 次 T_{h2p} 运算, 而 Qin 等人[17]的方案需要 2 次 T_b 运算.

在通信代价方面 (如表 1 所示), SM9-PAEKS 的关键词陷门长度为 $|\mathbb{G}_1|+2|\mathbb{Z}_N^*|$, Huang 等人[15]和 Qin 等人[17]的方案中的关键词陷门长度分别为 $2|\mathbb{G}_1|$ 和 $|\mathbb{G}_1|+|\mathbb{Z}_N^*|$. SM9-PAEKS 中关键词陷门长度为 $|\mathbb{G}_2|$, Qin 等人[17]的方案为

$|\mathbb{G}_1|$, 而 Huang 等人[15]的方案为 $|\mathbb{G}_T|$. 此外, 表 1 还列出了各个方案安全性所依赖的安全假设.

综合上述理论分析可知, SM9-PAEKS 与对比方案相比, 虽然在通信代价有所增加, 但其在计算开销上的性能有了一定的提升, 尤其是关键词陷门生成阶段的性能提升显著. 此外, 仅 SM9-PAEKS 是基于国密算法设计, 符合国家密码核心技术自主创新的发展战略和需求.

表 1 性能比较

方案	计算开销			通信代价			安全假设
	PAEKS	*Trapdoor*	*Test*	$\|PK\|$	$\|C_w\|$	$\|T_w\|$	
Huang等人[15]	$T_{h2p}+3T_{m1}$	$T_{m1}+T_b$	$2T_b$	$\|\mathbb{G}_1\|$	$2\|\mathbb{G}_1\|$	$\|\mathbb{G}_T\|$	DBDH、mDLIN
Qin等人[17]	$2T_{h2p}+2T_{m1}+2T_b$	$T_{m1}+T_{h2p}+T_b$	$T_{h2p}+T_b$	$\|\mathbb{G}_1\|$	$\|\mathbb{G}_1\|+\|\mathbb{Z}_N^*\|$	$\|\mathbb{G}_1\|$	CBDH、CDH
SM9-PAEKS	$3T_{m1}+T_e$	$T_{m1}+T_{m2}$	T_b	$\|\mathbb{G}_1\|$	$\|\mathbb{G}_1\|+2\|\mathbb{Z}_N^*\|$	$\|\mathbb{G}_2\|$	q-BDHI、Gap-q-BCAA1

4.2 实验测试

为了得到更加真实可信的比较结果, 本文在相同的实验环境下对各个方案进行了仿真实验测试. 具体实验环境为: HP 个人笔记本电脑、Windows 10 操作系统、CPU 为 i7-9750@2.59 GHz, 实验过程中使用 MIRACL 密码核心库 (https://github.com/miracl/MIRACL), 编程时选用 C++语言. 选用 $\mathbb{F}_{256}$ 上的 BN 曲线, 因此实验时 $\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$ 和 $\mathbb{Z}_N^*$ 中的单个元素长度分别为 64、128、384 和 32 字节.

首先分析实验过程中各方案的通信代价, 对于各个 PAEKS 方案而言, 本实验过程中关键词密文、关键词陷门以及总通信代价如图 2 所示. 由图 2 可知, SM9-PAEKS 的关键词密文长度因与 SM9 加密算法结构一致, 其长度为 192 字节, 略微高于对比的方案, Huang 等人[15]和 Qin 等人[17]方案中的关键词密文长度分别为 128 字节和 96 字节. SM9-PAEKS 的陷门长度和 Qin 等人[17]方案均为 64 字节, 而 Huang 等人[15]方案为 384 字节. Qin 等人[17]方案总通信代价最小, 为 160 字节, SM9-PAEKS 为 256 字节, 而 Huang 等人[15]方案总通信代价为 512 字节, 与对比方案中通信代价最低的 Qin 等人[17]相比, SM9-PAEKS 总通信代价增加了 96 字节. 然而与 Huang 等人[15]方案相比, SM9-PAEKS 的通信代价减少了 50%.

然后, 输入同一关键词并将各个方案中的算法运行 1000 次后取各算法单次耗时的平均值, 实验结果如图 3 所示. 由图 3 可知, 对于关键词密文生成算法, SM9-PAEKS 单次耗时为 62.71 ms, 而 Huang 等人[15]和 Qin 等人[17]方案分别耗时为 30.10 ms 和 264.77 ms. 对于关键词陷门生成算法, Huang 等人[15]和 Qin 等人[17]方案分别耗时 132.86 ms 和 137.03 ms, 而 SM9-PAEKS 仅需 30.77 ms, 与前两个方案相比耗时降低分别为 76.84% 和 77.55%, 可见在此阶段 SM9-PAEKS 的计算开销降低显著. 对于匹配算法 SM9-PAEKS、Huang 等人[15]和 Qin 等人[17]方案分别耗时为 120.48 ms、234.29 ms 和 124.36 ms. 对于总方案耗时而言, Huang 等人[15]和 Qin 等人[17]方案分别耗时 397.25 ms 和 526.16 ms, 而 SM9-PAEKS 仅需 213.96 ms, 与前两个方案相比耗时分别降低了 46.14% 和 59.34%.

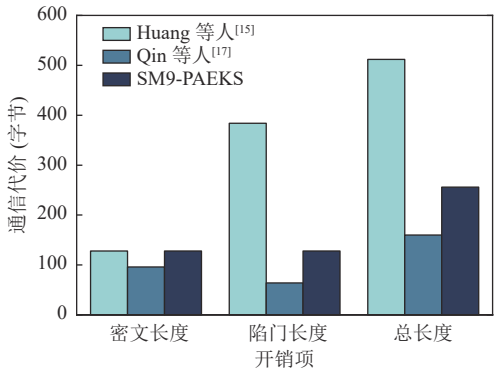

图 2 通信代价

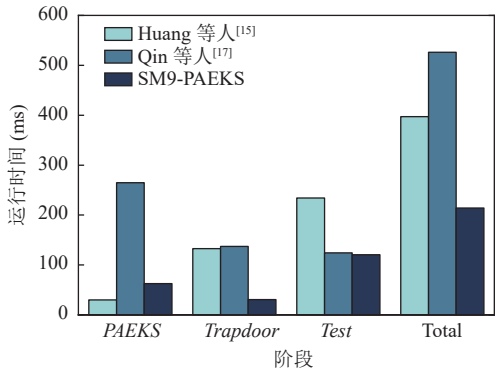

图 3 平均耗时

综上可知, SM9-PAEKS 与对比方案中通信代价最低的 Qin 等人方案[17]相比, SM9-PAEKS 通信代价增加 96 字节的情况下, 方案的总耗时降低了约 59.34%. 其中关键词陷门生成的耗时降低尤其显著, 约为 77.55%. 因此, SM9-PAEKS 提升了检索效率, 更适用于工业物联网、智能家居、智能穿戴等资源受限的设备. 最后, 为了更加全面地分析方案的性能, 本文在不同关键词个数的情况下, 对各个算法进行了多次测试以观察各算法随关键词个数变化时的时间开销变化情况, 实验结果如图 4 所示. 对比 Huang 等人[15]和 Qin 等人[17]方案的耗时增长情况, SM9-PAEKS 各算法在关键词个数增加的情况下, 算法耗时增长相对较平缓, 这主要得益于 SM9-PAEKS 方案中各算法涉及的高耗时运算较少.

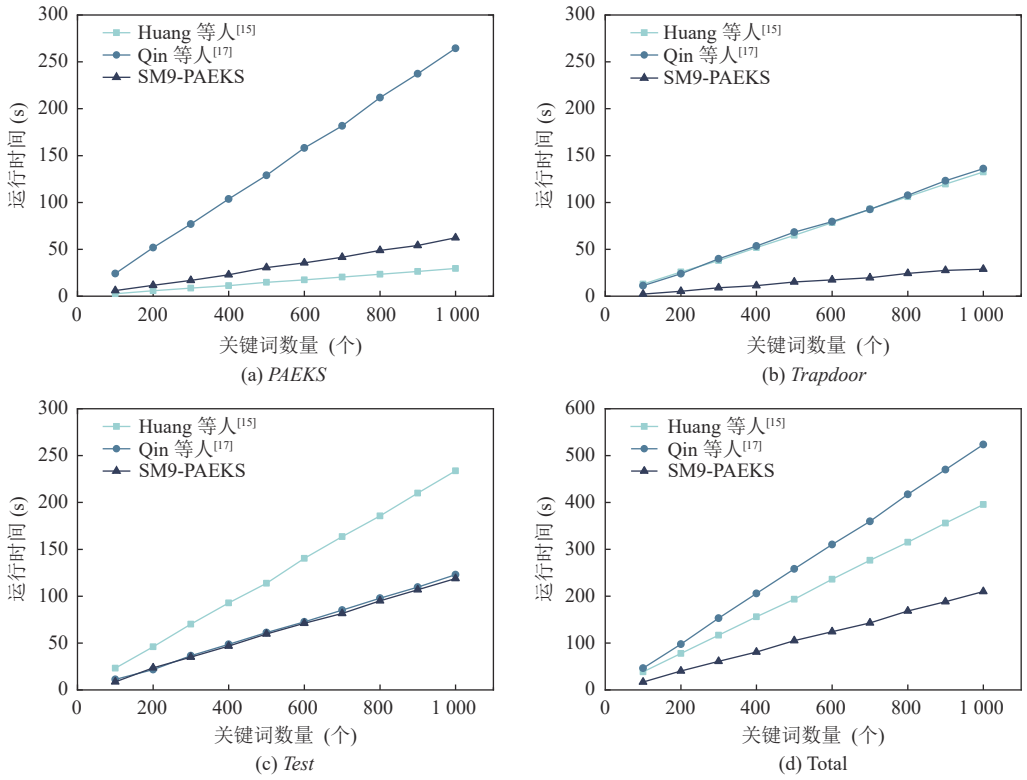

图 4 不同关键词数量下算法效率

5 总 结

本文从云存储系统的实用性和安全性出发, 以国产 SM9 加密算法为基础, 提出了 SM9-PAEKS 方案, 实现了国密算法在 PAEKS 的功能性扩展, 丰富了 SM9 密码算法的应用, 这是一个基于 SM9 的 PAEKS 方案. 本文在随机谕言模型下, 基于 q-BDHI 和 Gap-q-BCCA1 困难问题分别证明了 SM9-PAEKS 的关键词密文不可区分和关键词陷门不可区分性. 通过与经典 PAEKS 方案相比, 理论分析和大量实验仿真测试表明本文方案在牺牲较小通信代价且保证安全性的前提下, 方案的计算开销有了显著降低, 尤其是关键词陷门生成阶段. 本文的工作有助于国密算法功能性扩展, 同时可为云存储领域的数据加密与检索提供理论基础与技术支撑.

未来, 可围绕丰富搜索模式, 如探索支持单次多关键词、范围查询等检索方式的基于国密算法的 PAEKS 方案.

此外, 现有方案中云端服务器可能出于节省计算资源的目的, 返回错误检索结果对用户的权益造成损失, 因此未来还可考虑与区块链、智能合约、人工智能等技术结合实现功能更丰富、效率更优良的公平检索系统, 从而更有效保障双方权益.

References:

[1] Chuka-Maduji N, Anu V. Cloud computing security challenges and related defensive measures: A survey and taxonomy. SN Computer Science, 2021, 2(4): 331. [doi: 10.1007/s42979-021-00732-3]

[2] Zhou YH, Li N, Tian YM, An DZ, Wang LC. Public key encryption with keyword search in cloud: A survey. Entropy, 2020, 22(4): 421. [doi: 10.3390/e22040421]

[3] Yau WC, Heng SH, Goi BM. Off-line keyword guessing attacks on recent public key encryption with keyword search schemes. In: Proc. of the 5th Int'l Conf. on Autonomic and Trusted Computing (ATC 2008). Oslo: Springer, 2008. 100–105. [doi: 10.1007/978-3-540-69295-9_10]

[4] Jeong IR, Kwon JO, Hong D, Lee DH. Constructing PEKS schemes secure against keyword guessing attacks is possible? Computer Communications, 2009, 32(2): 394–396. [doi: 10.1016/j.comcom.2008.11.018]

[5] Song DX, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proc. of the 2000 IEEE Symp. on Security and Privacy (S&P 2000). Berkeley: IEEE, 2000. 44–55. [doi: 10.1109/SECPRI.2000.848445]

[6] Boneh D, Di Crescenzo G, Ostrovsky R, Persiano G. Public key encryption with keyword search. In: Proc. of the 2004 Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Interlaken: Springer, 2004. 506–522. [doi: 10.1007/978-3-540-24676-3_30]

[7] Goh EJ. Secure indexes. 2003. https://eprint.iacr.org/2003/216

[8] Abdalla M, Bellare M, Catalano D, Kiltz E, Kohno T, Lange T, Malone-Lee J, Neven G, Paillier P, Shi HX. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In: Proc. of the 25th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2005. 205–222. [doi: 10.1007/11535218_13]

[9] Byun JW, Rhee HS, Park HA, Lee DH. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data. In: Proc. of the 3rd VLDB Workshop on Secure Data Management. Seoul: Springer, 2006. 75–83. [doi: 10.1007/11844662_6]

[10] Park DJ, Kim K, Lee PJ. Public key encryption with conjunctive field keyword search. In: Proc. of the 5th Int'l Workshop on Information Security Applications (WISA 2004). Jeju Island: Springer, 2005. 73–86. [doi: 10.1007/978-3-540-31815-6_7]

[11] Tang Q, Chen LQ. Public-key encryption with registered keyword search. In: Proc. of the 6th European Workshop on Public Key Infrastructures, Services and Applications (EuroPKI 2009). Pisa: Springer, 2009. 163–178. [doi: 10.1007/978-3-642-16441-5_11]

[12] Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited. In: Proc. of the 2008 Int'l Conf. on the Computational Science and Its Applications. Perugia: Springer, 2008. 1249–1259. [doi: 10.1007/978-3-540-69839-5_96]

[13] Fang LM, Susilo W, Ge CP, Wang JD. A secure channel free public key encryption with keyword search scheme without random oracle. In: Proc. of the 8th Int'l Conf. on Cryptology and Network Security (CANS 2009). Kanazawa: Springer, 2009. 248–258. [doi: 10.1007/978-3-642-10433-6_16]

[14] Chen RM, Mu Y, Yang GM, Guo FC, Huang XY, Wang XF, Wang YJ. Server-aided public key encryption with keyword search. IEEE Trans. on Information Forensics and Security, 2016, 11(12): 2833–2842. [doi: 10.1109/TIFS.2016.2599293]

[15] Huang Q, Li HB. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. Information Sciences, 2017, 403–404: 1–14. [doi: 10.1016/j.ins.2017.03.038]

[16] Chen BW, Wu LB, Zeadally S, He DB. Dual-server public-key authenticated encryption with keyword search. IEEE Trans. on Cloud Computing, 2022, 10(1): 322–333. [doi: 10.1109/TCC.2019.2945714]

[17] Qin BD, Chen Y, Huang Q, Liu XM, Zheng D. Public-key authenticated encryption with keyword search revisited: Security model and constructions. Information Sciences, 2020, 516: 515–528. [doi: 10.1016/j.ins.2019.12.063]

[18] Li HB, Huang Q, Huang JY, Susilo W. Public-key authenticated encryption with keyword search supporting constant trapdoor generation and fast search. IEEE Trans. on Information Forensics and Security, 2023, 18: 396–410. [doi: 10.1109/TIFS.2022.3224308]

[19] Liu XG, Sun YY, Dong H. A pairing-free certificateless searchable public key encryption scheme for IoMT. Journal of Systems Architecture, 2023, 139: 102885. [doi: 10.1016/j.sysarc.2023.102885]

[20] Cheng LX, Meng F. Public key authenticated searchable encryption against frequency analysis attacks. Information Sciences, 2023, 640: 119060. [doi: 10.1016/j.ins.2023.119060]

[21] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data. In: Proc. of the 4th Theory of Cryptography Conf. (TCC 2007). Amsterdam: Springer, 2007. 535–554. [doi: 10.1007/978-3-540-70936-7_29]

[22] Shi E, Bethencourt J, Chan THH, Song D, Perrig A. Multi-dimensional range query over encrypted data. In: Proc. of the 2007 IEEE Symp. on Security and Privacy (S&P 2007). Berkeley: IEEE, 2007. 350–364. [doi: 10.1109/SP.2007.29]

[23] Xu P, Jin H, Wu QH, Wang W. Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack. IEEE Trans. on Computers, 2013, 62(11): 2266–2277. [doi: 10.1109/TC.2012.215]

[24] Li S, Xu MZ. Attribute-based public encryption with keyword search. Chinese Journal of Computers, 2014, 37(5): 1017–1024 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2014.01017]

[25] Chen BW, Xiang T, He DB, Li HW, Choo KKR. BPVSE: Publicly verifiable searchable encryption for cloud-assisted electronic health records. IEEE Trans. on Information Forensics and Security, 2023, 18: 3171–3184. [doi: 10.1109/TIFS.2023.3275750]

[26] Cheng ZH. Security analysis of SM9 key agreement and encryption. In Proc. of the 14th Int'l Conf. on Information Security and Cryptology (Inscypt 2018). Fuzhou: Springer, 2019. 3–25. [doi: 10.1007/978-3-030-14234-6_1]
[27] Lai JC, Huang XY, He DB, Wu W. Security analysis of SM9 digital signature and key encapsulation. Scientia Sinica Informationis, 2021, 51(11): 1900–1913 (in Chinese with English abstract). [doi: 10.1360/SSI-2021-0049]
[28] Qin BD, Zhang BX, Bai X. Mediated SM9 identity-based encryption algorithm. Chinese Journal of Computers, 2022, 45(2): 412–426 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2022.00412]
[29] Zhu LF, Li JG, Lai JC, Huang XY, Zhang YC. Attribute-based online/offline signature scheme based on SM9. Journal of Computer Research and Development, 2023, 60(2): 362–370 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.202220530]
[30] Peng C, He DB, Luo M, Huang XY, Li DW. An identity-based ring signature scheme for SM9 algorithm. Journal of Cryptologic Research, 2021, 8(4): 724–734 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000473]
[31] Pu L, Lin C, Wu W, He DB. A public-key encryption with keyword search scheme from SM9. Journal of Cyber Security, 2023, 8(1): 108–118 (in Chinese with English abstract). [doi: 10.19363/J.cnki.cn10-1380/tn.2023.01.08]
[32] Zhang C, Peng CG, Ding HF, Xu DQ. Searchable encryption scheme based on China state cryptography standard SM9. Computer Engineering, 2022, 48(7): 159–167 (in Chinese with English abstract). [doi: 10.19678/j.issn.1000-3428.0062771]
[33] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In: Proc. of the 2004 Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Interlaken: Springer, 2004. 223–238. [doi: 10.1007/978-3-540-24676-3_14]
[34] Chen LQ, Cheng ZH. Security proof of Sakai-Kasahara's identity-based encryption scheme. In: Proc. of the 10th IMA Int'l Conf. on Cryptography and Coding. Cirencester: Springer, 2005. 442–459. [doi: 10.1007/11586821_29]

附中文参考文献:

[24] 李双, 徐茂智. 基于属性的可搜索加密方案. 计算机学报, 2014, 37(5): 1017–1024. [doi: 10.3724/SP.J.1016.2014.01017]
[27] 赖建昌, 黄欣沂, 何德彪, 伍玮. 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(11): 1900–1913. [doi: 10.1360/SSI-2021-0049]
[28] 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(2): 412–426. [doi: 10.11897/SP.J.1016.2022.00412]
[29] 朱留富, 李继国, 赖建昌, 黄欣沂, 张亦辰. 基于商密 SM9 的属性基在线/离线签名方案. 计算机研究与发展, 2023, 60(2): 362–370. [doi: 10.7544/issn1000-1239.202220530]
[30] 彭聪, 何德彪, 罗敏, 黄欣沂, 李大为. 基于 SM9 标识密码算法的环签名方案. 密码学报, 2021, 8(4): 724–734. [doi: 10.13868/j.cnki.jcr.000473]
[31] 蒲浪, 林超, 伍玮, 何德彪. 基于 SM9 的公钥可搜索加密方案. 信息安全学报, 2023, 8(1): 108–118. [doi: 10.19363/J.cnki.cn10-1380/tn.2023.01.08]
[32] 张超, 彭长根, 丁红发, 许德权. 基于国密 SM9 的可搜索加密方案. 计算机工程, 2022, 48(7): 159–167. [doi: 10.19678/j.issn.1000-3428.0062771]

蒲浪(1998－), 男, 博士生, 主要研究领域为公钥可搜索加密, 应用密码学.

顾晶晶(1983－), 女, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为智能系统, 信息安全.

林超(1991－), 男, 博士, 副教授, CCF 专业会员, 主要研究领域为应用密码学, 区块链隐私保护.

何德彪(1980－), 男, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为应用密码学, 密码协议.

伍玮(1981－), 女, 博士, 教授, 主要研究领域为密码学, 信息安全.