对公钥可搜索加密中内部关键词猜测攻击的研究

魏忠凯[1], 张 茜[1], 刘晋璐[1], 秦 静[1,2]

[1]山东大学 数学学院 济南 中国 250100

[2]中国科学院信息工程研究所 信息安全国家重点实验室 北京 中国 100093

摘要 近年来, 随着云计算技术的发展和数据隐私保护的要求不断提高, 密码学作为保护信息安全的一种必要手段, 在生活中应用得越来越广泛。其中可搜索加密技术广受青睐, 因为它不仅能够保护用户数据的隐私性, 而且还可以实现用户对加密数据进行关键词搜索的功能。后续的很多研究者丰富了可搜索加密的功能和性质, 但是也还存在着关键词攻击等问题亟待解决。因为敌手一旦获得了关键词就会威胁到密文数据文件的安全, 而且也可能泄露数据接收者的搜索偏好和个人身份等隐私信息, 所以解决关键词猜测攻击问题是非常有意义而且十分重要的。目前对于抵抗外部敌手的离线关键词猜测攻击的研究已经日渐成熟, 但是对于抵抗内部敌手的离线关键词猜测攻击还有待进一步深化完善。

本文阐述了内部关键词猜测攻击的机理, 指出敌手可以进行内部关键词猜测攻击的主要原因在于云服务器可以得到关键词密文和陷门信息, 并且可以自由地做关键词密文和陷门信息的匹配测试。然后梳理了近年来抗内部关键词猜测攻击的常见解决方案, 主要包括使用双服务器模型、认证服务器模型、见证关键词模型、指定发送者模型、模糊关键词模型等五类解决方案, 并深入总结和比较了五类方案, 归纳出了解决内部关键词猜测攻击的一般思路, 并指出未来抵抗内部关键词猜测攻击将会成为公钥可搜索加密方案的一种基本属性, 要解决内部关键词猜测攻击就必须从服务器可以生成密文、获取陷门和独立运行测试算法三个方面入手, 最后提出了现阶段内部关键词猜测攻击需要解决的问题以及未来的三个研究思路, 能够为进一步解决公钥可搜索加密中的内部关键词猜测攻击问题有所帮助, 使得公钥可搜索协议真正为实际所用。

关键词 公钥可搜索加密; 内部关键词猜测攻击; 双服务器; 认证服务器; 见证关键词; 模糊关键词

中图法分类号 TP309.2 DOI 号 10.19363/J.cnki.cn10-1380/tn.2024.07.02

Research on Internal Keyword Guessing Attack in Public Key Searchable Encryption

WEI Zhongkai[1], ZHANG Xi[1], LIU Jinlu[1], QIN Jing[1,2]

[1] School of Mathematics, Shandong University, Jinan 250100, China

[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract In recent years, with the flourishing of cloud computing, data privacy receives more and more attention and cryptography is a widely used method in daily life to prevent data leakage. Searchable encryption can protect data from leaking and retain the search functionality over encrypted data simultaneously. Although there are many followed works on the expressive query and higher security, the keyword guessing attack(KGA)is one of the problems to be more explored. The keyword guessing attack makes adversaries infer the meaning of keyword ciphertext, so data privacy is compromised by leaking users' search preferences even the personal information of data receivers. Therefore, it is very meaningful and important to solve the keyword guessing attack problem. Specifically, pay more attention to how to solve the offline keyword guessing attack against internal adversaries under the fact that the research of resisting offline keyword guessing attacks against external adversaries has become mature gradually.

In this paper, we expound on the mechanism of an internal keyword guessing attack, that is, the cloud server can test whether the keyword ciphertext and the trapdoor match at will. Then, we summarize and compare the solutions against internal keyword guessing attack in recent years. More specifically, there are five kinds of solutions on the dual-server model, authentication server model, witness keywords model, designated sender model, and fuzzy keywords model respectively. Then, we point out that the general way to solve internal keyword guessing attacks is by hindering ability of the server to generate ciphertext, get trapdoor, and run test algorithms independently. Moreover, resistance to internal keyword guessing attack should be a basic attribute of the public key searchable encryption scheme. Finally, left problems on internal keyword guessing attacks and further works are discussed. It is helpful to further solve the internal keyword guessing attack problem in the public key searchable encryption, so that the public key searchable protocol is used in practice.

通讯作者: 秦静, 教授, 博士生导师, Email: qinjing@sdu.edu.cn。

本课题得到国家自然科学基金(No. 62072276, No. 61772311)资助。

收稿日期: 2022-07-19; 修改日期: 2022-11-14; 定稿日期: 2024-03-18

Key words public key searchable encryption; internal keywords guess attack; dual-server; authentication server; witness keywords; fuzzy keywords

1 引言

随着信息时代的日新月异, 人类产生和获取信息的速度、数量都呈现几何级暴涨。在今天这个信息大爆炸的时代, 拉开人与人之间差距的不再是信息的壁垒, 而是存储和处理海量信息的能力。云计算技术可以极大地提高人们存储和处理信息的能力, 实现了人们长期以来“把计算作为一种基础设施”的梦想。目前我们借助互联网技术尤其是 5G 通讯技术可以快速地将这些数据存储到具有强大数据存储和处理能力的云服务器上, 并且可以根据实际需求在云服务器端对数据进行处理[1-5]。

云计算技术的产生和发展弥补了用户本地存储能力和计算能力不足的缺陷, 这一技术在企业、政府和个人等领域应用越来越广泛, 但由于用户数据中可能具有隐私信息, 而云服务器又是由第三方控制的, 数据的安全和隐私问题就成了用户在使用云服务时的顾虑。而且近年来用户数据泄露的事件时有发生, 例如 2022 年根据识别盗窃研究中心的数据, 与 2021 年同期相比, 2022 年第一季度实际报告的违规事件数量增加了 14%, 达到 404 起。《中国云计算安全政策与法律蓝皮书》披露, 近年来, 云平台大规模数据泄露的安全事件不绝于耳, 无论对于云服务商的业务持续性保障, 还是用户自身的合法权益维护, 数据安全始终是政策立法必须优先解决的问题, 也是云安全中最为重要的内容。于是如何保护用户的数据隐私性便成为了一个研究热点, 云安全联盟已经指出: 在云上如果文件没有加密, 则此文件被认为已经丢失。密码学作为保护信息安全的一种必要手段, 可以用来保护用户的隐私信息。用户可以使用加密算法对海量数据进行加密处理然后上传服务器, 为了在大量数据中检索目标文件, 可以把密文全部下载, 在本地解密获得明文后进行检索, 但是这种方式违背了把数据存储在云上来减少本地存储和利用云服务器强大计算能力的初衷。如何既能够保证数据的隐私性, 又能够高效使用在云服务器上的数据? 可搜索加密技术[6-8]应运而生, 这一技术实现了用户在密文中检索目标文件的功能, 不仅能够保护用户数据的隐私性, 而且还可以对加密数据进行关键词搜索。

可搜索加密技术主要分为两种, 一类是对称可搜索加密技术(Searchable Symmetric Encryption, SSE), 于 2000 年由 Song 等人在文献[6]中提出, 另一类是公钥可搜索加密(Public-Key Encryption with Keyword Search, PEKS), 于 2004 年由 Boneh 等人在文献[7]中提出。本文主要研究公钥可搜索加密, 如图 1 所示, 公钥可搜索加密有数据发送者, 云服务器和数据接收者三个参与方, 主要有以下四个步骤:

(1)密文和索引生成: 数据发送者将明文数据提取关键词并建立明文索引, 然后利用数据接收者的公钥加密明文关键词生成密文索引, 并加密明文数据生成密文, 然后将密文和密文索引外包存储到云服务器上。

(2)陷门生成: 数据接收者利用自己的私钥和要搜索的关键词生成陷门, 并发送给服务器。

(3)进行搜索匹配: 云服务器进行陷门与密文索引的匹配计算, 如果匹配成功, 则返回给数据接收者密文索引对应的密文数据。

(4)密文解密: 数据接收者利用自己的私钥在本地进行解密。

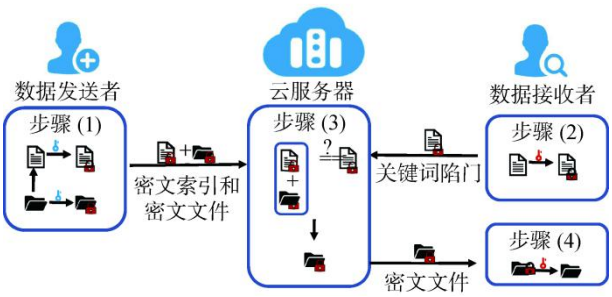

图 1 公钥可搜索加密的流程

Figure 1 The Processes in public key searchable encryption

公钥可搜索加密实现了数据接收者可以授权云服务器在加密文件中进行搜索的功能, 后来很多研究者不断丰富公钥可搜索加密的功能和性质, 其中一个重要的性质就是要能够抵抗外部敌手的离线关键词攻击, 目前对于抵抗外部敌手的关键词猜测攻击的研究已经日渐成熟, 但是对于抵抗内部敌手的关键词猜测攻击还有待完善。内部关键词猜测攻击(Inside Keyword Guessing Attack, IKGA)是指由内部敌手发起并通过猜测获取陷门中关键词信息的攻击方式。内部敌手是指诚实但好奇的云服务器(以及云服务器运营商), 即服务器会诚实地执行搜索协议, 但会尝试推断用户的关键词和隐私信息。敌手一旦获得了关键词就会威胁到密文数据文件的安全, 而且也意味着可能泄露了数据接收者的搜索偏好, 个

人身份等信息, 因此解决内部关键词猜测攻击问题是非常有意义而且重要的研究课题。

本文主要对PEKS方案中存在的IKGA问题展开研究, 按照时间顺序将抗IKGA的PEKS方案的发展历程划分为三个阶段, 如图2所示, 其中包括IKGA的问题提出, 解决IKGA问题的充分条件和近年来研究进展等内容, 侧重梳理了近年来使用双服务器模型, 认证服务器模型, 见证关键词模型和模糊关键词模型等5种抗IKGA的方法, 并讨论了现阶段解决IKGA需要解决的问题以及未来的研究思路。

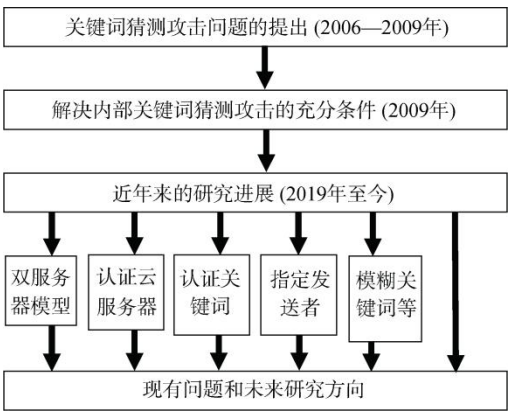

图 2　抗 IKGA 的 PEKS 方案发展历程

Figure 2　The development of PEKS that resist IKGA

2　内部关键词猜测攻击问题

本节重点围绕公钥可搜索加密的内部关键词猜测攻击问题介绍了其攻击机理, 攻击过程, 并总结了抗内部关键词猜测攻击的充分条件。

2.1　IKGA 问题的提出

2006年, Byun 等人[9]首先提出了对于公钥可搜索加密协议中的离线关键词猜测攻击问题, 并表明当可能的关键词数量受到某些多项式的限制时, 敌手容易发起离线关键词猜测攻击, 一些PEKS方案对关键词猜测攻击是不安全的。

在实际应用中, Byun 等人在文献[9]中指出, 用户通常会选取有具体含义的关键词, 使得关键词空间中常见的关键词数量有限信息熵比较小, 从而敌手有可能发起关键词猜测攻击。另外任何敌手都可以使用数据接收者的公钥生成关键词密文, 而且数据发送者、数据接收者和云服务器之间的通道是公开的, 敌手可以获得密文索引和数据接收者的陷门信息。如果敌手可以进行搜索匹配算法, 且密文索引与陷门匹配成功, 则陷门中的关键词和密文索引中关键词信息一致, 反之, 继续生成其他关键词信息进行匹配, 直到敌手匹配成功找到正确的关键词, 我们通常称之为离线关键词猜测攻击。

敌手也可以提前用数据接收者的公钥生成密文索引和密文文件一起发送给云服务器, 当数据接收者进行密文搜索时, 如果云服务器发送给数据接收者的密文中包含敌手生成的密文索引, 那么敌手就可以确认该数据文件中包含的关键词, 从而推断出数据接收者搜索的关键词, 这种攻击方式称之为在线关键词猜测攻击。以上两种攻击又非常容易由云服务器或者云服务器的管理者发起, 通常称之为内部关键词猜测攻击(IKGA)。如果攻击由服务器或者云服务器管理者之外的敌手发起, 则称之为外部关键词猜测攻击(OKGA)。

表 1　在线/离线关键词猜测攻击比较

Table 1　Comparison of online/offline keyword guessing attack

	提前生成密文索引	运行匹配算法	推断陷门信息时刻
在线关键词猜测攻击	需要	敌手不需要	云服务器返回给密文中含有敌手生成的密文时推断陷门信息
离线关键词猜测攻击	需要	敌手需要	密文索引与陷门匹配成功时陷门中的关键词和密文索引中关键词信息一致

敌手可以进行IKGA主要有两个原因: 首先, 敌手可以得到关键词密文和陷门信息。其次, 它可以自由地做关键词密文和陷门信息的匹配测试。离线模式下内部攻击者关键词猜测攻击[10]是由内部攻击者(一般为恶意服务器)执行的。攻击步骤为:

(1)在离线模式下, 内部攻击者首先确定攻击对象(数据接收者)。

(2)内部攻击者接收到目标接收者的关键词陷门 T 后, 准备想要执行猜测攻击的关键词 w, 借助目标接收方的公钥信息执行PEKS算法产生关键词密文 C_w。

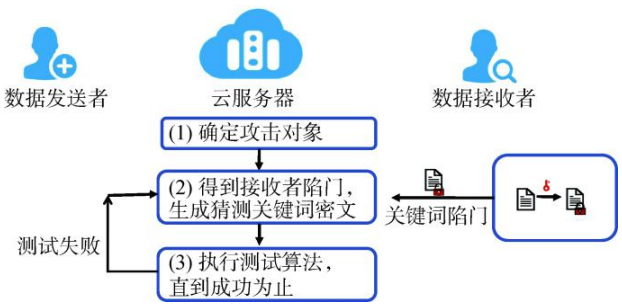

图 3　离线内部关键词猜测攻击流程

Figure 3　Processes in offline inside keyword guessing attack

(3)内部攻击者拥有了关键词陷门 T。以及关键

词密文C_w后, 执行测试实验, 直到攻击者猜测成功, 否则返回步骤(2)重新执行。

本文重点研究内部关键词猜测攻击, 因为内部敌手较之外部敌手具有更高的权限及合法性, 如果我们解决了内部关键词猜测攻击, 那么也能够解决外部敌手的攻击。另外内部关键词猜测攻击问题比较难以解决, 也是近年来的研究热点, 在未来抗内部关键词猜测攻击很可能成为 PEKS 方案的一个基本属性。

2.2 PEKS 中内部关键词猜测攻击过程

在文献[7]中 Boneh 等人的 PEKS 方案很容易受到内部关键词猜测的攻击, 本节我们展示下攻击过程。

2.2.1 PEKS 方案的定义

一个具有关键词搜索公钥可搜索加密方案主要有以下 5 个概率多项式时间算法构成。

(1)SysGen(1^γ): 系统参数生成算法, 输入安全参数1^γ, 输出系统参数 sp。

(2)KeyGen(sp): 密钥生成算法, 输入系统参数 sp, 输出数据接收者的公钥和私钥(pk, sk)。

(3)PEKS(sp, pk, w): 加密算法, 输入系统参数 sp, 关键词信息 w, 数据接收者公钥 pk, 输出关键词密文信息 CT_w=$E(sp, pk, w)$。

(4)Trapdoor(sp, sk, w'): 陷门生成算法, 输入系统参数 sp, 要搜索的关键词信息 w', 数据接收者的私钥 sk, 输出陷门信息 $T_{w'}$=Trapdoor(sp, sk, w')。

(5) Test(sp, CT_w, $T_{w'}$, pk): 匹配算法。输入系统参数 sp, 关键词密文信息, CT_w=E(sp, pk, w), 陷门信息 $T_{w'}$, 数据接收者公钥 pk。如果 $w = w'$, 输出是; 如果 $w \neq w'$输出否。

定义 1

若对于(pk, sk)=KeyGen(sp), 满足以下条件, 则称公钥可搜索加密方案是正确的。

(1)对于任意的 $w \in W$(关键词空间), 等式 Decrypt(E(w, pk), sk)=w 不成立的概率是可以忽略的。

(2)对于任意密文 C, Decrypt(C, sk)=w, 当且仅当 Test(sp, CT_w, $T_{w'}$, pk)=1。

第一条是要保密文的可解性; 第二条是保证对关键词密文搜索的正确性。

2.2.2 对 BDOP-PEKS 方案中 IKGA 的分析

假设云服务器是诚实但又好奇的, 为了恢复包含在陷门T_w中的关键词, 云服务器从关键词空间中选择一个关键词候选项 w', 并运行匹配算法, 测试w'是否等于T_w中包含的关键词 w, 关键词猜测攻击的工作原理如下[9]:

(1)假设数据接收者希望在加密的文档上搜索一些关键词, 它根据关键词计算一个陷门T_w, 并给服务器进行搜索。

(2)服务器将开始进行穷尽性搜索, 它从关键词空间中选择一个新的关键词候选项 w, 运行 PEKS 算法对 w 进行加密, 设密文为 C, 然后, 它在输入 C 和 T_w(以及接收方的公钥)上运行测试算法。如果算法输出 0, 则服务器选择另一个候选关键词并再次重复上述操作。否则, 服务器知道接收方想要搜索包含关键词 w 的文档。由于实际应用程序中的关键词空间通常不是那么大, 因此服务器将能够在相当短的时间内完成关键词猜测攻击。

2.3 解决 IKGA 问题的充分条件

Jeong 等人[11]提出构造一个抵抗内部攻击者的 PEKS 方案是不可能的, 因为关键词的数量是多项式级数, 又必须满足 Aballda 等人[12]方案中 PEKS 的一致性原则, 一致性即密文关键词和陷门是一一对应的, 意味着关键词的不安全性。

2009 年, Rhee 等人[13]证明了抗内部关键词猜测攻击的充分条件同时满足密文关键词不可区分性(Ciphertext Keyword Indistinguishability, CKI)和陷门信息不可区分性(Trapdoor Indistinguishability, TI), 其中 CKI 是保证敌手无法辨别区分出敌手要挑战的两个关键词的密文信息, 而 TI 则是为了保证敌手无法区分出敌手将要挑战的两个关键词的陷门信息。对 PEKS 方案而言, 如果方案能够抵抗内部攻击者的猜测攻击, 那么也一定能够抵抗外部攻击者的猜测攻击。

2.3.1 关键词密文不可区分

为了刻画 PEKS 的密文关键词的不可区分性, 我们考虑一个挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$ 之间的游戏(Game1), 最后要求敌手赢得游戏的优势 ε 是可以忽略的。敌手赢得游戏的优势定义为:

$$\varepsilon = Adv_A(k) = \left| \Pr[b = b'] - \frac{1}{2} \right|$$

Game1 游戏的具体步骤如下:

(1) 系统建立: 挑战者运行 KeyGen 算法成数据接收者的公私钥对(pk, sk), 并将其公钥 pk 公开。

(2) 阶段 1: 敌手可以像 Game1 一样自适应地询问预言机O_T, O_C多项式次。

其中O_T: 输入关键词 w, 预言机根据数据接收者的(pk, sk)计算相应陷门T_w, 并发送给敌手陷门信息T_w。

O_C: 输入关键词 w, 预言机根据数据接收者的(pk, sk)计算相应关键词密文C_w, 并发送给敌手关键

词密文C_w。

(3)挑战: 在某个时刻, 敌手发送两个没有询问过预言机的关键词 w_0, w_1 作为挑战信息给挑战者。挑战者随机选取 $b\in\{0, 1\}$将 C_{w_b}=PEKS(w_b, pk)发送给敌手。

(4)阶段 2: 敌手可继续阶段 1 的询问。但是不可以询问预言机关键词 w_0, w_1。

(5)猜测: 最终, 敌手将停止询问并输出猜测值 $b'\in\{0, 1\}$。

2.3.2 陷门信息不可区分

为了刻画PEKS的陷门信息不可区分性, 我们考虑一个挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$ 之间的游戏(Game2), 最后要求敌手赢得游戏的优势 ε 是可以忽略的。

敌手赢得游戏的优势定义为

$$\varepsilon=Adv_A(k)=\left|\Pr\left[b=b'\right]-\frac{1}{2}\right|$$

Game2 游戏的具体步骤如下:

(1)系统建立: 挑战者运行 $KeyGen$ 算法成数据接收者的公私钥对(pk, sk), 并将其公钥 pk 公开。

(2)阶段 1: 敌手可以自适应的询问预言机O_T, O_C多项式次。

(3)挑战: 在某个时刻, 敌手发送两个没有询问过预言机的关键词w_0, w_1作为挑战信息给挑战者, 挑战者随机选 $b\in\{0, 1\}$, 将 T_{w_b}=Trapdoor(w_b, sk)发送给敌手。

(4)阶段 2: 敌手可继续阶段 1 的询问, 但是不可以询问预言机关键词 w_0, w_1。

(5)猜测: 最终, 敌手将停止询问并输出猜测值 $b'\in\{0, 1\}$。

3 抗 IKGA 的 PEKS 方案的研究现状

本节将介绍抗 IKGA 的 PEKS 方案的研究现状, 重点介绍抗IKGA的五种主要方案: (1)双服务器模型; (2)认证服务器模型; (3)见证关键词模型; (4)指定发送者模型; (5)模糊关键词模型。

3.1 双服务器模型

2016 年, Chen 等人[14]首先使用双服务器模型来改进PEKS方案, 该方案把云服务器分为前向服务器和后向服务器, 使用两台云服务器协同完成数据存储和关键词密文与陷门的匹配检测, 两台云服务器分别接收来自于接收者发送的两部分陷门信息, 将测试算法分为两步进行, 使得任何一个单独的服务器都不能独立运行陷门和索引的测试算法, 内部敌手也就不能得到陷门和关键词密文之间的对应关系, 可以有效抵御 IKGA。

在双服务器的公钥可搜索加密协议模型中, 有四个参与者, 数据发送者, 数据接收者, 前向云服务器和后向云服务器, 如图所示。

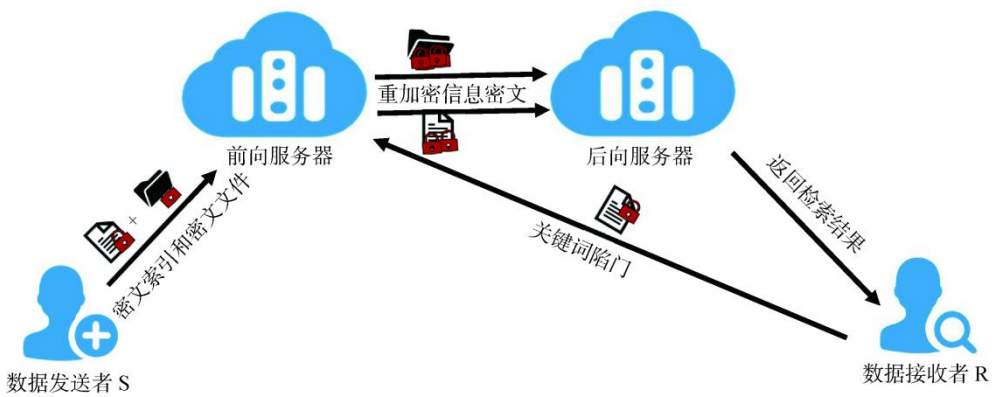

图 4 云存储中基于双服务器的公钥可搜索加密技术

Figure 4 Dual-Server Public-Key encryption with keyword search for secure cloud storage

具体过程:

(1)与传统公钥可搜索加密协议相同, 数据发送者使用标准的公钥加密系统对消息 m 进行加密获取消息密文 $C_{m,1}$。数据发送者使用数据接收者公钥pk_r, 前向服务器公钥 $pk_{s,1}$ 和后向服务器公钥 $pk_{s,2}$, 加密 w_i; 获取关键词密文 $C_{m,1}$; 关键词w_i与消息 m 相互关联, 然后上传密文 $C_{m,1}\|C_{w,i}$到前向云服务器。

(2)前向云服务器加密密文 $C_{m,1}$得到重加密密文 $C_{m,2}\|C_{w,i}$, 数据接收者使用其私钥 sk, 生成待搜索的关键词陷门T_w, 并上传T_w到前向云服务器中。

(3)前向云服务器使用陷门T_w和关键词密文 $C_{w,i}$来计算中间匹配结果C_T, 后向服务器利用C_T输出最后匹配结果。如果两者的关键词相等, 则发送给接收者的消息密文 $C_{m,2}$; 否则它返回 0。

(4)数据接收者解密密文得到 m, 在整个搜索过程中, 云服务器得不到任何关于关键词 w 和消息 m 的信息。

利用双服务器模型, 无论是对于外部敌手的离线关键词攻击, 还是对于内部敌手的离线关键词攻击, 以及在线的关键词猜测攻击都可以抵抗关键词猜测攻击。在数据安全方面, 协议达到数据文件的选择明文攻击的不可区分性安全和选择关键词攻击的不可区分性安全、陷门的不可区分性安全。

Chen 等人[15-16]的方案使用两个云服务器来防止 IKGA, 其中两个服务器不相互勾结。不幸的是, 文献[15]和文献[16]的工作是不安全的, 主要原因是他们的方案缺乏身份验证属性[17-19], 敌手可以生成一个有效的陷门来搜索加密数据。并且工作[16]需要一个可信的第三方来帮助用户生成预处理的关键词。

虽然双服务器的 PEKS 是 IKGA 的成功解决方案, 但系统中的两个服务器与处理关键词的功能有关, 所以它们不是独立的。因此, 在许多情况下, 很难保证两个服务器不会串通。此外, 在工作[19]中, 提出了一种新的 PEKS 方案来利用授权令牌来抵抗 KGA, 但是, 该方案需要数据所有者和数据用户之间的额外交互。

2022 年, Chen 等人[20]提出抵制内部关键词猜测攻击很可能成为所有新的 PEKS 方案的一个基本属性。他们定义了使用密钥搜索(DPAEKS)的双服务器公钥认证加密的概念, 通过利用两个不合作的服务器来保护 IKGA, 并支持身份验证属性, 提供了一个没有双线性配对的 DPAEKS 的结构, 该方案具有较高的效率和较强的安全性, 与 Chen 等人[14]使用的双服务器方法相比, 思路不同。在文献[14]中, 测试功能被分为两个部分, 用于两个独立的云服务器。这两个云服务器的公钥都用于生成密文和陷门。而 DPAEKS 中的这个想法是受到了经典的迪菲-赫尔曼密钥交换算法的启发, 每个关键词的密文生成和陷门生成不仅需要两个服务器的公钥, 还需要数据所有者和数据用户之间的共享密钥, 这确保了只有经过身份验证的用户才能搜索密文。

DPAEKS 采用了一个双服务器框架, 其中测试功能被分为两部分, 由两个独立的服务器处理. 没有一个服务器可以进行独立的测试。假设这两个服务器没有串通, 就可以实现抵抗 IKGA 的安全性。虽然可以通过引入更多的服务器来提高 DPAEKS 的安全性, 但多服务器方案可能存在较高的通信复杂度, 双服务器框架被认为是安全性和效率之间的一种权衡。

安全模型规定, 两台云服务器不能合谋。但是不能解决外部敌手的在线关键词猜测攻击, 而且实现起来比较复杂, 所以不适合应用于实际场景。

表 2 双服务模型的方案比较

Table 2 Scheme comparison of dual service model

方案	需要可信第三方	支持身份验证	需要额外交互
Chen 等[14]	×	×	×
Chen 等[15]	√	×	×
Chen 等[18]	×	×	√
Chen 等[20]	×	√	×

3.2 认证服务器模型

2015 年, Shao 等人[21]对云服务器是否完全安全可信提出了质疑, 提出了 IND-KGA-SERVER 的安全性, 其方案以指定测试人员进行关键词搜索(dPEKS)的方案[22]为基础, 利用了数字签名技术, 并引入了第三方认证机构(Certificate authority, CA), 以保护关键词信息的隐私性, 从而实现了抗内部关键词猜测攻击。

方案的设计思想如下: 当 dPEKS 的密文 C 由服务器自己生成时, 不应该再允许它运行 dTest 算法。为实现这个目标, 该文在 CA 中引入了确定性签名。在 dPEKS 方案中, 服务器输入其密钥作为 dTest 算法的参数, 该文要求 dPEKS 密文的发送者通过使用确定性签名方案来附加他的 ID 的签名。但是, 在不安全的通道中, 服务器可以捕获其他发件人发送的消息, 并获取 ID 签名。然后, 服务器构建一个消息, 其中密文是由他自己生成的, 但 ID 签名是其他发送者的, 因此, 服务器仍然可以成功地作弊。为解决这个问题, 我们应该要求发送方在其发送到 dTest 算法的消息上进行签名。因此, 新消息包括密文、ID 签名以及密文和 ID 签名的签名。我们应该注意的是, 这个签名方案不同于对于 ID 信息的签名方案, 而且为了安全起见, 它应该是概率性的。接收方与 CA 交互, 获得服务器的真实 ID 以及服务器的其他身份信息和密钥对之间的关系。他使用 RSA 签名在服务器的真实 ID 上进行签名, 并将此签名和服务器的真实 ID 视为陷门的一部分。当运行 dTest 时, 第一件事是检查概率签名, 如果签名无效, 它将中止. 否则, dTest 通过使用确定性签名 sig2 和作为算法输入参数一部分的服务器密钥来计算服务器真实 ID 上的 RSA 签名。然后, 他检查这个签名是否等于从发送方收到的签名。如果它们相等, 这意味着发件人是服务器, 因此阻止服务器运行 dTest. 如果两个签名不相等, 则会出现两种情况。第一种情况是发送者确实不是服务器, dTest 应该正常运行. 第二种情况是服务器是发送者, 但他生成了一个假 ID, 以表明他不是服

务器, 但是, 由于RSA签名的确定性特性, 他成功作弊的概率可以忽略不计, CA 的权威使得恶意服务器不可能进行作弊。从上面我们可以看到, 文章的解决方案是基于 CA 的权威, RSA 签名的确定性属性, 以及服务器提供他的密钥作为算法 dTest 的输入参数的事实, 但是该方案构造复杂, 并且运行效率不够高, 还有待进一步改进。

2016 年, Xie 等人[23]提出了一种有效的密文检索方案, 采用指定的测试者身份(dCRKS)的方案, 可以抵抗 IKGA, 首先建立一个新的密文检索系统框架, 关键词密文的生成涉及到安全服务器的私钥, 因此, 服务器不能为任何关键词生成有效的密文。因此, 服务器无法在 KGA 内部启动。其次, 与 Jiang 的方案[24]相比, 在该方案中删除了 TTP(可信的第三方)。因此, 该方案可以在没有 TTP 帮助的情况下实现抵抗内部攻击。此外, 只有一个指定的服务器才能测试给定的陷门是否匹配关键词密文, 该方案可以实现更强的安全性。最后, 执行分析表明, 该方案在测试和陷门的生成方面更有效。

2017 年, Wang 等人[25]提出了一个基于 ID 的多用户可搜索加密(IDB-MUSE)方案, 其中索引和搜索陷门是恒定的大小, 为了提高搜索效率, 文中将陷门的计算分为两个阶段, 即离线阶段和在线阶段。将 IDB-MUSE 的安全模型形式化, 其中正式定义了对选择关键词攻击(IND-sMID-CKA)不可区分性、对内部关键词猜测攻击不可区分性(IND-sMID-IKGA)和对内部身份猜测攻击不可区分性(IND-sMID-IIDGA)的安全概念。它允许一个点对点组中的多个社交网络用户在云中共享和搜索私有数据。在 IDB-MUSE 方案中, 只有授权的云用户, 即身份标识为生成索引输入的云用户才能搜索和访问共享组数据。基于此 IDB-MUSE 方案, Wang 等人提出了一种隐私保护数据搜索和共享协议, 该协议实现了源真实性、访问控制、数据隐私、搜索模式隐私、匿名性和搜索请求不链接性。由于固定的大小指数和搜索请求, 以及在陷门生成中的轻量值计算, 该方案适用于无线应用。但是 ID-MUSE 方案没有考虑用户的撤销。考虑到上述局限性, 学者们因此开始研究构建仅对某些密文有效的陷门的方法。

2019 年, Zhu 等人[26]提出了一种安全的数据共享方案, 结合 PKE 方案和 PEKS 方案, 提供关键词搜索和文档加密和解密功能。设计思路是为云服务器生成了一个密钥对, 只有指定的服务器才能通过加密的文档来搜索关键词, 以增强安全性。此外, 方案还满足了搜索结果的公共可验证性, 其中包括关键词和文档密文的正确性和完整性。由于数据接收者的数量增加会降低该方案中系统的有效性, 还需要进一步考虑在多数据接收者场景下构建一个 DSS 方案。

3.3 见证关键词模型

3.3.1 指定密文的 PEKS

2017 年, Andola 等人[27]提出了一种基于随机数的方案, 即在数据接收者和数据发送者之间共享一个随机数, 生成索引和陷门都需要这个相同的随机数, 就可以防止服务器内部敌手生成有效的索引, 从而抵抗 IKGA。

表 3 认证服务模型的方案比较

Table 3 Scheme comparison of authentication service model

方案	需要可信第三方	优点	缺点
Shao 等[21]	√	实现了抗内部关键词猜测攻击	构造复杂, 并且运行效率不够高
Xie 等[23]	×	实现更强的安全性, 在测试和陷门的生成方面更高效	没有考虑用户的撤销与多用户场景
Wang 等[25]	×	允许一个点对点组中的多个社交网络用户在云中共享和搜索私有数据	没有考虑用户的撤销
Zhu 等[26]	×	满足了搜索结果的公共可验证性	没有考虑在多数据接收者场景

在所提出的方案中, 所涉及的实体分别是数据发送者、服务器和数据接收者。过程如图 5 所示, 其主要思想如下:

(1)数据接收者选择一组需要为其发送秘密信息的数据发送者, 并秘密发送一组特定的随机数给数据发送者。并且发送一次随机数就够了, 在后续传输

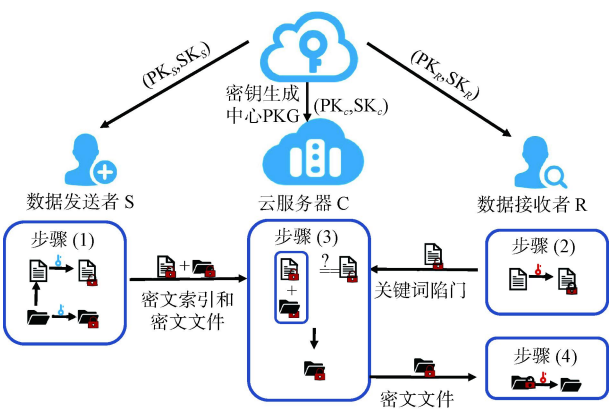

图 5 基于见证的可搜索加密

Figure 5 Witness-based searchable encryption

信息过程中, 数据接收者将不必为发送方和接收方之间的每次通信发送这个信息。

(2)当一个数据发送者要给数据接收者发送消息时, 他就会用数据接收者提供的随机数来修改该关键词, 使用接收者的公钥加密形成密文, 并将关键词密文和密文一起发送到服务器。

(3)数据接收者用一个特定的关键词和一个相同的随机数形成一个陷门, 最后用服务器的公钥对陷门进行加密, 并将其提供给服务器。

(4)服务器匹配关键词密文和陷门当中的关键词是否相同, 如果是, 云服务器将对应的密文发送给数据接收者。如果不是则继续匹配直至相同。

2017 年, Ma 等人[28]引入了一种新的密码学原语, 称为“基于见证的可搜索加密”, 其中只有当密文与陷门有见证关系时, 陷门才有效。该方案具有密文不可区分性、陷门不可区分性和用户见证等特性, 可以解决 IKGA 问题。此外, 该方案既支持模糊关键词搜索, 又支持多关键词搜索, 因此更加实用, 可以应用于一般的公共网络。尽管这些方案有其优点, 但它们要求数据发送者与数据接收器进行交互, 此外, 它们会带来额外的通信成本, 并且不适用于许多场景。

2021 年, Liu 等人[29]提出 DCSE(Designated-ciphertext searchable encryption)方案, 即指定密文可搜索加密方案, DCSE 中的每个陷门都被指定为一个特定的密文, DCSE 就是通过生成密文的标签, 把陷门和密文索引通过标签建立了联系, 服务器没有私钥打不开标签, 也就看不到密钥, 从而不能生成假密文索引和标签, 因此恶意的内部人员不能执行 IKGA。文章进一步提出了一种采用基于身份的加密和密钥封装机制的通用 DCSE 结构, 其本质是把陷门和密文索引通过标签建立了联系。因为服务器没有私钥打不开标签, 也就看不到密钥, 从而不能生成假密文索引和标签, 解决了 IKGA。

具体过程如图 6 所示, 发送者首先执行 DCSE(pk, w_i), 将关键词w_i生成一组密文C_i和密文的标签v_i, 标签中含有一些隐私信息, 其中 pk 是接收者的公钥。并且只有指定的接收者才能够从标签中提 取出来隐私信息, 这些标签和相应的密文是相关联的。发送者公开把标签v_i发送给使用者。接收者首先用自己的私钥 sk 从标签v_i中提取隐私信息 k, 然后用 k 和要查询的关键词w_i产生陷门t_i, 陷门就可以看成专门为指定密文设计的, 然后接收者发送(v_i, t_i) 给云服务器进行搜索。根据陷门, 云服务器返回匹配的文件给接收者, 因为云服务器不能随机选择关键词生成有效的关键词密文来匹配陷门, 所以云服务器不能够知道数据接收者正在搜索的关键词是什么。

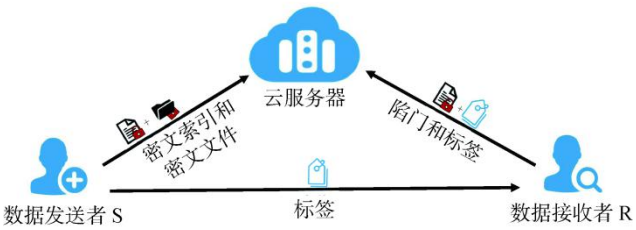

图 6 DCSE 的流程

Figure 6 The processes of DCSE

3.3.2 注册关键词的 PEKS

2010 年, Tang 等人[30]利用关键词注册技术, 提出了 PERKS(Public-key Encryption with Registered Keyword Search)方案, 它要求发送者先向接收方注册一个关键词, 然后才能为其生成一个关键词密文。换句话说, 在这个新的原语中, 接收方必须定义发送方可以为生成标签的关键词子集。

在 PEKS 的定义中, PERKS 方案涉及以下实体: 发件人、接收方和服务器。在形式上, 一个 PERKS 方案由以下多项式时间算法组成:

KeyGen(k): 由接收方运行, 该算法以一个安全参数 k 作为输入, 生成一个公钥和私钥对 (A_{pub}, A_{priv})。接收方还生成基数 N 的公共关键词集 W, 其中 $N\geqslant 2$ 是一个整数, 每个关键词都是一个二进制字符串。

KeywordReg(A_{priv}, W): 由接收方运行, 该算法以A_{priv}和一个关键词 W 作为输入, 并输出一个预密文的S_w。

PEKS(A_{priv}, W, S_w): 由发送方运行, 该算法以 A_{pub}、关键词 W 和预密文S_w作为输入, 并输出密文S_w。

Trapdoor(A_{priv}, W): 由接收方运行, 该算法以 A_{priv}和一个关键词 W 作为输入, 并输出一个陷门 T_w。

Test(A_{pup}、S_w、$T_{W'}$): 由服务器运行, 该算法以 A_{pub}、S_w、$T_{W'}$为输入, 如果 W=W'则输出 1, 否则为 0。

PERKS 的语义安全定义已经涵盖了所有潜在的敌手(包括一个好奇的服务器)但是接收方必须参与将注册的关键词发送给发送方, 并且发送方不能在没有事先与接收方交互的情况下自由选择关键词。显然, 关键词预注册是一个缺点, 计算复杂度比较高。

3.3.3 PAEKS

2017 年, Huang 和 Li 引入 PAEKS 的概念[31], 针对 PKES 中不能解决内部关键词猜测攻击的问题, 提出引入发送者私钥sk_s对关键词进行加密时认证的方法, 有效地阻止了云服务器能够独立地生成关键词密文, 从而是的内部敌手不能够进行内部关键词猜测攻击。它的安全模型可以充分满足密文关键词不可区分(CI)和陷门信息不可区分(TI)。在这个密码学原语中, 数据发送者不仅生成密文, 而且可以实现对密文进行身份验证, 而且数据接收者生成的陷门仅对由特定数据发送者进行身份验证的密文有效。因此, 云服务器无法执行 IKGA, 此外, 由于同样的原因, 云服务器也不能从接收者的搜索模式[32]中获得任何关键词信息, 因为云服务器不能生成密文来测试它的猜测。此外, 许多 PAEKS 方案[33-34]已经被制定出来, 以进一步应用于物联网以及云计算环境中。

与 PEKS 一样, PAEKS 也有三方: 数据发送方、数据接收方和服务器。算法与 PEKS 中的参与方相同, 只是 PEKS 加密算法现在需要发送方要输入自己的私钥, 而陷门生成算法和测试算法也需要发送方的输入自己的公钥, 在形式上, 我们考虑以下定义。

定义 2

一个基于关键词搜索的公钥认证加密(PAEKS)方案由以下多项式时间算法组成。

(1) SysGen(1^γ):系统参数生成算法, 输入安全参数1^γ, 输出系统参数 sp。

(2) KeyGen(sp) :密钥生成算法, 输入系统参数 sp, 输出数据接收者的公钥和私钥(PK_R, SK_R), 和数据发送者的公钥和私钥(PK_S, SK_S)。

(3) PEKS(sp, PK_R, SK_S, w): 加密算法, 输入系统参数 sp, 关键词信息 w, 数据接收者公钥 PK, 输出关键词密文信息 CT_w=E(sp, PK_R, SK_S, w)。

(4)Trapdoor(sp, PK_S, SK_R, w'): 陷门生成算法, 输入系统参数 sp, 要搜索的关键词信息 w', 数据接收者的私钥SK_R, 输出陷门信息 $T_{w'}$= Trapdoor(sp, PK_S, SK_R, w')。

(5) Test(sp, CT_w, $T_{w'}$, PK_S, PK_R): 匹配算法, 输入系统参数 sp , 关键词密文信息 CT_w=E(sp, PK, w), 陷门信息 $T_{w'}$, 数据接收者与数据发送者的公钥PK_S和PK_R。如果 w=w', 输出 1; 如果 $w\neq w'$输出 0。

(6)Decrypt(C, SK_R): 解密算法, 输入数据接收者收到云服务器返回的密文信息 C 和私钥 SK, 输出明文信息。

正确性

要求对于任何诚实生成的密钥对(PK_S, SK_S)和(PK_R, SK_R), 对于任何关键词 w, Test(T_w, C, PK_S, PK_R)=1w, 为概率 1, 其中$C \leftarrow$ PEKS(w，PK_S，PK_R)和 $T_w \leftarrow$Trapdoor(w, PK_S, PK_R)。

但是这篇文章的搜索陷门生成算法是确定性算法, 关键词统计信息无法隐藏, 因此仍存在信息泄露的问题, 并且只考虑了一个发送者和一个接收者的情况, 没有考虑多用户场景, 这种考虑在 PEKS 方案中更加符合现实情况, 也是必要的, 因为服务器可能从发送者给其他用户的信息中得到有用信息, 从而对目标用户进行攻击。

2018 年, Mahnaz Noroozi 和 Ziba Eslami 考虑了更为实际的多用户场景, 提出来对 PAEKS 的改进方案[35]。他们改进了方案模型以适用于多个用户的情况, 并且还证明了 Huang 和 Li 的 PAEKS 方案在多用户场景下对内部(甚至外部)KGA 都是不安全的, 并提出了一种改进的方案使得安全模型从单用户设置扩展到多用户设置, 使其更加实用。并且他们改进了安全模型, 生成密文索引时不再指定数据接收者为 S, 允许敌手可以知道发送者发送给任意接收者的密文索引, 生成陷门时也不再指定发送者为 R, 而是允许敌手可以获得任意接收者搜索发送者 S 的密文所生成的陷门。所以该方案的安全模型使用的密文和陷门预言机定义如下。

密文预言机 O_C: PAEKS$_{SK_S}$($\cdot$, PK)

陷门预言机 O_T: Trapdoor$_{SK_r}$($\cdot$, PK)

在挑战阶段，敌手可以挑选一个挑战关键词w_0，询问 O_C: PAEKS$_{SK_S}$(w_0, PK)来获得相应密文，只限制不可以把w_i询问O_T。另外 PAEKS 是概率加密，加密时引入了随机数 r, 保证了关键词w_0, 敌手即便询问 OT 也可以实现密文不可区分。因为两次加密w_0, 得到的密文结果不一样。但是，他们没有考虑多密文情况。

2020 年, Qin 等人[36]考虑了多密文的情况, 即敌手不能够区分两个文件中是否包含相同的关键词, 进一步修改完善了安全模型为多密文下不可区分安全(MCI-Security)和多陷门下不可区分安全 MTI-Security。该方案在新的安全模型中, 考虑了多密文情况: 文件$w_0=(w_{01}, \cdots, w_{0n})$。文件$w_1=(w_{11}, \cdots, w_{1n})$。安全模型使用的预言机模型定义如下。

密文预言机 O_C: PAEKS$_{SK_S}$($\cdot$, PK_r)

陷门预言机 O_T: Trapdoor$_{SK_r}$($\cdot$, PK_s))。

限制敌手不能拿w_{0i}，w_{1i}询问O_C，O_T。但是用户是指定的一对一模型 R 和 S, 并不适用于多用户场景下。

2021 年, Qin 等人[37]发现以前的 PAEKS 方案中不允许敌手使用挑战关键词询问加密关键词的预言机, 然后改进了 CI 安全模型, 并消除了这个限制, 并使得改进方案能够抵抗 Fully CKC(Chosen Keyword to Cipher-keyword)attacks 完全选择关键词的密文关键词攻击(完全 CKC 攻击), 即允许敌手可以询问预言机任意关键词。并且证明了在完全 CKC 攻击下的 CI 安全性意味着 MCI 安全性。

其安全模型中, 密文预言机 O_C: $\mathrm{PAEKS}_{\mathrm{SK_s}}(\bullet, PK)$, 陷门预言机 O_T: $\mathrm{Trapdoor}_{\mathrm{SK_r}}(\bullet, PK)$。

总结以上 PAKSE 方案, 如图 7 所示。并且我们给出了一个敌手在(多)密文不可区分下的安全模型的能力的概述。

表 4　在(多)密文不可区分安全模型中对敌手查询的限制

Table 4　Restrictions on an adversary's queries　in (M)CI-security model

安全模型	(多)密文不可区分安全	
	密文预言机	陷门预言机
Huang 等[31]	$pk = pk_R \wedge w \neq w_b^*$	$pk = pk_S \wedge w \neq w_b^*$
Noroozi 等[35]	$(pk,w) \neq (pk_R,w_b^*)$	$(pk,w) \neq (pk_S,w_b^*)$
Chi 等[38]	$(pk,w) \neq (pk_R,w_b^*)$	$(pk,w) \neq (pk_S,w_b^*)$
Qin 等[36]	$pk = pk_R \wedge w \neq w_{b,i}^*$	$pk = pk_S \wedge w \neq w_{b,i}^*$
Pan 等[39]	$pk = pk_R \wedge w \neq w_{b,i}^*$	$pk = pk_S \wedge w \neq w_{b,i}^*$
Qin 等[37]	$(pk,w) \neq (*,*)$	$(pk,w) \neq (pk_S,w_{b,i}^*)$

注: $b \in \{0,1\}$, $i \in \{1,\cdots,n\}$, *代表可以是任何关键词或者公钥。

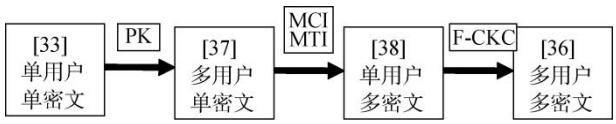

图 7　PAEKS 的发展

Figure 7　The development of PAEKS

Qin 的多密文不可区分的安全模型不仅遵循 Noroozi 等人的多用户安全模型, 而且还抵抗一个完全选择的关键词到密码关键词攻击, 即可以允许敌手获得任何数据接收者和他选择的任何关键词, 也不会透漏指定关键词的隐私。具体来说, 除了挑战密码关键词之外, 敌手仍然可以通过密码关键词预言机获得目标数据发送者和目标数据接收者之间的任何挑战关键词的密码关键词。但是, 这在所有其他多密文不可区分的安全模型中都是不允许的。Qin 等人在文献[37]中给出完全密文不可区分安全模型的正式定义, 并将其扩展到多个密文不可区分的安全模型, 这些模型是通过挑战者和敌手之间的游戏来定义的。然而, 2021 年 Cheng 等人[40]正式地分析了文献[37]不能实现多密文的不可区分性, 并且对多陷门不可区分性的证明也是不正确的。构造同时具有多密文不可分辨性和多陷门不可区分性的 PAEKS 方案仍然是一个有待解决的问题。

3.4　指定发送者模型

2017 年, Satio 等人[41]提出来只有指定的发送者才可以生成索引, 就阻止了内部敌手可以生成索引, 进而进行 IKGA。在指定发送者 PEKS 中, 数据接收者可以指定一组发数据送者。在这个模型中, 需要一个受信任的密钥中心, 它生成密钥并分发给用户。在密钥生成中, 生成的是对应的公钥和私钥, 关键词的陷门是使用数据接收者的私钥生成的。另一方面, 只有指定的数据发送方才能生成关键词的密文, 这可以在服务器中使用基于指定发送者的陷门进行测试。由于非数据接收者指定的服务器无法生成关键词的密文, 因此服务器无法启动内部关键词猜测攻击。同年, Jiang 等人[42]也利用了指定发送者的思想, 只有指定发送者能够生成有效密文, 因此可以抵抗 IKGA, 但是这两个协议都破坏了公钥可搜索加密的非对称性。

2018 年, Xie 等人[43]构建了一个新的体系来抵抗内部关键词猜测攻击问题。提出了一个基于该架构的具有指定测试人员(dCRKS)的有效密文检索实例, 该实例在 IKGA 下是安全的。如果没有发送方的密钥, 服务器就无法生成正确的关键词密文。同时, 如果没有接收方的密钥, 服务器就无法生成有效的陷门。因此, 恶意服务器无法启动 IKGA。尽管[24]对 IKGA 是安全的, 但在他们的方案中需要 TTP(受信任的第三方)。

2016 年, Peng 等人[24]基于一个新的框架, 提出了一个在线和离线密文检索(OOCR)方案对 KGA 内部是安全的, 其中陷门的生成被分为两个阶段: 离线阶段和在线阶段。陷门的大部分计算可以在知道关键词之前在离线阶段执行, 在线阶段可以有效地生成具有关键词的真实陷门。在他们的方案中, TTP(可信第三方)被引入密文检索方案, 以抵抗内部攻击。新型密文检索框架的工作流程运行如下, TTP 会根据数据发送者的身份为其颁发私钥, 发送方使用他的私钥、关键词以及接收方的一些相关参数生成可搜索的密文, 并将可搜索的密文上传到云服务器进行数据搜索。当接收方想要检索一些数据时, 他会使用发送方的身份、关键词和他的秘密参数生成一个陷门, 并将该陷门传输到服务器。服务器通过检查陷门是否与可搜索的密文相匹配来执行搜索操

作。如果标识和关键词相同, 服务器将加密的数据返回给接收方; 否则, 输出“不匹配”。这样, 云服务器就无法在不知道发送方的私钥的情况下生成有效的可搜索密文来匹配给定的陷门, 因此内部攻击不再工作。因此, 所提出的框架不仅实现了传统系统的原始功能和安全性, 而且还抵御了内部关键词猜测攻击。

表 5　指定发送者模型的方案比较

Table 5　Scheme comparison of designated-senders model

方案	优点	缺点
Satio 等[41]	阻止了内部敌手可以生成索引	破坏了公钥可搜索加密的非对称性, 需要可信第三方
Xie 等[44]	实现更强的安全性, 在测试和陷门的生成方面更高效	需要可信第三方
Peng 等[24]	不仅实现了传统系统的原始功能和安全性, 而且还抵御了在线/离线内部攻击	需要可信第三方
Sun 等[44]	采用签密算法加消息认证码, 安全性高	通信成本较高

2017 年, Sun 等人[44]采用签密算法加消息认证码的方式设计了一个基于任何公密钥加密系统的 IIKGA 的 PEKS 方案, 但是通信成本较高。其设计思路为: 在生成可搜索的密文时, 该方案采用信号加密算法(或签名再加密或加密再签名)。因此, 如果没有发送方的密钥, 云服务器就无法生成合法的可搜索密文来匹配接收到的陷门。受一个密码原语, 不可分辨性混淆器(IO)的启发, 该方案将陷门定义为一个感兴趣的关键词的信息密文、发送者的公钥和一个随机数, 它们使用对称加密算法(例如, AES)进行加密。因此, 通过在嵌入到接收方的对称密钥和解密密钥中的模糊密钥中执行解密和非信号加密操作, 可以匹配可搜索的密文和陷门。相反, 如果不使用 IO, 则很难将使用信号加密算法生成的可搜索密文和使用对称加密算法生成的陷门进行匹配。此外, 如果服务器是恶意的, 则在混淆程序中使用消息身份验证代码(MAC)函数, 以启用对返回的搜索结果的真实性检查。

3.5　模糊关键词模型等

2014 年, Shekokar 等人[45]首次提出了在密文数据上进行模糊关键词搜索的方案。在该方案采用了编辑距离来界定关键词间是否相似。编辑距离是指两个字符串之间, 由一个转成另一个所需的最少编辑操作的次数。许可的编辑操作包括将一个字符替换成另一个字符, 或者插入一个字符, 或者删除一个字符。一般来说, 如果编辑距离越小, 两个字符串的相似度就会越大。因为以往很多可搜索加密技术都只能执行精确关键词搜索, 若用户将检索关键词输入错误, 便检索不到想要的文件, 要求比较苛刻。但是模糊关键词搜索的模型允许数据用户在输入检索关键词的时候出现一些细微的错误, 为用户提供了更优的检索体验。同时又因为只提供给服务器模糊陷门, 因为两个或多个关键词共享相同的模糊关键词陷门, 因此服务器不能再学习推断确切的关键词。在可搜索加密过程中, 首先数据拥有者提取文档关键词集并构建相关的模糊集, 然后构造文档的安全索引和对应的验证标签, 最后将密文集、加密索引和验证标签上传并存储至云服务器端。合法授权的数据使用者向云服务器发送需要检索文档的陷门信息, 提交文档查询请求。云服务器根据收到的陷门信息开始检索密文文档, 并将满足条件的检索密文返回给用户。他们的方案在安全性和效率方面存在一些限制。一方面, 虽然服务器不能准确地猜测关键词, 但它仍然能够知道底层关键词属于哪个小集合, 因此关键词隐私没有很好地从服务器上保护。另一方面, 他们的方案是不切实际的, 因为接收方必须通过使用精确的陷门从从服务器返回的集合中过滤出不匹配的密文在本地找到匹配的密文。

2013 年, Wang 等人[46]提出了首个可验证的模糊关键词搜索方案, 比方案[43]增加了可以验证的功能, 以此来确保数据没有被恶意云服务器篡改, 只要用户输入的是已有模糊集中的关键词就能够顺利进行密文检索, 还能有效保护关键词信息的安全性, 最后用户也能对返回结果进行有效验证。

2016 年, Zhu 等人[47]提出了一种可验证的动态模糊关键词搜索方案, 该方案具有支持可验证、动态更新、模糊检索以及抗恶意攻击四大优点, 但在结果验证时由于采用了基于公钥系统的 RSA 累加器, 反而增加了操作的繁杂性, 占用了过多的时间。

2021 年, Ma 等人[48]引入了具有模糊关键词搜索的 PEKS, 即 m-PAEMKS 方案。在这种类型中, 除了原始的陷门外, 接收方还生成一个模糊的陷门, 因为多个关键词共享一个模糊的陷门, 允许服务器模糊地检查密文的关键词和陷门是相同的, 因此, 服务器最终无法猜测陷门的确切关键词。然而, 这种方法也意味着安全性和效率的降低。服务器仍然可以知道小集的关键词包括正确的关键词, 关键词隐私

保护方面安全性不够。为了提高效率, 由于服务器向接收器响应多个匹配的密文, 因此接收器必须使用精确的陷门在本地找到精确的密文。

此外, 2004 年, Peng 等人[49]提出了不经意关键词搜索 OSK(Oblivious Keyword Search), 目的是为了同时保护数据库端和用户端的隐私。一方面是隐藏用户查询数据库的目标, 另一方面是保证用户端除了得到查询目标对应值不会得到以外的其他任何信息。这个方案也保护了关键词的隐私, 云服务器不能够通过匹配陷门信息和关键词信息进行关键词猜测攻击。

该方案主要通过数据库和用户之间的不经意传输协议, 保护了用户和数据库的隐私, 即用户可以获取关键词陷门, 也只能查询和关键词匹配的加密数据, 同时数据库不知道用户查询的关键词。2016 年, Jiang 等人[50]提出来带授权的不经意关键搜索 OKSA(Oblivious Keyword Search with Authorization) 目的是为了限制用户查询的范围, 实现数据库对于被搜索关键词的授权。因为在一些诸如包含商业秘密或 DNA 信息的特殊数据库中, 数据需要高度保密, 对于访问的用户级别和权限有一定的限制。设 W 是授权的用户关键词集合, 那么用户只可以选择其中特定的关键词 $w \in W$, 数据库允只许用户检索与关键词 w 相对应的加密数据。数据库可以验证被选择的关键词是否属于集合 W, 但并不知道关键词本身是什么。但是 OKSA 方案的不足在于只是实现了单个文件对应单个关键词, 对用户来说要求比较严格, 因为如果猜不到文件对应的关键词, 就不能够进行搜索, 应该进一步推广, 实现多关键词下的不经意关键词搜索。

表 6　模糊关键词模型的方案比较

Table 6　Scheme comparison of fuzzy keyword model

方案	优点	缺点
Li 等[45]	允许数据用户在输入检索关键词的时候出现一些细微的错误, 为用户提供了更优的检索体验	在安全性和效率方面存在一些限制
Wang 等[46]	支持可验证、动态更新、模糊检索以及抗恶意攻击四大优点	操作的繁杂性, 占用了过多的时间
Peng 等[49]	同时保护数据库端和用户端的隐私	每个密文仅支持一个关键词的加密搜索
Jiang 等[50]	限制用户查询的范围, 实现数据库对于被搜索关键词的授权	限制范围是静态的, 不能增删数据, 不实用

3.6　小结

抵抗 IKGA 的方案主要从三个方面入手, 如图 8 所示:

(1)阻止服务器可以获得来自数据接收者的陷门

在几乎所有的公钥可搜索加密方案中, 内部敌手都是通过离线猜测候选关键词, 从而从给定陷门中恢复出关键词, 则需要解决陷门的安全性才能解决 IKGA。比如指定密文的 PEKS 通过共享秘密值使得陷门和关键词密文绑定在一起, 陷门只能和对应的关键词匹配。

(2) 阻止服务器可以加密候选关键词

如果能够阻止服务器可以加密关键词生成索引, 就能解决 IKGA。解决关键词密文的安全性的方法有见证关键词, 指定发送者, 注册关键词等方案, 利用数据发送者私钥来生成密文, 还有模糊关键词有效的解决了内部敌手生成关键词密文索引的问题。

(3)阻止服务器可以独立运行测试算法

如果能要求服务器虽然可以运行测试算法, 但是服务器不知道陷门和索引的对应关系, 也可以解决 IKGA。认证服务器和双服务器模型的提出就是要解决测试算法中暴露访问模式的问题。

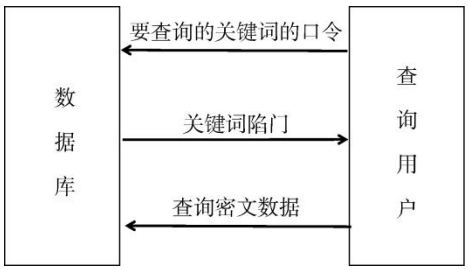

图 8　OSK 框架

Figure 8　OSK framework

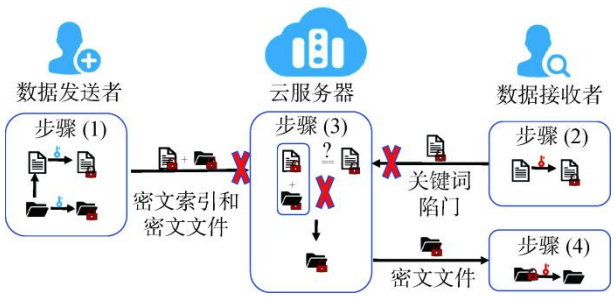

图 9　来自三个方面的内部关键词猜测攻击

Figure 9　Internal keyword guessing attacks mainly come from three aspects

从以上三个方面入手, 主要解决方案及方案的不足如下:

表 7 IKGA 解决方案对比

Table 7 Scheme comparison of the solution of IKGA

	服务器可以生成密文	服务器可以获取陷门	服务器可以独立运行测试算法
双服务器模型	√	√	×
认证服务器模型	√	√	√
见证关键词模型	×	×	√
指定发送者模型	×	√	√
模糊关键词模型	×	√	√

(1)双服务器模型, 可以阻止服务器独立运行测试算法, 但是不符合实际应用场景。应用两个服务器不便利, 并且很难保证两个服务器不会串通。

(2)认证服务器模型, 只有授权的云用户, 即身份标识为生成索引输入的云用户才能搜索和访问共享组数据。CA 的权威使得恶意服务器不可能进行作弊, 但是需要引入可信第三方。

(3)见证关键词模型, 引入发送者私钥 *SKs* 对关键词进行加密时见证的方法, 有效的阻止了服务器生成关键词密文, 从而不能够进行 IKGA。但是所有的 PAEKS 方案都是基于离散对数假设, 因此很容易受到量子攻击。

(4)指定发送者模型, 没有发送方的私钥 *SKs*, 云服务器就无法生成合法的可搜索密文来匹配接收到的陷门。只有指定发送者能够生成有效密文, 因此可以抵抗 IKGA, 但是破坏了公钥可搜索加密的非对称性。

(5)模糊关键词模型, 每个关键词都对应于一精确的陷门和一个模糊的陷门, 只提供给服务器模糊陷门, 因此服务器不能再学习推断确切的关键词, 但是效率比较低。

4 研究展望

就目前发展状况和当今研究中存在的一些不足, 本节给出一些需要进一步研究解决的问题。

4.1 抗量子攻击的 PAEKS 方案

由于量子计算机的快速发展, 当前网络工作协议的安全性受到了威胁[51]。一些科学家提出了理论上可行的方法, 利用量子计算机在很短的时间内可以打破目前使用的大多数加密算法[52], 例如 PAEKS 方案可以抵抗 IKGA 问题, 但这些方案基于离散对数假设, 这使得它们容易受到量子计算机的攻击。2021 年, Islam 等人[56]发现即使是这些基于格的方案仍然不能解决 IKGA 问题, 并基于格提出了新的可搜索加密方案以解决 IKGA。

在过去的几十年里, 人们对反量子密码学及相关领域进行了大量的研究, Zeng 等人[53]提出了一种基于格和属性的可搜索加密方案, 涉及授权和特殊关键词问题。Yu 等人[54]基于格给出了一个强大的方案, 可以撤销使用的关键词和阻止陷门暴露。最近的两种基于格的方案[51,55]是有效的和可证明安全的, 但是所有这些后量子方法都有一个缺陷: 不能提供对诚实但好奇的服务器模型下的安全保护。2021 年, Liu 等人[33]提出了一种基于 NTRU 假设的量子抗性 PAEKS 实例化。当前基于格的密码系统已经成为了主流的研究热点, 未来设计基于格密码实用的抗 IKGA 的密码系统仍是一项艰巨的任务。

4.2 轻量级的抗 IKGA 的 PEKS 方案

云辅助工业物联网(IIoT)依赖于云计算来提供大规模的数据存储服务。随着 5G 技术的快速发展, 5G 无线访问已逐渐成为一个关键网络访问技术, 在物联网领域依靠超高速度的优势、超高容量、超低延迟、超节能、全覆盖, 可满足物联网需求。另外云平台由于其强大的存储和计算能力而被广泛地应用于不同的应用程序中, 来自不同物理位置的用户可以通过在云平台[57]中上传数据来共享资源。从各种物联网传感器和设备收集到的数据被发送到云端进行处理和分析。

如何设计适用于物联网的轻量级抗 IKGA 的 PEKS 方案成为了研究热点。2021 年, Zhang 等人[55]提出了一种基于晶格假设的正向安全 PEKS 方案(FS-PEKS), 适合于云辅助物联网中加密工业数据的安全搜索, 可以抵抗 IKGA, 并且具有较低的通信开销。未来将在这个基础上进一步研究抵抗 IKGA 的可搜索加密技术, 增强物联网的安全性。

4.3 实现多用户场景下抗 IKGA 的 PEKS 方案

随着对隐私保护要求的不断提高, 抗内部关键词猜测攻击应成为 PEKS 方案的一个基本属性。将 IKGA 和其他性质结合在一起将是一个难点。例如 Zhu 等人[27]结合 PKE 方案和 PEKS 方案提出的一种安全的数据共享方案, 只有指定的服务器才能通过加密的文档来搜索关键词, 以增强安全性。由于数据接收者的数量增加会降低该方案中系统的有效性, 还需要进一步考虑在多数据接收者场景下构建一个 DSS 方案, 来实现多对多的用户场景。再比如见证关键词模型, 指定发送者模型和模糊关键词模型, 因限制了云服务器生成关键词密文, 所以就难以实现多对多的用户场景。2021 年 Cheng 等人[40]正式地分

析了[36]不能实现多密文的不可区分性, 并且对多陷门不可区分性的证明也是不正确的。因此, 构造同时具有多密文不可分辨性和多陷门不可区分性的PAEKS方案是一个有待解决的问题。如何将抗IKGA的属性与多实现用户场景及可验证性等属性相结合, 使 PEKS 更加实用是需要进一步研究的问题。

4.4 支持多关键词的不经意可搜索加密

不经意关键词搜索(OSK)方案可以同时保护数据库端和用户端的隐私。一方面是隐藏用户查询数据库目标, 另一方面是保证用户端不会得到查询目标对应值以外的其他任何信息, 同时也保护了关键词的隐私, 云服务器不能够通过匹配陷门信息和关键词信息进行关键词猜测攻击。但是该方案中每个数据文件只能关联一个关键词, 在加密过程中, 每个密文仅支持一个关键词的加密搜索。若一个文件存在多个关键词, 须对该文件进行多次加密。显然, 大多数文件都不仅仅存在一个关键词。我们可以拓展 OKS 协议将一个文件与它的多个关键词整合在一起, 使用户可以搜索这个文件中的所有关键词, 以验证是否为需要的文件。另外用户在执行搜索操作时, 可能因输入错误或无法确定要搜索的确切关键词, 导致所要搜索的关键词没有包含在服务器保存的关键词集合中, 最终搜索失败, 我们可以结合模糊关键词的加密搜索方案, 2015 年, Shekokar 等人[45]使用 Edit distance 来定义关键词之间的模糊度, 同时给出了两个构造模糊关键词集合的算法, 可以参照上述模糊度定义, 使用模糊关键词的方法构造算法, 扩展本协议的使用范围。

5 结束语

随着云计算技术的发展和数据隐私保护的要求不断提高, 公钥可搜索加密中的内部关键词猜测攻击成为研究的重点。本文主要从解决 IKGA 的五类方案出发, 梳理了 IKGA 的机理, 以及研究现状、解决方案之间的关系, 并讨论了现阶段内部关键词猜测攻击需要解决的问题, 以期为进一步解决公钥可搜索加密中的 IKGA 问题能够有所帮助, 使得公钥可搜索协议真正为实际所用。

参考文献

[1] Sun J M, Zhu B R, Qin J, et al. Confidentiality-Preserving Publicly Verifiable Computation Schemes for Polynomial Evaluation and Matrix-Vector Multiplication[J]. *Security and Communication Networks*, 2018: 5275132.

[2] Sun J M, Su Y, Qin J, et al. Outsourced Decentralized Multi-Authority Attribute Based Signature and Its Application in IoT[J]. *IEEE Transactions on Cloud Computing*, 2021, 9(3): 1195-1209.

[3] Yang H N, Sun J M, Qin J, et al. An Improved Scheme for Outsourced Computation with Attribute-Based Encryption[J]. *Concurrency and Computation*: *Practice and Experience*, 2019, 31(21): e4833.

[4] Yang H N, Su Y, Qin J, et al. Verifiable Inner Product Computation on Outsourced Database for Authenticated Multi-User Data Sharing[J]. *Information Sciences*, 2020, 539: 295-311.

[5] Yang H N, Su Y, Qin J, et al. Privacy-Preserving Outsourced Inner Product Computation on Encrypted Database[J]. *IEEE Transactions on Dependable and Secure Computing*, 2022, 19(2): 1320-1337.

[6] Song D X, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data[C]. *Proceeding 2000 IEEE Symposium on Security and Privacy*. *S&P*, 2000: 44-55.

[7] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public Key Encryption with Keyword Search[C]. *International Conference on the Theory and Applications of Cryptographic Techniques*, 2004: 506-522.

[8] Liu J L, Zhao B, Qin J, et al. Multi-Keyword Ranked Searchable Encryption with the Wildcard Keyword for Data Sharing in Cloud Computing[J]. *The Computer Journal*, 2023, 66(1): 184-196.

[9] Byun J W, Rhee H S, Park H A, et al. Off-Line Keyword Guessing Attacks on Recent Keyword Search Schemes over Encrypted Data[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 75-83.

[10] Lu Y, Li J G, Zhang Y C. SCF-PEPCKS: Secure Channel Free Public Key Encryption with Privacy-Conserving Keyword Search[J]. *IEEE Access*, 2019, 7: 40878-40892.

[11] 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.

[12] 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.

[13] Rhee H S, Susilo W, Kim H J. Secure Searchable Public Key Encryption Scheme Against Keyword Guessing Attacks[J]. *IEICE Electronics Express*, 2009, 6(5): 237-243.

[14] Chen R M, Mu Y, Yang G M, et al. Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(4): 789-798.

[15] Chen R M, Mu Y, Yang G M, et al. A New General Framework for Secure Public Key Encryption with Keyword Search[C]. *Australasian Conference on Information Security and Privacy*, 2015: 59-76.

[16] Chen R M, Mu Y, Yang G M, et al. Server-Aided Public Key Encryption with Keyword Search[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(12): 2833-2842.

[17] Wang D, Wang N, Wang P, et al. Preserving Privacy for Free:

Efficient and Provably Secure Two-Factor Authentication Scheme with User Anonymity[J]. *Information Sciences*, 2015, 321: 162-178.

[18] Huang X Y, Xiang Y, Chonka A, et al. A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2011, 22(8): 1390-1397.

[19] Wu L B, Chen B W, Choo K K R, et al. Efficient and Secure Searchable Encryption Protocol for Cloud-Based Internet of Things[J]. *Journal of Parallel and Distributed Computing*, 2018, 111(C): 152-161.

[20] Chen B W, Wu L B, Zeadally S, et al. Dual-Server Public-Key Authenticated Encryption with Keyword Search[J]. *IEEE Transactions on Cloud Computing*, 2022, 10(1): 322-333.

[21] Shao Z Y, Yang B. On Security Against the Server in Designated Tester Public Key Encryption with Keyword Search[J]. *Information Processing Letters*, 2015, 115(12): 957-961.

[22] Baek J, Safavi-Naini R, Susilo W. Public Key Encryption with Keyword Search Revisited[C]. *International Conference on Computational Science and Its Applications*, 2008: 1249-1259.

[23] Xie R, Xu C X, Li F G, et al. Ciphertext Retrieval Against Insider Attacks for Cloud Storage[C]. *2016 2nd IEEE International Conference on Computer and Communications*, 2016: 202-206.

[24] Jiang P, Mu Y, Guo F C, et al. Online/Offline Ciphertext Retrieval on Resource Constrained Devices[J]. *The Computer Journal*, 2016, 59(7): 955-969.

[25] Wang X F, Mu Y, Chen R M. Privacy-Preserving Data Search and Sharing Protocol for Social Networks through Wireless Applications[J]. *Concurrency and Computation*: *Practice and Experience*, 2017, 29(7).

[26] Zhu B R, Sun J M, Qin J, et al. A Secure Data Sharing Scheme with Designated Server[J]. *Security and Communication Networks*, 2019, 2019: 4268731.

[27] Andola N, Prakash S, Venkatesan S, et al. Improved Secure Server-Designated Public Key Encryption with Keyword Search[C]. *2017 Conference on Information and Communication Technology*, 2017: 1-6.

[28] Ma S, Mu Y, Susilo W, et al. Witness-Based Searchable Encryption[J]. *Information Sciences*, 2018, 453: 364-378.

[29] Liu Z Y, Tseng Y F, Tso R, et al. Designated- Ciphertext Searchable Encryption[J]. *Journal of Information Security and Applications*, 2021, 58: 102709.

[30] Tang Q, Chen L Q. Public-Key Encryption with Registered Keyword Search[C]. *European Public Key Infrastructure Workshop*, 2010: 163-178.

[31] 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.

[32] Liu C, Zhu L H, Wang M Z, et al. Search Pattern Leakage in Searchable Encryption: Attacks and New Construction[J]. *Information Sciences*: *an International Journal*, 2014, 265: 176-188.

[33] Liu Z Y, Tseng Y F, Tso R, et al. Public-Key Authenticated Encryption with Keyword Search: A Generic Construction and Its Quantum-Resistant Instantiation[J]. *The Computer Journal*, 2022, 65(10): 2828-2844.

[34] Li H B, Huang Q, Shen J, et al. Designated-Server Identity-Based Authenticated Encryption with Keyword Search for Encrypted Emails[J]. *Information Sciences*: *an International Journal*, 2019, 481(C): 330-343.

[35] Noroozi M, Eslami Z. Public Key Authenticated Encryption with Keyword Search: Revisited[J]. *IET Information Security*, 2019, 13(4): 336-342.

[36] Noroozi M, Eslami Z. Public Key Authenticated Encryption with Keyword Search: Revisited[J]. *IET Information Security*, 2019, 13(4): 336-342.

[37] Qin B D, Cui H, Zheng X K, et al. Improved Security Model for Public-Key Authenticated Encryption with Keyword Search[C]. *International Conference on Provable Security*, 2021: 19-38.

[38] Chi T Y, Qin B D, Zheng D. An Efficient Searchable Public-Key Authenticated Encryption for Cloud-Assisted Medical Internet of Things[J]. *Wireless Communications and Mobile Computing*, 2020, 2020: 8816172.

[39] Pan X Y, Li F G. Public-Key Authenticated Encryption with Keyword Search Achieving both Multi-Ciphertext and Multi-Trapdoor Indistinguishability[J]. *Journal of Systems Architecture*, 2021, 115: 102075.

[40] Cheng L X, Meng F. Security Analysis of Pan et al.'s "Public-Key Authenticated Encryption with Keyword Search Achieving both Multi-Ciphertext and Multi-Trapdoor Indistinguishability"[J]. *Journal of Systems Architecture*, 2021, 119: 102248.

[41] Saito T, Nakanishi T. Designated-Senders Public-Key Searchable Encryption Secure Against Keyword Guessing Attacks[C]. *2017 Fifth International Symposium on Computing and Networking*, 2017: 496-502.

[42] Jiang P, Mu Y, Guo F C, et al. Private Keyword-Search for Database Systems Against Insider Attacks[J]. *Journal of Computer Science and Technology*, 2017, 32(3): 599-617.

[43] Xie R, He C L, Xie D Q, et al. A Secure Ciphertext Retrieval Scheme Against Insider KGAs for Mobile Devices in Cloud Storage[J]. *Security and Communication Networks*, 2018, 2018: 7254305.

[44] Sun L X, Xu C X, Zhang M W, et al. Secure Searchable Public Key Encryption Against Insider Keyword Guessing Attacks from Indistinguishability Obfuscation[J]. *Science China Information Sciences*, 2017, 61(3): 038106.

[45] Shekokar N, Sampat K, Chandawalla C, et al. Implementation of Fuzzy Keyword Search over Encrypted Data in Cloud Computing[J]. *Procedia Computer Science*, 2015, 45: 499-505.

[46] Wang J F, Ma H, Tang Q, et al. Efficient Verifiable Fuzzy Keyword Search over Encrypted Data in Cloud Computing[J]. *Computer Science and Information Systems*, 2013, 10(2): 667-684.

[47] Zhu X Y, Liu Q, Wang G J. A Novel Verifiable and Dynamic Fuzzy Keyword Search Scheme over Encrypted Data in Cloud Computing[C]. *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016: 845-851.

[48] Ma Y, Kazemian H. Public Key Authenticated Encryption with Multiple Keywords Search Using Mamdani System[J]. *Evolving Systems*, 2021, 12(3): 687-699.

[49] Ogata W, Kurosawa K. Oblivious Keyword Search[J]. *Journal of Complexity*, 2004, 20(2/3): 356-371.

[50] Jiang P, Wang X F, Lai J C, et al. Oblivious Keyword Search with Authorization[C]. *International Conference on Provable Security*, 2016: 173-190.

[51] Yu X L, Xu C G, Dou B N. Conjunctive Keywords Searchable Encryption Scheme Against Inside Keywords Guessing Attack from Lattice[C]. *International Conference on Artificial Intelligence and Security*, 2020: 107-119.

[52] Shor P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. *SIAM Journal on Computing*, 1997, 26(5): 1484-1509.

[53] Zeng F G, Xu C X. A Novel Model for Lattice-Based Authorized Searchable Encryption with Special Keyword[J]. *Mathematical Problems in Engineering*, 2015, 2015: 314621.

[54] Yu X L, Xu C G, Xu L. Lattice-Based Searchable Encryption with Keywords Revocable and Bounded Trapdoor Exposure Resistance[J]. *IEEE Access*, 2019, 7: 43179-43189.

[55] Zhang X J, Xu C X, Wang H X, et al. FS-PEKS: Lattice-Based Forward Secure Public-Key Encryption with Keyword Search for Cloud-Assisted Industrial Internet of Things[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(3): 1019-1032.

[56] Islam S H, Mishra N, Biswas S, et al. An Efficient and Forward-Secure Lattice-Based Searchable Encryption Scheme for the Big-Data Era[J]. *Computers & Electrical Engineering*, 2021, 96: 107533.

[57] Kamara S, Lauter K. Cryptographic Cloud Storage[C]. *International Conference on Financial Cryptography and Data Security*, 2010: 136-149.

魏忠凯 于 2018 年在山东大学物理学专业获得学士学位。现在山东学校基础数学专业攻读博士学位。研究领域为可搜索加密, 研究兴趣包括云计算安全, 量子通信。Email: 17865196829@163.com

张茜 于 2018 年在河北师范大学数学与应用数学专业获得理学学士学位, 现在山东大学基础数学专业攻读博士学位。研究领域为密码学。研究兴趣包括可搜索加密, 云计算安全等。Email: mathxizhang@mail.sdu.edu.cn

秦静 于 2001 年在山东大学数学专业获得博士学位。现任山东大学数学学院教授、博士生导师。CCF 会员, 研究领域为加密搜索、外包计算。研究兴趣包括: 安全多方计算、不经意传输协议。Email: qinjing@sdu.edu.cn

刘晋璐 于 2019 年在山西大学数学科学学院获得理学学士学位, 现在山东大学基础数学专业攻读博士学位。研究领域为密码学。研究兴趣包括可搜索加密, 密钥聚合加密。Email: jinluliumath@163.com