

可搜索加密机制研究

李 雪¹, 罗圣美², 董振江², 蒋孝雯¹, 孙知信¹

(1. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室, 江苏 南京 210003;
2. 中兴通讯股份有限公司, 江苏 南京 210012)

摘 要:随着云存储技术的发展,越来越多的企业及个人将加密后的私有数据外包给云服务器,因此,对云服务器中加密数据的有效检索成为用户在选择云服务时关注的重点。通过分析国内外可搜索加密机制的研究成果,归纳了最新的可搜索加密技术,对现有的研究方法进行分类,包括支持关键字的可搜索加密机制、面向不同加密方式的可搜索加密机制和其他类的可搜索加密机制。分别分析总结了现有的不同的改进方法及其优缺点,特别研究分析了各类中最新的研究进展。对可搜索加密机制现阶段研究仍存在的信息泄露、实用性差以及搜索效率较低等问题进行了总结,并阐明了其未来可研究的方向。

关键词:云服务器;可搜索加密机制;公钥加密;对称加密

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2017)01-0097-06

doi:10.3969/j.issn.1673-629X.2017.01.022

Survey on Searchable Encryption Mechanism

LI Xue¹, LUO Sheng-mei², DONG Zhen-jiang², JIANG Xiao-wen¹, SUN Zhi-xin¹

(1. Key Laboratory of Broadband Wireless Communication and Sensor Network Technology of MOE,
Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. ZTE Corporation, Nanjing 210012, China)

Abstract: With the development of cloud storage technology, there is an increasing number of companies and individuals outsourcing their data to cloud sever. As a result, efficient retrieval of encrypted data stored on cloud server has become the issue that users may pay attention to when selecting cloud services. The latest searchable encryption technologies are summarized by analysis of the research achievement of searchable encryption technologies at home and broad, and the existing study methods are divided into different categories such as searchable encryption mechanism of supporting key words and of facing various encryption and others. The improved methods and their advantage and disadvantage are analyzed, especially for the latest development in each category. Some existing problems including information leakage, poor practicability and low search efficiency are summarized and further studies in the future are pointed out.

Key words: cloud server; searchable encryption mechanism; public key encryption; symmetric encryption

0 引言

现如今,云存储已被越来越多的IT公司所接受,作为其存储数据的解决方案。通过网络,用户可以将数据存储在云服务器中。如今已有数百万的用户通过基于云存储的公共网络与他们的朋友分享照片、视频等信息。商业用户也因其低价、高灵敏性、能够更好地利用资源等特点被深深吸引。包括IBM, EMC, Microsoft, Amazon等国际大型软件公司,都提供了基于“云”的解决方案,并在不断扩充和革新。最近国内的百度、腾讯、阿里巴巴等互联网公司,也分别发起了自

己的云战略。

然而,当用户把数据外包给云服务器之后,用户便没有办法再控制他们的数据。所以,云存储的安全问题成为云用户关注的重点。为了保证用户数据的隐私性,阻止数据被未授权的用户或攻击者所窃取,用户数据应该先加密,然后再存储到云服务器中。面对云服务器当中大量的加密数据,如何有效检索用户所需的数据已成为当前研究的热点问题。文中对可搜索加密机制进行研究,针对现有的研究方法对其进行分类,分别分析了支持关键词、加密以及其余的可搜索加密机

收稿日期:2015-06-27

修回日期:2015-10-14

网络出版时间:2017-01-04

基金项目:国家自然科学基金资助项目(61672299, 61373135);江苏省高校自然科学基金研究重大项目(12KJA520003);中兴通讯产学研项目

作者简介:李 雪(1992-),女,硕士研究生,研究方向为基于网络的计算机软件应用技术;孙知信,博士,教授,研究方向为计算机网络与安全。

网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20170104.1017.010.html

制的研究进展及其优缺点,对其进行总结并对可搜索加密机制未来的发展趋势做出展望。

1 可搜索加密机制研究

文献[1]最早提出了可搜索加密的概念,可搜索加密(Searchable Encryption, SE)是一种新型的密码体制,主要解决当数据加密存储在云端时,服务器不完全可信的前提下如何利用服务器来完成安全的关键词搜索的问题。它不仅保证数据接收方的隐私,同时提供了一种方法使用户无须对数据进行解密就能快速有效地进行搜索操作,以获得所需要的信息。现如今对 SE 加密机制的研究有很多,文中对相关文献进行分类总结,主要的研究思路如图 1 所示。

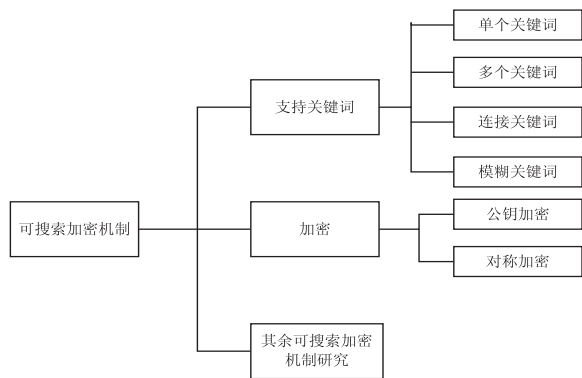


图 1 可搜索加密机制研究内容

1.1 基于关键词的研究

现阶段,对支持关键词可搜索加密机制的研究主要分为四个方面:单个关键词可搜索加密机制、多个关键词可搜索加密机制、连接关键词可搜索加密机制以及模糊关键词可搜索加密机制。

在加密文档中实现单个关键词搜索的方法在较早的时候便已提出,而且已存在很多证明过的单个关键词的可搜索加密机制。在单个关键词可搜索加密机制中,用户可以通过关键字查询判断文档中是否包含所要查询的关键字。文献[2]提出了一种单关键字可搜索加密机制,用户可以在不了解全部内容或者文件中有其他关键字的情况下决定文件是否包含一个特定关键字。该机制使用了中国剩余定理和一个单向函数用于存储关键字和验证目标。其优点是十分简单,不需大量计算,同时加密的工作量不会随着关键字出现次数的增大而增大。但是,其并未考虑到在不同的文件当中可能含有相同的关键字的情况,这就使得用户可能在检索过程中查得的结果不只一个,还需对大量的搜索结果进行进一步筛选才能找到自己想要的內容,降低了检索效率。

与单关键词可搜索加密不同,多关键词可搜索加密因为有多关键字限制查找文档的范围,可以较快

地找到用户要搜索的数据,效率较高。现阶段对于多关键字可搜索加密的研究很少,这是一个新的研究方向。文献[3]最早提出了多重可搜索加密关键字的概念并提出了第一个可行机制。该机制以双线性对映射及 C/S 模型为基础,以含有不同关键字的不同文件为前提条件来避免服务器上的攻击。它隐藏了数据和搜索陷门,能够成功地将用户陷门转化为多重搜索。但由于该机制是建立在随机预言模型的基础上验证其安全性,很难找到理想的散列函数模型加以实际应用。文献[4]提出一种可行、有效且没有随机预言的可搜索加密的新型应用场景,所有用户通过提交唯一的陷门均可以检索所有被存储在不可信服务器中的加密文档。任何用户可以在未来的关键字检索中与其他人共享自己的个人文件。但是其并未考虑到多关键字检索仍可能使得检索的结果不准确,还需要考虑到多条件的因素。

早期可搜索加密的研究机制,都限定在单个关键词搜索的情形当中,并未考虑关键词的布尔组合,这成了将可搜索加密技术应用到现实生活的最大阻碍。文献[5]最早提出了连接关键字可搜索加密机制,同时提供了两种对称密钥结构。但是这种机制的缺陷在于陷门规模在服务器上存储的数据总量是线性的,使得该机制在很多设定中不实用。文献[6]提出一种使用双线性的有效结构,双线性有连续规模的陷门,需要在搜索文件时执行成对操作。这种结构比起文献[5]在通信成本上更有效,但是对每个文件加密所花费的计算成本更大。因为对文件加密要求执行的成对操作要和相关总体关键字数量一样多。文献[7]提出一种有效的连接关键词可搜索加密方案,使陷门问题规模与单一关键字搜索几乎相同。在随机预言模型中的外部 co-Diffie-Hellman 假设下,该模型对于适应性选择关键字攻击安全性较高并且该机制花费的计算和通信成本更少。

单个关键词可搜索加密、多个关键词可搜索加密以及连接关键词可搜索加密机制都是在输入精确关键词的情形下研究的可搜索加密机制。而模糊关键词搜索可以容忍用户输入中含有的微小错误和存在的形式不一致,极大地提高了系统可用性和用户搜索体验。文献[8]描述了一种新的通用的可搜索加密原函数和安全模型。该机制允许对加密数据采用一些近似关键字进行搜索。使用这种机制时,对安全数据库进行有效请求以通过近似的估算得到精准的数据。这是第一个服务于容错可搜索加密和基于加密个人数据的生物识别身份认证协议的机制。但是其忽略了对搜索结果完整性的验证,使得搜索效率相对较低。文献[9]提出了一种基于混合云模型的可验证语义模糊可搜索加

密方案,弥补了目前大多数可搜索加密方案不能进行语义模糊搜索的不足,使其能够应对“不诚实且好奇”的服务器威胁。同时,实现了对搜索结果的验证,在确保搜索结果完整的同时也提高了搜索效率。

综上对基于关键词的可搜索加密机制的研究可知:针对多个关键词的可搜索加密要比单个关键词的可搜索加密搜索效率更高。当用户要通过云服务器检索所需的数据时,可以通过检索多个关键词限制检索范围,使得检索得到的结果更精确。多关键词的可搜索加密机制可以进一步考虑检索时多条件因素,进一步提高检索效率。连接关键词可搜索加密机制,考虑关键词的布尔组合,使得可搜索加密机制可以很好地应用到日常生活当中。为了使其更好地应用到生产、生活中,需要在健壮性和容错性方面进一步改进。模糊关键词可搜索加密不同于其他三种加密机制,考虑了用户输入关键词不精确的情况,可以在一定范围内容忍用户输入差错,提高了可搜索加密技术的实用性。

1.2 基于加密的研究

现阶段针对加密方法的可搜索加密机制的研究分为:公钥可搜索加密机制和对称可搜索加密机制。其中,公钥可搜索加密机制(即非对称可搜索加密^[10])使用两种密钥:公钥用于明文信息的加密和目标密文的检索,私钥用于解密密文信息和生成关键词陷门。公钥(非对称)可搜索加密算法通常较为复杂,加解密速度较慢,但是其具有公私钥相互分离的特点。公钥(非对称)加密模型如图 2 所示。

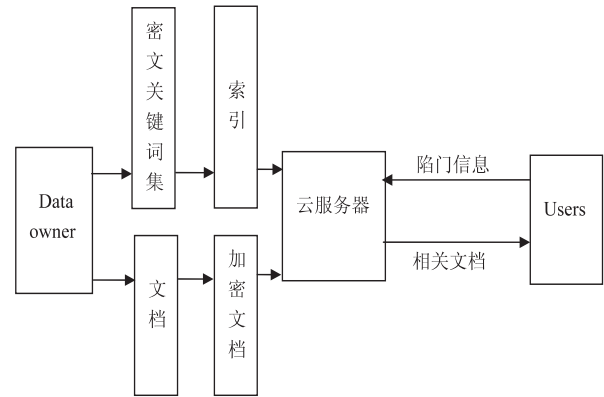


图 2 公钥(非对称)可搜索加密的模型

一直以来公钥可搜索加密机制都是可搜索加密研究的重点。文献[11]提出了可同时检索密文关键词与密文信息的可搜索加密机制。基于关键字搜索的公钥加密机制允许数据所有者委托给其他用户检索挑选出存储于外部的数据中的关键字。半可信第三方,也称“代理”,需要把数据所有者(委托方)使用公钥来计算的密文转换为能使用其他用户(受托方)的私钥被解密,这个私钥是使用数据产生的重加密生成的。在关键字搜索的公钥加密机制基础上,文献[12]提出了

一种支持对关键词进行交集搜索的公钥可搜索加密机制,提高了搜索效率。文献[13]提出了基于授权的公钥可搜索加密机制,在其构造的方案中,用户可以生成授权信息给特定的服务器,该服务器可以利用授权信息在不解密密文的情况下进行搜索。但是其在安全模型及效率方面均需要进一步提高。文献[14]通过关键字搜索的公钥加密对加密数据进行关键字搜索。这些加密数据是通过产生陷门而得到所需的关键字。该文献定义和实施了两个原函数:关键字搜索公钥加密界限值函数(TPEKS)和分发私钥匿名身份加密函数((n,t) -IBE)。TPEKS 是对关键字搜索的公钥加密在分发过程中产生陷门方面的扩展延伸。同时,其也提供了两种通用的转换方式:第一种是把一个匿名的 IBE 机制转换成一个匿名的 (n,t) -IBE;第二种是将一个 (n,t) -IBE 机制转换成安全的 TPEKS 机制。但是在实际应用中,调查员可能想要得到模糊的关键字,而该机制不能解决这个问题。文献[15]介绍和提出了一个新的时间释放可搜索加密(TRSE)理念,用来解决时间敏感的密文检索问题。文献以公钥时间释放可搜索加密(PKTRSE)为核心展开研究并建立了 PK-TRSE 模型。发送方对一条信息加密,因此只有预期接收者能够搜索包含特定关键字的目标密文,其中关键字是提前设定好在将来释放时间之后产生。另外给出了两种 PKTRSE 结构机制:一个通用机制和一个固定机制。这两种机制在随机语言模型里的 BDH 假设下都是安全的,并且得到了很好的应用。文献[16]分析了 3 种可搜索解密机制^[17-19],并挑选了在数据存储环境下最合适的机制。然后,通过消除冗余陷门生成算法以及简化相关解密算法降低了计算复杂度,提高了代理重加密机制的效率。

对称可搜索加密^[1]的构造通常基于伪随机函数,具有计算开销小、算法简单、速度快的特点,除了加解密过程采用相同的密钥外,其陷门生成也需密钥的参与。对称加密模型如图 3 所示

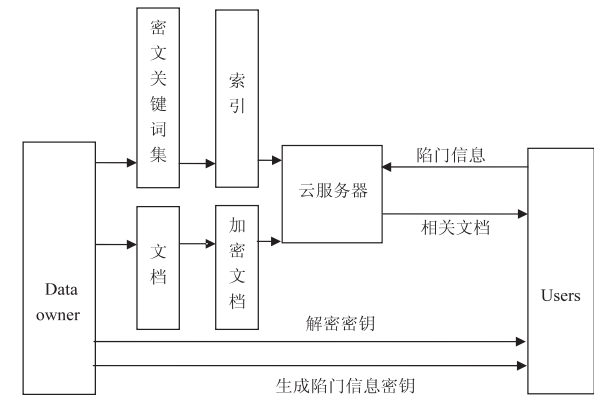


图 3 对称可搜索加密的模型

由图 2 和图 3 可知,公钥可搜索加密与对称可搜

索加密不同的是,数据的加密都利用了共享者的公钥,因此整个过程中,数据加密者不需要与数据共享者进行交互。传统的对称可搜索加密方法包括 SWP^[1], Z-IDX^[20], PPSSED^[21], SSE-1, SSE-2^[22], Van Liesdonk^[23]。文献[24]提出了一种用于获得指数和陷门的不可分辨性的有效对称可搜索加密算法。另外还引入了一种最新的定义限制,当数据库中每个单元加密后产生不可分辨性从而用于可搜索加密。该可搜索加密算法是第一个能同时满足高效和不可分辨性(安全性)的算法。文献[25]致力于对称可搜索加密运算速度及计算量的研究,使得运算速度更快、计算量更少。但是其忽略了对称可搜索加密算法的安全性对其性能的影响。文献[26]提出一种动态可搜索对称加密机制,允许客户端存储一个动态服务器加密文件的汇总,之后在这些加密文档上迅速执行关键词搜索,同时展现最少的信息给服务器。文献建立的原型演示了其在数据集不同于以往研究的效率,其不要求服务器提供除上传和下载数据以外的任何操作。因此,该机制中的服务器能单独基于云存储服务,而不是云计算服务。在建立动态 SSE 机制过程中介绍了一个叫 Blind Storage 的新原语,允许一个客户端存储一个文件集在一个远程服务器上。在这种方式中,服务器不了解有多少文件被存储,或者是每个文件的长度。当文件被检索时,服务器才了解到其存在,但是文件的内容及名称没有被显示。缺陷在于对抗不可信服务器时无法保证安全,同时不能支持多关键字搜索。

综上对可搜索加密的总结分析可知:对公钥可搜索加密的研究除了提高其安全性之外,还结合基于关键词可搜索加密技术,实现支持对关键词进行交集搜索的公钥可搜索加密方案,提高了公钥可搜索加密方案的搜索效率。对对称可搜索加密机制的研究实现了动态管理,方便文件的管理,减少了服务器的工作量。另外,现有的文献研究已经实现了对称可搜索加密的高效性和安全性,证明了可搜索加密技术可以更好地应用到云服务当中,给用户带来便利。

1.3 其余可搜索加密机制的研究

可搜索加密机制还有其余广泛的研究内容和范围。在可搜索加密机制研究的早期文献中,对密文检索顺序的排序^[27]、密文检索中的密文范围检索^[28-30]、可搜索加密方案中可能存在的关键词猜测攻击^[31]、全同态加密技术^[32]等方面进行了研究。其中,文献[32]中提出的全同态加密技术中服务器并不需要对密文进行解密,可以直接对密文进行操作。从功能上进一步增加了可搜索加密技术的应用前景,但是目前全同态加密技术从效率上还不够实际。

近年来,对可搜索加密机制的研究主要集中于多

用户可搜索加密机制、基于属性的可搜索加密机制、指定测试者身份、具有匿名性的可搜索加密机制等方面。文献[33]考虑了多用户请求场景,提出了基于双线性映射的实用性解决方案。该机制允许系统中任何人产生加密数据及关键字,任何人都可以用任何关键字进行搜索。但是该机制没有考虑访问控制的临界需求。

文献[34]提出了一个新的粗粒度访问控制的概念,并且用它来构造一个在混合云中的多用户可搜索加密模型。该构造中使用了两种典型机制,一种是广播加密(BE)机制来简化访问控制,另一种是单一用户可搜索加密机制,它能支持两相操作,当不信任服务器与对手合谋时这种机制是安全的。另外使用一个改进的可搜索对称加密机制来实施一种实用的机制,该机制是安全的。文献[35]提出一个一对多的公钥时间释放加密(PKTRSE)原型系统,称为多用户 PKTRSE (MUPKTRSE)。在一对一 PKTRSE 中,发送方把加密消息转化给服务器并且让消息在释放一定时间后被特定接收方搜索和解密。当这种 PKTRSE 应用于在同样的释放时间内为成倍增加的接收者加密消息,它的密文规模取决于用户规模。PKTRSE 能解决时间依赖密文检索问题。文献[36]提出一种针对多用户设置的可搜索加密技术,该技术加入了访问控制这一新的要求。Ciphertext-Policy Attribute-Based Encryption (CP-ABE)可以有效解决此问题。文献实现了对云存储的访问控制。关键词的索引以及陷门的生成是通过代理服务器实现的。为了实现有效的访问控制,第一个搜索数据的解决方案是一个用户可以使用偏序关系解密并且设计一种新的方法认证每一个用户的属性,而不需要公开用户的身份与属性之间的关系。为了减少解开销,该机制中用户把大部分的 CP-ABE 解密工作委托给代理服务器。文献[37]提出了一种改进的基于代理重加密的新型多用户可搜索加密机制。该机制中,密钥是再加密的,访问控制策略用来做重加密密钥以实现可区分的搜索,更好地撤销了权限控制。数据索引结构的设计是基于对云存储系统的实际物理结构的考虑,实现了更高的效率和更好的实用性。在新机制中,降低了客户端的计算开销。

基于属性加密的目的是提供对加密数据的细粒度访问控制,这个概念由文献[38]提出。主要有两种:密文策略属性加密(CP-ABE)^[39]和关键字策略属性加密(KP-ABE)^[40]。密文策略属性加密中,数据所有者能够定义一个访问策略并在该策略下对自己的数据进行加密。每个用户被指定一系列嵌入用户私钥的属性。用户只能在自己的属性与访问策略相匹配时才能解密密文。文献[41]针对特定环境下对加密数据进行检索的难题,给出了基于属性的可搜索方案(ATT

-PEKS)的定义及算法,该算法能够适应群组的公钥加密搜索,更大程度地共享信息,同时节省信息存储所需空间。文献[42]对指定测试者的基于身份可搜索加密方案进行研究,提出了基于身份密码系统下的指定测试者可搜索加密方案的定义和安全需求,并设计了一个高效的新方案,能够有效抵御离线关键字猜测攻击。文献[43]提出一种基于匿名性的基于身份可搜索加密方案(ANOIBEK)的定义和构造算法,对关键字信息以及消息查询方信息进行保护。该加密方案在随机预言机模型(Random Oracle)下是选择关键词攻击语义安全的(IND-CPA)。

综上对可搜索加密技术的总结和分析可知,现如今在不同的方向上均实现了对可搜索加密技术的改进,而这些改进使得可搜索加密技术搜索效率更高、安全性更好,可以实现多用户检索、基于属性可搜索加密、保护关键字及用户信息等等。这些改进使得可搜索加密技术可以更好地应用到用户在云服务器上搜索数据的过程中,使得云服务更可靠。但是若要将可搜索加密应用到日常生活中,使得更多的用户选择将自己的私密数据存放到云服务器中,除了安全性与高效性之外还要保证其健壮性。文献[44]通过考虑数字和非数字数据,提出一种健壮的可搜索的加密机制用于云计算中的数据外包,并且为云计算提供一些容错可用性,使得其可以更好地为用户服务。

2 结束语

在研究了大量可搜索加密机制的基础上,对可搜索加密机制的研究方法进行分类,包括:支持关键字的可搜索加密机制、面向不同加密方式的可搜索加密机制和其他类的可搜索加密机制。分别总结了不同的改进方法及其优缺点,特别研究分析了各类中最新的研究进展。通过以上的总结、分析可以看出:SE机制是解决云存储中的安全问题的研究热点之一,有利于云存储技术的普及。另外,通过对SE研究情况进行的总结和分析,可以了解到SE研究中值得深入研究的问题,包括:

(1)目前应用于密文搜索的可搜索加密技术都是确定性加密,如果保持关键字的相关特征,保持关键字在密文中的存储位置,保证加密后的大小关系,这些均存在信息泄露问题,另外也存在消息查询方身份泄露的问题。

(2)基于索引的密文搜索算法的索引构建大部分是静态的,即不能随着数据的增删进行动态更新,这就降低了其实用性。另外,在面临多用户的情况时,还要考虑进行用户的添加及删除的情况,包括对其访问权限及密文的有整据处理。

(3)在用户进行搜索时,用户仍需要在一定数量的搜索结果中再次进行搜索,找出自己想要查询的内容,降低了搜索效率。现阶段对该问题的解决方法的研究,或侧重多个关键字,或侧重多条件考虑,比较片面,不够完善,而且忽略了在不同的查询文件中关键字出现频率相同的情况。

参考文献:

- [1] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data[C]//Proceedings of IEEE symposium on security and privacy. [s. l.]:IEEE,2000:44-55.
- [2] Premasathian N, Choto S. Searchable encryption schemes: with multiplication and simultaneous congruences[C]//9th international conference on information security and cryptology. [s. l.]:IEEE,2012:147-150.
- [3] Popa R A, Zeldovich N. Multi-key searchable encryption[R]. [s. l.]:[s. n.],2013.
- [4] Yang J, Liu Z, Li J, et al. Multi-key searchable encryption without random oracle[C]//International conference on intelligent networking and collaborative systems. [s. l.]:IEEE,2014:79-84.
- [5] Colle P, Staddon J, Waters B. Secure conjunctive keyword search over encrypted data[C]//Applied cryptography and network security. Berlin:Springer,2004:31-45.
- [6] Byun J W, Lee D H, Lim J. Efficient conjunctive keyword search on encrypted data storage system[M]//Public key infrastructure. Berlin:Springer,2006:184-196.
- [7] Ryu E K, Takagi T. Efficient conjunctive keyword-searchable encryption[C]//21st international conference on advanced information networking and applications workshops. [s. l.]:IEEE,2007:409-414.
- [8] Bringer J, Chabanne H, Kindarji B. Error-tolerant searchable encryption[C]//IEEE international conference on communications. [s. l.]:IEEE,2009:1-6.
- [9] 林柏钢, 吴阳, 杨旸, 等. 云计算中可验证的语义模糊可搜索加密方案[J]. 四川大学学报:工程科学版,2014(6):1-6.
- [10] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[C]//Advances in cryptology-Eurocrypt 2004. Berlin:Springer,2004:506-522.
- [11] Zhang B, Zhang F. An efficient public key encryption with conjunctive-subset keywords search[J]. Journal of Network and Computer Applications,2011,34(1):262-267.
- [12] Fang L, Wang J, Ge C, et al. Decryptable public key encryption with keyword search schemes[J]. JDCTA,2010,4(9):141-150.
- [13] Ibraimi L, Nikova S, Hartel P, et al. Public-key encryption with delegated search[C]//Applied cryptography and network security. Berlin:Springer,2011:532-549.
- [14] Siad A. Anonymous identity-based encryption with distributed

- private-key generator and searchable encryption[C]//5th international conference on new technologies, mobility and security. [s. l.]: IEEE, 2012: 1-8.
- [15] Yuan K, Liu Z, Jia C, et al. Public key timed-release searchable encryption[C]//Fourth international conference on emerging intelligent data and web technologies. [s. l.]: IEEE, 2013: 241-248.
- [16] Rahman D A, Heng S H, Yau W C, et al. Implementation of a conditional searchable encryption system for data storage[M]//Computer science and its applications. Berlin: Springer, 2015: 469-474.
- [17] Chen X, Li Y. Efficient proxy re-encryption with private keyword searching in untrusted storage[J]. International Journal of Computer Network and Information Security, 2011, 3(2): 50-60.
- [18] Juang W S, Shue Y Y. A secure and privacy protection digital goods trading scheme in cloud computing[C]//Computer symposium on ICS. [s. l.]: IEEE, 2010: 288-293.
- [19] Wang X A, Huang X, Yang X, et al. Further observation on proxy re-encryption with keyword search[J]. Journal of Systems and Software, 2012, 85(3): 643-654.
- [20] Goh E J. Secure indexes[R]. [s. l.]: [s. n.], 2003.
- [21] Chang Y C, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data[C]//Applied cryptography and network security. Berlin: Springer, 2005: 442-455.
- [22] Curtmola R, Garay J, Kamara S, et al. Searchable symmetric encryption: improved definitions and efficient constructions[C]//Proceedings of the 13th ACM conference on computer and communications security. [s. l.]: ACM, 2006: 79-88.
- [23] van Liesdonk P, Sedghi S, Doumen J, et al. Computationally efficient searchable symmetric encryption[M]//Secure data management. Berlin: Springer, 2010: 87-100.
- [24] Yoshino M, Naganuma K, Satoh H. Symmetric searchable encryption for database applications[C]//14th international conference on network-based information systems. [s. l.]: IEEE, 2011: 657-662.
- [25] Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption[C]//Proceedings of the 2012 ACM conference on computer and communications security. [s. l.]: ACM, 2012: 965-976.
- [26] Naveed M, Prabhakaran M, Gunter C A. Dynamic searchable encryption via blind storage[C]//IEEE symposium on security and privacy. [s. l.]: IEEE, 2014: 639-654.
- [27] Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data[C]//IEEE 30th international conference on distributed computing systems. [s. l.]: IEEE, 2010: 253-262.
- [28] Hore B, Mehrotra S, Tsudik G. A privacy-preserving index for range queries[C]//Proceedings of the thirtieth international conference on very large data bases. [s. l.]: [s. n.], 2004: 720-731.
- [29] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data[M]//Theory of cryptography. Berlin: Springer, 2007: 535-554.
- [30] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data[C]//IEEE symposium on security and privacy. [s. l.]: IEEE, 2007: 350-364.
- [31] 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.
- [32] Gentry C. A fully homomorphic encryption scheme[D]. Stanford: Stanford University, 2009.
- [33] Bao F, Deng R H, Ding X, et al. Private query on encrypted data in multi-user settings[M]//Information security practice and experience. Berlin: Springer, 2008: 71-85.
- [34] Liu Z, Wang Z, Cheng X, et al. Multi-user searchable encryption with coarser-grained access control in hybrid cloud[C]//Fourth international conference on emerging intelligent data and web technologies. [s. l.]: IEEE, 2013: 249-255.
- [35] Yuan K, Liu Z, Jia C, et al. Multi-user public key timed-release searchable encryption[C]//Fourth international conference on emerging intelligent data and web technologies. [s. l.]: IEEE, 2013: 363-370.
- [36] Lv Z, Zhang M, Feng D. Multi-user searchable encryption with efficient access control for cloud storage[C]//IEEE 6th international conference on cloud computing technology and science. [s. l.]: IEEE, 2014: 366-373.
- [37] Ya-Ling Z, Kai L, Shang-Ping W, et al. A multi-users searchable encryption scheme with proxy re-encryption[C]//Tenth international conference on computational intelligence and security. [s. l.]: IEEE, 2014: 563-567.
- [38] Sahai A, Waters B. Fuzzy identity-based encryption[M]//Advances in cryptology - Eurocrypt 2005. Berlin: Springer, 2005: 457-473.
- [39] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//IEEE symposium on security and privacy. [s. l.]: IEEE, 2007: 321-334.
- [40] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proceedings of the 13th ACM conference on computer and communications security. [s. l.]: ACM, 2006: 89-98.
- [41] 李双, 徐茂智. 基于属性的可搜索加密方案[J]. 计算机学报, 2014, 37(5): 1017-1024.
- [42] 王少辉, 韩志杰, 肖甫, 等. 指定测试者的基于身份可搜索加密方案[J]. 通信学报, 2014, 35(7): 22-32.
- [43] 李双, 袁丁. 具有匿名性的可搜索加密方案[J]. 计算机工程与设计, 2013, 34(7): 2286-2290.
- [44] Huang J Y, Liao I E. A searchable encryption scheme for outsourcing cloud storage[C]//IEEE international conference on communication, networks and satellite. [s. l.]: IEEE, 2012: 142-146.