计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170627
54(10):2107-2120,2017

可搜索加密研究进展

董晓蕾　周　俊　曹珍富
(华东师范大学计算机科学与软件工程学院密码与网络安全系　上海　200062)
(dongxiaolei@sei.ecnu.edu.cn)

Research Advances on Secure Searchable Encryption

Dong Xiaolei, Zhou Jun, and Cao Zhenfu
(*Department of Cryptography and Network Security, School of Computer Science and Software Engineering, East China Normal University, Shanghai* 200062)

Abstract　With the development of big data and cloud computing, the issue of secure search via the technique of searchable encryption has increasingly been the focus of the researchers in cryptography and network security all over the world. In the light of the new theories, new solutions and new techniques of searchable encryption, this paper presents a survey mainly from the following four aspects: the modes, the security, the expressiveness and the efficiency of secure searchable encryption. It discusses the new theories which are essential to secure search for ubiquitous network, including searchable encryption, attribute-based encryption, and applying these cryptographic mechanisms to obtain the generalized solutions to the theoretical problems of secure search in types of new emerging network services. Based on the aforementioned theoretical results, this paper studies the new approaches to construct practical secure search for these network services, comprising the light-weight public-key cryptographic algorithms, reducing the times of applying the light-weight public-key cryptographic algorithms in secure search, and exploiting any public-key cryptographic algorithm only once to obtain new approaches for secure search in the environment of resource-constrained network applications. We also focus on studying how to apply the new theories and approaches to solve the problems associated to secure search in different kinds of networks, including body area network, wireless vehicular ad hoc network, smart grid and so on. It is traditionally required to apply inefficient public-key cryptographic algorithms a number of times to construct secure search protocols. How to manipulate the public-key cryptographic algorithms and make them suitable to be used in resource-constrained networks becomes the key issue. Light-weighting public-key cryptographic algorithms is certainly a convincing way to address it. On the other hand, minimizing the number (once would be ideal) of applying the light-weighted public-key cryptographic algorithms guarantees more efficient and practical solutions and thus is the key problem to address the issue. Finally, we suggest several interesting open research issues and the trend in the future.

收稿日期:2017-08-31;**修回日期**:2017-09-13
基金项目:**国家自然科学基金项目**(61632012,61672239,61602180);**上海市高新技术领域项目**(16511101400);**上海市自然科学基金项目**(16ZR1409200)
This work was supported by the National Natural Science Foundation of China (61632012, 61672239, 61602180), the Shanghai High-Tech Field Project (16511101400), and the Natural Science Foundation of Shanghai (16ZR1409200).
通信作者:**曹珍富**(zfcao@sei.ecnu.edu.cn)

Key words secure search; searchable encryption; lightweight; attribute-based encryption; efficient implementation

摘 要 随着大数据与云计算的发展,以可搜索加密为核心技术的安全搜索问题日益成为国内外研究的热点.围绕可搜索加密的新理论、新方法和新技术,针对可搜索加密的模式、安全性、表达能力和搜索效率等方面进行综述.主要内容如下:安全搜索必不可少的新理论研究进展,包括可搜索加密、属性基加密及其轻量化等相关理论问题的研究情况介绍;基于公钥密码算法(包括轻量化公钥密码算法)的安全搜索研究中,提出的减少公钥密码算法的使用次数的新方法概述;针对体域网、车载网、智能电网等新兴网络应用服务,介绍了前述新理论、新方法的应用情况.实现安全搜索,通常将不得不多次使用开销极大的公钥密码算法,所以在资源受限的网络中"怎么使用公钥密码算法"就成为一个关键问题.因此除了轻量化实现技术,减少使用公钥密码算法的次数(尤其是只使用一次)应成为高效解决这类问题的最为关键的步骤.此外,还指出了该领域当前研究中需要解决的公开问题和未来的发展趋势.

关键词 安全搜索;可搜索加密;轻量化;属性基加密;高效实现

中图法分类号 TP391

传统的信息检索系统一般是建立在明文系统上的,即服务器在明文上进行搜索操作.因此,服务器对整个数据库的数据及搜索的关键字一目了然.也即是说,服务器对于用户来说是完全可信的.之后,在服务器端加上访问控制功能,解决了合法用户的授权问题.然而服务器通常工作在半可信或恶意环境下,前者是指服务器诚实地遵照协议的规定执行,并通过与用户的交互最大限度地提取用户的秘密信息;后者是指服务器通过任意破坏行为来阻碍协议的执行.因此数据文件必须先加密再上传到服务器中外包存储.如何有效解决密文数据上的搜索问题,同时保护搜索的关键字隐私成为几年来亟待解决的重要研究课题.安全搜索也即应运而生.

安全搜索(secure search)通常指对加密数据的有效搜索.为了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的搜索问题,学者们提出了可搜索加密(searchable encryption, SE),作为安全搜索的核心技术.可搜索加密作为一种新兴的技术,具有广阔的应用前景,为云计算及大数据环境构造安全、高效的可搜索加密方案具有很强的理论及现实意义.然而,近年来随着无线通信与移动计算的迅猛发展,无线体域网、智能电网、车载网等一系列新兴网络应用均具有存储和计算资源受限的特点,因此,真正实现安全搜索仅依赖可搜索加密技术是不够的.我们可将安全搜索定义为:"可搜索加密+X",其中 X 可定义为轻量化技术、批处理技术等一系列使得安全搜索在新兴网络应用服务中达到高效实例化的各类其他技术.这方面研究主要侧重可搜索加密轻量化处理,其基本要求是:在不损失安全性的前提下使之适合各类资源受限的网络应用.

此外,属性基加密(attribute-based encryption, ABE)是近 10 年来的一个重要研究方向,它通过对用户私钥设置属性集(或访问结构)为数据密文设置访问结构(或属性集),由属性集和访问结构之间的匹配关系确定其解密能力.特别是密文策略的属性基加密(CP-ABE),其密文上的访问策略本身就是一种搜索策略,访问策略的表达能力从一定程度上反映了可搜索能力.

对于适用于资源受限的可搜索属性基加密的研究,主要体现在属性基加密的高效性和普适性研究上,包括属性集或访问结构的表达能力、方案的通信效率及计算效率、属性特征的研究,以及如何减少使用次数.所以,属性基加密的研究重点在提供丰富的可搜索功能和确保安全性的情况下,更注重实用性.效率问题是一个密码系统走向实用化过程中必须考虑并需要解决的问题.当前的属性基密码算法都在保证系统安全性的前提下,不断努力改进其效率,期望为各类资源受限的新兴网络应用提供坚实的基础.

在本文中,我们侧重于对安全搜索的核心技术——可搜索加密——进行较为系统地总结.期望通过总结,提出问题和未来的研究课题.我们的一个观点是:不管是安全搜索还是其他安全或隐私保护问题,如果频繁使用开销极大的公钥加密,其意义最多只是提供了一个"从无到有"的思路.一个方案要付诸实践,必须减少公钥密码的使用次数.

1 可搜索加密

随着云计算及大数据的流行,越来越多的敏感数据集中到云端,信息共享在我们的生活中无处不在,数据的安全和用户的隐私保护就成为一个重要的课题.为了保证数据安全和用户隐私,数据一般是以密文形式存储在云端服务器中,但是用户将会遇到如何在密文上进行查找的难题.可搜索加密 SE 是近年来发展起来的一种支持用户在密文上进行关键字查找的密码学原语,它能够为用户节省大量的网络和计算开销,并充分利用云端服务器庞大的计算资源进行密文上的关键字查找.可搜索加密技术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的搜索.

可搜索加密主要包含对称可搜索加密(symmetric searchable encryption, SSE)和非对称可搜索加密(asymmetric searchable encryption, ASE)两种类型,二者分别在功能和性能方面有不同的侧重点,分别用来解决云计算不同场景下的业务需求问题.在对称环境下,数据的产生者、搜索凭证的产生者以及解密者都是同一个用户.可搜索对称加密体制使得一个用户以私有的方式将自己的数据远程存储在一个半可信的云端服务器上,并保留选择性恢复所需文件的能力.如图 1 所示,可搜索加密的基本框架是:首先数据拥有者(发送者)对数据加密并且创建安全索引,然后将加密后的数据及其安全索引上传到云端服务器进行存储.当用户(接收者)需要对该文档进行搜索时,利用密钥对搜索关键字计算其搜索凭证(搜索令牌)发送给云服务器,云服务器利用搜索凭证为用户搜索所需要的文件数据.数据拥有者(发送者)和用户(接收者)在不同的网络环境下可以指定为不同或者相同的用户实体.在非对称环境下,假定数据的产生者、搜索凭证的产生者以及解密者是不同的用户实体,是对对称环境下可搜索加密的一种扩展与推广.

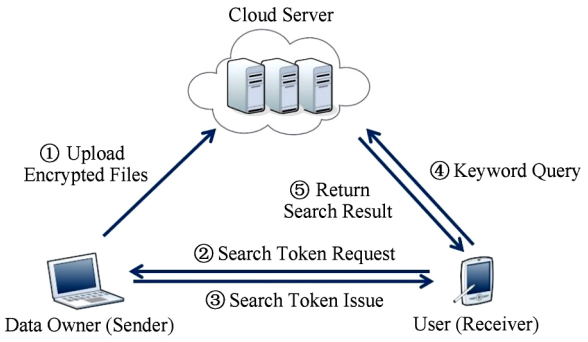

Fig. 1 Architecture of searchable encryption

图 1 可搜索加密基本框架

1.1 可搜索加密的模式

1) 一对一模式(one-to-one mode)

顾名思义,单写/单读模式即指方案仅允许单个数据拥有者(发送者)和单个用户(接收者)进行相互作用.这种模式的可搜索加密算法大都建立在对称加密体制上.2000 年 Song 等人[1]首次提出了一对一机制的可搜索加密.如图 2 所示,该模式只允许由持有私钥的用户对数据进行加密,也只能有持有私钥的用户对数据进行搜索,只相当于一个个人存储加密系统,在数据频繁交流的今天,这种模式显然不能满足人们的需求.

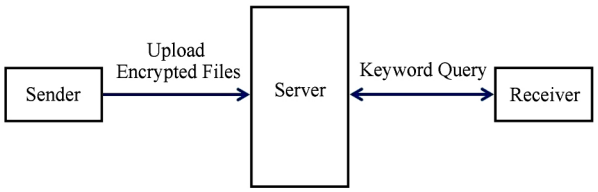

Fig. 2 One-to-one mode searchable encryption

图 2 一对一模式的可搜索加密

2) 多对一模式(many-to-one mode)

多对一模式的可搜索加密来源于公钥加密体制.如图 3 所示,它允许多个数据拥有者分别将各自的加密文件及其安全索引上传到云端服务器存储,并由单个用户发起基于关键词的查询.2004 年,Boneh 等人[2]首次提出多对一模式的可搜索加密.他们给出了基于公钥的可搜索加密(PEKS)的概念,并定义了公钥模式下可搜索加密方案的安全性定义.同年,Waters 等人[3]提出了一种新的方法构造可搜索的加密审计日志.它可以与任何现有的日志方案相结合,从而达到防篡改的目的.特别是他们还利用 Hash 链来保证数据的完整性.此外,Golle 等人[4]还提出了一种基于连接关键词的可搜索加密

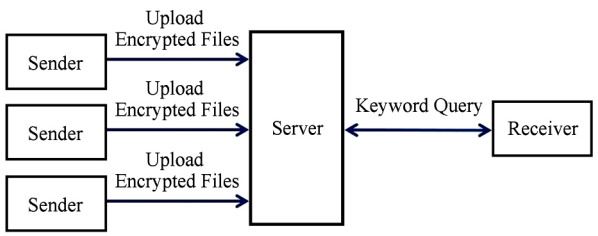

Fig. 3 Many-to-one mode searchable encryption

图 3 多对一模式的可搜索加密

方案,即方案可以搜索同时含有多个关键字的文件.但该方案的陷门过于繁琐,针对此问题,Park 等人[5]研究结合域关键词搜索的公钥加密方案问题.其主要思想是扩展 PEKS 到允许在公钥集合中连接关键词搜索.该工作也首次提出了具有常数陷门大小.

3) 一对多模式(one-to-many mode)

一对多模式的可搜索加密体制为了满足某种特定背景的应用需求而提出的.如图 4 所示,在一对多模式的方案中,允许数据拥有者创建可搜索的内容,而搜索陷门由预先设定的用户群组生成,该种模式可以使得多个用户对密文进行搜索.该类型的可搜索加密主要使用密钥共享、代理重加密等其他技术来实现.其主要工作由 Curtmola 等人[6]在 2006 年基于 Naor 的广播加密技术构造出的首个一对多模式下的可搜索加密.但是由于所有用户中仅共享一个密钥,因此每次撤销需要将新密钥分发给剩余的用户,这导致该方案具有极大的撤销开销.在其他方案中,每个用户可能具有其自己的密钥,这使得用户撤销更容易和更有效.

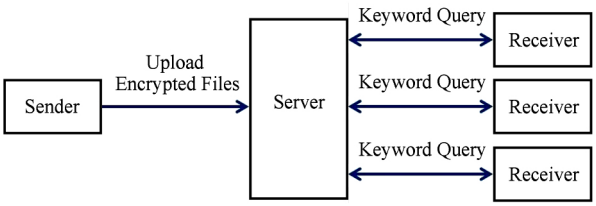

Fig. 4 One-to-many mode searchable encryption

图 4 一对多模式的可搜索加密

4) 多对多模式(many-to-many mode)

多对多模式是主要针对大型公司、网络等实体用户所设计的可搜索加密模式.如图 5 所示,其存储和搜索查询都针对预先设定的固定群组,且可以通过秘密共享技术、代理重加密等技术实现.2008 年 Wang 等人[7]引入门限隐私保护关键字搜索(trapdoor privacy preserving keyword search, TPPKS),并基于 Shamir 的秘密共享技术与 Boneh and Franklin 的基于身份的加密技术构造了第 1 个这类方案.其主要思想是仅仅允许合作用户搜索数据库.为保证搜索,每个用户使用自身的共享秘密生成一个共享陷门.随后,合作的用户验证他们的共享,若验证成功,则组合他们的共享生成一个目标关键词的陷门.为成功解密,每个用户生成一个解密共享子块用于解密.该方案是交互的,仅仅对于固定群的用户,不能进行用户添加及删除.此外,还有 Park 等人[8]利用代理重加密技术提出了 2 个多对多模式下的可搜索加密方案,方案中每个用户有自己唯一的密钥加密、搜索、加密数据,这 2 个方案均要求一个可信的密钥管理服务器.

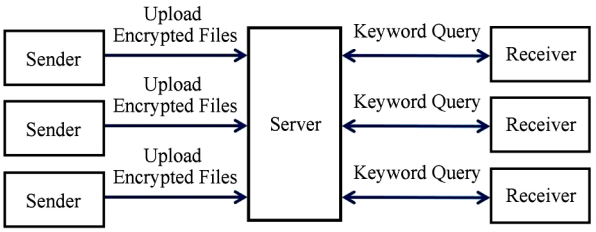

Fig. 5 Many-to-many mode searchable encryption

图 5 多对多模式的可搜索加密

模式匹配(字符串匹配)算法是指在一个文本字符串中查找模式串的一个或所有出现.考虑到数据安全和隐私保护的问题,用户在云计算环境中的模式匹配可以看作是可搜索加密的一个特例,模式串相当于关键字.密文中的模式匹配我们可称其为"安全模式匹配",可应用与云计算中的生物特征匹配、图像匹配等场景.

近几年有许多学者提出了各种安全模式匹配的实现.Baron 等人[9]提出了基于加法同态加密的安全模式匹配算法,该算法需要 $O((m+n)k^2)$ 带宽和 $O(m+n)$ 加密操作(其中 m 是模式串的长度,n 是文本串的长度).Hazay 等人[10]提出了基于模拟安全的模式匹配算法,该算法是基于 ElGamal 加密方案语义安全的前提下提出的,算法复杂度为 $O(mn)$.Faust 等人[11]在随机预言机模型下提出了可证明安全的外包模式匹配算法,该算法不依赖于加密的同态性,而是规约到子集和问题.无法同时保护文本隐私与模板隐私,且使用一系列零知识证明协议实现恶意环境下的防欺诈,效率低下.Chase 等人[12]定义了一种新的加密方案——可查询加密,提出了基于后缀树的模式匹配算法.Yasuda 等人[13]提出了一种基于 somewhat 同态加密的安全模式匹配算法,采用 somewhat 同态加密可实现密文的有限次加法和乘法运算.Saha 等人[14]进一步扩展了 Yasuda 的算法,提出了一种可实现带有通配符的安全模式匹配算法.Chase 等人[15]构造了一种子字符串可搜索对称加密方案,采用后缀树可达到与未加密时相当的渐近效率.2016 年 Strizhov 等人[16]采用位置堆树数据结构提出一种子字符串可搜索对称加密方案方案,支持高效地多用户查询的场景.

以上 4 种模式涵盖了目前可搜索加密体制的主

要的系统架构类型,也揭示了可搜索加密的一个发展历程.一般来说,可搜索加密体制的主要研究方向分为3个方面:在复杂网络环境下可搜索加密方案安全问题、可搜索加密的表达能力问题和可搜索加密方案的搜索效率问题.这3个方面涉及一个方案的底层架构,关乎整个数据层的安全性;决定实际应用过程中的通信、与存储开销,牵涉到方案的应用前景.目前可搜索加密的实现主要有3个工具:基于数论的可搜索加密、基于椭圆曲线的可搜索加密以及基于格的可搜索加密.他们都力求在方案安全性、搜索表达能力和搜索效率等方面有所突破.

1.2 可搜索加密的安全性

1996年Goldreich和Ostrovsky[17]在期刊《Journal of the ACM》上发表了重要论文"Software protection and simulation on oblivious RAMs",文中主要使用Oblivious RAMs研究如何在使用软件程序的过程中保护程序的隐私,开创了可搜索加密的研究方向.2000年,Song,Wagner和Perrig[1]在会议IEEE Symposium on Security and Privacy上发表"Practical techniques for searching on encrypted data",首次提出了在密文环境下进行关键字搜索的概念,第一次实现了对称的可搜索加密.但该方案没有提出具体的安全模型,隐含的采用了IND-CPA的安全模型.直观上理解,IND-CPA要求密文不泄露明文的任何信息.然而,在可搜索加密机制中,信息的泄露大都是通过搜索陷门和搜索操作产生的,因此,IND-CPA不适合作为可搜索加密的安全模型.Song等人[1]将文件看成由等长关键字组成的,用对称算法加密每个单词.使用流密码计算掩码,生成最后密文.搜索时,云服务器对整个密文进行扫描,依次对进行匹配搜索.缺点是该方案的搜索效率很低,时间复杂度和每篇文档的单词数量呈线性关系.为提高搜索效率,Goh[18]提出了安全索引的概念,并将其应用到可搜索加密方案中.在查询的过程中,服务器只对索引进行搜索,而不需要直接在数据密文中进行操作.

在安全性方面,Goh[18]提出了IND-CKA(semantic security against adaptive chose keyword attack)的安全模型,并基于安全索引提出了Z-INX方案,该方案利用布隆过滤器为每个文件建立一个索引.搜索时无需扫描全文,只要在建立的索引上进行匹配即可,因此,搜索复杂度降低为$O(n)$(n为文件的个数).然而,布隆过滤器的使用引入了误报的问题,使得服务器返回的结果不精确.Chang和Mitzenmacher[19]提出了第一个确定性的可搜索加密方案,该方案利用本地存储的数据字典为每个文件建立一个正向索引.每个文件索引的大小为数据字典的大小,用来表示该文件是否包含字典中对应的关键字.为了克服布隆过滤器带来的误报问题,文献[19]引入关键字字典的概念.用户为每个文件建立一个字典大小的索引,用来表明该文件包含哪些关键字.该方案实现了精确查询,不存在误报、错报的情况.倒排索引(inverted index),也常被称为反向索引,被用来存储在全文搜索下某个关键字在一个或多个文档中的映射.通过倒排索引,可以快速的获取包含这个关键字的文档列表.Curtmola等人[6]将Trapdoor的安全性以及查询泄露的2个关键字是否一样的信息这2方面同时包含在新的安全模型中,从而针对SSE提出了"适应性安全性"(adaptive security)和"非适应性安全性"(non-adaptive security)两个新的安全模型.这2个安全模型作为经典的安全模型,之后的工作或是直接使用或是为了设计方案需要,将其稍加修改.

同时,Curtmola等人[6]提出了一个适应性安全的SSE方案,它是目前为止唯一一个符合adaptive security安全模型的方案.适应性SSE方案的设计难度在于,方案证明阶段,模拟者需要以一种模棱两可的方式模拟出文件的索引,即使在没有得到敌手提出询问之前.也就是说,在敌手适应性地提出查询询问后,模拟者之前为文件建立的索引需要正确的反应出关键字和文件之间的关系.Kurosawa等人[20]将MAC添加到索引中,提出了可验证的可搜索方案,防止服务器的恶意攻击.通过将MAC值的产生使用文件标示而不使用文件密文,使得方案能够实现文件的动态更新,并在UC通用组合模型下证明其安全性.

2016年,Bost等人[21]进一步提出了具有前向安全性的可搜索加密方案.然而,现有的可搜索加密方案,一般来说其保存的密文或索引都会造成不同程度的信息泄露,如每个文件或者数据库所包含的关键词的数量,文件的长度,文件的数量,文件的ID或文件的相似性等.因此,设计可搜索加密方案的安全模型,使得无论是陷门还是索引都不泄露有关搜索关键词的任何信息,是我们今后的研究方向之一.

上述方案在设计时仅仅考虑了单用户模式.在多用户模式方面,Curtmola等人[6]结合SSE方案和广播加密方案提出了一个多用户可搜索方案,数据的拥有者动态的管理搜索凭证接收者的权限.Bao

等人[22]在“Private query on encrypted data in multi-user settings”一文中引入了一个可信第三方,即用户管理者,对搜索凭证接收者进行管理. 2016 年 Sun 等人[23]提出了支持布尔查询的非交互多用户可搜索加密方案. 2017 年 Rompay 等人[24]提出了一个能抵抗泄露攻击的多用户可搜索加密方案.

1.3 可搜索加密的表达能力

由于支持单词的 SSE 机制只允许用户一次只能发送一个单词的搜索凭证,这极不符合现实生活中多词搜索的应用需求,特别是当单词无法精确定位到用户所想要的文件时,单词搜索的限制可能需要用户使用不同关键字多轮搜索,或者是经过一轮密文搜索后,对返回结果解密,通过在明文上进行搜索来寻找目标文件,而这样的结果将给用户带来极差的操作体验. 针对这些不足,支持连接关键字搜索的可搜索加密机制开始得到研究者广泛的关注和研究. Shen, Shi 和 Waters[25]提出了基于谓词的对称加密方案,此方案可以作为设计可搜索对称加密方案的子模块. 虽然该方案不是专门为可搜索加密设计的,但是我们可以将其看成可搜索对称加密的一个通用形式. 该方案同时提出了一个基于谓词加密的安全模型,鉴于其作为可搜索对称加密的通用形式,其安全模型也较文献[6]更具一般性.

Golle 等人[4]针对之前的搜索机制中只能使用单词搜索的不足,提出了 2 种支持连接关键字搜索的 SSE 方案. 在他们的方案中,每个文件都有固定的数量的关键字域,每个域中都有特定的关键字来表征这些文件的特性. 第 1 个方案能够达到固定的在线网络开销,第 2 个方案使用固定网络开销的搜索凭证,但是依然与关键字域数量线性相关.

由于之前求关键字交集的工作时间复杂度都是线性的, Cash 等人[26]提出了一个提供布尔查询的 SSE 方案. 该方案使用了检索词频率的思想,设计了一个搜索时间复杂度为对数关系的方案,提高了搜索效率. 在加密数据库方面, Popa 等人[27]构造了适合 XML 数据类型的可搜索加密协议.

2007 年 Boneh 等人[28]提出了加密数据上连接关键字搜索、子集搜索与区间搜索. 如图 6 所示,该方案允许用户对关键词赋值位于特定区间密文文件进行查询. 2016 年 Li 等人[29-37]引入了相关相似度值和首选项的概念,利用超递增数列等技术,构造了一系列实现“AND”,“OR”,“NOT”等多功能关键字的可搜索加密方案. 与此同时, 2016 年 Wan 等人[38-39]进一步在多关键字可搜索加密的细粒度密文访问控制与搜索结果正确性可验证等方面取得了一些重要成果.

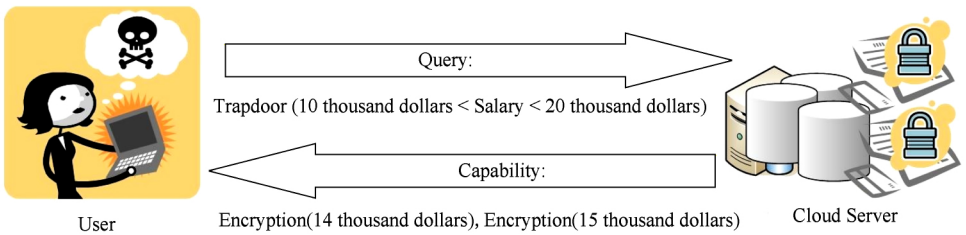

Fig. 6 Searchable encryption supporting range query

图 6 支持区间搜索的可搜索加密

属性基的可搜索加密能实现丰富的表达能力,但应同时考虑效率的问题时,主要存在于表达能力、通信效率、计算效率、属性特性 4 方面的优化与折中. 表达能力直接影响着可搜索能力,在具体应用当中,表达能力越强,则属性基加密的可搜索能力也越强. 在实际应用中,通信效率主要由密文长度决定,而计算效率主要由加解密算法产生的计算开销决定. 由于加解密是“一对多”的关系,在系统中解密对于加密而言是一个高频行为. 另一方面,目前绝大多数属性基加密方案都基于椭圆曲线的双线性群,解密计算中往往都存在双线性配对计算,双线性配对计算在实现效率方面要远远低于方案所需的其他类型运算(如指数运算). 在传统构造中,密文长度和解密代价往往都与相关属性个数线性相关,当密文中涉及很多属性时,效率将会变得很低.

根据属性的“容量”大小的分类,属性基加密方案一般可分为 2 类:支持小属性集合的方案和支持大属性集合的方案. 支持小属性集合的方案中的所有属性在公共参数建立时已经确定好,不能额外再加入更多的属性,除非系统进行重构. 相反,支持大属性集合的方案不必对所有属性进行初始化,可以随时加入新的属性. 相比而言,支持大属性集合的方案更加高效,也更贴近实际应用,但其构造的难度也更大. 因此,研究支持大属性集合的属性基加密是未

来发展的一个趋势,对于属性基加密的实际应用有着重要的推动作用.

另外,从属性是否可重用的角度考虑,属性基加密方案通常可分为属性可重用和不可重用2类方案.通常的属性基加密方案限制每个属性在访问结构中至多出现一次.如果需要出现多次,则通常将一个属性用多个"属性"来表示,但这样会导致效率变低.这也是影响属性基加密效率的一个因素.因此,研究属性的可重用性,对于属性基加密的高效实现有着重要的促进作用.

支持精确匹配的单关键字可搜索加密会泄露用户的访问模式.2007年Boneh等人[28]提出的改进方案中隐藏了用户的访问模式,但却需要更大的查询消耗.之后,为了解决陷门的安全传输问题,Dong等人[40]提出了d-PEKS方案.为应对离线消息恢复攻击,Tang等人[41]提出了注册关键词的可搜索(r-PEKS)方案.另外,精确查询意味着只返回完全匹配所查询关键字的文件.但是,输入错误和格式问题是很常见的,这时如果是支持精确查询的方案就不能返回正确的结果,基于这种应用场景,Li等人[42]首次提出了支持模糊查询的方案.如图7所示,该方案中使用通配符和编辑距离进行匹配,服务器能够返回与所查关键词相似的结果,但是却需要更大的存储空间和计算时间,但是云计算庞大的存储能力和计算能力是可以容忍的,Kamara等人[43]也对此作了研究,但这类方案依然处于初级阶段,有待进一步完善.2017年Yang等人[44]提出了一个支持通配符关键字查询的可搜索加密方案.该方案支持每个查询关键字中包含零个、一个或两个通配符的多关键字查询与灵活的用户授权与撤销,仅需一个搜索令牌便可实现对多个数据拥有者的加密文件进行批查询.Sahai和Waters[45]提出模糊身份加密方案时,只实现了最简单的访问表达能力——仅要求身份的交集达到给定的阈值,就将原先身份的匹配关系由原来的"完全匹配"变为"相似匹配",允许存在一些小的误差.Cheung和Newport[46]在标准模型和标准假设(BDBH假设)下给出了一个可证明安全的方案,但是访问结构只能支持与门.文献[46]以访问策略的表达能力(只支持一个AND关系)为代价、文献[47]以部分表达能力(有界的访问策略)和部分性能(较大的密文长度)为代价来设计了可证明安全的密文策略属性基加密(CP-ABE)系统.Emura等人[48]给出了一个常量密文的CP-ABE系统,但该系统的访问策略只能支持单一的AND关系.Herranz等人[49]则在访问策略的表达能力方面前进了一步,给出了能够支持门限策略的常量密文策略属性基加密系统.Lewko等人[50]和Okamoto等人[51]分别给出了属性个数完全不受限制的属性基加密方案,但这2个方案的效率不高且证明相对复杂.Rouselakis和Waters[52]给出了支持大属性集合的ABE方案,并利用"编程和取消"(program and cancel)证明技术和"q类"(q-type)困难问题假设对其方案给出了选择性安全性的证明.Green等人[53]结合云计算模型,允许用户提供给云服务器一个转换密钥,允许云服务器转换成满足用户属性的ElGamal型密文;而云服务器在此过程中并不能读取用户的明文.Lewko等人[54]首次在适应性模型下给出了支持属性在访问结构中重复出现任意多次的属性基加密方案.2013年Hohenberger和Waters[55]通过双线性群上的数学性质,将一些经典的属性基加密方案中的解密所需双线性运算次数都减小为常数.考虑到属性基加密在资源受限移动设备上的应用,Hohenberger等人[56]提出了高效的在线/离线属性基加密方案.Boneh等人[57]给出了基于格和全密钥同态加密(fully key-homomorphic encryption)的具有短密钥的(密钥策略)属性基加密系统.Yamada等人[58]给出了支持任意个属性集合和访问结构的紧凑参数(compact parameters)的非单调的CP-ABE.短密文属性基加密的构造,往往会导致弱的安全性——选择安全性或者需要参数化的假设.

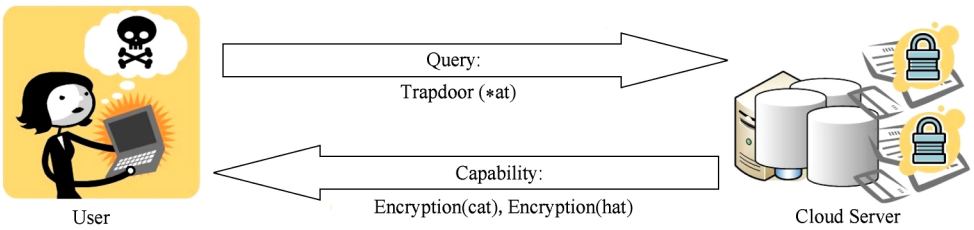

Fig. 7 Searchable encryption supporting fuzzy query

图7 支持模糊关键字搜索的可搜索加密

在属性基(身份基)加密的可搜索方案方面,Boneh 等人[59]针对隐私搜索问题,提出了函数隐私的身份基加密方案. Zheng 等人[60]分别基于 KP-ABE 及 CP-ABE 给出了 2 个可搜索属性基加密(ABEKS)的方案. 这 2 个方案不仅实现了关键字检索,还实现了验证服务器端对于用户给出检索查询是否正确回应. 随后 Sun 等人[61]和 Shi 等人[62]也分别提出了支持用户撤销和支持一定条件下关键字组合查询的方案的 ABEKS 方案. 后来 Khader[63]对 ABEKS 的模型进行了概括,并且定义了 5 个常规的参与者(一个中央权威中心、服务器、加密者、检索者、多个次级权威中心)以及他们各自负责的操作,同时对这种 ABEKS 的安全性进行了探讨. 2016 年 Sun 等人[64]进一步提出了具有外包搜索结果正确性可验证功能的属性基可搜索加密方案,同时实现了用户自适应授权查询与访问控制机制. 同年,我们[65]提出了一种新的密码学原语:在线/离线密文策略的属性基可搜索加密(OO-CP-ABSE),通过利用现有的在线/离线属性加密技术和属性基加密的外包解密技术,构造出高效的 OO-CP-ABSE 方案,使得数据拥有者端的在线计算代价最小化,同时使得数据用户端的解密计算代价最低;还给出了在云计算环境下,OO-CP-ABSE 方案在移动设备上的应用. 2017 年 Hu 等人[66]在云计算系统中提出了一个支持动态可搜索的属性基可搜索加密方案. 最近,我们① 提出了一个高效的、具有多值独立关键字搜索能力的的密文策略属性基可搜索加密方案.

然而,从当前国内外的研究现状来看,虽然当前属性基加密在表达能力、通信效率、计算效率以及属性特征方面受到了学术界广泛的研究,并越来越靠近实际应用,但距离资源受限的网络实际应用还有一定的距离. 鉴于属性基密码体制在安全可搜索当中的重要作用以及可预见的应用前景,因此,将属性基密码的安全可搜索、加密数据共享等理念应用于实际网络环境当中将是安全搜索与隐私保护的一个必然趋势,也是研究热点之一.

1.4 可搜索加密的效率

在实际应用中,用户的数据可能需要增加、删除或修改,这就要求可搜索加密方案支持这方面的需求,但是以上方案都是在用户数据是静态环境下设计的,不能满足动态修改的要求. Kamara 等人[43]提出了动态环境下的可搜索对称加密方案. 方案中,数据的加密以一种类似于同态加密的方法加密数据,索引的动态修改通过 Trapdoor 进行修改. 2016 年 Xia 等人[21,67-72]进一步在动态环境下提出了支持分级多关键字搜索的密文数据安全可搜索加密方案. 索引是一个基于平衡二叉树的树形索引,搜索时进行深度搜索,具有较高的搜索效率. 因为数据和索引的动态修改需要服务器的参与,服务器在动态修改的过程中,不可避免地会获取一定的泄露信息. 因此,在安全性要求方面要弱于静态环境下的方案. Hahn 和 Kerschbaum[73]给出一种“懒”的索引建立方法:凡是第一次询问的关键字,其索引使用全文扫描的方法建立;而之前询问过的关键字在原有的索引上更新即可. 随后,Kamara 和 Papamanthou[74]利用多核结构构造了可并行计算的可搜索加密方案. Kurosawa 等人[75]将索引中 MAC 值直接作用在密文上,使得文件的更新开销很大.

大多数的可搜索对称加密方案假设服务器在密文上进行全文扫描或者直接在索引上进行匹配. Chase 和 Kamara 等人[76]特别研究了具有结构化的数据(矩阵、带标签的数据、图、树、带标签的图)的可搜索加密体制,并且将其应用在泄露控制方案中. Wen 等人[77]在新兴智能电网市场拍卖应用场景中给出了相应的可搜索加密解决方案. Yang 等人[78]针对云计算应用场景给出了文件更新代价为常数的动态可搜索对称加密方案. Liu 等人[79]研究了可搜索加密中模式搜索泄露攻击以及相应的解决方案. Arriaga 等人[80]研究了非对称可搜索加密中的陷门隐私问题. Naveed 等人[81]通过引入一个新的密码原语盲化存储(blind storage)构造了一种动态可搜索加密方案. 随后,Emura 等人[82]给出了适应性安全的可搜索加密的通用构造. Hahn 等人[83]基于访问模式的索引学习提出了可搜索对称加密机制,该机制并支持了数据的高效更新. Bösch 等人[84]利用关键字字典的概念构造出一个高效的基于内积加密的可搜索方案. Ibraimi 等人[85]针对恶意邮件的拦截问题,提出了授权关键字搜索的概念,即网关能够生成由病毒作为关键字的陷门,从而可以对恶意邮件进行拦截. Sedghi 等人[86]提出了带通配符的搜索方案. Dong 等人[87]基于 RSA 问题,提出了代理重加密搜索方案,方案需要一个可信第三方存在作为

① 王海江, 董晓蕾, 曹珍富. 具有快速关键字查询功能的多值独立的密文策略属性基加密方案[J]. IEEE Trans on Service Computing, 2017. DOI:10.1109/TSC.2017.2753231. 待发表.

密钥管理方.云服务器可以将一个用户的数据密文通过代理重加密转换成另一用户的数据密文,这样可以实现用户的数据分享,同时,每个用户只需保有自己密钥而不用共享密钥.Kuzu 等人[88]利用最小邻近 Hash 函数和 Bloom 过滤器提出了一个高效的模糊关键字可搜索加密方案.2016 年 Krishna 等人[89]在此基础上进一步提出了隐私保护的多关键字分级模糊可搜索加密方案.

现有的隐私保护模式匹配协议多利用公钥(全)同态加密技术实现[90],其巨大的计算开销无法适应移动设备存储、计算资源受限的客观需求.为了解决上述问题,我们[91]不依赖于公钥全同态加密技术,基于任意单向陷门置换提出了高效的隐私保护外包模式匹配协议.该协议将外包模式匹配转化为外包多项式乘法与卷积运算,利用一次任意单向陷门置换在离线状态加密对称密钥,再用该对称密钥在在线状态下,通过仅包含简单加法、乘法运算的对称全同态映射对文本与模板中的每一个字符进行批加密;使得公钥加密在文本发送端与模板查询端的计算开销分别由 $O(n)$和 $O(m)$降低到 $O(1)$.然后,处于半可信或恶意模型下的云服务器在密文域上进行隐私保护的多项式运算,即完成外包模式匹配工作.在隐私保护模式匹配的基础上,我们还进一步提出了隐私保护的外包医疗图像特征提取与匹配算法[92],实现了安全智慧诊疗系统.

2 存在问题与未来研究方向

安全搜索领域的国内外学者,在一对一、多对一、一对多和多对多 4 种模式下,分别针对可搜索加密的安全性、搜索的表达能力和搜索效率等重要关键性问题进行研究,产生了一系列重要研究结果.但仍存在以下问题值得进一步研究.

1) 在可搜索加密的基础理论研究方面,可搜索加密是近年来发展起来的一种支持用户在密文上进行关键字查找的密码学原语,它能够为用户节省大量的网络和计算开销,并充分利用云端服务器庞大的计算资源进行密文上的关键字查找.因此,可搜索加密机制的基础理论研究主要集中在研究密文搜索语句的表达能力、可搜索加密方案的安全性、可搜索加密方案的高效性等方面.

① 研究密文搜索语句的表达能力.灵活的密文搜索语句不仅能够让用户可以更加精确地定位到所需要的加密数据文件,同时也可以让用户能够更加灵活地表述搜索需求.本项目致力于密文搜索能力的复杂性的探索,研究支持模糊搜索、有序搜索、区间搜索以及子集搜索等复杂性密文可搜索能力.

② 研究可搜索加密方案的安全性.针对不同需求,结合可搜索方案的不同表达能力,定义不同可搜索加密方案的安全级别.在不同安全级别的基础上,寻求简单高效的难题假设证明可搜索加密方案的安全性.

③ 研究可搜索加密方案的高效性.研究可搜索加密方案的搜索凭证、搜索关键字与密钥、密文间的关系,探索用越短的密钥、密文来实现表达能力越丰富的可搜索加密方案.进一步地,结合不同的需求和安全级别,探索高效安全的可搜索加密.

在利用属性基加密实现安全搜索方面,在属性基加密从理论走向实际应用的过程中,效率是一个主要因素.研究属性基加密以及签名的安全搜索与隐私保护的一般理论,主要集中在属性基加密以及签名的高效性上,包括表达能力、通信效率、计算效率以及属性特征等方面.

④ 寻求表达能力丰富的属性基加密方案.属性基密码最重要的特色就是具有丰富的表达能力,而表达能力的强弱也直接反映了可搜索能力的强弱.因此,寻求满足更丰富表达能力的能够支持任意语言的属性基加密方案,是研究属性基密码的可搜索机制的一个重要内容,也是高效可搜索的基石.

⑤ 寻求更短密文、短密钥、短公开参数的属性基加密方案.在同等安全性假设的基础上,短密文是密码方案设计中第一追求的目标.要构造高效的属性基加密方案,最关键的科学问题就是缩短密文的长短.寻求能够满足更短密文(密文长度为常数)、更短密钥(私钥长度为常数)以及更短公开参数(公开参数为常数)以及同时满足以上 3 个特点的高效属性基加解密算法,是基于属性可搜索机制的高效性的重要保证.

⑥ 寻求高效的解密方案及加密数据外包计算方案.配对计算会消耗很多时间,减少配对的使用次数会提高加密解密的工作效率,寻求快速解密功能的属性基密码方案,尤其是配对次数与属性数目相独立的解密方案;或者是探寻无配对的属性基密码方案;提出高效的加密数据外包计算方案.

⑦ 寻求简单的难题假设.假设的简单与否,也是影响属性基加密效率的一个因素.在同等安全级别的条件下,寻求越简单的难题假设,势必会使属性基加密在安全可搜索的应用方面起到非常大的促进作用.

⑧ 基于属性的隐私保护. 属性基加密提供了共享解密权限的机制,本身是对解密者的一种隐私保护. 进一步地,研究匿名属性基加密,以期提高属性和加密策略的隐私性.

此外,利用格等经典结构,设计抗量子攻击的可搜索加密方案. 鉴于格上困难问题可以抵抗量子攻击的特性来设计抗量子攻击的可搜索加密方案. 首先构建出可搜索加密方案的基本框架,其次,将方案的安全性归约到格上的困难问题,确定可以保证格上问题困难性的的相关参数范围,将该参数范围对应到加密方案中,确定方案中应选取的相关参数. 为此我们需要研究可搜索加密方案构造与格结构之间的关系及格上的困难问题的困难性. 借助于格上的困难问题,设计出可以抵抗量子攻击的可搜索加密方案,在保证安全性的条件下,对方案的效率进行分析优化,对其性能进行扩展,使得方案满足一定的鲁棒性、实用性.

2) 在安全搜索与隐私保护的基础理论研究的基础上,探索安全搜索与隐私保护的一般规律与方法,并在此基础之上进行方案的轻量化研究,并探索在安全搜索与隐私保护的过程中一次使用有关的公钥加密方案,以期适用于存储、计算资源受限网络环境.

① 探索可搜索加密轻量化方法. 可搜索加密作为安全搜索的一个基础理论与必要工具,在保证搜索语句的表达能力与可搜索加密方案达到一定安全级别的前提下,结合实际网络环境的应用需求,对可搜索加密方案进行轻量化. 由于在实际网络中资源受到限制,而普通的可搜索加密方案要求较大的计算能力及传输能力,因此无法直接应用. 相应地,我们需要将可搜索加密方案进行轻量化处理,降低其计算复杂度和传输复杂度. 研究支持模糊搜索、有序搜索、区间搜索以及子集搜索等复杂性可搜索能力的轻量化处理方法,探寻满足不同安全级别可搜索加密方案的轻量化方法,以期满足各类网络环境的不同需求.

② 探索属性基加密实现安全搜索的轻量化和高效实现方法. 属性基加密作为安全搜索与隐私保护的一种基本工具与方法,无论是现有的属性基加密方案还是属性基签名方案或属性基安全协议,都还远远不够高效,无法为实际所用. 特别对于资源受限的网络设备而言,加密系统的效率尤为重要. 故在研究基于属性基加密以及签名的安全搜索与隐私保护的一般理论的基础之上,需要对其进行优化,以期能够进一步提高效率,包括表达能力更加丰富、更短密文密钥以及公开参数、加解密配对次数越少、难题假设越简单等方面.

对于那些经过优化还未能达到应用于资源受限的网络设备的方案与协议,采取轻量化的方法,允许存在一次或多次轻量化方法,将原来资源与开销较大的计算进行轻量化,以期能够用于资源受限的网络设备. 同时,在保证高效轻量化的基础上,探索减少轻量化属性基加密的使用次数的途径或方法.

3) 在研究安全搜索与隐私保护的基础理论、探索安全搜索与隐私保护的新方法与新技术的基础上,针对各类新兴网络环境的不同应用场景,研究安全搜索与隐私保护的具体实施方案,减少大开销运算的使用,期待大开销达到“少量计算,多次使用”的目的,使其更适合在资源受限的网络中部署. 主要存在网络应用中的 2 个关键问题值得进一步研究:

① 传感存储服务中的动态安全搜索技术. 移动网络环境下的传感信息呈现动态性、实时性、大规模等特点,我们拟从保护数据安全和用户隐私出发,探寻在传感存储系统中的动态可搜索加密方案.

② 现代物流系统中隐私保护的动态查询技术. 现有的物流系统中,寄件人和收件人的信息都会显示在邮寄单上,用户的数据安全和用户隐私受到了极大的威胁. 同时,邮件单上的信息是静态的,而物品的位置是实时变化的,因此无法直接应用于移动设备中. 在移动网络环境下的物流系统中,在保证传统物流数据安全与隐私保护的基础上,着重解决物流地址的实时变化以及位置隐私保护问题. 同时,使用可搜索加密技术对物流传感信息提供实时查询追踪等服务.

3 结束语

本文围绕可搜索加密的新理论、新方法和新技术,针对可搜索加密的模式、安全性、表达能力和搜索效率等方面进行综述. 主要内容包括:安全搜索必不可少的新理论,包括可搜索加密、属性基加密及其轻量化等相关理论;基于轻量化公钥密码算法,并在此基础上研究减少公钥密码算法的使用次数实现资源受限网络安全搜索新方法;针对体域网、车载网、智能电网等具体网络应用服务,介绍新理论、新方法的应用,期望找到一些高效解决这类问题的具体方法. 最后,还指出了该领域当前研究中需要解决的公开问题和未来的发展趋势.

我们长期以来的一个观点是:不管是安全搜索还是其他安全或隐私保护问题,如果频繁使用开销极大的公钥加密,其意义最多只是提供了一个"从无到有"的思路.一个方案要付诸实践,在不得不使用公钥密码算法时,必须研究减少公钥密码的使用次数.

参 考 文 献

[1] Song Xiaodong, Wagner D, Perrig A. Practical techniques for searches on encrypted data [C] //Proc of IEEE Symp on Security and Privacy 2000. Piscataway, NJ: IEEE, 2000: 44-55

[2] Boneh D, Kushilevitz E, Ostrovsky R. Public Key encryption with keyword search [G] //LNCS 3027: Proc of Eurocrypt 2004. Berlin: Springer, 2004: 506-522

[3] Waters B, Balfanz D, Durfee G. Building an encrypted and searchable audit log [C] //Proc of NDSS 2004. Berlin: Springer, 2004: 5-6

[4] Golle P, Staddon J, Waters B. Secure conjunctive keyword search over encrypted data [C] //Proc of ACNS 2004. Berlin: Springer, 2004: 31-45

[5] Park D J, Kim K, Lee P J. Public key encryption with conjunctive field keyword search [J]. Information Security Applications, 2005, 3325: 73-86

[6] Curtmola R, Garay J A, Kamara S, et al. Searchable symmetric encryption: Improved definitions and efficient constructions [C] //Proc of ACM CCS 2006. New York: ACM, 2006: 79-88

[7] Wang Peishun, Wang Huaxiong, Pieprzyk J. Threshold privacy preserving keyword searches [G] //Proc of SOFSEM 2008. Berlin: Springer, 2008: 646-658

[8] Park D J, Cha J Y, Lee P J. Searchable keyword-based encryption, 2005/367 [R/OL]. IACR ePrint Cryptography Archive, 2005 [2017-06-30]. http://eprint.iacr.org/2005/367

[9] Baron J, Defrawy K. E, Minkovich K, et al. R. 5pm: Secure pattern matching [C] //Proc of the 8th Int Conf on Security and Cryptography for Networks. New York: ACM, 2012: 222-240

[10] Hazay C, Toft T. Computationally secure pattern matching in the presence of malicious adversaries [C] //Proc of ASIACRYPT 2010. Berlin: Springer, 2010: 195-212

[11] Faust S, Hazay C, Venturi D. Outsourced pattern matching [C] //Proc of Int Colloquium on Automata, Languages, and Programming 2013. Berlin: Springer, 2013: 545-556

[12] Chase M, Shen E. Pattern matching encryption, 2014/638 [R/OL]. IACR ePrint Cryptography Archive, 2014 [2017-06-30]. http://eprint.iacr.org/2014/638

[13] Yasuda M, Shimoyama T, Kogure J, et al. Secure pattern matching using somewhat homomorphic encryption [C] //Proc of ACM Workshop on Cloud Computing Security Workshop 2013. New York: ACM, 2013: 65-76

[14] Saha T K, Koshiba T. An enhancement of privacy-preserving wildcards pattern matching [C] //Proc of Int Symp on Foundations and Practice of Security 2016. Berlin: Springer, 2016: 145-160

[15] Chase M, Shen E. Substring-searchable symmetric encryption [J]. Proceedings on Privacy Enhancing Technologies, 2015 (2): 263-281

[16] Strizhov M, Osman Z, Ray I. Substring position search over encrypted cloud data supporting efficient multi-user setup [J]. Future Internet, 2016, 8(3): 1-26

[17] Goldreich O, Ostrovsky R. Software protection and simulation on oblivious RAMs [J]. Journal of the ACM, 1996, 43(3): 431-473

[18] Goh E-J. Secure indexes, 2003/216 [R/OL]. IACR ePrint Cryptography Archive, 2003 [2017-06-30]. http://eprint.iacr.org/2003/216, 2013

[19] Chang Yancheng, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data [C] //Proc of ACNS 2005. Berlin: Springer, 2005: 442-455

[20] Kurosawa K, Ohtaki Y. UC-secure searchable symmetric encryption [C] //Proc of Int Conf on Financial Cryptography and Data Security 2012. New York: ACM, 2012: 285-298

[21] Bost R. $\Sigma o\varphi o\zeta$: Forward secure searchable encryption [C] //Proc of ACM CCS 2016. New York: ACM, 2016: 1143-1154

[22] Bao Feng, Deng R H, Ding X, et al. Private query on encrypted data in multi-user settings [C] //Proc of Int Conf on Information Security Practice and Experience 2008. Berlin: Springer, 2008: 71-85

[23] Sun Shifeng, Liu J, Sakzad A, et al. An efficient non-interactive multi-client searchable encryption with support for boolean queries [C] //Proc of ESORICS 2016. Berlin: Springer, 2016: 154-172

[24] Rompay V, Cédric R Molva, Önen M. A leakage-abuse attack against multi-user searchable encryption [J]. Privacy Enhancing Technologies, 2017, 3(2017): 164-174

[25] Shen E, Shi E, Waters B. Predicate privacy in encryption systems [C] //Proc of Theory of Cryptography Conference 2009. Berlin: Springer, 2009: 457-473

[26] Cash D, Jarecki S, Jutla C, et al. Highly-scalable searchable symmetric encryption with support for boolean queries [C] //Proc of CRYPTO 2013. Berlin: Springer, 2013: 353-373

[27] Popa R A, Redfield C, Zeldovich N, et al. CryptDB: Protecting confidentiality with encrypted query processing [C] //Proc of the 23rd ACM Symp on Operating Systems Principles 2011. New York: ACM, 2011: 85-100

[28] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data [C] //Proc of Theory of Cryptography Conf 2007. Berlin: Springer, 2007: 535-554

[29] Li Hongwei, Yang Yi, Luan T H, et al. Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data [J]. IEEE Trans on Dependable and Secure Computing. 2016, 13(3): 312-325

[30] Chen Rongmao, Mu Yi, Yang Guomin, et al. Dual-server public-key encryption with keyword search for secure cloud storage [J]. IEEE Trans on Information Forensics and Security, 2016, 11(4): 789-798

[31] Chen Rongmao, Mu Yi, Yang Guomin, et al. Server-aided public key encryption with keyword search [J]. IEEE Trans on Information Forensics and Security, 2016, 11(12): 2833-2842

[32] Fu Zhangjie, Ren Kui, Shu Jiangang, et al. Enabling personalized search over encrypted outsourced data with efficiency improvement [J]. IEEE Trans on Parallel and Distributed Systems, 2016, 27(9): 2546-2559

[33] Li Hongwei, Yang Yi, Luan T H, et al. Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data [J]. IEEE Trans on Dependable and Secure Computing, 2016, 13(3): 312-325

[34] Fu Zhangjie, Wu Xinle, Guan Chaowen, et al. Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement [J]. IEEE Trans on Information Forensics and Security, 2016, 11(12): 2706-2716

[35] Yang Yang, Ma Maode. Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds [J]. IEEE Trans on Information Forensics and Security, 2016, 11(4): 746-759

[36] Zhang Wei, Lin Yaping, Xiao Sheng, et al. Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing [J]. IEEE Trans on Computers, 2016, 65(5): 1566-1577

[37] Shao Feng, Zhang Shun, Zhong Hong, et al. Keyword search protocol with privacy preservation using ID-based proxy reencryption [J]. International Journal of Security and Networks, 2016, 11(4): 188-195

[38] Wan Zhiguo, Deng R H. VPSearch: Achieving verifiability for privacy-preserving multi-keyword search over encrypted cloud data [J]. IEEE Trans on Dependable and Secure Computing, 2016, DOI: 10.1109/TDSC.2016.2635128

[39] Liang Kaitai, Huang Xinyi, Guo Fuchun, et al. Privacy-preserving and regular language search over encrypted cloud data [J]. IEEE Trans on Information Forensics and Security, 2016, 11(10): 2365-2376

[40] Dong Changyu, Russello G, Dulay N. Shared and searchable encrypted data for untrusted servers [J]. Journal of Computer Security, 2011, 19(3): 367-397

[41] Tang Qiang, Chen Liqun. Public-key encryption with registered keyword search [C] //Proc of European Public Key Infrastructures Workshop 2009. Berlin: Springer, 2009: 163-178

[42] Li Jin, Wang Qian, Wang Cong, et al. Fuzzy keyword search over encrypted data in cloud computing [C] //Proc of IEEE INFOCOM 2010. Piscataway, NJ: IEEE, 2010: 441-445

[43] Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption [C] //Proc of ACM CCS 2012. New York: ACM, 2012: 965-976

[44] Yang Yang, Liu Ximeng, Deng R H, et al. Flexible wildcard searchable encryption system [J]. IEEE Trans on Services Computing, 2017, DOI: 10.1109/TSC.2017.2714669

[45] Sahai A, Waters B. Fuzzy identity-based encryption [C] //Proc of EUROCRYPT 2005. Berlin: Springer, 2005: 457-473

[46] Cheung L, Newport C. Provably secure ciphertext policy ABE [C] //Proc of ACM CCS 2007. Berlin: Springer, 2007: 456-465

[47] Goyal V, Jain A, Pandey O, et al. Bounded ciphertext policy attribute based encryption [C] //Proc of Int Colloquium on Automata, Languages, and Programming 2008. Berlin: Springer, 2008: 579-591

[48] Emura K, Miyaji A, Nomura A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length [C] //Proc of Int Conf on Information Security Practice and Experience 2009. New York: ACM, 2009: 13-23

[49] Herranz J, Laguillaumie F, Ràfols C. Constant size ciphertexts in threshold attribute-based encryption [C] //Proc of PKC 2010. New York: ACM, 2010: 19-34

[50] Allison B Lewko, Waters B. Unbounded HIBE and attribute-based encryption [C] //Proc of EUROCRYPT 2011. Berlin: Springer, 2011: 547-567

[51] Okamoto T, Takashima K. Fully secure unbounded inner-product and attribute-based encryption [C] //Proc of ACNS 2012. Berlin: Springer, 2012: 349-366

[52] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption [C] //Proc of ACM CCS 2013. New York: ACM, 2013: 463-474

[53] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C] //Proc of USENIX 2011. New York: ACM, 2011: 34-49

[54] Lewko A, Waters B. New proof methods for attribute-based encryption: Achieving full security through selective techniques [C] //Proc of CRYPTO 2012. Berlin: Springer, 2012: 180-198

[55] Hohenberger S, Waters B. Attribute-based encryption with fast decryption [C] //Proc of PKC 2013. Berlin: Springer, 2013: 162-179

[56] Hohenberger S, Waters B. Online/offline attribute-based encryption [C] //Proc of PKC 2014. Berlin: Springer, 2014: 293-310

[57] Boneh D, Gentry C, Gorbunov S, et al. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits [C] //Proc of EUROCRYPT 2014. Berlin: Springer, 2014: 533-556

[58] Yamada S, Attrapadung N, Hanaoka G, et al. A framework and compact constructions for non-monotonic attribute-based encryption [C] //Proc of PKC 2014. Berlin: Springer, 2014: 275-292

[59] Boneh D, Raghunathan A, Segev G. Function-private identity-based encryption: Hiding the function in functional encryption [C] //Proc of CRYPTO 2013. Berlin: Springer, 2013:461-478

[60] Zheng Qingji, Xu Shouhuai, Ateniese G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data [C] //Proc of IEEE INFOCOM 2014. Piscataway, NJ: IEEE, 2014: 522-530

[61] Sun Wenhai, Yu Shucheng, Lou Wenjing, et al. Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud [C] //Proc of IEEE INFOCOM 2014. Piscataway, NJ: IEEE, 2014: 226-234

[62] Shi Jie, Lai Junzuo, Li Yingjiu, et al. Authorized keyword search on encrypted data [C] //Proc of ESORICS 2014. Berlin: Springer, 2014: 419-435

[63] Khader D. Introduction to attribute based searchable encryption [C] //Proc of Communications and Multimedia Security 2014. Berlin: Springer, 2014: 131-135

[64] Sun Wenhai, Yu Shucheng, Lou Wenjing, et al. Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud [J]. IEEE Trans on Parallel and Distributed Systems, 2016, 27(4): 1187-1198

[65] Chen Dongdong, Cao Zhenfu, Dong Xiaolei. Online/offline ciphertext-policy attribute-based searchable encryption [J]. Journal of Computer Research and Development, 2016, 53(10): 2365-2375 (in Chinese)

(**陈冬冬, 曹珍富, 董晓蕾. 在线/离线密文策略属性基可搜索加密**[J]. **计算机研究与发展**, 2016, 53(10): 2365-2375)

[66] Hu Baishuang, Liu Qin, Liu Xuhui, et al. DABKS: Dynamic attribute-based keyword search in cloud computing [C] //Proc of IEEE Int Conf on Communications (ICC 2017). Piscataway, NJ: IEEE, 2017: 1-6

[67] Xia Zhihua, Wang Xinhui, Sun Xingming, et al. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data [J]. IEEE Trans on Parallel and Distributed Systems, 2016, 27(2): 340-352

[68] Cui Baojiang, Liu Zheli, Wang Lingyu. Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage [J]. IEEE Trans on Computers, 2016, 65(8): 2374-2385

[69] Wang Qian, He Meiqi, Du Minxin, et al. Searchable encryption over feature-rich data [J]. IEEE Trans on Dependable and Secure Computing, 2016, DOI: 10.1109/TDSC.2016.2593444

[70] Wu Xinle, Fu Zhangjie, Sun Xingming. Text-based searchable encryption in cloud: A survey [J]. Journal of Internet Technology, 2017, 18(1): 207-213

[71] Pouliot D, Wright C V. The shadow nemesis: Inference attacks on efficiently deployable, efficiently searchable encryption [C] //Proc of ACM SIGSAC Conf on Computer and Communications Security 2016. New York: ACM, 2016: 1341-1352

[72] Li Jiguo, Lin Xiaonan, Zhang Yichen, et al. KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage [J]. IEEE Trans on Services Computing, 2016, DOI: 10.1109/TSC.2016.2542813

[73] Hahn F, Kerschbaum F. Searchable encryption with secure and efficient updates [C] //Proc of ACM CCS 2014. New York: ACM, 2014: 310-320

[74] Kamara S, Papamanthou C. Parallel and dynamic searchable symmetric encryption [C] //Proc of Int Conf on Financial Cryptography and Data Security 2013. New York: ACM, 2013: 258-274

[75] Kurosawa K, Ohtaki Y. How to update documents verifiably in searchable symmetric encryption [C] //Proc of Int Conf on Cryptology and Network Security 2013. Berlin: Springer, 2013: 309-328

[76] Chase M, Kamara S. Structured encryption and controlled disclosure [C] //Proc of ACNS 2010. Berlin: Springer, 2010: 577-594

[77] Wen Mi, Lu Rongxing, Lei Jingsheng, et al. Sesa: An efficient searchable encryption scheme for auction in emerging smart grid marketing [J]. Security and Communication Networks, 2014, 7(1): 234-244

[78] Yang Yi, Li Hongwei, Liu Wenchao, et al. Secure dynamic searchable symmetric encryption with constant document update cost [C] //Proc of GLOBECOM 2014. Piscataway, NJ: IEEE, 2014: 775-780

[79] Liu Chang, Zhu Liehuang, Wang Mingzhong, et al. Search pattern leakage in searchable encryption: Attacks and new construction [J]. Information Sciences, 2010, 265: 176-188

[80] Arriaga A, Tang Qiang, Ryan P. Trapdoor privacy in asymmetric searchable encryption schemes [C] //Proc of Int Conf on Cryptology in Africa 2014. Berlin: Springer, 2014: 31-50

[81] Naveed M, Prabhakaran M, Gunter C A. Dynamic searchable encryption via blind storage [C] //Proc of IEEE Symp on Security and Privacy 2014. Piscataway, NJ: IEEE, 2014: 639-654

[82] Emura K, Miyaji A, Rahman M S, et al. Generic constructions of secure-channel free searchable encryption with adaptive security [J]. Security and Communication Networks, 2015, 8(8): 1547-1560

[83] Hahn F, Kerschbaum F. Searchable encryption with secure and efficient updates [C] //Proc of ACM CCS. New York: ACM, 2014: 310-320

[84] Bösch C, Tang Qiang, Hartel P, et al. Selective document retrieval from encrypted database [C] //Proc of Int Conf on Information Security 2012. New York: ACM, 2012: 224-241

[85] Ibraimi L, Nikova S, Hartel P, et al. Public-key encryption with delegated search [C] //Proc of ACNS 2011. Berlin: Springer, 2011: 532-549

[86] Sedghi S, Van L P, Nikova S, et al. Searching keywords with wildcards on encrypted data [C] //Proc of Int Conf on Security and Cryptography for Networks 2010. Berlin: Springer, 2010: 138-153

[87] Dong Changyu, Russello G, Dulay N. Shared and searchable encrypted data for untrusted servers [J]. Journal of Computer Security, 2011, 19(3): 367-397

[88] Kuzu M, Islam M S, Kantarcioglu M. Efficient similarity search over encrypted data [C] //Proc of IEEE ICDE 2012. Piscataway, NJ: IEEE, 2012: 1156-1167

[89] Krishna C R, Mittal S A. Privacy preserving synonym based fuzzy multi-keyword ranked search over encrypted cloud data [C] //Proc of Computing 2016. Berlin: Springer, 2016: 1187-1194

[90] Li Dongmei, Dong Xiaolei, Cao Zhenfu. Secure and privacy-preserving pattern matching in outsourced computing [J]. Security and Communication Networks, 2016, 9(16): 3444-3451

[91] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al, PPDM: A privacy-preserving protocol for cloud-assisted e-healthcare systems [J]. IEEE Journal of Selected Topics in Signal Processing, 2015, 9(7): 1332-1344

[92] Zhou Jun, Cao Zhenfu, Dong Xiaolei. PPOPM: More efficient privacy preserving outsourced pattern matching [C] //Proc of ESORICS 2016. Berlin: Springer, 2016: 135-153

Dong Xiaolei, born in 1971. PhD, distinguished professor in East China Normal University. Her main research interests include number theory, cryptography and network security, and big data security and privacy preserving.

Zhou Jun, born in 1982. PhD, associate professor in East China Normal University. His main research interests include key theories for secure outsourced computation and privacy preserving, and the applied cryptography in big data processing (jzhou@sei.ecnu.edu.cn).

Cao Zhenfu, born in 1962. PhD, distinguished professor in East China Normal University. His main research interests include number theory and new theories for cryptography and network security (security and privacy preserving for cloud computing and big data processing).