doi:10.11959/j.issn.1000-436x.2016186

面向物联网搜索的数据隐私保护研究综述

王佳慧[1,2]，刘川意[2,3]，方滨兴[2,3]
（1. 北京邮电大学计算机学院，北京 100876；2. 哈尔滨工业大学深圳研究生院，广东 深圳 518055；
3. 东莞电子科技大学电子信息工程研究院，广东 东莞 523000）

摘 要：随着物联网和云计算、大数据技术的飞速发展和广泛应用，迫切需要实时、快速、精准地搜索现实世界中物理实体等相关信息，使物联网搜索引擎应运而生。然而，由于物联网搜索引擎的开放性，使在互联网搜索领域就已经存在的数据隐私问题变得更加突出。阐述了物联网搜索隐私保护的研究背景和挑战，提出了面向物联网搜索的数据隐私保护框架及相关技术。综述了近年来提出的、适用于物联网搜索的数据隐私保护技术的研究背景、最新研究进展以及主要研究方向，最后，指出了一些重要研究方向，为未来研究工作指明方向。

关键词：物联网搜索；隐私保护；属性加密；密文搜索；隐藏随机访问模式
中图分类号：TP309 **文献标识码**：A

Survey on data preserving for the search of internet of things

WANG Jia-hui[1,2], LIU Chuan-yi[2,3], FANG Bin-xing[2,3]
(1. School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Harbin Institute of Technology(Shenzhen), Shenzhen 518055, China;
3. Electronic and Information Engineering Institute, Dongguan University of Electronic Science and Technology, Dongguan 523000, China)

Abstract: With the rapid development of the internet of things(IoT) technology and big data technology, the search engine for internet of things become a hot research topic. However, because of the openness of the search of IoT, the privacy in traditional internet search area become more prominent and face more challenges. Firstly, the research background and challenges of privacy preservation for search of IoT were described. Secondly, the framework of data privacy preservation for search of IoT were presented and several main research domain in this framework were described. Thirdly, several privacy preservation technology appropriated for search of IoT were described in detail, including the background, recent research work, main research directions. Finally, the current problems and important research field for future were presented.

Key words: search for internet of things, privacy preservation, attribute based encryption, searchable encryption, oblivious random access machine

1 引言

在拥有海量实体的物联网[1]中，人们越来越需要实时、快速、精准地搜索现实世界中物理实体等相关信息，如附近哪里有无烟、环境好的咖啡厅、从家到机场的道路哪条是最畅通的等，由此，面向物联网的数据搜索引擎应运而生。由瑞士苏黎世联邦理工大学、德国吕贝克大学以及德国都科摩通信实验室设计的 Dyser[2]是一个物联网实时搜索引擎，不仅支持物理实体静态信息的搜索，还能根据用户

收稿日期：2016-05-05；**修回日期**：2016-06-15
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA016001）；广东省产学研合作基金资助项目（No.2016B090921001）；山东省自主创新及成果转化专项基金资助项目（No.2014ZZCX03411）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA016001), Production-Study-Research Cooperation Project in Guangdong Province (No.2016B090921001), Innovation Project in Shandong Province (No.2014ZZCX03411)

指定的当前状态实时搜索物理实体。Shodan[3]是提供在线设备的物联网搜索引擎，只要输入搜索关键字，就可以找到全世界与互联网相连的网络摄像头、路由器、信号灯、核电站、冰箱、医疗设备等包含信息漏洞的设备。然而这些原型系统都只支持物联网的特定搜索条件和场景的搜索，还无法真正解决目前全球化的物联网搜索问题，而且这些解决方案也未得到业界的一致认同和实际的广泛应用。

真正意义上全球化的物联网搜索是指根据一定的策略和方法从物联网上实时、快速、精准地获取各种物理实体、人物、信息等，并对这些对象进行高效的组织和管理，从而为用户提供各类搜索服务，返回满足其搜索请求的信息。尽管目前物联网搜索仍处于萌芽状态，由此带来的数据隐私问题却已经不容忽视。韩国产业研究院认为，2020 年因物联网安全隐私问题导致的经济损失将达到 180 亿美元[注1]。由于物联网搜索的应用领域广泛，包括国民经济和社会发展各个领域，所以其隐私泄露不仅包含传统的网络虚拟空间，还将进一步侵犯到实体生活当中，除了经济损失外，个人的生命安全以及国家基础设施也都将受到极大的威胁。由于物联网搜索对象和搜索空间的广泛性、搜索数据的高度动态性、搜索内容的高度时空性、搜索语言的复杂性等特点，使物联网搜索的数据隐私保护面临更大的安全挑战。可以说数据隐私保护是制约全球化的物联网搜索发展并实际应用于产业界的关键因素。

首先，物联网搜索服务提供者后台服务器系统存有大量通过摄像头、传感器等感知设备收集的数据信息，而由于物联网搜索应用领域广泛，包括国民经济各行业乃至社会发展各领域，这些数据信息如果不加以安全隐私的规范，将成为一个庞大的盯梢系统。类似于“棱镜计划”的通过内部数据搜索和挖掘导致的个人数据隐私侵犯将更加广泛和便利。因此，物联网搜索过程中的数据内容隐私保护变得十分必要。

其次，物联网搜索服务如果被攻击者恶意利用，则可能对个人的生命安全及国家基础设施构成严重威胁。黑客通过物联网搜索引擎可以搜索家庭中有安全漏洞的智能设备，进而控制其他安全设备，比如控制智能大门、解除监控摄像头的监视功能等。通过物联网搜索有安全漏洞的智能儿童鞋、智能手环等，可以查看孩子的地理位置和行为轨迹，如果被别有用心地利用，则可能对儿童安全构成更大的威胁。国际黑客安保论坛上曾经展示过现场破解医疗设备，并远程遥控糖尿病患者用的胰岛素泵和心脏病患者用的心跳器。而网站的研究者曾使用 Shodan 定位到了核电站的指挥和控制系统及一个粒子回旋加速器。由于物联网搜索引擎的存在，所有与物联网相连的实体，包括智能家庭、智能汽车、智能城市等显得更加不安全和脆弱。因此，如何确保物联网搜索服务不被别有用心的攻击者利用也是一个很大的挑战。

再次，通过物联网搜索引擎可以对用户访问模式等数据进行深度挖掘，使物联网搜索引擎对用户的行为、爱好更加了解，对敏感数据和隐私信息构成威胁。Pinkas 和 Reinman[4]指出，服务器通过分析用户的访问模式，再结合一定的背景知识，可以推断出用户的部分隐私信息。如果服务器监测到用户进行特定的数据访问序列(u_1, u_2, u_3)后，都会进行一次股票交易操作，那么当用户再次发起相同或相似的访问序列时，即使这些信息是加密的，服务器也可以以极高的概率推测出用户接下来要进行一次股票交易，进而推断出这些访问序列的内容。因此，隐藏访问模式对保护物联网搜索用户隐私起到很重要的作用。

本文针对上述物联网搜索数据隐私保护面临的安全挑战，提出面向物联网搜索的数据隐私保护框架，并在此基础上对现有的适用于物联网搜索隐私保护相关关键技术的国内外研究进展进行综述。最后给出了未来工作展望。

需要特别说明的是本文主要关注适用于物联网搜索的数据隐私保护，同时又不影响搜索服务质量的技术。而基于数据失真的技术和基于限制发布的技术都存在一定程度的信息丢失，因此不在本文的研究范畴。

2　物联网搜索隐私保护框架

典型的物联网搜索协议包括 3 个参与者：数据拥有者、数据搜索者和物联网搜索服务提供者。其中，数据搜索者也可能是数据拥有者本身。数据拥有者是指上传物理实体相关信息资源的个体或机构，数据搜索者是指使用物联网搜索服务的个体或

注1　物联网的致命弱点（经济观察网），http://www.eeo.com.cn/2016/0317/284248.shtml。

机构，物联网搜索服务提供者是指提供物联网搜索服务的提供商及后台系统。要想实现面向物联网搜索的数据隐私保护，就需要从 3 个参与者着手，采用隐私保护技术加以限制。

面向物联网搜索的数据隐私保护框架如图 1 所示，通过数据拥有者加密上传到物联网搜索服务提供者中的数据和数据搜索者加密搜索请求以及密文搜索方案来确保物联网搜索服务提供者无法对其后台系统中的数据进行窥探；通过细粒度的访问控制来确保物联网搜索服务不被滥用；通过隐藏用户访问模式来避免深度数据隐私挖掘。

后续依次对适用于物联网搜索的隐私保护技术：基于数据加密的搜索技术、基于属性加密的访问控制以及隐藏访问模式技术的研究进展进行综述。

3 基于密文搜索的隐私保护技术

3.1 总述

密文搜索技术使物联网搜索服务提供者在返回满足用户搜索请求数据的同时，无法得知数据的内容。如图 2 所示，基于数据加密的搜索技术分为 2 个阶段：系统初始化阶段和搜索阶段。系统初始化阶段包括系统初始化算法和数据加密算法。系统初始化算法由数据拥有者运行，用来生成系统的公开参数和数据拥有者的私钥。基于非对称密钥的密文搜索算法，公开参数也包括数据拥有者的公钥。数据加密算法由数据拥有者运行，用来生成加密的可搜索的数据结构（EDB，encryption database）和加密后的文件。在基于索引的方案中，还包括生成加密后的索引。

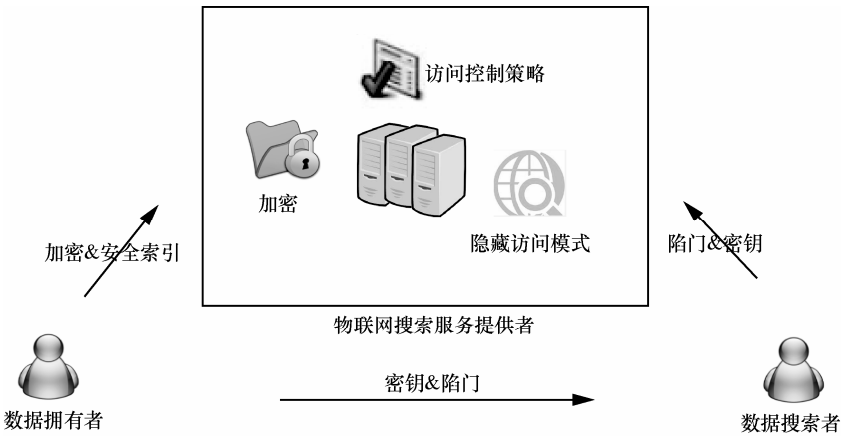

图 1 物联网搜索隐私保护框架

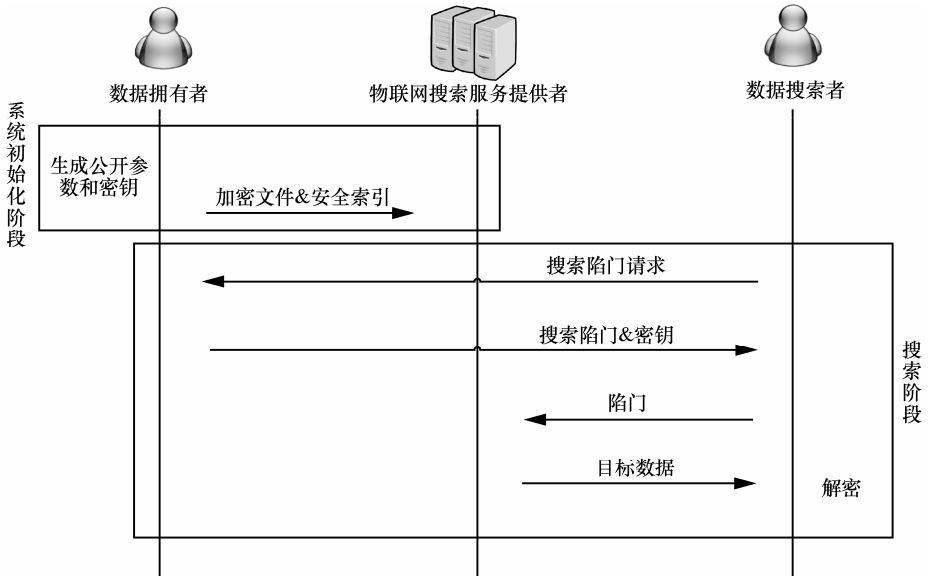

图 2 基于密文搜索的物联网隐私保护

在搜索阶段，数据搜索者要求物联网搜索服务提供者返回和某个指定搜索条件相关的所有加密文件，主要包括陷门生成算法和数据搜索算法。当数据搜索者搜索数据时，首先向数据拥有者提交搜索请求，然后数据拥有者运行陷门生成算法生成陷门，陷门包含搜索条件信息但不能泄露搜索条件的任何信息。物联网搜索服务提供者运行数据搜索算法利用该陷门和 EDB，逐一验证密文或索引是否满足指定的搜索条件，并返回相应的密文或者索引给数据搜索者。最后，数据搜索者使用密钥解密密文获得搜索结果。

如果物联网搜索服务提供者后台系统存储的数据都以密文的形式存在，就可以很大程度上避免数据拥有者的隐私泄露，除非使用的加密算法遭到攻击。然而在这种情况下，必须保证物联网搜索服务的可用性和效率，所以基于密文搜索的隐私保护技术的关键在于确保数据隐私的同时，设计安全、运行效率高且允许对数据进行复杂搜索的密文搜索算法。物联网密文搜索方案应该满足 2 个基本要求：方案生成的加密 EDB 不应该泄露用户 DB 的任何信息；用户生成的陷门不应该泄露有关搜索条件的任何信息给服务提供者。

3.2　现有密文搜索方案分类

现有的密文搜索方案依据采用的加密算法分为基于对称密钥的密文搜索（SSE，searchable symmetric encryption）方案和基于非对称密钥的密文搜索（PEKS，public encryption keyword search）方案。

3.2.1　SSE 方案

依据构建策略，SSE 主要分为基于顺序扫描的方案和基于安全索引的方案。其中，后者分为基于正向索引和基于反向索引构建的方案。

基于顺序扫描的 SSE 方案由 Song 等[5]于 2000 年首次提出，该方案把明文划分为“单词”并对其加密，然后当用户提交搜索请求时，通过对整个密文文件顺序扫描，比较密文单词和待检索关键字，返回包含关键字的密文文件。优点在于支持对文件中任意单词的搜索，缺点在于搜索时需要服务器遍历整个文件，因此效率极低，也使其无法应用在实际场景中，且该方案无法抵抗对密文的频率分析攻击。

Goh[6]提出了基于安全正向索引的 SSE 方案，搜索时由服务器对每个文件的安全索引进行关键字匹配搜索。优点在于，相比 Song[5]的方案，该方案能以较高效率支持用户的关键字搜索。但是由于构建索引所使用的 Bloom Filter 本身存在正向误检概率，使搜索结果不完全正确，可能给用户带来一些额外的带宽开销和计算开销。该方案的安全性达到选择关键词攻击下的不可区分性安全目标 IND-CKA。

Chang 等[7]的方案避免了 Goh 方案的正向误检概率，使用倒排索引构建方法，其抗选择关键字攻击能力也比 Goh 方案强，可以抗自适应选择关键字攻击。Curtmola 等[8]进一步改进并明确定义了 SSE 方案的安全性，提出在自适应和非自适应模型下达到不可区分性安全的 SSE-1 和 SSE-2 方案。该方案也是采用倒排索引构建，搜索操作只需要 $O(1)$时间，然而文件的添加和删除操作需要重新构建索引，时间开销大。

3.2.2　PEKS 方案

Boneh 等[9]提出了 PEKS 方案，并基于双线性对给出了几种构造方案。Abdalla 等[10]进一步提出 PEKS 方案的完整定义，同时给出了基于身份匿名方案构造 PEKS 的流程。文献[11~13]针对文献[9]方案需要使用安全通道的问题，分别设计了在随机预言模型下[11,12]和标准模型下[13]不需要安全通道的 PEKS 方案。文献[13,14]提出了基于身份加密方案的 PEKS 方案。

3.3　目前研究方向

目前，基于数据加密的搜索技术的主要研究方向有 3 个方面。

1) 支持搜索方式的扩展。以上所述方案大多只支持单一关键字搜索，而后续的很多方案对搜索方式进一步扩展，包括支持多关键字搜索[15~20]、子集搜索[21]、模糊搜索[17,18,22~24]、排序搜索[19,20,25]、范围查询[26]的方案。这些扩展都是基于关键字搜索的方式，而物联网搜索方式更加复杂，因此，亟需构建支持复杂搜索方式的密文搜索方案。

2) 支持对服务器存储的密文文件的动态添加、更新或删除[27~31]。如何设计高效的支持数据实时更新的密文搜索方案，适应物联网搜索数据的高度动态性，是一个非常大的挑战。

3) 搜索效率的提升，此方面主要是通过减少双线性对使用的频率或者使用其他技术替代双线性对来构造密文搜索方案[32,33]。总的来看，SSE 搜索效率高，但同 PEKS 相比，灵活性和可扩展性较低，不适用于物联网搜索场景。而 PEKS 现有方案大多

使用双线性对操作，使搜索效率大大降低。因此，研究适用于物联网搜索的高效密文搜索方案及其重要。

4 基于访问控制的数据隐私保护技术

4.1 总述

访问控制可以避免滥用物联网搜索服务导致的隐私泄露。传统的访问控制模型假设用户和服务器处于同一个信任域中，大多假设服务提供者是可信的，由服务提供者来进行授权，访问控制粒度也比较粗，无法为访问控制策略提供丰富的语义支持，因而并不适用物联网搜索大规模的、复杂的、动态的、多安全域的访问控制。而基于属性加密（ABE，attribute based encryption）的方案能确保物联网搜索服务提供者只允许具有特定属性的用户搜索其需要的实体相关信息。

ABE 方案首先由 Sahai 和 Waters 提出[34]，最初是为了改善基于生物信息的身份加密系统的容错性能。采用（t，n）门限访问结构，分别提出了适用于小规模属性全集和大规模属性全集的方案，并给出了在选择身份安全模型下的安全性证明。ABE 方案通常包括 3 个参与者，属性权威、数据拥有者和数据使用者。属性权威主要用来生成密钥和验证数据使用者属性或者策略。如图 3 所示，ABE 方案分为 4 个阶段，初始化阶段、密钥生成阶段、加密阶段和解密阶段。在加密阶段，属性权威生成一对主私钥和公钥，随后把公钥分发给数据拥有者和数据使用者。在密钥生成阶段，属性权威基于数据使用者的请求生成私钥并发送给数据使用者。而加密算法和解密算法由数据拥有者和数据使用者分别运行。

4.2 现有 ABE 方案分类

ABE 方案依据访问策略的实现方式不同分为 2 类[34]，基于属性的密钥策略加密方案（KP-ABE，key policy attribute based encryption）和基于属性的密文策略加密方案（CP-ABE，ciphertext policy attribute based encryption）。两者的主要区别在于访问策略关联的载体不同，前者是密钥和访问策略相关联，后者则是密文和访问策略相关联。CP-ABE 的解密算法通常包括 2 个阶段，将访问策略转化成访问树和将访问树嵌入数据中并加密。而且，由于 ABE 方案相对于对称加密方案来说开销非常大，因此，通常的做法都是使用 ABE 方案来加密对称密钥，如高级加密（AES，advanced encryption standard）协议密钥，然后使用 AES 协议来加密实际数据。由于 CP-ABE 中数据拥有者拥有访问策略制定的权力，一个密文可以由多个不同的密钥进行解密，访问控制策略改变时只需根据新的访问控制策略重新

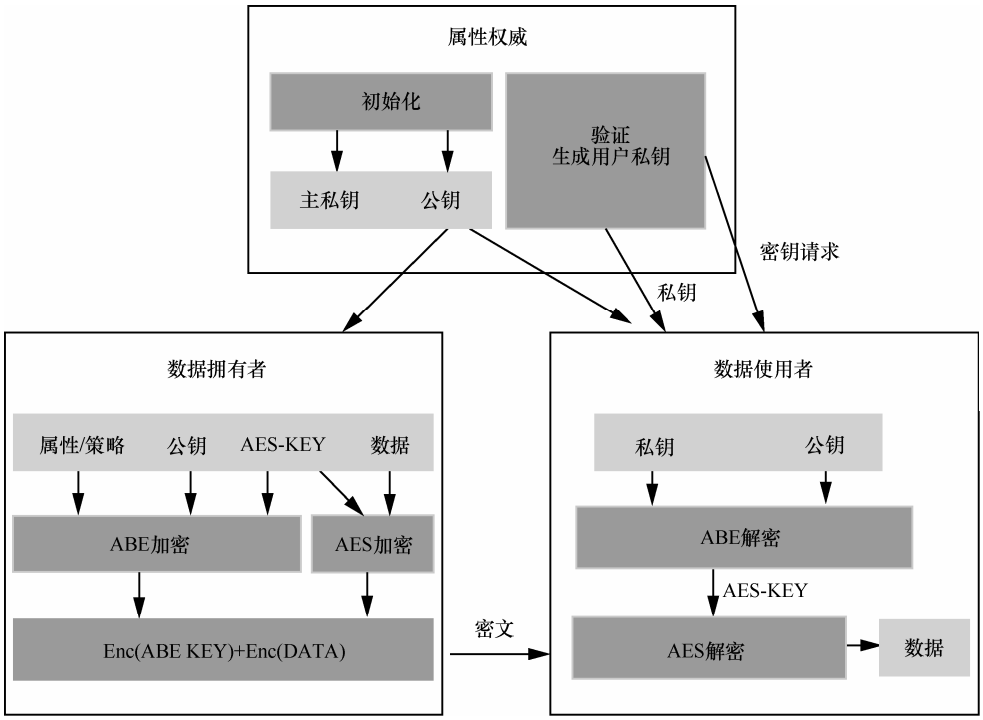

图 3 ABE 方案

加密密文，密钥管理开销较小等特点，更适用于物联网搜索场景下的基于访问控制的隐私保护。

4.2.1 KP-ABE 方案

Goyal 等[35]通过引入访问树结构，提出了一个细粒度访问控制的 KP-ABE 方案。该方案可以支持任意单调的包含与门、或门以及门限门的访问控制公式，增强了策略的逻辑表达能力，并证明了在选择身份安全模型下的安全性。Ostrovsky[36]方案支持非门，完善了文献[35]中访问策略的逻辑表达能力，构成了一个完整的逻辑表达系统，且支持非单调的访问结构。Lewko 等[37]进一步改进了 Ostrovsky 的方案，实现了高效的用户权限撤销。以上 CP-ABE 方案中密文大小随密文属性数目线性增长，Attrapadung 等[38]使密文大小为常数级，但却导致了密钥大小为属性数目的平方级。

4.2.2 CP-ABE 方案

Bethencourt 等[39]提出了访问结构为单调访问树的 CP-ABE 方案。Cheung 等[40]提出了一种可证安全的 CP-ABE 方案，并证明了标准模型下的安全性，但其访问策略仅支持与门，密文和密钥大小随属性线性增长。Goyal[41]和 Liang[42]都采用了有界树作为访问结构。文献[41]在标准模型下证明了其安全性，支持任何访问控制公式，改进了文献[39]方案只支持单调的访问结构和安全性证明是基于双线性群模型的不足。Ibraimi 等[43]使用通用访问树构造了 CP-ABE 方案，降低了开销，对于资源有限的设备是很有意义的。2013 年，Waters 等[44]提出了具有完全表达能力的 CP-ABE 方案，但是安全性证明是在群通用模型下完成的。Lewko 等[45]利用文献[44]中的编码技术提出了达到适应性攻击安全的 ABE 方案，但是其实际性能相比文献[44]有所降低。以上方案都是基于双线性对构造的，Zhang 等[46]提出了基于 n 元格构造的支持与门的 CP-ABE 方案，尽管其性能不高，但是其对于不使用双线性对相关假设来构造 ABE 方案是有意义的。

Attrapapdung 等[47]将 KP-ABE 方案和 CP-ABE 方案组合，提出了双策略 ABE 方案。它也可以根据实际需要转换成单个策略的 KP-ABE 方案或 CP-ABE 方案，并基于判定双线性 Diffie-Hellman 指数困难问题证明了安全性。

4.3 目前研究方向

目前，ABE 的主要研究方向有 4 个方面。

1) 支持多个密钥授权中心（KDC）的 ABE 方案[48~53]，与只支持单个 KDC 的 ABE 方案相比，其允许多个独立的 KDC 对属性和分发的密钥进行监督，分散了 KDC 的权利，更适合于物联网搜索对象和搜索空间广泛性的实际应用场景。

2) 支持灵活的细粒度的访问控制策略表示的 ABE 方案[54]，主要研究如何支持策略属性的灵活变更、用户属性的灵活变更，密钥管理如何更好地支持策略属性和用户属性发生变更以及如何设计更为细粒度的访问控制。

3) 支持审计的 ABE 方案，目的在于避免密钥滥用，包括支持审计的 KP-ABE[55,56]方案和支持审计的 CP-ABE[57~59]方案。

4) 基于属性的访问控制和密文搜索相结合[60~63]。Sun 等[60]和 Han 等[61]分别提出了基于属性的密文搜索方案（ABEKS，attribute based encryption with keyword search），其都是基于关键字密文搜索，搜索的范围相对于密文内容搜索存在较大的局限性，无法满足密文信息的搜索需求，且泄露了包含搜索关键词的文件数量，其使用 KP-ABE 的特性也不适用于物联网搜索场景。相比文献[61]，Kaci 等[63]的方案只需解密授权访问的密文，效率大为提升，同时避免了泄露包含搜索关键字的文件数量，并在文献[62]中进一步改进，使用 KP-ABE 和 CP-ABE 这 2 种策略完成访问控制，使用高性能计算来加速搜索效率。ABEKS 对于物联网搜索数据隐私保护来说是值得研究的方向。

5 基于隐藏访问模式的隐私保护技术

5.1 总述

密文搜索技术可以确保物联网搜索服务提供者返回给用户请求的搜索数据内容的机密性，很大程度上保证了用户数据信息的隐私性，但是却无法确保用户访问模式的机密性，而访问模式通常也蕴含了用户的隐私信息，已成为泄露用户隐私的一种潜在途径。文献[64]指出，用户的访问模式会泄露加密文件的信息，基于频率统计的攻击方式，利用访问模式成功地推断出关于一个加密邮件库搜索的概率大约为 80%。文献[65]指出可以通过访问模式获得用户隐私信息。由此可见，在物联网搜索中，隐藏用户的访问模式对于保护用户数据隐私是十分必要的。

隐私信息检索（PIR，private information retrieval）[66]和隐藏随机访问模式（ORAM，oblivious

random access machine）技术是隐藏访问模式最主要的 2 种方法。PIR 协议将用户的查询请求通过一个矩阵变换构造出 $N-1$ 个与其不可区分的伪查询，使攻击者对用户的真实意图无法准确把握，从而实现在数据搜索平台上用户访问模式的匿名。基于信息理论的 PIR 协议需要假设服务器非合谋，因此不适用物联网搜索应用场景；而基于计算理论的 PIR 协议服务提供者通常需要做大量复杂的运算，开销很大，目前在物联网搜索的数据隐私保护中主要用于和 ORAM 方案相结合[67,68]。

ORAM 技术最早由 Goldreich 和 Ostrovsky[69] 提出，为了保护软件版权和防止非法复制。ORAM 的目标在于用户从服务器读取或向服务器写入数据的同时，使服务器无法推测其真实的数据访问模式。将 ORAM 应用于物联网搜索服务当中，可以使用户使用物联网搜索服务同时，确保物联网服务提供者甚至恶意的攻击者无法获得其用户搜索结果的相关信息和用户的访问模式信息。

如图 4 所示，ORAM 通过对数据进行冗余读/写操作和动态改变数据存储位置的方式来隐藏访问模式。每次访问请求都需经过冗余处理成一系列读写操作，使除数据访问者之外的服务器和攻击者都无法区分访问请求。而每次访问请求执行之后，都会动态改变数据存储的位置。一个典型的 ORAM 方案包含 2 个参与者：数据访问者和服务器。设计一个 ORAM（setup、read、write）方案需要考虑 3 个子协议：系统建立协议、读协议、写协议。在系统建立阶段，需要设计服务器和用户端的数据结构，ORAM 方案构造服务器存储的数据结构，初始化数据结构，生成密钥。读/写协议在用户执行虚拟 IO 数据块的读/写操作时触发。由于 ORAM 必须使服务器不能区分用户是在执行读操作还是写操作，读协议和写协议通常实现相同。在大部分 ORAM 方案中，读协议和写协议用同一个算法描述。因此 ORAM 方案通常包含 2 个算法协议，即系统建立算法和访问算法，分别用 setup 和 access（operation，address，value）表示。为了达到访问后的隐藏性，还可能包含一个洗牌（shuffle）算法。将 ORAM 方案和密文搜索方案相结合，可以直接用读和写协议来模拟顺序搜索算法中的搜索操作，也可以通过构造 2 个 ORAM 结构分别支持对索引和文件集的隐藏访问模式搜索。

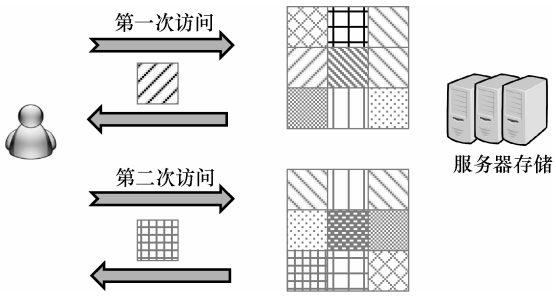

图 4 ORAM 方案

5.2 现有 ORAM 方案分类

根据服务器端是否需要进行读写之外的其他操作，将 ORAM 方案分为经典 ORAM 方案和现代 ORAM 方案。而后者由于可以利用物联网搜索后台强大的计算能力，因此更适用。

5.2.1 经典 ORAM 方案

经典 ORAM 方案主要包括平方根 ORAM 方案[69]、分层 ORAM 方案[69]和树 ORAM 方案[70]。其中，分层方案也可以看作是平方根方案的改进，仅是采用分层方法代替平方根中的缓存。而树方法可以看作是分层方案的分层改进，通过将重组开销分配到每次数据访问操作，降低了洗牌操作带来的最差情况下的开销。

1) 平方根 ORAM 方案

平方根 ORAM 方案由 Goldreich 和 Ostrovsky[69] 提出。数据存储结构如图 5 所示，N 为实际数据单元的总个数，将服务器所需的存储空间分为 2 个部分，分别记为 main_part 和 shelter，其中，main_part 包含一个由 N 个真实数据 $D_1,\cdots,D_N$ 和 $\sqrt{N}$ 个虚拟数据元素 $M_1, M_2, \cdots, M_{\sqrt{N}}$ 组成的伪随机排列，shelter 用来存储最近 $\sqrt{N}$ 个查询结果。分摊性能为 $O(\sqrt{N}\log^2 N)$，最坏情况下的性能为 $O(N)$。

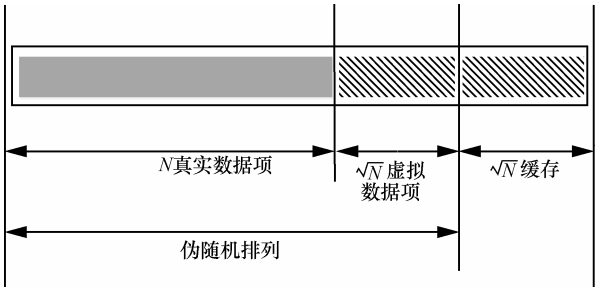

图 5 平方根 ORAM 数据存储结构

2) 分层 ORAM 方案

分层 ORAM 方案由 Goldreich 和 Ostrovsky[69] 提出。数据存储结构如图 6 所示，由一个多层的桶

式散列表[H_1,H_2,…,H_n]组成，其中，n=O(log$N$)，H_i 层由 2^i 个桶组成，每个桶包含的数据单元个数为 O(log$N$)，H_i 和一个普通散列函数 h_i 相关联。数据单元的位置由 H_{Location}=h_i(v)决定，将虚拟地址映射到散列表。分摊开销最优为 O(log^3N)，但隐藏的常数比较大，至少为 6 100，最坏情况下开销为 O(Nlog^2N)。相比平方根算法，分摊性能有所提高，但是最坏情况的性能和服务器存储复杂度都有所增加。

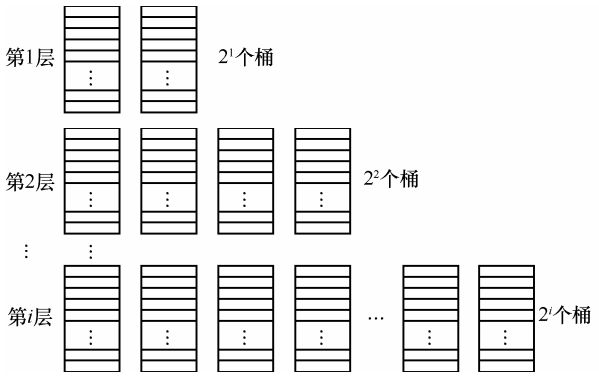

图 6　分层 ORAM 数据存储结构

Williams 等[71]首次在 ORAM 实用性方面做出探索，通过增加用户端存储开销来改进洗牌阶段的隐藏归并算法，使用户端存储开销增加到 $O(\sqrt{N})$ 的情况下，分摊开销降低到 O(log^2 N)。文献[72]进一步改进了分层算法，通过在每一分层引入加密 Bloom 过滤器[72]检测数据元素是否存在该层，使分摊开销降低为 O(log N log log N)。

Pinkas[4]指出文献[72]的实际开销要高得多，并使用 Cuckoo 散列[74]来构造 ORAM，在不增加用户端存储开销的情况下使分摊开销降低到 O(log^2N)，最差情况下的开销为 O(N log N)。

文献[75,76]的 GM、KLO12[77]、GMOT12[78]指出 PR 模型由于使用 Cuckoo 散列函数不够严谨，在某些情况下，服务器能以高概率获知用户的访问模式。并给出了解决方案。GMOT11a[79]将开销进一步分摊，使最坏情况下的开销等于分摊开销。

文献[80]提出了一种平方根和分层方法混合的构造方法，允许各层洗牌操作和虚拟 IO 操作并发执行。且第一次对在线开销和离线开销做出定义，在分摊开销为 O(N)的情况下，使在线开销为 O(1)。

文献[81]把服务器端的 ORAM 分区划分为若干小 ORAM 分区，并采用背景淘汰算法将洗牌操作均摊到每次用户访问操作中，使分摊开销在 20~35，而用户的存储空间仅是存储空间大小的 0.01%~0.3%。

3) 树 ORAM

前述方案洗牌阶段是算法的瓶颈，客户在访问服务器时会因洗牌而阻塞。为了避免洗牌过程，Shi 等[70]提出了基于二叉树构造的 ORAM 方案，使算法的复杂度和效率都大大提升。在该方案中，服务器端的数据存储结构如图 7 所示，二叉树的每个节点都是一个数据桶，每个数据桶都是一个完整的 ORAM，包含 O(log N)个数据块。用户端的数据存储结构为一个索引表，标明数据块到叶子节点的映射。当用户进行数据访问时，用户从索引表中查找该数据块对应的叶子节点，进而获得一条包含该数据块的从叶子节点到根节点的路径，服务器依次返回该路径上所有节点的每个桶的所有数据块。然后用户通过解密数据块，可以获得想要访问的数据内容。在用户访问数据之后，为了保证服务器端数据存储的随机性，用户将要访问的数据块重新加密，并更新索引表，以新的路径存储到服务器。最优性能可以达到分摊开销和最坏情况下的开销均为 O(log^2N)。

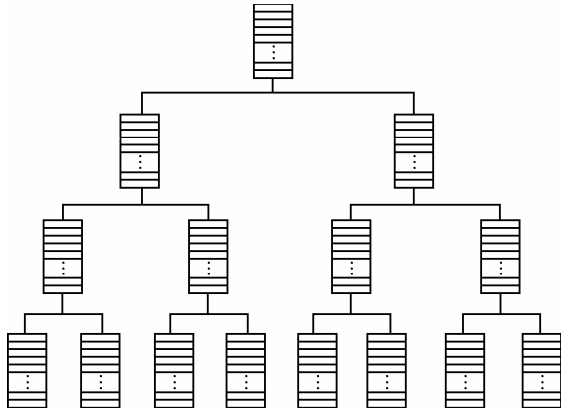

图 7　树 ORAM 存储结构

文献[81]进一步改进了文献[70]，优化树高度为 $O(\frac{\log N}{\log\log N})$，节点数目为 $O(\frac{N}{\log N})$，使用了新的淘汰策略，使分摊开销和最坏情况下的开销为 $O(\frac{\log^2 N}{\log\log N})$。

Path ORAM 基于二叉树的思想，把基于树的方法和分区思想[82]相结合，使分摊开销最优为 O(log N)，但没有对安全性进行形式化证明。后期有很多方案对 Path ORAM 改进，并给出形式化的安全证明[70,83]。MMBC14[84]讨论了如何使树 ORAM 可变尺寸。文

献[83,85~88]都基于树做了一些简化和改进。

5.2.2 现代 ORAM 方案

经典的 ORAM 方案在计算算法复杂性时不考虑加解密数据的复杂性。而加解密操作都由用户完成，因此保证了数据的安全性，数据加解密操作的数量不仅会增加用户的负担，服务提供者也无法发挥高性能搜索的好处，尤其对于物联网搜索应用，后台系统通常是基于云计算的平台，其具有强大的计算能力。而分摊开销是衡量 ORAM 性能的一个最重要因素，现代 ORAM 方案通过利用服务端强大的计算能力打破了 Goloreich 等[69]对分摊开销的限制，可以将分摊开销降低到常数级。由于服务器执行额外操作，就必须考虑服务器是否按预定方式执行，这使威胁模型变为恶意模型。根据服务器执行的额外操作种类分为 2 类。

1) 矩阵乘或者 XOR 操作

Stefanov[82]使用服务器执行矩阵乘操作来降低分摊开销，最优性能是分摊开销为 20~35 倍。Oblivistore[89]改进了文献[82]，通过并行执行读写操作和隐藏调度算法使分摊开销进一步降低到 18~26 倍。Burst ORAM[90]改进了 Oblivistore，通过优先执行在线 IO 降低了用户请求的在线开销。Ring ORAM[91]吸取了 SSS 和 Path ORAM 的技术，通过调节参数使其既适用于用户存储开销小的应用，又适用于用户存储开销大的应用。SR-ORAM[92]将交互复杂度降低到 $O(1)$。

2) 加同态或者全同态

Path-PIR[68]、OS-PIR[67]、KT-ORAM[93]允许服务器使用加同态加密。Path-PIR 把基于树的 ORAM 和 PIR 相结合，但没有明确说明在恶意模型下的安全性。KT-ORAM 使用多叉树来替代二叉树，进一步降低了分摊开销。OS-PIR 进一步改进了 Oblivistore，将其与 PIR 结合，使分摊开销是 Oblivistore 的一半。将 PIR 作为一个黑盒子使用，因此可以使用任何 PIR 方案。

VOS[94]、O-ORAM[81]、Onion-ORAM[95]、C-ORAM[96]服务器执行全同态加密或者 Somewhat 同态加密操作。O-ORAM 使用多叉树，只在半诚实模型下安全。VOS 使在数据块大小较大的情况下，分摊开销为常数级，服务器增加的开销为多项式对数级，交互轮数复杂度为常数级。Onion-ORAM 达到了最优常数级分摊开销和交互轮数复杂度。C-ORAM 在 Onion-ORAM 的基础上，优化了淘汰算法，进一步减少了服务器端的计算开销，放宽了 Onion-ORAM 对数据块大小的限制，从 $O(\log^6 N)$到 $O(\log^4 N)$，但是只分析了半诚实模型下的安全。

5.3 目前研究方向

目前，有些方案的分摊开销已经达到了常数级，但并不是所有达到常数级的方案都可以在实际中应用，仍然有一些限制，比如对数据分块大小的限制，数据块大小较小时，实践性能比较差。这就使 ORAM 方案还无法完全应用于通常意义上的物联网搜索。然而，这些方案仍然是有意义的。且在具体应用中需对安全和效率做出均衡，是否需要达到隐藏访问模式这样的高安全保障也要视具体场景而言。

ORAM 目前主要研究方向包括：使用并行算法来降低分摊开销；使用服务器端运算来降低用户端开销和分摊开销；构建不需要额外假设或者不需要 FHE 可验证的 ORAM 方案。

6 结束语

从物联网搜索服务提供者可能发生的数据窥探、攻击者滥用搜索服务、结合搜索访问模式挖掘用户数据导致的数据隐私泄露等角度出发，梳理了当前适用于物联网搜索数据隐私保护相关关键技术。但总体上说，当前国内外针对物联网搜索数据隐私保护的相关研究和进展还不充分，还存在许多问题，有待进一步研究。

1) 在物联网搜索服务使用权限方面，研究适用于物联网搜索的访问控制和授权机制，从物联网搜索服务用户的身份、行为、兴趣、位置、敏感度、时空等维度，结合物联网搜索服务的搜索种类，综合考虑设计动态、细粒度的访问控制机制，同时保证必要的追责，才能确保用户可以放心地使用物联网搜索服务。同时亟需建立隐私度量模型，量化隐私与服务的平衡，从而为物联网搜索访问控制模型决策提供支撑。

2) 现有的隐私保护技术或者支持静态数据集，或者支持动态数据集的效率不高。而在物联网搜索场景中，数据无时无刻不在变化，包括数据表现形式的改变、属性的增减、新数据加入、旧数据删除等，怎样在物联网搜索复杂的应用环境中同时实现对动态数据的搜索和隐私保护，是一个更具挑战的难题。

3) 现有的支持搜索的隐私保护技术，搜索的条

件主要是基于关键字的搜索，因此，研究支持物联网复杂搜索条件的隐私保护模型和应用或将复杂搜索条件合理转换成基于关键字的搜索十分必要。

4) 研究将基于数据加密的搜索技术和基于属性加密的访问控制技术有机结合，使数据拥有者能在最大限度地控制数据使用权的同时，实现物联网搜索的数据隐私保护。

5) 对于使用 ORAM 技术来隐藏物联网搜索模式，主要关注分摊性能、交互式复杂度、用户端开销几个重要性能衡量指标，因此，研究构造这几个性能指标均衡的 ORAM 方案对于保护物联网搜索数据隐私是非常重要的研究方向。

只有综合考虑上述几个方面，形成整体的解决方案，才能有效保护物联网搜索数据拥有者和数据搜索者的权益和隐私，促进物联网搜索服务的有序健康发展。

参考文献：

[1] ATZORI L, IERA A, MORABITO G. The internet of things: a survey[J]. Computer Networks, 2010, 54(15): 2787-2805.

[2] OSTERMAIER B, ROMER K, MATTERN, et al. A real-time search engine for the web of things[C]//Internet of Things. Tokyo, Japan, 2010:1-8.

[3] BODENHEIM R, BUTTS J, DUNLAP S. Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices[J]. International Journal of Critical Infrastructure Protection, 2014, 7(2): 114-123.

[4] PINKAS B, REINMAN T. Oblivious RAM revisited[C]//International Cryptology Conference. California, USA, 2010:502-519.

[5] SONG X D, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//The IEEE Symposium on Security and Privacy. California, USA, 2000:44-55.

[6] GOH E. Secure indexes[R]. IACR ePrint Cryptography Archive, 2003. http://eprint.iacr.org/2003/216.

[7] CHANG Y, MITZENMACHER M. Privacy preserving keyword searches on remote encrypted data[C]//The Applied Cryptography and Network Security. New York, USA, 2005:442-455.

[8] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption: Improved definitions and efficient constructions[C]//The 13th ACM Conference on Computer and Communications Security (CCS 2006). New York, USA, 2006:79-88.

[9] BONEH D, CRESCENZO G D, OSTROVSKY R. Public key encryption with keyword search[C]//EUROCRYP'04. Interlaken, Switzerland, 2004:71-82.

[10] ABDALLA M, BELLARE M, CATALANO D. Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions[C]//CRYPTO'05. California, USA, 2005:350-391.

[11] BAEK J, SAFAVI-NAINI R, SUSILO W. Public key encryption with keyword search revisited[C]//The International Conference on Computational Science and Applications (ICCSA 2008). Perugia, Italy, 2008:1249-1259.

[12] RHEE H S, PARK J H, SUSILO W, et al. Improved searchable public key encryption with designated tester[C]//Symposium on Information, Computer and Communications Security(ASIACCS 2009). New York, USA, 2009:376-379.

[13] FANG L, SUSILO W, GE C, et al. A secure channel free public key encryption with keyword search scheme without random oracle[C]//The Cryptology and Network Security (CANS 2009). Ishikawa, Japan, 2009:248-258.

[14] KERSCHBAUM F, SORNIOTTI A. Searchable encryption for outsourced data analytics[C]//The 7th European Conference on Public Key Infrastructures, Services and Applications (EuroPKI'10). Athens, Greece, 2010:61-76.

[15] CAO N, WANG C, REN K. Privacy-preserving multi-keyword ranked search over encrypted cloud data[C]//IEEE INFOCOM. Shanghai, China, 2011:222-233.

[16] SUN W, WANG B, CAO N. Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking[C]//ACM ASIACCS. Hangzhou, China, 2013:3025-3035.

[17] CHUAH M, HU W. Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data[C]//International Conference on Distributed Computing Systems Workshops. Minnesota, USA, 2011:273-281.

[18] WANG B, YU S, LOU W. Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud[C]//IEEE INFOCOM. Toronto, Canada, 2014:2112-2120.

[19] MASHAURI D, LI R, HAN H. Adaptive multi-keyword ranked search over encrypted cloud data[C]//International Conference, Collaborate Computing 2015. Wuhan, China, 2015:829-837.

[20] SUN X, WANG X, XIA Z. Dynamic multi-keyword top-*k* ranked search over encrypted cloud data[J]. International Journal of Security and its Applications, 2014,8(1):319-332.

[21] BONEH D, WATERS B. Conjunctive, subset, and range queries on encrypted data[C]//Proceedings of TCC. New South Wales, Australia, 2007:535-554.

[22] SUN W, WANG B, CAO N. Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(11): 3025-3035.

[23] LI J, WANG Q, WANG C. Fuzzy keyword search over encrypted data in cloud computing[C]//IEEE INFOCOM. CA, USA, 2010:1-5.

[24] MARK G, BROST G. *K*-word proximity search on encrypted data[C]//The 30th International Conference on Advanced Information Networking and Applications Workshops. Crans-Montana, Switzerland, 2016:365-372.

[25] WANG C, CAO N, REN K. Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. IEEE Transactions on Parallel and Distributed Systems (TPDS), 2011,23(8):1467-1749.

[26] SHI E, BETHENCOURT V, CHAN H. Multi-dimensional range query over encrypted data[C]//IEEE Symposium on Security and Privacy. California, USA, 2007:350-364.

[27] KAMARA S, PAPAMANTHOU C. Parallel and dynamic searchable symmetric encryption[C]//Financial Cryptography and Data Security(FC). Okinawa, Japan, 2013:258-274.

[28] KAMARA S, PAPAMANTHOU C, ROEDER T. Dynamic searchable symmetric encryption[C]//CCS. Vienna, Austria, 2012:775-780.

[29] STEFANOV E, PAPAMANTHOU C, SHI E. Practical dynamic searchable encryption with small leakage[C]//NDSS. California, USA, 2014:256-272.

[30] CASH D, JAEGER J, JARECKI S, et al. Dynamic searchable encryption in very large databases: data structures and implementation[C]//Network and Distributed System Security Symposium (NDSS). California, USA, 2014:171-182.

[31] NAVEED M, PRABHAKARAN M, GUNTER C. Dynamic search-

able encryption via blind storage[C]//IEEE Symposium on Security and Privacy. CA, USA, 2014:639-654.

[32] DI CRESCENZO G, SARASWAT V. Public key encryption with searchable keywords based on Jacobi symbols[C]//INDOCRYPT 2007. Chennai, India, 2007:282-296.

[33] LAI X, LU R, FOXTON K. An efficient searchable encryption scheme and its application in network forensics[C]//E-Forensics. Shanghai, China, 2010:66-78.

[34] SAHAI A, WATERS B. Fuzzy identity based encryption[C]// EUROCRYPT. Sofia, Bulgaria, 2005:674-651.

[35] GOYAL V, PANDEY O, SAHAI A. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security (CCS). VA, USA, 2006:89-98.

[36] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[C]//14th ACM Conference on Computer and Communications Security. New York, USA, 2007: 521-527.

[37] LEWKO A, SANAIS A, WATERS B. Revocation systems with very small private keys[C]//The IEEE Symposium on Security and Privacy (SP). California, USA, 2010:273-285.

[38] ATTRAPADUNG N, LIBERT B, PANAFIEU DE. Expressive key policy attribute-based encryption with constant-size ciphertexts[C]// Public Key Cryptography(PKC). Taormina, Italy, 2011:521-527.

[39] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//The IEEE Symposium on Security and Privacy. California, USA, 2007:90-108.

[40] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]//The 14th ACM Conference on Computer and Communications Security (CCS). New York, USA, 2007:321-324.

[41] GOYAL V, JAIN A, PANDEY O. Bounded ciphertext policy attribute based encryption[C]//International Colloquium on Automata, Languages and Programming(ICALP). Reykjavik, Iceland, 2008: 579-591.

[42] LIANG X, CAO Z, LIN H, et al. Provably secure and efficient bounded ciphertext policy attribute based encryption[C]//The 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (ASIACCS). Sydney, Australia, 2009:343-352.

[43] IBRAIMI L, TANG Q, HARTEL P. Efficient and provable secure ciphertext-policy attribute-based encryption schemes[C]//Information Security Practice and Experience (ISPEC). Xi'an, China, 2009:1-12.

[44] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]//The 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy, 2011:53-70.

[45] LEWKO A, OKAMOTO T, SAHAI A. Fully secure functional encryption: attribute-based encryption and (hierarchical)inner product encryption[C]//EUROCRYPT. Monaco and Nice, French Riviera, 2010:33-41.

[46] ZHANG J, ZHANG Z F. A ciphertext policy attribute based encryption scheme without pairings[C]//Information Security and Cryptology (ISC). Beijing, China, 2012:324-340.

[47] ATTRAPADUNG N, IMAI H. Dual-policy attribute based encryption[C]//Applied Cryptography and Network Security. Paris-Rocquencourt, France, 2009:168-185.

[48] CHASE M. Multi-authority attribute based encryption[C]//TCC. Amsterdam, The Netherlands, 2007:333-340.

[49] BOŽOVIC V, SOCEK D, STEINWANDT R. Multiauthority attribute-based encryption with honest-but-curious central authority[J]. International Journal of Computer Mathematics. 2012, 89(3): 268-283.

[50] CHASE M, CHOW S. Improving privacy and security in multi-authority attribute-based encryption[C]//The 16th ACM Conference on Computer and Communications Security (CCS). Chicago, USA, 2009:121-130.

[51] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//EUROCRYPT 2011. Tallinn , Estonia, 2011:568-588.

[52] LIU Z, CAO Z, HUANG Q. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles[C]//The European Symposium on Research in Computer Security (ESORICS). Leuven, Belgium, 2011:380-384.

[53] HAN J, SUSILO W, MU Y. Privacy-preserving decentralized key-policy attribute-based encryption[J]. IEEE Transactions on Parallel and Distributed Systems. 2012, 23(11):2150-2162.

[54] YU S, WANG C, REN K. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//IEEE INFOCOM. CA, USA, 2010:1-9.

[55] YU SC, REN K, LOU W J. Defending against key abuse attacks in KP-ABE enabled broadcast systems[C]//Security and Privacy in Communication Networks. Athens, Greece, 2009:56-74.

[56] WANG Y, CHEN K, LONG Y. Accountable authority key policy attribute-based encryption[J]. Science China: Information Sciences. 2012, 55(7):1631-1638.

[57] LI J, REN K, KIM K. A2BE: accountable attribute-based encryption for abuse free access control[R]. Cryptology ePrint Archive, 2009.

[58] LI J, REN K, ZHU B. Privacy-aware attribute based encryption with user accountability[C]//12th International Conference. Pisa, Italy, 2009.

[59] LI J, HUANG Q, CHEN X. Multi-authority ciphertext-policy attribute-based encryption with accountability[C]//The 6th International Symposium on Information, Computer and Communications Security (ASIACCS). Hong Kong, China, 2011:223-228.

[60] SUN W, YU S, LOU V. Protecting your right: attribute-based keyword with fine-grained owner enforced search authorization in the cloud[C]//IEEE INFOCOM. Toronto, Canada, 2014:1187-1198.

[61] HAN F, QIN J, ZHAO H. A general transformation from KP-ABE to searchable encryption[J]. Future Generation Computer Systems. 2014, 30: 107-115.

[62] BOUABANATEBIBEL T, KACI A. Parallel search over encrypted data under attribute based encryption on the cloud computing[J]. Computers & Security, 2015, 54(c):77-91.

[63] KACI A, BOUABANA-TEBIBEL T. Access control reinforcement over searchable encryption[C]//The 15th IEEE International Conference on Information Reuse and Integration. San Francisco, USA, 2014:130-137.

[64] ISLAM M, KUZU M, KANTARCIOGLU M. Access pattern disclosure on searchable encryption: ramification, attack and mitigation[C]// Network and Distributed System Security Symposium (NDSS). California, USA, 2012:56-78.

[65] ZHUANG X, ZHANG T, PANDE S. HIDE: an infrastructure for efficiently protecting information leakage on the address bus[C]//Proceedings of the 11th ASPLOS. Boston, USA, 2004:72-84.

[66] CHOR B, GOLDREICH O, KUSHILEVITZ E. Private information retrieval[C]//IEEE Symposium on Foundations of Computer Science. Milwaukee, USA, 1995:141-151.

[67] DAUTRICH J, RAVISHANKAR C. Combining ORAM with PIR to minimize bandwidth costs[C]//CODASPY. TX, USA, 2015:289-296.

[68] MAYBERRY T, BLASS E, CHAN A. Efficient private file retrieval by combining ORAM and PIR[C]//NDSS. California, USA, 2014: 123-131.

[69] GOLDREICH O，OSTROVSKY R. Software protection and simulation on oblivious RAMs[J]. Journal of the ACM (JACM),1996, 43(3): 431-473.

[70] SHI E, CHAN T H H, STEFANOV E. Oblivious RAM with O((log n)^3)worst-case[C]//17th International Conference on the Theory and Application of Cryptology and Information Security. Seoul, South Korea, 2011:95-100.
[71] WILLIAMS P, SION R. Usable PIR[C]//NDSS.CA, USA, 2008: 22-34.
[72] WILLIAMS P, SION R, CARBUNAR B. Building castles out of mud: practical access pattern privacy and correctness on untrusted storage[C]//CCS. Alexandria, USA, 2008:139-148.
[73] BLOOM B. Space/time trade-offs in hash coding with allowable errors[J]. Communications of the ACM,1970,13(7):422-426.
[74] PAGH R, RODLER F F. Cuckoo hashing[J]. Journal of Algorithms, 2004, 51(2):122-144.
[75] GOODRICH M T, MITZENMACHER M. Mapreduce parallel cuckoo hashing and oblivious ram simulations[J]. Clinical Orthopaedics and Related Research, 2010, 1007(1259):576-587.
[76] GOODRICH M, MITZENMACHER M. Privacy-preserving access of outsourced data via oblivious RAM simulation[C]//International Colloquium on Automata, Languages and Programming. Zurich, Switzerland, 2011:576-587.
[77] KUSHILEVITZ E, LU S, OSTROVSKY R. On the (in) security of hash-based oblivious RAM and a new balancing scheme[C]//The 23th Annual ACM-SIAM symposium on Discrete Algorithms. Philadelphia(SIAM). Kyoto, Japan, 2012:383-392.
[78] GOODRICH MT, MITZENMACHER M, OHRIMENKO O. Privacy-preserving group data access via stateless oblivious RAM simulation[C]//The 23th Annual ACM-SIAM Symposium on Discrete Algorithms. Philadelphia(SIAM). Kyoto, Japan, 2012:151-162
[79] GOODRICH M T, MITZENMACHER M，OHRIMENKO O. Oblivious RAM simulation with efficient worst-case access overhead[C]//The 3rd ACM Workshop on Cloud Computing Security Workshop(CCSW). Chicago, USA, 2011:99-108.
[80] BONEH D, MAZIERES D, POPA R A. Remote oblivious storage：making oblivious RAM practical[R]. http://dspace.mit.edu/handle/1721.1/62006. Technical Report (2011).
[81] GENTRY C, GOLDMAN K, HALEVI S. Optimizing ORAM and Using It Efficiently for Secure Computation[C]//PETS. Bloomington, USA, 2013:1-18.
[82] STEFANOV E，SHI E, SONG D. Towards practical Oblivious RAM[C]//NDSS. California, USA, 2012:203-214.
[83] CHUNG K, LIU Z, PASS R. Statistically-secure ORAM with $\tilde{o}$ ($\log_2 n$) overhead[C]//ASIACRYPT. 2014:62-81.
[84] MOATAZ T, MAYBERRY T, BLASS EO. Resizable tree-based oblivious RAM[C]//19th International Conference(FC). San Juan, Puerto Rico, 2015:147-167.
[85] CHUNG K M, PASS R. A simple ORAM[EB/OL]. Cryptology ePrint Archive, 2013. http://eprint.iacr.org/2013/243.
[86] MARC SA. Toward efficient data access privacy in the cloud[J]. Communications Magazine, IEEE, 2013,51(11):39-45.
[87] BOYLE E, CHUNG K M, PASS R. Oblivious parallel RAM[EB/OL]. Cryptology ePrint Archive, 2014. http://eprint.iacr.org/2014/594.
[88] MOATAZ T, BLASS E O, NOUBIR G. Recursive trees for practical ORAM[R]. Cryptology ePrint Archive, 2014.
[89] STEFANOV E, SHI E. ObliviStore: High performance oblivious cloud storage[C]//IEEE Symposium on Security and Privacy. CA, USA, 2013: 253-267.
[90] DAUTRICH J, STEFANOV E, SHI E. Burst ORAM: minimizing ORAM response times for bursty access patterns[C]//USENIX Security. San Diego, USA, 2014:58-69.
[91] REN L, FLETCHER CW, KWON A. Ring ORAM: closing the gap between small and large client storage oblivious RAM[EB/OL]. IACR Cryptology ePrint Archive, 2014: 997.
[92] WILLIAMS P, SION R. Single round access privacy on outsourced storage[C]//The 2012 ACM conference on Computer and Communications Security. NC, USA, 2012:293-304.
[93] ZHANG J, MA Q, ZHANG W. KT-oram: a bandwidth-effcient oram built on k-ary tree of pir nodes[R]. http://eprint.iacr.org/2014/624
[94] APON D, KATZ J , SHI E. Verifiable oblivious storage[C]//PKC. Buenos Aires, Argentina, 2014:131-148.
[95] DEVADAS S, MARTEN VAN D, CHRISTOPHER W. Onion ORAM: a constant bandwidth and constant client storage ORAM (without FHE or SWHE)[EB/OL]. Cryptology ePrint Archive, 2015
[96] MOATAZ T, MAYBERRY T, BLASS E. Constant communication ORAM with small blocksize[C]// ACM Sigsac Conference on Computer and Communications Security. Denver, Colorado, US, 2015: 862-873.

作者简介：

王佳慧（1983-），女，山西大同人，北京邮电大学博士生，主要研究方向为云计算与云安全、数据安全与数据保护等。

刘川意（1982-），男，四川乐山人，哈尔滨工业大学副教授，主要研究方向为云计算、数据安全与数据保护、网络存储、可信计算等。

方滨兴（1960-），男，江西万年人，中国工程院院士，北京邮电大学教授、博士生导师，主要研究方向为信息与网络安全、内容安全等。