doi:10.3969/j.issn.1000-436x.2014.11.001

移动互联服务与隐私保护的研究进展

李晖[1]，李凤华[2]，曹进[1]，牛犇[1]，孙文海[1]，耿魁[1]
(1.西安电子科技大学 综合业务网理论与关键技术国家重点实验室，陕西 西安 710071；
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 100093)

摘 要：随着宽带无线接入技术和移动终端技术的飞速发展，人们迫切希望能够随时随地从互联网获取信息和服务，移动互联网应运而生并迅猛发展。然而，由于云计算平台、移动通信网络和移动终端的开放性，传统互联网服务中信息传播和管控机制不再适应于移动互联网，信息安全和用户隐私保护已经成为移动互联网用户迫切关心和亟待解决的问题。结合国内外移动互联网发展的最新趋势，对移动互联网服务和隐私保护方面的研究进行了展望。首先对当前移动互联网服务模型和移动互联网服务架构进行了评述；其次对当前的移动互联网数据传播控制机制以及隐私保护机制进行了分析和讨论；最终给出了一些潜在的研究热点，为未来研究工作指明方向。

关键词：移动互联网服务；研究进展；信息安全；隐私保护
中图分类号：TN929 **文献标识码**：A **文章编号**：1000-436X(2014)11-0001-11

Survey on security and privacy preserving for mobile internet service

LI Hui[1], LI Feng-hua[2], CAO Jin[1], NIU Ben[1], SUN Wen-hai[1], GENG Kui[1]
（1.State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China;
2.State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China）

Abstract: With the development of the broadband wireless access technology and mobile terminal technology, mobile internet arises at the historic moment and has been rapid development, by which users can easily obtain information and services from the internet anywhere at any time. However, owing to the openness of cloud computing platform, the mobile communication network and mobile terminals, information transmission and control mechanisms in traditional internet are no longer fit in with that in mobile internet, it is a key point for mobile internet to ensure information security and user privacy protection. Combined with the latest trend of the development of the mobile internet at home and abroad, a number of contributions to mobile internet service and privacy protection are made. First, an overview of mobile internet service models and mobile internet services architectures is given. Second, the current data transmission control mechanisms and privacy protection mechanisms in mobile internet are ravened and discussed. Finally, the potential research issues for the future research works are shown.

Key words: mobile internet service; research process; information security; privacy protection

1 引言

移动通信和互联网的结合，使互联网信息的获取和应用变得更加便捷。随着移动终端的多元化，价格不断降低，功能不断增强。3G/4G/5G、WiFi、M2M 等各类宽带移动通信发展、云计算技术应用普及，“人”、“机”、“物”借助泛在异构的移动互联网络广泛互联互通，公共安全、智能交通、智慧家庭与智慧社会、环境监测、位置服务、移动支付等移动互联网新服务模型和业务不断涌现，信息的

收稿日期：2014-11-03；**修回日期**：2014-11-10
基金项目：国家自然科学基金资助项目（61170251，61272457，61402354）；国家高技术研究发展计划（“863”计划）基金资助项目（2012AA013102, 2012AA01A401）；数字版权保护技术研发工程基金资助项目（1681300000119）
Foundation Items: The National Natural Science Foundation of China (61170251, 61272457, 61402354); The National High Technology R&D Program of China (863 Program) (2012AA013102, 2012AA01A401); The Major Science and Technology Project of Press and Publication-Research and Development (1681300000119)

获取和利用已经或者即将达到“信息随心行，交互在指间”的理想境界。

然而，由于云计算平台、移动通信网络和移动终端的开放性，传统互联网服务中信息传播和管控机制不再适用于移动互联网，信息安全和用户隐私面临越来越大的威胁，已经成为移动互联网用户迫切关心和亟待解决的问题。在信息安全和用户隐私保护不能解决的情况下，移动互联网就没有充分的信息流通与服务，移动互联网服务和隐私保护面临以下新的需求。

1) 移动互联网服务对网络架构的新需求

随着3G、4G、5G的技术演进，移动通信带宽不断增加，移动互联网服务日益丰富，移动互联网服务内容不仅有文本数据，还越来越多地包含语音、视频等大流量数据。出于移动资费、终端能耗、网络负载的考虑，移动互联网服务的终端用户希望快速获取感兴趣的数据，运营商则需要节省面向大量用户的数据搜索和推送所消耗的宝贵带宽资源。传统的IP网络技术关注的是信息端到端传送，不再适应移动联网服务关注数据传送的情况。因此移动互联网服务需要新的以数据为中心的服务网络架构，以达到安全高效的信息获取和分发、节省能耗与带宽的效果。

2) 移动互联网信息传播管控、数据管理安全的需求

移动互联网信息生产呈现爆炸性的增长。用户或者数据所有者在移动互联网中分发、搜索获取各类视频、图片、语音、文本乃至公共安全、智能交通、环境监测、智慧家庭等物联网应用状态等信息，并在授权用户范围内控制数据的获取，希望能够采用有效的信息传播管控和访问控制机制；数据保存在云端系统中，并在移动互联网中被搜索和传播，造成数据所有权和管理权的分离，数据所有者自然希望对自己拥有的数据具有保护以获取相应权益的权利，对所拥有数据的使用方式和数据状态具有审计的权利，以保护和平衡数据所有者和数据使用者的利益。

3) 面向移动互联网服务多样化的隐私保护需求

用户在向服务提供者提出服务请求的同时，也希望能够保护自身的隐私，如自己的身份、所处的位置、自己的兴趣爱好、自身的各种状况等等，迫切需要多粒度隐私保护的机制。而服务提供者为了给用户提供更好的服务质量和体验，则必须要了解用户的习惯，因此隐私和服务质量之间存在一种折中关系，而信任则是其中的重要因素。用户、用户群、服务提供者之间的信任评价和管理体系对改善移动互联网服务用户体验、提高移动互联网服务的安全性有重要的作用。好的信任评价系统可以有效地保证隐私保护策略的实施。研究隐私、服务质量和信任之间的关系规律以及相应的隐私保护机制对于移动互联网服务的发展有重要的意义。

为了真正达到“信息随心行，交互在指间”的境界，满足移动互联网新的服务需求，需要对移动互联网服务和隐私保护的基础理论和关键技术开展研究，建立以数据为中心的移动互联网服务网络架构与协议体系，寻找兼顾隐私保护、传播安全和传播效率的细粒度数据安全传播控制与管理机制，研究粒度可控、结合信任的智能隐私保护机制。提高整个移动互联网服务的效率，保护服务提供者的利益，对数据使用者提供粒度可控的隐私保护。

2 移动互联网服务的模型与网络架构

2.1 移动互联网服务模型

近年来，Facebook、微信以及支持分发用户生成内容UGC(user generated content)的YouTube和优酷等社交网络应用不断涌现，使用移动设备访问这些服务的用户日益增多，而数据大多存储在服务提供商的服务器当中。虽然中心化结构的存储和分发数据的开销很高，但服务商可以挖掘用户数据，并可以通过广告获得收入。用户可以使用任何终端访问这些数据，不需要担心数据的维护。但缺点是用户隐私的降低以及对数据控制权的丢失。

另一方面，物联网技术的发展使联网传感器和设备飞速增长，出现了许多面向群体应用的平台，用户可以贡献和分享异构数据源的传感器数据，并在其上开发增值业务。代表性的平台包括Microsoft SenseWeb[1]、Global Sensor Networks (GSN)[2]、SensorBase[3]、IrisNet[4]和Semantic Sensor Web[5]。卡内基梅隆大学的Zhang等[6]提出了一个传感器数据即服务SDAS(sensor data as a service)的架构，设计了面向开放团体的服务平台以支持联盟传感器数据服务，即拥有传感器的团体可以加盟这个基于云技术的平台，实现异构传感器数据的互操作和重用。这是一个以移动数据为中心的服务部署和共享的联盟平台，提供可伸缩、上下文感知、可配置的传感器数据服务。存储、传感器数据管理以及面向

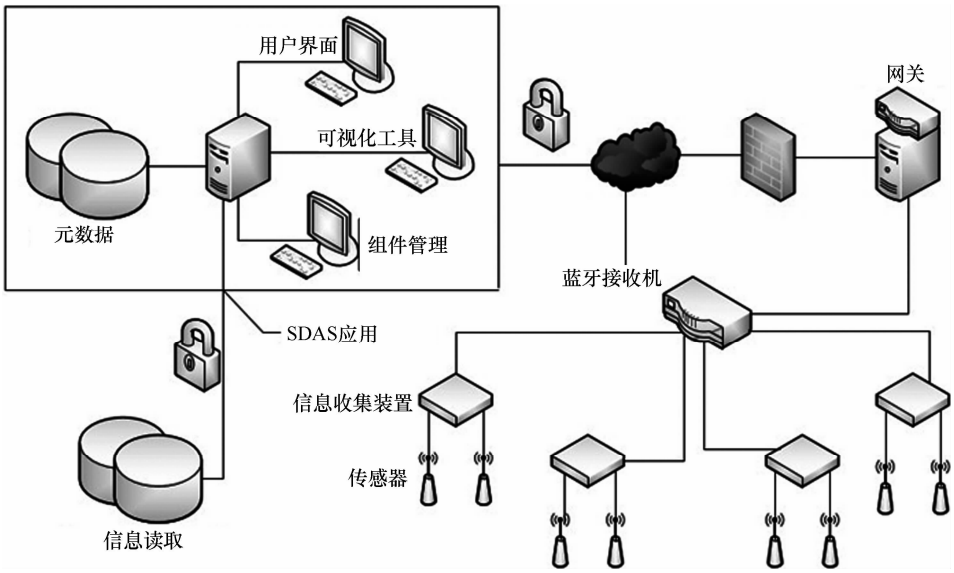


图 1　SDAS 部署架构

平台的元数据去耦合使其可以同时支持传感器的离散数据和流数据，其部署的架构如图 1 所示。

针对这些移动互联网服务模型，使用 Google、百度等搜索引擎可以在海量的数据中找到有用的信息，分布在同地域的在线用户也可以在网络空间中彼此交互，并共享照片、视频、图片、个人信息。但是移动应用是以数据为中心的，比如允许数据发送到具有特定属性的用户，然而目前的移动互联网通信方案不能很好地满足这样的需求。此外，现有的移动应用带来许多安全和隐私方面的担忧，未来移动物联网服务模型应该是以数据为中心，允许数据所有者对其数据拥有完全的控制，可以决定谁能够访问其发布的数据。

2.2　以数据为中心的移动互联网架构

随着互联网服务重要性的日益突出，面向资源、以数据为中心的互联网让用户将注意力集中在需要的数据而不是位置上，对所请求的数据和内容进行命名和编址，而不需要根据主机的位置进行寻址和路由，提高了数据组织、存储和传递的效率。近年来提出的网络系统架构包括 P2P、内容分发网络 CDN(content distribution network)、信息中心网络 ICN(information centric network)、命名数据网络 NDN(named data network)等。

移动 P2P 存储技术是大规模分布式移动互联网广泛应用的基础。根据构造“叠加”拓扑结构、放置文件及查询请求传播的不同，可把 P2P 文件系统分为 3 类基本模式[7]：无层叠网方式，非结构化 P2P 系统和结构化 P2P 系统。但是目前适用于移动环境的 P2P 分布式存储系统的研究还处于初级阶段，没有形成针对实际移动网络环境应用基本需求的理论和方法。

在移动社交网络应用中，为避免数据集中存放于服务提供商服务器中带来的隐私泄露和数据控制权丢失的问题，出现了分布式无中心的社交网络架构 DDSN（distributed decentralized social network），允许个人用户和团体在其移动设备上存储数据，并通过机会路由和 P2P 方式交换数据。Cutillo 等提出了 Safebook 方案[8]，可以在多个移动设备上复制存储数据，但这一过程中的通信和能耗开销都是需要考虑的，且在蜂窝网上共享大容量的多媒体数据会带来移动数据流量的指数性增长。

Diaspora[9]可能是唯一广泛应用的 DDSN，每个用户需要建立自己的服务器，但其针对固定网络的数据共享。Mobitribe[10]是基于移动终端复制分发内容，同时考虑节省带宽和能量的分布式 UGC 共享系统。SafeBook 是基于无中心和朋友间合作的概念构造安全的社交网络，朋友间设备复制数据以提高可用性，Mobitribe 在此基础上，适用了连接感知复制策略，当移动终端有低成本的 WiFi 连接时才在朋友间复制和传输数据。

CDN 网络架构是一种高效内容分发的网络。文献[11~13]在基于 CDN 网络的流媒体服务系统中的客户端之间引入了 P2P 机制，改善了 CDN 网络的服务性能，但是由于 P2P 机制仅仅限于客户端之间，

并不能提高CDN内部的数据分发性能。Chan等[14]进一步将P2P技术引入到CDN服务器的数据分发中，提高了数据分发的性能，但是其直接使用了Bittorent的运行机制，而CDN服务器和客户端存在明显差异，前者的规模相对较小，更重要的是节点非常稳定，和BT类软件的运行环境存在一定差异，BT类软件采用的完全自组织局部下载优化机制不利于整体数据分发性能的最优化。

CDN网络虽然为数据分发提供了较高的服务带宽，但是CDN服务器之间采用的C/S服务模型在处理大规模海量数据分发的时候存在很多问题，例如数据源服务器的网络带宽长时间被占用，整个数据分发的完成时间较长。单纯提高CDN网络的带宽并不能从根本上解决上述问题，而且会增加系统构建成本。

ICN是近年来面向下一代互联网提出的一种新的网络传输架构。其主要思想是互联网络越来越用于信息分发，而不仅仅是端点主机间的通信。通过对信息命名，ICN可以部署网络内的信息缓存和多播机制，从而更有效和快速地将信息分发给用户。而且除了信息分发之外，ICN还可以通过信息感知方法解决更多的移动性管理和安全增强技术。文献[15,16]对ICN的最新发展进行了全面的综述。欧美国家支持了许多面向ICN的项目，主要包括Berkeley的DONA[17]，欧盟支持的PURSUIT[18]和其后续的PSIRP[19]、SAIL[20]及其后续的4WARD[21]，内容感知的内容中继架构COMET[22]，CONVERGENCE[23]，美国支持的命名数据网络NDN[24]及其后续的内容中心网络CCN[25]、MobilityFirst [26]，还有法国支持的采用NDN架构的ANRConnect[27]。

2.3 信息命名机制

灵活高效的信息命名描述方案直接影响ICN中信息的传播效率和用户体验。由于移动互联网中用户的多属性、无线拓扑的不稳定性、海量数据存储等特性，高效灵活的信息描述方案就显得尤为重要。2010年由张丽霞和Van Jacobson主持的NDN项目不考虑数据存储所在的物理位置，直接建立命名数据网络体系。传统的数据命名方法[17,28]采用分布式散列表的方法来对数据进行命名，但是这种方法只支持预生成的数据。而当数据并没有发布到网络时，NDN[29]动态地传递用户的请求到潜在的数据源来确保数据生成的需求，且NDN可直接给每一块数据指派一个名字，从而无需任何映射系统可直接使用应用名称进行数据通信。在NDN中，内容的名称是由一个或多个可变长度的部分组成，这些部分对于网络并不透明，每个部分的边界都是通过“/”来区分。但是，文献[30]指出现存NDN数据命名是长度可变且无边界的，比现有的IPv4/6地址要长，而且具有分层架构且是粗粒度的，这导致NDN在做命名查看时需要大量的查看时间，而且必须匹配到最后一个部分的前缀内容，而IP只是匹配数字。文献[31]针对即时信息的应用场景采用基于序列号和用户名的方式来对数据内容进行命名。文献[32]提出了一种将多用户、多应用以及多传感器的分布式协同自适应传感系统（DCAS）实施在NDN架构上的概念验证。该方案提出了一种基于数据的地理位置和数据的类型来对数据进行命名的分层命名约定。这种命名方式并不关注传感器生成了哪些数据，而是通过让终端用户细化特定数据类型或事件的兴趣位置（AOI），从而不会遗忘相关传感器以及计算实体的位置。然而，文献[31,32]只适合于特定的即时通信应用以及DCAS系统。文献[33]提出了一种针对只读命名数据的自验证命名方式。该方案采用数据的密码杂凑值来作为数据的名称。自验证命名方式通过忽略可缓冲数据的签名，简化认证核查以及支持除PKI以外的多种认证方法来改进只读数据的传递。但是，这种方法只适合于特定的只读数据，对于大量的其他数据并不适用。

2.4 加密信息的搜索机制

信息获取（information retrieval）技术已被广泛研究和应用于数据库中，在移动互联网架构下，百度、谷歌等为移动客户端提供了高效、节能的信息获取方案。通常使用关键字对信息进行命名描述，利用高效的索引结构，如反向索引（inverted index）和各种树形结构对获取到的信息进行组织，使用搜索算法来达到高效获取信息的目的。越来越多的个人和企业用户的大量敏感数据，如电子邮件、个人健康记录、照片、信用记录、财务文件等，外包存储于云服务器中或者分散存储于用户移动设备之中。为了这些敏感数据的安全，人们越来越希望将数据加密存储，而传统的基于明文的信息描述和获取技术已不能提供隐私安全数据搜索服务。

针对这一安全需求，学术界提出了一系列可搜索的加密技术方案，用于云存储加密数据的搜索，其主要思想如图2所示。数据所有者对加密的数据

文件生成若干关键词，对所有文件的关键词构造索引表，对其采用可搜索加密形成安全索引。将安全索引和加密的文件分别存储到云存储服务商。

当用户需要搜索包含某些关键词的数据文件时，用户会产生陷门（采用非对称可搜索加密时）或者向数据所有者请求陷门（采用对称可搜索加密时），然后将陷门发送给云存储服务商。云存储服务商执行搜索算法，向数据使用者返回搜索的结果。搜索可以基于一定的排序准则。

可搜索加密大致可分为基于对称密钥的可搜索加密和基于非对称密钥的可搜索加密方案。

基于对称密钥的可搜索加密方案，其基本模式为数据的拥有者和对这些数据进行搜索的用户共享相同的密钥信息。Song 等[34]首次提出基于对称密钥的可搜索加密方案，可以对加密文件本身进行文本搜索，但搜索效率低下，不能抵抗对密文的频率分析攻击。随后的方案基本是构造安全索引，并对索引进行关键词搜索。Goh[35]提出了一种使用伪随机函数和布隆过滤器（Bloom filter）对每个文件构建一个安全索引的方案，搜索时间同文件数量成正比，由于使用布隆过滤器时不可避免地引入误差，使搜索结果不完全正确。Chang 等[36]和 Curtmola 等[37]几乎同时提出了利用伪随机技术构建关键词索引和查询请求，使搜索效率大为提高，但对动态的数据更新支持不够，更新时所需的计算量极大，或需要重构整个索引。Wang 等[38]使用反向索引，利用顺序保持加密（order-preserving encryption）技术对文件中的关键词频率进行加密，同时，能够使用户对返回的搜索结果进行验证。Kamara 等[39]利用同文献[37]相同的安全索引构造方法，提出了一种支持文件更新的加密数据检索技术。应当指出以上技术方案仅适用于单一关键词搜索，无法满足明文搜索中已广泛支持的多关键词搜索，即使利用多次单一关键词搜索后进行交集操作来实现，为此则需要较大的运算和通信开销，效率极低。Cao 等[40]通过对每一个文档建立索引向量，利用矩阵加密，运用查询搜索后内积值的大小排列来对密文进行多关键词搜索，并返回包含关键词最多的前 K 个文件，但搜索效率不高，需要遍历所有文件，且搜索结果的精确性较低。Vimercati 等[41]提出一种将访问控制和可搜索加密相融合的技术方案，通过访问控制列表对用户进行划分，用加盐操作使相同关键词在不同用户组中的索引不同，来保护关键词的隐私安全，但这一方案的使用场景特殊，不具有普遍意义。Sun 等[42]提出了一种安全多关键词密文搜索方案，通过使用多维 B 树（multi-dimensional B-tree）技术大大提高了密文搜索效率，同时利用余弦相似性测量(cosine similarity measure)方法提高了返回结果的精确度，并且能够对搜索结果进行验证[43]。

在基于非对称密钥的可搜索加密方案方面，Boneh 等[44]提出了第一个基于公钥的可搜索加密方案。在文献[45]中，Abdalla 等对基于非对称密钥的可搜索加密方案进行了改进。随后，学术界提出了支持布尔关键词操作[46]、子集操作[47]、范围查询[48]等一系列密文搜索技术方案。Kerschbaum 等[49]提出了基于身份加密的公钥可搜索加密方案。Lai 等[50]提出一种对单一关键词搜索的公钥加密方案，减少了对双线性对的使用，效率大为提高，并提出了适用于网络鉴证的应用场景。Hwang 等[51]在企业多用户场景下提出了一种支持固定关键词并集搜索的方案，同时使服务器利用用户列表对用户的搜索权限进行控制，但此方案的扩展性不高，当系统中存

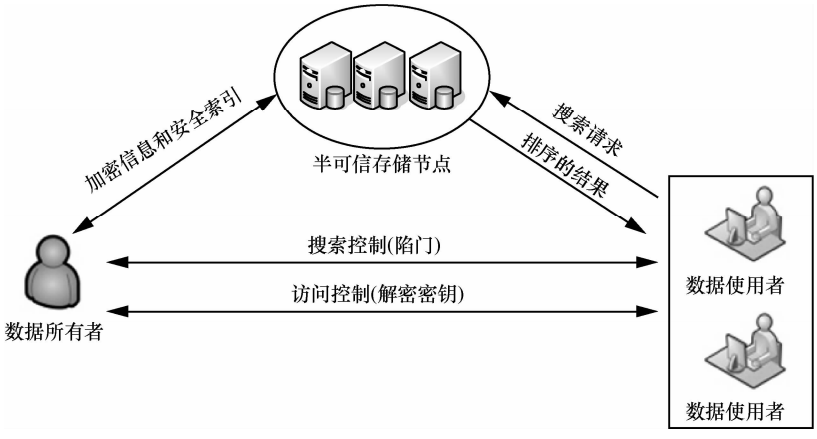


图 2　加密信息的搜索

在大量用户时，方案的效率会大幅降低，同时用户不能对多关键词进行自由搜索。Li 等[52]利用谓词加密（predicate encryption）技术设计了一种支持多用户，并可实现授权搜索的公钥可搜索加密方案，同样此方案存在着扩展性不高的问题，同时由于用户的搜索请求需要由可信的第三方产生，方案的效率较低，且不支持对文本、二进制等其他文件类型的搜索，限制了方案的应用场景。Sun 等[53]第一次在基于属性加密(attribute-based encryption)技术的基础上，提出了一种灵活的、扩展性强的、支持授权搜索的安全密文搜索技术，大大扩展了密文搜索的应用场景，此方案不仅支持单一关键词搜索，也支持固定多关键词的并集搜索。需要指出的是，虽然基于公钥的可搜索加密技术更适用于多用户的移动互联网模型，但因现有方案不可避免地存在对双线性对的操作，搜索效率不高，同时现有方案并不支持多关键词的自由搜索，这也影响了这一技术在实际场景中的使用，另外现有工作缺少对密文数据更新和对搜索结果进行认证的支持。基于对称密钥的可搜索加密方案搜索效率高，且能够支持对多关键词的自由搜索，但当系统存在大量用户，且需要对用户进行访问控制时，同基于公钥的密文搜索技术相比，方案的灵活性和可扩展性较低，应用场景的局限性较强。

从对查询的关键词的精确程度上划分，以上 2 种类型的可搜索加密方案均为针对精确的关键词搜索，除此以外，还有一类支持模糊关键词搜索的加密方案。Li 等[54]提出利用编辑距离来衡量关键词的相似程度，设计出基于通配符的模糊关键词搜索的加密方案，其方案只针对单一关键词搜索。Chuah 等[55]利用布隆过滤器构建关键词索引，提出一种支持多关键词模糊查询的可搜索加密方案，但应当指出这不是传统意义下的多关键词概念，而是利用概率分布将相关单词置于同一索引中。Wang 等[56]利用位置敏感的散列函数(locality-sensitive hash)技术提出了一种支持多关键词模糊查询的密文搜索方案，此方案真正实现了多关键词的自由搜索，方案的灵活性较强。但这类方案大多基于对称密钥实现，并不支持复杂的多用户场景。

由于在移动互联网应用中密文数据存储将不仅限于云存储这一种模型，还包括在移动设备中分布式密文数据存储的模型。针对后一种模型如何高效的构造安全搜引，并且适应移动终端的资源受限、数据信息多样性，移动用户属性动态变化的搜索构造方案和分布式可搜索加密算法将是一个新的待解决的问题。

3 数据传播模式和安全管控

随着移动互联网中大量的用户数据被存储在移动服务的云端系统中，数据管理权和所有权分离将带来诸如数据泄漏、数据非法访问及使用等问题。因此，需要采取一些措施来保证数据在移动互联网的安全管理。在移动互联网数据所有权与管理权分离的环境下对于数据安全的主要方法就是进行数据加密、可控解密与数据安全销毁。目前，学术界陆续提出了一些基于密码学的新技术来解决访问控制、数据销毁机制以及数据可靠存储状态审计的问题。

3.1 基于密码的访问控制技术

访问控制是一种有效的防止未授权的用户获取机密和隐私信息的技术。在近 30 年来，访问控制技术已经被学术界进行了大量的研究，提出了各种基于不同密码技术的访问控制系统[57~59]。然而，传统的访问控制模型都假设用户和服务器处于同一个信任域中，并不适用移动互联网环境。因此，移动互联网环境下的访问控制方案的设计必须使用新的加密技术，基于属性加密（ABE）的方案应该是一种适应于移动互联网信息分发场景下进行访问控制的方案。

ABE 方案首先由 Sahai 等提出[60]，Goyal 等[57]随后提出了一个细粒度访问控制的 ABE 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。该方案的访问控制策略是嵌入在私钥当中，当用户属性满足访问控制公式时可以恢复出密钥，从而解密消息，其本质是一个多级的秘密共享方案，因此被称为密钥策略 ABE 方案。KP-ABE 方案需要根据访问控制策略向具有权限的用户分配解密私钥份额，是当策略变化时，需要重新分配解密私钥份额，密钥管理开销很大。

Bethencourt[61]提出了密文策略的 ABE 方案(CP-ABE)，访问控制策略嵌入密文当中，而不同属性具有相应的解密私钥。因此当密文的访问控制策略改变时只需要根据新的访问控制策略重新加密密文，不需要重新分配属性对应的解密私钥。CP-ABE 方案更加类似于基于角色的访问控制。

目前 ABE 的主要研究包括支持访问控制策略

的灵活细粒度表示[59,62]、访问控制策略的隐藏[63,64]、ABE 在密文尺寸和计算效率上的提升[65~68]以及属性或用户撤销时的密钥管理等[69]。

从移动互联网环境下的数据传播安全、细粒度、规模化和动态的访问控制需求来看，高效的 CP-ABE 是更加适合的技术路径。但是密钥管理、策略管理、属性和用户管理等方面还有许多问题需要研究。

3.2　数据安全销毁机制

数据安全销毁是针对云计算应用中数据外包存储带来的数据所有者和数据管理权分离情况下如何删除数据的问题。在移动互联网数据传播过程中也面临同样的问题。由于数据在移动互联网传播和存储过程过程中采用加密机制，因此可以将安全销毁问题转化为对应解密密钥的安全销毁。一旦可以确保安全地销毁密钥，那么即使移动互联网当中仍然保留用户本该销毁的密文数据，这些数据也将不能再被读取，不会造成用户隐私数据的泄露。

Boneh 和 Lipton 提出了通过利用加密来删除信息的方案[70]。Di Crescenzo 等[71]针对一群文件中的任意一个文件的有效安全删除引进了树状结构。在树的根节点上的主密钥可删除，树中的每一个中间节点密钥都加密下面的多个密钥，叶子节点的密钥加密文件本身。Mitra 和 Winslett[72]提出了一种通过创建一个逆转存储数据记录的关键字索引的方法。这个方法利用加密并通过假设加密密钥被破坏的方法允许可选择的删除数据记录以及相关的索引中的关键字。Perlman[73]首次提出了基于时间的数据可信删除方法。在该方法中，数据可被安全删除并在预定的时间后数据将永久不可访问。FADE 系统[74]使用非对称密码并引入简单的利用布尔操作调整删除的策略。但是，FADE 的策略被限制为一层或者 2 层的布尔表达，并且它的策略需要使用复杂的非对称密码系统。Peterson 等[75]在数据块层使用全有或全无的变换规则（AONT）并化合覆盖的方法来实施安全删除。该方法通过 AONT 存储每一个数据块然后覆盖其中的一部分，这将使整个数据块不可用。Geambasu 等给出了一个基于时间的数据可信删除方法的原型 Vanish[76]。Vanish 将数据密钥划分为多个部分，然后被存储在 P2P 网络的不同节点中。每个节点将在自己的缓存中保存数据 8 小时，过了 8 小时后，节点将删除所分享的密钥部分。当文件在 8 小时后需要被接入时，文件拥有者需要更新节点缓存中的密钥部分。但是这种方法只依赖于时间的期满来实现数据的可信删除，并没有考虑到相关于文件不同的接入策略的更细粒度控制的可信删除方法。Cachin 等[77]首次严格地定义了基于加密的数据安全销毁的安全模型和安全定义。该方案通过利用图论（graph），对称加密和门限秘密共享（threshold secret sharing）相结合的方式来实现基于策略的数据安全销毁（policy- based secure deletion）。数据安全销毁在数据通过物理媒介传播的过程中也被广泛关注。构造适合于移动互联网环境下的基于策略的、细粒度、安全、可靠的数据可信销毁机制仍然是一个尚待解决的关键问题。

表 1　　**现有移动互联网中隐私保护方案分析**

方法	文献出处	可信第三方	*k*-anonymity	混淆	移动设备	身份泄漏	位置泄漏	兴趣泄漏	连续场景
CliqueCloak[78]	TMC'06	Y	Y	Y	N	N	N	Y	N
Casper[79]	VLDB'08	Y	Y	N	N	N	N	Y	N
P2Pcloaking[80]	GIS'06	N	Y	N	Y	N	N	Y	Y
k-anonymity[81] Footprint[81]	Infocom'08	Y	Y	N	N	Y	N	Y	N
CacheCloak[82]	Mobicom'09	Y	N	Y	Y	Y	Y	Y	N
Feeling-based pyramid[83]	CCS'09	Y	N	Y	N	N	N	N	N
CAP[84]	ICDCS'09	N	N	Y	Y	N	N	Y	N
Dummy-Q[85]	Infocom'11	N	N	Y	Y	N	N	Y	Y
ICliqueCloak[86]	TKDE'12	Y	Y	N	N	N	Y	Y	Y
MobiCrowd[87]	Mass'11	N	N	Y	Y	Y	Y	N	N
EPS[88]	Globecom'13	N	Y	Y	Y	Y	N	N	N
DLS[89]	Infocom'14	N	Y	N	Y	N	N	Y	N

4 隐私保护机制

针对移动互联网中用户的隐私相关问题，无论是政府、工业界还是学术界，都给予了极大的关注。

目前本领域的研究重点主要集中于基于数据失真或数据加密的隐私保护技术，包括基于隐私保护分类的数据挖掘算法、关联规则挖掘、分布式数据的隐私保护及协同过滤推荐、网格访问控制、基于分布受限的位置隐私保护技术等。

表1主要从移动用户的身份信息、位置信息以及兴趣信息3方面对隐私保护问题分析了现有研究成果所采用的主流技术及相应的优、缺点。从网络架构方面考虑，当前方案主要分为集中式网络架构和分布式网络架构。集中式网络架构往往依赖于一个可信第三方（TTP, trusted third party），用户将当前位置及请求的服务内容与身份等信息发送给TTP，由TTP根据用户发送的请求信息及用户当前位置信息做相应处理变换，之后再连同服务请求一起发送给服务提供商。服务提供商对用户的身份信息进行验证，并将查询到的服务信息返回给TTP，TTP经过过滤最终返回给用户。从表1提及的现有方案中可以看到，当前解决方案大都基于可信第三方，由可信第三方完成匿名或者混淆策略，从而保护用户的位置隐私和兴趣隐私。用户的身份认证一般由可信第三方或者服务提供商进行认证。CliqueCloak[78]和 Casper[79]作为最早的个性化匿名方案，为用户提供匿名区域大小可调的 *k*-anonymity，但其隐私保护的实现基于可信第三方（location anonymiser）。Footprint *k*-anonymity[81]利用移动用户的历史信息，通过在相遇用户之间构成一个虚拟的Mix-Zone 来完成对用户兴趣信息和身份信息的混淆，从而实现 *k*-anonymity。然而该方案仍未能避免可信第三方的介入。CacheCloak[82]作为另一种基于可信第三方的解决方案，它引入了缓存和预测的概念，通过缓存的用户历史轨迹等信息，预测用户下一步的移动，为用户提供实时的服务。但是当用户身处全新环境时，该方案的预测准确性会大幅降低。Xu 和 Cai[83]提出了 Feeling-based pyramid 解决方案，该方案将地图进行划分，并根据用户的感兴趣程度赋予不同的权重，通过分析历史信息，用信息熵的概念实现 P-popular trajectory （PPT）。该方案能够有效地保护用户的位置信息和兴趣信息，但对第三方的依赖以及其较高的计算资源消耗，使其难以直接用于当前移动互联网环境。Pan[86]等人提出了 ICliqueCloak，虽然该方案可以在连续场景下同时保护用户的位置信息和兴趣信息，但由于其较高的运算复杂度，难以适应移动环境。Zhu 等[87]首次提出通过将用户与证书之间的注册链条打断，并将各部分交由不同的实体进行管理的方案来实现对用户的身份信息的保护，进而实现用户个人信息的安全、有效更新，防止来自用户和服务运营商双方的欺骗和共谋等攻击。总体而言，以上基于集中式网络架构的解决方案存在的隐患相对较多且较为明显，集中表现在需要可信第三方的支持，难以提供对用户身份信息的保护，不能同时保护位置信息和兴趣信息，不支持连续场景下的隐私保护，且大都不支持移动设备等，因而不适合在移动互联网中广泛应用。

与此同时，有一些隐私保护技术并不依赖于TTP，其基本思想主要集中于用户和其他用户之间交互信息，通过 peer to peer（P2P）或者基于相遇的解决方案实现匿名集的构造，从而保护用户隐私。Chow[80]等人提出了一种基于 P2P 的解决方案，通过用户的相互协作，用近距离通信标准（WiFi或蓝牙技术）实现用户之间的信息交换，在考虑用户的最大移动距离基础上，实现连续场景下的 *k*-anonymity，以保护用户的位置隐私。然而由于用户的移动模式和近距离通信的通信距离限制，使真实用户的位置会以较大概率落在匿名集的中心区域。另外，用户仍需将自己的真实身份和兴趣信息发送给服务运营商，所以该方案难以同时保护用户的身份信息和兴趣信息。CAP[84]是一个基于四叉树和 various-grid-length Hilbert curve（VHC）的 P2P 解决方案，根据道路密度，CAP 用一个大小可调的希尔伯特曲线对地图进行填充，用四叉树的存储结构，在有效实现 *k*-anonymity 的基础上大幅度降低系统的计算和存储开销。Pingley 等[85]提出了 DUMMY-Q，通过在本地构建一个兴趣信息池（query-pool），利用虚假兴趣信息选择算法高效地实现 *k*-anonymity，从而有效抵御来自主动攻击者的推理攻击（inference attack）。但高额的兴趣信息池维护开销对手机用户而言难以负担。Shokri 等[88]提出了一种基于群组的用户隐私保护方案，当前用户通过将所需查询在群组内转发，由某一用户替代其向服务运营商发送服务请求，从而实现对当前用户身份信息、位置信息和兴趣信息的保护。但该方案

的问题在于代替当前用户进行发送请求的用户没有足够的动力来进行此类操作，加之移动设备的资源受限性，该方案难以在移动互联网中广泛应用。Niu 等[89]将 *k*-匿名和基于相遇的技术相结合，通过用户终端上的一个本地缓存，在不依赖任何第三方的基础上，由用户之间交互相关信息，从而实现对用户位置、兴趣信息及身份信息的保护。但该方案未能实现对连续场景的用户隐私保护。同时，Niu 等[90]考虑到背景信息以及匿名区域大小对 *k*-anonymity 效果的影响，结合信息熵设计了在拥有背景信息攻击者的场景下的用户隐私保护方案，该方案同时可以保证较大的匿名区域。然而该方案需要一定的 warm-up 时间，即不能在系统运行开始就为用户提供期望的隐私保护效果。总体而言，现有基于分布式网络架构的隐私保护方案大都依赖于用户之间的相互协作，个人信息需要在协作群里传递，进而对于由此产生的用户个人隐私保护问题的研究显得尤为重要。

5　结束语

未来移动互联网服务的安全和隐私保护应从以下几个方面开展研究。

1) 基于移动互联网信息传播、管控以及绿色节能的需求，优化设计移动互联网络服务的网络架构以及数据组织管理模式，而不是在网络架构上以打补丁的方式提供安全机制。在未来 5G 等移动互联服务网络架构中，可以考虑在基站增加信息缓存和内容分发功能，同时结合 D2D 机制形成混合信息共享的架构，进而研究相应的信息标记、映射和传播机制，并将安全管控和隐私保护进行整体设计。

2) 在移动互联网信息的传播管控机制方面，研究适应移动互联网信息传播访问控制的高效加密机制，基于属性加密应用于移动互联网传播管控时还需要解决属性密钥多安全域管理、数据销毁以及数据使用状态监控等一系列问题，只有数据所有者能够对其数据具有全生命周期管控的能力，才能保护数据所有者的权益，数据所有者才会愿意为移动互联网服务提供更加丰富的数据。

3) 从移动互联网用户的身份、行为、兴趣、位置等维度，结合对移动互联网服务的信任管理，综合考虑设计动态、细粒度的隐私保护机制，同时也要保证必要时的追责，这样才能保护用户放心地使用移动互联网服务。需要研究和建立隐私与利益的量化平衡模型，从而为移动互联网服务的隐私管理提供决策支持。

只有从上述 3 个方面形成整体的解决方案，才能有效保证移动互联网的绿色节能，保护所有者的权益以及信息使用者的隐私，从而促进移动互联网的健康有序发展。

参考文献：

[1] GROSKY W I, KANSAL A, NATH S. SenseWeb: an infrastructure for shared sensing[J]. IEEE MultiMedia, 2007, 14(4): 8-13.

[2] ABERER K, HAUSWIRTH M, SALEHI A. Infrastructure for data processing in large-scale interconnected sensor networks[A]. Proceedings of International Conference on Mobile Data Management[C]. Mannheim, Germany, 2007.198-205.

[3] CHANG K, YAU N, HANSEN M. SensorBase.org-a centralized repository to slog sensor network data[A]. Proceedings of International Conference on Distributed Computing in Sensor Network (DCOSS)/ Euro-American Workshop on Middleware for Sensor Networks (EAWMS)[C]. San Francisco, CA, USA, 2006.

[4] GIBBONS P B, KARP B, KE Y. IrisNet: an architecture for a world-wide sensor Web[J]. IEEE Pervasive Computing, 2003, 2(4): 22-33.

[5] SHETH A, HENSON C, SAHOO S. Semantic sensor Web[J]. IEEE Internet Computing, 2008:78-83.

[6] ZHANG J, IANNUCCI B, HENNESSY M. Sensor data as a servic: a federated platform for mobile data-centric service development and sharing[A]. IEEE 10th International Conference on Services Computing[C]. 2013.

[7] THEOTOKIS S A, SPINELLIS D. A survey of peer-to-peer content distribution technologies[J]. ACM Computing Surveys,2004,36(4): 516-527.

[8] CUTILLO L, MOLVA R, STRUFE T. Safebook: a privacypreserving online social network leveraging on real-life trust[J]. IEEE Commun Mag, 2009,47(12):94-101.

[9] Avaialable online[EB/OL]. http://joindiaspora.org.

[10] THILAKARATHNA K, PETANDER H, MESTRE J. MobiTribe: cost efficient distributed user generated content sharing on smartphones[J]. IEEE Transactions on Mobile Computing, 2014,13(9):2058-2070.

[11] XU D, KULKAMI S S, ROSENBERG C. Analysis of a CDN-P2P hybrid architecture for cost-effective streaming media distribution[J]. Multimedia Systems, 2006, 11(4):383-399.

[12] GUO L, CHEN S, REN S. PROP: A scalable and reliable P2P assisted proxy streaming system[A]. Proc of 24th International Conference on Distributed Computing Systems[C]. 2004.778-786.

[13] PAKKALA D, KOIVUKOSKI A, PAASO T. P2P middleware for extending the reach, scale and functionality of content delivery networks[A]. Proc of Second International Conference on Interact and Web Applications and Services[C]. 2007.

[14] CHAN H, LAM T. Efficiency of data distribution in BitTorrent-like systems[A]. Proc of 3rd International Conference on Algorithmic Aspects in Information and Management[C]. 2007.378-388.

[15] AHLGREN B, DANNEWITZ C, IMBRENDA C. A survey of information-centric networking[J]. IEEE Communications Magazine, 2012, 50(7):26-36.

[16] XYLOMENOS G, FOTIOU N, TSILOPOULOS C. A survey of information-centric networking research[J]. IEEE Communication Surveys & Tutorials, 2014,16(2):1024-1049.

[17] KOPONEN T, CHAWLA M, CHUN B. A data-oriented (and beyond)

network architecture[A]. ACM SIGCOMM[C]. 2007.181-192.
[18] FP7 PURSUIT project[EB/OL].http://www.fp7-pursuit.eu/ Pursuit-Web/.
[19] FP7 PSIRP project[EB/OL].http://www.psirp.org/.
[20] FP7 SAIL project[EB/OL].http://www.sail-project.eu/.
[21] FP7 4WARD project[EB/OL].http://www.4ward-project.eu/.
[22] FP7 COMET project [EB/OL].http://www.comet-project. org/.
[23] FP7 CONVERGENCE project[EB/OL].http://www. ictconvergence.eu/.
[24] NSF Named Data Networking project[EB/OL].http://www. named-data.net/.
[25] Content Centric Networking project[EB/OL].http://www. ccnx.org/.
[26] NSF Mobility First project[EB/OL]. http://mobilityfirst. winlab. rutgers.edu/.
[27] ANR Connect project[EB/OL]. http://anr-connect.org/.
[28] STOICA I, ADKINS D, ZHUANG S. Internet indirection infrastructure[A]. Proc of the ACM SIGCOMM[C]. 2002. 73-86.
[29] JACOBSON V, SMETTERS D K, THORNTON J D. Networking named content[A]. Proc of the 5th international conference on emerging networking experiments and technologies (CoNEXT '09)[C].2009. 1-12.
[30] JAYASUMANA A P. Distributed, multi-user, multi-application, and multi-sensor data fusion over named data networks[J]. Computer Networks, 2013, 57(16): 3235-3248.
[31] WANG J, PENG C, LI C. Implementing instant messaging using named data[A]. Proc of the Sixth Asian Internet Engineering Conference (AINTEC '10)[C]. 2010. 40-47.
[32] BAUGHER M, DAVIE B, NARAYANAN A. Self-verifying names for read-only named data[A]. Proc of Computer Communications Workshops (INFOCOM WKSHPS)[C]. 2012.274-279.
[33] WANG Y, DAI H, JIANG J. Parallel name lookup for named data networking[A]. Proc of GLOBECOM 2011[C]. 2011.5-9.
[34] SONG D, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[A]. Proc of S&P[C]. 2000. 44-55.
[35] GOH E J. Secure indexes, Cryptology ePrint Archive, Report 2003/216[EB/OL]. http://eprint.iacr.org/, 2003.
[36] CHANG Y C, MITZENMACHER M. Privacy preserving keyword searches on remote encrypted data[A]. Proc of ACNS’05[C].2005. 442-455.
[37] CURTMOLA R, GARAY J A. Searchable symmetric encryption: improved definitions and efficient constructions[A]. Proc of ACM CCS’06[C]. 2006.79-88.
[38] 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.
[39] KAMARA S, PAPAMANTHOU C, ROEDER T. Dynamic searchable symmetric encryption[A]. Proc of ACM CCS[C]. 2012. 965-976.
[40] CAO N, WANG C, REN K. Privacy-preserving multi-keyword ranked search over encrypted cloud data[A]. Proc of IEEE Infocom[C]. 2011. 222-233.
[41] FORESTI S, JAJODIA S, PARABOSCHI S. Private data indexes for selective access to outsourced data[A]. Proc of the 10th Workshop on Privacy in the Electronic Society (WPES 2011)[C].2011.69-80.
[42] SUN W, WANG B, CAO N. Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking[A]. Proc of ACM ASIACCS[C]. 2013.71-82.
[43] 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 (TPDS), 2013,25(11):3025-3035.
[44] BONEH D, CRESCENZO G D, OSTROVSKY R. Public key encryption with keyword search[A]. Proc of EUROCRYP’04[C]. 2004. 506-522.
[45] ABDALLA M, BELLARE M, CATALANO D. Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions[A]. Proc of CRYPTO’05[C]. 2005.205-222.
[46] GOLLE P, STADDON J, WATERS B R. Secure conjunctive keyword search over encrypted data[A]. Proc of ACNS’04[C]. 2004. 31-45.
[47] BONEH D, WATERS B. Conjunctive, subset, and range queries on encrypted data[A]. Proc of TCC[C]. 2007.535-554.
[48] SHI E, BETHENCOURT V, CHAN H. Multi-dimensional range query over encrypted data[A]. Proc of IEEE Symposium on Security and Privacy[C]. 2007.350-364.
[49] KERSCHBAUM F, SORNIOTTI A. Searchable encryption for outsourced data analytics[A]. Proc of the 7th European conference on Public key infrastructures, services and applications (EuroPKI'10)[C]. 2010. 61-76.
[50] LAI X, LU R, FOXTON K. An efficient searchable encryption scheme and its application in network forensics[A]. Proc of E-Forensics[C]. 2010.66-78.
[51] HWANG Y H, LEE P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system[A]. Proc of Pairing[C]. 2007. 2-22.
[52] LI M, YU S, CAO N. Authorized private keyword search over encrypted data in cloud computing[A]. Proc of IEEE ICDCS[C]. 2011.383-392.
[53] SUN W, YU S, LOU V. Protecting your right: attribute-based keyword search with fine-grained owner enforced search authorization in the cloud[A]. Proc of IEEE INFOCOM[C]. 2014.226-234.
[54] LI J, WANG Q, WANG C. Fuzzy keyword search over encrypted data in cloud computing[A]. Proc of IEEE INFOCOM[C]. 2010.1-5.
[55] CHUAH M, HU W. Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data[A]. Proc of 31st International Conference on Distributed Computing Systems Workshops[C]. 2011.273-281.
[56] WANG B, YU S, LOU W. Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud[A]. Proc of IEEE INFOCOM[C]. 2014.273-281.
[57] GOYAL V, PANDEY O, SAHAI A. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proc of the 13th ACM Conference on Computer and Communications Security (CCS’06)[C]. 2006. 89-98.
[58] AGRAWAL R, KIERNAN J, SRIKANT R. Order preserving encryption for numeric data[A]. Proc of The ACM SIGMOD'2004[C]. 2004. 563-574.
[59] YU S, WANG C, REN K. Achieving secure, scalable, and fine-grained data access control in cloud computing[A]. Proc of IEEE INFOCOM[C]. 2010.1-9.
[60] SAHAI A, WATERS B. Fuzzy identity based encryption[A]. Proc of EUROCRYPT 2005[C]. 2005.457-473.
[61] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Proc of the IEEE Symposium on Security and Privacy[C]. 2007.321-334.
[62] MÜLLER S, KATZENBEISSER S, ECKERT C. Distributed attribute-based encryption, information security and cryptology[A]. ICISC 2008[C]. 2009.20-36.
[63] KAPADIA A, TSANG P P, SMITH S W. Attribute-based publishing with hidden credentials and hidden policies[A]. Proc of NDSS[C]. VA: Internet Society, 2007.179-192.
[64] ZHANG Y H, CHEN X F, LI J. Anonymous attribute-based encryption supporting efficient decryption test[A]. Proc of the 8th ACM SIGSAC symposium on Information, Computer and Communications Security[C]. NY, 2013.511-516.

[65] HERRANZ J, LAGUILLAUMIE F, R`AFOLS C. Constant size ciphertexts in threshold attribute-based encryption[A]. LNCS 6056: Proc of Public Key Cryptography[C]. Berlin, Germany, 2010.19-34.

[66] ATTRAPADUNG N, HERRANZ J, LAGUILLAUMIE F. Attribute-based encryption schemes with constant-size ciphertexts[J]. Theoretical Computer Science, 2012, 422(9):15-38.

[67] ZHOU Z B, HUANG D J. On efficient ciphertext-policy attribute based encryption and broadcast encryption[A]. Proc of 17th ACM conference on Computer and communications security[C]. NY, 2010. 753-755.

[68] CHEN C, ZHANG Z F, FENG D G. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost[A]. Proc of PROVABLE SECURITY[C]. 2011.84-101.

[69] JUNBEOM H, DONG K N. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transaction on Parallel and Distributed Systems, 2011, 22(7): 1214-1221

[70] BONEH D, LIPTON R. A revocable backup system[A]. Proc of 6th USENIX Security Symposium[C]. 1996.

[71] DI CRESCENZO, FERGUSON N, IMPAGLIAZZO R. How to forget a secret[A]. Proc of 16th Symposium on Theoretical Aspects of Computer Science (STACS)[C]. 1999. 500-509.

[72] MITRA S, WINSLETT M. Secure deletion from invertedindexes on compliance storage[A]. Proc of Workshop on Storage Security and Survivability (StorageSS)[C]. 2006. 67-72.

[73] PERLMAN R. File system design with assured delete[A]. Proc of Network and Distributed Systems Security Symposium (NDSS)[C]. 2007.81-88.

[74] TANG Y, LEE P P C, LUI J C S. FADE: Secure overlay cloud storage with file assured deletion[A]. Proc of Secure Comm[C]. 2010.380-397, 2010.

[75] PETERSON Z N J, BURNS R, HERRING J. Secure deletion for a versioning file system[A]. Proc of 4th USENIX Conference on File and StorageTechnologies (FAST)[C]. 2005.143-154.

[76] GEAMBASU R, KOHNO T, LEVY A. Vanish: increasing data privacywith self-destructing data[A]. Proc of USENIX Security Symposium[C]. 2009.299-350.

[77] CACHIN C, HARALAMBIEV K, SORNIOTTI A. Policy-based secure deletion[A]. Proc of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13)[C]. 2013. 259-270.

[78] GEDIK B, LIU L. Protecting location privacy with personalized *k*-anonymity: architecture and algorithms[J]. IEEE Trans Mobile Computing, 2008, 7(1): 1-18.

[79] MOKBEL M F, CHOW C Y, AREF W G. The new casper: query processing for location services without compromising privacy[A]. Proc of VLDB[C]. 2006. 763-774.

[80] CHOW C Y, MOKBEL M F, LIU X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service[A]. Proc of GIS, 2006. 171-178.

[81] XU T, CAI Y. Exploring historical location data for anonymity preservation in location-based services[A]. Proc of INFOCOM[C]. 2008. 547-555.

[82] MEYEROWITZ J, CHOUDHURY R R. Hiding stars with fireworks: location privacy through camouflage[A]. Proc of MobiCom[C]. 2009. 345-356.

[83] XU T, CAI Y. Feeling-based location privacy protection for location-based services[A]. Proc of CCS[C]. 2009.348-357.

[84] PINGLEY A, *et al*. Cap: a context-aware privacy protection system for location-based services[A]. Proc of ICDCS[C]. 2009. 49-57.

[85] PINGLEY A, *et al*. Protection of query privacy for continuous location based services[A]. Proc of INFOCOM[C]. 2011.1710-1718.

[86] PAN X, XU J, MENG X. Protecting location privacy against location-dependent attack in mobile services[J]. IEEE Trans Knowledge and Data Engineering, 2012, 24(8):1506-1519.

[87] ZHU Z, CAO G. APPLAUS: a privacy-preserving location proof updating system for location-based services[A]. Proc of IEEE INFOCOM[C]. 2011.1889-1897.

[88] SHOKRI R, PAPADIMITRATOS P, THEODORAKOPOULOS G. Collaborative location privacy[A]. Proc of IEEE MASS[C]. 2011. 500-509.

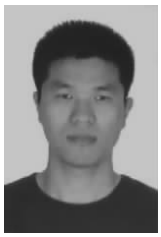
[89] NIU B, ZHU X, LEI X. EPS: encounter-based privacy-preserving scheme for location-based services[A]. Proc of GLOBECOM 2013[C]. 2013.

[90] NIU B, LI Q, ZHU X. Achieving *k*-anonymity in privacy-aware location-based services[A]. Proc of INFOCOM 2014[C]. 2014.

作者简介：

李晖（1968-），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。

李凤华（1966-），男，湖北浠水人，中国科学院信息工程研究所副总工、研究员、博士生导师，主要研究方向为网络与系统安全、可信计算。



曹进（1985-），男，陕西西安人，博士，西安电子科技大学讲师，主要研究方向为无线网络安全。

牛犇（1984-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为移动互联网隐私保护。

孙文海（1985-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为云计算安全。

耿魁（1989-），男，湖北红安人，西安电子科技大学博士生，主要研究方向为网络安全。