云存储环境下属性基加密综述*

赵志远[1], 王建华[1,2], 朱智强[1,3], 孙 磊[1]
(1. 信息工程大学, 郑州 450001; 2. 空军电子技术研究所, 北京 100195; 3. 郑州信大先进技术研究院, 郑州 450001)

摘 要: 属性基加密作为一种新型的密码方案,将用户私钥和密文与属性相关联,为解决云存储环境下数据安全共享、细粒度访问控制和安全存储等问题提供了一种解决思路。在对密钥策略属性基加密、密文策略属性基加密和混合策略属性基加密深入研究后,根据不同的功能扩展,针对隐藏访问结构、多授权机构、复杂计算安全外包、可搜索加密机制、属性撤销、叛徒追踪等重点难点问题进行了深入探讨研究。最后总结了现有研究工作的不足,并指出了未来的研究方向。

关键词: 云计算; 属性基加密; 访问结构; 细粒度访问控制
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2018)04-0961-08
doi:10.3969/j.issn.1001-3695.2018.04.001

Survey of attribute-based encryption in cloud storage environment

Zhao Zhiyuan[1], Wang Jianhua[1,2], Zhu Zhiqiang[1,3], Sun Lei[1]
(1. *Information Engineering University*, *Zhengzhou* 450001, *China*; 2. *Electronic Technology Institute of Air Force*, *Beijing* 100195, *China*; 3. *Zhengzhou Xinda Institute of Advanced Technology*, *Zhengzhou* 450001, *China*)

Abstract: As a new type of cryptography scheme, attribute-based encryption(ABE) associates the ciphertext and user's secret key with attributes, and provides a solution for the security sharing, fine-grained access control and security storage of data in cloud storage environment. Based on the study of key-policy ABE, ciphertext-policy ABE and dual-policy ABE, according to the different function expansion, this paper elaborated the related works of ABE, including hidden access structure, multi-authorities, security outsourcing of complex computing, searchable encryption mechanism, attribute revocation, traitor tracing. Finally, this paper summarized the shortcomings of existing works and pointed out the future research directions.
Key words: cloud computing; attribute-based encryption; access structure; fine-grained access control

0 引言

云计算是社会信息化发展中重要的新兴技术,它提供了一种全新的服务模式,为众多企业和个人提供了一个更好的服务平台。云计算技术因具有动态扩展、按需服务、按量计费等优势而成为继互联网之后又一次信息技术革命[1]。云存储是基于云计算建立起来的一个新型的网络存储技术,通过按需付费等方式向广大用户提供存储服务,免去用户管理资源和花费大量资金购买硬件等负担。如今广泛使用的云存储服务有亚马逊 S3、谷歌云存储、阿里云、百度云等。近年来,越来越多的用户在云端进行数据存储与共享,据 Gartner 公司分析,2016 年将有 36% 的数字内容和个人数据存储到云端服务器上[2]。

云存储以价格低廉、使用方便等优点为人们带来巨大便利的同时,也因为用户脱离对数据的实际控制而对用户的数据隐私要求带来严重威胁[3]。近年来,由于恶意用户的非法入侵和管理人员的非法操作导致很多安全事件,2014 年 9 月,iCloud 中的好莱坞演员账户被黑客破解,相册数据被泄露;2015 年 9 月,阿里云被曝出全部机器权限和用户资料被泄露;2016 年 8 月,百度云大量账号被盗,用户网盘中的数据被恶意窜改;同年 10 月,Dropbox 用户数据被泄露,影响近 6 900 万账号。国际数据分析机构 IDC 调查结果显示,云存储的数据安全问题已成为其推广所面临的难题之一[4]。

数据作为信息社会中人们的重要资产,历来都是被保护的关键对象,也是很多安全攻击的主要目标。多项调查报告显示,数据的安全与隐私保护被认为是云存储中用户的首要安全目标[5,6]。用户数据安全首先就是要确保用户数据的机密性,即保证数据为授权者所有而不会泄露给未经授权者。隐私保护主要涉及的是用户身份的安全,即保证用户身份对云存储服务提供商的匿名性以及用户身份的不可关联性等。

密码学作为信息安全的基石,可以提供信息的完整性、机密性、不可抵赖性、可控性及可用性[5],也是解决当前云存储安全问题的关键支撑技术之一。在云存储模式下,由于数据脱离了用户控制域,云存储服务商与用户之间缺乏信任机制,现阶段普遍的观点认为要实现用户数据的隐私保护,最直接有效的方法是将数据加密后再存储。这样,用户在享受云计算便利的同时,不必担心云服务器提供商非法获取用户的数据,而且即使云服务器被攻破,仍然可以将损失降至最低。但是在云存储这种模式下,这种方法牺牲了用户对数据的细粒度访问控制。

收稿日期: 2017-04-07; **修回日期**: 2017-05-21 **基金项目**: 国家重点研发计划资助项目(2016YFB0501900); 国家"973"计划资助项目(2013CB338000)

作者简介: 赵志远(1989-),男,吉林磐石人,博士研究生,主要研究方向为云安全与属性加密(zzy_taurus@foxmail.com); 王建华(1962-),男,北京人,教授,主要研究方向为云计算与信息安全; 朱智强(1961-),男,河南信阳人,教授,主要研究方向为云计算、信息安全; 孙磊(1973-),男,江苏靖江人,教授,博士,主要研究方向为云计算基础设施可信增强、可信虚拟化技术.

传统的对称加密技术和公钥加密技术难以应对云存储这种具有海量用户的复杂情况(密钥管理、密文副本数量多等问题)。

属性基加密(attribute-baesd encryption, ABE)[7]可以在密文或者密钥中嵌入访问控制策略,能够实现对数据的灵活访问控制[3],因此在云计算相关应用中有着广泛的应用前景。微软研究院密码技术小组 2010 年发布的《Cryptographic cloud storage》[8]白皮书中,也提出用属性基加密技术实现虚拟的私有云服务,解决备份、归档、健康记录系统、安全数据交换以及电子挖掘等加密数据的安全服务问题。

Boneh 等人[9]于 2001 年通过双线性对设计了第一个语义安全的身份加密方案(identity-based encryption, IBE),此后密码学界在身份加密领域展开广泛研究。2005 年欧密会上 Sahai 等人[7]为了改善基于生物信息加密系统的容错性能,基于上述身份加密方案提出基于模糊身份的加密方案(fuzzy identity-based encryption),该方案将用户身份分解成一系列描述用户身份的属性,加密者加密数据时指定一个属性集合和阈值 d,解密者必须拥有至少 d 个给定的属性才能正确解密密文。Sahai 等人开启了被大量企业和科研人员广泛研究的 ABE 的开端;随后,Goyal 和 Bethencourt 等人基于 ABE 提出两种变体机制,即密钥策略的 ABE 方案(key-policy ABE, KP-ABE)[10]和密文策略的 ABE 方案(ciphertext-policy ABE, CP-ABE)[11]。至今为止,仍有许多学者针对 ABE 方案的特点与实际情况,在增强安全性、提高加密效率、访问策略隐藏、多属性权威机构、数据加/解密及密钥产生安全外包、可搜索加密、属性或用户可撤销和叛徒可追踪等方面展开大量研究工作,如图 1 所示。

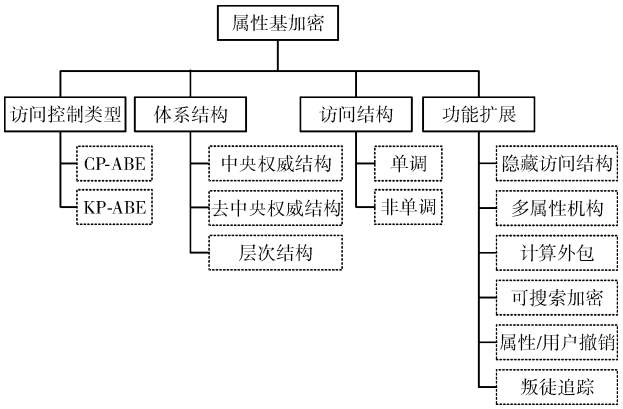

图 1 属性基加密分类

属性基加密具有广泛的应用。在 KP-ABE 中,管理机构根据用户的访问结构(权限)分发相应的解密私钥,而用户规定对接收消息的属性要求。因此,KP-ABE 适用于查询类的应用,如付费电视系统、视频点播系统、数字版权管理、审计日志和密文检索等。而在 CP-ABE 中,管理机构根据用户的属性集合分发解密私钥,加密者根据自己的意愿选定访问策略并利用该访问策略加密消息,只有那些属性满足密文访问策略的用户才能解密。因此,CP-ABE 适用于访问控制类的应用,如社交网络的访问、电子医疗系统(Microsoft HealthVault、Google eHealth)和教育系统等。

1 属性基加密方案分类

属性基加密包括密钥策略属性基加密方案、密文策略属性基加密方案和混合策略的属性基加密方案。

1.1 KP-ABE 方案

2006 年 Goyal 等人[10]基于 fuzzy IBE 提出一种细粒度访问控制的 ABE 方案,该方案将访问策略嵌入私钥中,而密文与属性集合相关联,因此被称为 KP-ABE。KP-ABE 本质是一种一对多的公钥加密技术,该方案通过引入访问树(access tree)结构,用一棵访问树来表示访问策略,并在标准模型下证明了方案的安全性。与模糊基于身份加密仅能支持单个门限访问结构相比,访问树结构能够支持任意的单调访问结构,可以很方便地实现属性间的与(and)、或(or)以及门限(threshold)操作,能够支持细粒度的访问控制。该方案的提出丰富了 ABE 的性质和适用范围,大大加快了 ABE 相关研究的发展。一般情况下,KP-ABE 方案的形式化定义如下:

a) Setup(λ)。该算法以一个安全参数 λ 作为输入,输出一个公共参数 PK 和一个主私钥 MK。

b) KeyGen(PK; MK; A)。该算法以访问结构 A、主私钥 MK 和公共参数 PK 作为输入,输出一个解密密钥 SK。

c) Encryption(PK; M; S)。该算法以明文消息 M、属性集合 S 和公共参数 PK 作为输入,输出密文 CT。

d) Decryption(PK; CT; SK)。该算法以密文 CT(关联属性集合 S)、解密密钥 SK(关联访问结构 A)和公共参数 PK 作为输入。如果 $S \in A$,则可以解密成功,获得明文消息 M,否则算法终止。

基本 KP-ABE 方案的结构图如图 2 所示。

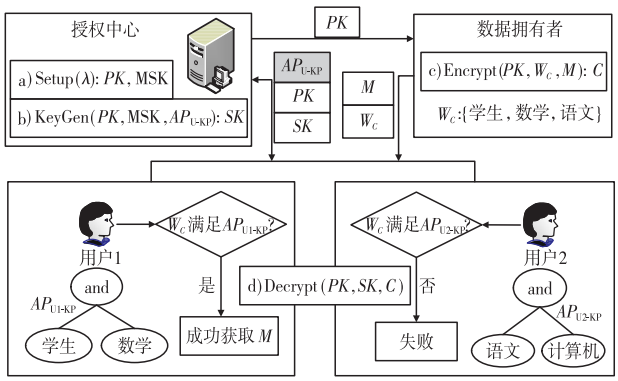

图 2 KP-ABE 结构图

Ostrovsky 等人[12]在 KP-ABE 体制的基础上加入了“非(not)”操作,构造了一个具有通用结构的 KP-ABE 方案,实现了非单调访问结构,进一步增强了逻辑表达能力。Zheng[13]提出一种具有强表达能力的 KP-ABE,其可以对加密数据实施细粒度访问控制。大多数 ABE 方案中,密文大小与密文属性数量成线性关系,Zheng 所提出的具有强表达能力的 KP-ABE 支持非单调访问结构,并且密文大小与属性数量无关,是一种定长密文的 ABE;同时该方案将双线性对运算缩小到常数级别,是一种更加有效的 KP-ABE。

为了提高 KP-ABE 方案的效率,可以引入对称加密算法。具体过程为:首先利用对称密钥加密每一个文件或者明文,然后利用 KP-ABE 方案加密该对称密钥,通过对该对称密钥实施细粒度访问控制以达到对文件或明文的细粒度访问控制。因为对称密钥往往要比文件或明文小很多,所以这种方法可以提高加密方案的效率,又可以达到 KP-ABE 方案的细粒度访问控制。

1.2 CP-ABE 方案

2007 年 Bethencourt 等人[11]提出 CP-ABE,该方案将访问

策略嵌入密文中,而密钥与属性集合相关联。该方案访问结构部署在密文中,发送者可以根据密文自己决定如何定义访问结构,因此灵活性较强。其与传统访问控制中的基于角色的访问控制(RBAC)相似。另外,该文献还提供了一个用于实现该方案的程序包,实验分析表明该密文策略的属性基加密体制具有很高的效率。但是该方案的安全性只是在一般群模型(generic group model)下进行了讨论,本质上并不具有可证明安全性。但这篇文章从此开启了 CP-ABE 体制研究与应用的大门,一般情况下,CP-ABE 方案的形式化定义如下:

a) Setup(λ)。该算法以一个安全参数 λ 作为输入,输出一个公共参数 PK 和一个主私钥 MK。

b) KeyGen(PK; MK; S)。该算法以属性集合 S、主私钥 MK 和公共参数 PK 作为输入,输出一个解密密钥 SK。

c) Encrypt(PK; M; A)。该算法以明文消息 M、访问结构 A 和公共参数 PK 作为输入,输出密文 CT。

d) Decrypt(PK; CT; SK)。该算法以密文 CT(基于访问结构 A)、解密密钥 SK(基于属性集合 S)和公共参数 PK 作为输入。如果 $S \in A$,则可以解密成功,获得明文消息 M,否则算法终止。

基本 CP-ABE 方案的结构图如图 3 所示。

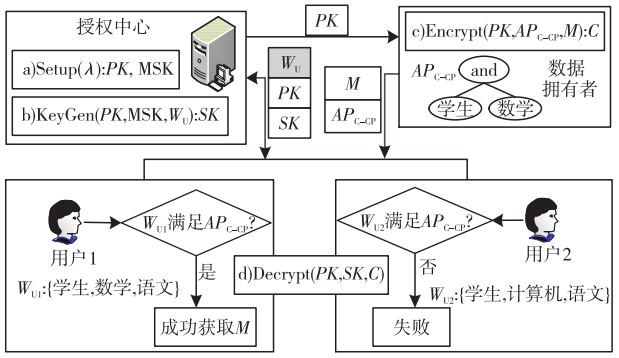

图 3　CP-ABE 结构图

2007 年 Cheung 等人[14]提出了第一个在标准模型下基于标准假设证明安全性的 CP-ABE 方案,该方案的访问结构是支持正属性和负属性的与门访问结构,该方案访问结构表达能力弱、公共参数长且与系统中属性个数成正比。Waters[15]在文献[7]的基础上,利用线性秘密共享方案(linear secret sharing scheme,LSSS)实现任意单调的访问结构,提出了一个高效的能够支持通用访问结构的密文策略属性基加密方案,并基于较强的数学困难问题假设证明了安全性。相比之前的密文策略属性基加密方案,该方案在安全性、效率以及表达力等方面都达到了较高水平,相应结果发表在 2011 年 PKC 会议上。Lewko 等人[16]通过合数阶双线性群(composite order bilinear groups)和双系统加密(dual system encryption)技术对 CP-ABE 方案进行改进创新,给出一种全新的安全性证明方式,使方案实现了自适应安全(adaptive security)。由于方案基于合数阶双线性群构造,导致方案效率不高。随后,Okamoto 等人[17]利用对偶配对向量空间(dual pairing vector space,DPVS)技术,在素数阶双线性群上构造了完全安全的属性基加密体制,该方案在安全性、表达力和效率方面都达到了令人满意的水平。2012 年,Lewko 等人[18]进一步研究了在素数阶双线性群上构造完全安全的属性基加密方案,在文献[17]的基础上改进了访问策略中每个属性至多只能出现一次的限制,提高了效率;此外,还研究了合数阶双线性群与素数阶双线性群中对偶配对向量空间 DPVS 的内在联系,给出了一种由选择性安全的属性基加密方案构造完全安全的属性基加密方案的转换方法。

1.3　混合策略 ABE 方案

2009 年,Attrapadung 等人[19]首先提出双策略的 ABE 方案(dual-policy attribute-based encryption,DP-ABE),该方案通过结合 KP-ABE 和 CP-ABE 两种方案,在密钥和密文中同时部署两种策略。密文的两种访问控制策略一个表示加密数据自身客观性质的属性,另一个表示对解密者需要满足条件的主观性质属性;密钥的两种访问策略一个表示用户凭证的主观属性,另一个表示用户解密能力的客观属性。只有当用户的主观属性和客观属性满足了密文的主观属性和客观属性时,用户才能解密密文。一般情况下,DP-ABE 方案的形式化定义如下:

a) Setup(λ)。该算法以一个安全参数 λ 作为输入,输出一个公共参数 PK 和一个主私钥 MK。

b) KeyGen(PK; MK; A; S)。该算法以客观访问结构 A 和主观属性集合 S、主私钥 MK 和公共参数 PK 作为输入,输出一个解密密钥 SK。

c) Encrypt(PK; M; Ψ; ζ)。该算法以明文消息 M、主观访问结构 Ψ、客观属性集合 ζ 和公共参数 PK 作为输入,输出密文 CT。

d) Decrypt(PK; CT; SK; A; S; Ψ; ζ)。该算法以密文 CT(基于访问结构 Ψ 和属性集合 ζ)、解密密钥 SK(基于访问结构 A 和属性集合 S)和公共参数 PK 作为输入。如果 $S \in \Psi$ 并且 $\zeta \in A$,则可以解密成功,获得明文消息 M,否则算法终止。

因为 DP-ABE 方案可以看做是 CP-ABE 和 KP-ABE 方案的结合,所以 DP-ABE 方案可以根据实际需要转换成单个策略的 ABE 方案(CP-ABE 或 KP-ABE)。文献[20,21]针对混合策略属性基加密方案中的密文长度、计算效率等方面展开研究。

2　属性基加密相关工作

属性基加密主要是保证信息系统中数据的机密性,实现细粒度访问控制。针对系统中各种需求和所预见的问题,相关研究机构和相关人员在设计属性基加密方案时,提出了隐藏访问结构、多属性权威机构、数据加/解密及密钥生成安全外包、可搜索加密、属性或用户可撤销和叛徒追踪等方面的相关功能,本章主要从这些方面介绍相关的研究工作。

2.1　隐藏访问结构

属性基加密中,属性集合或者访问策略往往需要同密文一同上传至云端,这种情况下,任何试图解密的用户都能够推导出一些属性信息,而有时这些属性信息往往是一个人的敏感信息(电子医疗系统中病人的疾病状况,个人用户如身份证号等敏感信息),这将使得用户的个人数据置于高泄露风险中。

与匿名加密体制一样,隐藏访问策略的属性基加密体制主要防止敌手得到关于加密者和接收者的敏感信息,使其免遭非法攻击。例如,如果某大型的跨国公司想招聘一批员工,能够面试的要求是他们能够满足此公司的一些招聘条件。但是这些条件中可能包括一些对手公司关心的敏感信息,因此就需要将这些敏感信息隐藏起来然后放在招聘栏里,这样对手公司不能根据这些招聘信息来获得他们招聘员工的条件和其中的一些公司发展的战略,于是就保护了公司的商业机密,同时应聘者又能根据招聘信息进行面试。

隐藏访问策略的属性基加密有两个优点,一是加密者可以

指定解密方的角色,二是利用 ABE 的模糊性,用属性来描述对象,可以保护加密者的敏感信息。

2007 年,Kapadia 等人[22]首先提出了隐藏访问策略的属性基加密体制。Nishide 等人[23]提出两种通过使用通配符来达到部分隐藏访问结构的 ABE 方案:a)每个属性仅有两个值,该方法的扩展性不好;b)每个属性可以有多个值,可以在系统建立之后随意增加新的属性,并且系统原来的公共参数无须改变。Yu 等人[24]将 CP-ABE 应用到内容分发网络 CDN 中来实现细粒度的访问控制,该方案中内容提供者可以使用隐藏的访问控制策略来加密数据,即使合法的解密者除了知道自己是否能够解密外,无法得到有关密文访问控制策略的任何信息;但是该方案只支持受限的访问结构,且效率不高。Li 等人[25]提出一种匿名 CP-ABE 方案,该方案在生成属性私钥时通过盲化用户身份以达到匿名性。2011 年,Lai 等人[26]基于合数阶双线性群提出了一种适应性安全的策略隐藏 CP-ABE 方案。随后,王海斌等人[27]改善了 Lai 的方案,提出了一种基于素数阶双线性群的策略隐藏 CP-ABE 方案,该方案中私钥长度为常量且解密运算是固定的双线性对操作,因此在大规模属性应用环境中具有更高的效率。但是这几种方案只支持受限的访问结构,策略表达能力方面非常弱。

2012 年,Lai 等人[28]提出一个高效、表达能力强的 CP-ABE 方案,该方案在系统初始化阶段只公布属性名称,数据拥有者在加密阶段隐藏属性值,通过这种方法保护用户部分隐私,并在完全安全模型下证明了方案的安全性。2013 年 Hur[29]提出了一个支持任意访问机构的 CP-ABE 方案,对密文中的访问策略进行盲化,实现了访问策略隐私;而且该方案由云存储中心和用户共同生成密文,解决了密钥托管问题。但是该方案的安全性是在通用群模型下证明的,通用模型安全通常被认为是启发式的安全,而不是可证明安全。2015 年,宋衍等人[30]提出一种基于新型访问树结构具有“与”“或”“陷门”强表达能力的策略隐藏属性加密方案,该方案在计算开销方面没有过多增加,在实际应用过程中更加灵活和有效。

2.2 多属性(授权)机构

单授权中心的 ABE 方案中,密钥分发工作完全由一个授权中心承担,给授权中心带来了严重的负担,同时需要假定该授权中心完全可信[31]。而在多授权中心的 ABE(MA-ABE)系统,属性被相互独立的属性中心管理,一个或多个属性中心合谋也不能破坏整个系统的安全性。大多数情况下不同的组织运用不同的策略来共享信息,因此也需要多个授权中心管控所有用户的属性,构造一个安全可靠的多属性机构的属性基加密系统是解决上述问题的关键。多属性中心的 ABE 系统一般架构如图 4 所示。

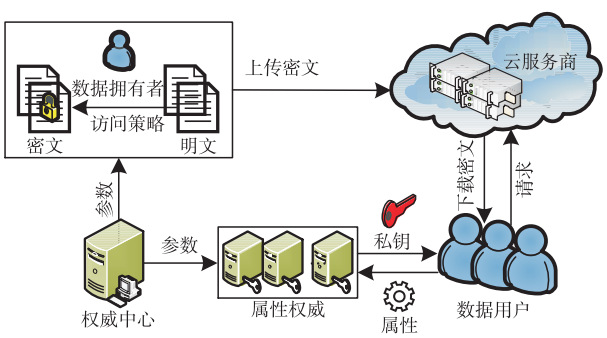

图 4 MA-ABE 系统架构

2007 年,Chase[32]首次实现了多授权机构下的 ABE 方案,该方案由多个授权机构分发密钥并管理属性。该系统中存在一个中央授权中心负责为其他的属性中心产生公钥和私钥,而用户从多个属性中心获得私钥。与单授权中心方案相比,多授权中心方案抵御用户合谋攻击问题更加困难。Chase 在方案中引入全局身份 GID,每一个用户被分配一个独一无二的 GID,而用户私钥与 GID 密切相关,这样即使多个用户合谋也无法解密一个他们单独无法解密的密文。但是该方案中多个恶意的授权中心能够通过跟踪用户 GID 搜集用户的属性信息,从而侵犯了用户的隐私权。

2009 年,Chase 等人[33]提出一个无中央授权中心的 MA-ABE,该方案通过使用一个分布式伪随机函数(PRF)来达到移除可信中央授权中心的目的。值得注意的是,在该方案中,用户通过使用一个匿名的密钥分发协议来获得自己的私钥,在这个过程中授权中心不能获得任何关于用户 GID 的相关信息,因此解决了保护用户隐私的问题。2011 年,Liu 等人[34]首次在标准模型下构造了无中央授权中心的多授权机构 ABE 模型,该方案中,在系统初始化阶段多个授权中心必须一起合作初始化系统;此外,如果要在系统中增加一个属性,多个授权中心必须一起合作重新设置系统。同年,Lewko 等人[35]利用合数阶双线性群在随机预言机模型下构建了一个多授权中心的 ABE 方案,该方案支持单调张成方案,但是仅支持有限集合(small universe)的属性,这也就意味着公共参数的大小与系统中属性个数成线性增长关系。

对于支持无限集合(large universe)属性的 ABE 方案,任何字符串都可以作为一个属性,并且这些属性无须预定义,也无须在系统建立阶段枚举出来。2015 年,Rouselakis 等人[36]提出一个随机预言机模型下支持无限集合属性的多授权中心的 ABE 方案,由于该方案使用素数阶双线性群,其在效率方面有一定优势;但是该方案只在选择安全模型下被证明是安全的。

2.3 复杂计算安全外包

随着移动互联网和移动智能终端的快速发展,使用移动终端访问云存储环境下的数据成为一种趋势,而移动智能终端的较弱计算能力、较低能量等问题致使其不能承载过大的计算负担和通信负担。传统的属性基加密在解密阶段往往需要大量的双线性对运算,这将给移动终端带来较大的电池损耗,所以在保证安全的情况下将部分计算外包给云服务商,是一种高效、经济的解决方案。复杂计算安全外包的基本思想是:通过改变系统的运算模式或利用外部计算资源承担一定的计算量等方法来减少本地的计算量[37]。云存储环境下加/解密安全外包的属性基加密方案架构如图 5 所示。

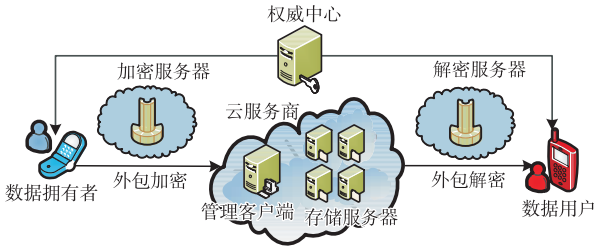

图 5 外包属性基加密方案架构

外包 ABE(OABE)方案提高了加密、解密的效率,但这也使 OABE 变得更加复杂。一方面,用户需要效率,但不希望云

服务器知道用户的私有信息;另一方面,云服务器可能是“懒惰”的,为了节省计算或带宽只计算部分操作并返回不正确的结果,错误的解密结果可能会导致严重的医疗事故。另外,如果在云供应商返回了正确结果的情况下发生了医疗事故,应该存在一个机制能够证明云供应商是无罪的。因此如何解决以下问题至关重要:如何防止公有云服务器获得私人信息? 如何验证公有云服务器返回结果的正确性?

针对上述问题,研究人员展开了深入的研究。2011 年,Green 等人[38]提出一种解密运算外包方案,该方案解密过程中首先将密文传送给解密外包服务器,解密外包服务器对密文进行一次密文转换获得中间密文再传送给用户,达到降低本地解密过程的计算量。Zhou 等人[39]提出了同时支持加密和解密外包的 ABE 方案。其中,通过对加密过程中的随机盲化因子 S 进行秘密共享,将部分访问策略的加密外包给了加密服务提供商,而只留下与外包策略通过 and 门连接的剩余访问策略在用户本地加密。Li 等人[40]通过 MapReduce 实现了 ABE 加/解密运算的外包计算,且该方案支持树型访问结构。但是上述方案都没有提出如何验证中间密文的正确性。

2013 年,Lai 等人[41]在实现外包解密的同时,支持了对外包服务的正确性验证。2014 年,Li 等人[42]提出一个分布式系统中能够验证外包解密正确性的数据外包方案,该方案需要一个以上的密钥生成服务提供商(KGSP),并且至少一个 KGSP 能够诚实地以正确的密文作为输入;否则,该验证模型将遭受 Green 安全模型[38]中存在的攻击。2015 年,王皓等人[37]给出了外包 ABE 方案的形式化定义,并构造了一个具体的外包 CP-ABE 方案,该方案在标准模型下基于双系统加密技术证明了方案是自适应安全的。Hohenberger 等人[43]提出在线/离线 ABE 方案,该方案将原始的方案分成两个阶段:a)离线阶段,在知道属性或访问策略之前通过大部分加密计算得到中间密文;b)在线阶段,得到属性或者访问策略之后通过中间密文迅速获得最终密文。该方案的离线阶段提出两种计算方案,即用户通过智能终端获得中间密文和一个高端可信服务器帮助使用低端设备的用户做离线工作。无论如何,在线/离线 ABE 方案缩短了加密阶段所需时间,尤其是利用可信服务器帮助用户做离线工作的方法也是一种复杂计算安全外包 ABE 方案。

2.4　可搜索加密机制

随着云计算的广泛应用,越来越多加密的数据存储到云服务器端,如何在云端安全高效地获取需要的密文是一个重要的问题,因此可搜索加密方案应运而生并得到广泛发展和应用。通过研究总结,目前可搜索加密机制的研究内容如图 6 所示[44]。

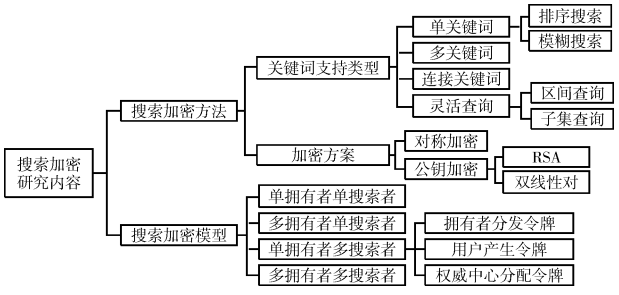

图 6　可搜索加密研究内容

广泛应用于云存储环境下的属性基加密方案更是需要可搜索加密机制。一般支持细粒度访问控制和关键词搜索的多用户加密云存储系统主要包括可信授权中心(trusted authority,TA)、云服务提供商(cloud services provider,CSP)、数据拥有者(data owner,DO)和数据使用者(data user,DU)。系统架构如图 7 所示。

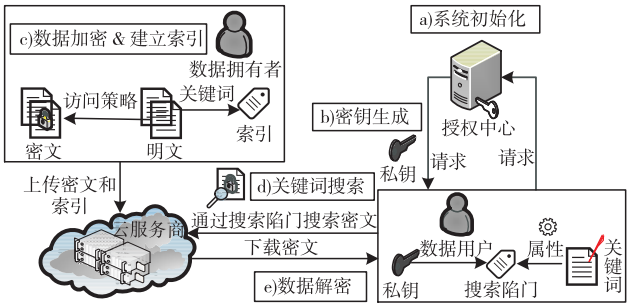

图 7　可搜索属性基加密系统架构

Song 等人[45]在 2000 年首次提出可搜索对称加密方案,该方案能够对密文进行文本搜索,但是其搜索效率不高,难以抵抗对密文的频率分析攻击。2004 年,Boneh 等人[46]利用公钥密码算法构造了一个可搜索加密方案(PEKS),对后来通过公钥密码学实现搜索加密方案具有重要指导作用。2011 年,Zhao 等人[47]提出了一种用于细粒度访问控制的安全数据共享的多用户关键字搜索方案,在云存储环境中搜索所有的关键词索引,然后与被给关键词相匹配,这种方法是不切实际的。因此该文献致力于使用 ABE 缩小搜索结果的范围,并且减少信息泄露和降低复杂度性,最后提出一种只对用户可以解密的相关文档进行搜索的方案,从而更加有效。2014 年,Cao 等人[48]提出一种多关键词可搜索公钥加密方案,该方案允许用户在同一时刻提交多个关键词进行检索,使得检索精度更加准确。Sun 等人[49]提出了一种具有高灵活性、强扩展能力,同时支持授权搜索的属性基加密方案,该方案在支持单关键词搜索的同时,也支持固定多关键词的并集搜索,这种搜索模式极大地增加了密文搜索的应用场景。Han 等人[50]提出一种从 KP-ABE 到 ABKES(attribute based encryption with keyword search)方案的一般转换方法,通过这种转换方法构建了一个具体的 ABEKS 方案,该方案允许多用户在远程加密数据上执行一个灵活的搜索。Zheng 等人[51]提出一种基于访问控制策略的、能够搜索和使用外包数据的新颖的加密方案,被称为 VABKS(verifiable attribute-based keyword search)。该方案中合法数据用户能够外包繁重的搜索操作到云端并且使用布隆过滤器和数字签名技术允许数据用户有效地验证云端是否忠诚地执行了用户搜索外包加密数据的操作。

当前多关键词排序搜索方案中,关键词字典是静态的,当关键词数量增加时不能轻易扩展。此外,当前方案也没有考虑用户行为和关键词访问频率的关系。对于包含大量文档的查询匹配结果,可能会出现排序问题,这使得数据使用者很难找到最有可能满足其需求的子集。为解决该问题,Li 等人[52]提出了一个灵活的多关键词查询方案,被称为 MKQE,该方案极大程度地降低了关键词词典扩展过程的维护开销。在生成查询结果时,该方案考虑了关键词权重和用户访问历史记录,因此,在搜索匹配结果集合中具有更高访问频率和更接近用户访问历史的文件能够获得更高的排名,通过实验表明 MKQE 方案在性能方面要优于当前其他方案。2015 年,Revathy 等人[53]提出一种基于自动标记搜索技术的可搜索和访问加密数据的安全 ABE 方案,该方案同时使用 KNN 技术可以将前 k 个搜索结果以排名的方式展现出来,该方案可以有效地提高系统的性

能、降低通信开销,也消除了不必要的通信。

2.5 属性或用户撤销

基于被撤销属性对系统用户的影响范围,可以将 ABE 属性撤销分为用户撤销、用户部分属性撤销和系统属性撤销三种情形[54]。其中,用户撤销即撤销该用户的所有属性,而不影响未撤销的其他用户;用户部分属性撤销即撤销该用户属性集合中的一些属性,撤销后该用户失去该属性所对应的权限,但不影响其他属性的权限;系统属性撤销即撤销具有该属性的所有用户的该属性权限。根据撤销执行者的不同,目前研究人员的工作方向主要有直接撤销和间接撤销两类。直接撤销由数据拥有者在加密明文时,直接列举出被撤销用户的信息,实现属性撤销。直接撤销与间接撤销相比,直接撤销方法的一个优点是,所有未撤销用户与授权中心无须在密钥更新阶段交互;然而,直接撤销方法的缺点是它需要数据所有者来管理当前的撤销列表,对于数据所有者来说这是一个烦扰的问题。间接撤销由授权机构周期性地更新未被撤销用户的密钥,并且只有未被撤销的用户才能更新密钥,然后通过更新的密钥解密新密文,而撤销用户无法接收到更新的密钥进而不能解密新密文。间接撤销方法的一个优点是数据所有者不需要知道撤销列表;然而,间接撤销方法的缺点是在密钥更新阶段,所有时间窗口中授权中心和未撤销用户需要通信。从不同方面对可撤销属性基加密分类情况如图 8 所示。

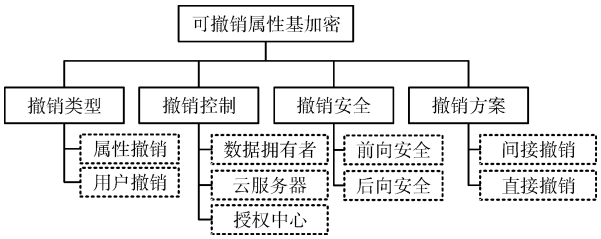

图 8 可撤销属性基加密分类

ABE 方案中,每一个属性可能被多个用户共享,所以用户撤销问题是难解决的。当撤销一个属性组中的任何属性或者一个用户时,将影响这个群组中的其他用户。这个问题是密钥更新过程的一个瓶颈,并且会成为 ABE 系统的安全威胁。

2006 年,Pirretti 等人[55]最先提出 ABE 属性撤销方案,其通过对每一个属性设定一个有效期,授权机构周期性地更新属性版本,通过撤销某个属性的最新版本以此达到用户属性撤销的目的。该方案中,由于授权中心密钥更新过程中的计算量与用户数据的多少成线性关系,所以效率不高。2008 年,Boldyreva 等人[56]提出一个有效撤销属性的 IBE 方案,它基于二叉树构建一个数据结构,但是这个方案不适用于 CP-ABE。

这种通过给每个属性设定时间周期来达到撤销目的的方法是一种粗粒度的撤销方案,其不能实现属性或用户的立即撤销。这种撤销方案主要有以下两个问题:a)前向安全(forward secrecy)和后向安全问题(backward secrecy)[57],其存在一个不受控制的时期被称为脆弱性窗口;b)可扩展性问题,授权中心需要通过单播方式在脆弱性窗口期发布一个密钥更新组件以确保所有未撤销用户能够更新他们的私钥,这可能是授权机构和所有未撤销用户的一个瓶颈。

为解决间接撤销所带来的问题,Ibraimi 和 Yu 等人[58,59]提出基于 CP-ABE 的立即属性撤销方案,但该方案没有实现数据的细粒度访问控制。2011 年,Hur 等人[60]提出一种具有属性和用户撤销能力的 CP-ABE 方案,该方案增强了用户访问控制的前向安全和后向安全,具有属性级别的属性撤销能力;同时当用户未及时更新私钥的情况下,仍可以通过一个二叉树解决这种状态丢失接收问题。2013 年,kan 等人[61]提出一种云存储环境下支持细粒度属性撤销的属性基加密方案,该方案无须服务器支持任何协作的访问控制,数据拥有者也无须实时在线,在效率方面较 Hur 等人[60]方案有所提高,但是该方案只是在随机预言机下证明其安全性。2013 年,Yang 等人[62]提出一种具有属性撤销能力的 CP-ABE 方案,该方案中授权中心需要更新密文并且产生新版本的密钥、更新密钥和私钥,无论如何,该方案中授权中心需要大量的计算资源。Zu 等人[63]提出一种云存储环境下具有有效撤销能力的 CP-ABE 方案,该方案中的访问结构是具有强表现能力的线性密钥共享方案。张维纬等人[64]提出了一种基于代理重加密技术的属性撤销 DRM 方案,该方案将复杂的解密运算部分外包给云服务商,减少了用户的解密负担,但是该方案没有给出具体的安全形式证明。Attrapadung 等人[65]第一个利用直接撤销和间接撤销的优势构建了一个具有混合撤销能力的 ABE 方案,该方案只支持用户级撤销而不支持属性撤销,并且该方案增加了用户私钥的长度。

2.6 叛徒可追踪性

在已有的 ABE 方案中,密钥滥用(key abuse)还是一个关键的、需要解决的问题。主要有两类密钥滥用问题:a)合谋用户间非法的密钥共享;b)半可信的属性机构非法的密钥分配。在属性基加密访问控制系统中,属性私钥直接意味着用户对于受保护的资源的访问能力。在当前的属性基加密方案中,都存在这样的密钥滥用问题,因为分配给用户的属性私钥只是与一般的共享用户属性相关联,不包括任何用户特有的信息。ABE 中的密钥滥用攻击可能阻碍它的广泛应用,尤其在版权敏感的系统中。因此,如何能够追踪泄露密钥的非法用户成为一个重要的研究内容。

Hinek 等人[66]第一次提出解决用户密钥滥用问题的方案,但是需要第三方来参与用户的解密操作,该方案在实际应用中缺乏合理性。Li 等人[67]关注于 CP-ABE 中的密钥滥用问题,提出具有可追踪性的 CP-ABE 来防止合谋用户之间的非法密钥共享。用户的可追踪性通过在分发给用户的属性私钥中嵌入附加的用户特有的信息来实现;半可信的属性机构的可追踪性通过使用用户的属性私钥中包含属性机构不知道的用户的秘密来实现。这些方法的关键点是把用户特有的信息或秘密作为另一个默认的属性。尽管 Li 等人[68]提出了这种解决方案,但是他们只是在匿名这样一个特定的应用中解决的用户可追踪性,当系统在云计算环境下使用时,还需要仔细考虑这个问题。Li 等人[68]通过使用叛逆者追踪实现了云计算环境下的用户可追踪性。Yu 等人[69]提出的 KP-ABE 方案可以做到当密钥滥用被检测到时,通过观察私有设备在某些特定输入下的输出来追踪非法的密钥分发者的 ID;之后,他们[70]实现了云计算环境下用户的可追踪性。Liu 等人[71]通过借鉴 Boneh 和 Boyen 的签名方案[72],构造了一个可追踪的 CP-ABE,不仅支持任意单调访问机构,且被证明是标准模型安全的。Liu 和 Ning 等人[73~75]对 CP-ABE 方案中的黑盒可追踪性、白盒可追踪性和支持无限属性域等方面进行了系统深入的研究,提出的方案可追踪泄露解密密钥的恶意用户,并且对恶意用户追踪的系统存储开销为常量级别。

3　未来研究方向

目前对属性基密码体制的研究虽然成果显著,但是由于理论上有一定的难度,所以还有许多问题有待进一步研究。下一步工作重点主要涉及到以下几个方面:

a)在隐藏访问结构机制方面,在增加访问结构的表现能力的基础上提高效率。用户的属性往往关系到用户的敏感信息,而这些敏感信息可能是一个人的身份证号、疾病信息,甚至是商业机密,因此隐藏访问结构至关重要。目前的研究方案中有的访问结构过于简单无法适用复杂情况,有的访问结构表现能力强,但是效率很低,实际应用还有一定难度。因此如何在增加访问结构表现能力的同时提高系统效率是一个重要问题。

b)在多授权机构机制方面,提高授权机构之间的通信效率。目前的多授权机构方案中,一种是存在一个可信的中央权威机构,该机构负责整个系统参数的生成和分发,另一种就是无中央权威机构方案。在无中央权威机构方案中,往往需要所有授权机构一起合作产生系统参数,这个过程是复杂的。因此如何协调各个授权中心产生系统参数值得研究。

c)在复杂计算安全外包机制方面,外包数据的可验证性依然是重点。复杂计算安全外包方案中,如何将加/解密及密钥产生都安全地提供给云服务商是一个值得深入研究的问题。如何确保这些外包数据的正确性,防止因为云服务商的"懒惰"行为而返回错误的结果至关重要。目前在这方面的研究已经很多,但是其大部分需要双加密系统,增加冗余组件来达到验证目的。因此设计一种高效的验证方案依然是重点。

d)在可搜索加密机制方面,支持模糊搜索(fuzzy search)、关系运算(>,<,=等)和搜索结果排序的搜索方案依然是未来需要研究的内容。现如今大部分搜索加密都是基于匹配搜索(equality search)、区间查询(range query)和子集查询(subset query),而关于模糊搜索、搜索结果排序方面的研究依然处于初始阶段,支持关系运算的效果也不够理想。所以在未来,研究支持模糊搜索、关系运算和搜索结果排序的搜索机制依然是一个重要内容。

e)在属性撤销机制方面,效率和安全依然是重中之重。授权中心需要产生每一个用户的私钥和其他方面的计算,大量用户频繁地改变自己的属性将占用授权中心大量的计算资源,因此如何避免密钥频繁地更新是一个重要的问题。权威中心产生用户私钥并通过安全通道分发给用户,因此如何设计一个公开信道传送私钥是一个值得深入研究的问题。

f)在叛徒可追踪性方面,密钥滥用问题比较严重,目前研究的大部分问题是如何追踪密钥泄露者。而在安全形势如此严峻的情况下,研究如何在部分密钥泄露的情况下仍能够保证系统的安全性是今后数据安全研究的重点。

4　结束语

属性基加密作为一种新型的密码方案,能够实现对数据的灵活细粒度访问控制,使得它可以广泛地应用于政治、军事、商业等诸多领域,尤其是属性基加密为解决云存储环境下数据的安全共享、细粒度访问控制和安全存储问题提供了一种解决思路。根据访问控制策略,属性基加密主要分为密钥策略、密文策略和混合策略。根据不同的功能扩展,详细介绍了属性基加密的相关研究工作,如隐藏访问结构、多授权机构、复杂计算安全外包、可搜索加密、撤销和叛徒追踪。最后总结了属性基加密现有研究工作的不足,并指出了未来的研究方向。

参考文献:

[1] Kale V. Guide to cloud computing for business and technology managers: from distributed computing to cloudware applications [M]. [S. l.]: CRC Press, 2014.

[2] Gartner: 2016 年超 36% 数字内容将存储至云端 [EB/OL]. (2013-07-16). https://club. 1688. com/article/32280571. htm.

[3] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.

[4] 张鹏飞. 云存储的数据安全问题研究[J]. 科学导报, 2016(6).

[5] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing [J]. Journal of Network and Computer Applications, 2011, 34(1): 1-11.

[6] Pearson S. Taking account of privacy when designing cloud computing services [C]//Proc of ICSE Workshop on Software Engineering Challenges of Cloud Computing. Washington DC: IEEE Computer Society, 2009: 44-52.

[7] Sahai A, Waters B. Fuzzy identity-based encryption [C]//Proc of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457-473.

[8] Kamara S, Lauter K. Cryptographic cloud storage [C]//Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2010: 136-149.

[9] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [C]//Proc of Annual International Cryptology Conference. Berlin: Springer, 2001: 213-229.

[10] Goyal V, Pandey O, Sahai A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data [C]//Proc of the 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006: 89-98.

[11] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2007: 321-334.

[12] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures [C]//Proc of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 195-203.

[13] Zheng Yao. Key-policy attribute-based encryption scheme implementation [EB/OL]. (2012). http://www. cnsr. ictas. vt. edu/resources. html.

[14] Cheung L, Newport C. Provably secure ciphertext policy ABE [C]//Proc of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 456-465.

[15] Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C]//Proc of International Workshop on Public Key Cryptography. Berlin: Springer, 2011: 53-70.

[16] Lewko A, Okamoto T, Sahai A, *et al*. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption [C]//Proc of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 62-91.

[17] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption [C]//Proc of Annual Cryptology Conference. Berlin: Springer, 2010: 191-208.

[18] Lewko A, Waters B. New proof methods for attribute-based encryption: achieving full security through selective techniques [C]//Proc of the 32nd Annual Cryptology Conference. Berlin: Springer, 2012: 180-198.

[19] Attrapadung N, Imai H. Dual-policy attribute based encryption: simultaneous access control with ciphertext and key policies [J]. IEICE Trans on Fundamentals of Electronics Communications &

Computer Sciences, 2010, 93-A(1): 116-125.
[20] Miyaji A, Tran P V X. Constant-ciphertext-size dual policy attribute based encryption [C]//Proc of International Conference on Cyberspace Safety and Security. Berlin: Springer, 2012: 400-413.
[21] Rao Y S, Dutta R. Computationally efficient dual-policy attribute based encryption with short ciphertext [C]//Proc of the 7th International Conference on Provable Security. New York: Springer-Verlag, 2013: 288-308.
[22] Kapadia A, Tsang P P, Smith S W. Attribute-based publishing with hidden credentials and hidden policies [C]//Proc of Network and Distributed System Security Symposium. 2007: 179-192.
[23] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [C]//Proc of International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2008: 111-129.
[24] Yu Shucheng, Ren Kui, Lou Wenjing. Attribute-based content distribution with hidden policy [C]//Proc of the 4th Workshop on Secure Network Protocols. Washington DC: IEEE Computer Society, 2008: 39-44.
[25] Li Jin, Ren Kui, Zhu Bo, *et al.* Privacy-aware attribute-based encryption with user accountability [C]//Proc of International Conference on Information Security. Berlin: Springer, 2009: 347-362.
[26] Lai Junzuo, Deng R H, Li Yingjiu. Fully secure cipertext-policy hiding CP-ABE [C]//Proc of International Conference on Information Security Practice and Experience. Berlin: Springer, 2011: 24-39.
[27] 王海斌, 陈少真. 隐藏访问结构的基于属性加密方案 [J]. 电子与信息学报, 2012, 34(2): 457-461.
[28] Lai Junzuo, Deng R H, Li Yingliu. Expressive CP-ABE with partially hidden access structures [C]//Proc of the 7th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2012: 18-19.
[29] Hur J. Attribute-based secure data sharing with hidden policies in smart grid [J]. IEEE Trans on Parallel and Distributed Systems, 2013, 24(11): 2171-2180.
[30] 宋衍, 韩臻, 刘凤梅, 等. 基于访问树的策略隐藏属性加密方案 [J]. 通信学报, 2015, 36(9): 119-126.
[31] 唐强, 姬东耀. 多授权中心可验证的基于属性的加密方案 [J]. 武汉大学学报:理学版, 2008, 54(5): 607-610.
[32] Chase M. Multi-authority attribute based encryption [C]//Proc of Theory of Cryptography Conference. Berlin: Springer, 2007: 515-534.
[33] Chase M, Chow S S M. Improving privacy and security in multi-authority attribute-based encryption [C]//Proc of the 16th ACM Conference on Computer and Communications Security. New York: ACM Press, 2009: 121-130.
[34] Liu Zhen, Cao Zhenfu, Huang Qiong, *et al.* Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles [C]//Proc of the 16th European Symposium on Research in Computer Security. Berlin: Springer, 2011: 278-297.
[35] Lewko A, Waters B. Decentralizing attribute-based encryption [C]//Proc of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 568-588.
[36] Rouselakis Y, Waters B. Efficient statically-secure large-universe multi-authority attribute-based encryption [C]//Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 315-332.
[37] 王皓, 郑志华, 吴磊, 等. 自适应安全的外包 CP-ABE 方案研究 [J]. 计算机研究与发展, 2015, 52(10): 2270-2280.
[38] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C]//Proc of the 20th USENIX Conference on Security. Berkeley: USENIX Association, 2011: 34.
[39] Zhou Zhibin, Huang Dijiang. Efficient and secure data storage operations for mobile cloud computing [C]//Proc of the 8th International Conference on Network and Service Management. Laxenburg: International Federation for Information Processing, 2012: 37-45.
[40] Li Jingwei, Jia Chunfu, Li Jin, *et al.* Outsourcing encryption of attribute-based encryption with MapReduce [C]//Proc of the 14th International Conference on Information and Communications Security. Berlin: Springer, 2012: 191-201.
[41] Lai Junzuo, Deng R H, Guan Chaowen, *et al.* Attribute-based encryption with verifiable outsourced decryption [J]. IEEE Trans on Information Forensics and Security, 2013, 8(8): 1343-1354.
[42] Li Jin, Huang Xinyi, Li Jingwei, *et al.* Securely outsourcing attribute-based encryption with checkability[J]. IEEE Trans on Parallel and Distributed Systems, 2014, 25(8): 2201-2210.
[43] Hohenberger S, Waters B. Online/offline attribute-based encryption [C]//Proc of International Workshop on Public Key Cryptography. Berlin: Springer, 2014: 293-310.
[44] 沈志荣, 薛巍, 舒继武. 可搜索加密机制研究与进展 [J]. 软件学报, 2014, 25(4): 880-895.
[45] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data [C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2000: 44-55.
[46] Boneh D, Di Crescenzo G, Ostrovsky R, *et al.* Public key encryption with keyword search [C]//Proc of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 506-522.
[47] Zhao Fangming, Nishide T, Sakurai K. Multi-user keyword search scheme for secure data sharing with fine-grained access control [C]//Proc of International Conference on Information Security and Cryptology. Berlin: Springer, 2011: 406-418.
[48] Cao Ning, Wang Cong, Li Ming, *et al.* Privacy-preserving multi-keyword ranked search over encrypted cloud data [J]. IEEE Trans on Parallel and Distributed Systems, 2014, 25(1): 222-233.
[49] 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.
[50] Han Fei, Qin Jing, Zhao Huawei, *et al.* A general transformation from KP-ABE to searchable encryption [J]. Future Generation Computer Systems, 2014, 30(1): 107-115.
[51] Zheng Qingji, Xu Shouhuai, Ateniese G. VABKS: verifiable attribute-based keyword search over outsourced encrypted data [C]//Proc of IEEE INFOCOM. 2014: 522-530.
[52] Li Ruixuan, Xu Zhiyong, Kang Wanshang, *et al.* Efficient multi-keyword ranked query over encrypted data in cloud computing [J]. Future Generation Computer Systems, 2014, 30(1): 179-190.
[53] Revathy B D, Anbumani A, Ravishankar M P. Enabling secure and efficient keyword ranked search over encrypted data in the cloud [J]. International Journal of Recent Advances in Science & Engineering, 2015, 1(1): 28-32.
[54] 李勇, 曾振宇, 张晓菲. 支持属性撤销的外包解密方案 [J]. 清华大学学报: 自然科学版, 2013, 53(12): 1664-1669.
[55] Pirretti M, Traynor P, McDaniel P, *et al.* Secure attribute-based systems [C]//Proc of the 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006, 99-112.
[56] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation [C]//Proc of the 15th ACM Conference on Computer and Communications Security. New York: ACM Press, 2008: 417-426.
[57] Rafaeli S, Hutchison D. A survey of key management for secure group communication [J]. ACM Computing Surveys, 2003, 35(3): 309-329.
[58] Ibraimi L, Petkovic M, Nikova S, *et al.* Mediated ciphertext-policy attribute-based encryption and its application [C]//Proc of International Workshop on Information Security Applications. Berlin: Springer, 2009: 309-323.
(下转第973页)

tual machines [C]//Proc of ACM Symposium on Applied Computing. 2010: 173-180.

[30] Keller E, Szefer J, Rexford J, *et al.* NoHype: virtualized cloud infrastructure without the virtualization [J]. ACM SIGARCH Computer Architecture News, 2010, 38(3): 350-361.

[31] Martin R, Demme J, Sethumadhavan S. TimeWarp: rethinking timekeeping and performance monitoring mechanisms to mitigate side-channel attacks [C]//Proc of the 39th Annual International Symposium on Computer Architecture. 2012: 118-129.

[32] Yu Si, Gui Xiaolin, Tian Feng, *et al.* A security-awareness virtual machine placement scheme in the cloud [C]//Proc of IEEE International Conference on Embedded and Ubiquitous Computing. 2013: 1078-1083.

[33] Raj H, Nathuji R, Singh A, *et al.* Resource management for isolation enhanced cloud services [C]//Proc of ACM Workshop on Cloud Computing Security. New York: ACM Press, 2009: 77-84.

[34] Zhang Yinqian, Juels A, Oprea A, *et al.* HomeAlone: co-residency detection in the cloud via side-channel analysis [C]//Proc of IEEE Symposium on Security & Privacy. 2011: 313-328.

[35] Domnitser L, Jaleel A, Loew J, *et al.* Non-monopolizable caches: low-complexity mitigation of cache side channel attacks [J]. ACM Trans on Architecture & Code Optimization, 2012, 8(4): 146-149.

[36] Wang Zhenghong, Lee R B. Covert and side channels due to processor architecture [C]//Proc of the 22nd Annual Computer Security Applications Conference. Washington DC: IEEE Computer Society, 2006: 473-482.

[37] Wang Zhenghong, Lee R B. New cache designs for thwarting software cache-based side channel attacks [J]. ACM SIGARCH Computer Architecture News, 2007, 35(2): 494-505.

[38] Kong Jingfei, Aciicmez O, Seifert J P, *et al.* Deconstructing new cache designs for thwarting software cache-based side channel attacks [C]//Proc of the 2nd ACM Workshop on Computer Security Architectures. New York: ACM Press, 2008: 25-34.

[39] Kong Jingfei, Aciicmez O, Seifert J P, *et al.* Hardware-software integrated approaches to defend against software cache-based side channel attacks [C]//Proc of the 15th International Symposium on High Performance Computer Architecture. 2009: 393-404.

[40] Wang Zhenghong, Lee R B. A novel cache architecture with enhanced performance and security [C]//Proc of the 41st IEEE/ACM International Symposium on Microarchitecture. Washington DC: IEEE Computer Society, 2008: 83-93.

[41] Godfrey M, Zulkernine M. Preventing cache-based side-channel attacks in a cloud environment [J]. IEEE Trans on Cloud Computing, 2014, 2(4): 395-408.

[42] Pattuk E, Kantarcioglu M, Lin Zhiqiang, *et al.* Preventing cryptographic key leakage in cloud virtual machines [C]//Proc of the 23rd USENIX Security Symposium. Berkeley: USENIX Association, 2014: 703-718.

[43] Erlingssonú, Abadi M. Operating system protection against side-channel attacks that exploit memory latency, MSR-TR-2007-117 [R]. 2007.

[44] Han Yi, Chan J, Alpcan T, *et al.* Virtual machine allocation policies against co-resident attacks in cloud computing [C]//Proc of IEEE International Conference on Communications. 2014.

[45] Varadarajan V, Ristenpart T, Swift M. Scheduler-based defenses against cross-VM side-channels [C]//Proc of the 23rd USENIX Conference on Security. Berkeley: USENIX Association, 2014: 687-702.

[46] Ali M, Khan S U, Vasilakos A V. Security in cloud computing: opportunities and challenges [J]. Information Sciences, 2015, 305(6): 357-383.

(上接第 968 页)

[59] Yu Shucheng, Wang Cong, Ren Kui, *et al.* Attribute based data sharing with attribute revocation [C]//Proc of the 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2010: 261-270.

[60] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Trans on Parallel and Distributed Systems, 2011, 22(7): 1214-1221.

[61] Kan Yang, Jia Xiaohua, Ren Kui. Attribute-based fine-grained access control with efficient revocation in cloud storage systems [C]// Proc of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. New York: ACM Press, 2013: 523-528.

[62] Yang Kan, Jia Xiaohua. Security for cloud storage systems [M]. New York: Springer-Verlag, 2013.

[63] Zu Longhui, Liu Zhenhua, Li Juanjuan. New ciphertext-policy attribute-based encryption with efficient revocation [C]//Proc of IEEE International Conference on Computer and Information Technology. Washington DC: IEEE Computer Society, 2014: 281-287.

[64] 张维纬, 冯桂, 刘建毅, 等. 云计算环境下支持属性撤销的外包解密 DRM 方案 [J]. 计算机研究与发展, 2015, 52(12): 2659-2668.

[65] Attrapadung N, Imai H. Attribute-based encryption supporting direct//indirect revocation modes [C]//Proc of IMA International Conference on Cryptography and Coding. Berlin: Springer, 2009: 278-300.

[66] Hinek M J, Jiang Shaoquan, Safavi-Naini R, *et al.* Attribute-based encryption with key cloning protection [EB/OL]. (2008-11-09). https://eprint.iacr.org/2008/478.pdf.

[67] Li Jin, Ren Kui, Kim K. A^2BE: accountable attribute-based encryption for abuse free access control [EB/OL]. (2009-04-14). https://eprint.iacr.org/2009/118.pdf.

[68] Li Jin, Zhao Gansen, Chen Xiaofeng, *et al.* Fine-grained data access control systems with user accountability in cloud computing [C]// Proc of the 2nd International Conference on Cloud Computing Technology and Science. Washington DC: IEEE Computer Society, 2010: 89-96.

[69] Yu Shucheng, Ren Kui, Lou Wenjing, *et al.* Defending against key abuse attacks in KP-ABE enabled broadcast systems [C]//Proc of International Conference on Security and Privacy in Communication Systems. Berlin: Springer, 2009: 311-329.

[70] Yu Shucheng, Wang Cong, Ren Kui, *et al.* Achieving secure, scalable, and fine-grained data access control in cloud computing [C]// Proc of the 29th Conference on Information Communications. Piscataway: IEEE Press, 2010: 534-542.

[71] Liu Zhen, Cao Zhenfu, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures [J]. IEEE Trans on Information Forensics and Security, 2013, 8(1): 76-88.

[72] Boneh D, Boyen X. Short signatures without random oracles [C]// Proc of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 56-73.

[73] Liu Zhen, Cao Zhenfu, Wong D S. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on eBay [C]//Proc of ACM SIGSAC Conference on Computer & Communications Security. New York: ACM Press, 2013: 475-486.

[74] Liu Zhen, Cao Zhenfu, Wong D S. Traceable CP-ABE: how to trace decryption devices found in the wild [J]. IEEE Trans on Information Forensics and Security, 2015, 10(1): 55-68.

[75] Ning Jianting, Dong Xiaolei, Cao Zhenfu, *et al.* White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes[J]. IEEE Trans on Information Forensics and Security, 2015, 10(6): 1274-1288.