计算机科学
COMPUTER SCIENCE

基于属性的可搜索加密综述

严莉, 殷田, 刘培顺, 冯洪新, 王高洲, 张闻彬, 呼海林, 潘法定

引用本文

严莉, 殷田, 刘培顺, 冯洪新, 王高洲, 张闻彬, 呼海林, 潘法定. 基于属性的可搜索加密综述[J]. 计算机科学, 2024, 51(11A): 231100137-12.

YAN Li, YIN Tian, LIU Peishun, FENG Hongxin, WANG Gaozhou, ZHANG Wenbin, HU Hailin, PAN Fading. Overview of Attribute-based Searchable Encryption[J]. Computer Science, 2024, 51(11A): 231100137-12.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231100137

基于属性的可搜索加密综述

严　莉[1]　殷　田[2]　刘培顺[2]　冯洪新[2]　王高洲[1]　张闻彬[1]　呼海林[1]　潘法定[1]
1　国网山东省电力公司信息通信公司　济南 250013
2　中国海洋大学信息科学与工程学部　山东 青岛 266400
(617498012@qq.com)

摘　要　随着大数据时代的到来,数据规模和复杂性持续增加,对数据隐私和安全保障的需求也日益迫切。然而,传统的加密方法无法满足在大规模数据集中进行高效搜索的需求。为了解决这一问题,可搜索加密技术引入了陷门函数和其他密码学技术,使得无需解密整个数据集即可在加密的数据中进行搜索。然而,单独采用可搜索加密仍无法满足现实世界中复杂的数据访问控制需求。因此,研究人员将属性基加密的概念引入可搜索加密,从而实现了属性基可搜索加密体制,旨在实现在加密的数据集合中按属性进行高效搜索的功能。属性基可搜索加密在隐私保护、数据共享和云计算等领域具有广泛的应用前景,从隐私保护增强、计算效率提升以及灵活性增强3个方面对其发展趋势进行了阐述,并介绍了涉及到的相关方案。在隐私保护增强方面,主要讨论了策略隐藏技术、权限管理技术以及安全性增强技术;针对效率优化的方案主要涉及外包计算、在线/离线加密机制以及索引结构优化等。同时,在灵活增强方面讨论了属性基可搜索加密在访问策略表达能力和搜索能力方面的提升。此外,还介绍了几个常见的应用领域,并总结了研究人员提出的相关方案。最后,讨论了属性基可搜索加密面临的挑战以及未来方向。

关键词:基于属性的加密;可搜索加密;属性基可搜索加密;隐私保护;数据共享;云计算
中图分类号　TP309

Overview of Attribute-based Searchable Encryption

YAN Li[1],YIN Tian[2],LIU Peishun[2],FENG Hongxin[2],WANG Gaozhou[1],ZHANG Wenbin[1],HU Hailin[1] and PAN Fading[1]
1 Information and Telecommunication Company,State Grid Shandong Electric Power Company,Jinan 250013,China
2 Faculty of Information Science and Engineering,Ocean University of China,Qingdao,Shandong 266400,China

Abstract　With the advent of the big data era,the size and complexity of data continue to increase,which makes the requirement for data privacy and security increasingly urgent. However,traditional encryption methods cannot meet the demand for efficient searching in large-scale datasets. To address this problem,searchable encryption introduces trapdoor functions and other cryptographic techniques that allow searching in encrypted data without decrypting the entire dataset. However,searchable encryption alone still cannot meet the complex data access control needs in the real world. Therefore,researchers have introduced the concept of attribute-based encryption into searchable encryption,resulting in attribute-based searchable encryption. This approach aims to achieve efficient search by attributes in encrypted data sets. Attribute-based searchable encryption has a wide range of applications in the fields of privacy protection,data sharing and cloud computing. In this paper,we describe the development trends in terms of enhancing privacy protection,improving computational efficiency,and increasing flexibility. We also present the related schemes involved. In terms of enhancing privacy protection,we discusstechniques such as policy hiding,permission management,and security enhancement. The current methods for optimizing efficiency primarily involve outsourcing computation,online/offline encryption mechanisms,and index structure optimization,among others. Additionally,the improvement of the attribute-based searchable encryption scheme in terms of access policy expression ability and search capability is discussed. In addition,this paper introduces several common application areas and summarizes the relevant schemes proposed by researchers. In addition,it discusses the challenges and future directions of attribute-based searchable encryption.

Keywords　Attribute-based encryption,Searchable encryption,Attribute-based searchable encryption,Privacy preservation,Data sharing,Cloud computing

1　引言

在云计算和大数据环境下,越来越多企业和用户将大量数据上传到云服务器,而云计算中的数据和资源依赖不可靠的网络通信和半可信的云存储服务[1]。为了保护数据安全,目前有效的做法是数据拥有者将数据进行加密后上传服务器,在需要时由数据使用者解密。

为使数据使用者拥有对云存储中密文的控制权,即在不

基金项目:国网山东省电力公司科技项目(520627230004)
This work was supported by the State Grid Shandong Electric Power Company Technology Project(520627230004).
通信作者:殷田(yintian@stu.ouc.edu.cn)

解密密文的情况下仍可以搜索密文，可搜索加密（Searchable Encryption，SE）技术应运而生。如 Song 等[2]提出了使用对称加密体制实现的可搜索加密（Searchable Symmetric Encryption，SSE）方案，以及 Boneh 等[3]提出的关键字搜索公钥加密（Public Key Encryption with Keyword Search，PEKS）方案。但是基于传统的加密方法，如公钥加密体制和对称密码体制，无法实现多用户设置中的细粒度访问控制。

基于属性的加密（Attribute-Based Encryption，ABE）机制解决了上述问题。ABE 提供细粒度的访问控制策略，支持在半可信的云存储上安全地存储数据。ABE 思想源于基于身份的加密（Identity-Based Encryption，IBE）方案，ABE 的前身是 Sahai 等[4]提出的模糊的基于身份的加密（Identity-Free Binary Encryption，FIBE）方案。此后，Goyal 等[5]在 FIBE 的基础上提出了基于密钥策略属性加密（Key-Policy Attribute-Based Encryption，KP-ABE）方案，Bethencourt 等[6]提出了基于密文策略属性加密（Ciphertext-Policy Attribute-Based Encryption，CP-ABE）方案，这两种方案普遍被认为是 ABE 的两大基本机制。

为了在保证数据安全性和隐私性的同时实现高效搜索和访问控制机制，一些研究人员结合属性基加密的思想提出了基于属性的可搜索加密方案。如 Khader[7]提出了基于属性加密的可搜索加密（Attribute-Based Searchable Encryption，ABSE），这是一种结合了 ABE 思想的 PKSE 方案。Zheng 等[8]提出了基于属性的关键字搜索（Attribute-Based Keyword Search，ABKS）。其中，属性加密机制保证了数据拥有者能够指定访问控制策略，为满足属性要求的数据使用者提供解密和搜索密文的权限；可搜索加密技术实现了对密文数据的检索。

文章综述了 ABSE 近年的发展进程，主要贡献有：

1）简要介绍了 ABE，SE 以及 ABSE；

2）将从安全性增强、计算效率提升、灵活性增强 3 个方面详细介绍 ABSE 的发展趋势和进程；

3）总结了 ABSE 常见的应用领域，如智能电网、医疗健康、物联网以及移动应用，并整理了相关方案；

4）讨论了 ABSE 可能面临的挑战和未来的发展方向。

本文第 2－4 章简单回顾了 ABE，SE 以及 ABSE；第 5 章介绍属性基可搜索加密的发展趋势和进程；第 6 章介绍常见的应用以及相关的实现；最后总结全文并展望未来。

2 属性基加密

2.1 属性基加密简介

ABE 的概念是由 Sahai 和 Waters[4]在 2005 年实现 FIBE 中首次提出，所以 FIBE 也被视为是 ABE 系统的前身。在 ABE 系统中，访问策略与密文相关联，用户属性与私钥相关联。只有满足数据访问策略的用户，其私钥才能与密文相匹配，从而成功解密数据。

2006 年，Goyal 等[5]在 Sahai 的基础上正式提出了 ABE 概念，将其分为 KP-ABE 和 CP-ABE，并给出了 KP-ABE 方案的构造；次年，Bethencourt 等[6]实现了 CP-ABE 方案。ABE 提供灵活且细粒度的访问控制机制，允许数据在加密的状态下共享，即在保护数据安全的同时完成数据共享，并且用户使用属性进行解密无需公开自己的身份信息，可以有效地保护用户隐私。随着研究人员对 ABE 探索的深入，在功能和安全性等方面都出现了更多的扩展。2011 年，Waters[9]使用 LSSS 设计了更具表达性的 ABE 方案，但以上方案只满足了选择身份的安全性；2012 年，Lewko 等[10]使用对偶系统加密实现了完全安全的 ABE 方案。

基本的 ABE 体制是由 3 个参与方协作完成，包括发送方、授权机构和接收方；通常由 4 个算法组成，包括初始化算法、密钥生成算法、加密算法和解密算法（Setup，KeyGen，Encrypt，Decrypt）。授权机构执行 Setup 算法生成系统主密钥和公钥，并执行 KeyGen 算法生成用户的属性私钥。发送方执行 Encrypt 算法加密数据。当用户请求访问数据时，需提供其用户密钥以验证用户属性是否满足访问策略，当且仅当属性匹配成功时，接收方执行 Decrypt 算法解密消息。基于属性的加密流程如图 1 所示。

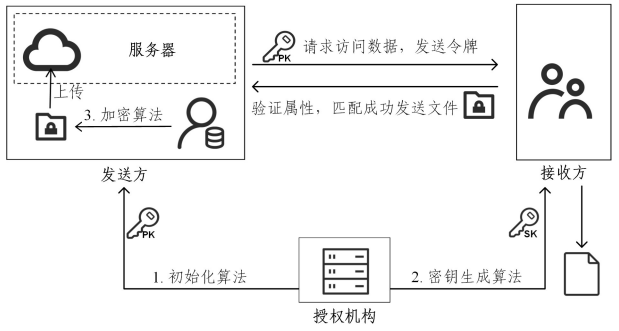

图 1 基于属性的加密流程

Fig. 1 ABE process

2.2 属性基加密分类

为了更灵活地表达访问控制策略，ABE 被分为 CP-ABE 和 KP-ABE。

在 CP-ABE 中，接收方的私钥将与属性相关联，在加密消息时，发送方将指定一个与属性相关的访问策略，只有在用户的属性与访问策略匹配时才可以解密密文，这种设计更加接近现实场景；而在 KP-ABE 中，密文对应一个属性集合，而接收者的私钥与一个访问结构相关联。由于 CP-ABE 和 KP-ABE 有不同的性质，它们也适应于不同的场景。CP-ABE 允许数据拥有者定义复杂的访问策略，因此适合应用在多个用户之间共享数据的场景，如云计算环境和跨组织数据共享等；CP-ABE 提供了细粒度访问控制机制，因此适用于需要精确控制数据访问权限的场景，例如敏感数据的访问控制、个性化数据访问等。KP-ABE 支持多级访问控制，适用于需要实现多级访问控制的场景，例如分层管理权限和多级数据分类等；KP-ABE 可用于在云计算环境中对数据进行加密和访问控制，确保只有授权的用户能够解密和处理数据。KP-ABE 和 CP-ABE 的对比如表 1 所列。

表 1 CP-ABE 和 KP-ABE 的对比

Table 1 Comparison between CP-ABE and KP-ABE

机制	CP-ABE	KP-ABE
属性集合相关	用户密钥	密文
访问策略相关	密文	用户密钥
灵活性	支持复杂的访问策略	针对特定密钥的访问策略
应用场景	多用户共享数据、精确的访问控制	文件级访问控制、多级访问控制

当然，CP-ABE 和 KP-ABE 也可以结合使用，以实现更加复杂的访问控制策略和数据共享方案。

3　可搜索加密

3.1　可搜索加密简介

2000 年,Song 等[2]首次提出了 SE 的概念。可搜索加密协议是具有密文搜索功能的加密系统,它能够在保证数据加密的基础上提供关键词检索能力,并只返回与其搜索条件匹配的结果。但其使用对称加密进行实现,只允许拥有私钥的用户进行加密和搜索。2004 年,Boneh 等[3]提出基于公钥加密的关键词搜索模型,提高了数据和身份的安全性。后来,研究人员对可搜索加密的功能、效率和安全性方面都进行了研究和完善。

可搜索加密协议通常由 3 个参与方协作完成,包括数据所有者、服务器以及数据使用者。可搜索加密方案通常由 4 种基本算法构成,包括加密算法(Encrypt)、陷门生成算法(Trapdoor)、陷门匹配算法(Decrypt)和解密算法。数据所有者运行 Encrypt 算法对数据进行加密,并上传到服务器中;数据使用者运行 Trapdoor 算法,利用公钥和搜索关键字生成陷门数据,发送给服务器;服务器运行 Search 算法,并将匹配到的数据返回给数据使用者;数据使用者运行 Decrypt 算法进行解密。在使用公钥体制的可搜索加密中,还需要 KeyGen 算法分配公钥和私钥对。可搜索加密流程如图 2 所示。

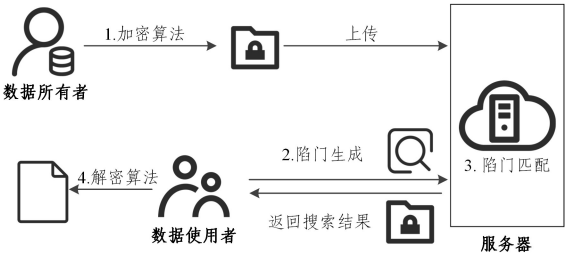

图 2　可搜索加密流程

Fig. 2　SE process

3.2　可搜索加密分类

可搜索加密可以根据不同的特性和功能进行不同的分类,但是最常见的是基于加密方案将其分为 SSE 和 PEKS。SSE 使用对称加密机制对数据进行加密和搜索操作,其搜索操作具有高效性和简单性,但需要对对称密钥进行安全分发和管理。PEKS 使用公钥加密算法对数据进行加密和搜索操作,通过使用公钥和私钥对的方式克服了对称可搜索加密中密钥分发和管理的问题,但是其搜索操作更加复杂且耗时。

SSE 和 PEKS 由于特点不同,因此适用于不同的场景。SSE 的加密和搜索操作使用相同的对称密钥,避免了密钥切换和复杂的加密计算,使之具有高效性和实时响应的特点。相对于 PEKS,SSE 使用的对称密钥较短,密钥分发和管理较为简单,不需要复杂的密钥管理系统,但是加密和构建索引都是由数据所有者操作,所以要求数据所有者是可信任的。基于以上特点,SSE 适合应用于云搜索、云计算、数据传输、物联网和搜索引擎等场景。PEKS 分离了加密和解密密钥,并且索引构建的过程更加安全,数据拥有者不需要完全可信,其安全性高于 SSE,并且适用于分布式环境下的数据共享和搜索需求。因此,PEKS 适用于多租户环境、云环境、外包计算和医疗保健领域等。SSE 和 PEKS 的对比如表 2 所列。

表 2　SSE 和 PEKS 的对比

Table 2　Comparison between SSE and PEKS

机制	SSE	PEKS
加密技术	对称加密技术	非对称加密技术
额外的安全通道	需要(共享密钥)	不需要
处理速度	快(加解密使用相同的密钥)	慢(加解密使用不同的密钥)
密钥管理	使用对称密钥进行加解密	使用公钥生成关键词密文,使用私钥生成关键词陷门
应用场景	云搜索和云计算、数据传输、物联网和搜索引擎	多租户环境、云环境和外包计算和医疗保健领域

4　属性基可搜索加密

4.1　属性基可搜索加密简介

ABSE 是允许基于数据属性进行数据加密的可搜索加密方案,主要解决了数据隐私保护和数据搜索功能之间的平衡问题,能够在保证数据安全性和隐私性的同时实现高效搜索和访问控制机制。ABSE 与 SE 和 ABE 密切相关但又有所不同,表 3 列出了 SE,ABE 和 ABSE 在搜索操作、访问控制和数据可见性的异同点。

表 3　SE,ABE 和 ABSE 的对比

Table 3　Comparison between SE,ABE and ABSE

技术	搜索操作	访问控制	数据可见性
SE	√	×	满足搜索条件
ABE	×	√	满足访问策略
ABSE	√	√	同时满足搜索查询和访问策略

ABSE 主要分为两类:Key-policy ABSE(KP-ABSE)和 Ciphertext policy ABSE(CP-ABSE)。这两种策略主要在密钥生成和加密过程存在差异,提供了不同的灵活性和控制方法,以满足不同的安全需求和访问控制需求。在 CP-ABSE 中,密钥与一组属性相关联,文档和索引基于访问策略进行加密。在 KP-ABSE 中,密钥与访问策略相关,文档和索引使用一组属性进行加密。

4.2　属性基可搜索算法模型

ABSE 通常包含 4 种类型的实体:数据所有者(Data Owner,DO)、数据使用者(Data User,DU)、服务器(Cloud Server,CS)、可信第三方(Trusted Application,TA)。TA 初始化系统并为 DO 和 DU 生成公钥或密钥对;DO 加密文件,建立安全索引,并将密文上传到 CS;DU 可以搜索加密文件,并且在获得授权的情况下访问加密文件;CS 提供多种服务,包括数据存储、计算、检索等。当 DU 提交被加密文件的关键字生成的搜索令牌进行查询时,CS 将搜索令牌与索引进行匹配,并向 DU 返回相应的搜索结果。属性基可搜索加密流程如图 3 所示。

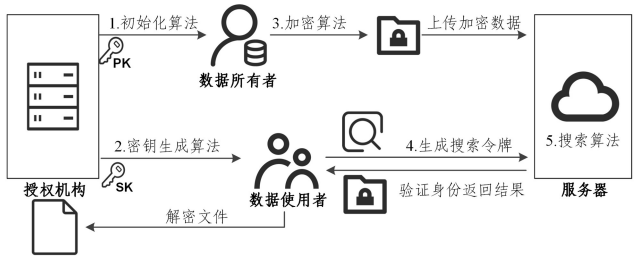

图 3　属性基可搜索加密流程

Fig. 3　ABSE process

一个基于属性的可搜索加密机制通常由 5 个概率多项式

时间的算法组成：

1) $Setup(\lambda, U) \rightarrow (PK, MK)$：TA 执行该算法。输入安全参数 λ 和属性集合 U，输出公共参数 PK 和主密钥 MK。

2) $KeyGen(PK, MK, S) \rightarrow sk$：TA 执行该算法。输入 PK，MK 和用户属性 S，为用户输出密钥 sk。

3) $Enc(W, P) \rightarrow C_W$：DO 执行该算法。输入关键字集 W 和访问策略 P，使用访问策略 P 对关键字集 W 进行加密，以获得密文 C_W。

4) $Trapdoor(sk, \omega) \rightarrow T_\omega$：DU 执行该算法。算法根据 sk 和关键字 ω 生成搜索陷门 T_ω。

5) $Query(C_W, T_\omega) \rightarrow (0, 1)$：CS 执行该算法。如果索引中的关键字和陷门的关键字相匹配，则该算法返回 1，否则返回 0。

接下来将介绍 ABSE 在安全性、计算效率以及灵活性方面的发展进程。

5 发展趋势和进展

ABSE 作为一种关键的隐私保护技术，持续受到学者们的关注。目前对 ABSE 机制的拓展主要集中在安全性增强、搜索效率提升、灵活性增强等方面，以满足日益增长的数据隐私保护和计算成本需求。

5.1 安全能力增强

ABSE 机制旨在保护用户的隐私，确保在加密数据上进行搜索操作时，不会泄露关键信息。近年来，研究人员提出了更加安全的 ABSE 方案。以下技术常被用于提高 ABSE 系统安全性。

表 4 中对近些年一些经典 ABSE 系统的安全能力进行了对比。

表 4 搜索能力和安全性的对比

Table 4 Comparison of search capability and security

系统	搜索能力	可追踪性	可撤销性	搜索效率	安全性
[48]	●	×	×	×	CKA
[77]	●	×	√	外包计算	CKA/ CPA
[45]	○	√	√	外包解密	CPA/ CKA
[55]	○	×	×	分布式索引	KGA/CKA
[49]	●	×	×	外包解密	CKA\ CPA
[34]	●	√	√	边缘计算	CKA\ CPA
[74]	○	×	×	倒排索引	适应性安全
[21]	○	×	×	×	IND-CKA
[50]	●	×	×	×	IND-CKA\ CCA
[69]	●	×	×	在线/离线机制	IND-CKA
[58]	○	×	×	×	IND-RCCA
[52]	●	×	×	×	IND-CKA
[51]	○	×	×	边缘计算	CKA

注：○表示只支持单关键字搜索，●表示支持多关键字搜索。

5.1.1 策略隐藏

最初提出的 CP-ABE 方案中，访问策略以明文形式嵌入数据密文，任何获得数据密文的人，不管其是否具有解密权限，都可以得到访问策略的内容[11]。攻击者可以通过访问策略获取相关信息，这可能导致隐私泄露和潜在的身份盗窃。因此，策略隐藏技术是隐私保护的重要手段之一。

策略隐藏主要分为两类，分别是部分策略隐藏和完全策略隐藏。部分策略隐藏主要有通配符替代法和属性名与属性值分割等方案，完全策略隐藏主要采用内积谓词加密机制(Inner Product Encryption，IPE)。

2008 年，Nishide 等[12]提出了部分策略隐藏概念，并使用通配符替代法给出了方案实现，但其只能支持“与”门结构，并且只能验证随机预测模型。2011 年，Lai 等[13]在 Nishide 等[12]的基础上做出改进，使用 IPE 机制实现了一种完全策略隐藏 CP-ABE 方案，但是该方案依然只支持“与”门的访问控制结构，且密文的长度会随着访问控制策略中属性的数量线性递增。2010 年，Balu 等[14]提出了一种基于访问控制树的完全策略隐藏 ABE 方案，但在访问控制策略较为复杂时容易出现迭代层数过多等问题。2012 年，Lai 等[15]将每个属性划分为属性名称及其值两部分，通过将两者分离实现访问策略的部分隐藏，这是首次提出基于 LSSS 访问结构的自适应安全的部分策略隐藏方案。此类方案虽给出了其安全证明，但执行解密的成本过高。2018 年，Zhang 等[16]在 Lai 等[15]工作的基础上减少了部分冗余运算，提高了加解密效率，但由于该方案使用的依然是合数阶双线性群，所以整体效率依旧较低。

在 ABSE 系统中，策略隐藏对于安全性提升同样非常重要。2013 年，Koo 等[17]提出了一种实现访问策略隐藏的 ABSE 方案，支持快速密文搜索和丰富的访问策略表达式，但后来[18]证明其是不安全的。次年，Shi 等[19]通过 LSSS 结构来隐藏访问策略，这是一种低成本保护访问策略的方法，然而，在生成搜索陷门时会造成大量的双线性对计算。2020 年，Wang 等[20]提出了一种具有隐藏访问策略和优化搜索性能的方案，该方案是多值无关的，存储开销不变。同年，Chaudhari 等[21]提出了 keySey，其隐藏了访问策略，并优化了搜索时间，无论访问策略中的属性数量有多少，配对操作的次数都是最少且恒定的。对于单索引搜索文档的时间复杂度为常数，对于多索引搜索文档的时间复杂度为线性。2021 年，Miao 等[22]提出的 ABKS-SM 系统，可以在共享多所有者设置中保护隐私，隐藏访问策略并跟踪恶意数据用户。但文献[23]表明 ABKS-SM 方案无法抵御其声称的离线关键字猜测攻击。

5.1.2 权限管理技术

可追踪性和可撤销性是权限管理技术中非常关键的两个能力，常与 ABSE 机制结合，提高其安全性。

1)可追踪性

可追踪性指系统能够追溯到加密数据的使用和访问记录，能够解决数据共享问题。其主要分为白盒追踪和黑盒追踪。白盒追踪是根据已知泄露密钥追踪到恶意用户；黑盒追踪是一个更强的追踪概念，需要追踪解密设备[24]。

可追踪性是 ABE 系统中的技术。2008 年，Hinek 等[25]首次提出可追踪密钥的选择安全性系统，解密者在解密时需要与可信第三方机构进行交互，这降低了系统的可拓展性和性能。2009 年，Yu 等[26]通过在访问策略中嵌入身份信息的方式实现可追踪 KP-ABE 系统。2012 年，Katz 等[27]提出了谓词加密的可追踪性概念。次年，Liu 等[28-29]提出了白盒追踪和黑盒追踪两种方法，并且实现了选择性追踪。上述 Katz 和 Liu 提出的基于谓词加密的可追踪系统的计算开销随着用户数量的增加呈线性增长，这使得系统仅适用于用户量较少的环境。2016 年，Liu[30]提出黑盒追踪方案，其支持大属性域，但追踪成本大，无法提供前向安全性。2021 年，Ziegler 等[31]提出了白盒去中心化的可追踪性。同年，Luo 等[32]提出了基于格密码的黑盒

追踪,其具有抗量子攻击能力,但是计算开销大。

近几年,与 ABSE 结合的技术主要是白盒追踪。2020 年,Yang 等[33]提出了一种轻量级的可共享和可跟踪安全的移动健康系统(LiST),但是其在解密时必须提供格式良好的密钥。2021 年,Miao 等[22]提出了在共享多所有者设置中的 ABKS-SM 方案,其改进的系统实现了白盒追踪,但其后来被证明无法满足其声明的安全性。文献[33]提出在多权威机构中,能够追踪恶意属性管理机构的 ABSE 方案。2022 年,Varri 等[34]提出的 FELT-ABKS 系统支持可追踪性,并且把大部分计算转移到 fog 节点中,在用户端实现最小计算成本,但其同样需要提供格式良好的密钥。

2)可撤销性

可撤销性指能够撤销已经授予的访问权限或加密数据的共享许可,通常与可追踪性结合。可撤销性包括用户级撤销和属性级撤销。撤销方式可分为直接撤销、间接撤销和混合撤销[35]。直接撤销的执行者是数据拥有者,间接撤销的执行者是权威机构或者第三方,混合撤销指采用间接撤销和直接撤销相结合的方式实现撤销。

2006 年,Pirretti 等[36]首次提出可撤销属性的加密算法,利用时间戳设置有效期限,但这种方式需要与权威中心交互,增加了系统的通信开销。2007 年,Ostrovsky 等[37]首次提出可直接撤销的 CP-ABE 方案,将用户的身份 ID 信息作为一个属性,撤销用户后会在访问结构中加入该用户 ID 的否,使得被撤销用户无权限访问加密数据,但此方案开销较大。2009 年,为解决计算开销问题,Attrapadung 等[38]提出了广播 ABE 系统,需要维护用户列表以提供混合可撤销性,但其只能支持用户撤销而不支持属性撤销。2018 年,Wang 等[39]利用属性群密钥实现了直接属性撤销机制,但其计算成本高,且存在安全性问题。针对上述方案的局限性,2021 年 Tu 等[40]实现了安全的属性撤销方案,但是其密钥更新也需要较高的计算成本。2020 年,Dong 等[41]提出了基于格的可撤销方案,其此方案具有抗量子攻击能力。2021 年,Wei 等[42]提出了支持动态用户撤销的 ABE 方案,其具有低开销和高安全性,但用户撤销不能即时执行。

在 ABSE 中,可撤销性允许数据的所有者或授权机构撤销已经授予的访问权限,从而限制数据的进一步访问,使得系统能够灵活地管理和控制数据的访问权限,提高数据的安全性和隐私保护水平。近五年,有多篇论文实现了 ABSE 中的可撤销性,并且为了提高系统效率,通常会将部分操作外包给云服务器。

2022 年,Bao 等[43]通过构建二叉树实现间接撤销,以限制撤销用户的访问权限,但其计算较为复杂。同年,Varri 等[34]提出 FELT-ABKS,其支持在 fog 节点处进行白盒追踪和属性撤销,大大提高了系统速率,但不能用于用户撤销。文献[33-44]利用用户撤销列表实现用户级撤销,将用户撤销列表维护在云服务器上,在收到查询请求时,需要先检索用户撤销列表。文献[45-46]基于区块链技术实现了用户级撤销,但不能进行属性撤销。2023 年,Yu 等[47]提出去中心化的用户撤销以及属性更新(撤销)。

5.1.3　安全模型

随着计算能力的不断进步和发展,加密方案需要具备足够的安全性以适应更加强大的计算能力需求。安全模型是在密码学和信息安全领域中使用的一种框架或规范,用于描述和评估一个安全系统或算法的安全性属性和性能,安全模型定义了攻击者的能力、攻击策略和系统的目标,以便能够进行系统的安全性分析和设计。

在近几年的 ABSE 机制中,常见的攻击行为有选择关键字攻击(Chosen Keywords Attack,CKA)、关键字猜测攻击(Keyword Guessing Attack,KGA)、选择明文攻击(Chosen Plaintext Attack,CPA)和选择密文攻击(Chosen Ciphertext Attack,CCA)等。

1)选择关键字攻击 CKA:攻击者可以选择性地攻击特定关键字以获得所选关键字的解密,并观察系统的行为,获取信息或推导出加密密钥等敏感信息。文献[21,34,44-45,48-53]都具有抵抗选择关键字攻击的能力。

2)关键字猜测攻击 KGA:攻击者猜测可能的关键字并生成密文进行测试,通过监听搜索结果来判断搜索关键字。文献[22-23,54-56]在面对攻击者进行关键字猜测攻击时,能够保持较高的安全性。

3)选择明文攻击 CPA:攻击者可以选择一些明文并观察相应的密文。攻击者可以利用这些选择的明文和相应的密文对来获取有关加密算法或密钥的信息,以便进行更进一步的攻击。文献[34,45,49,53,57]都具有抵抗选择明文攻击的能力。

4)选择密文攻击 CCA:攻击者可以选择一些密文进行解密或者进行其他操作,并观察相应的结果。攻击者可以根据观察到的结果来获取系统的更多信息,进而可能实施更复杂的攻击。文献[50,53]都能有效地抵御选择密文攻击。

还有一个常见的安全目标,即不可区分性安全 IND(Indistinguishability):攻击者是否无法从密文中推断出有关明文的任何信息。不可区分性攻击通常与 CPA 或 CCA 等攻击能力组合,得到安全定义。例如,IND-CPA 和 IND-CCA 都是常见的安全定义。Chaudhari 等[21]提出具有对密文策略和所选择的关键字攻击不可区分性的 ABSE 方案,Wang 等[50]提出的方案具有选择关键词攻击和选择密文攻击的不可区分性,Yang 等[58]提出了具有不可区分性的随机化选择密文攻击方案,Liu 等[52]提出的方案能够实现选择关键字攻击下的不可区分性,Niu 等[53]的方案满足选择明文和选择密文攻击下的不可区分性安全。

5.2　计算效率提升

为了保证安全性,ABSE 技术通常会产生大量的计算开销。研究人员为了提高 ABSE 的实际可行性,已经提出了许多高效的运算方法,包括引入外包计算、在线/离线加密机制以及优化索引结构等。这些技术可以减少搜索时间和计算开销,使得 ABSE 在实际应用中更具可行性。

5.2.1　外包计算

随着云计算的日益普及,云用户可以将数据外包给云服务器进行存储和计算。这使得云用户能够利用云计算提供的优势减少用户端或终端的计算开销,减轻本地计算负担。2014 年,Zheng 等[8]提出 ABKS,并结合外包计算提高搜索效率。目前,外包计算已被广泛应用于提高 ABSE 的计算效率。

研究人员在处理计算量庞大且复杂的数据时,需要综合考虑算法简化和其他效率提升的方案,仅仅将解密等昂贵操作外包给云服务器而没有考虑系统的可扩展性和性能提升,

可能无法达到预期的效果。

例如，2021 年 Miao 等[59]提出预先计算中间密文，并结合外包计算，将解密等操作外包给云服务器，以实现轻量级系统；2023 年，Zhang 等[60]提出使用树结构优化查询。但外包计算涉及将敏感数据交给云服务器进行处理，由于云服务器诚实且好奇的特性，在使用外包计算提高效率的同时，需要保证访问策略等敏感信息的安全。近几年提出的方案[33,47,49,53,61-62]在将昂贵的计算外包给云的同时保证了其安全性。

对于一些实时性要求高、需要低延迟和大带宽的应用场景，仅依靠云计算可能也无法满足需求。例如，2022 年 Varri 等[34]提出将最大的计算量转移到 fog 节点，以实现用户端最小计算成本；Gao 和 Wang 等[51,63]将计算任务转移到边缘服务器，结合边缘资源优势，提高运算效率，降低延迟。

5.2.2 在线/离线加密机制

1990 年，Even 等[64]为其数字签名方案提出在线/离线机制的概念。2014 年，Hohenberger 等[65]首次在 ABE 方案中结合了在线/离线机制，设计了 OOABE 方案。在第一阶段中预先生成中间密文，使得大部分计算脱机完成；第二阶段只需要少量计算即可在线生成最终密文，但其不具备高安全性。2015 年 Datta 等[66]提出了第一个完全安全的在线/离线谓词加密和基于属性的加密方案，2018 年 Liu 等[67]提出将使用在线/离线机制的 ABE 方案用于共享医疗数据，但上述两方案在解密端涉及大量的配对和指数操作。

在线/离线机制同样被用于 ABSE 机制中以减轻加密端的计算压力，近年来的方案同时考虑到了解密端的计算开销，优化了上述问题。例如，2019 年 Cui 等[68]提出的 OO-KP-ABKS 方案和 2022 年 Bao 等[43]提出的 ERPF-DS-KS 方案属于 KP-ABSE 方案；2021 年，Miao 等[59]提出的 MABKS 和 2022 年 Liu 等[69]提出的 EMK-ABSE 属于 CP-ABSE 方案，其都采用了在线/离线机制和外包计算，同时减轻了加密端计算资源压力和解密端的计算开销。当然，在线/离线加密机制只是将一些密文组件生成的操作“转移”到空闲时间，实际上并没有减少计算资源和能量的消耗，研究人员仍需探索在 ABSE 中减轻计算压力的方案。

5.2.3 索引结构优化

在 ABSE 中，计算开销主要集中于加解密算法和搜索算法，而优化索引构造对于提高搜索效率至关重要。目前，倒排索引和基于树的索引构造是构建高效索引的流行技术。

2015 年，Wang 等[70]在可搜索加密中引入了基于树的索引结构来提高搜索效率，其后常被用于实现 ABSE 方案。2016 年，Xia 等[71]提出基于树的索引结构的可搜索加密方案，该方案支持范围查找且实现了亚线性搜索复杂度，但随着搜索数据量增大，树结构深度增加，搜索速率将降低。为弥补树结构的这一缺陷，2023 年 Zhang 等[60]提出通过聚合相似实体，设计索引树结构，在状态变化时只更新动态索引向量，从而实现高效搜索和索引更新。

虽然树结构能实现亚线性搜索复杂度且支持范围查找，但其空间开销较大，且不能支持高维数据。倒排索引能够弥补这方面的缺陷。倒排索引为关键词构造一组指向文档的指针，通过使用关键字搜索文档，能够依据用户提供的关键词快速检索文档，减少了时间成本和内存存储。2011 年，Curtmola[72]首次在可搜索加密中引入了倒排索引结构，实现了具有亚线性的 SSE 方案，但其安全性较低。2013 年 Cash[73]实现了倒排索引结构的 SSE 方案，但其只考虑了一种对称情况，这限制了其在多用户共享情况中的扩展性。2021 年 Zhang 等[74]引入了一种新的基于属性的授权范式的倒排索引方案，既能实现亚线性搜索复杂度，同时也解决了在多用户之间的共享问题。2020 年 Yin 等[75]提出的 ABSE 方案将倒排索引应用在真实世界数据中，实现了亚线性搜索复杂度，虽然其确实能达到预期效果，但在授权和搜索过程中产生了大量的计算开销。为解决此问题，Yin 等[76]提出了使用异或链的反向索引，并引入了动态更新数据机制。

5.3 灵活性增强

在 ABSE 系统中，灵活性主要体现在能够支持更丰富的访问策略表达式和更复杂的搜索条件。表 5 中总结了近些年一些经典 ABSE 系统在灵活性方面的对比。ABSE 允许用户根据自己的需求指定访问策略以及搜索条件。

表 5 不同方案的灵活性对比

Table 5 Comparison of flexibility of different schemes

序号	系统	年份	大属性域	访问结构	表达能力	策略隐藏
1	[48]	2018	是	访问树	●	否
2	[77]	2020	是	访问树	●	否
3	[45]	2020	是	LSSS	●	否
4	[55]	2020	是	访问树	●	否
5	[49]	2021	是	LSSS	●	否
6	[34]	2021	否	LSSS	●	否
7	[74]	2021	否	两值属性与	◐	否
8	[21]	2022	是	多值属性与	○	是
9	[50]	2022	是	多值属性与	○	否
10	[69]	2022	是	LSSS	●	否
11	[58]	2023	是	LSSS	●	否
12	[52]	2023	否	IPE	○	是
13	[51]	2023	是	LSSS	●	否

注：○表示支持 AND 操作；◐表示支持 AND 和 NOT 操作；●表示支持 AND，OR 和门限操作。

5.3.1 搜索能力增强

在搜索能力方面，主要包括单关键字查询和多关键字查询。单关键字查询指使用单个关键字进行搜索的查询操作，但其很难满足越来越复杂的用户需求；多关键字查询适用于更复杂和精确的搜索需求，在此基础上，研究人员扩展了范围查询、子集查询等功能。

自从 2000 年，Song 等[2]引入了 SSE 的概念，研究人员针对单关键字的查询进行了一系列拓展，直到 2004 年，Golle 等[78]首次提出了联合关键字搜索的概念，即在单个查询中对包含几个关键字的加密数据进行搜索。同年，Park 等[79]定义了一个使用连接关键字搜索的 PEKS 安全模型，此后出现了一系列多关键的方案，包括连接查询、布尔查询、范围查询和子集查询等。

ABSE 机制中，被授权用户可以通过检索关键字来搜索满足特定条件的加密数据项。2014 年，Shi 等[19]提出了一种授权关键字的搜索方案，该方案支持任意布尔公式搜索，并利用了一种具有部分隐藏访问结构的双策略 ABE 方案的变体，但此方案都是基于组合阶双线性群，将产生巨大的计算开销，且只支持单用户查询。2014 年，Zheng 等[8]提出了一种基于属性的外包加密数据的可验证关键字搜索方案，该方案是在多用户设置中进行的，但它只支持单关键字搜索。2015 年，

Zhang[80]提出支持多用户设置中的布尔查询,He[81]提出的基于属性的混合布尔关键字搜索同样支持多用户设置。2018年,Cui等[54]和Miao等[48]分别提出了支持连接查询的ABSE方案,但这两种方案都是选择性安全性,而非完全安全性。2023年,Huang等[82]实现了支持AND,OR,NOT以及门限值表达式的多关键词查询,并且实现了对结果的排序。同年,Miao等[44]提出的电子健康系统可以支持用户匹配指定时间间隔内的索引,但其不支持隐藏访问策略;Liu等[46]提出了基于区块链实现的子集多关键字查询,但其同样没有考虑到隐藏访问策略;Liu等[52]提出子集多关键词检索,返回包含搜索到多关键词的所有文件,并且实现了策略隐藏。

5.3.2　访问策略表达能力的多样性

在属性基加密中,访问策略的表达能力和灵活性是评价系统的重要指标,访问结构是访问控制策略的逻辑结构。最早的访问结构基于Shamir[83]提出的(t,n)门限结构,将秘密信息分为n份秘密份额,使用者必须获得至少t份秘密份额才能重构共享秘密信息,但其表达能力过于简单。随后,Goyal等[5]和Bethencourt等[6]构造了访问树结构,将"与"操作看作(n,n)门限,将"或"操作看作$(1,n)$门限,使得访问策略支持AND,OR以及门限操作,但其安全性被证明是基于一般群模型。2007年,Cheung等[84]实现了标准模型下可证明的CP-ABE,其采用两值属性的"与"操作来构建满足布尔访问策略的方案,但其表达不够灵活。Waters[9]提出的LSSS矩阵,同样采取线性秘密共享方案的思想,将访问树映射到LSSS矩阵中,可以实现AND,OR和门限表达,并且实现了标准模型下的可证安全。

目前的ABSE方案,在实现细粒度访问控制方面普遍采取了上述4种单调访问结构[85],并基于此进行拓展应用。2015年,Zhang等[80]基于门限结构实现了支持AND连接的访问控制策略方案,在文献[65,86]的启发下实现了可使用授权切换模块,可以非交互的更新访问策略,但其表达形式较为单一,2021年,Zhang等[57]提出了基于访问树结构设计的支持AND和OR的访问策略的ABCKS系统,但其只能证明在一般群系统中的安全性。2022年,Bao等[62]提出基于LSSS结构的策略来支持AND,OR和门限表达,并给出了严格证明。

大多数访问策略和属性之间的比较过程都是基于等式关系,虽然简单的做法是利用等式关系表达不等关系,但会产生大量额外的计算开销和存储开销。2018年,Miao等[48]在Xue等[87]的基础上利用0编码和1编码将可比属性转换为字符串实现属性的不等关系匹配。2023年,Zhang等[88]提出了基于属性的双边访问控制,其不仅支持布尔访问策略,而且实现了发布者的真实性和匿名性。

5.3.3　支持大属性域

根据属性域大小可以将属性基加密算法分成两类:有限属性域和大属性域。传统的ABE算法需要输入一个有限的属性域,在系统建立的时候就已确立属性域的大小和种类;若在系统初始化后出现了新的属性,则无法进入后续的加解密算法,这严重影响了系统的灵活性和拓展性。

2011年,Lewko等[89]构造了一个支持大属性域的KP-ABE方案,并且在标准模型下证明了方案的选择性安全。该方案是真正意义上首个支持大属性域特性的属性基加密方案。支持大属性域的方案的特点是具体的属性基不需要在系统建立阶段就预先设定,属性可以是任何字符串,并在方案运行的过程中随时加入所需的属性。2012年,Lewko等[10]提出了另一个支持大属性域的KP-ABE方案,并在标准模型下证明了方案的适应安全性,但是其访问控制策略表达性单一,且存在大量计算开销。2013年,Rouselakis等[90]首次基于素数阶双线性映射构造了一个支持大属性域的CP-ABE方案,并证明了其是选择明文安全的。近五年的ABSE大多支持大属性域,这使得方案更具有灵活性,例如文献[21,58,69]中的方案都支持大属性域。

6　应用领域

随着云计算技术的快速发展,日益增多的组织机构选择将用户的数据存储在云端,而这些数据大多包含如保健、运动、行为和医药处方等个人隐私数据,存在数据泄露和滥用的安全隐患。ABSE方案特别适用于如物联网、医疗等的数据共享场景,在提供数据可用性的同时也保护了用户数据的隐私。

6.1　智能电网

近年来,智能电网中的安全和隐私问题得到了广泛的研究和关注。2019年,Zhang等[91]提出关于智能电网的安全框架,从各方面指导智能电网各业务系统实施信息安全保护工作。针对智能电网中的安全挑战问题,目前已有一些经典的安全方案,例如,Rogers等[92]提出了一种使用时间戳和数字签名的身份验证和完整性协议。

智能电网中包含大量的电力数据,一方面其中可能包含敏感信息;另一方面其涉及多个参与方,例如供电公司、用户以及能源管理公司等,在数据共享与授权的过程中也需要防止隐私信息泄露,这使得ABE越来越多地应用于智能电网。Su等[93]提出使用属性基加密保证在分布式环境中电力交易用户的隐私;Ge等[94]改进了ABE控制方案,针对电网的传输能力和协同访问数据的特点,将其应用于智能电网的协同数据控制。但加密后的数据很难直接用于搜索,目前大多数先进的可搜索算法都是针对一般文本,无法应用于智能电网。为在数据加密的基础上完成搜索功能,Li等[95]提出使用对称加密机制的可搜索加密系统保护智能电网中产生的隐私数据。

为了同时满足可搜索性和访问控制能力,结合ABSE是不二之选。Eltayieb等[96]提出一种基于属性的在线/离线可搜索加密方案ABOOSE,将其部署在智能电网服务器,授权用户搜索用电数据的权限,因此用户可以通过查看自己的用电读数来防止操纵用电量等问题。

6.2　医疗健康

伴随云计算和物联网等技术的广泛应用,电子病历(Electronic Health Record,EMR)、个人健康记录(Personal Health Records,PHR)得到了更多的利用,但如何安全地实现共享成为一大问题。ABSE是其中一种解决方案,通过使用ABSE机制,可以对这些敏感数据进行加密,并实现基于属性的搜索。医生和研究人员可以根据需要搜索特定属性的医疗记录,同时保护患者的隐私。

文献[33,44,97-98]是云辅助的属性基可搜索加密的医疗数据共享系统,利用云服务器的存储和计算能力,减少本地

存储负担,实现医疗研究人员之间的数据共享。文献[46,51]是基于区块链技术辅助的基于属性的可搜索加密的 EMR 和 PHR 共享方案,区块链和智能合约的采用保证了数据的完整性,提供了可追溯性。文献[43,61-62]设计了基于 ABSE 的医疗物联网(Medical Internet of Things,mIoT)数据共享方案,通过收集大量的实时数据,可以更有效地监护患者的生理情况。

6.3 物联网

物联网技术(Internet of Things,IoT)是正日益流行的技术之一,通过传感器和嵌入式设备等获取大量实时数据,这需要物联网具有强大的隐私保护和数据处理能力。结合 ABSE 方案,可以在保护存储在物联网上的数据的安全性的同时,提供可搜索能力。物联网经常与其他场景结合,如上文提到的医疗物联网(mIoT)和工业物联网(Industrial IoT,IIoT)等。文献[49,99-102]都是应用在工业物联网中的属性基可搜索加密方案,以实现数据的安全性和可搜索性。

6.4 移动应用

随着移动设备的普及,移动应用也越来越多元化,ABSE 可以应用于移动应用中来实现数据的安全存储和搜索。

移动众包是一种通过移动设备和互联网平台将任务外包给大量移动用户完成的模式。Miao 等[48]提出利用 ABSE 实现移动众包在各种情况下的问题搜索查询和细粒度访问控制。移动健康(mHealth)将患者数据在移动设备上聚合起来并进行加密,然后上传到云端供研究人员访问。Yang 等[33]提出利用 ABSE 提高系统高效的数据加密和可伸缩性的细粒度访问控制。

7 结束语

7.1 未来方向

7.1.1 安全性增强

ABSE 需要确保搜索操作的安全性和隐私保护。未来的研究将致力于进一步提高 ABSE 方案的安全性,包括对抗不同类型的攻击,如关键字猜测攻击、侧信道攻击等。同时,需要设计更加健壮和可证明安全的 ABSE 方案,以提供更高的安全保障。

近年来,量子计算机建设取得重大突破,量子时代正在到来,这突出了构建量子安全的 ABSE 方案的重要性和紧迫性,但目前的 ABSE 实现大多依赖于传统的数字理论假设,例如方案等,并不具备抗量子攻击能力。因此,考虑量子攻击构建新的 ABSE 方案将是一个新的方向。例如,基于格的加密方案建立在离散数学中的格理论上,具有量子攻击的困难性和抗量子计算机攻击性等特点,被认为是有潜力应对量子攻击的加密技术。

7.1.2 效率提升

ABSE 的搜索操作通常需要耗费大量的计算和存储资源。结合目前数据爆炸的社会背景,ABSE 将越来越多地应用于大数据场景,未来的研究需要注重安全性与高效性的结合,一方面继续挖掘算法的优化方式,另一方面也可以通过并行计算和硬件加速等技术来加速搜索过程,以适应资源短缺型设备、大规模数据集以及实时搜索等场景。

7.1.3 灵活性增强

ABSE 需要支持灵活的访问控制策略和属性管理机制以及更加多样化的表达形式。未来的研究将致力于提供更灵活的访问控制策略,包括更加细粒度的权限管理、动态的属性授权和撤销机制等。此外,还需要研究更加多样化的表达形式和查询语言,以适应更复杂的查询要求,如可比查询、结果排序等。

7.1.4 多应用领域结合

ABSE 不仅可以在传统的数据隐私保护领域应用,还可以结合其他应用领域进行研究和应用。目前常见的应用领域有智能电网、医疗保健、物联网和大数据分析等,未来 ABSE 将探索在不同领域的应用方案,以满足各种实际要求。

7.1.5 结合先进技术

ABSE 可以与其他先进技术相结合,以增强 ABSE 的功能和性能。例如,结合区块链技术,可以提供去中心化的属性管理和审计机制。Zhang 等[57]提出了一种具有可验证性和公平性的 ABCKS 方案,采用区块链和智能合约技术验证搜索结果,并确保在不可信情况下的公平支付。Gao 等[51]提出了一种基于区块链的知识存储和共享架构,可以在智能物联网中实现安全的知识管理,通过上链加密实现数据在链上存储和传输过程中的机密性和安全性,通过智能合约检索存储的密文,可以保证知识的安全性和隐私性。未来的研究将探索 ABSE 与其他技术的结合,以提供更加强大和全面的解决方案。

7.2 总结

文章通过综述了近几年在隐私保护增强、计算效率提升、灵活性增强 3 个方面对 ABSE 体制的相关研究,总结了目前属性基可搜索加密的发展现状。从策略隐藏技术、权限管理技术以及安全性增强方面介绍了 ABSE 近年来在隐私保护增强方面取得的成果;总结了不同作者在外包计算、在线/离线加密机制以及索引结构优化等方面提出的 ABSE 方案;讨论了 ABSE 机制在访问策略表达能力以及搜索能力方面的提升;总结了目前 ABSE 与应用领域结合的诸多方案。最后讨论了 ABSE 的未来发展方向。

参 考 文 献

[1] ZHANG Y, WANG X, LIU X, et al. Survey on Cloud Computing Security [J]. Journal of Software, 2016, 27(6): 1328-1348.

[2] SONG D X D, WAGNER D, PERRIG A, et al. Practical techniques for searches on encrypted data[C]// Proceedings of the 2000 IEEE Symposium on Security and Privacy (S&P 2000). Berkeley, CA, USA, 2000: 14-17.

[3] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search [C]// Advances in Cryptology—Eurocrypt 2004, 2004: 506-522.

[4] SAHAI A, WATERS B. Fuzzy identity-based encryption [C]// Advances in Cryptology—Eurocrypt 2005. 2005: 457-473.

[5] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]// Proceedings of the 13th ACM conference on Computer and Communications Security. 2006

[6] BETHENCOURT J, SAHAI A, WATERS B, et al. Ciphertext-

policy attribute-based encryption [C]// Proceedings of the IEEE Symposium on Security and Privacy(S&P 2007). Berkeley, CA, 2007:20-23.

[7] KHADER D. Introduction to Attribute Based Searchable Encryption[C]// Proceedings of the 15th Joint IFIP TC-6 and TC-11 International Conference on Communications and Multimedia Security (CMS). Univ Aveiro, Aveiro, PORTUGAL, 2014: 25-26.

[8] ZHENG Q, XU S, ATENIESE G, et al. VABKS: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data [C] // Proceedings of the 33rd IEEE Annual Conference on Computer Communications(IEEE INFOCOM). Toronto, CANADA, 2014.

[9] WATERS B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization [C] // Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography(PKC 2011). Taormina, ITALY, 2011:6-9.

[10] LEWKO A, WATERS B. New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques[C]// Proceedings of the 32nd Annual International Cryptology Conference (CRYPTO). Santa Barbara, CA, 2012: 19-23.

[11] WANG S, WANG J, DONG Q, et al. A Survey of Attribute-based Encryption Technology [J]. Netinfo Security, 2019(9): 76-80.

[12] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]// Proceedings of the 5th International Conference on Applied Cryptography and Network Security. New York, NY, 2008:3-6.

[13] LAI J, DENG R H, LI Y. Fully secure cipertext-policy hiding CP-ABE[C]// proceedings of the Information Security Practice and Experience: 7th International Conference (ISPEC 2011). Guangzhou, China, 2011.

[14] BALU A, KUPPUSAMY K. Privacy Preserving Ciphertext Policy Attribute Based Encryption [C]// Proceedings of the 3rd International Conference on Network Security and Applications. Chennai, INDIA, 2010:23-25.

[15] LAI J, DENG R H, LI Y, et al. Expressive CP-ABE with Partially Hidden Access Structures[C]// Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security(ASIACCS). Korea Federat Sci & Technol Soc, Seoul, SOUTH AFRICA, 2012:2-4.

[16] ZHANG Y, DENG R H, HAN G, et al. Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things [J]. Journal of Network and Computer Applications, 2018, 123:89-100.

[17] KOO D, HUR J, YOON H. Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage [J]. Computers & Electrical Engineering, 2013, 39(1): 34-46.

[18] CHAUDHARI P, DAS M L. On the security of a searchable anonymous attribute based encryption[C]// Proceedings of the Mathematics and Computing: Third International Conference (ICMC 2017). Haldia, India, 2017:17-21.

[19] SHI J, LAI J, LI Y, et al. Authorized Keyword Search on Encrypted Data[C]// Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS). Wroclaw Univ Technol, Wroclaw, 2014:7-11.

[20] WANG H, DONG X, CAO Z. Multi-Value-Independent Ciphertext-Policy Attribute Based Encryption with Fast Keyword Search [J]. IEEE Transactions on Services Computing, 2020, 13(6):1142-1151.

[21] CHAUDHARI P, DAS M L. KeySea: Keyword-Based Search With Receiver Anonymity in Attribute-Based Searchable Encryption [J]. IEEE Transactions on Services Computing, 2022, 15(2):1036-1044.

[22] MIAO Y, LIU X, CHOO K K R, et al. Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3):1080-1094.

[23] SUN J, XIONG H, NIE X, et al. On the Security of Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-Owner Setting [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(5):2518-2519.

[24] LIU Z, CAO Z, WONG D S. Traceable CP-ABE: How to Trace Decryption Devices Found in the Wild [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(1):55-68.

[25] HINEK M, JIANG S, SAFAVI-NAINI R, et al. Attribute based encryption with key cloning protection: Report 2008/478 [R]. 2008.

[26] YU S, REN K, LOU W, et al. Defending against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems[C]// Proceedings of the 5th International ICST Conference on Security and Privacy in Communication Networks. Athens, GREECE, 2009:14-17.

[27] KATZ J, SCHRÖDER D. Tracing insider attacks in the context of predicate encryption schemes [C]// Proceedings of the Proc ACITA. 2011.

[28] LIU Z, CAO Z, WONG D S. White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1):76-88.

[29] LIU Z, CAO Z, WONG D S. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on ebay[C]// Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. 2013.

[30] LIU Z, WONG D S. Traceable CP-ABE on prime order groups: Fully secure and fully collusion-resistant blackbox traceable [C]// Proceedings of the International Conference on Information and Communications Security. Springer, 2015.

[31] ZIEGLER D, MARSALEK A, PALFINGER G. White-Box Traceable Attribute-Based Encryption with Hidden Policies and Outsourced Decryption [C]// Proceedings of the 20th IEEE International Conference on Trust, Security and Privacy in Computing and Communications(IEEE TrustCom). Shenyang, 2021: 20-22.

[32] LUO F, AL-KUWARI S. Generic Construction of Black-Box Traceable Attribute-Based Encryption [J]. IEEE Transactions on Cloud Computing, 2023, 11(1):942-955.

[33] YANG Y, LIU X, DENG R H, et al. Lightweight Sharable and Traceable Secure Mobile Health System [J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(1): 78-91.

[34] VARRI U S, KASANI S, PASUPULETI S K, et al. FELT-ABKS: Fog-Enabled Lightweight Traceable Attribute-Based Keyword Search Over Encrypted Data [J]. IEEE Internet of Things Journal, 2022, 9(10): 7559-71.

[35] LI L, ZHU J, YANG C. Overview of Research on the Revocable Mechanism of Attribute-Based Encryption [J]. Netinfo Security, 2023(4): 39-50.

[36] PIRRETTI M, TRAYNOR P, MCDANIEL P, et al. Secure attribute-based systems [C]// Proceedings of the 13th ACM conference on Computer and Communications Security. 2006.

[37] OSTROVSKY R, SAHAI A, WATERS B. Attribute-Based Encryption with Non-Monotonic Access Structures[C]// Proceedings of the 14th ACM Conference on Computer and Communication Security. Alexandria, VA, 2007: 29.

[38] ATTRAPADUNG N, IMAI H. Conjunctive Broadcast and Attribute-Based Encryption[C]// Proceedings of the 3rd International Conference on Paring-Based Cryptography. Stanford Univ, Palo Alto, CA, 2009: 12-14.

[39] WANG S, ZHANG X, ZHANG Y. Efficient revocable and grantable attribute-based encryption from lattices with fine-grained access control [J]. IET Information Security, 2018, 12(2): 141-149.

[40] TU S, WAQAS M, HUANG F, et al. A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing [J]. Computer Networks, 2021, 195.

[41] DONG X, ZHANG Y, WANG B, et al. Server-Aided Revocable Attribute-Based Encryption from Lattices [J]. Security and Communication Networks, 2020.

[42] WEI J, CHEN X, HUANG X, et al. RS-HABE: Revocable-Storage and Hierarchical Attribute-Based Access Scheme for Secure Sharing of e-Health Records in Public Cloud [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(5): 2301-2315.

[43] BAO Y, QIU W, TANG P, et al. Efficient, Revocable, and Privacy-Preserving Fine-Grained Data Sharing With Keyword Search for the Cloud-Assisted Medical IoT System [J]. IEEE Journal of Biomedical and Health Informatics, 2022, 26(5): 2041-2051.

[44] MIAO Y, LI F, LI X H, et al. Time-controllable keyword search scheme with efficient revocation in mobile e-health cloud [J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 3650-3665.

[45] LIU S, YU J, XIAO Y, et al. BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT [J]. IEEE Internet of Things Journal, 2020, 7(9): 7851-7867.

[46] LIU S, CHEN L, WU G, et al. Blockchain-Backed Searchable Proxy Signcryption for Cloud Personal Health Records [J]. IEEE Transactions on Services Computing, 2023, 16(5): 3210-3223.

[47] YU J, LIU S, XU M, et al. An Efficient Revocable and Searchable MA-ABE Scheme With Blockchain Assistance for C-IoT [J]. IEEE Internet of Things Journal, 2023, 10(3): 2754-2766.

[48] MIAO Y, MA J, LIU X, et al. Practical Attribute-Based Multi-Keyword Search Scheme in Mobile Crowdsourcing [J]. IEEE Internet of Things Journal, 2018, 5(4): 3008-3018.

[49] ZHANG K, LONG J, WANG X, et al. Lightweight Searchable Encryption Protocol for Industrial Internet of Things [J]. IEEE Transactions on Industrial Informatics, 2021, 17(6): 4248-4259.

[50] WANG H, FAN K, ZHANG K, et al. Secure and efficient data-privacy-preserving scheme for mobile cyber-physical systems [J]. IEEE Internet of Things Journal, 2022, 9(22): 22375-22388.

[51] GAO H, HUANG H, XUE L, et al. Blockchain-enabled fine-grained searchable encryption with cloud-edge computing for electronic health records sharing [J]. IEEE Internet of Things Journal, 2023, 10(20): 18414-18425.

[52] LIU J, FAN Y, SUN R, et al. Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system [J]. IEEE Internet of Things Journal, 2023, 10(24): 21377-21388.

[53] NIU S, HU Y, ZHOU S, et al. Attribute-Based Searchable Encryption in Edge Computing for Lightweight Devices [J]. Ieee Systems Journal, 2023, 17(3): 3503-3514.

[54] CUI H, WAN Z, DENG R H, et al. Efficient and Expressive Keyword Search Over Encrypted Data in Cloud [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(3): 409-422.

[55] YU Y, SHI J, LI H, et al. Key-Policy Attribute-Based Encryption With Keyword Search in Virtualized Environments [J]. IEEE Journal on Selected Areas in Communications, 2020, 38(6): 1242-1251.

[56] SHI J, YU Y, YU Q, et al. Toward Data Security in 6G Networks: A Public-Key Searchable Encryption Approach [J]. IEEE Network, 2022, 36(4): 166-713.

[57] ZHANG D, WANG S, ZHANG Q, et al. Attribute-based conjunctive keywords search with verifiability and fair payment using blockchain [J]. IEEE Transactions on Services Computing, 2023, 16(6): 4168-4182.

[59] MIAO Y, DENG R H, LIU X, et al. Multi-Authority Attribute-Based Keyword Search over Encrypted Cloud Data [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(4): 1667-1680.

[60] ZHANG P, CHUI Y, LIU H, et al. Efficient and Privacy-Preserving Search Over Edge-Cloud Collaborative Entity in IoT [J]. IEEE Internet of Things Journal, 2023, 10(4): 3192-3205.

[61] LIU X, YANG X, LUO Y, et al. Verifiable Multikeyword Search Encryption Scheme With Anonymous Key Generation for Medical Internet of Things [J]. IEEE Internet of Things Journal, 2022, 9(22): 22315-22326.

[62] BAO Y, QIU W, CHENG X. Secure and Lightweight Fine-Grained Searchable Data Sharing for IoT-Oriented and Cloud-Assisted Smart Healthcare System [J]. IEEE Internet of Things Journal, 2022, 9(4): 2513-2526.

[63] WANG J, LIN X, WU Y, et al. Blockchain-Enabled Lightweight Fine-Grained Searchable Knowledge Sharing for Intelligent IoT [J]. IEEE Internet of Things Journal, 2023: 1-.

[64] EVEN S, GOLDREICH O, MICALI S. On-line/off-line digital signatures [J]. Journal of Cryptology, 1996, 9(1): 35-67.

[65] HOHENBERGER S, WATERS B. Online/Offline Attribute-

Based Encryption[C]// Proceedings of the 17th Annual IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC). Buenos Aires, ARGENTINA, 2014: 26-28.

[66] DATTA P, DUTTA R, MUKHOPADHYAY S. Fully Secure Online/Offline Predicate and Attribute-Based Encryption[C]// Proceedings of the 11th International Conference on Information Security Practice and Experience(ISPEC). Beijing, China, 2015: 5-8.

[67] LIU Y, ZHANG Y, LING J, et al. Secure and fine-grained access control on e-healthcare records in mobile cloud computing [J]. Future Generation Computer Systems-the International Journal of Escience, 2018, 78: 1020-12206.

[68] CUI J, ZHOU H, XU Y, et al. OOABKS: Online/offline attribute-based encryption for keyword search in mobile cloud [J]. Information Sciences, 2019, 489: 63-77.

[69] LIU J, LI Y, SUN R, et al. EMK-ABSE: Efficient Multikeyword Attribute-Based Searchable Encryption Scheme Through Cloud-Edge Coordination [J]. IEEE Internet of Things Journal, 2022, 9(19): 18650-18662.

[70] WANG B, LI M, WANG H. Geometric Range Search on Encrypted Spatial Data [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(4): 704-719.

[71] XIA Z, WANG X, SUN X, et al. A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data [J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(2): 340-352.

[72] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption: improved definitions and efficient constructions[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. 2006.

[73] CASH D, JARECKI S, JUTLA C, et al. Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries [C]// Proceedings of the 33rd Annual International Cryptology Conference(CRYPTO). Santa Barbara, CA, 2013: 18-22.

[74] ZHANG K, WEN M, LU R, et al. Multi-client sub-linear Boolean keyword searching for encrypted cloud storage with owner—enforced authorization [J] IEEE Transactions on Dependable and Secure Computing, 2021, 18(6): 2875-2887.

[75] YIN H, QIN Z, ZHANG J, et al. A fine-grained authorized keyword secure search scheme with efficient search permission update in cloud computing [J]. Journal of Parallel and Distributed Computing, 2020, 135: 56-69.

[76] YIN H, LI Y, DENG H, et al. Practical and Dynamic Attribute-Based Keyword Search Supporting Numeric Comparisons Over Encrypted Cloud Data [J]. Ieee Transactions on Services Computing, 2023, 16(4): 2855-2867.

[77] MIAO Y, MA J, LIU X, et al. Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing [J]. IEEE Transactions on Services Computing, 2020, 13(6): 985-998.

[78] GOLLE P, STADDON J, WATERS B. Secure conjunctive keyword search over encrypted data [C]// Applied Cryptography and Network Security. 2004: 31-45.

[79] PARK D J, KIM K, LEE P J. Public key encryption with conjunctive field keyword search [C]// Information Security Applications. 2005: 73-86.

[80] ZHANG K, WANG X, NING J, et al. Multi-client Boolean file retrieval with adaptable authorization switching for secure cloud search services [J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(6): 4621-4636.

[81] HE K, GUO J, WENG J, et al. Attribute-Based Hybrid Boolean Keyword Search over Outsourced Encrypted Data [J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(6): 1207-1217.

[82] HUANG Q, YAN G, WEI Q. Attribute-Based Expressive and Ranked Keyword Search Over Encrypted Documents in Cloud Computing [J]. IEEE Transactions on Services Computing, 2023, 16(2): 957-968.

[83] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[84] CHEUNG L, NEWPORT C. Provably Secure Ciphertext Policy ABE[C]// Proceedings of the 14th ACM Conference on Computer and Communication Security. Alexandria, 2007.

[85] CHEN Y. Research on Attribute-Based Encryption Systems and Its Applications [D]. Nanjing: Nanjing University of Posts and Telecommunications, 2014.

[86] LAI J, DENG R H, YANG Y, et al. Adaptable ciphertext-policy attribute-based encryption [C]// Proceedings of the Pairing-Based Cryptography-Pairing 2013: 6th International Conference. Beijing, China, 2013: 22-24.

[87] XUE K, HONG J, XUE Y, et al. CABE: A New Comparable Attribute-Based Encryption Construction with 0-Encoding and 1-Encoding [J]. IEEEE Transactions on Computers, 2017, 66(9): 1491-1503.

[88] ZHANG K, WANG X, NING J, et al. Secure Cloud-Assisted Data Pub/Sub Service With Fine-Grained Bilateral Access Control [J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 5286-5301.

[89] LEWKO A, WATERS B. Unbounded HIBE and Attribute-Based Encryption[C]// Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn, ESTONIA, 2011: 15-19.

[90] ROUSELAKIS Y, WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption [C]// Proceedings of the 2013 ACM SIGSAC Conference on Computer C Sommunications Scurity. 2013.

[91] ZHANG T, LIN W, WANG Y, et al. The design of information security protection framework to support smart grid[C]// Proceedings of the 2010 International Conference on Power System Technology. IEEE, 2010.

[92] ROGERS K M, KLUMP R, KHURANA H, et al. An Authenticated Control Framework for Distributed Voltage Support on the Smart Grid [J]. IEEE Transactions on Smart Grid, 2010, 1(1): 40-47.

[93] SUQ, ZHANGR, XUER, etal. DistributedAttribute-BasedSignature With Attribute Dynamic Update for Smart Grid [J]. IEEE Transactions on Industrial Informatics, 2023, 19(9): 9424-9435.

[94] GE J, WEN M, WANG L, et al. Attribute-Based Collaborative Access Control Scheme with Constant Ciphertext Length for Smart Grid[C]// Proceedings of the IEEE International Confer-

ence on Communications(ICC). Seoul, SOUTH KOREA, 2022: 16-20.

[95] LI J, NIU X, SUN J S, et al. A Practical Searchable Symmetric Encryption Scheme for Smart Grid Data[C]// Proceedings of the IEEE International Conference on Communications(IEEE ICC). 2019.

[96] ELTAYIEB N, ELHABOB R, HASSAN A, et al. An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid [J]. Journal of Systems Architecture, 2019, 98: 165-172.

[97] GE X, YU J, HAO R, et al. Verifiable Keyword Search Supporting Sensitive Information Hiding for the Cloud-Based Healthcare Sharing System [J]. IEEE Transactions on Industrial Informatics, 2022, 18(8): 5573-5583.

[98] MAMTA, GUPTA B B, LI K C, et al. Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System [J]. IEEE-CAA Journal of Automatica Sinica, 2021, 8(12): 1877-1890.

[99] WANG W, XU P, LIU D, et al. Lightweighted Secure Searching Over Public-Key Ciphertexts for Edge-Cloud-Assisted Industrial IoT Devices [J]. IEEE Transactions on Industrial Informatics, 2020, 16(6): 4221-4230.

[100] ALI M, SADEGHI M R, LIU X, et al. Verifiable online/offline multi-keyword search for cloud-assisted Industrial Internet of Things [J]. Journal of Information Security and Applications, 2022, 65(C): 103101.

[101] ZHOU R, ZHANG X, WANG X, et al. Device-Oriented Keyword-Searchable Encryption Scheme for Cloud-Assisted Industrial IoT [J]. IEEE Internet of Things Journal, 2022, 9(18): 17098-17109.

[102] YIN H, ZHANG W, DENG H, et al. An Attribute-Based Searchable Encryption Scheme for Cloud-Assisted IIoT [J]. IEEE Internet of Things Journal, 2023, 10(12): 11014-11023.

YAN Li, born in 1975, master. Her main research interests include smart grid, data analytics and artificial intelligence.

YIN Tian, born in 2001, postgraduate. Her main research interests include information security and cryptography.