计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2021.20210805
58(10):2079-2098,2021

云数据安全保护方法综述

沈 剑[1] 周天祺[1] 曹珍富[2]
[1](南京信息工程大学计算机与软件学院 南京 210044)
[2](上海市高可信计算重点实验室(华东师范大学) 上海 200062)
(s_shenjian@126.com)

Protection Methods for Cloud Data Security

Shen Jian[1], Zhou Tianqi[1], and Cao Zhenfu[2]
[1](*School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing* 210044)
[2](*Shanghai Key Laboratory of Trustworthy Computing (East China Normal University), Shanghai* 200062)

Abstract The rapid development of computer networks and the popularization of big data have promoted the further development of cloud computing. The cloud environment is an important platform for data interaction in the network and information age. It provides great convenience for the efficient data interaction of individuals, enterprises and countries, but it also poses new challenges for the security of cloud data. In this paper, we first present the existing cloud computing model, investigate and analyze the threats in cloud data security protection schemes. On this basis, a systematic analysis of the latest research results of cloud data security protection schemes at home and abroad is conducted, namely, access control, key agreement, secure data auditing and secure data sharing. Secondly, we conduct systematic research and propose solutions to the problems such as easy disclosure of user privacy during the access control process, difficulty in controlling overhead during key generation, low efficiency in dynamic operations during auditing, and difficulty in tracking malicious users during data sharing in existing cloud data security protection schemes. Finally, the current challenges and future research directions of cloud data security protection are discussed, with a view to promoting the establishment of a more complete cloud data protection system.

Key words cloud data security; access control; key agreement; secure data auditing; secure data sharing

摘 要 计算机网络的快速发展与大数据的普及推动了云计算技术的进一步发展.云环境是网络与信息时代下数据交互的重要平台,为个人、企业和国家的数据高效交互提供了极大的便利,但同时也为云数据安全和隐私保护提出了新的挑战.首先给出了现有云计算模型,调研和分析云数据安全保护中存在的威胁.在此基础上,从云数据安全的访问控制、密钥协商、安全审计和安全共享4个方面出发,对国内外云数据安全保护方案的最新研究成果进行系统分析.其次,针对现有云数据安全保护方案存在访问控制过程中用户隐私易被泄露、密钥生成过程中开销难以控制、审计过程中动态操作效率低下、错误恢复较难实现、数据共享过程中恶意用户难以追踪等问题,进行系统研究,提出解决思路.最后,探讨云数据安全保护当前面临的挑战和未来研究方向,以期推动更加完善的云数据保护体系的建立.

收稿日期:2021-08-13;**修回日期**:2021-08-24
基金项目:国家自然科学基金项目(61922045, U1836115, 61672295);江苏省自然科学基金项目(BK20181408);鹏城实验室网络空间安全研究中心项目(PCL2018KP004)
This work was supported by the National Natural Science Foundation of China (61922045, U1836115, 61672295), the Natural Science Foundation of Jiangsu Province (BK20181408), and the Project of the Cyberspace Security Research Center, Peng Cheng Laboratory of Guangdong Province (PCL2018KP004).

关键词 云数据安全;访问控制;密钥协商;安全数据审计;安全数据共享

中图法分类号 TP391

云计算作为互联网产业中的重要新型数字基础设施,为大数据、5G、人工智能等领域的进一步发展奠定了重要基础.如今,云计算及其提供的各类应用与人们的日常生产生活息息相关,在互联网环境下,人们的日常沟通交流、工作、学习等或多或少都会使用到云计算提供的各类资源.全球著名市场研究公司——国际数据公司(International Data Corporation, IDC)预测:截止 2021 年底全球公有云收入将达到 2 783 亿元.本质上来说,人们进行的各类操作、使用的各种应用都可以归结为数据流通.因此,数据的安全直接决定着云计算的安全和其所支持的各类应用的合规合法.然而,随着云计算的发展和普及,数据安全与隐私保护问题日益严峻.腾讯安全云鼎实验室联合 GeekPwn 发布的《2019 云安全威胁报告》中显示在所有国内攻击源中云资源作为攻击源占比已接近一半[1].同时,该报告指出,当前数据安全威胁已成为云企业面必须直面的挑战.

云计算是传统计算机与网络技术发展融合的产物,为个人的数据存储和使用、企业的数据开发和利用、国家的数据监控和管控提供极大的便利.云计算主要特点是可提供大量数据存储和计算服务.尽管云计算为人们的生产生活提供了极大便利,数据安全威胁仍是云计算当前所面临的巨大挑战.此外,用户或企业对外包云数据的安全考量将极大影响云计算及其相关服务领域的进一步发展.另一方面,近年来数据泄露、数据丢失、用户隐私泄露等各类云数据安全攻击事件激增,各类攻击手段层出不穷.因此,如何保护云计算的数据安全成为近年来国内外的研究热点.值得注意的是,密码学中的加密、签名、密钥协商等基本密码原语作为可抵抗上述安全威胁事件的可靠技术受到了工业界、学术界乃至国家的广泛关注.

1 云计算模型

本节主要介绍云计算网络模型、安全模型和安全需求.

1.1 网络模型

云计算是一种集成了传统计算机网络,各类硬件资源,并通过虚拟化技术、资源优化技术、并行计算技术等先进的技术进行优化的生态系统.云计算的基础架构如图 1 所示.具体来说,云计算的架构主要可分为 3 层,即,基础设施层(infrastructure as a service, IaaS)、平台层(platform as a service, PaaS)和软件服务层(software as a service, SaaS).IaaS 层主要包括云计算基础架构及其硬件设备;PaaS 层可以看作云计算的操作系统,是云平台和应用软件的稳定良好运行的基础平台;SaaS 层提供软件即服务,是一种基于互联网的云平台应用软件付费使用的新型模式.

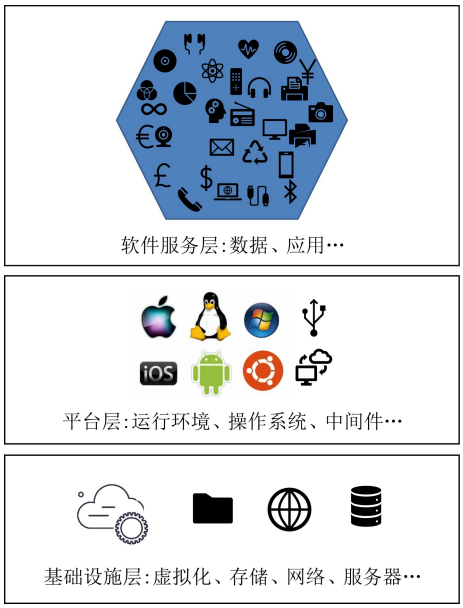


Fig. 1 The architecture of cloud computing

图 1 云计算架构

1.2 安全模型

云计算 3 层体系涉及到的安全问题主要包括:数据安全、终端安全、访问控制管理、应用安全、主机和网络安全、物理和基础设施安全.本文主要讨论云计算中的数据安全和访问控制安全.云上的数据生存周期及数据安全威胁如图 2 所示.其中,数据的生存周期指数据自产生开始,经历存储、使用、共享、归档直至最终销毁经历的 6 个阶段.在这过程中,数据安全主要面临数据泄露、数据丢失、数据损坏、密钥攻击等威胁.

云计算可以实现计算机和网络资源的共享应用,提高计算效率和存储容量,保障存储可靠.云计算可以为用户提供大容量数据存储高性能计算服务,云数据服务的系统模型可以概括为图 3 所示.其中,

云服务器为单个用户或者企业公司等群组用户提供数据存储和计算服务;可信第三方负责对存储在云上的外包数据进行审计,确保数据的完整性和正确性;单个用户可以存储或者访问存储在云上的外包数据;群组用户除了可以存储和访问外包数据,还可通过云进行数据共享,组管理员可执行身份追踪、访问控制、成员注册、容错检测等保证数据共享过程中群组用户数据安全的操作.

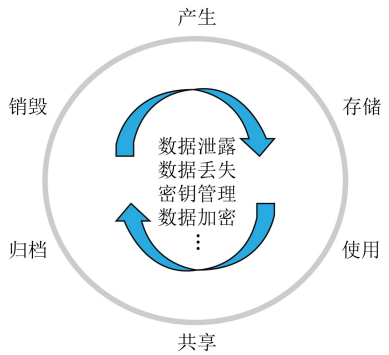


Fig. 2　Data life cycle and data security threats

图 2　数据生存周期及数据安全威胁

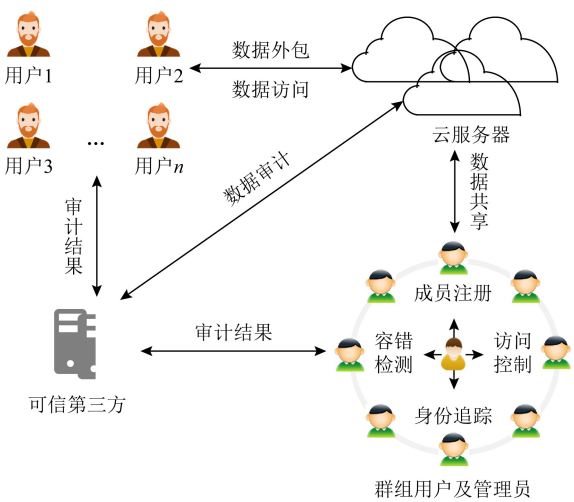


Fig. 3　The system model of cloud data service

图 3　云数据服务的系统模型

1.3　安全需求

云数据安全保护的安全需求以及为其提供保障的密码原语可概括如表 1 所示.

首先,不可伪造[2]和合法访问[3]指非法用户无法通过身份认证进而访问云上数据,该属性是云数据安全保护的关键环节.其次,数据的完整性和正确性[4]是指外包存储在云上的数据没有出现错误,与用户上传的数据一致且完整,完整性和正确性是云服务发展的基础同时也是用户使用云的重要前提.再次,数据机密性[5]和隐私保护[6]是指存储数据安全,攻击者或者好奇的云在没有密钥的情况下无法获知数据所包含任何有价值信息,该属性是云数据安全的重要特征.最后,隐私保护是指用户身份和数据隐私安全,目前,隐私保护越来越受到人们关注,同时大数据环境下驱动的各领域多方协作可极大推进科技的发展,但协作过程中的隐私保护是各方参与协作的必要前提,因此隐私保护已成为云进一步发展的关键瓶颈.

Table 1　Data Security Requirements and Corresponding Cryptographic Primitives

表 1　数据安全需求及相应密码原语

安全需求	功能	密码原语/协议
不可伪造性	确保用户身份无法伪造	签名、零知识证明
合法访问	确保非法用户无法获取数据	属性加密、密钥管理
数据完整性	确保存储数据完整	审计协议
数据正确性	确保存储数据正确	审计协议
数据机密性	确保存储数据安全	加密、密钥管理
隐私保护	确保身份/数据隐私	加密、不经意存储、同态技术

针对上述安全需求,密码学中的加密、签名、认证、密钥协商等密码原语作为保证数据机密性、身份合法性、数据完整性的技术具有重要作用.当前,云环境中较为有效的数据安全和隐私保护技术包括:基于属性的加密、同态加密技术、代理重加密、零知识证明技术、多方密钥协商、群签名技术等.

2　背景知识

本节介绍云数据安全保护涉及到的密码学相关背景知识,主要包括:秘密共享、多方密钥协商、数据审计和代理重加密.

2.1　秘密共享

秘密共享是一种将秘密分割的重要密码学原语.在秘密共享技术中,秘密持有者根据需求选取门限值 t 并基于特定技术将秘密值 S 分割为 n 个子秘密份额 $\{s_1,s_2,s_3,\cdots,s_n\}$.目前,用于生成子秘密份额的技术主要包括一元 N 次多项式、中国剩余定理、多维向量空间等.当且仅当合作的用户数量大于门限值 t 时,恢复出秘密值 S.秘密共享包括 4 个算法:

1) 初始化.输入安全参数 l、门限值 t.输出子秘密份额生成函数 $Gen()$ 和秘密恢复函数 $Rec()$.

2) 秘密分割.输入秘密值 S、门限值 t,参与秘密

共享的人数 n,子秘密份额生成函数 $Gen()$.输出 n 个子秘密份额$\{s_1,s_2,s_3,\cdots,s_n\}$.

3) 秘密份额分发.在安全信道下或采用安全加密算法 $Enc()$将秘密份额分发给 n 个参与者.

4) 秘密恢复.输入秘密份额$\{s_1,s_2,s_3,\cdots,s_m\}$,$m\geqslant t$,秘密恢复函数 $Rec()$.输出秘密值 S.

秘密共享的基本安全需求包括 2 方面:正确性和隐私性.正确性要求具有高效的算法能够根据满足门限要求的秘密份额$\{s_1,s_2,s_3,\cdots,s_m\}$,$m\geqslant t$ 恢复出原始秘密值 S;隐私性要求任何不满足门限 t 要求的秘密份额组合$\{s_1,s_2,s_3,\cdots,s_m\}$,$m<t$ 都无法恢复出秘密值S,即秘密值 S 和任何不满足门限t 要求的秘密份额组合是相互独立的.

2.2 多方密钥协商

多方密钥协商是保证公开网络下多方安全交互的基础密码原语,多方密钥协商主要包括 3 个算法:

1) 初始化.输出系统安全参数 l,用户数量 n.输出子密钥生成函数 $SubGen()$,共享密钥生成函数 $SessionGen()$.

2) 子密钥生成.每个用户选取随机数 r 和用户私钥 sk,根据子密钥生成函数 $SubGen()$计算子密钥 k_i.

3) 共享密钥生成.输入 n 个用户的子密钥,共享密钥生成函数 $SessionGen()$,输出 n 个用户的共享密钥 K.

多方密钥协商的基本安全需求要求参与用户外的任何人都无法获知生成的共享密钥 K.

2.3 数据审计

数据审计方案是保障云存储数据完整性的重要密码学原语.数据审计方案主要包括 4 个算法:

1) 初始化.输出系统安全参数 l.输出用户公私钥对(pk,sk).

2) 验证标签生成.输入公私钥对(pk,sk)和文件块 f.输出验证标签 T_f.

3) 证明生成.输入挑战 $chal$,文件公钥 pk,文件块 f 及其对应的验证标签 T_f.输出被挑战块的持有性证明 P.

4) 证明验证.输入公私钥对(pk,sk),挑战 $chal$ 和证明 P.输出成功或失败.

数据审计方案的安全性要求以极大的概率检测出外包数据的损坏或丢失.

2.4 代理重加密

代理重加密是云环境下保证数据共享安全的有效密码原语.本质上来说,代理重加密是实现云环境下密文转换的一种技术,即将用户 A 可解密的加密数据转换成用户 B 可解密的加密数据.该特性可有效支持云环境用户动态变化情况下的高效密文更新.代理重加密包括 5 个算法:

1) 初始化.输出系统安全参数 l.输出用户公私钥对(pk,sk).

2) 初始加密.用户持有者 A 采用加密函数加密消息 M,生成初始密文 $C=Enc(M)$.

3) 转换密钥生成.用户持有者根据其意愿分享数据的接收方生成转换密钥 K_{A-B}.并将初始密文和转换密钥提交给代理.

4) 重加密.代理根据初始密文 C 和转换密钥 K_{A-B}对密文进行转换,生成转换密文 C_T.

5) 解密.符合用户 A 授权的用户在收到经过代理转换的密文后使用自己的解密密钥解密出明文 M.

代理重加密的安全性要求代理在转换的过程中无法获知明文的任何信息.

3 云计算数据安全保护方案

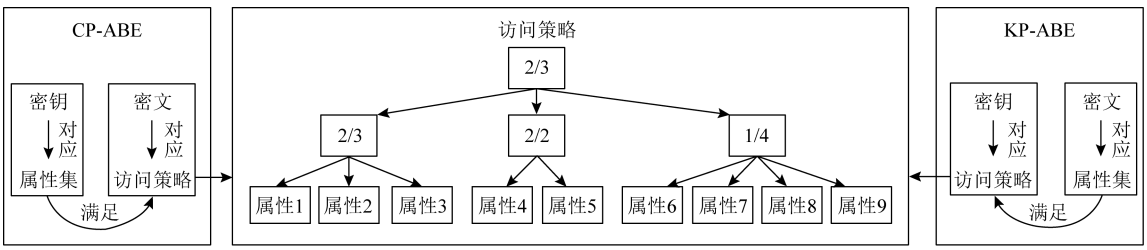
当前,国内外的研究学者们已对各类云数据安全保护方案展开研究,取得了一系列研究成果.研究成果主要集中在访问控制、密钥协商、安全审计和安全共享 4 个方面.

3.1 访问控制

为了保障外包数据安全,云服务器提供商应只允许合法用户进行数据访问和操作,因此访问控制是云数据安全的第一道屏障,目前,属性加密、秘密共享、签名等密码技术已广泛应用于云环境以实现访问控制.

2005 年,Sahai 和 Waters[7] 在欧密会上对存储数据的生命周期各阶段的数据安全和隐私保护问题进行了简要而全面的分析,并改进基于身份的加密(identity based encryption, IBE)方案,提出了基于属性的加密(attribute based encryption, ABE)方案.该方案可支持一对多安全数据共享,在不可靠的存储环境中实现细粒度的访问控制.随后,ABE 的研究主要分为 2 个分支:密文策略属性加密(ciphertext policy attribute based encryption, CP-ABE)[8-9] 和密钥策略属性加密(ciphertext policy attribute based encryption, KP-ABE)[10-11].相对于 KP-ABE,CP-ABE 可支持密文的隐式授权且不依赖于密钥分发中心,适用于更多应用领域.KP-ABE 和 CP-ABE 基本结构如图 4 所示.在 ABE 中属性代表一系列标

识用户的元素,如身份、出生年月、工作等可以标识用户的特征,访问策略则规定了何种属性组合符合要求.在 KP-ABE 中,密文与用户属性绑定,密钥包含访问策略,当且仅当密文所绑定的用户属性满足密钥包含的访问策略时可正确解密.CP-ABE 则相反,即密钥与用户属性绑定,密文包含访问策略,当且仅当密钥所绑定的用户属性符合密文包含的访问策略时可正确解密.CP-ABE 方案可保护不可信云服务器环境下的数据机密性,有效支持细粒度数据访问控制.



注:X/Y表示Y个属性中至少需X个属性满足条件.

Fig. 4　The structure of KP-ABE and CP-ABE

图 4　KP-ABE 和 CP-ABE 基本结构

此外,ABE 方案的关键部分,即访问策略的制定,通常与秘密共享技术[12]密切相关,在图 4 的访问策略中,叶子节点代表用户属性,其余节点均表示门限值,秘密共享方案可以为门限的设计提供良好的解决方案.2010 年 Yu 等人[13]基于 ABE、代理重加密、延迟重加密技术提出了云环境下安全、可扩展和细粒度的数据访问控制方案.该方案还实现了用户密钥问责功能和访问权限隐私保护.2015 年,王皓等人[11]针对 ABE 方案计算效率低的问题,引入外部资源优化计算效率,形式化定义了外包 ABE 方案和协议安全模型,在此基础上,基于合数阶双线性群构造了一个具体的外包 CP-ABE 方案,并基于双系统加密技术证明协议的自适应安全性.2017 年,杨腾飞等人[14]将分类分级的属性层级支配关系嵌入 ABE 机制,实现了访问控制的层次化授权特性和存储数据隔离,但该系统复杂度较高,且用户撤销带来的开销较大.同年,Huang 等人[15]提出了一种基于分层属性加密的安全、细粒度数据访问控制方案,支持轻量密钥管理,有效降低了本地服务器的负担.此外,该方案仅需更新策略而无需更新加密密文,进一步提高了方案的动态性.此后,Li 等人[16]针对信息中心网络(information centric network, ICN)中可能存在的内置病毒防护缺失问题,提出了一种强制性内容访问控制方案(mandatory content access control, MCAC),使得内容提供者根据需求对网络节点的缓存内容进行控制,该文针对不同内容定义安全标签,根据标签判断路由器是否需要缓存,从而保证了访问控制的缓存内容的安全.Xue 等人[17]指出现有的 CP-ABE 方案中,单属性授权机构由于需执行耗时的用户合法性验证和密钥分配操作,可能导致单点失效问题.另一方面,多权限访问控制方案也存在权限管理属性集不相交的问题,导致访问控制效率低下.该文针对上述问题提出了一种具备审计机制的访问控制方案,并引入可信第三方验证用户合法性、实现密钥分配、支持错误审核,有效提升访问控制方案的效率保证密钥分配的安全.2019 年,Xue 等人[18]指出现有访问控制方案不支持用户协作获得访问许可.针对该问题,Xue 等人设计了支持用户协作的访问控制结构,定义了访问控制中的转换节点,通过将转换密钥嵌入 BSW 方案[10]的密钥中,为每个转换节点添加转换值.转换密钥和转换值的组合使支持用户可以相互协作满足策略树规定的策略.2020 年,杜瑞忠等人[19]针对雾计算环境下节点资源受限的实际情况,基于模加法一致性秘密分享技术和重加密机制优化 CP-ABE 方案的加解密和属性更新效率.然而,改方案没有考虑节点域的划分的问题,随着设备来源增多,存在虚假节点和用户骗取数据的状况.针对该问题,潘瑞杰等人[20]针对云环境跨域访问控制易受恶意用户攻击的问题,提出了一种基于动态用户信任度的访问控制模型(ABAC based on dynamic user trust in loud computing, CT-ABAC),将主体、客体、权限、环境和用户信任度等属性纳入访问请求并设计采用动态细粒度的授权机制,支持用户动态变化.此外,引入时间、安全域间评价相似度、惩罚机制等元素计算用户信任度属性,进一步优化了用户的可信度评估,保证跨域访问控制的安全性.

然而仅依靠 ABE 并不能从根本上彻底解决密文

访问控制问题.曹珍富等人[21]在此基础上构建了高效的可追踪、可撤销、多机构的 ABE 方案.具体而言,在可追踪方面,刘振和曹珍富等人[22]给出了第一个同时支持高表达力和抗全合谋黑盒可追踪性的密文策略属性基加密系统,其密文大小达到了目前所知的最好水平,即与系统的总用户数成亚线性关系.在可撤销方面,董晓蕾等人[23]提出了无需授权的可撤销 ABE 方案,引起 Sahai 等人[24]的兴趣,在 2012 年的美密会(CRYPTO 2012)上提出了另一个可撤销属性基加密方案,去掉了撤销列表.在多机构属性基加密方面,刘振和曹珍富等人[25]给出了一个标准模型下适应性安全的多机构密文策略属性基加密方案,其中的任何机构都不能独立解开任何密文,克服了 Waters 等人[26]在欧密会(EUROCRYPT 2011)上的分布式 ABE 工作中"每个机构都能独立解开部分密文"的弱点,彻底解决了属性基加密系统中固有的密钥托管问题.周俊和曹珍富等人[27]还提出了同时具有白盒可追踪、可撤销性质的多机构属性基加密方案,在电子医疗云计算系统中实现了多级隐私保护.近年来,曹珍富等人[28]还提出了自治路径代理重加密算法,实现了对代理路径的高效的细粒度密文访问控制方法.代理者可以按优先权由高到低指定一系列期望的被代理者,使得代理者可以完全控制代理过程以及代理路径的管理.

综上所述,国内外研究学者已对基于属性加密的访问控制方案展开了广泛的研究,但是,已有的研究成果仍然存在用户隐私易泄露的问题.在云环境下一方面由于云是半可信的,可能窃取用户隐私;另一方面,用户对隐私保护的意识和需求不断提升.因此,云环境下支持隐私保护的访问控制方案仍需进一步研究.

3.2 密钥协商协议

密钥协商协议是保证外包数据机密性,支持数据共享、访问控制、数据审计等安全操作的基础密码组件.1976 年,Diffie 和 Hellman 首次提出了密钥协商的概念[29],该工作奠定了公钥密码学的基础.Diffie-Hellman 协议为在公开信道下创建 2 个参与者的会话密钥提供了有效的解决方案,协议的安全性要求仅通信双方可获知会话密钥,其余任何信道监听者都无法知道最终生成的会话密钥,该会话密钥可用于保证通信双方后续通信安全.然而,该协议缺乏认证机制,无法抵抗中间人攻击,此外,该协议仅能支持两方进行密钥协商,无法拓展至多用户场景的密钥协议.此后,大量的研究工作围绕密钥协商协议的安全和性能展开.针对密钥协商过程中的安全问题,Matsumoto 等人[30]对 DH 协议进行了扩展,实现了支持隐式密钥认证的密钥协商协议,保证通信双方能确保对方的真实身份.然而,Law 等人[31]指出该协议无法实现密钥确认的安全需求,并提出了一种可扩展至任意有限群的带密钥确认功能的密钥协商协议.在这段时间内,针对密钥协商协议的安全需求,涌现出相当一部分具有代表性的安全模型.第一个密钥协商安全模型[32]由 Bellare 和 Rogaway 提出,基于该模型定义了密钥协商协议语义安全性,并设计了一个两方带认证的密钥协商协议.此后,Blake-Wilson 等人[33]提出了适用于公钥密码体制下密钥协商的 BJM97 模型.Bellare 等人[34]提出了 BPR00 模型,该模型适用于基于口令的密钥协商协议.Canetti 和 Krawczyk[35]提出了 CK01 模型,该模型定义了目前公认的会话密钥协商安全模型,并且给出了一种证明协议安全的简单模块化证明方法.Lamacchia 等人[36]基于 CK01 模型提出了一种增强的 eCK 模型,该模型保留了原模型能够抵抗密钥伪装攻击的功能,并且允许敌手查询临时私钥和长期私钥等,但是不允许攻击者查询会话内部状态.Cremers[37-38]对 CK 和 eCK 模型进行了详细的比较和分析,并得出 2 个模型间并无强弱好坏之分.针对标准模型下的密钥协商安全性证明问题,高志刚等人[39]基于身份加密,提出了标准模型下可证明安全的基于身份加密方案.王圣宝等人[40]提出了一个标准模型下的基于身份的密钥协商协议.然而,郭华等人在文献[41]中指出该协议需要基于强困难性假设,且不能抵抗扩充的私钥泄漏模仿攻击.近年来,随着在线群组协作的需求增加和大规模共享平台的构建,从两方/三方向多方扩展已经成为密钥协商协议的重要研究方向.一般来说,密钥协商协议主要分为交互式密钥协商和非交互密钥协商.其中交互式密钥协商主要是基于两方/三方密钥协商或者加密方案通过多方交互最终生成会话密钥的过程.协议的效率要求交互过程中的通信开销和交互轮数尽可能的少.非交互式密钥协商的发展则主要依赖于多线性对、不可区分混淆等技术的创新.在非交互式密钥协商领域,自 1976 年 Diffie-Hellman 协议[29]提出以来,直到 2000 年,三方非交互式密钥协商协议才由 Joux 等人[42]提出,该协议基于双线性对实现了三方密钥协商,同时这也是双向性对在密码学上的首次正面地应用.2002 年,Boneh 等人[43]提出了基于多线性对(multilinear pairing)构造多方非交互式

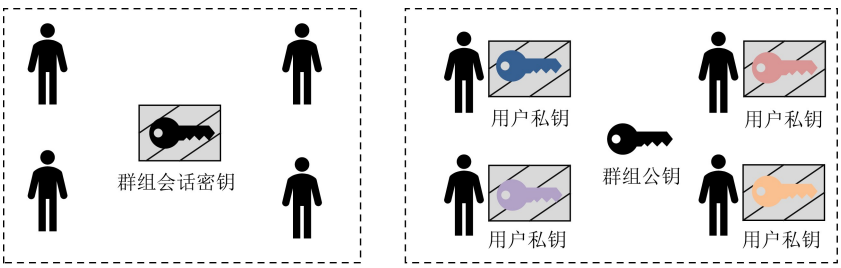
协商协议的思想,然而多线性对的构造在当时依然是一个悬而未决的问题.直到 2013 年,Garg,Gentry 和 Halevi 团队[44]以及 Coron,Lepoint 和 Tibouchi 团队[45]才分别构造出具体的多线性对.然而,由于多线性对较为抽象且实现困难,至今仍没有被应用于实际环境下的多方密钥协商协议.2014 年,Boneh 和 Zhandry[46]在美密会上提出了基于不可区分混淆技术(indistinguishability obfuscation, iO)构造的多方密钥协商协议,相较于多线性对,基于 iO 技术的密钥协商协议不需要初始化操作即可运行.然而,由于混淆程序的设计和运行耗时问题,基于 iO 技术的多方密钥协商也没有被投入实际应用.

不难看出,非交互式密钥协商发展缓慢,现有安全模型也大都针对交互式密钥协商协议提出,难以直接适配非交互式密钥协商的安全性证明.此外,现有基于多线性对或者 iO 技术的密钥协商协议仍难以投入实际应用.非交互式密钥协商具备优越的性能,因此如何构建适用于非交互式密钥协商的安全模型,设计实用的数学工具以实现安全高效的非交互式多方密钥协商协议是密钥协商发展中亟待解决的问题.在交互式密钥协商领域,根据协商交互模型的组织结构,可以将其分为环形模型、分层模型和广播模型的协议.Ingemerson 等人[47]基于 Diffie-Hellman 协议,设计了密钥协商的环形交互模型,将协商人数扩展至多方.然而,该协议基于较弱的安全模型,导致协议仅能抵抗具有窃听功能的敌手.Atenise 等人[48]在多方密钥协商协议中引入了认证功能,并对主动攻击进行了启发式的安全分析.Steiner 等人[49]考虑了组成员增减变动、更新等不同情况,提出了一个支持用户动态变动的多方密钥协商协议.以上方案都采用启发式的分析方法对主动攻击行为进行分析,缺少严格的安全性证明,在真实环境下,不可避免地存在很多潜在的安全威胁.

Kim 等人[50]基于两方密钥协商,提出了一种基于二叉树结构的交互模型,并基于此设计了多方密钥协商协议,基于二叉树的灵活性,该协议可以很好地支持用户的变动.然而,该协议仅对协议的安全性进行了启发式的证明.Nalla 和 Reddy[51]基于二叉树交互模型中引入认证技术,设计了可认证的多方密钥协商协议.Barua 等人[52]结合 Joux 三方密钥协商协议[42],设计了基于三叉树结构的交互模型,并在此基础上提出了一种基于三叉树交互模型的多方密钥协商协议.然而,该协议不提供认证功能.王志伟等人[53]也提出了一种基于树结构和门限思想的组密钥协商协议,但是该协议具有较大的计算开销.Burmester 和 Desmedt[54]提出了一个非认证组密钥协商协议该协议的优点是密钥协商过程只需 2 轮通信,并且能够抵抗外部节点的假冒攻击,但是该协议需要一个认证广播信道且无法抵抗内部恶意节点的攻击.Bresson 等人[55]提出基于口令的组密钥协商协议,然而,此协议所需的交互轮数与参与通信的用户总数量成线型关系.2006 年,Damiani 等人[56]提出了选择性加密和分级密钥分配的概念,以此来实现密钥的管理.2010 年,Blundoa 等人[57]提出了一种启发式的密钥管理方案,大大减少了用户访问控制所需的认证密钥数量.为了降低用户认证的成本,启发式方案利用最小生成树进行密钥优化.然而,该方案不能实现用户密钥的更新.2014 年,Odelu 等人[58]提出了一种基于对称密钥体制和单向散列函数的动态密钥管理方案.该方案可以实现对安全类的添加、删除和更改操作.在上述方案的基础上,Hong 等人[59]提出了一种基于中国剩余定理的分层密钥管理方案,该方案可以管理用户访问外包数据的权限,同时也可以降低密钥更新的成本.

近来在交互式密钥协商协议方面的工作大都集中在对协议性能的改进上和对功能的增加上.毛江栋等人[60]、陈海红等人[61]、曾继强等人[62]对基于三叉树结构的密钥协商协议进行改进,引入椭圆曲线加密技术并设计成员管理机制,实现了改进的支持成员动态变化的群组密钥协商.2016 年,陈勇等人[63]基于零知识证明技术,设计了一种可否认群密钥协商协议,实现了密钥协商过程中的隐私保护.Teng 等人[64]在密钥协商协议中引入矩阵论,有效支持协商过程中用户动态变化问题,然而,该协议交互信息量较多,计算和通信开销较大.方亮等人[65]基于秘密共享技术,提出了无需在线可信第三方的密钥协商协议.然而,该协议需要较大的计算和通信开销.邓淑华等人[66]基于 ElGamal 体制,提出了一种安全组播密钥管理方案,提升了组密钥管理的可扩展性,然而,该协议基于集中式模型,存在单点失效以及成员贡献失衡问题.为了平衡多方密钥协商协议所需的通信开销、交互次数和协议功能性.2009 年,Wu 等人[67]在欧密会上提出了一种非对称群组密钥协商协议(asymmetric group key agreement, ASGKA),平衡了非交互式密钥协商难以实现以及交互式密钥协商轮数偏高,安全性不足等问题.该协议基于可聚合签名广播密码原语实现了多方单轮群组密钥协商,该协议执行效率高且在 n-BDHE(n-bilinear diffie-

hellman exponentiation, n-BDHE)假设下是可证明安全的.ASGKA 密钥协商模型和传统多方密钥协商模型如图 5 所示,在传统多方密钥协商协议中,每个群组成员协商完成后将生成一个群组会话密钥,该密钥需要保密以保证后续通信安全,ASGKA 协议中,协商完成后每个群组成员将生成各自的用户私钥(群组私钥)和一个群组公钥,每个成员所持有的不相同的用户私钥可以解密群组公钥加密的信息.ASGKA 协议相较于传统群组密钥协商协议具备无需管理员参与(dealer-free)、密钥自认证(key self-confirmation)、恶意参与方识别(identification of disruptive principals)等优势.然而,通过该协议得到的群组公私钥需要基于公钥加密实现安全通信,其运行效率将低于传统群组密钥协商得到的对称密钥.此外,该协议具备密钥同态的特性,若存在恶意参与者,则会导致协议受到共谋攻击.谢涛等人[68]研究了 ASGKA 协议[67]中的共谋攻击问题,定义了非对称群组密钥交换的叛逆追踪性,并严格证明了具备密钥同态性质的非对称密钥协商协议中合谋者构成的集合满足非模糊性导致合谋者是不可追踪的.2019 年,Shen 等人[69]创新了会话密钥的协商方式,定义了基于对称平衡不完全区组设计(symmetric balanced incomplete block design, SBIBD)的负载均衡、通信轻量的多播协商模型.设计了(7,3,1)-SBIBD 结构多方密钥协商协议并进一步根据 SBIBD 的结构特性,构造 SBIBD 的通用数学表达,设计 SBIBD 结构转换算法,使其适用于离散多方密钥协商协议,该结构转换算法如图 6 所示.



(a) 传统密钥协商模型 (b) ASGKA密钥协商模型

Fig. 5 The model of ASGKA protocol and the traditional key agreement protocol

图 5 ASGKA 密钥协商模型和传统多方密钥协商模型

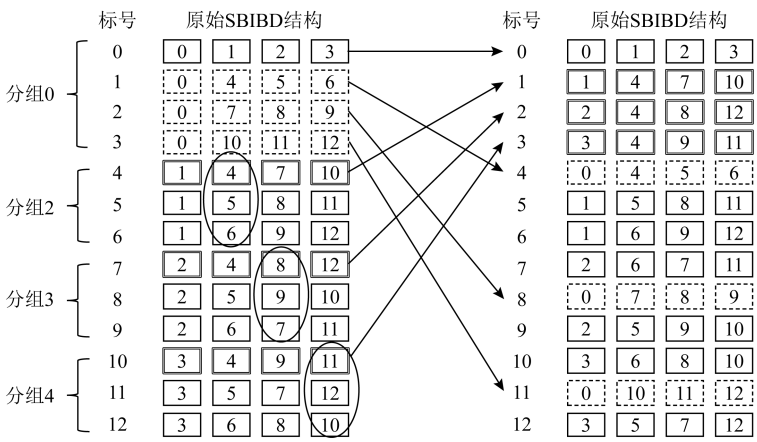


Fig. 6 The transformation algorithm of the SBIBD structure

图 6 SBIBD 结构转换算法

进一步地,Shen 等人[69]突破其结构局限,创新地引入“volunteer”参与密钥协商协议,适应性地将参与协议的用户数量扩展到任意多人,最终实现了多方数据共享的全用户域可扩展,验证了密钥协商过程中应用 SBIBD 的理论可行性,为任意数量用户的密钥协商提供理论支撑.所提出的多播协商模型执行过程仅需 2 轮交互.具体来说,对于参与用户数量为 n 的密钥协商协议,传统的密钥基于环形(线型)和树型交互模型的密钥协商协议,所需的交互轮数分别为 n 和 $\log_3 n$,且存在群组成员对会话密钥贡献失衡的问题.基于 SBIBD 的交互模型仅需 2 轮交互,通信复杂度从 $O(n^2)$ 降至 $O(n\sqrt{n})$.最终,

构建了第一个基于 SBIBD 的多方密钥协商协议,显著提高了密钥协商协议的执行效率,当用户数量为 100 时,协议的执行效率提高超过 70%.

不难看出,国内外研究学者已在密钥协商相关领域做出了一系列有益的探索,在两方密钥协商领域已提出很多经典的方案并投入实际使用.在多方密钥协商领域,针对交互式多方密钥协商的交互计开销和协议安全性已展开了大量研究.然而,面对新环境如区块链、大数据、云环境等应用领域,支持隐私保护、分层管理、高效更新等需求的新型交互式多方密钥协商协议仍有待研究.在非交互式多方密钥协商领域,高效实用的非交互式多方密钥协商协议的设计依赖于适用的具备如有限域上的离散对数、椭圆曲线上的离散对数陷门性质的数学工具的开发.

3.3　安全审计

外包数据的完整性是云存储的基本需求,该属性是可供数据所有者参照的反映外包数据安全的直接参数.

当数据以密文形式存储在服务器中时,数据的直接可用性会降低,并且为用户端对数据的存储完整性验证带来了困难.为了解决上述问题,出现了大量针对密文数据完整性验证的研究成果[70-74].2007 年,Ateniese 等人[75] 首次提出了公共审计方案,该方案定义了"公共审计"的概念,并提出了"概率性审计"的思想极大地降低了审计的计算和通信开销.具体来说,在 1%的数据被损坏时,该方案仅需取样数据文件 4.6%的数据块即能以 99%的概率检测到数据的损坏.由于不需对整个数据文件进行审计,该方案对大小为 768 KB 的文件进行审计的开销较传统方案提升了 185 倍.

2007 年,Sebé 等人[76] 基于 Diffie-Hellman 协议设计了一种可支持随机数据块存储检查的数据持有性验证协议,使得用户可在无需取回全部数据的情况下对数据的完整性进行验证.随后,为了提高数据完整性验证结果的可信度和公平性,一些学者通过引入一个可信第三方(third party auditor, TPA)设计了一种可支持公共审计的数据存储审计协议.Wang 等人[77] 提出了一个公共云数据审计协议,该协议基于密码学中的同态消息认证码和随机掩码技术支持审计过程中的用户隐私保护.为了在审计中实现数据动态操作,Wang 等人[78] 通过在审计协议的设计中引入 Merkle-Hash-Tree 技术,使得审计协议可支持数据动态操作.2013 年,Zhu 等人[79] 设计了一种基于索引哈希表的审计方案,相较之前的协议而言,该方案的计算和通信开销都有所减少.但是,鉴于该协议中所采用的索引哈希表是一种顺序表,按照顺序表的属性,当遇到插入、删除等会改变索引哈希表结构的动态操作时,该协议开销仍然较大,不适用于数据的动态操作.2015 年,Liu 等人[80] 基于再生码技术(regenerating codes)提出了一种支持容错性和故障修复功能的数据审计方案,该方案解决了审计过程中要求数据所有者实时在线的问题,降低了数据拥有者的在线负担.然而,该方案中数据所有者委托的代理可以伪造任何数据块的身份验证器,导致该协议并不安全.2018 年,He 等人[81] 针对云辅助无线体域网环境下(wireless body area networks, WBANs)资源受限问题,提出了一种高效的无证书公共审计(certificateless public auditing, CLPA)方案,解决了审计协议中的密钥管理和密钥托管问题,能够抵御传统基于身份(identity-based, ID-based)和基于公钥密钥体制的审计方案中的Ⅰ型敌手和Ⅱ型敌手,其中Ⅰ型敌手具备替换用户公钥的能力,Ⅱ型敌手具备访问主密钥的能力.

另一方面,共享数据审计是验证共享数据完整性的重要方案.在云存储服务中,由于数据的所有权和数据的控制权分离,使得共享数据的完整性成为用户使用云存储最大的担忧.共享数据审计方案有效实现云数据完整性的验证,保障了共享数据的完整性.已有的共享数据审计协议,多采用基于线性同态认证子技术进行实现,但这些协议都基于复杂的密钥管理,通常采用 PKI 基础设施管理密钥,证书的生成、存储、撤销、更新是很昂贵的操作,复杂的密钥管理导致协议在具体实施时效率不高.针对共享数据审计的效率不高问题,Yu 等人[82] 提出了一系列具备简化密钥管理的云数据完整性审计模型,包括基于身份的云数据完整性审计协议、基于生物特征的云数据完整性审计协议等.正规化了这些新型协议的系统模型、安全需求和安全模型,并提出可证明安全的一系列协议.方案中提出基于身份的云数据完整性审计协议系统模型,给出其安全性定义,该系统模型能有效抵抗恶意的云服务器、防止对第三方审计者泄露信息.

结合基于身份的签名方案及非对称群组密钥协商技术,给出基于身份的云数据完整性审计协议的具体构造,其中挑战响应协议由第三方审计者与云服务器进行协商完成,在生成共享密钥时必须包含挑战块,并在一般群模型下证明基于身份的云数据完整性审计协议的安全性.通过原型系统执行云数据

完整性审计协议,性能分析表面随着挑战块数的增加,时间开销呈递增趋势,当挑战 460 块时,验证者验证响应只需花费 3.0 s,服务器生成响应花费 0.7 s.这一协议提升云数据审计协议安全性的同时满足实用性需求,为共享数据审计提供了有效的解决方案.

共享数据审计协议使得验证者无需下载数据能够有效检查数据的完整性.但现有的数据审计协议的密钥管理相对复杂,为解决复杂的密钥管理这一挑战,Li 等人[83]在共享数据完整性审计中引入模糊身份认证机制,结合现实应用,将用户生物特征(如指纹、虹膜)作为模糊身份进行数据完整性审计,提出基于生物特征的云数据完整性审计协议,形式化定义其系统模型和安全模型,如图 7 所示,并给出基于生物特征的云数据完整性审计协议架构.其主要包含 3 个阶段:1)注册.采用专用设备(如指纹扫描仪)采集用户生物特征,提取特征向量,生成用户私钥;2)存储.用户对元数据进行预处理,生成文件标签及认证子;3)审计.根据挑战-响应算法,审计数据完整性.结合模糊身份加密思想与门限秘密共享方案,给出具体的基于生物特征技术的模糊身份云数据完整性审计协议,其有效保障数据完整性,同时提供了有效容错性,当且仅当 2 个身份足够接近时,其中一个用户身份可以验证对另一身份响应的正确性.借助可证明安全理论,在选择身份安全模型下证明协议基于计算 Diffie-Hellman 假设和离散对数假设的安全性.通过原型系统部署基于生物特征的云数据完整性审计协议,当挑战 300 个数据块,第三方审计者需要 0.997 3 s 进行验证和服务器花费 9.071 s,而当挑战 460 个数据块,第三方审计者花费 1.324 s 和服务器 12.938 s.协议实现模糊身份审计功能,同时满足有效性及实用性.数据审计的相关模型和协议等成果已被同行推广至数据动态操作、多副本数据持有性证明、数等场景.

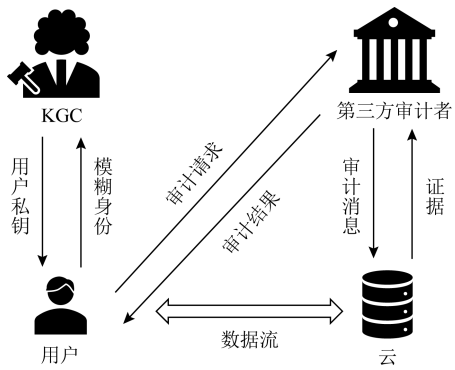


Fig. 7 The system model of fuzzy identity-based data integrity auditing protocol.

图 7 基于模糊身份的云数据完整性审计协议系统模型

针对当前的研究工作中,防篡改、防泄露的云审计协议无法解决更新数据操作复杂、定位数据位置耗时等问题,导致计算资源占用过度、审计效率低下,难以满足云数据在共享过程中即时验证的需求.Shen 等人[84]定义了一种新型的双向链式信息表(doubly linked info table),如图 8 所示,有效地解决了云存储服务中数据块物理位置与索引号之间存在的映射问题,在不引入额外开销的前提下更好地支持了数据的动态更新.同时,提出了面向云数据安全共享的双向链式审计协议,支持低开销、高效率的云

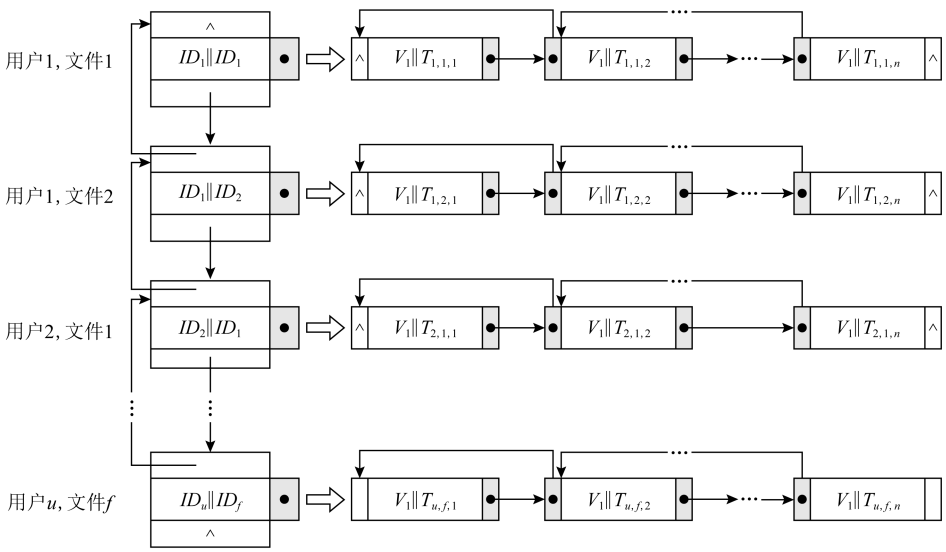


Fig. 8 Doubly linked info table

图 8 双向链式信息表

数据动态操作和批量审计,提供公开、无块验证,从而有效防止云中的数据(特别是涉及隐私的数据)被验证者窃取.实验表明:在审计 20 000 个数据块时,相较于传统的基于动态哈希表结构的审计协议,数据更新效率、数据审计效率均提高 150%.

不难看出,国内外研究学者已在数据审计方面展开了较为充分的研究.但是,已有的研究成果动态操作效率低下,在完整性和正确性的监测、检验,以及数据的可用性的保障等方面仍有所欠缺.此外,目前少有合适的数据审计协议能在精确定位的前提下实现数据恢复.

3.4　安全共享

数据安全共享作为云计算的重要应用受到了国内外学者的广泛关注,产生了大量的研究成果.目前国内外在数据安全共享领域的研究成果颇丰.代理重加密(proxy re-encryption, PRE)技术能让数据拥有者将加密数据的解密权限委托给授权接收者而无需直接交互[85-90].

传统的公钥密码学和身份密码学(identity-based cryptography, IBC)方案分别在证书管理和密钥托管方面存在问题.2012 年,Xu 等人[91]在文献[92]的基础上,提出一种无证书 PRE 方案以克服密钥托管问题.2013 年,Liu 等人[93]针对数据共享过程中的用户动态变化问题,基于动态广播加密和群签名技术,提出了一种用户可撤销的云数据共享方案.该方案中,组管理员维护一张记录用户撤销列表(revocation list, RL)如表 2 所示,其中,ID_{group} 为群组标识符,三元组(A_i, x_i, t_i)表示用户 i 在 t_i 时刻被撤销,P_i 为群组管理员使用主私钥和群 G_1 上的随机元素计算得到,其余参数 Z_r,t_{RL},$sig(RL)$为撤销列表相关参数.基于撤销列表可判断用户的合法性,实现高效的用户撤销操作.然而,随着撤销用户的增多,撤销列表的管理和查询将影响组管理员和用户数据共享的效率.此外,该方案易遭受云和撤销用户的共谋攻击,将导致被撤消的用户获得共享数据并泄露其他合法成员的秘密.2015 年,李继国等人[94]在 CP-ABE 方案的基础上提出了保护隐私且支持用户撤销的属性加密方案.2016 年,Lu 等人[95]构建了一个无双线性对的 CB-PRE 方案,但该方案的安全性只能在随机预言机模型中得到证实.因此,在标准模型中构造无双线性对的 CB-PRE 方案将是可探究的方向.2017 年,Li 等人[96]提出了一种移动用户端基于属性的数据共享方案,该方案通过使用变色龙哈希函数产生即时密文的方法实现了移动用户间的安全数据共享,然而,其尚未对用户属性的直接撤销展开研究.

Table 2　Revocation List

表 2　撤销列表

用户参数	用户私钥	撤销时间	更新参数
A_1	x_1	t_1	P_1
A_2	x_2	t_2	P_2
⋮	⋮	⋮	⋮
A_r	x_r	t_r	P_r

2017 年,Shen 等人[97]针对现有数据共享方案的设计多专注于一对多的共享模式,限制了数据交互的灵活性,且存在难以追踪数据来源,易于遭受共谋攻击等问题,无法保证安全高效的匿名抗共谋数据共享.突破匿名抗共谋数据共享的传统设计观念,设计了特殊结构的组公钥,生成专属标签,用于匿名标记及用户追踪;借助群密钥构建组内/组间通信框架,减少冗余的授权操作;合理定义系统参数更新方式,提高密钥生成的安全性,如图 9 所示.此外,在可追踪、抗共谋数据共享算法的基础上,设计了容错检测机制,如图 10 所示,有效保护了数据共享的安全高效执行.具体地说,在初始化期间,每个成员需向组管理员提交一个关于子密钥的承诺.在密钥协商之后,组管理员在所有成员之间广播消息已验证会话密钥的一致性.若有成员发现不一致,则其将向组管理员提交一份错误报告,此后,组管理员先根据发送错误报告用户的承诺验证该用户的合法性,若用户合法,则其余所有成员都将进行错误检测以抵御差别密钥攻击.

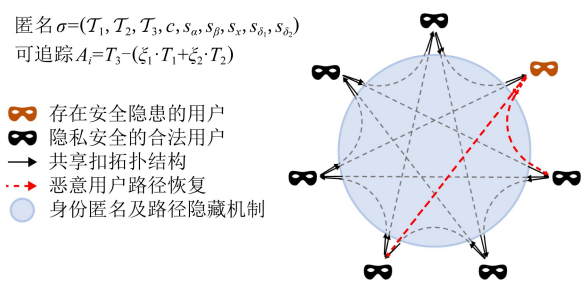


Fig. 9　Traceable and collusion-resistant data sharing model

图 9　可追踪、抗共谋数据共享模型

2019 年,Shen 等人[98]针对共享过程中敏感信息易暴露的问题,提出了一种远程数据完整性审计方案,方案中用户将与原始文件的个人敏感信息相对应的数据块隐藏起来,并生成相应的签名,然后将

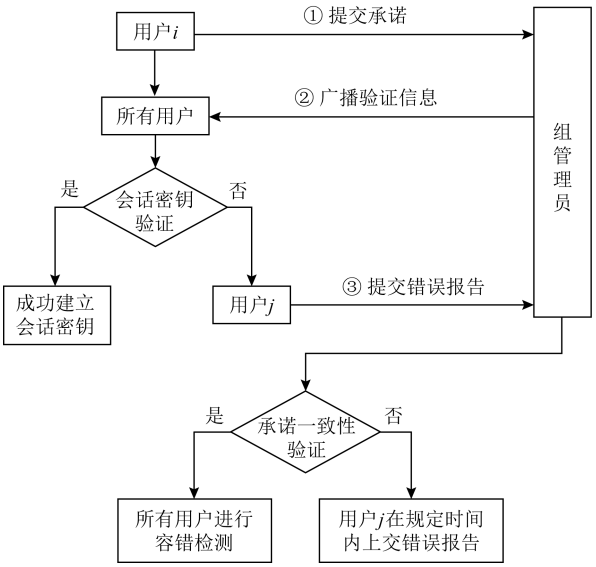


Fig. 10 Fault-tolerant detection mechanism

图 10 容错检测机制

其发送给清理程序.清理程序将这些隐藏的数据块清理为统一格式,并且还清理了与组织的敏感信息相对应的数据块.它还会将相应的签名转换为已清理文件的有效签名.该方案实现了远程数据完整性审计,同时支持在云存储中保护敏感信息的情况下进行数据共享.同年,Wei 等人[99]针对个人电子病历共享过程中的隐私保护问题,考虑了外包个人医疗数据强安全性和特定的安全需求,具体来说为了增强系统安全性并满足特定应用的需求,在基础 ABE 方案中引入用户撤销,秘密密钥委派和密文更新机制,并提出了基于可撤消存储分层属性的加密(revocable-storage hierarchical attribute-based encryption, RS-HABE)方案.所提出的 RS-HABE 方案同时具有前向安全性(被撤消的用户不能再访问以前的加密数据)和后向安全性(被撤消的用户也不能访问后续的加密数据),并且在双线性困难性问题假设下能够达到选择性安全.

2020 年,Pu 等人[100]针对边缘计算数据共享过程中的隐私泄露问题,提出了一种隐私保护、可恢复和可撤销的边缘数据共享方案.该方案设计了一种基于区块链的属性撤销链,实现了 CP-ABE 方案中的属性撤销.同时,针对单个 ES 被劫持的情况,引入了秘密共享方案辅助数据恢复.此外,该方案提出了相应的高效检测机制和密钥更新策略,以保证方案的安全稳定运行.同年,Huang 等人[101]针对现有数据共享研究仅考虑同组用户共享的问题,提出了一种基于区块链的数据共享方案有效支持多组协作数据共享.该方案基于联盟区块链技术,在无需 TPA 参与的情况下实现了共享数据的高效和公共验证.此外,该方案可以支持用户的匿名性、可追溯性和不可陷害性.

此外,还有一系列工作针对密文计算结果的安全数据共享开展研究.国内外现有做法是利用公钥全同态加密技术,在计算结果接收方的公钥下对每一个数据进行全同态加密,从而使得授权的接收方能用其私钥正确解密明文计算结果.2009 年,Gentry 等人[102]首次提出了公钥 FHE,他们先构造了 SWHE 方案,并使它可引导.然而,基于 Gentry 等人[102]的公钥全同态加密方案需要对明文消息逐比特加密,计算开销非常巨大,所以无法直接用于边缘计算底层资源受限的本地设备.Halevi 等人[103]建立了一个名为 HElib 的 FHE 算法库,以实现全同态加密系统和自引导方法.Chen 等人[104]利用重线性化技术和密文打包技术,基于门限全同态加密算法提出了多密钥全同态加密算法,并将其应用于密文域的神经网络训练与预测.虽然上述国内外关于公钥全同态加密(FHE)的工作取得了一定成效,但其高计算、存储和通信开销仍然无法满足边云数据安全计算和安全共享中资源受限的本地设备的客观性能需求.近年来,周俊和曹珍富等人[105-106]不依赖公钥全同态加密,通过减少公钥加密使用次数,提出了单用户多数据轻量级隐私保护外包计算新方法,实现了云计算系统中高效的可验证隐私保护模式匹配协议;同时将该方案进一步扩展到多用户多数据场景,基于常数次任意单向陷门置换提出了轻量级的多密钥全同态映射数据封装机制,其中的单项陷门置换可用基于身份加密、基于属性加密及抗量子攻击的公钥加密算法进行实例化,从而实现不同场景下为满足多种安全性及应用需要设计的安全数据共享协议.

综上所述,研究人员已经对安全数据共享相关技术做出了大量探究,但是已有的基于属性的数据共享方案不能较好地解决用户属性撤销的问题.同时,在数据共享方面仍没有完整的代理重加密方案能够同时在标准模型中支持密钥更新、抵御撤销用户的共谋攻击和降低服务器开销.

4 总结与展望

从国内外研究动态的分析可知,云环境中的数据保护已经引起了国内外学者长期广泛的关注,取得了很多研究成果,但现有研究还存在 4 个主要问题:

1) 现有的访问控制方案中都需要授权中心的参与,授权中心在整个访问控制中起到至关重要的作用.然而,对授权中心的过度依赖也限制了这一类方案的使用,可能导致用户隐私泄露.同时,基于属性加密的访问控制方案无法抵抗共谋攻击,缺乏对云存储准入控制的安全性保护.因此,研究隐私保护且具备抗共谋机制的云数据访问控制方案具有重要的理论和实践意义.

2) 现有交互式多方密钥协商协议存在结构单一偏大等问题,且安全性证明不完善.另一方面,目前虽然已有将 iO 技术和多线性对技术应用于非交互式多方密钥协商协议的设计中,但协议的运行开销较大难以投入使用,且安全性尚不明确.因此,研究新型结构以降低交互式多方密钥协商协议的通信开销,优化协议性能,开发实用数学工具以支持非交互式多方密钥协商协议的高效实现将是多方密钥协商领域亟待解决的问题.

3) 现有数据审计方案存在隐私易泄露、错误定位精度较低、恢复困难等问题.因此,如何在保证审计正确性和效率的基础上保护用户隐私,如何在发现错误后支持高精度错误定位以及有效的数据恢复是数据审计协议领域值得研究的方向.

4) 现有的数据共享方案无法较好地支持用户撤销和新增等动态操作,且存在成员动态管理开销偏大、难以追踪恶意用户的问题.同时,现有数据共享方案容错性不足,恶意用户的参与将导致共享失效.因此,研究支持群组动态操作,设计容错可追踪机制是云数据共享领域值得进一步研究的方向.

4.1　总　结

本文从云数据安全的访问控制、密钥协商、安全审计和安全共享 4 个方面出发,对国内外云数据安全保护方案的最新研究成果进行系统分析.从密码学的角度出发,总结出现有云数据安全保护方案涉及到的相关密码原语、技术,如图 11 所示,并对其进行深入分析:

1) 在访问控制方案研究中既要保证只有合法

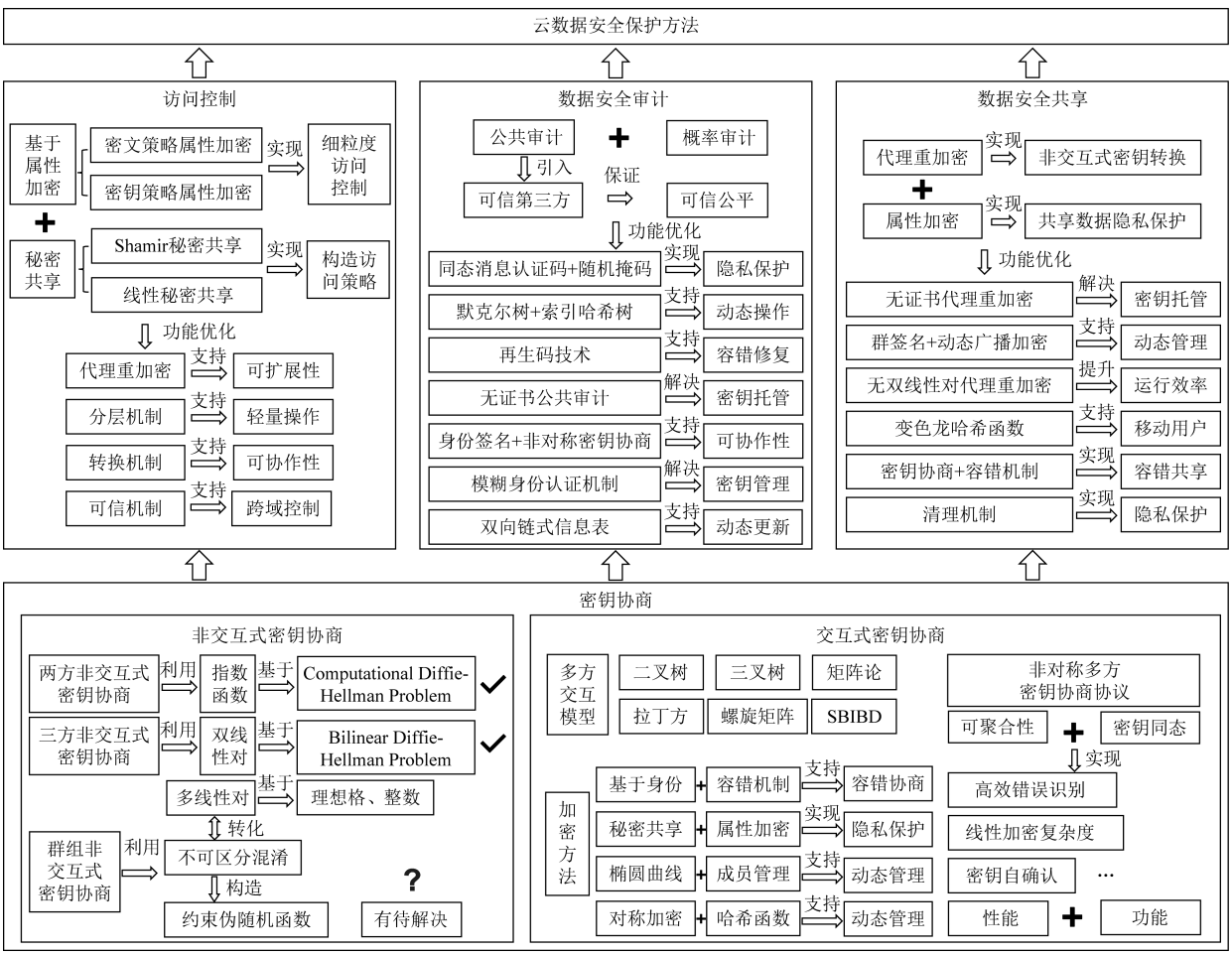


Fig. 11　Data security in cloud computing and the related cryptographic technologies

图 11　云数据安全保护方法及相关密码技术

用户才可访问数据,又要保护合法用户隐私.由此,基于属性加密是实现隐私保护访问控制的较好选择.一般来说,属性加密机制中的访问控制结构可基于秘密共享方案构造实现,常用的有 Shamir 秘密共享和线性秘密共享方案.在此基础上,可通过引入代理重加密、分层机制、转换机制、可信机制等支持访问控制过程中的可扩展性、轻量操作、可协作性、跨域控制等功能.

2) 在数据安全审计方案设计中,首先需要保证公共审计和概率审计的特性,同时引入可信第三方保证审计结果的公平可信.在此基础上,基于同态消息认证码、随机掩码、默克尔树、索引哈希树、再生码、身份签名、非对称密钥协商、双向链式信息表等支持审计中的隐私保护、动态操作、可协作性、动态更新等特性,基于无证书密码体制和模糊身份机制解决审计中的密钥托管和密钥管理问题.

3) 在数据安全共享方案设计中主要基于代理重加密技术和属性加密技术实现共享数据密钥的高效转换和保护共享数据隐私.在此基础上利用群签名、动态广播加密、无双线性对密码体制、变色龙哈希函数、多方密钥协商、容错机制、清理机制等支持数据共享过程中的动态管理、移动用户、容错共享、隐私保护,并基于无证书密码体制解决数据共享过程中的密钥托管问题.

4) 在密钥协商方案的设计中主要分为非交互式密钥协商和交互式密钥协商,其中非交互式多方密钥协商目前仅有两方和三方非交互式密钥协商具有实用价值,大于 3 人的非交互式密钥协商方案需要利用多线性对、不可区分混淆、约束伪随机函数等技术.多线性对和不可区分混淆可以相互转化,同时这两者可用于构造约束伪随机函数.然而,目前多线性对需要基于理想格或整数进行构造,安全性难以证明且效率较低.交互式密钥协商的设计主要基于多方交互模型和交互过程中使用的加密方法.交互模型主要包括二叉树、三叉树、矩阵论、拉丁方、螺旋矩阵、区组设计;加密方法主要有基于身份加密、属性加密、椭圆曲线加密、对称加密等并可在此基础上引入容错机制、秘密共享、成员管理、哈希函数等实现或支持协商过程中的容错协商、隐私保护、动态管理.此外,为了平衡多方的功能需求和协议的运行性能,非对称多方密钥协商协议基于可聚合性和密钥同态的特性实现了高效地多方密钥协商并可支持高效错误识别、线性加密复杂度、密钥自确认等功能.

4.2 展 望

立足于国家“建设国家数据统一共享开放平台,保障国家数据安全,加强个人信息保护”的战略需求,云数据安全保护方案的未来发展方向主要包括 3 个分支.

1) 可信认证模式的统一

实现云数据安全访问的前提条件是对各类不同来源、不同类型数据的可信认证.现阶段云数据访问控制在隐私保护、可信评估和来源认证等方面已经积累了一定的经验和基础,取得了一定的研究成果,然而目前成果缺乏针对数据复杂异构场景的特殊化模式设计.因此,为了云数据安全访问控制,推动云技术的进一步应用,迫切需要实现不同来源、不同类型数据认证模式的统一,其具体内涵包括:

①推进不同来源、不同类型数据结构归一化,打破跨域访问控制的壁垒.②推进数据可信评估标准统一,完善云数据可信评估体系.保障数据来源可信是确保数据真实合法的前提条件.然而,现有的评估指标体系构建不完善,评估标准不一,无法对云数据的可信度进行系统科学的评估和决策.因此,迫切需要针对云数据复杂异构特点,实现可信评估标准统一,并在此基础上引入深度学习技术,建立智能化的云数据可信评估模型.③推进数据拥有者身份去特征化隐藏,确保云数据的隐私保护.云数据多涉及个人隐私乃至国家机密,对数据隐私保护提出更高要求.因此,迫切需要对数据拥有者进行身份去特征化隐藏,保证其行为的匿名.

2) 安全传输技术的创新

数据安全传输技术是云数据安全交互的重要保证.目前,密钥协商、数字签名、签密等关键的密码原语在其发展和实践过程中已趋于成熟,能够保障基本的数据传输安全,然而,现有关键密码原语的代表算法和解决方案多为国外组织或团队设计发明,且其具体的设计结构、对接方法和关系映射缺少针对云数据安全交互场景的具体实践性创新.因此,目前云数据安全交互所用传输技术如何实现交互模型结构、传输对接模式及地址映射关系上的演进创新是值得研究的方向,其具体内涵包括:

①创新多方密钥协商交互模型结构,提高云数据交互对象间的协商交互效率.云数据互通涉及大规模、多方并行的数据交互实际需求,现有的研究成果交互模型构建复杂、群组结构单一固化、用户交互轮数偏高、通信开销偏大,传输所需密钥生成效率无法得到保障.因此,迫切需要在数据传输初始阶

段,结合组合数学等跨学科基本理论方法,优化多方交互结构,构建具有普适性的多方密钥协商模型,为云安全互通传输提供密钥保障.②创新轻量数据安全传输对接模式,实现数据传输方法的自适应切换.云数据安全互通囊括多种应用场景,现有的数据传输方式单一,难以满足用户多场景下数据传输的实际需求,限制了云数据传输过程中数据相关群体间对接的灵活性.因此,迫切需要在数据传输中进行自适应签密算法的设计,为丰富和创新云数据交互对接模式创造条件.③创新云数据储存地址映射关系,保障用户动态操作数据的痕迹隐藏.现有的数据存储方案能够在一定程度上保证数据的存储和安全需求,然而,多数存储方案存在动态操作繁杂、算法时间复杂度偏大、存储痕迹易泄漏、资源利用率低下、访问模式单一等问题,数据外包存储服务提供商缺乏进一步保障数据拥有者、使用者隐私安全及数据存取效率.因此,迫切需要在云数据传输至外包服务器进行存储的过程中设计全新的无痕化地址序列映射关系,为后续云数据安全共享提供数据保障.

3) 安全共享组件的创新

实现数据安全共享是云数据的重要应用.当前云数据应用在目标选取、公共审计、数据聚合等重要组件方面已经积累了一定的经验和基础,然而这些组件多依附于全球先进的安全算法进行设计,且缺乏云数据安全共享场景下实际急需的隐私匹配、数据恢复、同态分析以及容错共享等特性.因此,目前云数据现行的共享组件如何实现功能性跃迁是具备应用前景的发展方向,其具体内涵包括:

①落实用户隐私数据细粒度匹配,保障隐私保护的共享对象的精准定位.现有的数据共享研究工作能够定位共享对象,但是,少部分实现细粒度的算法不能兼备可验证、防泄漏、抗共谋等安全性质,共享的对象往往在确认过程中需要牺牲其部分数据的私密性,阻碍了云数据共享过程中对用户隐私的可靠保护.因此,需要在数据共享中进行支持隐私保护的细粒度目标匹配,保证云数据可靠互通共享中的数据服务提供对象享有合理的隐私权.②强化共享云数据审计过程中的可恢复特性,确保重要的共享数据因不可抗力损毁后能够极大程度地挽回所造成的损失.现有的数据共享方案能够对数据实现一定程度的完整性校验,然而,执行效率无法满足实际需要且不支持损毁数据的恢复,共享机制的防灾抗毁能力较弱,难以为云数据共享提供可靠的审计服务.因此,需要在数据共享中实现可恢复的公共审计,为云数据安全共享体系的预防性抗毁能力构筑重要基石.再次,贯穿用户数据聚合的同态特性,进一步保护数据拥有者、数据使用者的隐私.现有的数据共享方案能够完成实验室场景下的单一目标数据聚合,但是,多数聚合策略存在操作单一、隐私易泄漏和难以抵抗共谋攻击等问题,无法为敏感多级数据的合法拥有者和使用者提供完善的隐私信息保护,限制了数据相关人员隐私的可靠保护力度.因此,需要在数据共享中进行同态的数值计算,为云数据安全共享中的数据统计、分析提供支持隐私保护的方法.③建立多对多共享的隐私保护——可容错协同防御机制,增强共享技术在内外攻击下的功能完备.现有的数据共享方案能够保障单一链路的投递实现,然而,多对多共享模式的容错性不足,数据交互灵活性差,且存在用户隐私易泄漏、共享过程中易出错等问题,无法为云数据安全共享提供可靠的服务.因此,需要在数据共享中引入约束伪随机函数、门限秘密共享等密码组件,构建隐私保护——可容错协同防御机制,为云数据安全共享中完备的“内防外抗”提供技术支撑.

参　考　文　献

[1] 腾讯安全云鼎实验室. GeekPwn. 2019 云安全威胁报告[R/OL]. 腾讯安全, 2019[2021-01-15]. https://cloud.tencent.com/developer/article/1562051

[2] Ma Jinhua, Huang Xinyi, Xu Junpeng, et al. Public accountable redactable signature scheme [J]. Journal of Electronics & Information Technology, 2020, 42(5): 1079-1086 (in Chinese)
(马金花, 黄欣沂, 许俊鹏, 等. 公开可审计的可修订签名方案[J]. 电子与信息学报, 2020, 42(5): 1079-1086)

[3] Wang Lei, Li Gang, Wang Feiyu. Cloud computing security access control strategy based on improved attribute encryption combined with proxy re-encryption [J]. Computer Applications and Software, 2019, 36(7): 327-333 (in Chinese)
(王磊, 李刚, 王斐玉. 改进属性加密结合代理重加密的云计算安全访问控制策略[J]. 计算机应用与软件, 2019, 36(7): 327-333)

[4] Xu Guangwei, Bai Yanke, Yan Cairong, et al. Check algorithm data integrity verification results in big data storage [J]. Journal of Computer Research and Development, 2017, 54(11): 2487-2496 (in Chinese)
(徐光伟, 白艳珂, 燕彩蓉, 等. 大数据存储中数据完整性验证结果的检测算法[J]. 计算机研究与发展, 2017, 54(11): 2487-2496)

[5] Tian Hongliang, Zhang Yang, Li Chao, et al. A survey of confidentiality protection for cloud databases [J]. Chinese Journal of Computers, 2017, 40(10): 2245-2270 (in Chinese)
(田洪亮, 张勇, 李超, 等. 云环境下数据库机密性保护技术研究综述[J]. 计算机学报, 2017, 40(10): 2245-2270)

[6] Ke Changbo, Wu Jiayu, Cao Yan. Research on oriented application layer evolution privacy protection method in cloud computing [J]. Computer Engineering and Applications, 2020, 56(11): 60-66 (in Chinese)
(柯昌博, 吴嘉余, 曹彦. 面向云计算应用层演化的隐私保护方法研究[J]. 计算机工程与应用, 2020, 56(11): 60-66)

[7] Sahai A, Waters B. Fuzzy identity-based encryption [C] // Proc of the 24th Annual Int Conf on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005). Berlin: Springer, 2005: 457-473

[8] Wang Changji, Luo Jianfa. An efficient key-policy attribute-based encryption scheme with constant ciphertext length [J]. Mathematical Problems in Engineering, 2013, 2013(3): 87-118

[9] Han Jinguang, Susilo W, Mu Yi, et al. Privacy-preserving decentralized key-policy attribute-based encryption [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(11): 2150-2162

[10] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of the 28th IEEE Symp on Security and Privacy (SP'07). Piscataway, NJ: IEEE, 2007: 321-334

[11] Wang Hao, Zheng Zhihua, Wu Lei, et al. Adaptive secure outsourcing ciphertext-policy attribute-based encryption [J]. Journal of Computer Research and Development, 2015, 52(10): 2270-2280 (in Chinese)
(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)

[12] Tian Youliang, Yang Kedi, Wang Zuan, et al. Algorithm of blockchain data provenance based on ABE [J]. Journal on Communications, 2019, 40(11): 101-111 (in Chinese)
(田有亮, 杨科迪, 王缵, 等. 基于属性加密的区块链数据溯源算法[J]. 通信学报, 2019, 40(11): 101-111)

[13] 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 IEEE Conf on Computer Communications (INFOCOM 2010). Piscataway, NJ: IEEE, 2010: 1-9

[14] Yang Tengfei, Shen Peisong, Tian Xue, Feng Rongquan. Access control mechanism for classified and graded object storage in cloud computing [J]. Journal of Software, 2017, 28(9): 2334-2353 (in Chinese)
(杨腾飞, 申培松, 田雪, 等. 对象云存储中分类分级数据的访问控制方法[J]. 软件学报, 2017, 28(9): 2334-2353)

[15] Huang Qinlong, Wang Licheng, Yang Yixian. DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices [J]. World Wide Web, 2018, 21(1): 151-167

[16] Li Qi, Sandhu R, Zhang Xinwen, et al. Mandatory content access control for privacy protection in information centric networks [J]. IEEE Transactions on Dependable and Secure Computing, 2015, 14(5): 494-506

[17] Xue Kaiping, Xue Yingjie, Hong Jianan, et al. RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 953-967

[18] Xue Yingjie, Xue Kaiping, Gai Na, et al. An attribute-based controlled collaborative access control scheme for public cloud storage [J]. IEEE Transactions on Information Forensics and Security, 2019, 14(11): 2927-2942

[19] Du Ruizhong, Yan Peiwen, Liu Yan. Fine-grained attribute update and outsourcing computing access control scheme in fog computing [J]. Journal on Communications, 2021, 42(3): 160-170 (in Chinese)
(杜瑞忠, 闫沛文, 刘妍. 雾计算中细粒度属性更新的外包计算访问控制方案[J]. 通信学报, 2021, 42(3): 160-170)

[20] Pan Ruijie, Wang Gaocai, Huang Hengyi. Attribute access control based on dynamic user trust in cloud computing [J]. Computer Science, 2021, 48(5): 313-319 (in Chinese)
(潘瑞杰, 王高才, 黄珩逸. 云计算下基于动态用户信任度的属性访问控制[J]. 计算机科学, 2021, 48(5): 313-319)

[21] Cao Zhenfu, Dong Xiaolei, Zhou Jun, et al. Research Advances on Big Data Security and Privacy Preserving [J]. Journal of Computer Research and Development, 2016, 53(10): 2137-2151 (in Chinese)
(曹珍富, 董晓蕾, 周俊, 等. 大数据安全与隐私保护研究进展[J]. 计算机研究与发展, 2016, 53(10): 2137-2151)

[22] 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 the 2013 ACM Conf on Computer and Communications Security (CCS 2013). New York: ACM, 2013: 475-486

[23] Qian Junlei, Dong Xiaolei. Fully secure revocable attribute-based encryption [J]. Journal of Shanghai Jiaotong University (Science), 2011, 16(4): 490-496

[24] Sahai A, Seyalioglu H, Waters B. Dynamic credentials and ciphertext delegation for attribute-based encryption [C] // Proc of the 32nd Annual Cryptology Conf (CRYPTO 2012). Berlin: Springer, 2012: 199-217

[25] 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 Symp on Research in Computer Security (ESORICS 2011). Berlin: Springer, 2011: 278-297

[26] Lewko A, Waters B. Decentralizing attribute-based encryption [C] //Proc of 30th Annual Int Conf on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2011). Berlin: Springer, 2011: 568-588

[27] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems [C] //Proc of the 34th IEEE Conf on Computer Communications (INFOCOM 2015). Piscataway, NJ: IEEE, 2015: 2398-2406

[28] Cao Zhenfu, Wang Hongbing, Zhao Yunlei. AP-PRE: Autonomous path proxy re-encryption and its applications [J]. IEEE Transactions on Dependable and Secure Computing, 2019, 16(5): 833-842

[29] Diffie W, Hellman M. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[30] Matsumoto T, Takashima Y, Imai H. On seeking smart public-key-distribution systems [J]. IEICE TRANSACTIONS (1976—1990), 1986, 69(2): 99-106

[31] Law L, Menezes A, Qu Minghua, et al. An efficient protocol for authenticated key agreement [J]. Designs, Codes and Cryptography, 2003, 28(2): 119-134

[32] Bellare M, Rogaway P. Entity authentication and key distribution [C] //Proc of 13th Annual Int Cryptology Conf (CRYPTO' 93). Berlin: Springer, 1993: 232-249

[33] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis [C] //Proc of the 6th IMA Int Conf on Cryptography and Coding. Berlin: Springer, 1997: 30-45

[34] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks [C] //Proc of the 19th Annual Int Conf on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2000). Berlin: Springer, 2000: 139-155

[35] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels [C] //Proc of the 20th Annual Int Conf on the Theory and Application of Cryptographic Techniques (EUROCRYPT 2001). Berlin: Springer, 2001: 453-474

[36] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange [C] //Proc of the 1st Int Conf on Provable Security (ProvSec 2007). Berlin: Springer, 2007: 1-16

[37] Cremers C J F. Session-state reveal is stronger than ephemeral key reveal: Attacking the NAXOS authenticated key exchange protocol [C] //Proc of the 7th Int Conf on Applied Cryptography and Network Security (ACNS 2009). Berlin: Springer, 2009: 20-33

[38] Cremers C. Examining indistinguishability-based security models for key exchange protocols: the case of CK, CK-HMQV, and eCK [C] //Proc of the 6th ACM Symp on Information, Computer and Communications Security (ASIACCS'11). New York: ACM, 2011: 80-91

[39] Gao Zhigang, Feng Dengguo. Efficient identity-based authenticated key agreement protocol in the standard model [J]. Journal of Software, 2011, 22(5): 1031-1040 (in Chinese)
(高志刚, 冯登国. 高效的标准模型下基于身份认证密钥协商协议[J]. 软件学报, 2011, 22(5): 1031-1040)

[40] Wang Shengbao, Cao Zhenfu, Dong Xiaolei. Provably secure identity-based authenticated key agreement protocols in the standard model [J]. Chinese Journal of Computers, 2007(10): 1842-1852 (in Chinese)
(王圣宝, 曹珍富, 董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报, 2007(10): 1842-1852)

[41] Guo Hua, Zhang Fan, Li Zhoujun, et al. Cryptanalysis and improvement of a new identity-based key exchange protocol [J]. Computer Science, 2010, 37(10): 78-81 (in Chinese)
(郭华, 张帆, 李舟军, 等. 对一个基于身份的密钥协商协议的分析与改进[J]. 计算机科学, 2010, 37(10): 78-81)

[42] Joux A. A one round protocol for tripartite Diffie - Hellman [C] //Proc of the 4th Int Symp on Algorithmic Number Theory. Berlin: Springer, 2000: 385-393

[43] Boneh D, Silverberg A. Applications of multilinear forms to cryptography [J]. Contemporary Mathematics, 2003, 324(1): 71-90

[44] Garg S, Gentry C, Halevi S. Candidate multilinear maps from ideal lattices [C] //Proc of the 32nd Annual Int Conf on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2013). Berlin: Springer, 2013: 1-17

[45] Coron J S, Lepoint T, Tibouchi M. Practical multilinear maps over the integers [C] //Proc of the 33rd Annual Int Cryptology Conf (CRYPTO 2013). Berlin: Springer, 2013: 476-493

[46] Boneh D, Zhandry M. Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation [C] //Proc of the 34th Annual Int Cryptology Conf (CRYPTO 2014). Berlin: Springer, 2014: 480-499

[47] Ingemarsson I, Tang D, Wong C. A conference key distribution system [J]. IEEE Transactions on Information Theory, 1982, 28(5): 714-720

[48] Ateniese G, Steiner M, Tsudik G. New multiparty authentication services and key agreement protocols [J]. IEEE Journal on Selected Areas in Communications, 2006, 18(4): 628-639

[49] Steiner M, Waidner M, Tsudik G. CLIQUES: A New Approach to Group Key Agreement [C] //Proc of the 18th Int Conf on Distributed Computing Systems (ICDCS'98). Piscataway, NJ: IEEE, 1998: 380-387

[50] Kim Y, Perrig A, Tsudik G. Tree-based group key agreement [J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 60-96

[51] Nalla D, Reddy K C. ID-based tripartite Authenticated Key Agreement Protocols from pairings [R/OL]. IACR Cryptol. ePrint Arch., 2003 [2021-08-01] http://eprint.iacr.org/2003/004

[52] Barua R, Dutta R, Sarkar P. Extending Joux's protocol to multi party key agreement [C] //Proc of the 4th Int Conf on Cryptology in India (INDOCRYPT 2003). Berlin: Springer, 2003: 205-217

[53] Wang Zhiwei, Gu Dawei. A group key agreement protocol based on tree and threshold idea [J]. Journal of Software, 2004, 15(6): 924-927 (in Chinese)
(王志伟, 谷大武. 基于树结构和门限思想的组密钥协商协议[J]. 软件学报, 2004, 15(6): 924-927)

[54] Burmester M, Desmedt Y. A secure and efficient conference key distribution system [C] //Proc of the Workshop on the Theory and Application of of Cryptographic Techniques (EUROCRYPT'94). Berlin: Springer, 1994: 275-286

[55] Bresson E, Chevassut O, Pointcheval D. Group Diffie-Hellman key exchange secure against dictionary attacks [C] //Proc of the 8th Int Conf on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2002). Berlin: Springer, 2002: 497-514

[56] Damiani E, Di Vimercati S D C, Foresti S, et al. Selective data encryption in outsourced dynamic environments [J]. Electronic Notes in Theoretical Computer Science, 2007, 168: 127-142

[57] Blundo C, Cimato S, Di Vimercati S C, et al. Managing key hierarchies for access control enforcement: Heuristic approaches [J]. Computers & Security, 2010, 29(5): 533-547

[58] Odelu V, Das A K, Goswami A. A secure effective key management scheme for dynamic access control in a large leaf class hierarchy [J]. Information Sciences, 2014, 269: 270-285

[59] Hong S, Kim H I, Chang J W. An efficient key management scheme for user access control in outsourced databases [J]. World Wide Web, 2017, 20(3): 467-490

[60] Mao Jiangdong, Zhang Laishun, Guo Yuanbo, et al. An elliptic curve cryptography and triple tree based group key agreement scheme [J]. Computer Applications and Software, 2010, 27(7): 30-32, 36 (in Chinese)
(毛江栋, 张来顺, 郭渊博, 等. 基于椭圆曲线和三叉树的群组密钥协商方案[J]. 计算机应用与软件, 2010, 27(7): 30-32, 36)

[61] Chen Haihong, Li Junyi. Novel ID-based group authenticated key agreement scheme [J]. Computer Engineering and Applications, 2017, 53(21): 103-109 (in Chinese)
(陈海红, 李军义. 新的基于身份认证的群密钥协商协议[J]. 计算机工程与应用, 2017, 53(21): 103-109)

[62] Zeng Jiqiang, Shi Guozheng. Ternary tree group key agreement scheme based on ECC [J]. Computer Applications and Software, 2018, 35(9): 311-316 (in Chinese)
(曾继强, 史国振. 基于 ECC 的三叉树群组密钥协商方案[J]. 计算机应用与软件, 2018, 35(9): 311-316)

[63] Chen Yong, He Mingxing, Zeng Shengke, et al. Two-round deniable group key agreement protocol [J]. Journal of Cryptologic Research, 2016, 3(2): 137-146 (in Chinese)
(陈勇, 何明星, 曾晟珂, 等. 两轮次的可否认的群密钥协商协议[J]. 密码学报, 2016, 3(2): 137-146)

[64] Teng Jikai, Wu Chuankun, Tang Chunming. An ID-based authenticated dynamic group key agreement with optimal round [J]. Science China Information Sciences, 2012, 55(11): 2542-2554

[65] Fang Liang, Liu Fengnian, Miao Fuyou. Group key negotiate scheme based on secret sharing [J]. Computer Engineering and Applications, 2018, 54(12): 69-73, 151 (in Chinese)
(方亮, 刘丰年, 苗付友. 基于秘密共享的组密钥协商方案[J]. 计算机工程与应用, 2018, 54(12): 69-73, 151)

[66] Deng Shuhua, Zhao Zemao. Secure and reliable centralized multicast key management scheme [J]. Computer Science, 2011, 38(Z10): 50-52, 65 (in Chinese)
(邓淑华, 赵泽茂. 一种安全可靠的集中式组播密钥管理方案[J]. 计算机科学, 2011, 38(Z10): 50-52, 65)

[67] Wu Qianhong, Mu Yi, Susilo W, et al. Asymmetric group key agreement [C] //Proc of the 28th Annual Int Conf on the Theory and Applications of Cryptographic Techniques (EUROCRPY 2009). Berlin: Springer, 2009: 153-170

[68] Xie Tao, Teng Jikai. Traitor traceability of asymmetric group key agreement [J]. Communications Technology, 2019, 52(5): 1210-1214 (in Chinese)
(谢涛, 滕济凯. 非对称群组密钥交换协议的叛逆追踪性[J]. 通信技术, 2019, 52(5): 1210-1214)

[69] Shen Jiann, Zhou Tianqi, He Debiao, et al. Block design-based key agreement for group data sharing in cloud computing [J]. IEEE Transactions on Dependable and Secure Computing, 2017, 16(6): 996-1010

[70] He Kai, Huang Chuanhe, Wang Xiaomao, et al. Aggregated privacy-preserving auditing for cloud data integrity [J]. Journal on Communications, 2015, 36(10): 119-132 (in Chinese)
(何凯, 黄传河, 王小毛, 等. 云存储中数据完整性的聚合盲审计方法[J]. 通信学报, 2015, 36(10): 119-132)

[71] Shen Jian, Liu Dengzhi, Sun Xingming, et al. Efficient cloud-aided verifiable secret sharing scheme with batch verification for smart cities [J]. Future Generation Computer Systems, 2020, 109: 450-456

[72] Wang Cong, Wang Qian, Ren Kui, et al. Privacy-preserving public auditing for data storage security in cloud computing [C] //Proc of the 29th Conf on Information Communications (INFOCOM'10). Piscataway, NJ: IEEE, 2010: 525-533

[73] Zhu Yan, Hu Hongxin, Ahn G J, et al. Cooperative provable data possession for integrity verification in multicloud storage [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(12): 2231-2244

[74] Tian Hui, Nan Fulin, Jiang Hong, et al. Public auditing for shared cloud data with efficient and secure group management [J]. Information Sciences, 2019, 472: 107-125

[75] Ateniese G, Burns R, Curtmola R, et al. Provable data possession at untrusted stores [C] //Proc of the 14th ACM Conf on Computer and Communications Security (CCS'07). New York: ACM, 2007: 598-609

[76] Sebé F, Domingo-Ferrer J, Martinez-Balleste A, et al. Efficient remote data possession checking in critical information infrastructures [J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(8): 1034-1038

[77] Wang Cong, Chow S S M, Wang Qian, et al. Privacy-preserving public auditing for secure cloud storage [J]. IEEE Transactions on Computers, 2013, 62(2): 362-375

[78] Wang Qian, Wang Cong, Ren Kui, et al. Enabling public auditability and data dynamics for storage security in cloud computing [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(5): 847-859

[79] Zhu Yan, Ahn G J, Hu, Hongxin, et al. Dynamic audit services for outsourced storages in clouds [J]. IEEE Transactions on Services Computing, 2011, 6(2): 227-238

[80] Liu Jian, Huang Kun, Rong Hong, et al. Privacy-preserving public auditing for regenerating-code-based cloud storage [J]. IEEE Transactions on Information Forensics and Security, 2015, 7(10): 1513-1528

[81] He Debiao, Zeadally S, Wu Libing. Certificateless public auditing scheme for cloud-assisted wireless body area networks [J]. IEEE Systems Journal, 2015, 12(1): 64-73

[82] Yu Yong, Au M H, Ateniese G, et al. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage [J]. IEEE Transactions on Information Forensics and Security, 2016, 12(4): 767-778

[83] Li Yannan, Yu Yong, Min Geyong, et al. Fuzzy identity-based data integrity auditing for reliable cloud storage systems [J]. IEEE Transactions on Dependable and Secure Computing, 2017, 16(1): 72-83

[84] Shen Jian, Shen Jun, Chen Xiaofeng, et al. An efficient public auditing protocol with novel dynamic structure for cloud data [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(10): 2402-2415

[85] Canetti R, Hohenberger S. Chosen-ciphertext secure proxy re-encryption [C] //Proc of the 14th ACM Conf on Computer and Communications Security (CCS'07). New York: ACM, 2007: 185-194

[86] Libert B, Vergnaud D. Unidirectional chosen-ciphertext secure proxy re-encryption [C] //Proc of the 11th Int Workshop on Practice and Theory in Public-Key Cryptography (PKC 2008). Berlin: Springer, 2008: 360-379

[87] Liang Kaitai, Au M H, Liu J K, et al. A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing [J]. IEEE Transactions on Information Forensics and Security, 2014, 9(10): 1667-1680

[88] Liu Qin, Wang Guojun, Wu Jie. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment [J]. Information Sciences, 2014, 258: 355-370

[89] Luo Song, Shen Qingni, Chen Zhong. Fully secure unidirectional identity-based proxy re-encryption [C] //Proc of the 14th Int Conf on Information Security and Cryptology (ICISC'11). Berlin: Springer, 2011: 109-126

[90] Liang Kaitai, Liu J K, Wong D S, et al. An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing [C] //Proc of the 19th European Symp on Research in Computer Security (ESORICS 2014). Berlin: Springer, 2014: 257-272

[91] Xu Lei, Wu Xiaoxin, Zhang Xinwen. CL-PRE: A certificateless proxy re-encryption scheme for secure data sharing with public cloud [C] //Proc of the 7th ACM Symp on Information, Computer and Communications Security (ASIA CCS'12). Berlin: Springer, 2012: 87-88

[92] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C] //Proc of the 9th Int Conf on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2003). Berlin: Springer, 2003: 452-473

[93] Liu Xuefeng, Zhang Yuqing, Wang Boyang, et al. Mona: Secure multi-owner data sharing for dynamic groups in the cloud [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 6(24): 1182-1191

[94] Li Jiguo, Shi Yuerong, Zhan Yichen. A privacy preserving attribute-based encryption scheme with user revocation [J]. Journal of Computer Research Development, 2015, 52(10): 2281-2292 (in Chinese)
(李继国, 石岳蓉, 张亦辰. 隐私保护且支持用户撤销的属性基加密方案[J]. 计算机研究与发展, 2015, 52(10): 2281-2292)

[95] Lu Yang, Li Jiguo. A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds [J]. Future Generation Computer Systems, 2016, 62: 140-147

[96] Li Jin, Zhang Yinghui, Chen Xiaofeng, et al. Secure attribute-based data sharing for resource-limited users in cloud computing [J]. Computers & Security, 2018, 72: 1-12

[97] Shen Jian, Zhou Tianqi, Chen Xiaofeng, et al. Anonymous and traceable group data sharing in cloud computing [J]. IEEE Transactions on Information Forensics and Security, 2017, 13(4): 912-925

[98] Shen Wenting, Qin Jing, Yu Jia, et al. Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage [J]. IEEE Transactions on Information Forensics and Security, 2018, 14(2): 331-346

[99] Wei Jianghong, Chen Xiaofeng, Huang Xinyi, 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, 2019. DOI: 10.1109/TDSC.2019.2947920

[100] Pu Yuwen, Hu Chunqiang, Deng Shaojiang, et al. R²PEDS: A recoverable and revocable privacy-preserving edge data sharing scheme [J]. IEEE Internet of Things Journal, 2020, 7(9): 8077-8089

[101] Huang Hui, Chen Xiaofeng, Wang Jianfeng. Blockchain-based multiple groups data sharing with anonymity and traceability [J]. Science China Information Sciences, 2020, 63(3): 3-15

[102] Gentry C. A fully homomorphic encryption scheme [D]. Stanford, CA: Stanford University, 2009

[103] Halevi S, Shoup V. Bootstrapping for helib [C] //Proc of the 34th Annual Int Conf on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2015). Berlin: Springer, 2015: 641-670

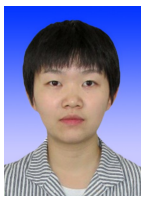
[104] Chen Hao, Chillotti I, Song Y. Multi-key homomorphic encryption from TFHE [C] //Proc of the 25th Annual Int Conf on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2019). Berlin: Springer, 2019: 446-472

[105] Zhou Jun, Choo K K R, Cao Zhenfu, et al. PVOPM: Verifiable privacy-preserving pattern matching with efficient outsourcing in the malicious setting [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(5): 2253-2270

[106] Zhou Jun, Cao Zhenfu, Qin Zhan, et al. LPPA: Lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs [J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 420-434

Shen Jian, born in 1985. PhD, professor, PhD supervisor. Member of CCF. His main research interests include public key cryptography, cloud computing security, and information security.

沈 剑,1985 年生.博士,教授,博士生导师.CCF 会员.主要研究方向为公钥密码学、云计算安全、信息安全等.



Zhou Tianqi, born in 1994. PhD candidate, Her main research interests include public key cryptography and combinatorics.

周天祺,1994 年生.博士研究生.主要研究方向为公钥密钥学和组合数学等.

Cao Zhenfu, born in 1962. PhD, distinguished professor in East China Normal University. Senior member of IEEE. His main research interests focus on number theory and new theories for cryptography and network security, including blockchain security, AI security, 5G security and privacy preserving.

曹珍富,1962 年生.博士,华东师范大学教授.IEEE 高级会员.主要研究方向为数论、密码学和网络安全新理论,包括区块链安全、AI 安全,5G 安全和隐私保护等.