# 适用于区块链的分布式密码技术综述

胡云帆[1) ] 熊 虎[1)] 方黎明[2),3)] 彭长根[4)] 秦 臻[1)] 秦志光[1)]

[1)](电子科技大学信息与软件工程学院网络与数据安全四川省重点实验室 成都 610054)

[2)](南京航空航天大学计算机科学与技术学院 南京 211106)

[3)](南京航空航天大学深圳研究院 广东 深圳 518057)

[4)](贵州大学计算机科学与技术学院省部共建公共大数据国家重点实验室 贵阳 550025)

**摘 要** 区块链是一种允许多个陌生节点利用共识机制在不依赖可信第三方节点支持的情况下建立信任的技术。考虑到区块链的“去中心化”特点,标准的密码技术需要进行分布式改造以适用于区块链场景。本文对适用于区块链的分布式密码学框架、分布式密钥管理、分布式数字签名、分布式密钥协商与分布式审计等分布式密码技术进行了综述。具体地,本文分析了以上几种技术的研究现状,并依托经典方案梳理了各种技术的构造思想。同时,本文比较了各方案的属性与性能,评估了各方案在安全性、效率和可扩展性等方面的优缺点,并讨论了该领域当前面临的挑战。最后,对未来的发展前景进行了展望。

**关键词** 区块链;分布式密码学;密钥管理;数字签名;密钥协商;审计

**中图法分类号** TP309 **DOI 号** 10.11897/SP.J.1016.2025.01670

# A Survey of Distributed Cryptography Suitable for Blockchain

HU Yun-Fan[1)] XIONG Hu[1)] FANG Li-Ming[2),3)] PENG Chang-Gen[4)] QIN Zhen[1)] QIN Zhi-Guang[1)]

[1)](Sichuan Province Key Laboratory of Network and Data Security, School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054)

[2)](College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106)

[3)](Nanjing University of Aeronautics and Astronautics Shenzhen Research Institute, Shenzhen, Guangdong 518057)

[4)](The State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550025)

**Abstract** Blockchain is a technology that enables multiple unfamiliar nodes to establish trust through a consensus mechanism without relying on the support of trusted third-party nodes. Considering the decentralized nature of blockchain, standard cryptographic techniques require distributed adaptations to suit blockchain scenarios. This paper presents a survey of distributed cryptographic techniques including distributed cryptographic frameworks, distributed key management, distributed digital signatures, distributed key agreement, and distributed auditing, which are suitable for blockchain applications. Specifically, this paper analyses the state of art of the aforementioned techniques and organizes the design principles based on classic schemes. Furthermore, it compares the attributes and performance of various schemes, evaluates their strengths and weaknesses in terms of security, efficiency, and scalability, and discusses the challenges currently faced in this field. Finally, the paper offers insights into future development prospects.

**Keywords** blockchain; distributed cryptography; key management; digital signature; key agreement; audit

收稿日期:2024-08-30;在线发布日期:2025-03-28。本课题得到国家重点研发计划(2022YFB2701400)、国家自然科学基金项目(U22B2029,62272228)、深圳市科技计划项目(JCYJ20210324134408023)资助。**胡云帆**,博士研究生,主要研究方向为密码学、人工智能安全。E-mail:202311090901@std.uestc.edu.cn。**熊 虎**(通信作者),博士,教授,中国计算机学会(CCF)会员,主要研究领域为密码学、区块链。E-mail:xionghu@uestc.edu.cn。**方黎明**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为密码学、区块链、人工智能安全。**彭长根**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为密码学、信息安全。**秦 臻**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为人工智能安全、多源数据融合。**秦志光**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为信息安全。

## 1　引　言

区块链作为一种分布式账本技术，通过去中心化结构与共识机制，保障了交易的透明性与可追溯性。去中心化意味着不存在单一节点控制交易与数据，所有参与节点共同参与交易验证与数据存储，这使得数据不易被篡改和伪造，从而提高了数据的可信度与安全性。共识机制能够令所有参与节点就区块链状态达成一致，保证了数据的一致性和公开性，使交易记录对任何人可见，从而确保了交易的透明性与可追溯性。以上基本特性使区块链技术成为保障数据安全的有力工具，为加密货币如比特币提供基础，并在金融、供应链管理、物联网等各个领域得到广泛应用。然而，尽管区块链在许多领域取得成功，安全问题仍然存在，如公开交易信息引发的数据隐私问题，以及智能合约执行异常可能导致不可预料的交易执行结果，造成了区块链在安全上的局限性，因此需要引入其他技术来加强保护措施。分布式密码学在传统密码学的基础上拓展为分布式结构，兼具安全性、灵活性与鲁棒性，提升了隐私保护能力。具体而言，分布式密码学是一门研究如何在分布式系统中设计、分析和实现密码协议的学科，其核心目标是通过分布式交互在多个缺乏互信关系的参与方之间实现密码功能[1]。因此，为增强区块链的安全性，可借助分布式密码学弥补安全性与灵活性方面的不足，从而提供更坚实的安全基础。

近年来，国内外已有多篇文献涉及区块链中分布式密码技术的综述，但大多文献将分布式密码技术作为解决区块链隐私保护问题的方法之一，且仅囊括了部分常用技术，并未将其作为综述的主要对象，对其在区块链中的应用进行全面的系统性分析与深入的探讨。Zhu 等人[2]从区块链结构的角度出发，讨论了网络层、交易层和应用层中的隐私保护机制，并将数据加密技术作为交易层中隐私保护的手段之一，对相关研究进行了综述。Li 等人[3]则从包括分布式密码学方案在内的多个角度对区块链隐私保护研究现状进行了汇总与分析。此后，不少研究者对密码学中的常用技术在区块链隐私保护方面的相应研究与应用进行了分类与汇总，如 Feng 等人[4]重点关注混合服务、环签名、非交互式零知识证明与同态加密，对区块链隐私保护的相关文献进行了讨论。Yao 等人[5]在此基础上，对涉及零知识证明、同态加密与环签名等多个技术的方案进行了全面地对比与分析，其中包括对审计方面的讨论。分布式密码技术近些年蓬勃发展，已取得大量成果，并催生了丰富的分支领域，如分布式的密码框架、密钥管理、数字签名、密钥协商与审计等，如图 1 所示。其中，分布式密码框架[6]在区块链中为密钥管理、数字签名等其他密码技术提供了基础支撑，了解其设计原理可以为分布式密码技术提供指导，并确保系统的安全性和可靠性；分布式密钥管理[7]通过部分高级权限者管理密钥，尤其适合在联盟链和存在委员会的区块链应用中保障密钥的安全，确保只有授权用户能够访问区块链上的数据；分布式数字签名[8]是保证数据完整性的重要手段，在区块链数据传输和身份验证方面发挥着重要作用，引入先进、完善的分布式数字签名能够提升区块链交易的可信

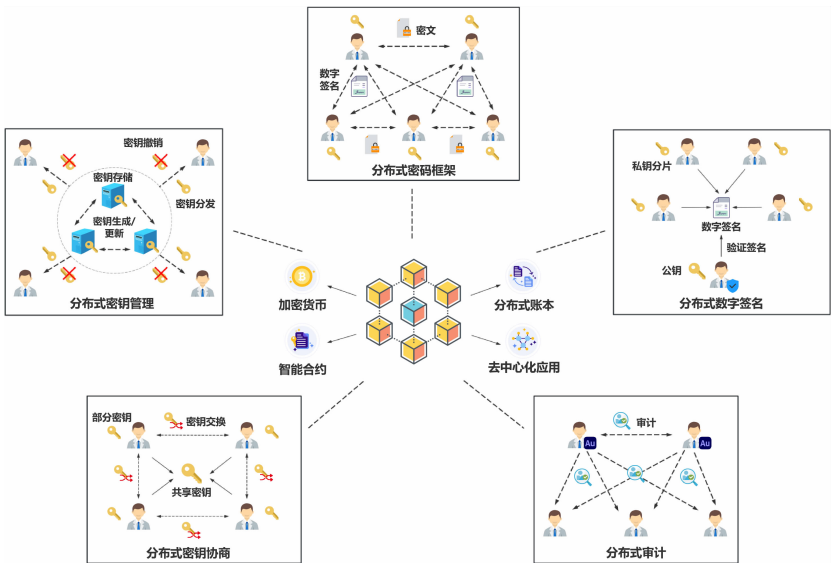



图 1　区块链中的分布式密码技术

度;分布式密钥协商[9]能够使平等且互不信任的多方共同生成共享密钥,是确保公有链等通常不存在可信第三方与高级权限者的分布式系统安全通信的重要手段;分布式审计[10]在区块链中发挥着监督与验证的作用,由审计者有效地监控系统,及时发现并应对安全事件和异常行为,这在联盟链和存在委员会的区块链应用中尤为适用。在分析和阐述分布式密码技术时,应主要针对以上五个方面从设计原理、协议构造、安全性分析、性能评估和实际应用等多个维度进行全面综述。具体而言,应分析不同分布式密码方案的设计思想与核心构造方法,依据通信复杂度和计算开销等指标评估其性能表现,深入讨论各类方案在功能性与安全性方面的优缺点,并进行系统性分析以明确其适用场景。然而,以上综述文献并未从分布式密码技术的分支领域对丰富的研究成果进行归纳与总结,也缺乏对构造思想的梳理与深度分析,以及对现有方案的系统性分析。

因此,本文旨在弥补以往综述的不足,对适用于区块链的分布式密码技术进行系统性的综述,全面梳理和呈现当前技术方案的特点,力求通过分析客观地反映各项技术的实际情况,避免主观臆断其优劣。我们以常用且适用于区块链的几大密码学原型为主要对象,分别对其研究现状进行了系统性的回顾,并对各方案的安全性、效率等属性进行了对比与分析。我们以研究现状中的部分经典方案为例,深入探讨了其具体的技术路线与构造思想,有助于更加清晰地理解分布式密码技术在区块链应用中的设计思路。此外,本文还对部分方案进行了性能实验与对比分析,并结合该领域当前面临的挑战,探讨了未来潜在的发展方向。

## 2 预备知识

本节将简单介绍本文相关的预备知识,包括区块链概述、密码学原语与密码学组成要素三个方面。2.1 节将介绍区块链的概念、特点和分布式机制;2.2 节将介绍本文涉及的密码学原语,即直接应用于区块链场景并提供安全属性的密码学原型;2.3 节将介绍本文涉及的密码学组成要素,这些要素为分布式密码学提供理论支撑,使其适应区块链场景。

### 2.1 区块链概述

区块链作为一项引领数字时代的创新技术,构建了一种高度安全、透明和去中心化的数据管理体系,它由多个数据块(称为区块)构成的链式结构组成,每个区块都包含了一系列交易信息。这些交易信息在一个分布式网络中被分发和存储,消除了传统中心化系统的单点故障风险,提高了系统的鲁棒性和可信度。另外,加密技术的应用保证了区块链中数据的安全性与完整性,使其成为一个可信任的信息记录和传输方式。区块链技术具有一系列独特的特点,其中去中心化是其显著特征之一。其次,区块链具备一定的透明性,即所有的交易信息都被公开记录,从而提高了系统的可信度。同时,区块链具有不可篡改性,当数据被添加到区块链中,非法修改会导致链中的后续数据块无法验证,因此数据很难被篡改或删除。这些特性使得数据的真实性和完整性得到高度保护,为区块链提供了可信的数据存储。区块链的分布式机制是其核心特征,主要包括共识机制、节点通信与分布式账本。这些分布式的设计使得区块链能够实现高度的去中心化、数据安全性与一致性,从而在各个领域的应用场景下充分地发挥重要作用。为解决单点故障,区块链中的多个节点之间通过共识机制达成一致,常用的共识算法包括工作量证明(PoW)和权益证明(PoS)。节点通信是分布式机制的另一个重要组成部分,在区块链中,各节点通过点对点通信来传递交易和区块数据,这种通信方式确保了数据在整个网络中能够被快速地分发与同步,从而降低了数据丢失和错误的风险。分布式账本是区块链机制的核心组成部分,也是数据一致性的必要基础。各节点通过共识机制对交易信息达成一致后,将信息添加到本地的账本中,这种分布式账本的结构消除了单点故障,增强了数据的安全性,并确保了其不可篡改性。

### 2.2 密码学原语

本小节将介绍本文涉及的密码学原语,即能够在区块链场景中提供安全属性或功能的密码学原型,包括密码框架、密钥管理、数字签名、密钥协商与审计。

#### 2.2.1 密码框架

传统的密码框架一般以单一实体作为中心,例如服务器或中心机构,由其进行加解密、身份验证等操作。用户与设备与该中心实体通过密码学方法进行交互以实现安全通信,并将本地数据发送至中心实体进行处理与存储。然而,这样的集中式框架十分依赖对中心实体的信任,如果中心实体受到攻击或存在故障,则数据与系统安全都将面临威胁。因此在分布式场景中,为应对这样的单点故障,架构与

协议通常被拓展为分布式以提升系统的鲁棒性。

2.2.2　密钥管理

密钥管理是实现加密通信与保障数据安全的关键环节，通常需要一个可信第三方或多个权限较高的成员进行密钥生成、分发、存储、更新与撤销等操作，以确保只有授权用户能获取有效密钥，访问加密数据。有效的密钥管理能够防止非法访问、防止数据被篡改、保护数据隐私以及提升系统的鲁棒性，从而确保了信息安全的可靠性和完整性。

(1) 密钥生成：使用公共参数 $pp$ 生成一对公私钥 $K=(pk,sk)=\mathrm{GenerateKey}(pp)$。

(2) 密钥分发：通过使用安全通道或借助可信第三方(如证书颁发机构，CA)实现。

(3) 密钥存储：公钥 $pk$ 可公开存储，例如由 PKI 存储。私钥 $sk$ 被秘密保存，由消息的接收者存储。

(4) 密钥更新：当密钥到达预定使用期限或满足其他更新条件时，可通过密钥更新算法将旧密钥转化为新密钥 $K_{\mathrm{new}}=\mathrm{UpdateKey}(K_{\mathrm{old}})$。

(5) 密钥撤销：密钥可能因为证书过期、密钥泄露、持有者权限变化等原因而失效，为了实现有效的密钥管理，需要撤销失效密钥。

2.2.3　数字签名

数字签名是一种用于验证数字信息真实性和完整性的非对称密码学技术，它允许信息的发送者在发送信息之前对其进行签名，以便接收者通过该签名来验证信息的来源正确与未被篡改。因此，数字签名在保证通信消息的完整性和身份验证方面具有重要作用，其基本原理与流程如下：

(1) 根据公共参数 $pp$ 生成用于签名的密钥对：$(pk,sk)=\mathrm{Gen}(pp)$。

(2) 签名者用私钥 $sk$ 对消息 $m$ 进行签名：$\sigma=\mathrm{Sign}(m,sk)$。

(3) 验证者用签名者的公钥 $pk$ 对签名 $\sigma$ 进行验证，若 $\mathrm{Ver}(pk,m,\sigma)=1$，则签名有效。

实际应用中，消息接收者可以通过数字签名判断信息的发送者是否合法。由于私钥具有唯一性，只有合法的发送者才能生成有效的签名，这不仅保证了签名的不可伪造性，也为相关的审计工作提供了便利。此外，数字签名通常由消息 $m$ 经过处理(例如计算其哈希值)后生成，因此只需验证签名与 $m$ 的处理结果是否匹配即可验证数据的完整性。数字签名被广泛应用于网络通信、电子文档认证、电子商务与数字身份验证等领域，为数字世界中的信息提供了重要的安全保障。

2.2.4　密钥协商

密钥协商是通信双方在建立安全连接时，通过信息交互生成一个共享的加密密钥的过程。该过程协商出来的密钥将用于加解密双方之间传输的数据，从而保护通信内容的机密性与完整性。区别于密钥管理中的密钥生成与分发，密钥协商的参与方之间是平等关系，且无需可信第三方或其他权限较高者的干预。密钥协商作为密码学的关键组成要素，在保障信息安全与隐私保护等方面发挥着至关重要的作用，是安全通信中不可或缺的环节之一。Diffie-Hellman 密钥交换协议是一种常见的、基础的密钥协商协议，允许两个通信方在不直接传输密钥的情况下建立共享的密钥。为直观体现密钥协商的原理，我们以 Diffie-Hellman 密钥交换为例：

(1) 通信双方 Alice 与 Bob 共享一个大质数 $p$ 及其一个原根 $g$。

(2) Alice 与 Bob 各自随机选取一个私密的整数 $a,b(0<a,b<p-1)$，并分别计算各自的公钥，即 Alice 计算 $A=g^a \bmod p$，Bob 计算 $B=g^b \bmod p$。

(3) Alice 将 $A$ 发送给 Bob，Bob 将 $B$ 发送给 Alice。

(4) 双方各自用收到的公钥与自己的私钥计算共享密钥 $K=B^a \bmod p=A^b \bmod p$。

2.2.5　审计

密码学包含众多具有身份验证功能的原语，这使密码学成为审计和监管用户与服务器行为的有效工具。通过密码学技术，我们能够建立可靠的身份验证机制，确保通信各方身份的真实性，并能够对日志中的行为追溯到具体的用户或服务器。这为监管提供了可靠的依据，也为制定可监管方案提供了技术支持。在具体实施中，审计的主要方式依赖于一个核心系统或实体，通过收集、分析日志与事件，对各参与方进行监管，对潜在的安全威胁或异常行为进行检测，从而确保通信和交易的安全性与合规性。随着分布式系统的发展，逐渐出现了分布式的审计与监管技术，在保证安全性的同时，兼顾了分布式场景，规避了单点故障的风险，为密码学在审计领域的应用提供了更加灵活的选择。

### 2.3　密码学组成要素

本小节将介绍本文涉及的密码学中重要的组成要素，包括同态加密、零知识证明、Shamir 秘密共享与不经意传输。这些理论为密码学的分布式扩展提

供理论支撑，使其得以应用于区块链的分布式场景。

2.3.1 同态加密

同态加密（Homomorphic Encryption，HE）是密码学中的一种特殊的加密技术，其主要特点在于能够在加密的状态下执行某些计算操作，而无需解密数据。具体地说，对多个密文进行运算操作，其结果等于对这些密文对应的明文进行计算操作后的密文，即满足：

$$\mathrm{Enc}(m_1)\odot\mathrm{Enc}(m_2)\odot\cdots\odot\mathrm{Enc}(m_n)=\mathrm{Enc}(m_1\oplus m_2\oplus\cdots\oplus m_n),$$

其中，$m_i$为明文，$\oplus$与$\odot$分别为针对明文与密文的运算操作。以上特性使得 HE 能够在不解密的情况下，对加密后的数据直接进行计算和分析，从而保障数据和隐私的安全性，这对于保护敏感数据并进行有效的分析和计算具有重要意义。然而，HE 也面临一些挑战，如计算速度慢、资源消耗大、实现复杂性高，以及密钥安全问题。尽管如此，随着加密技术与安全协议的进步，HE 有望在数据分析和隐私需求之间找到平衡点，成为安全计算与隐私保护领域的关键工具。

2.3.2 零知识证明

零知识证明（Zero-Knowledge Proof，ZKP）是一种涉及两方或多方的密码学协议，它允许一个主体向另一个主体证明某陈述为真，而无需涉及该陈述的具体内容。这意味着证明者可以向验证者证明其拥有某信息，而不必透露该信息的实际内容，从而在保护信息隐私的同时实现验证。其基本思想是通过模拟一系列随机性质的询问与回答来向验证者证明一个陈述的正确性，具体流程如下：

（1）证明者 $P$ 向验证者 $V$ 发送一个承诺 $Com$。

（2）验证者 $V$ 向证明者 $P$ 发送一个随机挑战 $rc$。

（3）证明者 $P$ 根据随机挑战与拥有的信息 $s$，生成证明 $\Pi$，发送给验证者 $V$。

（4）验证者 $V$ 根据所有已知信息，对证明 $\Pi$ 进行验证：$\mathrm{Ver}(\Pi,Com,rc)$。

在整个交互过程中，验证者 $V$ 只能确定证明者 $P$ 是否拥有 $s$，而无法获取关于 $s$ 的任何实际信息，因此以上过程被称为交互式 ZKP。随着 ZKP 的发展，逐渐衍生出了非交互式 ZKP（Non-Interactive Zero-Knowledge Proof，NIZK），将交互过程简化至一轮，大大降低了通信开销。ZKP 在隐私保护、身份验证与密码学安全协议等领域具有广泛的应用，为确保信息的隐私性与身份的可靠性提供了强大的技术保障。

2.3.3 Shamir 秘密共享

秘密共享是一种密码学技术，可将秘密分割成多个部分，分发给不同的参与方，并确保仅在满足特定条件时才能恢复原始秘密。秘密共享的使用有助于提高数据安全性，降低单点故障的风险，适用于多种应用场景。Shamir 秘密共享是其中的一种经典方法，以数学严密性与安全性著称，因此在分布式场景被广泛应用，其大致原理如下：

（1）选择大素数 $p_1$，秘密共享分片总数 $n$ 与阈值 $t$，随机选择 $t-1$ 个系数 $(a_1,a_2,\cdots,a_{t-1})$，将秘密 $s$ 作为常数项，构造一个 $t$ 次多项式 $f(x)=s+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1} \bmod p$。

（2）选择 $n$ 个不同的 $x$ 值，代入多项式计算对应值并作为分片：$s_i=f(x_i) \bmod p$。

（3）收集至少 $t$ 个分片 $s_i$，利用拉格朗日插值法恢复原始多项式

$$f(x)=\sum_{i=1}^{t} y_i \cdot \prod_{j=1,j\neq i}^{t} \frac{x-x_j}{x_i-x_j},$$

$f(0)$即为原始秘密 $s$。若收集少于 $t$ 个 $s_i$ 则无法获得任何关于秘密的信息。

2.3.4 不经意传输

不经意传输（Oblivious Transfer，OT）是密码学中的一个重要协议，被广泛应用于安全多方计算中，它允许接收者 $R$ 从发送者 $S$ 持有的两条（或多条）消息中选择一条进行接收，但发送者 $S$ 却不知道具体选择的是哪条信息，且接收者 $R$ 无法获得未选择消息的任何内容。其基本原理与流程如下：

（1）发送者 $S$ 拥有消息 $m_1,m_2,\cdots,m_n(n\geq 2)$，接收者 $R$ 选择索引 $i$。

（2）发送者 $S$ 对所有消息进行处理，使得只有 $m_i$能够被接收者 $R$ 获取，且发送者 $S$ 无法得知索引 $i$。

（3）接收者 $R$ 对接收到的信息进行反向处理，得到 $m_i$。

为实现以上过程中的第二步，发送者 $S$ 与接收者 $R$ 需要进行一系列的通信与协商。在实际应用中，因为场景与需求的不同，该步骤拥有丰富多样的变体与拓展。

## 3 研究现状

密码技术在区块链领域中应用广泛，根据功能和层次可将适用于区块链的密码技术分为基础密码算法、应用密码协议和整体密码方案三类。基础密

码算法指提供核心密码功能的算法，如 ElGamal 算法、ECDSA 算法等，这些算法侧重于理论性构造并为系统的安全性提供基础支撑；应用密码协议是在基础密码算法之上设计的多方协议，用于在多方交互的过程中实现密码功能，例如基于 ECDSA 算法的多方签名协议通过多方协作实现分布式数字签名；整体密码方案则是利用基础算法和协议应对系统性问题的解决方案，通常表现为解决实际问题的框架或系统。这类密码技术更加侧重于综合集成、场景适配与优化，如通过多方 ECDSA 签名技术实现区块链系统中的多签钱包。

本节旨在深入探讨当前分布式密码学与区块链领域针对隐私保护的研究现状，针对分布式密码框架、分布式密钥管理、分布式数字签名、分布式密钥协商与分布式审计等关键内容，从理论构造、功能实现、场景适配与优化等角度分析各个方向的发展现状、趋势、创新技术以及现实应用，以帮助读者了解这些领域的发展历程、前沿动态、挑战与机遇。具有重要意义的技术路线与文献列于图 2 中。通过对这些重要研究方向与思路的详细介绍，本节旨在为读者提供一个全面的视角，更好地理解该领域的发展方向，为未来的研究与实践提供有益的指引。

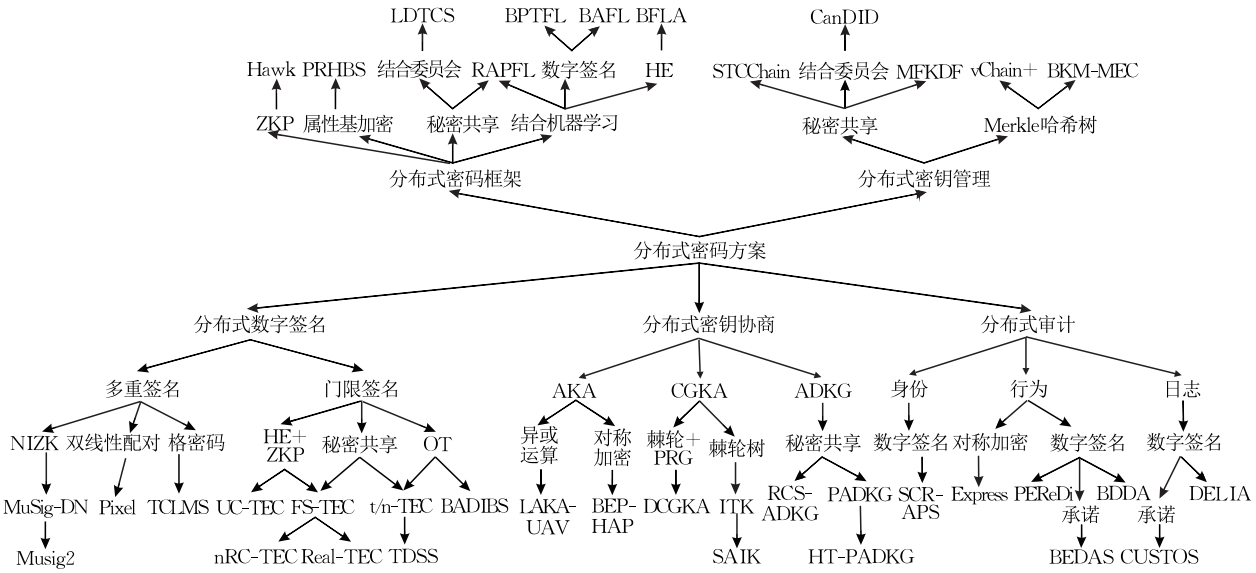



图 2　分布式密码方案研究现状

### 3.1　分布式密码框架

区块链已经成为一种重要的基础设施，去中心化特性是其重要特征之一，然而这种特性也带来了一系列的挑战。区块链网络包含大量节点，需要进行复杂的通信，而在该过程中，信息的安全性尤为关键。因此，采用加密技术对区块链中的数据进行保护显得尤为重要。然而，对于区块链这样的分布式系统，单纯依赖加密技术虽然能够确保单个交易或数据块的安全，却容易面临单点故障与可扩展性问题，无法确保整个系统的安全性和隐私性。为解决该问题，需要引入整体化的隐私保护机制，即分布式密码框架，将加密技术与分布式系统相结合，通过分布式存储、多方计算和 ZKP 等技术手段，实现对整个区块链网络的隐私保护。本小节对现有分布式框架方案进行了归纳与总结，部分方案对比如表 1 所示。

**表 1　分布式密码框架方案对比**

| 框架 | 密码体制 | 同/异步 | 理论支撑 | 框架层数 | 健壮性 |
|---|---|---|---|---|---|
| Hawk[11] | 对称/非对称 | 同步 | ZKP | 2 | 恶意第三方 |
| LDTCS[12] | 非对称 | 同步 | 秘密共享 | 2 | 单点故障 |
| PRHBS[13] | 非对称 | 同步 | 属性基加密、可穿刺加密 | 3 | 篡改、非授权访问 |
| RAPFL[14] | 非对称 | 同步 | 秘密共享 | 2 | 恶意客户端 |
| BPTFL[15] | 非对称 | 同步聚合、异步审计 | 差分隐私、数字签名 | 2 | 单点故障 |
| BFLA[16] | 非对称 | 同步 | 差分隐私、HE | 3 | 篡改、恶意第三方 |
| BAFL[17] | 非对称 | 异步 | 数字签名 | 2 | 投毒攻击 |

面向区块链本身的分布式密码框架主要针对去中心化网络中的多角色协作,核心任务是保障数据交互的安全性与参与方身份的可信性,协助区块链系统实现其主要功能。这类分布式密码框架通常采用加密技术保障交易信息、智能合约数据和链上敏感信息在传输和存储过程中的机密性,通过数字签名和零知识证明等技术验证用户或节点的身份以确保其合法性,结合哈希算法和共识机制保障链上数据的完整性与不可篡改性。因此,与传统的中心化密码框架相比,这类分布式密码框架需要适应区块链网络的去中心化特性,强调效率、鲁棒性以及对不同类型区块链(如公有链、联盟链、私有链)的适配能力。Kosba 等人[11]提出了一种去中心化的智能合约系统(Hawk),它在区块链上以密文形式存储金融交易,从而保护交易隐私。该系统的编译器会自动生成一个高效的加密协议,合同方使用 ZKP 等原语与区块链进行交互,使用者以直观的方式编写智能合约而不泄露隐私。Aitzhan 等人[18]提出了一个名为 PriWatt 的系统,使用多重签名和匿名加密消息流实现了在不依赖可信第三方的情况下去中心化交易系统的概念验证,保证了匿名协商与交易的安全性。在大规模场景中,设备数量庞大且分布广泛,数据的传输、存储和计算过程都面临着诸多安全问题。Benhamouda 等人[12]提出了一种在传统的多服务器环境与区块链环境中运行的大规模阈值密码服务的部署方法,并能够满足大量服务器和高频率阈值操作的要求,使得阈值密码应用能够在更具挑战性的分布式无权限系统中运行,如当代的区块链系统。该方案的模型建立在不可预测的动态委员会上,其成员能够躲避攻击者定位,并在大网络中以高扩展性的方式执行临时角色。为保护医疗保健区块链系统中数据的机密性与完整性,Xu 等人[13]提出了一种隐私保护的医疗保健区块链系统 PRHBS,实现了安全的数据共享、细粒度的块级数据压缩与去重。该方案采用变色龙哈希函数与属性基加密提供灵活的访问控制,并结合可穿刺加密保证数据机密性,以较少的解密权限更新密钥,简化区块链实体对机密数据的管理。

在部分区块链场景中,对大规模数据挖掘与分析具有重要意义,例如在医疗链中,分析医疗数据能够帮助医疗行业实现精准诊断、个性化治疗等目标,因此区块链需要分布式机器学习框架为其提供强大的数据处理能力。然而,区块链中的数据往往涉及隐私,仅依靠机器学习无法做到隐私保护。为应对这一挑战,一些研究者将密码框架与机器学习相结合,提出了一些适用于区块链的分布式密码框架。与面向区块链本身的密码框架不同,在区块链与机器学习相结合的场景中,分布式密码框架的设计需要满足分布式环境下数据隐私保护与协作计算的需求,因此其核心目标是服务于安全多方计算。这类分布式密码框架通常结合同态加密和差分隐私等技术,保障参与方在隐私不暴露的前提下协作完成模型训练与推理。同时,此类密码框架需充分适应区块链的去中心化特性,配合区块链系统协调任务分配和结果验证,支持安全多方计算的高效执行。针对大规模边缘计算,Warnat-Herresthal 等人[19]提出了一种去中心化的机器学习方法(Swarm Learning),能够与包括函数加密和加密迁移学习在内的多种技术相结合,在不需要中央协调器的前提下提供具有隐私保护的机器学习。为提高容错性,该方案动态地选取聚合方,以代替传统框架中的中心服务器,实现了完全的去中心化。联邦学习(Federated Learning,FL)是一种将模型训练分散到多个本地设备或节点上的分布式机器学习框架,避免了数据离开本地造成的安全问题。将其与分布式密码技术结合能提供更安全的分布式机器学习方案,尤其适用于区块链场景中跨组织或跨边界的数据共享应用,如医疗链等对隐私保护有较高要求的应用场景。为消除对客户端半诚实假设的依赖,Awan 等人[14]提出了一个隐私保护联邦学习框架,使用 HE 保护模型交换过程中的 FL 局部模型,并采用代理重加密技术对聚合服务器中的聚合值进行重新加密。该方案中的各参与方可作为区块链节点,使用分布式账本记录组件中 FL 任务、局部和全局模型的更新日志,为区块链应用中的模型训练提供准确且安全的模型更新。为了防止 FL 中参与节点和数据的隐私泄露,Zhu 等人[15]采用伪公钥地址加密保护 FL 中的本地数据,并引入数字签名确保数据传输的不可抵赖性,提出了一种去中心化的联邦学习框架。该方案适用于区块链场景,可由参数聚合链代替中心参数服务器,利用区块链记录训练的中间参数,再引入差分隐私对其进行保护。此外,该方案激励协作节点进行参数验证与审计,从而降低恶意攻击与计算偏差的风险。Jia 等人[16]针对联邦学习中的梯度聚合,提出了一种适用于区块链的分布式数据保护聚合方案。该方案在数据聚合之前,采用基于差分隐私和 HE 的分布式 $K$-means 聚类、具有差分隐私的分布式随机森林,以及具有 HE 方法的分布式 AdaBoost,在

数据共享和模型共享中实现对数据的多重保护。此外，有研究者意识到同步方案在效率方面的短板，采用异步框架提升计算效率。Feng 等人[17]提出了一种异步联邦学习（BAFL）框架，通过数字签名对区块链中的数据与身份进行验证，并通过异步学习加快全局模型聚合。该方案使用交叉验证法，使区块链中的参与者对彼此的模型更新进行打分。分数由多个指标根据熵权法决定，并影响各参与者对全局聚合的贡献度。得益于该机制，此方案在抵御毒化攻击方面有更高的效率和性能。

综上所述，分布式密码框架方案的早期发展主要关注消除可信第三方的依赖，而随着技术的发展和需求的增加，提升整体安全性与效率的问题逐渐受到重视。现有方案虽然在这些方面有所提升，但仍然存在异步方案较少、响应不及时等问题亟需解决。

### 3.2　分布式密钥管理

密码学技术在区块链中扮演着关键角色，被用于保护数据的安全性，而确保有效且安全地管理密钥是实现此目标的一大关键。集中式密钥管理存在单点故障等明显缺点，管理中心受到攻击会严重威胁整个系统的密钥安全，影响系统的正常运作，因此无法满足区块链场景的需求。区别于集中式密钥管理，分布式密钥管理能够将密钥分散存储在区块链的多个节点上，从而避免单点故障，确保密钥的安全使用，提高系统的灵活性、安全性和稳定性。本小节对现有分布式密钥管理方案进行了归纳与总结，部分方案对比如表 2 所示。

**表 2　分布式密钥管理方案对比**

| 方案 | 密码体制 | 加密算法 | 设备要求 | 安全等级 |
|---|---|---|---|---|
| BKM-HIT[20] | 非对称 | ECIES、ECDSA | 安全管理（SM）网络 | 保证前后向安全性 |
| DB-KMM[21] | 非对称 | ECIES、ECDSA | 无需 PKI | 抗内外部攻击、DoS、公钥篡改、共谋攻击 |
| BAAKM[22] | 非对称 | 未指定 | KGC | 保证前后向安全性、抗单点故障、内外部攻击、重放攻击 |
| CanDID[23] | 非对称 | 未指定 | 节点委员会 | 抗 Sybil 攻击、密钥丢失 |
| BKM-MEC[24] | 非对称 | ECDSA | 无需 PKI | 保证前后向安全性 |
| BASA[25] | 非对称 | SM9-IBS | KFC、BAS、AAS、无需 PKI | 保证前向安全性 |

不少研究者致力于区块链中的分布式密钥管理，为密钥的生成、分发与更新提供更安全可靠的解决方案。Lei 等人[20]提出了一个提供安全密钥管理的异构网络方案。该方案由两部分组成，第一部分引入去中心化的网络拓扑结构，以简化异构系统中的密钥管理；第二部分则采用动态的周期性事务收集技术，减少密钥转移时间以提升效率。为解决基于区块链的车载自组织网络（Vehicular Ad-Hoc Network，VANET）中的密钥管理问题，Ma 等人[21]提出了一种高效的去中心化密钥管理机制（DB-KMM）。该管理机制对用户的公钥进行分布式存储，排除了单点故障的风险，并能够结合 VANET 中区块链的智能合约实现公钥的自动注册、更新与撤销，提高密钥管理的效率。此外，该管理机制能够充分利用区块链不可篡改与去中心化的特点，通过去中心化投票机制防御恶意用户。Wang 等人[26]提出了一种新的可搜索区块链系统（vChain+），并设计了一种对象注册索引方法，实现了实用的安全公钥管理。该方案将对象 ID 注册为小整数，并将 ID 索引至每个数据对象，从而将全域大小限定在一个较小的范围，以限制公钥大小，提升密钥管理的效率与实用性。Dodis 等人[27]提出了一种高效的密钥存储方案，允许多个用户仅维护少量本地状态，将不断增长的密钥集合委托给服务器存储，从而降低了存储和通信开销。同时，该方案支持用户通过状态变化实现密钥的更新与撤销，确保了密钥管理的灵活性和效率。Long 等人[22]指出现有密钥管理通常依赖于可信方定期颁发证书，无法抵抗单点故障，并提出了一种灵活的匿名认证和密钥管理方案。该方案利用切比雪夫混沌映射，为区块链中通信实体之间的认证提供了安全高效的群组密钥生成和管理，保障了群组成员的安全通信。

鉴于区块链的去中心化结构，不少研究者结合秘密共享机制实现用户密钥的分布式存储与恢复。为防止私钥丢失与隐私泄露，Tan 等人[28]提出了一种阈值数据保护方案（STCChain），该方案使用 Shamir 秘密共享对私钥进行拆分与加密，并将其分布式地存储在区块链上，实现了无需可信第三方的分布式密钥分发与加密数据存储。与之相比，Maram 等人[23]为区块链添加了节点委员会，提出了一个去中心化的身份管理平台（CanDID），通过分散的节点委员会实现用户认证与用户密钥的分布式存储。在用户注册时，委员会通过 SHARK 证明确保

注册的合规性，采用基于安全多方计算的模糊匹配确定恶意方并将其剔除。此外，委员会可分散地存储用户密钥，并基于 Shamir 秘密共享将其恢复，从而兼顾其机密性与可恢复性。Nair 等人[29]扩展了基于密码的密钥派生函数(Key Derivation Function，KDF)，为几种流行的身份验证因素提供了该结构，并提出了一个 $t$-of-$n$ 的阈值多因子密钥派生函数(Multi-Factor KDF，MFKDF)结构。该阈值 MFKDF 基于 Shamir 秘密共享机制，允许用户在有因子丢失的情况下，进行密钥的恢复与重建。

边缘计算是一种高效的计算模式，通过将数据处理放在靠近数据源或数据消费者的位置，提升响应速度与效率。然而，边缘节点数量庞大，分布广泛，因此也需要一种高效、可靠的密钥管理机制来确保通信的安全性。针对该问题，Li 等人[24]提出了一种移动边缘计算密钥管理方案，以确保区块链中设备移动时的安全群组通信。在该方案中，子网内所有移动设备的公钥被打包成一个区块，并广播给其他用户。当该设备移动至另一个子网时，新子网的所有移动设备可检查其在本地或更高层次子网区块链中的记录并快速验证其身份，从而实现对移动设备的有效密钥管理，支持后续的群组通信。类似于以上情形，当涉及不同子网或不同域中节点之间的协作时，它们之间的信任是一大问题。对于跨域场景下的信任问题，Shen 等人[25]通过引入身份基数字签名(Identity-Based Digital Signature，IBS)实现了联盟链中的身份验证，并以此构建了不同域节点之间的信任，提出了一种高效的安全设备认证机制 BASA，解决了跨域通信中的安全与隐私问题。同时，为保证隐私性，Shen 等人还设计了一种身份管理方法，能够在设备隐私被泄露时撤销其公钥，并保证被认证设备的匿名性。

综上所述，分布式密钥管理的工作重心由最初的解决单点故障问题和提升效率，逐渐转变为实现动态密钥管理，增加密钥可撤销、可恢复重建等功能。然而，现有方案仍然存在缺乏异步管理的能力、无法应对频繁变动等问题。

### 3.3 分布式数字签名

分布式数字签名是传统数字签名的分布式形式，在去中心化等场景下为保障信息真实性与完整性发挥着重要作用。与传统数字签名不同，它允许由持有各自签名密钥的两个或多个参与方在不恢复完整签名密钥的情况下，通过交互生成完整有效的数字签名。分布式数字签名分为多重签名与门限签名，二者在设计机理与应用场景上存在一定区别。多重签名是指多个签名者使用各自持有的公私钥对一个消息进行签名，并将这些签名组合成最终签名 $\sigma$。验证 $\sigma$ 则需要使用所有签名者的公钥，因此验证者知道所有签名者的身份。而 $t$-of-$n$ 门限签名中只存在一个公私钥对，需要 $n$ 个签名者中任意不少于 $t$ 个签名者用各自持有的私钥分片对消息进行签名，最终聚合成完整的有效签名。使用该门限方案的公钥即可验证该签名，但不会向验证者暴露签名者的身份。现代区块链的网络规模不断扩大，对去中心化特性和可扩展性等方面都提出了较高的要求，分布式数字签名因其更高的安全性与灵活性，比传统数字签名更加适用于这类需要高度安全性和防止单点故障的场景，因此得到了广泛的发展和应用。本小节对现有分布式数字签名方案进行了归纳与总结，部分方案属性对比如表 3 所示。

**表 3 分布式数字签名方案属性对比**

| 方案 | 签名算法 | 密码学假设 | 安全性 | 安全性证明 | 理论支撑 |
|---|---|---|---|---|---|
| FS-TEC[30] | ECDSA | ECDDH、强 RSA | 选择性 | ROM | HE、ZKP、秘密共享 |
| $t/n$-TEC[31] | ECDSA | ECCDH | 选择性 | ROM | OT、秘密共享 |
| FROST[32] | Schnorr | DLP | 选择性 | ROM | ZKP、秘密共享 |
| UC-TEC[33] | ECDSA | ECDDH、强 RSA | 适应性 | ROM | HE、ZKP |
| ROAST[34] | Schnorr | OMDL、Schnorr-KoE | 适应性 | ROM | ZKP、秘密共享 |
| nRC-TEC[35] | ECDSA | ECDDH、强 RSA | 选择性 | ROM | HE、ZKP、秘密共享 |
| R-TEC[36] | ECDSA | 子群成员困难假设 | 选择性 | ROM | HE、ZKP、秘密共享 |
| TDSS[37] | SM2 | ECDLP | 选择性 | ROM | OT、秘密共享 |
| BADIBS[38] | IBS | DLP | 选择性 | ROM | OT |

在数字签名发展早期，产生了一些单方签名方案，这些方案都能够通过聚合多个独立签名扩展为多方签名方案。然而，这种简单扩展方法会导致签名长度与签名者的数量呈线性增长，效率低下。针对该问题，Itakura[39]基于 RSA 签名算法提出了第一个多重签名方案，从此多重签名便成为了密码学领域的研究热点之一，近年来被广泛应用于区块链等分布式场景。Maxwell 等人[40]提出了一种多重

Schnorr 签名协议(MuSig)，并证明其在离散对数(DL)假设 PPK 模型下是安全的。次年，Nick 等人[41]提出了 MuSig 的一个变种(MuSig-DN)，该方案是第一个具有确定性签名特性的 Schnorr 多重签名方案，其中签名者根据消息和所有签名者公钥的伪随机函数，以确定性的方式生成他们的随机数，并通过向其他签名者提供 NIZK，证明他们确实按照上述方式生成了随机数。然而，MuSig[40]的签名过程需要进行三轮通信，为了提升通信效率，Nick 等人[42]在之前的方案上进行改进，将通信轮数减少为两轮，提出了 MuSig2。该方案不仅支持密钥聚合，还实现了并发签名场景下的安全性，同时也是第一个在 DL 假设下支持对除了第一轮以外的所有轮次进行预处理的多重签名方案。此后，Boschini 将 MuSig[40]与格密码结合，提出了 MuSig-L[43]，实现了在线阶段只进行一轮通信的支持密钥聚合与并发场景的多重签名方案，并仅根据标准的 SIS 和 LWE 假设证明了其在 PPK 模型下的安全性。Chen[44]提出了一种基于格的多重签名方案(DualMS)，该方案利用无陷门的双签名模拟替代传统基于格的陷门技术，具有比 MuSig-L 更小的公钥和签名大小，以及更低的通信开销。Drijvers 等人[45]提出了一种基于配对的前向安全多重签名方案 Pixel，专为在区块链中使用而优化，可大幅节省带宽、存储需求与验证工作开销。该签名由两个群元素组成，验证不受签名者数量的影响，并支持将单个签名非交互式聚合为多重签名。该签名保证前向安全，从而防止对区块链的后向破坏攻击。基于 Gamma 签名，Xiao 等人[46]提出了一种可应用于区块链平台上的安全高效的多重签名方案 AGMS(Advanced Gamma Multi-Signature)，该方案使用拥有证明，可抵御密钥篡改攻击和 $k$-sum 问题。为进一步提升效率，该签名算法改变运行顺序以减少计算步骤，并采用分布式密钥聚合算法与签名算法。Damgard 等人[47]构建了基于格的低轮次复杂度分布式签名协议(TCLMS)，实现了两轮的多重签名。该方案在遵循 FSwA 范式的签名中，对同态承诺上加上陷门，以防止恶意方在发送第一个消息后中止而造成的隐私泄露。

1987 年至 1989 年，阈值密码学相关理论的提出使门限签名得到了快速的发展。Desmedt 等人[48]基于 RSA 提出了第一个 $t$-of-$n$ 的门限签名方案，将完整的签名密钥拆分成 $n$ 份，分别分发给 $n$ 个参与方，任意 $n'(t\leq n'\leq n)$ 个参与方都能够共同生成完整有效的数字签名。此后，门限签名得到了蓬勃的发展，产生了众多基于 RSA、DSA、Schnorr 等不同签名算法的门限方案，也使得门限签名成为了区块链场景的一个重要工具。Gennaro 等人[49]基于 HE 构造了在诚实多数场景下具有鲁棒性的门限 ECDSA 签名方案，并提出了“阈值最优”的概念，即在门限为 $t$ 时，只需不少于 $t$ 个诚实方参与签名。这类阈值最优方案的提出，摒弃了对冗余诚实方的需求，大大提升了门限签名的实用性。Gennaro 等人[30]为降低 ECDSA 中非线性计算的开销，采用 Paillier HE 构造了乘转加(Multiplicative to Additive，MtA)协议，并基于该协议构造了第一个支持任意 $t\leq n$ 的门限签名。MtA 协议以两个秘密 $a$ 与 $b$ 为输入，在不暴露二者的情况下，将满足 $\alpha+\beta=ab$ 的 $\alpha$ 与 $\beta$ 分别输出给 $a$ 与 $b$ 的拥有者，从而将秘密的乘共享转为加共享。同年，Lindell 等人[50]同样基于 Paillier HE，提出了一个类似于 MtA 协议的“私有乘法”协议，并构造了一个实用的全阈值 ECDSA 门限签名方案，该方案具有快速签名和快速密钥分发的功能。Doerner 等人[51]在构造 2-of-$n$ 门限 ECDSA 签名时提出了基于 OT 的双方 MtA 协议，紧接着又在次年将其扩展为多方 MtA 协议，并将其应用于 $t$-of-$n$ 的门限 ECDSA 方案[31]中。该方案通过一种新的、适用于任何数量的参与者的一致性检验，降低了通信与计算开销，并采用基于 OT 的 MtA 协议，在性能上优于基于 Paillier HE 的 MtA 协议。此外，高通信轮数带来的通信开销也是导致门限签名效率低下的原因之一，为解决该问题，Crites 等人[52]提出了一种仅需三轮交互的门限 Schnorr 签名方案(Sparkle)，并证明了其在不同威胁模型下的安全性，其中包括在随机预言机模型和 DL 假设下实现适应性安全。然而，Bacho 等人[53]指出 Sparkle 在不使用代数群模型的条件下只能容忍 $t/2$ 个恶意参与方，并基于线性函数提出了在同等条件下能够容忍 $t$ 个恶意方的门限签名算法 Twinkle 以克服上述限制。Komlo 等人[32]提出了 FROST，一种灵活的低通信轮数门限 Schnorr 签名方案。该方案在签署多条消息时只需要进行一次分布式密钥生成(Distributed Key Generation，DKG)，且可以抵抗并发场景下的伪造攻击。此外，该方案以获取待签署消息 $m$ 的时间为界，将签名过程划分为包含大部分数据处理的离线预处理阶段与只需一轮通信的在线签名阶段，从而降低签名操作期间的计算与通信开销。这种包含预处理阶段与单轮交互的正式签名阶段的签名称为非交互式(Non-Interactive，NI)签名，

被广泛应用于高效门限签名的研究中。为了更好地分析 NI 门限签名方案，Bellare 等人[54]提出了一套分层次的安全性定义模式和统一的规则，并基于高效 DKG 协议提出了 FROST 的更高效版本 FROST2。Canetti 等人[33]为提升效率，在 Gennaro 等人[30]和 Lindell 等人[50]协议的基础上，提出了两个在复杂度和轮数上各有优势的非交互式门限 ECDSA 协议，并采用定期刷新机制提供适应性安全。此外，二者都能够在一个或多个参与方违反协议时及时中止协议，并确保诚实参与方能够识别出违反协议者的身份，从而实现问责机制，这种特性被称为可识别中止(Identifiable Abort，IA)。Xue 等人[55]继续从 MtA 协议的角度优化效率，提出了一种“在线友好”的双方 ECDSA 协议，该协议将 ECDSA 中 $k$ 的构造由 $k=k_1+k_2$ 修改为 $k=k_1(r_1+k_2)$，将 MtA 协议的使用次数减少到一次，并可以很容易地通过 Shamir 秘密共享机制扩展到 2-of-$n$ 的门限 ECDSA 协议，从而显著地提升了基于 MtA 协议的签名方案的效率。Bacho 等人[56]为 DKG 引入了一个新的安全概念(oracle-aided simulatability)，并假设任意 DKG 协议都具有此属性，在此基础上模块化地证明了门限 BLS 方案的不可伪造性。Crites 等人[57]构造了一种将单方 BLS 签名转化为门限 BLS 签名的通用方法，并提出了首个基于无配对群的门限 BLS 签名。与其他同类方案相比，通过该通用方法构造的签名方案具有更短的签名长度。Abram 等人[58]通过伪随机相关发生器(Pseudorandom Correlation Generators，PCG)与随机种子连续产生随机数，降低了通信开销，提出了第一个将预处理阶段的通信复杂度降低到对数级的门限 ECDSA 签名协议，并实现了对于任意 $t\leq n$ 的适应性安全。Aggarwal 等人[59]提出了一种具有更正功能的非交互式多方 ECDSA 签名协议，该方案采用消息传递机制实现多方之间的信息交互，在签名生成时引入 ZKP 验证公钥和公共随机数，以降低通信开销，并基于拜占庭协议，保证在恶意参与方存在的情况下仍能生成正确的签名。然而，以上方案都建立在同步通信模型上，在实际情况中容易受到迟钝参与者的影响。因此，Ruffing 等人[34]提出了一种封装协议 ROAST，能够将包含预处理阶段与在线签名阶段、具有可识别中止，且在并发情况下是不可伪造的底层签名协议，转换为具有鲁棒性的异步签名方案。Cui 等人[60]针对 Castagnos-Laguillamie(CL)加密与其密文上的同态操作，提出了轻量级的 ZKP。该 ZKP 有助于在不影响主动安全性和非交互性的情况下构建安全高效的门限 ECDSA。Bouez 等人[35]指出以往的门限方案在分发签名随机数 $k$ 之前就已经从 $n$ 个参与方中选出了 $t$ 个诚实的参与方，这本质上是一种不符合实际情况的假设。因此，Bouez 等人在 Gennaro 等人[30]的基础上进行改进，将签名随机数 $k$ 以 Shamir 秘密共享的形式分发给 $n$ 个参与方，代替以往方案中的加共享，并在正式签名阶段选定 $t$ 个签名者，提出了更加符合实际的门限签名方案。Wong 等人[36]针对同一问题，提出了一种“真阈值”的门限 ECDSA 方案，该方案在整个预处理和签名过程中不断检测并剔除恶意参与方，真正实现了 $t$-of-$n$ 门限签名的灵活性，并实现了可识别中止。Chen 等人[37]基于 SM2 签名算法提出了一种符合 ISO/IEC 签名标准的灵活门限签名协议，并将其应用于工业区块链中基于联邦学习的空-天-地-海模型训练。该方案采用了 Doerner 等人[31]提出的基于 OT 的 MtA 协议，实现了有效的签名转换和签名分片的构建，并具有较高的签名效率。为解决安全数字通信和交易过程中的密钥托管与单点故障问题，Li 等人[38]将基于 OT 的 MtA 协议引入 IBS，提出了一种符合 IEEE P1363 标准的完全分布式 IBS 协议，完全消除了对可信密钥生成中心(Key Generation Center，KGC)的需求，表现出优异的效率与实用性。

环签名由 Rivest 等人[61]提出，是一种匿名式的数字签名方案，能够由一组用户中的一方签署消息，而验证者无法在该组用户中确定具体的签名者，既可以确保签名的有效性，又可以保护签名者的隐私。Bresson 等人[62]将环签名拓展到了门限场景，基于 RSA 提出了第一个门限环签名方案，并在随机预言机模型下实现了可证明安全。自此，门限环签名成为了区块链场景下备受关注的一种签名方案，被广泛应用于匿名交易、匿名投票等区块链场景中。Haque 等人[63]提出了第一个针对主动对手的 $t$-of-$n$ 门限环签名，该方案能够抵抗参与系统并随意偏离规定程序的主动攻击者。此外，该方案提出了一种基于任何陷门承诺的后量子安全实现，并证明了其在量子随机预言机模型下是安全的。为防止签名过程中参与方将身份暴露给其他签名者，Haque 等人继续致力于门限环签名，提出了一个不需要签名者进行交互的门限环签名方案[64]，并具有 $O(\log(n))$ 的签名长度与标准模型下的可证明安全性。然而，现有门限环签名要求所有签名者必须同意选定的签

名者集合，这实际上假设了签名者之间存在协调，会对匿名性形成限制。因此，Aranha 等人[65]提出了一种可扩展的门限环签名以消除这一限制。该方案可将两个签名者集合合并为一个更大的集合，并具有更高的门限，这增强了签名的匿名性，并使新的签名者能够匿名地支持其他人已经做出的陈述。然而，Avitabile 等人[66]指出，Aranha 等人[65]的工作仅能针对已知最后一个签名的对手，而无法抵抗知晓整个过程的对手。因此，Avitabile 等人提出了一个更强的安全定义，并引入了可扩展的非交互式见证知识证明，不仅解决了上述安全问题，还提升了签名的效率。

综上所述，在分布式数字签名的发展初期，签名方案的效率受到了广泛关注，而随着应用需求的增加，可识别中止和处理高并发等功能的引入使得分布式数字签名方案变得更加安全和实用，但也使得现有方案在大规模场景下的可拓展性与效率方面存在明显不足。

### 3.4　分布式密钥协商

在公有链等区块链场景中，通常不存在可信第三方，各参与方需要在平等且互不信任的前提下生成共享密钥，以确保系统的安全通信。密钥协商能够在这种情况下实现密钥的共享，然而传统的密钥协商往往局限于两个通信实体之间密钥的协商与交换，随着互联网的快速发展，分布式场景中的通信实体数量众多，且通信关系复杂多变，传统的密钥协商方案已无法满足区块链等分布式场景的需求，多方密钥协商方案应运而生，逐渐成为了解决区块链等分布式场景安全通信问题的重要手段之一，并取得了显著的发展与广泛的应用。本小节对现有分布式密钥协商方案进行了归纳与总结，部分方案对比如表 4 所示。

**表 4　分布式密钥协商方案对比**

| 方案 | 密码学假设 | 安全性证明 | 计算复杂度 | 消息数量 | 通信轮数 |
|---|---|---|---|---|---|
| LAKA-UAV[67] | ECDDH | Real-or-Random OM | $O(n)$ | $O(n)$ | 1 |
| BEPHAP[68] | ECDLP | ROM | $O(n)$ | $O(n)$ | 1 |
| BMASKA[69] | ECDLP、ECCDH | ROM | $O(n)$ | $O(n)$ | 1 |
| 链式 CmPKE[70] | SSDDH | ROM | $O(n^2)$ | $O(n)$ | 1 |
| AB-AGKA[71] | $k$-BDHE | ROM | $O(n^3)$ | $O(n^2)$ | 1 |
| SAIK[72] | DDH | ROM | $O(n\log n)$ | $O(n\log n)$ | 1 |
| RCS-ADKG[73] | DDH | ROM | $O(n^3)$ | $O(n^3)$ | $O(n)$ |
| HT-PADKG[74] | DLP | ROM | $O(n^2)$ | $O(n^2)$ | $O(\log n)$ |

为了解决分布式密钥协商的效率问题，使其能够更好地为区块链中的移动设备协商密钥，Xi 等人[75]为移动设备设计了一种名为 TDS 的高效身份验证和密钥协商。TDS 将信道状态信息作为合法设备之间的公共秘密，并只允许物理距离在一定距离之内的设备使用密钥。该方案具有高效、健壮等优点，能够有效防御可预测信道攻击，并支持群组密钥协商，适用于分布式场景。然而，由于物理距离的限制，该方案的短板也十分明显。同样针对于移动设备，Ma 等人[21]指出 VANET 中的信道是开放且不安全的，并提出了一种基于二元多项式的轻量级认证密钥协商(Authenticated Key Agreement，AKA)协议，以保证通道的安全。该协议通过密钥协商在车辆与路边单元之间建立共享会话密钥，并通过智能合约协商后续的密钥更新与撤销。Wang 等人[76]针对基于边缘计算与区块链的智能电网系统，提出了一种双向 AKA 协议。该协议基于身份注册，以保证新的成员变动不影响现有成员。此外，该协议能够使用区块链中的智能合约，确保只有注册机构能够将公钥与对应用户的真实身份一一对应，从而提供了条件可追溯性和可撤销性。Kumar 等人[77]针对分布式的无人机网络，提出了一个安全 AKA 方案，支持无人机、边缘服务器和云服务器之间的双向认证与密钥协商，保证了通信数据的安全性。此外，该方案能够充分利用区块链场景中基于智能合约的共识机制，使点对点云服务器能够使用经过无人机认证的数据进行交易验证、区块创建与添加。Yu 等人[67]基于哈希函数和异或运算等轻量级加密原语，提出了一种轻量级的 AKA 方案，确保了数据共享的完整性与去中心化特性，并将其运用于基于区块链的无人机自组织网络中。Xie 等人[68]提出了一种包含密钥协商的高效隐私保护切换认证协议(BEPHAP)，基于对称加密和变色龙哈希函数等轻量级的加密原语，实现了密钥协议的匿名跨域相互切换认证。Cui 等人[69]为基于区块链的跨域工业物联网提出了一种高效的 AKA 协议，能够在跨域认证过程中产生只能在通信实体之间共享的会话密钥。该协议将边缘计算与基于假名的隐私保护方法

相结合，由边缘服务器生成假名，消除了对可信第三方的依赖，确保了设备的条件匿名性。

为进一步提升安全性，兼顾前向安全性与后向安全性，研究者们提出了一系列群组中的密钥协商方案。Hashimoto 等人[70]提出了链式 CmPKE，这是一种带宽成本非对称的连续群组密钥协商(Continuous Group Key Agreement，CGKA)，能够在动态群组中连续更新群组成员之间的共享密钥，从而保证通信的安全性。在群成员更新密钥的过程中，该方案的消息上传和下载开销不同，总体开销较之前的方法(如 TreeKEM)有所下降。此外，Hashimoto 等人为该协议提出了后量子原语，进一步降低了上传消息的开销，提升了效率。然而，现有的非对称群组密钥协商无法有效控制协议参与者的访问。为解决该问题，Li 等人[71]提出了一种非对称群组密钥协商协议。该协议通过细粒度的访问控制保护用户的身份信息，并通过多方属性基数字签名减少开销。此外，该协议能够结合应用场景中区块链的不可篡改性与可追溯性保证交易过程信息的完整性，配合智能合约实现自动验证，并在云服务中存储一些关键信息来实现前向安全性与后向安全性。Alwen 等人[72]引入服务器辅助 CGKA(saCGKA)概括标准的 CGKA 通信模型，并提出了一个高效的 CGKA 协议(SAIK)。该协议在 ITK[78]的基础上进行了修改，用多消息多接收者 PKE(mmPKE)取代 ITK 中标准的(CCA 安全)PKE，大大降低了通信和计算复杂度。此外，Alwen 等人还为 saCGKA 引入了一个直观而精确的安全模型，使得 SAIK 的安全证明更简单、更模块化。Alwen 等人[79]考虑到分布式网络环境中的并发情况，提出了一种支持并发操作的高效 CGKA 协议，通过增加更新轮次并引入服务器辅助计算技术，在支持并发的前提下兼顾了安全性与效率。该协议解决了以往 CGKA 协议在并发更新和大规模群体中效率低下的问题，更加适用于区块链等大规模动态分布式环境。针对 CGKA 协议在恶意网络环境中由于用户视图不一致而面临的群组状态统一(也称为分叉恢复)问题，Alwen 等人[80]提出了一种分叉容忍的 CGKA 扩展协议。该协议支持乱序网络流量处理和群组状态提取技术，在实现高效分叉恢复的同时，保留了 CGKA 的可扩展性和前向安全性。为了使 CGKA 更加适应区块链等去中心化结构，Weidner 等人[81]将安全的群组消息应用于去中心化网络，消除了对服务器的信任依赖，定义了一种新的密码学原语，去中心化连续群组密钥协商(Decentralized CGKA，DCGKA)，并给出了一个协议实例。该协商协议结合伪随机数生成器(Pseudorandom Generator，PRG)与密钥推断函数，采用一种特殊的密钥更新机制，实现了前向安全性与后向安全性，能够在动态群组中持续更新、协商密钥，支持安全通信，并合理应对并发情况。

DKG 是一种分布式协议，能够使各参与方在不相互信任且不存在可信第三方的情况下生成共享密钥，以确保安全通信和多方参与的机密性。近年来，DKG 的发展取得了重大进展，为解决效率问题，Kokoris-Kogias 等人[73]提出了首个异步分布式密钥生成(Asynchronous DKG，ADKG)算法，并去除了共识算法所依赖的可信设置假设。该方案引入了高阈值异步可验证秘密共享(Asynchronous Verifiable Secret Sharing，AVSS)，通过非对称双变量多项式对秘密进行编码，并构建了一种名为“最终完美共同硬币”的抽象概念，从而实现了首个 ADKG 和可验证的异步拜占庭协议(VABA)，并具有较低的复杂度。自此，ADKG 成为了解决效率问题的一大热点，不少研究者投入其中。Abraham 等人[82]同样基于 AVSS 技术构造 ADKG 与 VABA 协议。与以往的方案相比，该方案在同等的开销的情况下实现了适应性安全，在面对更强大的威胁模型时依然能够稳定运行，增强了协议的安全性与适用性。然而，在重构阈值大于总节点的三分之一的场景下，现有的 ADKG 方案效率低下。为解决此问题，Das 等人[83]基于他们之前的工作(PADKG)，提出了一种简单高效的 ADKG 协议[74]，可容忍至多 $t$ 个恶意节点，并支持任意大于 $t$ 的阈值。该方案以一个异步协议为核心，对一个阶数为阈值的随机多项式进行秘密共享，从而实现高阈值 ADKG 协议。

综上所述，在不断追求效率提升的同时，为了适应现代网络环境和应用需求，分布式密钥协商不断引入新的技术和方法，逐渐增添了异步性、灵活性、前向安全与后向安全性。然而，为了增强灵活性和动态性，现有方案忽略了对频繁变动造成安全隐患的讨论。

### 3.5 分布式审计

虽然区块链具有不可篡改性和可追溯性，但它主要关注的是数据的存储与传输安全，并不能保证数据的真实性、合规性与有效性，因此需要引入基于密码技术的审计机制。然而，区块链中具有大量的终端设备和节点，易受恶意攻击、篡改或滥用，集中式审计方法无法应对如此复杂的网络环境。分布式

审计能够充分利用区块链去中心化的特性，通过多个节点之间的协作，收集、存储系统中的日志数据，并进行过滤、交叉验证与校验，从而确保审计数据的准确性和一致性，使审计过程更加公正和可靠。本小节对现有分布式审计方案进行了归纳与总结，部分方案对比如表 5 所示。

**表 5　分布式审计方案对比**

| 方案 | 审计方式 | 审计方 | 审计对象 | 理论支撑 |
|---|---|---|---|---|
| SCRAPS[84] | 内部 | 智能合约 | 远程用户的身份合法性 | 数字签名 |
| Express[85] | 外部 | 三台服务器 | 客户端与服务器的行为 | 对称加密 |
| BEDAS[86] | 内部 | 智能合约 | 存储者的行为 | 承诺、数字签名 |
| PEReDi[87] | 内部 | 审计委员会 | 交易参与方的行为 | 数字签名 |
| BDDA[88] | 内部 | 审计节点 | 存储者的行为 | 数字签名 |
| CUSTOS[89] | 内部 | 各节点的审计组件 | 日志完整性 | 承诺、数字签名 |
| DELIA[90] | 外部/内部 | 第三方审计员/服务器联盟 | 日志完整性 | 数字签名 |

区块链系统中存在着众多情况复杂的参与者，为确保区块链系统的安全性和可信性，对参与方身份实行有效审计显得至关重要，它能够验证各参与者的身份合法性，防止未经授权的访问和潜在的恶意行为。远程认证是一种对用户身份进行验证的过程，通常用于确保远程用户访问系统或服务的身份合法性。为满足现代需求，解决单点故障问题并提升效率，Petzi 等人[84]将验证者的职责外包给智能合约以实现可扩展性，并利用数字签名弥补智能合约不提供保密性这一缺点，构建了可扩展的集散远程认证(SCRAPS)，缓解了针对验证者与被验证者的 DoS 攻击。此外，SCRAPS 中的证据是可公开验证的，大大减少了证明的计算开销。

即使参与者身份合法，也可能存在恶意行为，因此仍有必要对区块链中各方的行为进行审计。Zheng 等人[91]在他们基于安全多方计算的端到端协作学习平台(Cerebro)中添加了加密审计机制。该机制令各方对私有计算期间使用的输入生成承诺与数字签名，并假设诚实但好奇的审计第三方对各方进行审计，使各方对其行为负责。然而，该方案仍未解决对可信第三方的依赖问题。Eskandarian 等人[85]提出了一种高效的元数据隐藏通信系统(Express)，采用含有三台服务器的架构与对称加密，提供针对任意数量的恶意客户端和一个恶意服务器的加密安全性。该系统中包含一种新的审计协议，能够检测格式错误的消息，不仅比 Riposte[92]的效率更高，还消除了对审计第三方的依赖。Du 等人[86]结合多项式承诺和 BLS 签名提出了一个满足安全性和效率要求的存储审计框架，通过零知识审计保护区块链中存储审计方案的完整性，并优化了概念验证原型，显著地提高了链上与链下的审计效率。此外，该存储审计方案可扩展到动态场景，并从参与者的角度进一步提高可用性。Kiayias 等人[87]提出了一种新的中央银行数字货币模型(PEReDi)与一种兼具隐私性与可监管性的高效分布式框架，可承受少量恶意参与方。该框架使用加密工具抵御中间人攻击，并包含一种新颖的可追溯机制，较之前的方案有显著的性能提升。此外，当发送方和接收方诚实时，该框架能够消除拜占庭协议或广播，大大简化通信模式以降低通信开销。为及时地对区块链中实体的行为进行审计，Zhang 等人[88]提出了一种具有时效性的动态数据审计方案，将时间戳封装到由数字签名构造的同态可验证标签中，同时验证数据的完整性和时间戳的有效性，并利用 Merkle 哈希树存储标签，从而允许块级的动态操作。

区块链日志记录着交易信息、智能合约的调用和执行结果等内容，是验证交易合法性的基础，如果日志被篡改，整个区块链的安全性和完整性将受到威胁。因此，对日志的完整性进行审计是必要的。Paccagnella 等人[89]提出了一个系统日志篡改检测框架(CUSTOS)，该框架由一个防篡改日志层和一个分布式审计协议组成，前者负责降低日志更新成本，后者负责实时检测侵害日志完整性的行为。该方案通过对区块链中日志块上生成的增量哈希进行签名，生成加密时间承诺，并将其与日志一起存储以实现审计功能。此外，该方案利用现成的可信执行环境，分离加密事件承诺与日志，安全地降低记录成本。Chen 等人[90]提出了一种高效的分布式日志完整性审计框架(DELIA)，采用分布式账本对审计信息进行保护，并采用状态通道提高分布式账本的吞吐量。此外，该框架通过对日志状态生成数字签名，确保日志的完整性和不可篡改性，使得域中服务器或外部审计员能够有效检测到日志的变动，从而实现有效的域内监督。此外，该框架还包括一种日志状态生成方案(LSG)，以便在频繁更新的日志中生成稳定的日志状态，以及一种用于降低延迟的分层

多方状态通道方案(HMSC)。

综上所述,分布式审计方案逐渐摆脱了对可信第三方和外部审计员的依赖,并在效率和准确率上取得了一定的进步。然而,现有的分布式审计方案大多存在委员会或审计机制过于复杂的问题,严重影响了审计的时效性与可靠性。

## 4 构造思想

本节列出了适用于区块链的分布式密码学方案中几种主流的构造思想,并选取了几篇具有代表性的经典方案作为示例,通过梳理其中涉及的理论支撑与构造思路,重点介绍了如何运用分布式密码学解决区块链隐私问题。本节旨在为读者梳理目前主流的技术路线,深入理解各方案解决问题的思路,并分析其优劣与在实际应用中的可行性。

### 4.1 分布式密码框架

为提升密码学框架的灵活性与鲁棒性,将其运用于去中心化的区块链,破解单一中心带来的单点故障是解决问题的关键。对于该问题,摒弃对可信第三方的依赖,转为使用拓展性更强的委员会是一条重要的解决思路。

Benhamouda 等人[12]基于动态委员会,将阈值密码学应用于去中心化的现代区块链中,加强了对隐私的保护。该方案中的动态委员会在全体参与方中通过子采样产生,其成员仅承担临时任务,并频繁地进行随机更换,以躲避攻击者的定位与攻击,提升系统的安全性。该方案建立在多秘密分享者可验证秘密共享的基础上,即多个秘密分享者(Dealers,$D_i$)共同将秘密分割成多个部分,分发给各个参与方,并使得在一定条件下,份额持有者(Shareholders,$SH_j$)能够重建出原始的秘密。在秘密分享者和份额持有者之间存在两个中间委员会,一个称为验证委员会(Verification Committee,$VC_k$),负责验证份额并将其发给份额持有者,另一个称为响应委员会(Response Committee,$RC_l$),负责在验证失败时进行相应的处理。大致的协议如下:

(1)初始化参数:$n\geq 2t-1$,群$\mathbb{G}$的生成元向量$\boldsymbol{G}=(G_0,G_1,\cdots,G_n)$。

(2)各秘密分享者$D_i(i\in[n])$拥有秘密$s_i\in\mathbb{Z}_q$,随机选取$t-1$次多项式$f_i(\cdot)$,$f_{ij}(\cdot)$与$g_{ik}(\cdot)$,令$f_i(0)=s_i$,$f_i(k)=s_{ik}$,$f_{ij}(0)=s_{ij}$,$f_{ij}(k)=\epsilon_{ijk}$,$g_{ik}(0)=e_{ik}$,$g_{ik}(k)=e_{ikl}$,$\boldsymbol{\epsilon}_{ik}=(\epsilon_{ik0},\epsilon_{ik1},\cdots,\epsilon_{ikn})$,其中$j,k,l\in[n]$,$e_{ik}$为$D_i$与$VC_k$通信的对称密钥。用$e_{ik}$将$\boldsymbol{\epsilon}_{ik}$加密为$E_{ik}$,并计算列检验值$\mathcal{C}_{ik}=\sum_{j=0}^{n}\epsilon_{ijk}G_j$与$\boldsymbol{e}_{il}=(e_{i1l},e_{i2l},\cdots,e_{inl})$的承诺$Com_{il}$。向验证委员会广播$\{\mathcal{C}_{ik},E_{ik},e_{ik}\}$,向响应委员会广播$\{Com_{il},e_{il}\}$。

(3)各验证委员会成员$VC_k$解密出所有$\boldsymbol{\epsilon}_{ik}$,并验证各$\mathcal{C}_{ik}$,如验证失败则广播对$D_i$的指控。提出超过$t$个指控的验证委员会成员将被忽略,收到超过$t$个指控的$D_i$将被认为是不合格的。对于所有剩下的$D_i(i\in\mathbb{N}_k)$,令$\boldsymbol{\epsilon}'_{jk}=(\epsilon_{ijk})$,用与$D_i$相同的方法构造对$\boldsymbol{\epsilon}'_{jk}$的承诺$Com'_{jk}$。令$\boldsymbol{Com}'_k=(Com'_{1k},Com'_{2k},\cdots,Com'_{nk})$,$\boldsymbol{a}_k=(a_{ik})\in\mathbb{Z}_q^{|\mathbb{N}_k|}\leftarrow O(l,\boldsymbol{Com}'_k,\mathbb{N}_k)$,并计算$\mathcal{P}_{jk}=\sum_{i\in\mathbb{N}_k}\epsilon_{ijk}a_{ik}$与行检验值$\mathcal{R}_{jk}=\mathcal{P}_{jk}G_j$,其中$O$为随机预言机。计算$NIZK_{jk}:\mathcal{P}_{jk}=DL_{G_j}(\mathcal{R}_{jk})$以证明两个离散对数相等。将$\boldsymbol{\epsilon}'_{jk}$发送给$SH_j$,并广播$(Com'_{jk},\mathcal{R}_{jk},NIZK_{jk})$。

(4)各响应委员会成员$RC_l$响应指控$(VC_k\rightarrow D_i)$,解密出$\boldsymbol{e}_{il}$,获得并向$SH_j$广播$e_{ijl}$及其承诺。

(5)各份额持有者$SH_j$用响应委员会广播的$e_{ijl}$及其承诺恢复出$\boldsymbol{\epsilon}_{ik}$,并对$\mathcal{C}_{ik}$进行检验以进一步淘汰不诚实的秘密分享者。对于未被忽略的$VC_k$,检验其承诺、$NIZK_{jk}$、$\mathcal{R}_{jk}$以及$\sum_{u=0}^{n}\mathcal{R}_{ku}=\sum_{i\in\mathbb{N}_k}a_{ik}\mathcal{C}_{ik}$。若最后剩下的验证委员会成员少于$t$,$SH_j$终止协议,否则用有效份额恢复秘密$s_i$。

该协议的优越性在于其不仅使用了阈值密码学技术保障系统的鲁棒性,还通过动态且随机地选择委员会成员,将验证、指控等特殊权限短暂地分给系统中的部分节点,降低了恶意节点长期干扰系统正常运作的可能性,使系统能够抵抗静态敌手,并提升了对于动态敌手的抵抗能力。

### 4.2 分布式密钥管理

保护密钥是确保通信和数据安全的基础,集中式密钥管理存在单点故障的风险,因此分布式的密钥管理显得尤为重要。分布式密钥管理允许多个节点共同参与密钥的管理,其中包括对密钥进行分布式存储,不仅具有传统密钥管理的保密性与安全性,还具有一定的容错性与可拓展性。与分布式密码框架类似,引入节点委员会也是分布式密钥管理的一大技术路线。

Maram 等人[23]引入节点委员会进行密钥的分布式存储,在他们的方案中,委员会能够通过 Shamir 秘密共享对用户的密钥进行分布式备份与恢复,大致流程如下:

(1) 参与方 $P$ 进行备份注册，随机选取一个公钥 $pk$，生成一个经过身份认证的预证书 $PC=(ID, Com, pk, \pi)$，其中 $Com$ 为对 $P$ 的身份 $ID$ 的承诺，$\pi$ 表示已经过身份认证。

(2) 验证者 $V$(委员会成员或公共验证者)利用数字签名对预证书 $PC$ 进行验证，确认参与方 $P$ 的身份，即验证 $P$ 拥有与 $pk$ 对应的私钥 $sk$。

(3) 委员会 $C=\{C_1, C_2, \cdots, C_n\}$ 通过 Shamir 秘密共享对参与方 $P$ 的私钥 $sk$ 进行备份，各成员 $C_i$ 分别获取其分片 $sk_i$，将其与参与方 $P$ 的相关信息 $ID_{\text{key}}$(由 $ID$ 生成)进行绑定，并存储$(ID_{\text{key}}, sk_i)$。

(4) 当参与方 $P$ 恢复丢失的密钥 $sk$，重复注册步骤，由 $ID$ 推导出与密钥分片 $sk_i$ 绑定的相关内容 $ID_{\text{key}}$，并将其发送给各委员会成员 $C_i$，以获取 $sk_i$，恢复出原密钥 $sk$。

由 Shamir 秘密共享的性质可知，该协议中的参与方 $P$ 需要至少 $t$ 个 $sk$ 的分片以恢复密钥，因此该方案具备一定的鲁棒性。与其他基于秘密共享的协议相比，该方案的优越性在于支持参与方通过零知识参数提供信息凭证，而无需将所有身份信息暴露给委员会，这使得委员会无法获取指定参与方的真实身份信息，从而提供了成员隐私。

### 4.3 分布式数字签名

分布式数字签名作为传统数字签名在分布式场景下的拓展，不仅继承了传统数字签名身份验证、保护数据完整性与防止篡改的功能，还能够适应分布式系统，允许多个签名者合作，实现相同的安全目标。因此，众多研究者将分布式数字签名广泛应用于区块链隐私保护领域，并形成了多种技术路线与构造思想。本小节将以两个具有代表性的方案为例，对两种常用的构造思想进行简单介绍。

#### 4.3.1 HE&ZKP

HE 与 ZKP 的搭配是构造分布式数字签名最常用的方式之一，在分布式场景中，HE 的特性能够使方案在隐私保护的前提下引入更多的数据处理方，而 ZKP 则能够在不泄露任何具体信息的情况下，证明签名者确实拥有有效密钥或确为诚实方。Gennaro 等人[30]引入 Paillier 加密，提出了 MtA 协议，将方案中的乘共享转化加共享，并采用 ZKP 确保发布签名共享的有效性。

在该方案中，各签名者 $P_i$ 拥有签名私钥分片 $x_i$、随机数分片 $k_i$ 等用于签名的信息，并需要在生成数字签名时用这些分片计算 $kx$ 等信息。以 $kx$ 为例，可以根据分片的共享方式将其拆成下列形式：

$$kx=\sum_{i,j\in S}k_i x_j,$$

其中 $S$ 为签名者集合。由上式可知，为了得到完整的 $kx$，签名者需要进行两两之间的非线性运算，开销较大。针对该问题，基于 Paillier 加密的 MtA 协议能够在互相不暴露 $k_i$ 与 $x_j$ 的前提下，将 $k_i x_j$ 转化为 $\alpha_{i,j}+\beta_{j,i}$，从而避免了非线性运算，降低了计算开销。该协议大致步骤如下：

(1) $P_i$ 计算 $K_i=\text{Enc}_i(k_i)$，发送给 $P_j$。

(2) $P_j$ 选取 $\beta_{j,i}$，计算 $D_{i,j}=(K_i \odot x_j)\oplus \text{Enc}_i(-\beta_{j,i})=\text{Enc}_i(k_i x_j-\beta_{j,i})=\text{Enc}_i(\alpha_{i,j})$，发送给 $P_i$。

(3) $P_i$ 解密 $D_{i,j}$，得到 $\alpha_{i,j}$。

该方案的 ZKP 主要出现在两个部分，首先是在密钥生成的最后阶段，各方 $P_i$ 通过 Schnorr 协议[93]证明其拥有 $x_i$，并通过任何与整数分解相关的 ZKP，证明其拥有 HE 中与 RSA 相关的两个大质数 $p_i$ 与 $q_i$。另一部分出现在形成有效签名的最后阶段，首先在 $P_i$ 计算 $g^{k^{-1}}$ 时，也需要其通过 Schnorr 协议证明其拥有随机数 $\gamma_i$。其次，在生成共享分片和将其广播之间，$P_i$ 需要选取 $c_i, d_i\in\mathbb{Z}_q$，计算并广播 $V_i=g^{k^{-1}\sigma_i c_i}$，$C_i=g^{d_i}$，$D_i=g^{c_i d_i}$。随后 $P_i$ 通过 ZKP 证明其拥有 $\sigma_i$ 与 $c_i$，该证明遵循以下用于验证诚实性的经典 ZKP：

(1) 证明者 $P_i$ 选取 $a_i, b_i\in\mathbb{Z}_q$，并发送 $\alpha_i=g^{k^{-1}a_i b_i}$ 与 $\beta_i=C_i^{b_i}$。

(2) 验证者 $P_j(j\neq i)$ 发送一个随机挑战 $rc\in\mathbb{Z}_q$。

(3) 证明者 $P_i$ 回复 $u_i=a_i+rc\cdot\sigma_i \bmod q$ 与 $t_i=b_i+rc\cdot c_i \bmod q$。

(4) 验证者 $P_j$ 验证：$g^{k^{-1}u_i t_i}=\alpha_i V_i^{rc}$ 与 $C_i^{t_i}=\beta_i D_i^{rc}$。

ECDSA 的签名构造过程中存在如 $kx$ 这样的非线性运算，而在门限场景中，其计算时间受参与方数量影响较大，导致签名效率低下。针对这一问题，该协议通过 HE 将非线性运算转换为计算时间更短的线性运算，降低了构造签名的复杂度，显著提升了签名算法的效率。然而，HE 和 ZKP 的引入为签名的构造带来了额外的开销，在签名效率上仍有提升的空间。

#### 4.3.2 秘密共享 &OT

$t$-of-$n$ 门限签名允许 $n$ 个签名参与方共同生成一个公钥，并各自拥有其对应私钥的共享分片。同样针对于 ECDSA 中的非线性运算，Doerner 等人[31]避免使用开销较大的 HE 与 ZKP，而是采用 OT 构造 MtA 协议，将其与秘密共享机制结合构造分布式数字签名，并将方案中的门限 ECDSA 签名

的阈值从 2 推广到了不超过参与方总数的任意阈值 $t(t\leq n)$。

在该协议中,假设 Alice 为发送者,拥有的秘密分片为 $\boldsymbol{\alpha}\in\mathbb{Z}_q^{\ell}$($\ell$ 为向量维度),Bob 为接收者,拥有的秘密分片为 $\boldsymbol{\beta}\in\mathbb{Z}_q^{\ell}$,二者要在互相不暴露 $\boldsymbol{\alpha}$ 与 $\boldsymbol{\beta}$ 的前提下,分别获取 $\boldsymbol{a},\boldsymbol{b}\in\mathbb{Z}_q^{\ell}$,并使得

$$\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{\alpha}\cdot\boldsymbol{\beta},$$

从而消除开销较大的非线性运算。为达到此目的,首先取 $\boldsymbol{v}\in\mathbb{Z}_q^{\ell}$作为公共工具向量,用于添加掩码,Bob 计算

$$\boldsymbol{B}\leftarrow\{0,1\}^{\ell\cdot\xi},$$

$$\tilde{\boldsymbol{\beta}}:=\{\langle\boldsymbol{v},\{\boldsymbol{B}_j\}_{j\in[i\cdot\xi+1,(i+1)\cdot\xi]}\rangle\}_{i\in[1,\ell]},$$

并将 $\tilde{\boldsymbol{\beta}}$ 作为其掩码,其中 $\xi$ 为向量中每个元素的随机选择位数。Alice 计算

$$\tilde{\boldsymbol{\alpha}},\hat{\boldsymbol{\alpha}}\leftarrow\mathbb{Z}_q^{\ell},$$

$$\boldsymbol{A}:=\{\tilde{\alpha}_1\|\hat{\alpha}_1\}_{j\in[1,\xi]}\|\cdots\|\{\tilde{\alpha}_n\|\hat{\alpha}_n\}_{j\in[1,\xi]},$$

并将 $\tilde{\boldsymbol{\alpha}}$ 作为其掩码。然后 Alice 和 Bob 调用 OT 协议,以 $\boldsymbol{A},\boldsymbol{B}$ 为各自的输入,获得协议返回的输出

$$\boldsymbol{O}_A=\{\tilde{\boldsymbol{a}}_j\|\hat{\boldsymbol{a}}_j\}_{j\in[1,\ell\cdot\xi]},$$

$$\boldsymbol{O}_B=\{\tilde{\boldsymbol{b}}_j\|\hat{\boldsymbol{b}}_j\}_{j\in[1,\ell\cdot\xi]},$$

并对共享的秘密分片减去掩码以防止其暴露,然后将结果发给对方。在接收到结果之后,计算转换为加法共享之后的分片

$$\boldsymbol{a}:=\left\{\boldsymbol{\alpha}_i\cdot(\boldsymbol{\beta}_i-\tilde{\boldsymbol{\beta}}_i)+\sum_{j\in[1,\xi]}\boldsymbol{v}_j\cdot\tilde{\boldsymbol{a}}_{i\cdot\xi+j}\right\}_{i\in[1,\ell]},$$

$$\boldsymbol{b}:=\left\{\tilde{\boldsymbol{\beta}}_i\cdot(\boldsymbol{\alpha}_i-\tilde{\boldsymbol{\alpha}}_i)+\sum_{j\in[1,\xi]}\boldsymbol{v}_j\cdot\tilde{\boldsymbol{b}}_{i\cdot\xi+j}\right\}_{i\in[1,\ell]}。$$

该方案的核心思想在于其舍弃了开销较高的 HE 与 ZKP,仅基于 OT 给出了一种双方的 MtA 协议,使得原本双方之间的乘共享转换为加共享。此外,对于多方情景,可以通过组合与并行化处理双方 MtA 协议,实现多方 MtA 协议,从而实现高效的多方门限签名。

### 4.4 分布式密钥协商

分布式场景中,往往不存在可信的第三方进行密钥分发,因此需要各参与方相互通信,进行密钥协商。分布式不仅保留了传统密钥协商的机密性、完整性与安全性,还允许多个参与者在分布式环境中合作来生成密钥。分布式密钥协商的对象可以是通信密钥,也可以是签名密钥,这使得分布式密钥协商成为区块链、多方计算和云安全等领域中的重要工具。本小节将以具有代表性的方案为例,简单介绍两类常见的分布式密钥协商的构造思想。

#### 4.4.1 连续群组密钥协商

连续群组密钥协商(CGKA)作为一种密码学技术,能够持续地进行群组成员之间的安全密钥协商,因此常被用于动态变化的群组中。在区块链等复杂的分布式环境中,群组成员可能频繁变化,或者密钥本身需要定期更新,因此需要一种机制来支持群组内成员的动态变化。Ratchet(棘轮)是一种密码学机制,能够在特定条件触发后或定期更新密钥,以保持通信的安全性,因此常被用来实现 CGKA。Weidner 等人[81]通过多个棘轮与 PRG 进行密钥更新,保证了群组中的前向安全性与后向安全性,实现了去中心化的 CGKA(DCGKA)。

该方案的核心思想是用棘轮连续更新密钥,用不同的密钥加密每条消息以实现前向安全性。图 3 显示了棘轮的基本原理,其中不同的密钥 $k_i$ 各自负责一对明文($m_i$)与密文($c_i$)之间的加解密。PRG 负责根据当前的棘轮状态,不断生成新的密钥与棘轮状态,使敌手无法用当前的密钥对之前的消息进行解密。后向安全性则需要通过更新秘密 $s_i$ 实现,起初棘轮通过 $s_1$ 对状态进行初始化,并生成最初的一些密钥 $k_i$。当达到特定条件时,可以通过输入新的 $s_i$,重新生成与之前状态不相关的棘轮状态与新的密钥。这使得只知道之前的棘轮状态,而不知道更新秘密 $s_i$ 的敌手无法获取更新后的棘轮状态与密钥,从而实现了后向安全性,因此这种棘轮状态与密钥的更新被称为后向安全性更新。

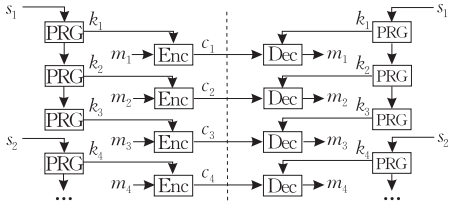



图 3 连续群组密钥协商的棘轮

各参与方都有棘轮结构,只要获得相同的更新秘密 $s_i$,各方就能够生成通用的密钥 $k_i$,因此,CGKA 的实现可以被简化成生成一系列可用的更新秘密 $s_i$。为减少密钥更新时的通信次数,Weidner 等人定义了一个新的随机值 *seed*,由需要更新的一方生成并广播,供其他参与方计算更新秘密 $s_i$。

与其他方案相比,该 CGKA 协议的优越性在于使用了 PRG 与棘轮结构持续更新密钥,并引入了更新秘密 $s_i$ 更换 PRG 的随机种子,将密钥更新的消息数量从 $O(n^2)$降低至 $O(n)$,在保证 DCGKA 协议

的前后向安全性的同时兼顾了通信效率。

4.4.2　异步分布式密钥生成

与传统的密钥生成方法不同，异步分布式密钥生成(ADKG)在分布式系统中生成安全密钥时，不要求参与者的行动在时间上同步，这使得其较之传统方法更具灵活性与鲁棒性。因此，异步分布式密钥生成被广泛应用于复杂多变，或不易实现时间同步的区块链分布式系统中。异步分布式密钥生成通常使用一些先进的密码学协议和技术，其中，高阈值异步秘密共享是实现异步分布式密钥生成的重要技术路线之一。

Kokoris-Kogias 等人[73]利用一种名为“共同硬币”的抽象概念，为异步环境提供了共同随机性来源，并结合高阈值 AVSS，提出了第一个 ADKG 算法。该方案基于 Cachin 等人[94]的 AVSS 方案，并将其拓展至高阈值情况，给出以下定义。

**定义 1.**　$n$ 方群组中，恶意参与方数量为 $f$，秘密重构阈值为 $t$，且 $f+1<t\leq n-f$。HAVSS 协议“$ID.ss$”由以下两个阶段组成：

(1) 分享阶段：分享者 $P_{ss}$ 将秘密 $s\in\mathbb{Z}_q$ 分享给接收者。若 $P_{ss}$ 发出消息($ID.ss$，$in$，$share$，$s$)，则称其开始了“$ID.ss$”的分享。若接收者发出消息($ID.ss$，$out$，$shared$)，则称其完成了“$ID.ss$”的分享。

(2) 重构阶段：参与方 $P_i$ 重构秘密，结果记为 $z_i$。若其发出消息($ID.ss$，$in$，$reconstruct$)，则称其开始了“$ID.ss$”的重构。若其输出消息($ID.ss$，$out$，$reconstructed$，$z_i$)，则称其完成了“$ID.ss$”的重构。

高阈值 AVSS 的主要机制利用了非对称双变量多项式，其中一个维度用于从 $t$ 个共享分片中恢复出秘密 $s$，另一个维度用于从 $f+1$ 个诚实参与方中恢复出共享分片。令 $p$，$q$ 为两个大素数且满足 $p|(q-1)$，$q>n$，其中 $n$ 为参与方数量，$\mathbb{G}$为$\mathbb{Z}_p$的 $q$ 阶乘法子群，$g$ 为$\mathbb{G}$的生成元。高阈值 AVSS 的大致流程如下：

(1) 交易者 $P_{ss}$ 计算秘密 $s$ 的一维共享，并用非对称双变量多项式对其进行二维共享。选取随机二元多项式 $v\in\mathbb{Z}_q[x,y]$，其中维度$[x]$的次数为 $t-1$，维度$[y]$的次数为 $f$。令 $v(0,0)=s$，且

$$v(x,y)=\sum_{j,k=0}^{t-1,f}v_{jk}x^jy^k。$$

令承诺矩阵$\mathbb{C}=\{Com_{jk}\}=\{g^{v_{jk}}\}$，其中 $j\in[0,t-1]$，$k=[0,f]$。交易者向各参与方 $P_i$ 发送消息，其中含有承诺矩阵$\mathbb{C}$，$t-1$ 阶的共享多项式 $a_i(x):=v(x,i)$ 与 $f$ 阶的恢复多项式 $b_i(y):=v(i,y)$。

(2) $P_i$ 接收到 $P_{ss}$ 的消息后，计算两个多项式中能够与其他参与方 $P_j$ 的多项式重叠的点，即 $a_i(j)$，$b_i(j)$，并将其与$\mathbb{C}$一并发送给 $P_j$。

(3) $P_i$ 在接收到 $t$ 个包含一致的承诺矩阵$\mathbb{C}$与有效重叠点的消息之后，运用插值法将消息中的点恢复成两个多项式 $\bar{a}_i(x)$与 $\bar{b}_i(y)$，并验证其是否与 $P_{ss}$ 发送的消息中的多项式(即 $a_i(x)$与 $b_i(y)$)吻合，若吻合则向其他参与方发送验证通过的消息。

(4) 一旦 $P_i$ 接收到 $n-f$ 条验证通过的消息，则其完成共享，共享分片为 $s_i=\bar{b}_i(0)$。为保证其余各方(包括诚实但响应较慢的参与方)也完成共享，$P_i$ 将通过验证的消息集合与 $a_i(j)$发送给 $P_j$。

(5) 对于诚实但响应较慢的参与方，它们接收 $f+1$ 个以上消息并间接完成共享。

因此在重建阶段，各诚实参与方 $P_i$ 能够在接收其他正确共享分片之后，通过插值法恢复出秘密 $s=v(0,0)$，再结合“共同硬币”为异步场景提供的公共随机性来源，实现完整的 ADKG 协议。

以往的 DKG 方案通常采用同步的秘密共享，需要参与者同步行动，导致等待时间较长，一定程度上限制了效率。相比之下，该方案引入了 AVSS，能够异步地进行分布式密钥生成，更加适用于区块链等分布式场景。

### 4.5　分布式审计

区块链中的数据操作分散在多个节点，传统审计难以有效跟踪或监控所有节点的活动。此外，传统审计通常依赖于集中的审计日志或数据库，面临着单点故障的风险。因此，不依赖可信的单一审计中心，能够监管多个节点的分布式审计更加适合区块链的审计场景。系统日志是审计的主要途径之一，因此，不少研究者从日志的分布式存储与审计入手，以实现对分布式系统的监管。

Paccagnella 等人[89]在防日志篡改的系统中，引入了一项去中心化的审计协议，能够近乎实时地检测日志的完整性，实现高效分布式审计。在日志生成阶段，所有的参与方在本地以区块的形式存储日志，并对其哈希值进行签名。在审计阶段，各参与方利用本地的审计组件对彼此的日志进行审计，通过验证签名与哈希值，判断日志是否经过篡改。去中心化审计协议大致如下：

(1) 参与方 $P_i$ 作为审计方，每隔时间 $T$ 进行一轮审计，随机挑选 $n$ 个参与方 $P_j$ 并生成审计挑战出 $c_{ij}=(ID_{c_{ij}},b_1,b_2)$，其中 $ID_{c_{ij}}$ 为挑战 ID，$b_1$ 和 $b_2$ 分别代表本次审计首位日志块的索引值且初始化为空，等待 $P_j$ 填入。用私钥 $sk_i$ 对所有挑战分别生成签名 $\sigma_{c_{ij}}=\mathrm{Sign}(c_{ij},sk_i)$，并与挑战 $c_{ij}$ 一同发送给 $P_j$。

(2)各 $P_j$ 响应审计挑战,令 $b_2=e$,其中 $e$ 为当前最新的日志块,调整 $b_1$ 的值,使本次审计的内容包括本地未被审计达到 $r$ 次(审计之前设定)的日志块。用私钥 $sk_j$ 对日志块 $L_l(l\in[b_1,b_2])$ 生成签名 $\sigma'_{jl}=\mathrm{Sign}(L_l,sk_j)$,并将其与日志块 $L_l$ 串联,得到 $L=L_{b_1}\|\sigma'_{jb_1}\|\cdots\|L_{jb_2}\|\sigma'_{jb_2}$,再将其与 $ID_{c_{ij}}b_1b_2$ 串联,用私钥 $sk_j$ 生成签名 $\sigma'_{\mathrm{msg}}=\mathrm{Sign}(ID_{c_{ij}}\|b_1\|b_2\|L,sk_j)$。将所有 $L_l$,$\sigma'_{jl}$ 与 $\sigma'_{\mathrm{msg}}$ 发给对应审计方 $P_i$。

(3)审计方 $P_i$ 等待并处理响应,通过检验接收的各种数据的完整性进行审计,并判定出以下三种审计结果:

① 在时间 $\tau(\tau\leq T)$ 内没有接收到响应,判定为审计挑战失败。

② 在规定时间内接收到响应,且通过所有验证,判定为日志未被篡改。

③ 在规定时间内接收到响应,存在未通过的验证,判定为日志已被篡改。

(4)审计方 $P_i$ 向通过验证的 $P_j$ 发送以 $sk_i$ 签署的确认信息。若 $P_j$ 在时间 $\tau$ 内收到确认消息,则更新本地日志块的被审计次数。若 $P_j$ 在时间 $\tau$ 内未收到确认消息,则舍弃审计挑战 $c_{ij}$。

该审计方案的核心之处在于通过签名与哈希值验证日志的完整性,并采用了定期审计机制,在审计的过程中为审计挑战设置了响应时限,将超出时间的审计挑战判定为失败,从而实现了对日志完整性的实时检测。

# 5 方案分析

## 5.1 安全性分析

安全性是密码技术关注的焦点之一,鉴于本文涉及的密码技术众多导致安全性分析不够集中,本节将总结如何对密码技术进行安全性分析。如前文所述,适用于区块链的密码技术可根据功能和层次分为基础密码算法、应用密码协议和整体密码方案。

基础密码算法和应用密码协议通常具有较为完整的安全模型和安全性证明,其安全性可以归约到已知的数学困难问题(如离散对数问题)上,这使得密码技术的安全性与这些困难问题紧密相关。此外,这两类技术的安全性还与威胁模型和规约过程中所做的安全假设息息相关,例如是否依赖随机预言机模型、攻击者是否具备适应性攻击能力等。假设越强,意味着方案安全性依赖的前提条件越多,实际的安全性保障就相对越弱。因此,通过分析威胁模型和假设的合理性,可以有效地评估基础密码算法和应用密码协议的安全性。对于以二者为主要内容的分布式数字签名与分布式密钥协商,我们在表 3 和表 4 中列出了各方案采用的安全模型和假设,以帮助读者对其安全性进行分析比较。

整体密码方案通常结合了多种密码算法或协议,涉及复杂的系统模型。在安全性分析中,此类方案需要明确敌手的身份和能力,例如敌手是否具有主动攻击或协作能力,是否能够监听或篡改通信等。在对以上内容进行合理假设后,同样可将方案的安全性归约到特定的数学困难问题。然而由于整体方案的复杂性,这类密码技术需要综合分析各方面因素,其中包括多种攻击场景(例如针对不同类型或身份的攻击者,方案安全性的体现方式不同,规约的困难问题可能也不同),协议交互中可能的潜在漏洞,以及不同算法组合可能导致的安全性隐患等。因此,对整体密码方案进行安全性分析尤为具有挑战性,需在复杂的系统模型和威胁模型下进行全面细致的考量,以确保其安全性能够覆盖实际应用中的各种威胁。对于以整体密码方案为主要内容的分布式密码框架、分布式密钥管理与分布式审计,由于各方案实现的密码功能不同,其具体使用的困难问题和安全假设可能存在较大差异,不适合直接对此进行统一列举和比较。因此,我们围绕敌手能力和攻击场景等要素进行总结并列举在表 1、表 2 和表 5 中,以帮助读者分析比较这类密码技术的安全性。

## 5.2 性能分析

本节将通过理论分析与性能实验对各方案的性能表现进行评估,由于篇幅原因,我们首先从总体角度阐述如何对适用于区块链的密码技术进行性能分析,再以分布式数字签名中部分具有代表性的门限方案为例,进行具体且直观的性能分析与性能实验。

### 5.2.1 分析方式概述

总体而言,性能分析主要关注执行效率,即在实现预期功能的前提下,系统的计算开销、通信开销以及响应时间等方面的表现。对于分布式数字签名和密钥协商等技术,由于它们通常具有较为固定的流程来实现特定的密码功能,因此分析其计算复杂度和通信复杂度(如表 4)是一种直观且有效的方法。这种分析能够量化每个参与方的计算开销、消息传输的频率和大小,从而评估该类技术在不同规模和网络条件下的性能表现。然而,对于分布式密码框架、分布式密钥管理和分布式审计等技术,由于功能更为复杂且流程不固定,仅通过计算复杂度和通信复杂度来对比分析性能并不公平,不足以全面反映各方案的性能表现。在这些场景下,需要综合分析

系统在资源利用率、任务完成时间以及扩展能力等方面的表现。例如，评估技术在不同硬件环境下的计算和存储消耗、在大规模并发条件下的处理能力，以及在动态区块链网络中的响应效率等。

### 5.2.2　性能分析实例

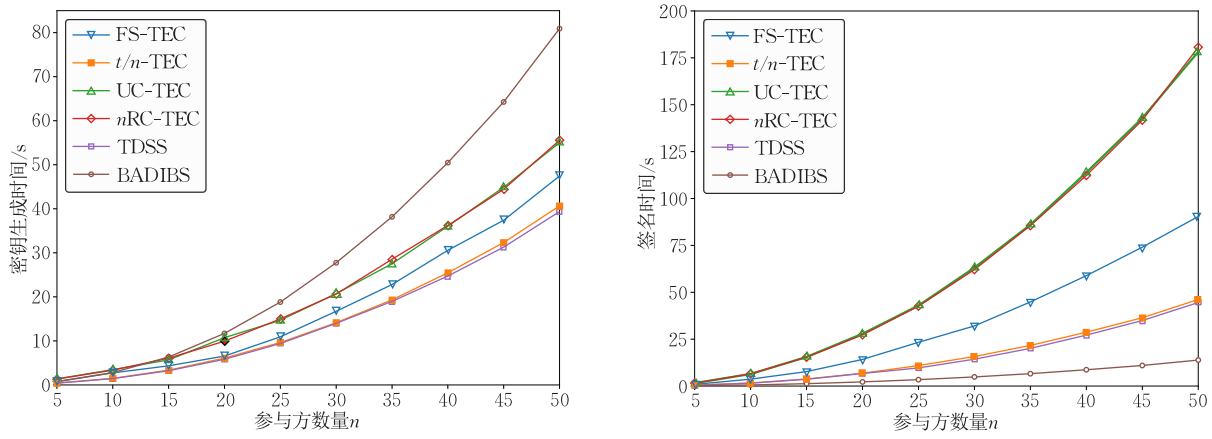
门限签名方案的核心思想在于实现门限机制，其通常的构造方式是通过秘密共享的形式为多个签名者生成签名密钥，令他们分别生成签名分片，随后聚合这些分片以实现门限签名。对于 ECDSA 等涉及非线性运算的签名算法，许多方案采用 MtA 协议将非线性运算转化为线性运算以提升协议的效率。MtA 协议以秘密 $a$ 与 $b$ 为输入，能够在不暴露二者的前提下向二者的持有者分别输出满足 $\alpha+\beta=ab$ 的 $\alpha$ 与 $\beta$，从而将秘密的乘共享转化为加共享。该协议有效地避免了多方之间效率较低的乘法运算，已被广泛应用于门限签名方案中，其主要实现方式有基于 HE 与基于 OT 两种(详细内容见第 4.3 节)。针对研究现状中的众多门限签名方案，我们重点关注 MtA 协议在门限签名方案中的应用这一挑战性议题，筛选出构造思想相近且具有一定开创性的方案作为实验对象。另外，对于同一批研究人员发表的类似于前作与续作的多篇论文，我们针对其中最新的研究成果进行实验。

如表 6 所示，我们从理论层面梳理了各方案的底层签名算法以及是否支持对签名进行预处理，并将各方案中 MtA 协议的构造方式分为了基于 HE 与基于 OT 两类。此外，我们总结了各方案的计算复杂度、通信轮数与签名长度。基于 HE 构造 MtA 协议的方案都进行常数轮的信息交互，各参与方在每一轮都需要与所有其他参与方进行通信，而基于 OT 构造 MtA 协议的方案则采用 $t/n$-TEC[31] 中提出的多方乘法协议，简化了每一轮的信息交互，但需要对数级的通信轮数。对于签名长度，门限签名算法最终生成的有效签名应与其所对应的单方签名形式相同，因此签名长度与验证时间也与单方签名方案相同。

**表 6　分布式数字签名方案性能对比**

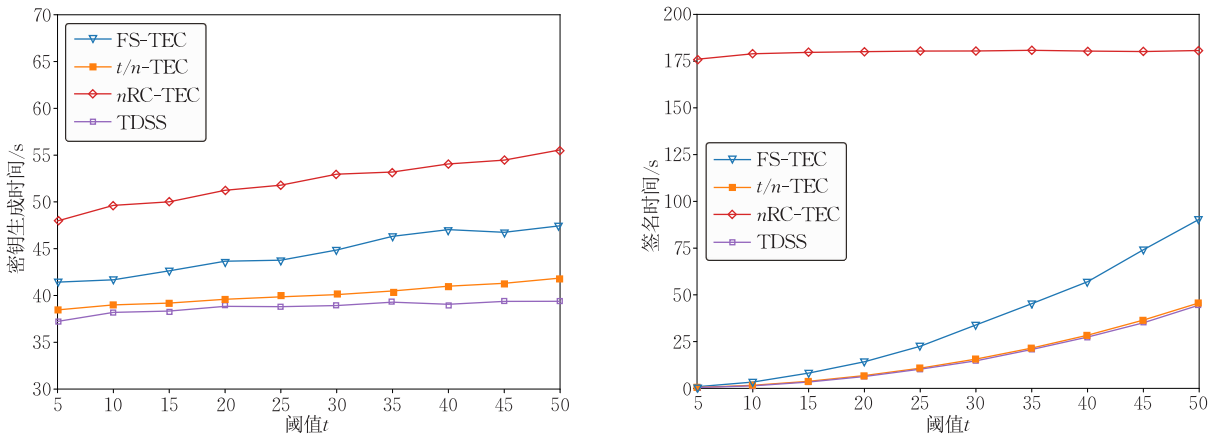
| 方案 | 签名算法 | MtA | 预处理 | 计算复杂度 | 通信轮数 | 签名长度 |
|---|---|---|---|---|---|---|
| FS-TEC[33] | ECDSA | HE | × | $O(n^2)$ | 15 | $2\lvert\mathbb{Z}_q\rvert$ |
| $t/n$-TEC[31] | ECDSA | OT | × | $O(n^2)$ | $\log t+6$ | $2\lvert\mathbb{Z}_q\rvert$ |
| UC-TEC[33] | ECDSA | HE | √ | $O(n^2)$ | 12 | $2\lvert\mathbb{Z}_q\rvert$ |
| $n$RC-TEC[35] | ECDSA | HE | √ | $O(n^2)$ | 16 | $2\lvert\mathbb{Z}_q\rvert$ |
| TDSS[37] | SM2 | OT | × | $O(n^2)$ | $\log t+3$ | $2\lvert\mathbb{Z}_q\rvert$ |
| BADIBS[38] | IBS | OT | × | $O(n^2)$ | $2\log t+3$ | $\lvert\mathbb{Z}_q\rvert+\lvert\mathbb{G}\rvert$ |

由于实际运行时间单位较小，易受代码编写的差异影响，为获得准确的实际运行时间，我们对各方案在同一环境下(Intel Core i9-10900X CPU@3.70 GHz)进行了对比实验。在表 6 所列出的方案中，UC-TEC[33] 与 BADIBS[38] 为 $n$-of-$n$ 的门限方案，因此我们首先令其余方案中的阈值 $t=n$，对所有方案的密钥生成阶段与签名阶段分别进行了实验，运行时间如图 4 所示，其中图(a)为密钥生成时间，图(b)为签名时间。此外，为探究阈值 $t$ 对门限签名的影响，我们将参与方数量 $n$ 设定为定值，计算了在阈值 $t$ 不同的情况下，各 $t$-of-$n$ 门限方案的密钥生成与签名时间，结果如图 5 所示。由实验结果可知，门限




(a) 密钥生成时间　　(b) 签名时间

图 4　分布式数字签名方案密钥生成时间与签名时间($t=n$)




(a) 密钥生成时间 (b) 签名时间

图 5 分布式数字签名方案密钥生成时间与签名时间($n=50$)

签名中密钥生成阶段的时间主要受到参与方数量 $n$ 的影响,而对于签名阶段,只有 $n$RC-TEC[35] 的签名时间受 $n$ 影响较大,其余的 $t$-of-$n$ 方案的签名时间主要由阈值 $t$ 决定。导致这一差异的原因是各方案的密钥生成阶段都是由所有参与方共同执行,但只有 $n$RC-TEC[35] 的签名阶段也由所有参与方执行,其余方案则是在签名阶段一开始就选出了 $t$ 个签名者执行该阶段,这也是 $n$RC-TEC[35] 指出的大多数方案无法实现真正的门限签名的原因。

## 6 挑战与未来展望

近些年,为解决区块链应用场景中的隐私问题,研究者们结合分布式密码学构造解决方案,尽管已经取得了显著的进展,但仍然存在一些挑战需要克服。本文从五个角度详细探讨了这一领域的研究现状,分析了各方案的优劣,并总结了以下几个有潜力的研究方向:

(1) 加强对异步通信方案的研究:现有方案绝大部分采用同步通信,导致系统等待时间较长,效率低下,且无法适应高并发情况,从而面临隐私保护不及时、拒绝服务攻击等安全问题。因此应推广异步通信机制,适当增加节点的离线计算量,增强其并发处理能力,舍弃非必要的节点通信,以减少通信轮数,减少通信阻塞,提升系统并发性与响应速度。

(2) 提出轻量级、非交互式的方案:现有方案计算与通信复杂度较高,使得这些分布式密码技术可能无法对区块链中的数据隐私进行及时的保护,从而造成安全隐患。因此,未来的研究应致力于提出轻量级与非交互式方案,例如结合轻量级、非交互式的 ZKP 以提升性能,确保在复杂环境下的高效运行。

(3) 避免频繁、随意的成员权限变化:尽管现有方案已支持成员权限的动态变化,但并未对权限变化进行有效的限制,容易造成权限管理混乱,面临隐私泄露的风险。为保障系统的稳定性与安全性,未来的解决方案应为权限变动添加限制,例如设置固定的权限更新周期,或采用门限签名等方式对成员变动进行投票,以维持系统的稳定运行。

(4) 优化委员会选举机制与审计机制:现有的委员会机制降低了通信开销,但其机制的复杂性仍是对效率的一大挑战,而长时间的选举机制与审计机制同样会导致隐私保护的延迟,造成安全隐患。未来的工作应侧重于优化委员会选举与审计机制,提高系统的效率与可靠性,例如引入属性基加密与访问控制策略,以简化对委员会成员与审计者的管理。

总体而言,分布式密码学与区块链的结合在以上各个领域都有巨大的潜力,但仍然需要克服一系列技术挑战。因此,未来的研究应该聚焦于实际的应用需求,对症下药,设计更多创新性与实用性并存的方案,为区块链及其应用场景带来更安全、更高效的解决方案。

## 7 总 结

区块链作为一种去中心化、可追溯的分布式账本技术,具有一定的安全优势,将分布式密码学应用于区块链场景,能够加强对隐私的保护。本文回顾了适用于区块链场景的分布式密码技术,梳理了主要的构造思想与技术路线,分析了各方案的性能优势与局限,为读者提供了评估与选择的参考。最后,本文讨论了当前的挑战,如系统响应时间较长和对复杂环境的适应性不足等问题。未来,我们期待通过进一步的研究与创新来克服这些挑战。分布式密码学与区块链的结合已经为隐私保护与数据安全提

供了强大的保障，但我们仍需持续努力以提出更高效、更安全的解决方案。我们相信，在不断创新下，分布式密码学与区块链将在保护用户隐私和数据安全方面取得更高的成就。

**致　谢**　感谢所有为本研究工作提供支持与建议的同行！

## 参　考　文　献


[1] Andrychowicz M, Dziembowski S. PoW-based distributed cryptography with no trusted setup//Proceedings of the CRYPTO 2015. Santa Barbara, USA, 2015: 379-399

[2] Zhu Lie-Huang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017, 54(10): 2170-2186(in Chinese)
(祝烈煌，高峰，沈蒙等. 区块链隐私保护研究综述. 计算机研究与发展，2017，54(10)：2170-2186)

[3] Li Xu-Dong, Niu Yu-Kun, Wei Ling-Bo, et al. Overview on privacy protection in bitcoin. Journal of Cryptologic Research, 2019, 6(2): 133-149(in Chinese)
(李旭东，牛玉坤，魏凌波等. 比特币隐私保护综述. 密码学报，2019，6(2)：133-149)

[4] Feng Qi, He De-Biao, Zeadally S, et al. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 2019, 126: 45-58

[5] Yao Shuang, Zhang Da-Wei, Li Yong, et al. A survey on privacy protection of transaction content in blockchain. Journal of Cryptologic Research, 2022, 9(4): 596-618(in Chinese)
(姚爽，张大伟，李勇等. 区块链交易内容隐私保护技术研究综述. 密码学报，2022，9(4)：596-618)

[6] Canetti R. Universally composable security: A new paradigm for cryptographic protocols//Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science. Newport Beach, USA, 2001: 136-145

[7] Lin Jen-Chiun, Chou Chun-Yen, Lai Fei-Pei, et al. A distributed key management protocol for dynamic groups//Proceedings of the 27th Annual IEEE Conference on Local Computer Networks(LCN 2002). Tampa, USA, 2002: 113-122

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

[9] Lee P, Lui J, Yau D. Distributed collaborative key agreement protocols for dynamic peer groups//Proceedings of the 10th IEEE International Conference on Network Protocols. Paris, France, 2002: 322-331

[10] Mounji A, Charlier B, Zampunieris D, et al. Distributed audit trail analysis//Proceedings of the 1995 Symposium on Network and Distributed System Security(NDSS 1995). San Diego, USA, 1995: 102-112

[11] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts//Proceedings of the 2016 IEEE Symposium on Security and Privacy. San Jose, USA, 2016: 839-858

[12] Benhamouda F, Halevi S, Krawczyk H, et al. Threshold cryptography as a service (in the multiserver and YOSO models)//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security(CCS'22). New York, USA, 2022: 323-336

[13] Xu Sheng-Min, Ning Jian-Ting, Li Xiao-Guo, et al. A privacy-preserving and redactable healthcare blockchain system. IEEE Transactions on Services Computing, 2024, 17(2): 364-377

[14] Awan S, Li Feng-Jun, Luo Bo, et al. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security(CCS'19). New York, USA, 2019: 2561-2563

[15] Zhu Jian-Ming, Zhang Qin-Nan, Gao Sheng, et al. Privacy preserving and trustworthy federated learning model based on blockchain. Chinese Journal of Computers, 2021, 44(12): 2464-2484(in Chinese)
(朱建明，张沁楠，高胜等. 基于区块链的隐私保护可信联邦学习模型. 计算机学报，2021，44(12)：2464-2484)

[16] Jia Bin, Zhang Xiao-Song, Liu Jie-Wen, et al. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. IEEE Transactions on Industrial Informatics, 2022, 18(6): 4049-4058

[17] Feng Lei, Zhao Yi-Qi, Guo Shao-Yong, et al. BAFL: A blockchain-based asynchronous federated learning framework. IEEE Transactions on Computers, 2022, 71(5): 1092-1103

[18] Aitzhan N, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 840-852

[19] Warnat-Herresthal S, Schultze H, Shastry K, et al. Swarm learning for decentralized and confidential clinical machine learning. Nature, 2021, 594: 265-270

[20] Lei Ao, Cruickshank H, Cao Yue, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 2017, 4(6): 1832-1843

[21] Ma Zhuo, Zhang Jun-Wei, Guo Yong-Zhen, et al. An efficient decentralized key management mechanism for VANET with blockchain. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5836-5849

[22] Long Yang-Yang, Peng Chang-Gen, Tan Wei-Jie, et al. Blockchain-based anonymous authentication and key management for Internet of Things with Chebyshev chaotic maps. IEEE Transactions on Industrial Informatics, 2024, 20(5): 7883-7893

[23] Maram D, Malvai H, Zhang Fan, et al. CanDID: Can-do decentralized identity with legacy compatibility, sybil-resistance,

and accountability//Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, USA, 2021: 1348-1366

[24] Li Jia-Xing, Wu Ji-Gang, Chen Long, et al. Blockchain-based secure key management for mobile edge computing. IEEE Transactions on Mobile Computing, 2023, 22(1): 100-114

[25] Shen Meng, Liu Hui-Sen, Zhu Lie-Huang, et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE Journal on Selected Areas in Communications, 2020, 38(5): 942-954

[26] Wang Hai-Xin, Xu Cheng, Zhang Ce, et al. vChain+: Optimizing verifiable blockchain Boolean range queries//Proceedings of the IEEE 38th International Conference on Data Engineering. Kuala Lumpur, Malaysia, 2022: 1927-1940

[27] Dodis Y, Jost D, Marcedone A. Compact key storage//Proceedings of the CRYPTO 2024. Santa Barbara, USA, 2024: 75-109

[28] Tan Liang, Yu Ke-Peng, Yang Cai-Xia, et al. A blockchain-based Shamir's threshold cryptography for data protection in industrial Internet of Things of smart city//Proceedings of the 1st Workshop on Artificial Intelligence and Blockchain Technologies for Smart Cities with 6G. New York, USA, 2021: 13-18

[29] Nair V, Song D. Multi-factor key derivation function (MFKDF) for fast, flexible, secure, & practical key management//Proceedings of the 32nd USENIX Security Symposium. Anaheim, USA, 2023: 2097-2114

[30] Gennaro R, Goldfeder S. Fast multiparty threshold ECDSA with fast trustless setup//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS'18). New York, USA, 2018: 1179-1194

[31] Doerner J, Kondi Y, Lee E, et al. Threshold ECDSA from ECDSA assumptions: The multiparty case//Proceedings of the 2019 IEEE Symposium on Security and Privacy. San Francisco, USA, 2019: 1051-1066

[32] Komlo C, Goldberg I. FROST: Flexible round-optimized Schnorr threshold signatures//Proceedings of the 27th International Conference on Selected Areas in Cryptography (SAC 2020). Halifax, Canada, 2020: 34-65

[33] Canetti R, Gennaro R, Goldfeder S, et al. UC Non-interactive, proactive, threshold ECDSA with identifiable aborts//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS'20). New York, USA, 2020: 1769-1787

[34] Ruffing T, Ronge V, Jin E, et al. ROAST: Robust asynchronous Schnorr threshold signatures//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22). New York, USA, 2022: 2551-2564

[35] Bouez A, Singh K. One round threshold ECDSA without roll call//Proceedings of the Topics in Cryptology- CT-RSA 2023: Cryptographers' Track at the RSA Conference 2023. San Francisco, USA, 2023: 389-414

[36] Wong H W H, Ma J P K, Yin H H F, et al. Real threshold ECDSA//Proceedings of the 30th Annual Network and Distributed System Security Symposium (NDSS 2023). San Diego, USA, 2023

[37] Chen Jing-Xue, Wang Zeng-Xiang, Srivastava G, et al. Industrial blockchain threshold signatures in federated learning for unified space-air-ground-sea model training. Journal of Industrial Information Integration, 2024, 39: 100593

[38] Li Ruo-Xia, Wang Zeng-Xiang, Fang Li-Ming, et al. Efficient blockchain-assisted distributed identity-based signature scheme for integrating consumer electronics in metaverse. IEEE Transactions on Consumer Electronics, 2024, 70(1): 3770-3780

[39] Itakura K. A public-key cryptosystem suitable for digital multisignature. NEC Research and Development, 1983, 71: 1-8

[40] Maxwell G, Poelstra A, Seurin Y. Simple Schnorr multi-signatures with applications to bitcoin. Designs, Codes and Cryptography, 2019, 87: 2139-2164

[41] Nick J, Ruffing T, Seurin Y, et al. MuSig-DN: Schnorr multi-signatures with verifiably deterministic nonces//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS'20). New York, USA, 2020: 1717-1731

[42] Nick J, Ruffing T, Seurin Y. MuSig2: Simple two-round Schnorr multi-signatures//Proceedings of the CRYPTO 2021. Virtual, 2021: 189-221

[43] Boschini C, Akira T, Mehdi T. MuSig-L: Lattice-based multi-signature with single-round online phase//Proceedings of the CRYPTO 2022. Santa Barbara, USA, 2022: 276-305

[44] Chen Yan-Bo. DualMS: Efficient lattice-based two-round multi-signature with trapdoor-free simulation//Proceedings of the CRYPTO 2023. Santa Barbara, USA, 2023: 716-747

[45] Drijvers M, Gorbunov S, Neven G, et al. Pixel: Multi-signatures for consensus//Proceedings of the 29th USENIX Security Symposium. Berkeley, USA, 2020: 2093-2110

[46] Xiao Yue, Zhang Peng, Liu Yu-Hong. Secure and efficient multi-signature schemes for fabric: An enterprise blockchain platform. IEEE Transactions on Information Forensics and Security, 2021, 16: 1782-1794

[47] Damgard I, Orlandi C, Takahashi A, et al. Two-round $n$-out-of-$n$ and multi-signatures and trapdoor commitment from lattices. Journal of Cryptology, 2022, 35: 14

[48] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures//Proceedings of the CRYPTO 1991. Santa Barbara, USA, 1991: 457-469

[49] Gennaro R, Goldfeder S, Narayanan A. Threshold-optimal DSA/ECDSA signatures and an application to bitcoin wallet security//Proceedings of the 14th International Conference on Applied Cryptography and Network Security (ACNS 2016). Guildford, UK, 2016: 156-174

[50] Lindell Y, Nof A. Fast secure multiparty ECDSA with practical distributed key generation and applications to cryptocurrency custody//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS'18). New York, USA, 2018: 1837-1854

[51] Doerner J, Kondi Y, Lee E, et al. Secure two-party threshold ECDSA from ECDSA assumptions//Proceedings of the 2018 IEEE Symposium on Security and Privacy. San Francisco, USA, 2018: 980-997

[52] Crites E, Komlo C, Maller M. Fully adaptive Schnorr threshold signatures//Proceedings of the CRYPTO 2023. Santa Barbara, USA, 2023: 678-709

[53] Bacho R, Loss J, Tessaro S, et al. Twinkle: Threshold signatures from DDH with full adaptive security//Proceedings of the EUROCRYPT 2024. Zurich, Switzerland, 2024: 429-459

[54] Bellare M, Crites E, Komlo C, et al. Better than advertised security for non-interactive threshold signatures//Proceedings of the CRYPTO 2022. Santa Barbara, USA, 2022: 517-550

[55] Xue Hai-Yang, Au M H, Xie Xiang, et al. Efficient online-friendly two-party ECDSA signature//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security(CCS'21). New York, USA, 2021: 558-573

[56] Bacho R, Loss J. On the adaptive security of the threshold BLS signature scheme//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22). New York, USA, 2022: 193-207

[57] Crites E, Komlo C, Maller M, et al. Snowblind: A threshold blind signature in pairing-free groups//Proceedings of the CRYPTO 2023. Santa Barbara, USA, 2023: 710-742

[58] Abram D, Nof A, Orlandi C, et al. Low-bandwidth threshold ECDSA via pseudorandom correlation generators//Proceedings of the 2022 IEEE Symposium on Security and Privacy. San Francisco, USA, 2022: 2554-2572

[59] Aggarwal A, Swain S. Poster: Correctness of $n$-parties ECDSA by the claim of byzantine agreement//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22). New York, USA, 2022: 3319-3321

[60] Cui Han-Dong, Chan Kwan-Yin, Yuen Tsz-Hon, et al. Bandwidth-efficient zero-knowledge proofs for threshold ECDSA. The Computer Journal, 2024, 67(4): 1265-1278

[61] Rivest R, Shamir A, Tauman Y. How to leak a secret//Proceedings of the ASIACRYPT 2001. Gold Coast, Austria, 2001: 552-565

[62] Bresson E, Stern J, Szydlo M. Threshold ring signatures and applications to ad-hoc groups//Proceedings of the CRYPTO 2002. Santa Barbara, USA, 2002: 465-480

[63] Haque A, Scafuro A. Threshold ring signatures: New definitions and post-quantum security//Proceedings of the 23rd IACR International Conference on Public-Key Cryptography(PKC 2020). Edinburgh, UK, 2020: 423-452

[64] Haque A, Krenn S, Slamanig D, et al. Logarithmic-size (linkable) threshold ring signatures in the plain model//Proceedings of the 25th IACR International Conference on Public-Key Cryptography(PKC 2022). Virtual, 2022: 437-467

[65] Aranha D, Hall-Andersen M, Nitulescu A, et al. Count me in! extendability for threshold ring signatures//Proceedings of the 25th IACR International Conference on Public-Key Cryptography(PKC 2022). Virtual, 2022: 379-406

[66] Avitabile G, Botta V, Fiore D. Extendable threshold ring signatures with enhanced anonymity//Proceedings of the 26th IACR International Conference on Public-Key Cryptography (PKC 2023). Atlanta, USA, 2023: 281-311

[67] Yu Sung-Jin, Lee J, Sutrala A, et al. LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted Unmanned Aerial Vehicle using blockchain in flying ad-hoc networks. Computer Networks, 2023, 224: 109612

[68] Xie Xian-Wang, Wu Bin, Hou Bo-Tao. BEPHAP: A blockchain-based efficient privacy-preserving handover authentication protocol with key agreement for internet of vehicles. Journal of Systems Architecture, 2023, 138: 102869

[69] Cui Bo-Tao, Zhu Yi-Hu, Zhong Hong, et al. Efficient blockchain-based mutual authentication and session key agreement for cross-domain IIoT. IEEE Internet of Things Journal, 2024, 11(9): 16325-16338

[70] Hashimoto K, Katsumata S, Postlethwaite E, et al. A concrete treatment of efficient continuous group key agreement via multi-recipient PKEs//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security(CCS'21). New York, USA, 2021: 1441-1462

[71] Li Ju-Yan, Qiao Zhi-Qi, Peng Jia-Liang. Asymmetric group key agreement protocol based on blockchain and attribute for industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2022, 18(11): 8326-8335

[72] Alwen J, Hartmann D, Kiltz E, et al. Server-aided continuous group key agreement//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security(CCS'22). New York, USA, 2022: 69-82

[73] Kokoris-Kogias E, Malkhi D, Spiegelman A. Asynchronous distributed key generation for computationally-secure randomness, consensus, and threshold signatures//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security(CCS'20). New York, USA, 2020: 1751-1767

[74] Das S, Xiang Zhuo-Lun, Kokoris-Koggias L, et al. Practical asynchronous high-threshold distributed key generation and distributed polynomial sampling//Proceedings of the 32nd USENIX Security Symposium. Berkeley, USA, 2023: 5359-5376

[75] Xi Wei, Qian Chen, Han Jin-Song, et al. Instant and robust authentication and key agreement among mobile devices//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16). New York, USA, 2016: 616-627

[76] Wang Jing, Wu Li-Bing, Choo K, et al. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Transactions on Industrial Informatics, 2020, 16(3): 1984-1992

[77] Kumar R, Aljuhani A, Kumar P, et al. Blockchain-enabled secure communication for unmanned aerial vehicle (UAV) networks//Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond. Sydney, Australia, 2022: 37-42

[78] Alwen J, Jost D, Mularczyk M. On the insider security of MLS//Proceedings of the CRYPTO 2022. Santa Barbara, USA, 2022: 34-68

[79] Alwen J, Auerbach B, Noval M, et al. CoCoA: Concurrent continuous group key agreement//Proceedings of the EUROCRYPT 2022. Trondheim, Norway, 2022: 815-844

[80] Alwen J, Mularczyk M, Tselekounis Y. Fork-resilient continuous group key agreement//Proceedings of the CRYPTO 2023. Santa Barbara, USA, 2023: 396-429

[81] Weidner M, Kleppmann M, Hugenroth D, et al. Key agreement for decentralized secure group messaging with strong security guarantees//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS'21). New York, USA, 2021: 2024-2045

[82] Abraham I, Jovanovic P, Maller M, et al. Adaptivity and asynchrony in verifiable secret sharing and distributed key generation//Proceedings of the CRYPTO 2023. Santa Barbara, USA, 2023: 39-70

[83] Das S, Yurek T, Xiang Zhuo-Lun, et al. Practical asynchronous distributed key generation//Proceedings of the 2022 IEEE Symposium on Security and Privacy. San Francisco, USA, 2022: 2518-2534

[84] Petzi L, Yahya A E B, Dmitrienko A, et al. SCRAPS: Scalable collective remote attestation for pub-sub iot networks with untrusted proxy verifier//Proceedings of the 31st USENIX Security Symposium. Berkeley, USA, 2022: 3485-3501

[85] Eskandarian S, Corrigan-Gibbs H, Zaharia M, et al. Express: Lowering the cost of metadata-hiding communication with cryptographic privacy//Proceedings of the 30th USENIX Security Symposium. Berkeley, USA, 2021: 1775-1792

[86] Du Yue-Feng, Duan Hua-Yi, Zhou An-Xin, et al. Enabling secure and efficient decentralized storage auditing with blockchain. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3038-3054

[87] Kiayias A, Kohlweiss M, Sarencheh A. PEReDi: Privacy-enhanced, regulated and distributed central bank digital currencies//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22). New York, USA, 2022: 1739-1752

[88] Zhang Chuan, Xuan Hao-Jun, Wu Tong, et al. Blockchain-based dynamic time-encapsulated data auditing for outsourcing storage. IEEE Transactions on Information Forensics and Security, 2024, 19: 1979-1993

[89] Paccagnella R, Datta P, Hassan W U, et al. CUSTOS: Practical tamper-evident auditing of operating systems using trusted execution//Proceedings of the 27th Annual Network and Distributed System Security Symposium (NDSS 2020). Berlin, Germany, 2020

[90] Chen Jing, Chen Xin, He Kun, et al. DELIA: Distributed efficient log integrity audit based on hierarchal multi-party state channel. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3286-3300

[91] Zheng Wen-Ting, Deng R, Chen Wei-Keng, et al. Cerebro: A platform for multi-party cryptographic collaborative learning //Proceedings of the 30th USENIX Security Symposium. Berkeley, USA, 2021: 2723-2740

[92] Corrigan-Gibbs H, Boneh D, Mazieres D. Riposte: An anonymous messaging system handling millions of users//Proceedings of the 2015 IEEE Symposium on Security and Privacy. San Jose, USA, 2015: 321-338

[93] Schnorr C. Efficient signature generation by smart cards. Journal of Cryptology, 1991, 4: 161-174

[94] Cachin C, Kursawe K, Lysyanskaya A, et al. Asynchronous verifiable secret sharing and proactive cryptosystems//Proceedings of the 2002 ACM SIGSAC Conference on Computer and Communications Security (CCS'02). New York, USA, 2002: 88-97

**HU Yun-Fan**, Ph. D. candidate. His research interests include cryptography and artificial intelligence security.

**XIONG Hu**, Ph. D., professor. His research interests include cryptography and blockchain.

**FANG Li-Ming**, Ph.D., professor. His research interests include cryptography, blockchain and artificial intelligence security.

**PENG Chang-Gen**, Ph. D., professor. His research interests include cryptography and information security.

**QIN Zhen**, Ph. D., professor. His research interests include artificial intelligence security and multi-source data fusion.

**QIN Zhi-Guang**, Ph. D., professor. His research interest is information security.

**Background**

As a revolutionary innovation, blockchain has achieved significant breakthroughs in various fields. However, with its widespread adoption, privacy concerns have become increasingly prominent, particularly in the context of blockchain scenarios. To address this issue, numerous solutions dedicated to privacy protection in blockchain technology and its applications have emerged internationally. Despite the existence of several surveys in this research area, few have comprehensively summarized and categorized the extensive research results from the perspective of distributed cryptographic techniques. Specifically, while existing research has produced a wide range of privacy protection solutions for blockchain, current surveys often lack a thorough analysis of construction principles and systematic examinations of available solutions. In previous studies, despite the presence of privacy protection solutions for blockchain, most of these solutions focus on specific technologies or application scenarios, lacking comprehensive reviews and comparative analyses of the overall research landscape.

Therefore, this paper aims to fill this gap by providing a comprehensive synthesis of the research achievements in the field of distributed cryptographic techniques, shedding light on the construction ideas and conducting in-depth analyses which have been lacking in existing surveys. This paper seeks to contribute to the research field by conducting an in-depth investigation into privacy protection issues within blockchain, offering a panoramic view from the perspective of distributed cryptographic primitives, and addressing the shortcomings in existing review literature. At the beginning, this paper primarily focuses on cryptographic primitives suitable for blockchain, providing a systematic review and comparative analysis of state of the art. Additionally, it will delve into specific technical methodologies and construction ideologies by exploring some selected classical solutions, in order to support the construction of more comprehensive and profound privacy protection schemes.

Through an in-depth exploration of privacy protection in the blockchain, this paper aims to provide theoretical support for strengthening the integration of distributed cryptographic techniques with blockchain technology. The ultimate goal is to lay a solid foundation for the development of more secure and efficient blockchain applications.

This work is supported by the National Key Research and Development Program of China (No. 2022YFB2701400), the National Natural Science Foundation of China (Nos. U22B2029, 62272228), and the Shenzhen Science and Technology Program (No. JCYJ20210324134408023).