GM/Y 5004-2024

数据安全密码技术应用研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

摘要

随着《数据安全法》和《个人信息保护法》的颁布实施，以及大数据、云计算、人工智能、区块链、数字货币等信息技术的快速发展，数据安全对于数字经济与大数据产业的健康发展越来越重要。密码技术是保障数据安全的核心技术和基础支撑，因此研究数据安全中的密码技术具有重要意义。

本报告的目的是研究保障数据安全的各种密码技术，分析各种密码技术的原理、特点、应用，总结现有的政策、法律法规和标准情况，为数据安全密码技术的标准制定打下坚实基础。本报告首先从数据和数据安全的涵义、全生命周期的安全需求等方面，分析密码技术在数据安全中的作用；然后，从基本的对称密码算法、非对称密码算法、密码杂凑算法、分组密码算法工作模式等方面，介绍了密码算法的种类和作用；重点分析了特殊数字签名、密文查询和计算、数据共享与访问控制、数据外包存储与计算等方面的典型密码技术与应用；最后，分析了国内外数据安全与密码相关的政策、法律和标准情况，并提出了制定数据安全密码技术应用指南的标准建议。

关键词：数据安全，密码算法，密码协议，密码技术

目录

前言

《数据安全密码技术应用研究》项目是由密码行业标准化技术委员会根据国家密码管理局批准的《2021 年密码行业标准制/修订计划》下达的标准研究任务，项目所属工作组为基础工作组。山东大学作为牵头单位，成立相应的编制工作组，组织完成该标准研究报告的编制工作。

本研究报告主要包括数据安全的各种密码技术以及应用，包括对称密码算法、非对称密码算法、密码杂凑算法等基本密码算法，用于数据共享与访问控制、数据密态查询与计算、数据外包存储与计算等应用场景的各种新型密码技术，以及国内外相关政策和标准制定情况，为各个数据安全领域提供密码技术应用指导和参考。

本报告起草单位：山东大学、三未信安科技股份有限公司、中国电力科学研究院有限公司、北京信安世纪科技股份有限公司、中国科学技术大学、中电科网络安全科技股份有限公司、兴唐通信科技有限公司、格尔软件股份有限公司、北京数字认证股份有限公司、北京国脉信安科技有限公司、中国科学院信息工程研究所。

本报告主要起草人员：孔凡玉、张岳公、高志权、刘会议、杨国强、翟峰、李智虎、汪宗斌、林璟锵、张立廷、王现方、王妮娜、郑强、夏鲁宁、袁峰、高能、李敏、陶云亭、孙欣蓉。

数据安全密码技术应用研究

1. 概述

1.1 数据内涵与价值

1.1.1 数据资源的价值

习近平总书记强调，发展数字经济是把握新一轮科技革命和产业变革新机遇的战略选择。2021年10月18日，习近平总书记在中共中央政治局第三十四次集体学习时强调：数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。2022年01月12日，国务院印发《“十四五”数字经济发展规划》[1]，明确了“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施。

数据资源是数字经济的关键要素，并已成为国家基础性战略资源。党的十九届四中全会指出，要“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制”，正式将数据作为生产要素。2020年4月9日，《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》将数据作为一种新型生产要素，明确要加快培育数据要素市场，推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护。《“十四五”数字经济发展规划》[1]提出，数据要素是数字经济深化发展的核心引擎，数据的爆发增长、海量集聚蕴藏了巨大的价值，为智能化发展带来了新的机遇。

1.1.2 数据的涵义

《中华人民共和国数据安全法》[2]（以下简称《数据安全法》），自2021年9月1日起正式施行。《数据安全法》给出了数据、数据处理等概念的定义：“数据是指任何以电子或者其他方式对信息的记录。数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。”《数据安全法》的颁布实施，有利于规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

数据与信息是两个既有联系又有区别的定义。根据百度百科对“信息”的解释，信息是指音讯、消息、通讯系统传输和处理的对象，泛指人类社会传播的一切内容。1948年，信息论开创者香农(Shannon)在论文“通讯的数学理论”中提出：“信息是用来消除随机不定性的东西”，这是在信息通信领域被广泛接受的定义。

因此，数据可以看作是信息的记录和载体，信息是数据的内在涵义和抽象价值，本研究报告中，将更多的采用“数据”这个词语。

1.2 数据安全内涵与外延

1.2.1 数据安全的涵义

《数据安全法》[2]给出了对“数据安全”的定义：“数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力”。维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

数据安全是一个广泛的概念，与网络安全、信息安全、计算机安全等安全概念紧密联系，又有所区别，以下是与数据安全相关的一些概念：

——《网络安全法》[3]给出了网络安全的定义：“网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力”。因此，网络安全既包含了网络系统安全，又包含了网络数据的完整性、保密性、可用性等安全范围。

——GB/T 25069-2010《信息安全技术 术语》给出了信息安全的定义：“信息安全，保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质”。

——美国 NIST SP 800-12《An Introduction to Computer Security: The NIST Handbook》将计算机安全定义为：“为自动化信息系统提供的保护，以达到保持信息系统资源(包括硬件、软件、固件、信息/数据、通信)的完整性、可用性和机密性的目标”。这就是著名的 CIA 三要素：机密性(Confidentiality)、完整性(Integrity)和可用性(Availability)。机密性(Confidentiality)在一些文献中又称为“保密性”，本报告中采用“机密性”这个名词。

——《密码法》[4]指出：“密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务”。传统密码技术包括数据加密算法、消息鉴别码/认证码、数字签名等，其主要作用是实现数据/信息的机密性、真实性、完整性和抗抵赖性。

通过对以上概念分析可知，数据安全应包括可用性、机密性、真实性、完整性、抗抵赖性等方面，同时，随着大数据应用的发展，数据安全还包括可追溯性、隐私性、安全共享、安全多方计算等方面。

密码技术是保障数据安全的核心技术和基础支撑，能够解决数据的机密性、真实性、完整性、抗抵赖性，并能够实现数据安全共享、安全多方计算、隐私保护等功能。2020 年 1 月 1 日，《中华人民共和国密码法》[4]正式实施，是我国密码领域的综合性、基础性法律。2021 年，《中华人民共和国数据安全法》[2]、《中华人民共和国个人信息保护法》[5]先后颁布实施，我国的数据安全相关法律体系日趋完善。随着大数据、云计算、人工智能、区块链、数字货币、物联网等信息技术的快速发展，数据安全对于数字经济与大数据产业的健康发展越来越重要，因此，研究数据安全中的密码技术以及应用具有重要意义。

本报告旨在对保障数据安全用到的密码技术进行研究，分析各种密码技术的原理、特点、应用，总结现有的政策、法律法规和标准情况，为数据安全密码技术的标准制定提供参考。需要注意的是，不是所有的数据安全问题都通过密码技术解决，有一些不是密码技术的范畴，例如，可用性需要通过多机备份、并行技术、集群技术等实现。本报告主要分析数据安全的密码技术和应用。

1.2.2 数据的全生命周期：各个阶段的安全需求

《“十四五”数字经济发展规划》提出，要提升数据安全保障水平，建立数据分类分级保护制度，研究推进数据安全标准体系建设，规范数据采集、传输、存储、处理、共享、销毁全生命周期管理。

《数据安全法》将数据处理的环节进行了定义：“数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等”。

根据 GB/T 25069-2022《信息安全技术 术语》第 3.572 条，数据生存周期是数据从

产生，经过采集、传输、存储、处理(包括计算、分析、可视化等)、交换，直至销毁等各种生存形态的演变过程。

根据 GB/T37988-2019《信息安全技术 数据安全能力成熟度模型》[6]，数据的生命周期分为采集、传输、存储、处理、交换和销毁六个阶段，数据在不同的生命周期阶段具有不同的安全需求：

数据采集安全：是组织内部系统新产生数据，以及从外部系统收集数据的阶段的安全。数据采集安全包括数据分类分级、数据采集安全管理、数据源鉴别及记录、数据质量管理四部分。a）对数据进行分类分级，对不同类别和级别的数据建立相应的访问控制、数据加解密、数据脱敏等安全管理和控制措施。b）对数据采集进行安全管理，明确采集数据的目的和用途，确保满足数据源的真实性、有效性和最少够用等原则要求，保证数据采集过程中个人信息和重要数据不被泄露，并对采集的数据进行校验，支持对数据采集和获取操作过程的可追溯。c）对数据源进行鉴别和记录，应对产生数据的数据源进行身份鉴别和记录，防止数据仿冒和数据伪造，并对追溯数据进行安全保护。d）建立组织的数据质量管理体系，保证对数据采集过程中收集/产生的数据的准确性、一致性和完整性，明确数据格式要求、数据完整性要求、数据源质量评价标准等要求。

数据传输安全：是数据从一个实体传输到到另一个实体的阶段的安全。数据传输安全包括数据传输加密和网络可用性管理。a）数据传输加密需要采用密码技术，保证传输通道、传输节点和传输数据的安全，包括传输通道两端的主体身份鉴别、传输通道加密(例如 SSL/TLS、IPSec 等)、数字签名、密钥管理等，防止传输过程中的数据泄露。b）网络可用性管理，则是指通过网络基础设施及网络层数据防泄漏设备的备份建设，实现网络的高可用性，从而保证数据传输过程的稳定性。

数据存储安全：是数据以数字格式进行存储的阶段的安全。数据存储安全包括存储媒体安全、逻辑存储安全、数据备份和恢复。a）存储媒体安全要求针对组织内需要对数据存储媒体进行访问和使用的场景，提供有效的技术和管理手段，防止因为对媒体的不当使用而引发数据泄露。b）逻辑存储安全要求组织能基于组织内部的业务特性和数据存储安全要求，建立针对数据逻辑存储、存储容器等的有效安全控制，包括身份鉴别、权限管理、访问控制，以及对个人信息、重要数据等敏感数据的加密存储能力、数据完整性保护等。c）数据备份和修复要求能够通过执行定期的数据备份和恢复，实现对存储数据的冗余管理，保护数据的可用性，包括对备份数据的压缩、加密、完整性保护、访问控制等。

数据处理安全：是指对数据进行计算、分析、可视化等操作的阶段的安全。数据处理安全包括数据脱敏、数据分析安全、数据正当使用、数据处理环境安全、数据导入导出安全。a）数据脱敏要求对敏感数据进行脱敏处理，保证数据可用性和安全性。b）数据分析安全要求在数据分析过程中要采取适当的安全控制措施，防止数据挖掘、分析过程中有价值信息和个人隐私泄露。c）数据正当使用要求保护国家秘密、商业秘密和个人隐私，防止数据资源被用于不正当目的。d）数据处理环境安全要求组织提供统一的数据计算、开发平台，确保数据处理过程中有完整的安全控制管理和技术支持。e）数据导入导出安全要求在对数据进行导入导出操作时，确保数据自身的可用性和完整性，降低可能存在的数据泄露风险。

数据交换安全：是组织与组织或个人进行数据交换的阶段的安全。数据交换安全包括数据共享安全、数据发布安全、数据接口安全。a）数据共享安全要求组织通过业务系统、产品对外部组织提供数据时，以及通过合作的方式与合作伙伴交换数据时执行共享数据的安全风险控制，以降低数据共享场景下的安全风险，采用的技术包括数据加密、数据脱敏等。b）数据发布安全要求在对外部组织进行数据发布的过程中，通过对发布

数据的格式、适用范围、发布者与使用者权利和义务执行的必要控制，实现数据发布过程中的数据的安全可控与合规。c）数据接口安全要求组织建立对外数据接口的安全管理机制，防范组织数据在接口调用过程中的安全风险，应采用技术实现对数据接口调用的身份鉴别和访问控制，跨安全域的数据接口调用应采用安全通道、加密传输、时间戳等安全措施。

数据销毁安全：是使数据彻底删除且无法通过任何手段恢复的过程的安全。数据销毁安全包括数据销毁处置、存储媒体销毁处置。a）数据销毁处置需要针对数据的删除、净化机制，实现对数据的有效销毁，防止因对存储媒体中的数据进行恢复而导致的数据泄露风险。b）存储媒体销毁处置要求建立存储媒体安全销毁的规程和技术手段，防止因存储媒体丢失、被窃或未授权的访问而导致存储媒体中的数据泄露的安全风险。

综上所述，数据生命周期的各个阶段的安全需求涉及到数据的机密性、完整性、可用性、不可抵赖性、可追溯性等，其中密码技术是数据全生命周期安全保障中的核心技术，可用于实现身份鉴别、访问控制、数据加密、数据完整性、数字签名、数据溯源等安全措施，有效保证数据采集、传输、存储、处理、交换和销毁等全生命周期安全。

2. 数据安全的密码技术

2.1 基本密码算法与技术

密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。传统密码技术包括数据加密算法、密码杂凑算法(Hash)、消息鉴别码/认证码(MAC)、数字签名、密钥协商协议、随机数生成等，其主要作用是实现数据和信息的机密性、真实性、完整性和抗抵赖性等。根据密钥的类型划分，密码算法包括对称密码算法、公钥密码算法(又称为非对称密码算法)和密码杂凑算法。

自 2012 年以来，国家密码管理局陆续发布了我国的一系列商用密码技术标准，密码算法、密码协议、密码产品、密码应用、密码检测等多个方面。GM/Y 5001-2021《密码标准使用指南》[7]给出了已颁布的密码标准的介绍和使用指南。密码算法标准包括 SM2、SM3、SM4、SM9、ZUC 算法(即“祖冲之密码算法”)等。其中 SM2、SM9 为公钥密码算法，SM3 为密码杂凑算法，SM4 为分组对称密码算法，ZUC 为序列密码算法。密码协议标准包括数字认证、访问控制、密钥交换/协商、密钥管理、安全通信等协议。

2.1.1 对称密码算法

对称密码算法是加密密钥和解密密钥为同一个密钥的密码算法，主要用于数据加密、消息鉴别码等，包括序列密码算法和分组密码算法。

GB/T 33133《信息安全技术 祖冲之序列密码算法》[8]规定了祖冲之（ZUC）序列密码算法，用于实现消息和数据的机密性和完整性保护。祖冲之密码算法是我国自主设计的序列密码算法，已被 3GPP 组织采纳为 LTE 的标准密码算法之一。祖冲之密码算法不仅适合于移动通信场景，也适用于其它的数据加密和完整性保护场景。

GB/T 32907《信息安全技术 SM4 分组密码算法》[9]规定了 SM4 分组密码算法，是一种密钥长度 128 比特，分组长度也是 128 比特的密码算法。SM4 分组密码算法用于实现对明文数据的加密保护，并可以通过 CBC-MAC 等工作模式实现数据的完整性保护。

2.1.2 非对称密码算法

非对称密码算法，又称为公钥密码算法，按功能可划分为非对称加密算法、数字签

名算法和密钥协商协议，可用于数据的机密性、完整性、真实性、抗抵赖性以及密钥协商等功能。非对称密码算法包含一对密钥：一个称为公钥（public key)，可以公开，用于加密或验证签名；一个称为私钥(private key)，必须保密，用于解密或数字签名。

GB/T 32918《信息安全技术 SM2 椭圆曲线公钥密码算法》[10]规定了基于椭圆曲线的 SM2 公钥密码算法，包括公钥加密算法、数字签名算法和密钥交换协议，可用于SSL/TLS、TLCP、IPSec 等网络安全协议，以及电子签章、电子支付等应用场景。

GB/T 38635《信息安全技术 SM9 标识密码算法》[11]规定了基于标识的 SM9 密码算法，其是构建在双线性对的困难问题之上的密码算法，可用于数据加密、数字签名、密钥协商等典型用途。在基于标识的密码算法中，用户公钥是由用户身份标识唯一确定的，例如身份证号、手机号、电子邮箱等，因此不需要使用“数字证书”绑定用户身份与其公钥的关系。用户标识对应的私钥由密钥生成中心（KGC）根据用户的标识计算而得出，因此密钥生成中心（KGC）拥有所有用户的私钥。

2.1.3 密码杂凑算法

密码杂凑算法(Hash 算法)是将任意长数据生成固定长度杂凑值的算法，在数据安全中具有广泛用途：（1）在数字签名机制中，首先使用密码杂凑算法对明文计算杂凑值，然后使用用户私钥对杂凑值签名，用于保护数据完整性、真实性和抗抵赖性；（2）在 HMAC 消息鉴别码机制中，可用于构造明文消息的“消息鉴别码（MAC）”，以保护数据完整性；（3）密码杂凑算法可用于伪随机数发生器和随机数发生器的后处理单元，确保随机数质量；(4)密码杂凑算法还常被用作登录口令保护，即对用户键入的口令计算杂凑值，将杂凑值传输或存储。

GB/T 32905《信息安全技术 SM3 密码杂凑算法》[12]规定了 SM3 密码杂凑算法，其是一种杂凑输出长度为 256 比特的密码杂凑算法可用于数字签名和验证、消息鉴别码的生成与验证、伪随机数的生成等应用场景。

2.1.4 抗量子密码算法

量子计算机的迅速发展给传统的 RSA 密码、ECC 等公钥密码体制带来严重的安全威胁。在量子计算机上设计的密码攻击算法，如 Shor 算法，能够在多项式时间内攻破 RSA、ECC 等传统密码算法；Grover 算法实现了穷举算法的质的提升，可以将 128 位密钥的 AES 算法的攻击复杂度从 2^{128} 降低到 2^{64}。这给基于大整数分解问题和离散对数问题的 RSA 密码算法、ECC 密码算法和对称密码算法的安全性带来了严重威胁。

在量子计算机迅速发展的同时，设计新一代的抗量子/后量子密码体制（Quantum-resistant Cryptosystem/Post-quantum Cryptosystem）具有重要意义。根据所基于的困难问题的类型，抗量子密码算法包括基于格的密码算法、基于多变量的密码算法、基于编码的密码算法等，其中基于格的密码算法被广泛认可。格密码在平均情况与最坏情况下具有相同的 NP 困难性，其矩阵运算和向量运算效率比较高，可用于设计基于身份加密（IBE）和全同态加密算法（FHE），成为后量子密码时代最重要的密码体制。

在标准化方面，2016 年，美国国家标准与技术研究院（NationalInstitute of Standards and Technology，NIST）开始征集抗量子密码算法标准。该标准征集工作中，基于格的密码体制占据了候选算法的主流。2022 年，NIST 公布了首批入选的四种抗量子算法（Crystals-Kyber、CRYSTALS-DILITHIUM、FALCON、SPHINCS+）。2018 年，中国密码学会首次举办全国密码算法设计竞赛，广大密码科技工作者积极响应，踊跃组队参加竞赛，共有 60 个密码算法（22 个分组算法，38 个公钥算法）进入竞赛，包括了多个

抗量子密码算法，积极推动了我国密码算法设计和实现技术的进步。

2.1.5 随机数生成和检测

随机数在密码学中具有重要地位，是生成对称密钥、非对称密钥等密钥参数的关键因子，也是产生初始加密向量、身份认证随机因子的关键元素。随机数包括真随机数和伪随机数：真随机数是通过自然界的温度、声音、辐射等物理现象获取的随机信息，在密码产品中常采用物理噪声源芯片等作为真随机数发生器；伪随机数是通过密码算法将一个随机数种子进行扩展得到的伪随机序列，密码学上使用的伪随机数应具有统计不可区分的安全性。

GB/T 32915《信息安全技术二元序列随机性检测方法》[13]是针对随机数序列的质量检测规范，适用于随机数发生器软硬件产品，或含有随机数发生器单元的密码产品的生产和检测。此标准规定的检测项目共有 15 项，包括单比特频数检测、块内频数检测、扑克检测、重叠子序列检测、游程总数检测、游程分布检测、块内最大"1"游程检测、二元推导检测、自相关检测、矩阵秩检测、累加和检测、近似性检测、线性复杂度检测等。

GM/T 0103《随机数发生器总体框架》给出了随机数发生器的设计框架，GM/T 0078《密码随机数生成模块设计指南》给出了硬件随机数发生器的设计指南，GM/T 0105《软件随机数发生器设计指南》给出了软件随机数发生器的设计指南。

2.1.6 密钥管理与 PKI/CA 体系

密钥是密码的核心参数，包括对称密钥和非对称密钥，其安全性至关重要。

GM/T 0051《密码设备管理对称密钥管理技术规范》[14]为密码设备制定了统一的对称密钥管理及相关安全技术标准，适用于对称密钥管理系统的研制、建设、运行及管理，包括对称密钥管理安全要求、系统体系结构及功能要求、密钥管理安全协议及接口设计要求、管理中心建设、运行及管理要求等。

在非对称密钥管理方面，主要采用基于数字证书的 PKI 公钥基础设施体系，由 CA 数字认证系统和相应的密钥管理系统进行管理；另外，基于标识的密码(ID-based)体系不需要使用数字证书，而是由一个可信的密钥生成中心（KGC）管理所有用户的私钥。

以数字签名、数字证书为代表的 PKI/CA 体系是现代密码学应用的典型代表。

GB/T 20518《信息安全技术 公钥基础设施数字证书格式规范》[15]、GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》[16]、GM/T 0014《数字证书认证系统密码协议规范》[17]等标准规定了数字证书和证书撤销列表的格式、安全协议流程、密码函数接口等内容，以及数字证书认证系统的设计、建设、检测、运行及管理规范，适用于数字证书认证系统的研发、数字证书认证机构的运营以及基于数字证书的安全应用。

电子签章是数字签名的典型应用场景之一，用于保障文件等数据的完整性和抗抵赖性。GM/T 0031《安全电子签章密码应用技术规范》[18]规定了电子签章产品的技术要求、数据结构和密码处理流程，用于规范电子签章的标准化和互联互通。

电子文件是电子数据的常用形式。GM/T 0055《电子文件密码应用技术规范》[19]规范了电子文件保护所涉及的密码技术，通过绑定文件和标签形成安全电子文件，由中间件实现电子文件的安全控制机制。

2.1.7 密码软件安全与白盒密码

密码算法软件实现的关键问题是保证密钥的安全性，而密码算法在 CPU 软件实现过

程中，密钥会以明文形式出现在内存中，存在被窃取的风险。白盒密码技术是解决密码软件安全的方法之一。

白盒密码的安全模型，是假定攻击者能够完全控制密码算法运行环境的情形，可以获取算法的运行状态、读取任何信息等。2022 年，Chow 首先提出了白盒密码的概念(White-box cryptography)，并设计了基于混淆和查表方法的 AES 和 DES 的白盒密码算法，其基本原理是将密钥隐藏于密码算法的运算过程中，而明文密钥不再直接出现，因此攻击者即使控制了整个密码运算过程，也很难分析出密钥。后来，很多研究者又设计了一系列白盒密码算法，并不断被破解和分析。

白盒密码技术适用于采用软件方式实现密码算法的数据安全应用场景，例如数字版权保护(DRM)、移动终端安全等应用领域。需要注意的是，如果没有其他安全措施的话(例如与设备的绑定、使用权限等)，攻击者把白盒密码软件复制并运行在相同的计算环境中，虽然不能分析出密钥，但是可以进行加解密运算。因此，白盒密码除了抵抗数学攻击的安全性，还需要通过一系列措施防止被攻击者非法使用。

2.2 分组密码算法的工作模式-数据加密和鉴别

分组密码算法每次加密运算处理一个分组数据，例如 SM4 算法的分组长度为 128 比特。分组密码算法处理多个分组数据的方法，称为分组密码算法的工作模式。分组密码算法的工作模式主要用来实现加密和鉴别(认证)，用于保证数据的机密性、完整性、真实性；一些工作模式将加密和认证相结合，称为可鉴别的加密机制(认证加密模式)。

GB/T 17964-2021《信息安全技术 分组密码算法的工作模式》[20]规定了分组密码算法的九种工作模式，包括 ECB、CBC、CFB、OFB、CTR、XTS、HCTR、BC、OFBNLF 等模式，用于保护数据的机密性，不适用于保护数据完整性。

GB/T 15852.1-2008《信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制》[21]规定了分组密码算法的六种消息鉴别码机制，可用于数据完整性检验、消息源合法性验证。

GB/T 36624-2018《可鉴别加密功能的工作模式》[22]规定了五种可鉴别的加密机制，将分组加密和鉴别机制结合，用于实现数据机密性、完整性和数据源鉴别。

2.2.1 ECB/CBC/CFB/OFB/CTR 模式

ECB/CBC/CFB/OFB/CTR 模式是分组密码算法的几种常用工作模式。

ECB 模式是将每一个分组分别独立加密，可以实现多个分组之间的并行加密/解密运算。但是，由于明文中相同的分组，密文也相同，当敌手得到多个明文密文对时，可以进行已知明文攻击。

CBC 模式的加密方式是将前一段密文与当前的明文段进行异或运算后再加密，安全性更好；加密不能并行处理，解密可以并行；CBC 加密模式可用于实现消息鉴别码。

OFB 与 CFB 适合用于对流数据的加密。

CTR 模式（Counter mode，CM）称为计数器模式，通过加密一个递增的计数器产生密钥流，将密钥流与明文异或得到密文，具有可并行性等优点。

2.2.2 块存储加密和 XTS 模式

GB/T 17964-2021《信息安全技术 分组密码算法的工作模式》[20]和 IEEE P1619《Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices》[23]标准均规定了 XTS 加密工作模式，适合于以数据单元(例如扇区、逻辑磁

盘块等)为基础结构的磁盘加密等块存储加密的应用场景。

XEX 结构(Xor-Encryption-Xor (XEX) construction)是构造可调分组密码的一种结构，明文分组与掩码相异或后，使用分组密码算法加密，再将密文分组与掩码相异或。

XTS 工作模式(XEX tweakable block cipher with ciphertext stealing)，即带密文挪用的 XEX 可调分组密码工作模式，分组密码算法的一种工作模式，利用 XEX 结构完成数据的加密和解密。

2.2.3 可鉴别加密模式与 AEAD 机制

可鉴别的加密机制(authenticated encryption mechanism)是同时提供数据机密性、完整性和数据源鉴别的分组密码算法工作模式,例如GCM模式和CCM模式。又称为AEAD，即 Authenticated encryption with associated data (AEAD)，也就是带附加数据的加密和鉴别算法

GCM(Galois/Counter Mode)模式是将 CTR 加密模式与 GMAC 消息鉴别码相结合的可鉴别加密机制，适用于 IPSec、SSL/TLS、TLCP 等网络安全协议的传输加密保护。GMAC(Galois Message Authentication Code)是利用伽罗华域（Galois Field，GF，有限域）乘法运算来计算消息的 MAC 值。

CCM(counter CBC-MAC)模式是将 CTR 加密模式与 CBC-MAC 消息鉴别码相结合的可鉴别加密机制，也是一种常用的可鉴别加密模式。

2.2.4 保留格式加密

在数据加密实际应用场景中，需要对个人身份信息、电子邮箱、信用卡号等敏感信息进行加密。当采用传统的加密技术对敏感数据进行加密时，可能会改变数据类型和数据长度，从而破坏数据和数据库的原始结构，影响数据的使用。

保留格式加密（Format-Preserving Encryption，FPE）将明文加密成相同格式的密文，即密文的类型、长度与明文相同，能够保证密文和明文具有相同的格式。密码行业标准研究报告《基于国密算法的保留格式加密(FPE)研究》[24]和刘哲理等的文献[25]对保留格式加密进行了详细的分析和研究。

保留格式加密(FPE)自 1981 年提出后，至今已有 40 多年的研究历史，近几年随着数据安全需求的快速增长，保留格式加密(FPE)成为一个研究热点。2002 年，Black 和 Rogaway 提出三种常用的保留格式加密(FPE)构造方法为：Prefix、Cycle-walking、Generalized-Feistel。目前常用的三种加密模型分别是：FFSEM、FFX、RtE 模型。

美国 NIST 在 2016 年发布了 NIST SP 800-38G，描述了 FPE 的两种操作模式 FF1 和 FF3，其加密算法使用 AES 分组密码算法。为了防止中间相遇(meet-in-the-middle)攻击,FF1 和 FF3 要求的最低 radixminlen 不小于 100,但是通常建议其值至少为一百万。2016 年以来，研究者对 FF1 和 FF3 进行了多种密码分析攻击，NIST 在 2019 年 2 月 28 号发布了 FPE 标准的修正版《Draft NIST Special Publication 800-38G Revision 1 Recommendation for Block Cipher Modes of Operation Methods for Format-Preserving Encryption》，给出了修正后的 FF1 和 FF3 算法结构。

FPE 被提出后,已经有很多国际公司对其进行研究并应用在各自的产品中。2008 年，美国 Voltage 公司公布了软件工具包 SecureData 安全产品以及采用的 FPE 技术的白皮书，介绍了已有的 FPE 研究成果，提出了社会保险号和信用卡号的 FPE 方案。

密码算法可以作为一种重要的数据脱敏技术，尤其是 FPE 加密模式能够保持数据格式的不变，具有广泛的数据安全应用场景。FPE 作为一种分组密码算法的工作模式，既具有可解密的特点，又不改变数据类型和数据长度，可以作为数据脱敏的一种有效方法。

2.3 具有特殊功能的数字签名算法

2.3.1 概述

数字签名（digital signatures）是公钥密码体制的重要组成部分，签名者使用自己的私钥生成签名，验证者使用签名者的公钥进行签名验证，数字签名用于实现数据的完整性、真实性和抗抵赖性保护。常见的数字签名算法包括 SM2 数字签名算法、RSA 数字签名算法、ElGamal 数字签名算法、Schnorr 数字签名算法、DSA 数字签名算法、ECDSA 椭圆曲线数字签名算法等。

在一些具体的应用场景和领域，需要具有特殊功能的数字签名算法，例如在群组环境下的群签名/环签名/多签名/门限签名/代理签名等，在电子支付等场景下的盲签名，以及将加密和签名功能合二为一的签密方案等，与传统的签名方案相比，能够满足更复杂场景下的安全需求。区块链系统具有很多特殊数字签名的应用场景，文献[45, 46, 47]介绍了一些数字签名的方案。

2.3.2 多签名/门限签名/群签名/环签名/代理签名

多签名/门限签名/群签名/环签名等数字签名方案是在一个群组/组织机构内的数字签名机制，实现所有人或其中某一部分成员共同进行签名的功能。

多签名（multi-signature）：1983 年，K. Itakura 和 K. Nakamura 首次提出多签名的概念[48]，实现多个用户一起对同一个消息进行签名，可以应用于一个组织机构内部需要多个部门或领导对某一个文件进行签名的应用场景。

门限签名（threshold signature）：1987 年，Yvo Desmedt 首次提出门限签名机制的概念[49]，将门限秘密分享机制用于数字签名，即 n 个签名人中的任意≥k 个签名人能够生成签名，但<k 个签名人则不能生成签名。

群签名（group signature）：1991 年，David Chaum 等首次提出群签名的概念[50]，一个群体中的任意一个成员可以匿名地代表整个群体对消息进行签名，签名结果可以通过公钥进行公开验证；需要追溯时，群管理员能够识别签名人的身份。

环签名（ring signature）：2001 年，Ron Rivest 等在 ASIACRYPT’01 提出环签名的概念(How to leak a secret, in: ASIACRYPT’01)，环签名是一种特殊的群签名，但是环签名没有管理员，不能识别签名人的身份。

代理签名（proxy signature）：1996 年，Masahiro Mambo 等首次提出代理签名的概念[51]，原始签名人能够指定代理签名人进行代理签名，但是并不需要泄露原始签名人的私钥。

Mambo 等提出了一个代理签名方案，该方案的过程描述具体如下：

1. 委托过程

   （1）A随机选取$k \in Z_q^*$，并计算$K = g^k mod\ p$；

   （2）A计算$\sigma = x_A + kK\ mod\ q$，然后将$(\sigma, K)$秘密地发送给$B$；

   （3）B检验$g^\sigma = y_A K^K\ mod\ p$，如果检验结果是等式不成立，那么$A$重新执行 1)。

2. 代理签名的生成过程

   B受到A发来的(σ, K)，使用值σ作为代理密钥计算$s = Sign_\sigma(m)$从而生成代理签名(s, K)，并发送给验证方。

3. 代理签名的验证过程

   在收到(s, K)后，验证人在知道消息m的情况下做出以下验证步骤：

（1）计算：$v = y_A K^K \ mod \ p$

（2）验证：$Ver(y_A,(s,K),m) = True \Leftrightarrow Ver(v,s,m) = True$。

2.3.3 盲签名（blind signature）

1982 年，David Chaum 首次提出盲签名的概念[52]，签名人在不知道消息内容的情况下，能够对盲化后的消息进行签名，保证了签名的匿名性和不可追踪性，可以用于电子银行、电子支付等应用场景。

RSA 盲签名方案：

令 n、d 和 e 分别为签名者的 RSA 密钥参数，其中 n 和 e 是公钥，d 是私钥。

（1）消息盲化：当消息拥有方需要签名者对消息 M 进行盲签名时，其中 M＜n，则其选取随机正整数 r ＜ n 使得 gcd(n,r) = 1，并用 r 作为盲化因子，然后计算：$M_r = M * r^e \ mod \ n$，并将 M_r 发送给签名者。

（2）盲签名：签名者对盲化后的消息 M_r 进行签名，得到 $s_r = M_r^d \ mod \ n$。

（3）去盲因子：因为 $de \equiv 1(mod\ \Phi(n))$ 且 gcd(n, r) = 1，所以从费马小定理可得 $r^{de} \equiv r(mod\ n)$，及 r 可逆，即 $r^{-1} \ mod \ n$ 有定义. 因此，消息拥有方可做如下运算将掩盖因子从 s_r 除去：

$(s_r \cdot r^{-1}) mod n.$

甲方可得

$s_M = s_r \cdot r^{-1} \ mod \ n$

$= M^d \cdot r^{de} \cdot r^{-1} \ mod \ n$

$= M^d \cdot r \cdot r^{-1} \ mod \ n$

$= M^d \ mod \ n.$

即消息拥有方获得了签名者对消息 M 的数字签名，但是签名方不能看到 M 的内容。

2.3.4 签密（signcryption）

1997 年，Yuliang Zheng 首次提出签密的概念[53]，将数字签名和加密功能集成在一个密码方案中，比传统的先签名后加密的分步骤方案具有更高的效率和更小的密文/签名数据量，可以用于同时需要加密和数字签名的应用场景，实现数据机密性、完整性、真实性和抗抵赖性保护。

Yuliang Zheng 提出的签密方案描述如下：设 p 是一个大素数，q 是 p-1 的一个大素因子，g 是一个 q 阶生成元，x_a 是签名者的私钥，$y_a=g^{xa}$ 是签名者的公钥。令 E 表示对称密码算法的加密算法，D 表示对称密码算法的解密算法。

（1）签名流程：

- 选取一个随机数 x，计算 $k=y_b^x \ mod \ p$，将 k 划分为 k_1 和 k_2；
- 计算 $r=Hash(k_2, m)$；
- 计算 $s=x/(r+x_a) \ mod \ q$；
- 计算 $c=E_{k1}(m)$；
- 则签密的密文为（c, r, s）。

（2）解密和验签流程：

- 通过 r, s , g, p, ya, xb 等数值，计算 $k=(ya*gr)s*xb \ mod \ p$；
- 将 k 划分为 k1 和 k2；
- 计算 m=Dk1(c)；
- 验证 r==Hash(k2, m)是否成立，如果成立则验证签名通过。

2.4 支持密文查询和计算的密码技术

2.4.1 半同态(部分同态)加密算法

2.4.1.1 概述

同态加密是支持对密文计算的加密算法，允许用户直接对密文进行特定运算，解密后的结果与对明文进行相同运算的结果一样。同态加密的优点是支持在数据密文状态下仍能进行各种计算，保证了用户数据安全与个人隐私。

同态加密的概念提出可以追溯到 20 世纪 70 年代，在 RSA 密码体制刚提出不久，Rivest 等人提出了同态加密的概念[26]，这一概念的提出成为密码学界的开放难题。同态加密算法包括半同态加密算法和全同态加密算法，半同态加密算法是只支持乘法或加法密文计算的同态加密算法，全同态加密算法是同时支持乘法与加法密文计算的同态加密算法。

同态加密在许多领域和场景都有应用价值，例如：同态加密是安全多方计算协议的基本工具之一，与秘密分享机制、茫然传输协议等都是 MPC 协议设计的基础；在云外包计算、隐私计算、联邦学习等应用场景方面，同态加密可以实现对密文信息的运算，保护数据的隐私性。

2.4.1.2 标准化

1978 年，Rivest 等人在《On data banks and privacy homomorphic》[26]中首次提出同态加密的概念。在同态加密概念提出的四十多年时间里，各种同态加密方案不断被提出，包括半同态加密和全同态加密方案，其中 Paillier 同态加密算法[27]已经成为 ISO 国际保准。关于同态加密的发展历程可参见[28]，全同态加密算法的相关进展参见[29, 30]。

2019 年 5 月，国际标准化组织 ISO 发布了同态加密标准（ISO/IEC 18033-6:2019）。该标准仅涉及半同态加密，具体包含两种较为成熟的半同态加密机制：ElGamal 乘法同态加密和 Paillier 加法同态加密，并规定了参与实体的参数和密钥生成、数据加密、密文数据解密、密文数据同态运算等步骤的具体过程。

2.4.1.3 Paillier 加法同态加密算法

（1）方案简介

Paillier 加法同态加密算法[27]是由 Pascal Paillier 在 1999 年提出的一种公钥加密算法。该加密算法基于合数N分解的困难性，满足语义安全，这里合数N为两个大素数的乘积。此外，Paillier 加密算法是一种加法同态加密算法，满足加法和数乘同态。Paillier 加法同态加密算法被 ISO 组织列为标准同态加密算法。

（2）符号

下列符号适用于本部分的协议：

——κ: 安全参数。

——$\mathbb{N}$: 自然数集。

——p, q: 大素数

——$\mathbb{Z}$: 整数集

——S: 集合S。

——$s \leftarrow S$: 从有限集S中随机地选取出一个元素s。

——gcd(): 最大公约数。

——lcm(): 最小公倍数

（3）密钥生成过程

a)选取两个相近的大素数p,q且满足 $\gcd\big(pq,(p-1)(q-1)\big)=1$；

b)令$\lambda=\mathrm{lcm}(p-1,q-1)$，$N=pq$；

c)输出公钥：$pk=N$，私钥：$sk=\lambda$。

（4）加密过程

输入一个待加密的消息$m\in\mathbb{Z}_N$，选取一个随机数$r\leftarrow\mathbb{Z}_N^*$，计算并输出密文：

$$c=(1+N)^m\cdot r^N \ mod\ N^2。$$

（5）解密过程

输入私钥 sk 和一个待解密的合法密文c，计算并输出相应的明文 m：

$$\mathrm{m}=\frac{(c^\lambda \bmod N^2)-1}{N}\cdot\lambda^{-1}\bmod N$$

$$=\frac{\big((1+N)^{\lambda m}\cdot r^{\lambda N} mod\ N^2\big)-1}{N}\cdot\lambda^{-1} mod\ N$$

$$=\frac{1+\lambda mN-1}{N}\cdot\lambda^{-1} mod\ N$$

$$=m$$

（6）加法同态特性

记 Enc()是加密过程函数，加密两个消息m_1和m_2，加法同态特性如下：

$$\mathrm{Enc(m_1)\oplus Enc(m_2)}=(1+\mathrm{N})^{\mathrm{m_1}}\mathrm{r_1}^{\mathrm{N}}\cdot(1+\mathrm{N})^{\mathrm{m_2}}\mathrm{r_2}^{\mathrm{N}}\bmod\mathrm{N}^2$$

$$=(1+\mathrm{N})^{\mathrm{m_1+m_2}}(\mathrm{r_1r_2})^{\mathrm{N}}\ \bmod\mathrm{N}^2$$

$$\rightarrow\mathrm{Enc(m_1+m_2)}$$

给定一个常数 a：

$$Enc(m_1)^a=((1+N)^{m_1}{r_1}^N)^a\bmod N^2$$

$$=(1+N)^{am_1}{r_1}^{aN}\bmod N^2$$

$$\rightarrow\mathrm{Enc}(am_1)$$

2.4.2 全同态加密算法

2.4.2.1 概述

2009 年，Gentry 提出第一个基于格问题的全同态加密方案[31]，开启了全同态加密的研究热潮。全同态加密同时支持数据密文的加法和乘法运算，是实现数据密文计算和隐私保护的非常好的方法，但是实现效率问题是制约全同态加密应用的主要问题之一。全同态加密方案的研究经历了三个阶段：

第一代是基于理想格的全同态加密方案，包括 2009 年的 Gentry 方案，首先构造出一个能够进行有限次同态加法和同态乘法计算的类同态加密方案(Somewhat homomorphic encryption, SWHE)，然后利用自举（Bootstrapping）方法进行重加密降低噪声，从而使方案拥有任意次密文同态计算的能力。

第二代是基于 LWE/RLWE 问题的全同态加密方案，包括 BGV、BFV 等方案。2011 年，Brakerski 和 Vaikuntanathan 提出了 BV 模型[32]；2012 年，Brakerski，Gentry 和 Vaikuntanathan 提出了基于 LWE 问题的全同态加密算法[33]，通过密钥交换和模交换等技术控制噪声；BFV(Brakerski/Fan-Vercauteren) [34]是与 BGV 方案类似的第二代全同态加密方案，只使用密钥交换解决密文乘法带来的密文维数膨胀问题。

第三代是基于近似特征向量的 GSW 方案。2013 年，Gentry、Sahai 和 Waters 利用近似特征向量构造出了 GSW 全同态加密方案[35]，该方案的密文形式是矩阵，同态加法和乘法通过相应矩阵的矩阵加法和矩阵乘法来实现，构造更简单，但是该方案仅支持单比特加密。

2017 年，Cheon J H 等提出了可用于近似密文计算的 CKKS 方案[36]，能够用于浮点数的密文计算，由于允许误差的存在，使得 CKKS 进行了较大的简化，计算效率有了很大提升。

除了 LWE/RLWE 等困难问题外，还有一类困难问题是整数上近似最大公约数(Approximate Greatest CommonDivisor, AGCD)[37]。

在全同态加密的开源代码库方面，已有许多开源代码项目实现了经典的全同态加密方案，例如：HELib 实现了 BGV 加密方案；SEAL 库实现了 BFV 和 CKKS 方案；HEANN 库实现了 CKKS 方案；其它的开源库还有 PALISADE。

2.4.2.2 标准化

2017 年 7 月，全同态加密标准化开放联盟 HomomorphicEncryption.org 成立[38]，在微软研究院举办了首届全同态加密标准化研讨会，开始推进全同态加密标准草案的编写工作，并发布了全同态加密安全、API、应用三份白皮书。其中，安全白皮书定义了同态加密的安全性属性，介绍了 BGV 和 BFV 方案，以及三种可选方案：YASHE，NTRU / LTV 和 GSW；描述了 RLWE 等安全性假设；描述了已知的攻击以及推荐的具体参数；最后介绍了方案的其他功能。API 白皮书介绍了用于同态加密的 API 接口、编程模型的设计。应用白皮书介绍了同态加密的几种典型应用场景，包括在基因医学、国家安全/关键基础设施、教育、医疗保健、控制系统保护等场景的应用。

2019 年，深圳市商用密码行业协会发布了一项同态加密相关的团体标准 T/SCCIA 001-2019《基于整数同态加密的密文查询算法》，该标准给出了基于整数同态加密的密文查询算法的具体定义，并且描述了其依赖的数学背景和数学难题，并给出了相应的安全性证明。标准文本详细描述了 AGCD 问题、密钥参数如何选取、密钥生成的具体步骤、基于整数同态的加解密过程、密态数据库的生成流程和密文查询算法的具体流程并在附录中给出了一组具体实现的参考示例数据。

2.4.2.3 GSW 方案

GSW 方案[35]是基于近似特征向量的层次全同态加密方案，其同态加法和同态乘法直接对应于矩阵的加法和乘法，GSW 方案主要包括密钥产生、加密、解密、密文计算等步骤，

（1）密钥产生：

密钥产生模块分为三个步骤，分别是$Setup$、$SecretKeyGen$和$PublicKeyGen$，如下所示：

$Setup(1^{\lambda},1^{L})$：选择一个长度为$\kappa=\kappa(\lambda,L)$比特的模数q，格维数为$n=n(\lambda,L)$，误差分布为$\chi=\chi(\lambda,L)$，参数$m=m(\lambda,L)=O(nlog\,q)$，令$params=(n,q,\chi,m)$，$\lfloor log_2 q\rfloor+1, N=(n+1)\cdot l$。

$SecretKeyGen(params)$：取样$\underset{t}{\rightarrow}\leftarrow Z_q^n$，输出私钥$sk=\underset{s}{\rightarrow}\leftarrow(1,-t_1,\ldots,-t_n)\in Z_q^{n+1}$，令向量$\underset{v}{\rightarrow}=Powersof2(\underset{s}{\rightarrow})$。

$PublicKeyGen(params, sk)$：均匀产生矩阵$B \leftarrow Z_q^{m\times n}$，向量$\underset{e}{\rightarrow} \leftarrow \chi^m$，$\underset{b}{\rightarrow} = B \cdot \underset{t}{\rightarrow} + \underset{e}{\rightarrow}$，令A是由向量$\underset{b}{\rightarrow}$和矩阵$B$合并成的$m \times (n+1)$矩阵，所以公钥$pk = A$。

（2）加密：

对于明文消息$\mu \in \{0,1\}$，随机选择一个矩阵$R \in \{0,1\}^{N\times m}$，输出密文$C$如下所示：

$$C = Flatten(\mu \cdot I_N + BitDecomp(R \cdot A)) \in Z_q^{N\times N}.$$

因为$Flatten$操作不影响密文与向量$\underset{v}{\rightarrow}$的点积，所以上述变换之后的加密算法仍然正确。

（3）解密：

令密文矩阵C的第i行为C_i，C_i是一个N维行向量，根据加密算法$C \cdot \underset{v}{\rightarrow} = \mu \cdot \underset{v}{\rightarrow} + \underset{e}{\rightarrow}$可得解密算法，首先计算$x \leftarrow < C_i, \underset{v}{\rightarrow} > \mu \cdot v_i + e_i$，可得解密之后的明文为$\mu = \lfloor x/v_i \rceil$。

（4）密文同态计算：

GSW方案支持常量乘积（MultConst）、同态加法（Add）、同态乘法（Mult）、与非运算（NAND）四种密文同态计算，并可以利用这四种同态运算组合成任意电路的密文同态计算，四种同态运算如下：

$\mathrm{MultConst}(\mathrm{C}, \alpha)$：已知常数$\alpha \in Z_q$，密文矩阵$C \in Z_q^{N\times N}$，令$M_\alpha \leftarrow Flatten(\alpha \cdot I_N)$，输出结果$Flatten(M_\alpha \cdot C)$，正确性证明如下：

$$\mathrm{MultConst}(\mathrm{C}, \alpha) \cdot \underset{v}{\rightarrow} = M_\alpha \cdot C \cdot \underset{v}{\rightarrow} = M_\alpha \cdot (\mu \cdot \underset{v}{\rightarrow} + \underset{e}{\rightarrow}) = \mu \cdot (M_\alpha \cdot \underset{v}{\rightarrow}) + M_\alpha \cdot \underset{e}{\rightarrow}$$

若$M_\alpha \cdot \underset{e}{\rightarrow}$足够小，则常量乘积是同态的，满足同态正确性。

$Add(C_1, C_2)$：给定密文$C_1, C_2 \in Z_q^{N\times N}$，输出结果$Flatten(C_1 + C_2)$。

$\mathrm{Mult}(C_1, C_2)$：给定密文$C_1, C_2 \in Z_q^{N\times N}$，输出结果$Flatten(C_1 \cdot C_2)$，正确性证明如下：

$$\mathrm{Mult}(C_1, C_2) \cdot \underset{v}{\rightarrow} = C_1 \cdot C_2 \cdot \underset{v}{\rightarrow} = C_1 \cdot (\mu_2 \cdot \underset{v}{\rightarrow} + \underset{e_2}{\rightarrow}) = \mu_2 \cdot (\mu_1 \cdot \underset{v}{\rightarrow} + \underset{e_1}{\rightarrow}) + C_1 \cdot \underset{e_2}{\rightarrow}$$

$$= (\mu_1 \cdot \mu_2) \cdot \underset{v}{\rightarrow} + \mu_2 \cdot \underset{e_1}{\rightarrow} + C_1 \cdot \underset{e_2}{\rightarrow}$$

$\mathrm{NAND}(C_1, C_2)$：给定密文$C_1, C_2 \in Z_q^{N\times N}$，输出$Flatten(I_N - C_1 \cdot C_2)$，

$$\mathrm{NAND}(C_1, C_2) \cdot \underset{v}{\rightarrow} = (I_N - C_1 \cdot C_2) \cdot \underset{v}{\rightarrow} = (1 - \mu_1 \cdot \mu_2) \cdot \underset{v}{\rightarrow} - \mu_2 \cdot \underset{e_1}{\rightarrow} - C_1 \cdot \underset{e_2}{\rightarrow} \quad 。$$

2.4.3 可搜索加密

2.4.3.1 概述

2000年，X. Song等首次提出可搜索加密（Searchable encryption，SE）的概念[39]，能够支持对密文数据的全文关键词搜索。可搜索加密可以用于数据库加密、文件

加密、云外包存储等应用场景，在不需要解密的情况下，实现对密文数据的关键词搜索。

根据构造算法的不同，可搜索加密方案可以分为两类：基于对称密码的可搜索加密（SSE）和基于公钥密码的可搜索加密（PKSE）。SSE 主要采用对称密码算法、伪随机函数和密码杂凑算法，计算效率更高。PKSE 主要采用基于双线性对等困难问题的公钥密码算法，计算速度慢。

2000 年，Song 等提出的第一个 SSE 方案是一种全文搜索方案[39]，将明文数据划分为若干个“单词”并分别对其加密，关键词搜索的过程中需要扫描整个密文文件，与密文关键词进行对比，因此搜索复杂度和加密数据的大小呈线性关系，效率比较低。

2003 年，Goh 等提出了基于索引的 SSE 方案[[40]，建立密文关键词的文件索引，提高了密文检索的效率。近年来，多数可搜索方案是基于密文索引的方案，此类型的 SSE 方案主要包括KeyGen, Encrypt, Trapdoor, Search, Decrypt：

1) $K = Keygen(\lambda)$：输入安全参数 λ，产生随机密钥K。
2) $(I, C) = Encrypt(K, D)$:输入对称密钥K和明文文件集$D = (D_1, D_2 \ldots, D_n)$，输出索引$I$和密文文件集$C = (C_1, C_2 \ldots, C_n)$。
3) $T_W = Trapdoor(K, W)$:输入对称密钥K和关键词W，输出关键词陷门T_W。
4) $D(W) = Search(I, T_w)$:输入索引I和陷门T_W，输出包含关键词W的文件集合$D(W)$。
5) $D_i = Decrypt(C_i)$:输入对称密钥和加密的文件C_i，输出相应的明文文件D_i。

2.4.3.2 Song 基于关键词的方案

2000 年，Song 等在 IEEE S&P 会议上提出了第一个可搜索加密方案[39]，方案如下：

（1）加密阶段：

假设一个文件中包含l个单词：$W_1, \ldots, W_l$，利用伪随机生成器产生伪随机值$S_1, \ldots, S_l$。之后，生成两个密钥K''和K'。

首先对每一个单词W_i使用分组密码E逐个加密得到$X_i = E(K'', W_i)$；

之后将密文分为L_i和R_i两个部分$X_i =< L_i,\ R_i >$；

基于L_i生成二进制字符串$S_i||F(K_i, S_i)$，其中$K_i = f(K', L_i)$，||代表字符串链接，F和f为伪随机函数。

$X_i \oplus (S_i||F(K_i, S_i))$以形成$W_i$的密文单词$C_i$。

（2）陷门生成阶段：

为了查询文件是否包含关键词W，用户生成陷门$T_w = (E(K'', W), K = f(K', L))$给服务器，其中$L$为$E(K'', W)$的左部。

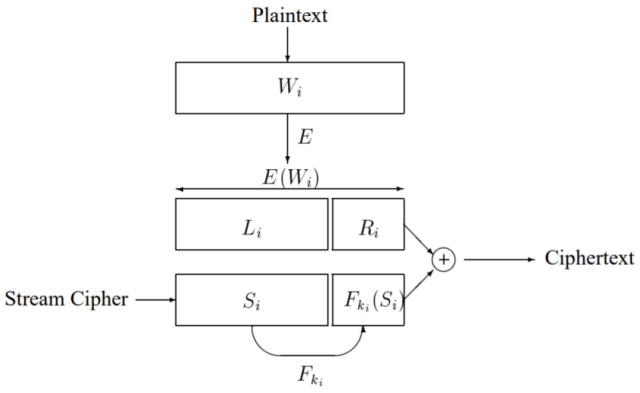

图 1 陷门生成

（3）搜索阶段：

服务器遍历密文文件中所有的单词C，计算$C \oplus E(K', W) = S||T$，判断$F(K, S)$是否和T相等。若相等，则C即为W在文件中的密文；否则，继续计算下一个密文单词。

2.4.3.3 Curtmola 的基于索引的方案

2011 年，Curtmola 等[41]针对两种安全模型——抗非自适应选择关键词攻击的语义安全（IND-CKA1）和抗自适应选择关键词攻击的语义安全（IND-CKA2），分别提出了两个高效的、支持次线性搜索的关键词搜索方案（SSE-1 和 SSE-2），SSE-1 方案如下：

（1）初始化阶段：

选择两个对称加密算法$SKE1$和$SKE2$；生成 3 个k比特的随机数K_1, K_2, K_3以及对称加密算法$SKE2$一个k比特的对称密钥K_4。

（2）加密索引阶段：

- 扫描明文文件集D，生成一个关键字集合$\sigma(D)$;对于所有的$w \in \sigma(D)$，生成文件标识符集合$D(w)$；初始化一个全局计数器$ctr = 1$
- 建立数组A：

对于每一个$i \in [1, |\sigma(D)|]$：

建立一个带有节点$N_{i,j}$链表L_i，并按照如下方式将其存放在数组A中：首先生成一个k比特的密钥$K_{i,0}$；对于每一个$j \in [1, |D(w_i)| - 1]$:

a) 随机选取对称加密算法$SKE1$的密钥$K_{i,j}$；

b) 首先记 $id(D_{i,j})$为$D(W_i)$中字典序下第j个文件标识符；创建一个节点 $N_{i,j} = id(D_{i,j})||K_{i,j}||\psi(K_1, ctr + 1))$，其中$\psi()$为伪随机函数;将节点$N_{i,j}$用密钥$K_{i,j-1}$加密存储在数组$A$中，$A[\psi(K_1, ctr)] = SKE1.Enc(K_{i,j-1}, N_{i,j})$，之后设置$ctr = ctr + 1$。

c) 对于 L_i 中的最后一个节点 $N_{i,|D(w_i)|}$，将其设置成 $N_{i,|D(w_i)|} = id(D_{i,|D(w_i)|})\big||0^k|\big|NULL$。节点$N_{i,|D(w_i)|}$用密钥$K_{i,|D(w_i)|-1}$加密存储在数组$A$中，$A[\psi(K_1, ctr)] = SKE1.Enc(K_{i,|D(w_i)|-1}, N_{i,|D(w_i)|})$。设置 $ctr = ctr + 1$。

- 创建查找表：对于所有的$w_i \in \sigma(D)$，设置

$$T[\pi(K_3, w_i)] = (addr_A(N_{i,1})||K_{i,0}) \oplus f(K_2, w_i).$$

$f()$为伪随机函数，$\pi()$为伪随机置换，$addr_{A()}$表示该链表节点在数组A中的地址。

- 输出索引表：对于$i \in [1, n]$，n为文件的数量，计算$c_i = SKE2.Enc(K_4, D_i)$。将(I, c)发送给服务器，其中$I = (A, T), c = (c_1, \ldots, c_n)$。

（3）构造陷门阶段：

对于关键词w，用户构建陷门$T_w = (\pi(K_3, w), f(K_2, w))$并将其发送给服务器。

（4）搜索阶段：

利用搜索陷门，服务器首先寻找相关w链表首结点的间接位置 $\Theta = T[\pi(K_3, w)]$，$\Theta \oplus f(K_2, w) = \alpha || K'$，$\alpha$为$L_w$首节点在$A$中的地址，$K'$为首节点加密使用的对称密钥。返回$L_w$中所有文件的标识符。

（5）解密阶段：

输出文件$D_i = SKE2.Dec(K_4, c_i)$。

2.4.4 保序加密

2.4.4.1 概述

针对数据库等存储方式的常用查询操作，包括对数值型数据的区间查询(范围查询)、最大值、最小值等查询操作。当数值型数据被加密之后，将破坏原有明文的顺序信息，传统的加密算法不支持对密文的以上数值查询操作，因此需要设计专门的保序加密算法，即加密后的数值型数据仍然保持与明文相对应的顺序，于是能够进行数值查询操作。既然保序加密的密文泄露了明文的顺序/大小信息，因此其安全性具有一定的问题。

保序加密是目前解决密文数值型数据查询问题的有效方法，既保护用户数据的机密性，又能够实现密文数据的数值型查询。2004 年，由 Agrawal 等首次提出保序加密的概念[42]，即密文仍然保留原有明文顺序，可以保证区间查询(范围查询)、最大值、最小值等查询操作可以在密文空间进行。保序加密技术的研究进展可参见文献[43]。

按照是否建立索引表，可以将保序加密方案分为无索引结构的保序加密方案和基于索引结构的保序加密方案。无索引结构的保序加密方案是指加密密文直接保留原有明文顺序。基于索引结构的保序加密方案，是指明文数据使用普通密码算法（例如 AES 等）进行加密，同时又建立一个保序索引结构，其可以用于比较明文顺序。

对于基于索引结构的保序加密方案，其最初灵感来自于可搜索加密方案，依据可搜索加密中构建索引结构对密文环境中的关键词进行搜索，考虑构建一种带索引结构的保序加密方案。对于密文数据，采用传统的加密方案进行加密，在加密数据的同时建立一个保序索引，用来指引云服务器进行范围查询。目前，保序加密采用的索引结构主要有桶索引、哈希索引结构、B+树索引、线性索引结构、非线性索引结构、B 树或二叉树数据结构索引等。

2.4.4.2 BCLO 方案

2009 年，Boldyreva 等提出了一种保序加密方案[44]，在 BCLO 方案中，假设函数 $f: A \to B$ 为一个保序函数，即：对于任意的 $i, j \in A$ 有 $f(i) > f(j)$ 当且仅当 $i > j$。我们可以由保序函数 $f(\cdot)$ 构造保序加密方案 $\Pi = (Key; Enc; Dec)$，其中 $c = Enc(K; m) = f(m)$。因此，BCLO 方案的构造便转化为寻找一个保序函数。算法 1 和算法 2 描述了保序函数的生成与求逆[43,44]。

表 1 OPF 算法

算法 1: OPF 加密算法	算法 2: OPF 解密算法
Encrypt$(a, b, f(a), f(b), m)$	Decrypt$(a, b, f(a), f(b), c)$
1. $x \leftarrow (a+b)/2$	1. $x \leftarrow (a+b)/2$
2. $y \leftarrow f(b) - f(a)$	2. $y \leftarrow f(b) - f(a)$
3. 使用确定性种子函数 $S(a, b, f(a), f(b))$ 初始化伪随机函数生成器 F	3. 使用确定性种子函数 $S(a, b, f(a), f(b))$ 初始化伪随机函数生成器 F
4. 随机选取 $z \leftarrow_R [0, y]$ 使得 $\Pr(z \in [y/4, 3y/4])$ 为可忽略的	4. 随机选取 $z \leftarrow_R [0, y]$ 使得 $\Pr(z \in [y/4, 3y/4])$ 为可忽略的
5. $f(x) \leftarrow f(a) + z$	5. $f(x) \leftarrow f(a) + z$
6. 若 $x = m$, 则返回 $f(x)$	6. 若 $f(x) = c$, 则返回 x
7. 若 $x > m$, 则回到 Encrypt$(a, x, f(a), f(x), m)$	7. 若 $f(x) > c$, 则返回 Decrypt$(a, x, f(a), f(x), c)$
8. 若 $x < m$, 则回到 Encrypt$(x, b, f(x), f(b), m)$	8. 若 $f(x) < c$, 则返回 Decrypt$(x, b, f(x), f(b), c)$

2.5 用于数据共享与访问控制的密码技术

2.5.1 秘密分享

2.5.1.1 概述

秘密分享(Seret Sharing)[54, 55]是将秘密信息拆分成 n 个份额，并将拆分后的每一个份额分别独立分发给 n 个参与者，只有满足一定条件的若干个参与者一起协作才能恢复秘密消息，不满足条件的若干参与者无法恢复秘密信息。

秘密分享可以用于密钥等秘密消息、重要数据的分布式安全存储，将秘密信息、关键数据拆分成若干份进行存储，一方面提高了秘密信息的安全性，避免一个存储点被攻击后造成秘密信息泄露的风险，另一方面提高了秘密信息存储的鲁棒性和可靠性，即使一份或几份份额丢失，仍然能够恢复整个秘密信息。

一般化的秘密分享方案称为访问结构秘密分享方案(access structure secret sharing scheme)，可以任意规定所有参与者集合的哪些子集具有恢复秘密信息的能力，这些子集称为授权子集。门限秘密分享机制是一类特殊的、最简单的秘密分享方案，可以规定 n 个参与者中的任意 t 个参与者一起协作能够恢复秘密信息，称为(t, n)门限秘密分享机制。

秘密分享技术也是安全多方计算、门限数字签名等密码方案的基本工具之一，广泛应用于密钥管理、身份认证、数字签名、安全多方计算、电子投票等多个应用场景。

2.5.1.2 发展历程和标准化

秘密分享方案可以基于拉格朗日多项式插值、投影几何、中国剩余定理、图存取结构等技术构建，其中基于拉格朗日插值的 Shamir 秘密分享方案构造是最简单的方案，应用最广泛。1979 年，Shamir 提出了基于拉格朗日多项式插值的(t, n)门限秘密分享方案[54]，Blakley 采用几何方法设计了门限秘密分享方案[55]。当门限秘密分享方案无法实现一些特殊的应用场景要求时，就需要设计通用的访问结构秘密分享方案。为了满足不同应用场景的实际需求，还存在多秘密分享、可验证秘密分享、无分发者的秘密分享等安全方案。

在国际标准方面，国际标准化组织（ISO）发布了两套有关秘密分享的加密标准，分别是 ISO/IEC 19592-1:2016 和 ISO/IEC 19592-2:2017。其中，ISO/IEC 19592-1:2016 定义了秘密分享的参与方、相关术语以及方案的参数和特性；ISO/IEC 19592-2:2017 规定了秘密分享方案及其特性。

2.5.1.3 Shamir 秘密分享方案

1979 年，Shamir 提出了基于拉格朗日多项式插值的门限秘密分享方案[54]，Shamir 门限秘密分享方案是基于拉格朗日插值法的(t,n)门限访问结构秘密分享，在方案中存在一个管理者 D 和n个子份额持有者$P_1,P_2,\dots,P_n$，方案由秘密分发和秘密恢复两部分组成。

1）秘密拆分和共享：

管理者 D 首先选择一个大素数p，所有的计算都在素数域Z_p上进行，选择一个$t-1$阶多项式：

$$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}\ mod\ p$$

秘密值s设为$f(x)$的常数项，即$s=a_0=f(0)$。管理者为每位子份额持有者P_i选择一个公开值$x_i(x_i\neq 0)$，计算子份额$s_i=f(x_i)$。最后，管理者将s_i保密发送给对应的子份额持有者P_i。

2）秘密恢复：

根据(t,n)门限的访问结构，任意不少于t个子份额持有者应当可以恢复秘密。设任意$m(t\leq m\leq n)$个子份额持有者$P_{i_1},P_{i_2},\dots,P_{i_m}$参与秘密恢复过程，每位参与者需要将自己的子份额发送给他人并收集其它子份额。完成这一过程后可得到m个点$(x_{i_1},y_{i_1}),(x_{i_2},y_{i_2}),\dots,(x_{i_m},y_{i_m})$，再利用拉格朗日插值法计算秘密值：

$$s=f(0)=\sum_{j=1}^{m}s_{i_j}\prod_{k=1,k\neq j}^{m}\frac{-x_{i_k}}{y_{i_j}-y_{i_k}}\ mod\ p。$$

2.5.2 广播加密

2.5.2.1 概述

广播加密(Broadcast Encryption)是一种应用于数据分发和共享的安全方案[56]，在不安全信道中采用加密的方式向若干个用户广播密文数据，只有授权用户能够解密信息，适用于“一对多”的数据广播分发场景。

传统的密码方案中，可以采用数字信封的方式进行数据的广播分发，即选择一个对称密钥加密数据，然后用接收者的公钥加密对称密钥，如果存在很多个接收者，则需要很多次公钥加密运算。广播加密方案是设计更有效的专门密码方案，解决面向若干个接收者的广播加密问题。

根据所依赖的密码体制进行分类，可以将广播加密分为对称广播加密和非对称广播加密（即公钥广播加密）。对称广播加密的效率更高，但是需要一个密钥分配中心作为可信第三方进行密钥管理和分发；公钥广播加密具有更灵活方便的密钥管理机制，但是存在运算效率低的问题。

广播加密可以应用于数字版权保护、数字电视、电子邮件系统、视频会议、文件加密系统、数据分发与访问控制、云存储等应用场景。

2.5.2.2 对称广播加密和完全二叉树方案

1993 年，Fiat 和 Naor 在 Broadcast encryption 论文中首先提出了广播加密的概念[56]，给出了广播加密的安全性定义、设计思想和几种广播加密方案，用于解决单点对多点的数据分发和共享问题。文献[57]中也有关于广播加密的内容。

2001 年，Naor D 等在 Revocation and Tracing Schemes for stateless Receivers

论文[58]中提出一种针对无状态接收者的“子集-覆盖”（Subset-Cover）架构，已成为经典的广播加密方案之一。文献[59]对广播加密进行了论述，一种具体的完全二叉树方案如下[58, 59]：

（1）密钥分发：

密钥管理中心 KGC(即广播中心，数据拥有者)创建一棵满二叉树，其叶子节点代表每一个用户。KGC 为满二叉树的每一个节点随机选择一个对称密钥，每个用户(即叶子节点)拥有自己到根节点路径上的所有节点的密钥。

（2）数据加密并广播：

广播中心(数据拥有者)从用户密钥树中选取相应的加密密钥对数据进行加密，并将加密结果广播式发送给所有用户。

（3）数据解密：

每一个用户拥有用户密钥树中的与自己相关的密钥，接收数据密文并利用自己持有的密钥解密数据。

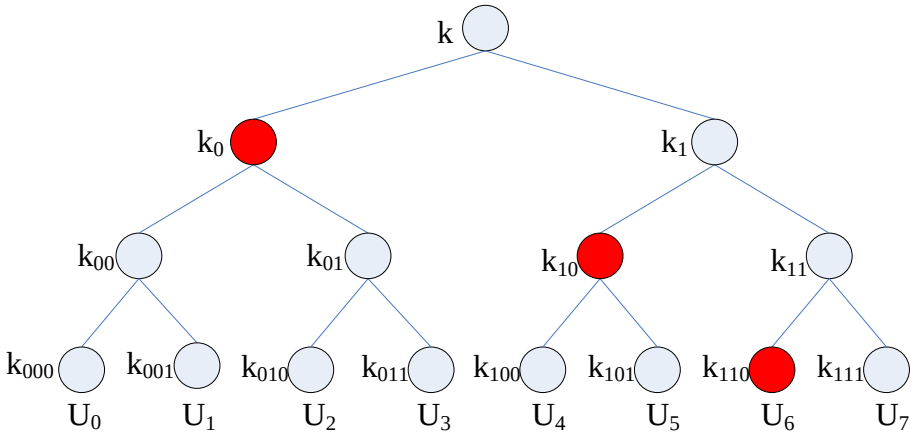

图 2 密钥树

如图 3 所示，选择红色节点处的密钥集{k0，k10，k110}进行数据加密，则未授权的普通用户就是 U7，他将无法解密数据。

2.5.3 属性加密

2.5.3.1 概述

基于属性的加密 (简称属性加密，ABE—Attribute-Based Encryption) 是将属性集合作为公钥，将数据的访问控制策略与用户私钥与密文中相关联，解密的过程就是将属性集合与访问控制策略相匹配的过程，若匹配成功则能够成功解密。

属性加密是解决数据分享和访问控制问题的密码技术之一，通过将一系列属性于访问控制策略和细粒度的授权用户集合相关联，实现数据机密性和访问控制的安全保障。当需要把数据传输、共享给第三方时，数据拥有者可以通过属性加密机制，灵活方便地指定哪些用户能够解密并访问数据。

2005 年, Sahai 和 Waters 首先提出了基于生物特性信息的身份加密方案[60], 称为模糊身份加密方案(Fuzzy Identity-based Encryption, Fuzzy-IBE)。在该方案中, 用户的身份信息被特征化为一组属性, 而身份的匹配关系由原来的“完全匹配”变为“相似匹配”：对两个由 n 个属性组成的身份信息, 它们之间匹配允许存在一些小的误差, 这个模糊身份加密方案可以看作是属性密码学的“雏形”。

基于属性的加密方案主要分为以下两类：密钥策略属性加密（Key-Policy ABE，KP-ABE）和密文策略属性加密（Ciphertext-Policy ABE，CP-ABE）。2006 年，Goyal 等给出了属性加密的概念[61]，并分为 KP-ABE 和 CP-ABE 两种类型，同时首次提出了一个 KP-ABE 方案。2007 年，Bethencourt 等首次提出了一个 CP-ABE 方案[62]。文献[63]是属性密码学的综述，文献[64]是属性加密技术的专著。

属性加密在数据的细粒度访问控制、数据安全分享等应用场景中，具有广泛的应用。KP-ABE 适用于付费视频分发、定向广播、日志审计管理等；CP-ABE 适合于云计算环境下的数据加密存储的访问控制，由云端负责管理并分发属性给用户，数据所有者决定哪些用户可以解密数据。

2.5.3.2 标准化进展

在国际标准方面，2018 年 8 月，欧洲电信标准协会(ETSI)发布了两个安全访问控制的加密标准(CRYPTOGRAPHIC STANDARDS FOR SECURE ACCESS CONTROL)，分别为 ETSI-TS-103-458 和 ETSI-TS-103-532，采用 ABE 属性加密提供细粒度的个人数据保护，可以用于 5G、IoT 物联网等分布式系统。

ETSI-TS-103-458 规定了属性加密的高层次要求，一个目的是提供对用户身份 ID 的保护，防止泄露给未授权的第三方。本标准规定了在 IoT 物联网设备、广域网(WLAN)、云服务和移动服务等应用场景下的个人数据保护。

ETSI-TS-103-532 规定了基于属性加密实现数据访问控制的信任模型、功能和协议，该标准提供了支持密文策略及密钥策略两种类型属性加密的加密层，适用于云计算、移动互联网及 IoT 物联网等应用场景。而且，这个加密层具有可扩展性，便于将来不断增加新的密码方案，例如抗量子密码算法。

ETSI-TS-103-458 和 ETSI-TS-103-532 标准遵循 GDPR(the General Data Protection Regulation)通用数据保护条例。

两类最经典的属性加密算法，即密钥-策略属性加密（KP-ABE）算法和密文-策略属性加密（CP-ABE）算法。

2.5.3.3 KP-ABE 协议

KP-ABE 框架[61]包含如下四个算法：

a) 初始化系统：以安全参数γ和属性全集U为输入，初始化系统并生成系统公共参数pk及主密钥mk。
b) 生成密钥：以系统公共参数 pk、主密钥 mk 及用户的属性集合w为输入，输出与 w对应的用户私钥 SK_w。
c) 加密：以系统公共参数 pk、访问控制策略 T及明文 m 为输入，输出密文 CT_T。
d) 解密：以系统公共参数pk、用户私钥SK_w 及密文CT_T 为输入，当且仅当SK_w对应的属性集合w满足CT_T 对应的访问控制策略T时，算法输出明文m。

（1）符号

下列符号适用于本部分的协议：

——p：素数。

——Z_p：$[0,\dots,p-1]$中整数的集合。

——t_i, y, s：Z_p中的元素。

——e：双线性映射。

——G_1, G_2：阶为p循环群。
——g：G_1的生成元。
——$parent(x)$：结点x的父结点。
——$index(x)$：结点x的索引值。
——$att(x)$：叶子结点x的属性。
（2）初始化系统

定义属性集$\mathcal{U} = \{1，2，\cdots, \mathrm{n}\}$，对于每一个属性$i \in \mathcal{U}$，选择一个随机数$t_i \in \mathbb{Z}_p$，选择$y \in \mathbb{Z}_p$。输出公共参数$PK$，

$$T_1 = g^{t_1}, \cdots, T_{|\mathcal{U}|} = g^{t_{|\mathcal{U}|}}, Y = e(g,g)^y$$

主密钥MK是：$t_1, \cdots, t_{|\mathcal{U}|}, y$。

（3）加密

$Encryption\ (M, \gamma, PK)$：加密在属性集合$\gamma$下的明文$M$，随机选择$s \in \mathbb{Z}_p$，然后计算

$$E = (\gamma, E' = MY^s, \{E_i = T_i^s\}_{i \in \gamma})$$

（4）生成密钥

$Key\ Generation\ (\mathcal{T}, MK)$：该算法输出一个基于属性$\gamma$的解密密钥，当且仅当$\mathcal{T}(\gamma) = 1$。算法执行如下的操作：

为访问树中的每一个结点x（包括叶子结点）选择一个多项式q_x，这些多项式的选择从根结点开始从上往下进行。具体的操作如下：

- 设定多项式q_x的阶d_x：$d_x = k_x - 1$，其中k_x是结点x的门限值。
- 对于根结点r，令$q_r(0) = y$, 多项式q_r的其他点随机选择。
- 对于其他结点x，令$q_x(0) = q_{parent(x)}(index(x))$，多项式$q_x$的其他点随机选择。

一旦多项式被确定，对于每个叶子结点x，计算下面的秘密值给用户：

$$D_x = g^{\frac{q_x(0)}{t_i}}, i = att(x)$$

秘密值的集合就是解密密钥D。

（5）解密

$Decryption\ (E, D)$：我们将解密过程指定为一个递归算法。

定义递归算法$DecryptNode(E, D, x)$, 该算法输出一个$\mathbb{G}_2$中的元素或者$\perp$。

如果结点x是叶子结点，令$i = att(x)$，那么计算：

$$DecryptNode(E, D, x) = \begin{cases} e(D_x, E_i) = e\left(g^{\frac{q_x(0)}{t_i}}, g^{s \cdot t_i}\right) = e(g,g)^{s \cdot q_x(0)}, if\ i \in \gamma \\ \perp, otherwise \end{cases}$$

如果x不是叶子结点，对于x的所有的子结点z，调用$DecryptNode(E, D, z)$，并将其输出结果记为F_z。令S_x是任意k_x个$F_z \neq \perp$的子结点z的集合，如果这样的集合不存在，那么返回$\perp$，否则，$F(x)$计算如下：

$$F_x = \prod_{z \in S_x} F_z^{\triangle_{i, S_x'}(0)}, \qquad where\ i = index(z), S_x' = \{index(z) : z \in S_x\}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{s \cdot q_z(0)}\right)^{\triangle_{i,S'_x}(0)}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{s \cdot q_{parent(z)}(index(z))}\right)^{\triangle_{i,S'_x}(0)}$$

$$= \prod_{z \in S_x} e(g,g)^{s \cdot q_x(i) \cdot \triangle_{i,S'_x}(0)}$$

$$= e(g,g)^{s \cdot q_x(0)}$$

然后返回该结果。

递归计算根结点的$DecryptNode(E,D,r)$的值$F_r = a(g,g)^{ys} = Y^s$, 则$M = \frac{E'}{F_r} = \frac{MY^s}{Y^s}$。

2.5.3.4 CP-ABE 协议

CP-ABE 协议框架[62]：

a) 初始化系统：以安全参数γ和属性全集U为输入，初始化系统并生成系统公共参数pk及主密钥mk。

b) 生成密钥：以系统公共参数 pk、主密钥 mk 及用户的属性集合w为输入，输出与 w对应的用户私钥 SK_w。

c) 加密：以系统公共参数 pk、访问控制策略 T及明文 m 为输入，输出密文 CT_T。

d) 解密：以系统公共参数pk、用户私钥SK_w 及密文CT_T 为输入，当且仅当SK_w对应的属性集合w满足CT_T 对应的访问控制策略T时，算法输出明文m。

（1）符号

下列符号适用于本部分的协议：

——p：素数。

——$\mathbb{G}_0$：阶为p循环群。

——g：$\mathbb{G}_0$的生成元。

——e：双线性映射。

——Z_p：$[0,\dots,p-1]$中整数的集合。

——α,β,r：Z_p中的元素。

——$parent(x)$：结点x的父结点。

——$index(x)$：结点x的索引值。

——$att(x)$：叶子结点x的属性。

（2）初始化系统

选择一个双线性群$\mathbb{G}_0$，其素数阶为p，生成元为g。然后随机选择两个数$\alpha,\beta \in \mathbb{Z}_p$，输出公钥$PK$：

$$PK = \{\mathbb{G}_0.g, h = g^\beta, f = g^{\frac{1}{\beta}}, e(g,g)^\alpha\}$$

主密钥$MK = (\beta, g^\alpha)$

（3）加密

$Encrypt(PK, M, \mathcal{T})$：该算法加密在访问结构$\mathcal{T}$下的消息$M$。

首先为访问树中的每一个结点x（包括叶子结点）选择一个多项式q_x，这些多项式的选择从根结点开始从上往下进行。具体的操作如下：

设定多项式q_x的阶d_x：$d_x = k_x - 1$，其中k_x是结点x的门限值。

对于根结点R，令$q_R(0) = s, s \in \mathbb{Z}_p$，多项式$q_R$的其他点随机选择。

对于其他结点x，令$q_x(0) = q_{parent(x)}(index(x))$，多项式$q_x$的其他点随机选择。

令 Y 表示在访问树$\mathcal{T}$中叶子结点的集合。

$$CT = \{\mathcal{T}, \tilde{C} = Me(g,g)^{\alpha s}, C = h^s, \forall y \in Y: C_y = g^{q_y(0)}, C_y' = H\big(att(y)\big)^{q_y(0)}\}$$

（4）生成密钥

$KeyGen(MK, S)$:该算法输入属性集S，输出与该集合对应的私钥。首先选取随机数$r \in \mathbb{Z}_p$, 然后为每个属性$j \in S$，随机选取$r_j \in \mathbb{Z}_p$，计算私钥如下

$$SK = \{D = g^{\frac{\alpha + r}{\beta}}, \forall j \in S: D_j = g^r \cdot H(j)^{r_j}, D_j' = g^{r_j}\}$$

$Delegate(SK, \tilde{S})$：该算法输入对应属性集S的私钥SK和另一个属性集$\tilde{S} \subseteq S$，输出对应$\tilde{S}$的私钥$\widetilde{SK}$。首先随机选择$\tilde{r}$和$\tilde{r}_k, \forall k \in \tilde{S}$，然后计算

$$\widetilde{SK} = \left\{\widetilde{D} = Df^{\tilde{r}}, \forall k \in \tilde{S}: \widetilde{D}_k = D_k g^{\tilde{r}} H(k)^{\tilde{r}_k}, \widetilde{D}_k' = D_k' g^{\tilde{r}_k}\right\}$$

（5）解密

$Decrypt(CT, SK)$：定义递归算法$DecryptNode(CT, SK, x)$, 该算法输出一个$\mathbb{G}_2$中的元素或者$\perp$。

如果结点x是叶子结点，令$i = att(x)$，那么计算：

$$DecryptNode(CT, SK, x)$$

$$= \begin{cases} \dfrac{e(D_i, C_x)}{e(D_i', C_x')} = \dfrac{e\left(g^r \cdot H(i)^{r_i}, g^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})} = e(g,g)^{r q_x(0)}, if\ i \in S \\ \perp, otherwise \end{cases}$$

如果x不是叶子结点，对于x的所有的子结点z，调用$DecryptNode(CT, SK, z)$，并将其输出结果记为F_z。令S_x是任意k_x个$F_z \neq \perp$的子结点z的集合，如果这样的集合不存在，那么返回$\perp$，否则，$F(x)$计算如下：

$$F_x = \prod_{z \in S_x} F_z^{\triangle_{i, S_x'}(0)}, \qquad where\ i = index(z), S_x' = \{index(z): z \in S_x\}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{r \cdot q_z(0)}\right)^{\triangle_{i, S_x'}(0)}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{r \cdot q_{parent(z)}(index(z))}\right)^{\triangle_{i, S_x'}(0)}$$

$$= \prod_{z \in S_x} e(g,g)^{r \cdot q_x(i) \cdot \triangle_{i,S'_x}(0)}$$

$$= e(g,g)^{r \cdot q_x(0)}$$

计算$A = DecryptNode(CT, SK, R) = e(g,g)^{rq_R(0)} = e(g,g)^s$,然后计算

$$M = \frac{\tilde{C}}{\frac{e(C,D)}{A}} = \frac{\tilde{C}}{\frac{e\left(h^s, g^{\frac{\alpha+r}{\beta}}\right)}{e(g,g)^{rs}}}$$

2.5.4 代理重加密

2.5.4.1 概述

代理重加密体制（Proxy Re-Encryption，PRE）是一种具备将密文转加密功能的公钥加密方案，代理者可以将 A 方能够解密的密文转化成 B 方能够解密的密文，而且代理者不能得到相应的明文信息，B 方也不能获得 A 方的私钥。代理重加密技术可以帮助用户实现方便快捷的数据共享。

在代理重加密方案中，代理者（Proxy）拥有一个由委托者授权的针对被委托者的密文转换密钥（重加密密钥），具备密文转加密的功能，能够将委托者（Delegator）公钥加密的密文转换为由被委托者（Delegatee）公钥加密的密文，因此被委托者可以用其私钥解密转换后的密文。在数据共享过程中，数据拥有者(即委托者)不需要重新解密、加密数据，而是由代理者实现转加密的操作，从而提高了数据共享的实际效率，不仅使得数据更加方便存储，也使分享更灵活快捷。

代理重加密可以应用于数据共享与分发、文件授权管理和访问控制等方面，例如加密文件管理系统、电子邮件系统、区块链、数字版权保护等应用场景。文献[65, 66]介绍了云计算数据安全的密码技术。

2.5.4.2 发展历程和 BBS 代理重加密方案

1997 年，Mambo 和 Okamoto 首次提出代理重密码的概念[67]，包括代理重签名、代理重签密和代理重加密等定义。1998，Matthew Blaze, Gerrit Bleumer 和 Martin Strauss 提出了代理重加密 (Proxy Re-Encryption，PRE)的概念[68]，并基于 ElGamal 加密算法构造了第一个双向的代理重加密方案，并引出了如何构造一个单向的代理重加密方案的问题。文献[69]也介绍了代理重加密技术的发展历程和典型方案。

BBS 代理重加密方案，代理者可以将 A 方能够解密的密文转化成 B 方能够解密的密文。在代理重加密方案中，代理者会企图获取用户私钥、明文等秘密信息。因此，必须保证代理者在协议执行过程中，既不能获得明文信息，也不能得到任意一方的私钥；而且在协议执行过程中，B 方也不能获得 A 方的私钥。

代理重加密方案分为单向和双向两种类型：在单向代理重加密方案中，只能从一方向另一方进行重新加密；在双向代理重加密方案中，可以在双方之间互相进行重新加密。BBS 代理重加密方案是一种双向代理重加密方案，它采用了 ElGamal 公钥加密算法，具体算法流程如下[67, 68, 69]:

（1）系统参数建立

选取一个大素数p 以及乘法群Z^*_p中的一个生成元g，将g和p作为公开参数。

（2）密钥生成

- Alice 首先均匀随机地选取一个正整数$a < p$，作为自己的私钥，计算$g^a \bmod p$ 作为自己的公钥。
- Alice 然后随机地选取一个正整数$b < p$ ，并通过秘密的信道将b 发送给 Bob，作为 Bob 的私钥。
- Bob 计算$g^b \bmod p$ 作为自己的公钥。

（3）加密

Alice 用 Elgamal 公钥加密算法将明文m加密如下：

- 均匀地随机选取一个正整数k；
- 计算密文$(mg^{ak} \bmod p,\ g^k \bmod p)$；
- 然后，Alice 将密文发给代理 Eve。

（4）解密

对于密文$(mg^{ak} \bmod p,\ g^k \bmod p)$，Alice 可以用自己的私钥$a$ 解密密文如下：

$$(mg^{ak} \bmod p) \cdot (g^{ka} \bmod p)^{-1} = m.$$

（5）重加密密钥生成

当 Alice 想授权给 Bob，使 Bob 也能够解密密文，但又不想用 Bob 的公钥加密明文的方法来实现. Alice 向 Eve 发送b/a作为重加密密钥，由 Eve 重新加密密文并发给 Bob.

（6）重加密

对于密文$(mg^{ak} \bmod p,\ g^k \bmod p)$，代理方 Eve 使用重加密密钥$b/a$进行重加密如下：

$(mg^{akb/a} \bmod p,\ g^k \bmod p)$ ，并将重加密后的密文发给 Bob. 对于这个密文，Bob 可以用自己的私钥b 进行解密。

BBS 代理重加密方案不能抵御合谋攻击，即如果代理方 Eve 和受托方 Bob 合谋，则能够计算出委托方 Alice 的私钥. 改进的代理重加密方案,例如单向代理重加密方案，能够弥补这一缺陷，但改进算法采用了一种称为配对函数的函数，计算成本比较高。

2.6 用于数据外包存储与计算的密码技术

2.6.1 数据的密文检索技术

数据外包存储是用户将自己的数据存储于云端服务器等第三方平台，例如，一些云盘支持将用户的通讯录、照片、通话记录、文件等用户敏感数据存储于云盘。为了防止云平台、非授权机构或个人、非法入侵者等获取自己的数据，用户首先在本地对数据进行加密，再将密文发送给云服务器等第三方平台。在保护数据机密性和用户隐私的前提下，如何保证数据的可用性是一个关键问题。特别是当用户存储了大量数据和文件在第三方平台，如何解决在大量密文数据中搜索包含某个关键词的文件成为数据外包存储的一个重要问题。

当用户想从云端等第三方获取包含有某个关键词或词组的文件，一个最直接的办法是用户从云端下载所有的文件，在本地进行解密，再搜索包含这个关键词或词组的文件。但是，这个方法的效率非常低，不但需要下载所有文件，而且需要全部解密后才能搜索。解决这个问题的方法是在云端在不解密的环境下直接搜索包含这个关键词或词组的密文文件，这样只要把符合条件的密文文件发回给用户即可。

密文检索技术包括针对关键词/词组的检索、区间查询、范围查询等类型，其中数据文件的外包存储的应用场景主要是针对关键词/词组的检索技术。本报告的 2.4.3 可

搜索加密技术主要用于针对关键词、词组的检索，2.4.4 保序加密技术主要用于针对数值型数据的区间查询。文献[59, 65, 66, 69, 70]都有关于可搜索加密技术的介绍。

可搜索加密方案可以分为两类：基于对称密码的可搜索加密方案（SSE）和基于公钥密码的可搜索加密方案(PKSE)。第一个可搜索的对称加密方案是 Dawn X. Song、David Wagner 和 AndrianPerrig 在 2000 年共同设计的，它实现了在诚实而好奇的远程存储模型下对密文的关键词检索，而且关键词也是加密的。远程服务器通过用户提供的密文关键词或词组，能够检索出包含此关键词或词组的密文文件，并发回给用户. 这类方案称为可搜索对称加密方案。在可搜索加密方案中，用户提供查询所需的密文关键词等信息，称为查询陷门。查询结束后，服务端只知道哪些密文包含了加密的关键词及文件的大小，但不知道所查询的关键词和文件的明文内容，保证了密文检索的隐私性。可搜索加密方案非常适合于云存储等数据外包存储环境下的密文检索，实现用户数据的安全存储和隐私保护。Goh 等提出安全索引的方法，解决了 Song 的全文搜索方案搜索开销过大的问题；Curtmola 等提出了对称可搜索加密方案的构造方法和安全性定义，并给出两种具体的对称可搜索加密方案。2004 年，Boneh 等人提出了第一个公钥可搜索加密方案（PEKS）。

在单关键词的密文搜索方案的基础上，一些扩展的、更复杂的密文搜索方案被提出来，包括支持词组、多关键词、模糊关键词等可搜索加密方案。

2.6.2 数据的完整性审计

2.6.2.1 概述

在数据外包存储应用中，用户将自己的数据存储在具有丰富存储资源的云服务器等第三方平台。用户为了确认自己远程存储数据的可用性、正确性，必须验证第三方平台是否完整、正确地为用户提供了存储服务，即验证用户数据是否由于软硬件故障、黑客攻击、人为破坏等原因而遭到损坏、篡改，这个验证工作称为数据的完整性审计。

数据完整性审计方案可分为两类：可证明的数据持有性证明(Provable Data Possession , PDP)和数据可恢复性证明(Proof of Retrievability, PoR)。

2007 年，Ateniese 等提出了可证明的数据持有性证明 PDP 方案的概念[71]，并基于 RSA 算法提出第一个 PDP 方案，此方案仅用于静态存储的数据，不支持存储数据的动态更新，而且计算复杂性较高。之后，一些研究者相继提出了多个支持数据动态更新（添加、更改和删除）的 PDP 方案。

2007 年，Juels 和 Kaliski 等提出第一个数据可恢复性证明 PoR 方案[72]，不但可以验证数据的完整性，还能够利用纠错码技术来实现部分数据的可恢复性。针对特定的场景设计不同数据完整性审计方案，是一个重要的问题。

2.6.2.2 可证明的数据持有性证明 PDP 方案

2007 年，Ateniese 等在信息安全顶级会议 CCS 国际会议上，提出了第一个 PDP 方案[71]，该方案是基于 RSA、同态验证标签和抽样检测。

定义一个伪随机函数f，一个伪随机置换π，以及一个哈希函数H。

（1）密钥生成：

生成一个公钥$pk=(N,g)$以及一个私钥$sk=(e,d,v)$。这里$ed\equiv 1(mod p'q')$, $N=pq$, $p=2p'-1$, $q=2q'-1$。e是一个大素数，g是一个生成元。v是一个k比特的随机数，k是一个安全参数。

（2）建立阶段：

一个文件F可以分为n块：$m_1,\ldots..,m_n$。对于每一个数据块m_i，为其建立一个标签

(W_i, T_{i,m_i})，其中$W_i = v||i$ 和 $T_{i,m_i} = (h(W_i) \cdot g^{m_i})^d \ mod\ N$。随后将$pk, F$和$\sum = (T_{i,m_1}, \ldots, T_{i,m_i}, \ldots, , T_{i,m_n})$发送给服务器存储。

（3）挑战阶段：

客户端为文件中的c个数据块生成一个挑战查询 $\text{chal} = (c, k_1, k_2, g_s)$。这里$k_1, k_2$是两个$k$比特的随机数，$g_s = g^s$，$s$是群$Z_N^*$中的一个随机元素。客户端将chal发送给服务器。

（4）证明生成阶段：

根据chal, pk, F和$\sum = (T_{i,m_1}, \ldots, T_{i,m_i}, \ldots, , T_{i,m_n})$，服务器按照如下方式生成一个证明$V$：对于每一个$j \in [1, c]$，计算数据块的索引$i_j = \pi(k_1, j)$和系数$a_j = f(k_2, j)$。计算$T = T_{i_1,m_{i_1}}^{a_1} \cdot \ldots \cdot T_{i_c,m_{i_c}}^{a_c} = (h(W_{i_1})^{a_1} \cdot \ldots \cdot h(W_{i_c})^{a_c} \cdot g^{a_1 m_{i_1} + \ldots + a_c m_{i_c}})^d \ mod\ N$。计算$\rho = H(g_s^{a_1 m_{i_1} + \ldots + a_c m_{i_c}} \ mod\ N)$。服务器返回$V = (T, \rho)$。

（5）验证阶段：

客户端设置$\text{chal} = (c, k_1, k_2, s)$，按照如下方式验证：设置$\tau = T^e$。对于每一个$j \in [1, \text{c}]$，客户端计算$i_j = \pi(k_1, j)$，$W_{i_j} = v||i_j$和$a_j = f(k_2, j)$以及$\tau = \frac{\tau}{h(W_{i_j})^{a_j}} \ mod\ N$。如果$H(\tau^s \ mod\ N) = \rho$，验证成功；否则，验证失败。

2.6.3 数据密文去重技术

2.6.3.1 概述

在数据外包存储服务模式下，很多机构和个人将自己的数据加密后存储在云服务器等第三方平台，这些数据中存在着大量重复的数据和文件，大大浪费了云服务器的存储资源。数据密文去重技术是对加密后的数据去掉重复的数据和文件，而不泄露数据的明文，可以减少占用的存储空间、避免不必要的数据传输，提高数据存储的效率。

一种类型的密文去重方案是使用由文件生成的加密密钥进行加密，相同的文件具有相同的密文，因此由云端/服务端进行去重操作。2002 年，Douceur 等首先提出了收敛加密(CE, convergent encryption)的密文去重技术[73]，将文件的哈希值作为加密密钥，相同的文件具有相同的加密密钥和密文，所以容易实现密文文件的去重。2013 年，Bellare 等提出了消息锁加密(MLE, message-locked encryption)的概念[74]，涵盖了由文件本身生成加密密钥的机制，是收敛加密的一般化和推广，并提出了第一个基于 MLE 的数据安全去重方案。2015 年，Chen 等提出了一个基于消息锁加密(MLE)的密文去重方案[75]。

另一种类型的密文去重方案是在客户端进行密文去重的安全方案，用户在向云端上传文件之前先与云端进行交互，若云端没有存储该文件，则进行加密后上传储存；若云端文件已经存在，则用户需要向服务器证明其拥有该文件。2011 年，Halevi 等提出了基于数据拥有性证明 PoW(Proof of ownership, PoW)的密文去重方案[76]，这是一种基于客户端的安全去重技术。

2.6.3.2 一种密文去重方案

2015 年，Chen 等提出了一个基于消息锁加密(MLE)的密文去重方案[75]，需要少量元数据就能实现文件级和块级的数据去重、消息块的密钥管理和所有权证明关系。

方案描述：

（1）初始化阶段：

给定一个安全性参数 λ，生成一系列的系统参数 $P =< p, g, G, G_T, e, H_1, H_2, H_3, s, u_1, u_2, \ldots u_s >$，其中，$p$是一个大素数，$g$是群$G$的一个生成元，$e$是一个双线性映射：$G \times G \to G_T$。$H_1, H_2, H_3$是三个哈希函数，$H_1: \{0,1\}^* \to Z_p, H_2: \{Z_p\}^s \to G, H_3: G \to \{Z_p\}^s$。$u_1, u_2, \ldots u_s$是随机从群$G$选择的$s$个元素。

（2）密钥生成阶段：

给定一个数据文件$M = M[1]||\ldots||M[n]$。对于$i \in [1, n]$以及$M[i] \in \{Z_p\}^s$，用户按照如下方式计算其主密钥和相应的块密钥：

$$k_{mas} = H_1(M),\ k_i = H_2(M[i]).$$

（3）加密阶段：

对于每一个数据块$M[i]$和相应的块密钥k_i，用户计算相应数据块的密文$C[i] = H_3(k_i) \oplus M[i]$。

（4）解密阶段：

对于每一个密文数据块$C[i]$ 相应的块密钥k_i，用户恢复出相应的明文数据块$M[i]$ $H_3(k_i) \oplus C[i]$。如果$k_i = H_2(M[i])$，输出明文数据块$M[i]$。

（5）生成标签阶段：

给定一个数据文件$M = M[1]||\ldots||M[n]$，用户按照如下方式生成相应的文件标签T_0和每一个块标签T_i：

a) 用户生成文件标签$T_0 = g^{k_{mas}}$。

b) 用户将每一个密文块$C[i]$分成s块：$\{C[i][j]\}_{1 \le j \le s}$。计算相应的块标签 $T_i = (k_i \prod_{j=1}^{s} u_j^{C[i][j]})^{k_{mas}}$。

c) 用户生成辅助信息 $aux_i = e(k_i, T_0)$。

用户将密文，标签以及服务信息发送给服务器。

（6）服务器检测阶段：

服务器在接收到用户上传的数据之后，会进行两个检测：

a) 一致性检查，即检查密文数据块和标签是否一致。给定一个密文数据块$C[i]$，标签T_i以及辅助性息aux_i，服务器验证$e(T_i, g)$与$aux_i \cdot e(\prod_{j=1}^{s} u_j^{C[i][j]}, T_0)$是否相等.

b) 冗余检查，即检查两个不同文件的数据块是否相同。给定两个块标签T_i和T'_i以及两个文件标签T_0和T'_0。服务器验证$e(T_i, T'_0)$与$e(T'_i, T_0)$是否相等。

（7）用户密钥恢复阶段：

给定一个密文数据块$C[i]$和相应的标签T_i，用户可以计算相应的块密钥$k_i = T_i^{k_{mas}} (\prod_{j=1}^{s} u_j^{C[i][j]})^{-1}$。

（8）可拥有证明生成阶段：

给定一个文件M一个挑战查询$Q=\{(i,v_i)\}$，计算块标签T_i，发送证明$P_T=\prod_{(i,v_i)\in Q}T_i^{v_i}$给服务器。

（9）可拥有证明验证阶段：

给定一个挑战查询$Q=\{(i,v_i)\}$和证明P_T以及存储的文件块标识$\{T_i\}_{1\le i\le n}$，服务器计算验证信息$V_T=\prod_{(i,v_i)\in Q}T_i^{v_i}$。服务器验证$P_T$和$V_T$是否相等。

2.6.4 安全外包计算

2.6.4.1 概述

安全外包计算(secure outsourcing computation) 是解决大规模复杂运算的一种外包方式，即计算资源有限的用户将大规模的复杂运算外包给具有强大计算能力的云端服务器，同时需要保证用户原始数据和计算结果的机密性，并能够验证返回计算结果的正确性。

从外包计算模型的服务器数量来看，包括单服务器模型、双服务器模型以及多服务器模型。从外包计算的安全威胁模型来看，包括诚实而好奇的服务器、恶意的服务器等模型。在诚实而好奇的模型下，服务器会诚实地按照协议执行每个步骤，但会试图获取用户的数据内容和秘密信息；在恶意模型下，服务器有可能不按照协议的要求进行执行，会试图通过欺骗用户来获取用户的数据内容或秘密信息。

从安全外包计算解决的复杂运算类型来看，可以包括大规模的科学运算、大数据处理、机器学习、复杂的密码学运算等。例如，大规模科学运算包括矩阵运算、线性方程组运算、线性规划、序列比较等；复杂的密码学运算包括模幂运算、椭圆曲线点乘运算、双线性配对运算等；在机器学习和人工智能领域，资源受限的用户可以将机器学习中的模型训练、结果预测等外包给云端，包括卷积神经网络、图神经网络、决策树等等机器学习算法。

2002 年，Atalla 等首次提出了一个安全外包科学计算的基本框架[77]，采用不同的伪装盲化技巧去解决多种科学计算问题，但是不支持可验证功能。在针对密码学的外包计算方面，2005 年，Hohenberger 等首次提出了双服务器模型下的安全外包模幂的方案[78]，采用(g,g^b)盲化模幂运算中的指数和底数进行拆分，方案的验证概率为 1/2。之后，还有针对椭圆曲线点乘运算、双线性对等密码运算的安全外包计算方案[79, 80, 81]。

2.6.4.2 安全外包计算方案实例

一个安全外包计算方案主要包含五个步骤：

（1）密钥生成：给定一个安全性参数k和一个目标函数F，随机化密钥生成算法生成一个密钥SK。这个密钥SK将用来加密原始的输入和输出。

（2）问题转化：利用密钥SK将问题原始的输入x加密成一个公开值σ_x以及一个生成一个秘密值τ_x。σ_x发送到云服务器，τ_x安全存放在本地。

（3）计算：给定一个目标函数F和加密的输入σ_x，服务器计算σ_y，其σ_y是$y=F(x)$的一个加密值。

（4）验证：基于密钥SK和返回的σ_y，客户端进行验证结果的正确性。

（5）结果恢复：基于密钥SK，秘密值τ_x以及返回值σ_y，客户端进行结果恢复，得到原始的计算结果$y = F(x)$。

2005 年，Hohenberger 等在 Theory of Cryptography Conference 首次给出了外包计算的形式化定义[78]，并且提出了第一个在双服务器下的安全外包模幂的算法，具体方案如下：

模幂运算的输入是$a \in Z_q$和$u \in Z_p$，其中p和q是两个大素数并且满足$q|p-1$。

模幂运算的输出是$u^a \ mod \ p$。

（1） 盲化阶段：

用户首先运行两次子程序$Rand$生成两个盲化对(α, g^α)和(β, g^β)并将其表示为：

$$v = g^\alpha 和 v^b = g^\beta，其中 b = \beta/\alpha.$$

为了盲化u和a，对其进行两步逻辑拆分。第一步盲化u按照如下方式：

$u^a = (vw)^a = v^a w^a = v^b v^c w^a$，其中$w = u/v$，$c = a - b$.

随机选择两个随机元素$d \in Z_q$和$f \in G$，G是一个阶为q的群。第二步盲化a按照如下方式：

$$v^b v^c w^a = v^b (fh)^c w^{d+e} = v^b f^c h^c w^d w^e, 其中 h = v/f, e = a - d.$$

用户运行四次子程序$Rand$生成测试对(t_1, g^{t_1})，(t_2, g^{t_2})，(r_1, g^{r_1})和(r_2, g^{r_2})。

（2） 计算阶段：

用户向服务器U_1查询以下几个模幂运算：

$$U_1(d, w) \to w^d, \ U_1(c, f) \to f^c, U_1(t_1/r_1, g^{r_1}) \to g^{t_1}, \ U_1(t_2/r_2, g^{r_2}) \to g^{t_2}.$$

用户向服务器U_2查询以下几个模幂运算：

$$U_2(e, w) \to w^e, \ U_2(c, h) \to h^c, \quad U_2(t_1/r_1, g^{r_1}) \to g^{t_1}, \quad U_2(t_2/r_2, g^{r_2}) \to g^{t_2}.$$

（3） 验证解密阶段：

用户验证两个服务器输出的g^{t_1}和g^{t_2}是否正确。若正确，则按照如下方式进行解密：

$$v^b f^c h^c w^d w^e = v^{b+c} w^{d+e} = v^a w^a = (vw)^a = u^a.$$

2014 年，Chen 等提出了一个安全外包线性方程组的方案[82]。该方案是第一个仅需客户端与服务器端进行一轮通信就可解决线性方程组的方案，而且客户端能以 1 的概率验证返回结果的正确性，方案不需要复杂的密码运算。

线性方程组的输入时一个系数向量$b \in R^n$以及一个系数矩阵$A \in R^{n*n}$，输出是一个向量$x \in R^n$，满足$Ax = b$。

（1） 密钥生成：首先选择一个随机盲化向量$r \in R^n$以及两个稀疏矩阵$M, N \in R^{n*n}$。

（2） 问题转化：计算$c = Ar + b$。接下来计算$d = Mc$和$T = MAN$。

（3） 计算：客户端将d与T发送给服务器，服务器返回y满足$Ty = d$。

（4） 验证：客户端验证$Ty = d$是否成立。

（5） 结果恢复：客户端计算$x = Ny - r$。

2.7 数据安全的隐私计算密码协议

2.7.1 安全多方计算

2.7.1.1 概述

1982 年，姚期智提出的百万富翁问题被认为是安全多方计算（Secure Multiparty Computation，MPC）理论的开始，MPC 技术的目标是保证多个参与方共同完成一个计算任务，同时各方均不泄露自己的数据。

MPC 技术在数据安全和隐私计算等实际应用中具有广阔的应用前景，MPC 通过混淆电路、秘密分享、茫然传输、同态加密等密码技术，实现基本的算术/布尔运算（包括 XOR、AND、加法、乘法等运算），进而可以组合成更复杂的多方之间的数据计算功能，可提供隐匿查询、集合求交、联合统计、安全机器学习、联合预测等多种算法服务和应用服务，主要应用于多方数据计算、深度学习和隐私计算等场景中。文献[83]给出了安全多方计算技术的详细研究报告。

从技术应用方向看，MPC 系统主要分为通用安全多方计算平台、隐匿查询系统、基于集合求交的联合统计系统、隐私保护机器学习等系统，MPC 技术已逐渐开始推广应用。

2.7.1.2 MPC 标准化进展

国际标准：

- ITU-T

（1）2019 年 8 月，全球近 40 个国家和地区的 205 名专家代表在日内瓦召开 ITU-T SG17（国际电联安全研究组）会议时，通过了阿里巴巴主导的《Technical framework for Secure Multi-Party Computation》国际标准立项。

（2）ITU-T X.1770 (10/2021) 《Technical guidelines for secure multi-party computation》一文建立了多方计算（MPC）的技术指南并为信息和通信技术（ICT）提供了技术标准基础。

- IEEE

2020 年 10 月，IEEE（电器和电子工程师协会）国际标准 2842《Recommended Practice for Secure Multi-party Computation》已经基本定稿。该多方安全计算标准由 2019 年 10 月在全球最大的专业技术协会之一 IEEE 成功立项并主导推动，有望成为全球首个多方安全计算领域的国际标准。

2021 年 5 月 11 日，IEEE 2842-2021 标准《IEEE Recommended Practice for Secure Multi-Party Computation》正式出版。

- ISO/IEC

目前 ISO 正在制定 MPC 标准 ISO/IEC NP 4922-1/2《Proposal for a new work item on Information security -- Secure multiparty computation》。该标准共分为两部分：MPC 概述和秘密分享机制，具体包括 MPC 基本概念、安全模型、参与方、输入输出、参数等。目前该标准尚处于草案阶段。

国内标准：

- 工信部信通院通信团体标准《基于多方安全计算的数据流通产品技术要求和测试方法》

该标准规定了基于多方安全计算的数据流通产品必要的技术要求和相应的测试方法，适用于基于多方安全计算的数据流通产品的研发、测试、评估和验收等。

- 金融行业标准《JR/T 0196—2020 多方安全计算金融应用技术规范》

2020 年 11 月中国人民银行发布多方安全计算金融标准。该标准主体内容包括基本功能要求、安全性要求、性能要求，适用于金融机构开展多方安全计算金融应用的产品设计,软件开发。

- 多方安全计算密码技术框架

2021 年 7 月，密码行业标准《多方安全计算密码技术框架》已经正式立项编制，阐述了多方安全计算的术语和定义、协议框架和系统组成、协议安全要求和应用技术体系框架等，已经完成全国征求意见。

2.7.2 零知识证明

2.7.2.1 概述

1982 年，Goldwasser，Micali 和 Rackoff 首次提出零知识证明（zero-knowledge proof）的概念[84]。零知识证明是由证明者（Prover）和验证者（Verifier）参与进行的的两方安全协议，该协议允许证明者使得验证者确信某一断言(相信证明者拥有某知识)的正确性，但是不会泄露任何额外的信息。文献[85]给出了对零知识证明技术的详细研究报告。根据功能性和安全性，零知识证明需要满足如下三个性质：

a) 完备性（Completeness）
   当断言为真/证明者拥有知识时，证明者能够以压倒性的概率令验证者接受该证明。
b) 可靠性（Soundness）
   当断言为假/证明者不拥有该知识时，证明者不能让验证者相信断言为真，即证明者通过验证者验证的概率可以忽略。
c) 零知识性（Zero-knowledge）
   协议执行结束后，除了被证明断言的正确性外，验证者不能从协议执行过程中获取任何额外信息。

零知识证明包括交互式零知识证明和非交互式零知识证明。1988 年，Blum 等首次提出非交互式零知识证明[86]，非交互式零知识证明系统有许多不同于交互式证明的特性。交互式零知识证明系统可用于身份认证等密码协议的构造，非交互式零知识证明系统可用于区块链系统等。

1991 年，Goldreich，Micali 和 Wigderson 证明了如果单向函数存在，那么任何属于 NP 类语言的问题都存在相应的零知识证明系统[87]。这项工作为零知识证明奠定了坚实的理论基础，零知识证明得以被广泛应用于各种密码学任务。

2.7.2.2 标准化进展

在国际标准方面，ZKProof 是一个在国际上知名的零知识证明进行标准化的组织。该组织于 2018 年第一次召开研讨会，由最初的专家团体讨论零知识证明技术标准化的主题，每年都会召开一次零知识证明技术研讨会。经过多年的努力，该组织已经对零知识证明的标准化和主流化做出了重要贡献。

目前，ZKProof 在标准化方面设立了 5 个工作组(working groups (WG))和 3 个研讨组(Discussion Groups)。其中 5 个工作组(working groups (WG))包括：

- Commit-and-Prove ZKP Systems & Extensions 工作组：研究利用零知识证明系统实现可验证的承诺和加密机制的相关标准。
- Σ-protocols 工作组：研究交互式零知识证明的求和协议的相关标准。
- DAPOL 工作组：研究分布式审计债务证明相关的标准。

- zkInterface 工作组：研究零知识证明系统中的前端和后端系统的互操作相关的标准。
- Snark-Friendly Primitives 工作组：研究零知识证明系统中的密码算法等密码原语应用的相关标准。

3. 国内外政策、法律和标准发展情况

3.1 我国数据安全和密码政策和法律

3.1.1 数据安全和密码相关法律

《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》，这四部法律的陆续颁布和实施，以国家总体安全观为指引，形成了我国网络安全和数据安全的一套有机完善的法律体系，是国家安全法体系重要组成部分。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式施行，这是我国第一部全面规范网络空间安全而制定的基础性法律，是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定的法律。其中第十八条规定：“国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。”

2020 年 1 月 1 日，《中华人民共和国密码法》正式施行，这是中国密码领域的综合性、基础性法律，是为了规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，制定的法律。其中第八条规定：“商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。” 密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务，是保障数据安全的核心技术。

2021 年 9 月 1 日，《中华人民共和国数据安全法》正式施行，这是我国第一部专门规定数据安全的法律，是为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益而制定的法律。根据《数据安全法》的规定，数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力；维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力；坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展；国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。

2021 年 11 月 1 日，《中华人民共和国个人信息保护法》正式施行，这是一部为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用而制定的法律。根据《个人信息保护法》，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息；个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

3.1.2 数据安全相关法规和管理办法

2021 年以来，为进一步落实《中华人民共和国数据安全法》（“《数据安全法》”）以及《中华人民共和国个人信息保护法》（“《个人信息保护法》）”），工信部和国家

互联网信息办公室（“网信办”）分别起草了数据安全相关的各种条例和管理办法，并面向社会公开征求意见，具体包括《网络数据安全管理条例（征求意见稿）》《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》等。

2021 年 11 月 14 日，国家互联网信息办公室发布《网络数据安全管理条例（征求意见稿）》公开征求意见的通知[88]，此条例的目的是为了落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益。该条例针对《数据安全法》和《个人信息保护法》中的相关制度设计了实施路径，对相关要求进行细化和明确，增加了一些新的要求等。

《网络数据安全管理条例（征求意见稿）》规定[88]：“第三条 国家统筹发展和安全，坚持促进数据开发利用与保障数据安全并重，加强数据安全防护能力建设，保障数据依法有序自由流动，促进数据依法合理有效利用。”“第五条 国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。各地区、各部门应当按照国家数据分类分级要求，对本地区、本部门以及相关行业、领域的数据进行分类分级管理。”

为了贯彻落实《中华人民共和国密码法》，2020 年 8 月 20 日，国家密码管理局正式下发《关于〈商用密码管理条例（修订草案征求意见稿）〉公开征求意见的通知》[89]，向社会公开征求意见建议。征求意见稿共九章六十四条，修订内容主要集中在立法宗旨、管理范围、管理体制、科技创新与标准化、检测认证和产品及服务管理、电子认证、进出口、应用促进、监督管理等九方面。其中第三十六条规定：“国家支持网络产品、服务使用商用密码提升安全性，支持并规范商用密码在信息领域新技术、新业态、新模式中的应用。”

2021 年 09 月 30 日和 2022 年 2 月 10 日，工业和信息化部两次发布对《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》公开征求意见的通知[90]，此管理办法是的目的是贯彻落实《数据安全法》等法律法规，加快推动工业和信息化领域数据安全管理工作制度化、规范化，提升工业、电信行业数据安全保护能力，防范数据安全风险。该办法根据《数据安全法》等法律法规要求，在工业和信息化领域对国家数据安全管理制度进行细化，明确开展数据分类分级保护、重要数据管理等具体要求，构建工业和信息化领域数据安全监管体系。

针对云计算、汽车数据安全等重要领域，相关部门出台了一系列管理办法。2019 年 7 月 2 日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部发布了《云计算服务安全评估办法》[91]，目的是提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平。

2021 年 7 月 5 日，《汽车数据安全管理若干规定（试行）》经国家互联网信息办公室审议通过并发布[92]，并经国家发展和改革委员会、工业和信息化部、公安部、交通运输部同意，自 2021 年 10 月 1 日起施行。此规定是为了规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法律、行政法规而制定的规定。文件规定：“利用互联网等信息网络开展汽车数据处理活动，应当落实网络安全等级保护等制度，加强汽车数据保护，依法履行数据安全义务。”

3.1.3 数据安全发展规划

2022 年 01 月 12 日，国务院印发《“十四五”数字经济发展规划》，明确了“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施。《“十四五”数字经济发展规划》提出，数据要素是数字经济深化发展的核心引擎，数据的爆发增长、海量集聚蕴藏了巨大的价值，为智能化发展带来了新的机遇；协同推进技术、模式、业态和制度创新，切实用好数据要素，将为经济社会数字化发展带来强劲动力。

《“十四五”数字经济发展规划》提出了数据安全保障的要求：“提升数据安全保障水平。建立健全数据安全治理体系，研究完善行业数据安全管理政策。建立数据分类分级保护制度，研究推进数据安全标准体系建设，规范数据采集、传输、存储、处理、共享、销毁全生命周期管理，推动数据使用者落实数据安全保护责任。依法依规加强政务数据安全保护，做好政务数据开放和社会化利用的安全管理。依法依规做好网络安全审查、云计算服务安全评估等，有效防范国家安全风险。健全完善数据跨境流动安全管理相关制度规范。推动提升重要设施设备的安全可靠水平，增强重点行业数据安全保障能力。进一步强化个人信息保护，规范身份信息、隐私信息、生物特征信息的采集、传输和使用，加强对收集使用个人信息的安全监管能力。”

2022 年 3 月 5 日，李克强总理代表国务院在十三届全国人大五次会议上作《政府工作报告》，其中提到数字经济与数据安全的相关内容：“推进国家安全体系和能力建设。强化网络安全、数据安全和个人信息保护。……。促进数字经济发展。加强数字中国建设整体布局。……。完善数字经济治理，培育数据要素市场，释放数据要素潜力，提高应用能力，更好赋能经济发展、丰富人民生活。”

2022 年 12 月 2 日，中共中央、国务院发布了《关于构建数据基础制度更好发挥数据要素作用的意见》，又称为“数据二十条”，提出构建数据产权、流通交易、收益分配、安全治理等制度，提出“原始数据不出域、数据可用不可见”的要求，提出要强化数据安全保障体系建设，把安全贯穿数据供给、流通、使用全过程。

3.2 国际数据安全和密码政策/法律

2018 年 5 月 25 日，欧洲联盟出台《通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）[93]，其前身是欧盟在 1995 年制定的《计算机数据保护法》。该条例的适用范围非常广泛，任何收集、传输、保留或处理涉及到欧盟所有成员国内的个人信息的机构组织均受该条例的约束。一个主体不属于欧盟成员国的公司，只要满足下列两个条件之一，即收到此条例的约束：

（1）为了向欧盟境内可识别的自然人提供商品和服务而收集、处理他们的信息。

（2）为了监控欧盟境内可识别的自然人的活动而收集、处理他们的信息，其就受到 GDPR 的管辖。

1974 年 12 月，美国国会通过《隐私权法》（Privacy Act），这是一部保护公民隐私权和知情权的重要法律，针对联邦行政部门收集、利用和保护个人数据等方面做出规定。1986 年，美国国会制定《电子通讯隐私法》（ElectronicCommunicationsPrivacyAct，ECPA），目的是禁止未经授权的第三方截获或监听个人通信信息，是对原先电话有线监听管理制度的延伸和扩展。关于美国的数据安全和隐私保护的法律法规情况，参见文献[94, 95]。

美国的一些州制定了关于数据安全和隐私保护的地方法律法规。2018 年 6 月，《加州消费者隐私法案》(California Consumer Privacy Act，以下简称“CCPA”），该法

赋予了消费者若干权利，包括：有权要求删除个人数据；有权要求机构公开如何收集和共享信息；有权要求机构不得出售个人数据；对违反本法律的人或机构，消费者有权提出诉讼。 此外，法律还要求机构对所有消费者一视同仁，即使他们拒绝机构收集数据。其他一些州，例如佛蒙特州、伊利诺伊州、华盛顿州、得克萨斯州等都制定了数据安全和隐私保护的相关法律。

2005 年 4 月 1 日起，日本《个人信息保护法》正式施行；2015 年，该法律进行了大幅修正,2017 年 5 月 30 日起施行;2021 年 8 月 3 日,日本个人信息保护委员会(″PPC″）公布了日本《个人信息保护法》(″APPI″）2020 年修正案的指南，征求公众意见，并将于 2022 年 4 月 1 日起正式实施。

2020 年 1 月 9 日，韩国国会通过了《个人信息保护法》、《信用信息法》、《信息通信网法》修订案。《个人信息保护法》修订案的主要内容是在没有本人同意的情况下，可以将经过处理无法识别特定个人的假名信息用于统计和研究等目的。内容还包括将监督误用、滥用、泄露个人信息的机构划归个人信息保护委员会。

2012 年 10 月 15 日，新加坡颁布了《个人数据保护法》，该法是一部规范个人数据的收集、使用和披露的综合性立法。2013 年 1 月 2 日，新加坡成立了个人数据保护委员会（PDPC），负责管理和执行《个人数据保护法》的相关事项。2020 年 5 月 14 日，新加坡通信信息部（MCI）和个人数据保护委员会（PDPC）联合发布了《个人数据保护法（修订）》草案（全文翻译见下文），并向社会公众公开征求意见。2020 年 11 月 2 日，新加坡通过了《2020 年个人数据保护（修正）法案》，这是 PDPA 自 2012 年颁布以来的首次全面修订，引入了强制数据泄露通知制度。

3.3 数据安全和密码技术标准情况

3.3.1 数据安全标准情况

3.3.1.1 国际标准情况

1979 年,ISO/TC97 国际标准化组织信息处理技术委员会开始数据加密技术标准化；1984 年 1 月在联邦德国波恩正式成立分技术委员会 SC20，从此数据加密技术标准化工作在 ISO/TC97 内正式展开；在 SC20 存在的五年期间完成了两个正式标准：ISO 8372 和 ISO 9160；1986 年 10 月，ISO 将密码算法的标准化工作从 SC20 的工作范围内取消。关于数据安全和密码技术的国际标准情况，参见文献[96, 97, 98]。

1989 年 6 月,ISO 正式撤消 SC20,组建新的 SC27;1990 年 4 月,ISO 正式成立 SC27，其名称为：信息技术-安全技术，ISO/IDC JTC1/SC27 负责通用信息技术安全标准的制定。SC27 制定了一些数据安全相关的标准，包括 ISO/IEC 27040:2015《信息技术 安全技术 存储安全》、ISO/IEC 29100:2011《信息技术 安全技术隐私保护框架》、ISO/IEC 27550《信息技术 安全技术 隐私保护工程》、ISO/IEC 29190《信息技术 安全技术 隐私保护能力评估模型》、ISO/IEC 20547-4《信息技术 大数据参考架构 第 4 部分：安全与隐私保护》、ISO/IEC 27045《大数据安全与隐私保护过程》、《大数据安全实施指南》等，其中后面三项标准由我国主导制定。2018 年，我国在 SC27 提出《Data Security (数据安全)》研究项目，主要研究数据安全标准化的顶层设计、传统的和新兴的数据保护技术标准，以及数据在云计算、大数据、物联网、移动互联网、智慧城市等新技术领域的安全问题和需求。2020 年 9 月，ISO/IEC 27046《大数据安全与隐私实现指南》形成了第三版草案，进行新一轮的意见征集。

2014 年,国际标准化组织 ISO/IECJTC 1 成立了大数据工作组(ISO/IEC JTC1/WG 9，

WG 9)，编制大数据相关的国际标准。WG9 工作组制定了 ISO/IEC 20547-4《Part 4: Security and Privacy (第 4 部分：安全与隐私保护)》；2016 年 3 月，将该标准转交给 SC27 技术委员会。

国际电信联盟电信标准分局（International Telecommunication Union Telecommunication Standardization Sector，ITU-T） 的安全工作组（Study Group 17, ITU-T SG17）制定了一些数据安全相关的标准，包括 X.1033《运营商提供的个人信息服务安全指南》、，X.1641《云服务客户数据安全指南》、。X.GSBDaaS《大数据服务安全指南》等。

国际标准化组织金融服务技术委员会（ISO/TC68）作为金融标准委员会，也制定了很多密码技术和信息安全的标准。

2013 年 5 月，美国国家标准化研究院（National Institute of Standards and Technology，NIST）于成立了 NIST 大数据公共工作组(NIST Big Data Working Group，NBD-PWG)，发布了大数据框架等标准；NIST 还发布了 SP 800-122、NISTIR 8053 等多项数据安全相关标准。

3.3.1.2 国内标准情况

为了加快推动我国大数据安全标准化工作，全国信息安全标准化技术委员会（以下简称“全国信安标委”，委员会编号为 TC260）在 2016 年 4 月成立大数据安全标准特别工作组（以下简称“特别工作组”，SWGBDS），主要负责制定和完善我国大数据安全领域标准体系，组织开展大数据安全相关技术和标准研究，制定 GB / T 35274-2017《信息安全技术 大数据服务安全能力要求》、GB/T 37932-2019《信息安全技术 数据交易服务安全要求》、GB / T 37973-2019《信息安全技术 大数据安全管理指南》、GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》、GB/T 35273-2020《信息安全技术 个人信息安全规范》及《信息安全技术 政务信息共享 数据安全技术要求》等国家标准。2017 年和 2018 年，大数据安全标准特别工作组（SWG-BDS）编制发布了《大数据安全标准化白皮书》。

GB / T 35274-2017《信息安全技术 大数据服务安全能力要求》[99]规定了大数据服务提供者应具有的组织相关基础安全能力和数据生命周期相关的数据服务安全能力，适用于对政府部门和企事业单位建设大数据服务安全能力，也适用于第三方机构对大数据服务提供者的大数据服务安全能力进行审查和评估。

GB/T 37932-2019《信息安全技术 数据交易服务安全要求》[100]规定了通过数据交易服务机构进行数据交易服务的安全要求，包括数据交易参与方、交易对象和交易过程的安全要求。该标准适用于数据交易服务机构进行安全自评估，也可供第三方测评机构对数据交易服务机构进行安全评估时参考。

GB / T 37973-2019《信息安全技术 大数据安全管理指南》[101]标准为组织的大数据安全管理提供指导，提出大数据安全管理基本原则、基本概念和大数据安全风险管理过程。本标准提出大数据的数据收集、数据存储、数据使用、数据分发、 数据删除等主要阶段的基本概念和管理要求，并规范了组织内部不同大数据角色的安全职责。

GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》[6]给出了组织数据安全能力的成熟度模型架构，规定了数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、通用安全的成熟度等级要求。该标准适用于对组织数据安全能力进行评估，也可作为组织开展数据安全能力建设时的依据。

GB/T 35273-2020《信息安全技术 个人信息安全规范》[102]针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，规范个人信息控制者在收

集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。我国数据安全标准化情况参见文献[103]。

我国为电信和互联网行业数据安全标准化工作，工业和信息化部在前期做了大量研究基础上，在 2020 年 8 月公开征求对《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》的意见，并历时 4 个月的修订时间，于 12 月正式发布了《电信和互联网行业数据安全标准体系建设指南》。

2022 年 2 月 25 日，工业和信息化部办公厅发布了《车联网网络安全和数据安全标准体系建设指南》，建立健全车联网网络安全和数据安全保障体系，为车联网产业安全健康发展提供支撑。

在金融行业标准中[104]，数据安全相关标准主要有：JR/T 0158—2018 《证券期货业数据分类分级指引》、JR/T 0171—2020 《个人金融信息保护技术规范》、JR/T 0197—2020 《金融数据安全　数据安全分级指南》、JR/T 0223—2021《金融数据安全　数据生命周期安全规范》等标准。

2021 年 4 月 8 日，《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）（以下简称《规范》）正式获批发布实施。《规范》由中国人民银行科技司发起，全国金融标准化技术委员会归口管理。金融数据复杂多样，对数据实施生命周期安全管理，可以进一步明确数据生命周期各阶段的保护要求，有助于金融业机构合理分配数据保护资源和成本，建立完善的数据生命周期防护机制。同时，合理、准确、完善的数据生命周期管理制度能够促进金融数据在机构间、行业间安全应用和共享，有利于数据价值挖掘与实现。

在电子政务领域[105]，GB/T 39477—2020《信息安全技术 政务信息共享 数据安全技术要求》中，从政务信息共享交换中的数据安全与保护出发，依据数据分类与分级原则及数据安全能力成熟度模型，提出了规范政务信息交换共享中的数据安全防护技术要求。

3.3.2 密码技术标准情况

3.3.2.1 我国密码标准体系建设

密码是网络安全的核心技术和基础支撑。《中华人民共和国密码法》专门规定了要密码标准体系建设：

“第二十二条　国家建立和完善商用密码标准体系。国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准。国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

第二十三条　国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用。国家鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。“

为满足密码领域标准化发展需求，充分发挥密码科研、生产、使用、教学和监督检验等方面专家作用，更好地开展密码领域的标准化工作，2011 年 10 月，经国家标准化管理委员会和国家密码管理局批准，成立“密码行业标准化技术委员会”（以下简称“密标委”），英文名称“Cryptography Standardization Technical Committee”（简称“CSTC”）。密标委是在密码领域内从事密码标准化工作的非法人技术组织，归口国家密码管理局领导和管理，主要从事密码技术、产品、系统和管理等方面的标准化工作。密标委目前下设秘书处和总体、基础、应用、测评四个工作组。

自 2012 年以来，国家密码管理局陆续发布了我国商用密码技术标准，截止 2022 年 3 月，已发布密码行业标准 102 项，范围涵盖密码算法、密码协议、密码产品、密码应用、密码检测等多个方面，已初步形成体系化，基本能够满足我国社会各行业在构建信息安全保障体系时的应用需求。自 2015 年起，以全国信息安全标准化技术委员会 WG3 工作组为依托，具有通用性的密码行业标准陆续向国家标准升级，已颁布 20 多项密码国家标准。

图 3 密码标准技术体系框架

密码标准主要包括以下七大类型：

密码基础类标准主要对通用密码技术进行规范，它是体系框架内的基础性规范，主要包括密码术语与标识标准、密码算法标准、密码设计与使用标准等。

基础设施类标准主要针对密码基础设施进行规范，包括：证书认证系统密码协议、

数字证书格式、证书认证系统密码及相关安全技术等。

密码产品类标准主要规范各类密码产品的接口、规格以及安全要求。对于智能密码钥匙、VPN、安全认证网关、密码机等密码产品给出设备接口、技术规范和产品规范；对于密码产品的安全性，则不区分产品功能的差异，而以统一的准则给出要求；对于密码产品的配置和技术管理架构，则以 GM/T 0050《密码设备管理设备管理技术规范》为基础统一制定。

应用支撑类标准针对密码报文、交互流程、调用接口等方面进行规范，包括通用支撑和典型支撑两个层次。通用支撑规范（GM/T 0019）通过统一的接口向典型支撑标准和密码应用标准提供加解密、签名验签等通用密码功能，典型支撑类标准是基于密码技术实现的与应用无关的安全机制、安全协议和服务接口，如可信计算可信密码支撑平台接口、证书应用综合服务接口等。

密码应用类标准是对使用密码技术实现某种安全功能的应用系统提出的要求以及规范，包括应用要求和典型应用两类。应用要求旨在规范社会各行业信息系统对密码技术的合规使用，典型应用则定义了具体的密码应用，如动态口令、安全电子签章等。

密码检测类标准针对标准体系所确定的基础、产品和应用等类型的标准出台对应检测标准，如针对随机数、安全协议、密码产品功能和安全性等方面的检测规范。其中对于密码产品的功能检测，分别针对不同的密码产品定义检测规范；对于密码产品的安全性检测则基于统一的准则执行。

密码管理类标准主要包括国家密码管理部门在密码标准、密码算法、密码产业、密码服务、密码应用、密码监查、密码测评等方面的管理规程和实施指南。

3.3.2.2 国内外密码技术标准情况

GM/Y 5001-2021《密码标准使用指南》给出了已颁布的密码行业标准的介绍和使用指南。我国的密码算法标准包括 SM2、SM3、SM4、SM9、ZUC 算法(即“祖冲之密码算法”)等，其中 SM2、SM9 为公钥密码算法，SM3 为密码杂凑算法，SM4 为分组对称密码算法，ZUC 为序列密码算法。其他的基础类标准包括 GM/T 0005《随机性检测规范》、GM/T 0006《密码应用标识规范》等。

密码协议标准包括数字认证、访问控制、密钥交换/协商、密钥管理、安全通信等协议。GB/T 20518《信息安全技术 公钥基础设施数字证书格式规范》、GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》、GM/T 0014《数字证书认证系统密码协议规范》等标准规定了数字证书和证书撤销列表的格式、安全协议流程、密码函数接口等内容，以及数字证书认证系统的设计、建设、检测、运行及管理规范，适用于数字证书认证系统的研发、数字证书认证机构的运营以及基于数字证书的安全应用。

分组密码算法是用于数据加密和消息鉴别的常用算法，GB/T 17964-2021《信息安全技术 分组密码算法的工作模式》规定了分组密码算法的九种工作模式,包括 ECB、CBC、CFB、OFB、CTR、XTS、HCTR、BC、OFBNLF 等模式，用于保护数据的机密性，不适用于保护数据完整性。GB/T 15852.1-2008《信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制》规定了分组密码算法的六种消息鉴别码机制，可用于数据完整性检验、消息源合法性验证。GB/T 36624-2018《可鉴别加密功能的工作模式》规定了五种可鉴别的加密机制，将分组加密和鉴别机制结合，用于实现数据机密性、完整性和数据源鉴别。密码行业标准研究报告《基于国密算法的保留格式加密(FPE)研究》对保留格式加密进行了详细的分析和研究。

同态加密算法是用于密文计算、安全多方计算、隐私保护等应用场景的重要算法类型。2019 年 5 月，国际标准化组织 ISO 发布了同态加密标准（ISO/IEC 18033-6:2019）。

该标准仅涉及半同态加密算法，具体包含两种较为成熟的半同态加密机制：ElGamal 乘法同态加密算法和Paillier 加法同态加密算法，并规定了参与实体的参数和密钥生成、数据加密、密文数据解密、密文数据同态运算等步骤的具体过程。2017 年 7 月，全同态加密标准化开放联盟 HomomorphicEncryption.org 成立，在微软研究院举办了首届全同态加密标准化研讨会，开始推进全同态加密标准草案的编写工作，并发布了全同态加密安全、API、应用三份白皮书。2021 年，我国的密码行业标准研究项目《全同态加密研究》已经立项，对全同态加密技术进行系统的研究。

在数字签名方案方面，ISO/IEC 发布的一系列的数字签名算法标准，包括：

（1）带消息恢复的数字签名算法标准系列 ISO/IEC9796，包括基于大数分解的 9796-2、基于离散对数的 9796-3。

（2)带附录的数字签名算法标准系列 ISO/IEC14888，包括基于大数分解的 14888-2、基于离散对数的 14888-3、基于状态哈希的 14888-4。

（3）匿名签名算法标准系列 ISO/IEC20008，包括基于群公钥签名的 20008-2、基于多公钥签名的 20008-2。

（4）盲签名算法标准系列 ISO/IEC18370，包括基于离散对数的 18370-2。

（5）可修订的签名算法系列 ISO/IEC23264，包括基于非对称技术的可修订签名 23264-2。在我国的国家标准和密码行业标准方面，关于数字签名的标准很多，其中一部分标准是等同采用 ISO 国际标准。

在国家标准方面，关于数字签名的标准很多，其中一部分标准是等同采用 ISO 国际标准，与特殊数字签名相关的一部分国家标准如下：

表 2 部分数字签名国家标准

编号	名称	标准类型
20210972-T-469	信息技术 安全技术 带附录的数字签名 第 1 部分：概述 Information technology—Security techniques—Digital signature with appendix—Part 1:General	国家标准制定中
GB/T 38647.1-2020	信息技术 安全技术 匿名数字签名 第 1 部分：总则 Information technology—Security techniques—Anonymous digital signatures—Part 1: General	国家标准
GB/T 38647.2-2020	信息技术 安全技术 匿名数字签名 第 2 部分：采用群组公钥的机制 Information technology—Security techniques—Anonymous digital signatures—Part 2: Mechanisms using a group public key	国家标准
GB/T 15851.3-2018	信息技术 安全技术 带消息恢复的数字签名方案 第 3 部分：基于离散对数的机制 Information technology—Security techniques—Digital signature schemes giving message recovery—Part 3：Discrete logarithm	国家标准

	based mechanisms	

表 2 部分数字签名国家标准（续）

编号	名称	标准类型
GB/T 34953.2-2018	信息技术 安全技术 匿名实体鉴别 第 2 部分：基于群组公钥签名的机制	国家标准
	Information technology — Security techniques—Anonymous entity authentication —Part 2: Mechanisms based on signatures using a group public key	
GB/T 17902.3-2005	信息技术 安全技术 带附录的数字签名 第 3 部分:基于证书的机制	国家标准
	Information technology-Decurity techniques-Digital signatures with appendix-Part3:Certificate-based mechanisms	
GB/T 17902.2-2005	信息技术 安全技术 带附录的数字签名 第 2 部分:基于身份的机制	国家标准
	Information technology-Security techniques-Digital signatures with appendix-Part2:Identity-based mechanisms	
GB/T 17902.1-1999	信息技术 安全技术 带附录的数字签名 第 1 部分:概述	国家标准
	Information technology--Security techniques--Digital signature with appendix--Part 1:General	

在秘密分享技术方面，国际标准化组织（ISO）发布了两套有关秘密分享的加密标准，分别是 ISO/IEC 19592-1:2016 和 ISO/IEC 19592-2:2017。其中，ISO/IEC 19592-1:2016 定义了秘密分享的参与方、相关术语以及方案的参数和特性；ISO/IEC 19592-2:2017 规定了秘密分享方案及其特性。我国密码行业标准研究项目《秘密分享技术研究》正在进行中。

在属性加密方面，在国际标准方面，2018 年 8 月，欧洲电信标准协会(ETSI)发布了两个安全访问控制的加密标准(CRYPTOGRAPHIC STANDARDS FOR SECURE ACCESS CONTROL)，分别为 ETSI-TS-103-458 和 ETSI-TS-103-532，采用 ABE 属性加密提供细粒度的个人数据保护，可以用于 5G、IoT 物联网等分布式系统。

在多方安全计算方面，2019 年 8 月，全球近 40 个国家和地区的 205 名专家代表在日内瓦召开 ITU-T SG17（国际电联安全研究组）会议时，通过了阿里巴巴主导的《Technical framework for Secure Multi-Party Computation》国际标准立项。ITU-T X.1770 (10/2021) 《Technical guidelines for secure multi-party computation》一文建立了多方计算（MPC）的技术指南并为信息和通信技术（ICT）提供了技术标准基础。

2020 年 10 月,IEEE(电器和电子工程师协会)国际标准 2842《Recommended Practice for Secure Multi-party Computation》已经基本定稿。该多方安全计算标准由 2019 年 10 月在全球最大的专业技术协会之一 IEEE 成功立项并主导推动，有望成为全球首个

多方安全计算领域的国际标准。2021 年 5 月 11 日，IEEE 2842-2021 标准《IEEE Recommended Practice for Secure Multi-Party Computation》正式出版。

目前 ISO 正在制定 MPC 标准 ISO/IEC NP 4922-1/2《Proposal for a new work item on Information security -- Secure multiparty computation》。该标准共分为两部分：MPC 概述和秘密分享机制，具体包括 MPC 基本概念、安全模型、参与方、输入输出、参数等。目前该标准尚处于草案阶段。

工信部信通院制定了通信团体标准《基于多方安全计算的数据流通产品技术要求和测试方法》，该标准规定了基于多方安全计算的数据流通产品必要的技术要求和相应的测试方法。

2020 年 11 月，中国人民银行发布金融行业标准《JR/T 0196—2020 多方安全计算金融应用技术规范》。该标准主体内容包括基本功能要求、安全性要求、性能要求，适用于金融机构开展多方安全计算金融应用的产品设计,软件开发。

2021 年，密码行业标准《多方安全计算密码技术框架》已经正式立项编制，阐述了多方安全计算的术语和定义、协议框架和系统组成、协议安全要求和应用技术体系框架等已进行全国征求意见。

在零知识证明方面,ZKProof 是一个在国际上知名的零知识证明进行标准化的组织。该组织于 2018 年第一次召开研讨会，由最初的专家团体讨论零知识证明技术标准化的主题，每年都会召开一次零知识证明技术研讨会。经过多年的努力，该组织已经对零知识证明的标准化和主流化做出了重要贡献。目前，ZKProof 在标准化方面设立了 5 个工作组(working groups (WG))和 3 个研讨组(Discussion Groups)。

4. 数据安全密码技术体系与标准化

目前，国内外数据安全的法律和标准相继出台，在云服务、金融、医疗、政务等领域的数据安全标准已经颁布或正在制定过程中。在密码行业标准方面，SM 系列标准密码算法、分组密码算法的工作模式、随机数生成、数字证书、密钥管理等标准已经颁布并实施推广，为数据安全领域提供了最基础的密码技术支撑；安全多方计算、秘密分享、同态加密、零知识证明、可搜索加密等，作为数据安全领域亟需的密码技术，多数正在进行标准制定或研究项目。

本研究项目将通过对数据安全实际需求、相关密码技术的分析、梳理，针对数据安全典型的应用场景，提出数据安全密码技术体系框架（见图 4），为下一步的标准化工作提供理论和技术支撑。

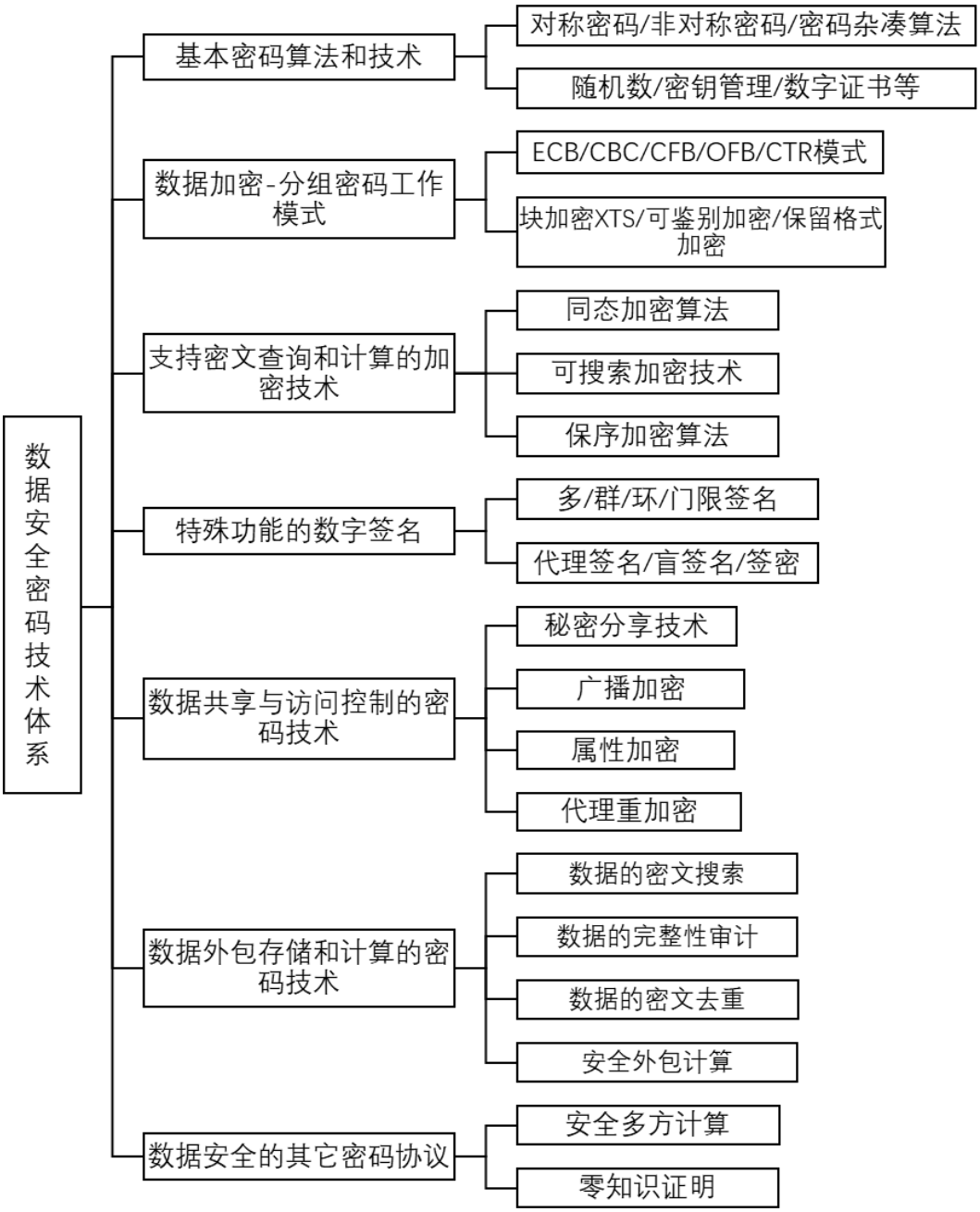

图 4 数据安全密码技术体系

在我国的密码行业标准方面，针对数据安全密码技术应用的总体标准的研究依旧处于空白阶段，亟需研究并制定数据安全的密码技术应用标准，规范数据安全应用中的新型密码技术，为各个领域的数据安全提供密码技术实施和应用的指南，并为数据安全其他相关标准的制定提供支持。

参考文献

[1] 国发〔2021〕29 号，《“十四五”数字经济发展规划》，中华人民共和国国务院

[2] 《中华人民共和国数据安全法》

[3] 《中华人民共和国网络安全法》

[4] 《中华人民共和国密码法》

[5] 《中华人民共和国个人信息保护法》

[6] GB/T37988-2019 信息安全技术 数据安全能力成熟度模型

[7] GM/Y 5001-2021 密码标准使用指南

[8] GB/T 33133 信息安全技术 祖冲之序列密码算法

[9] GB/T 32907 信息安全技术 SM4 分组密码算法

[10] GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

[11] GB/T 38635 信息安全技术 SM9 标识密码算法

[12] GB/T 32905 信息安全技术 SM3 密码杂凑算法

[13] GB/T 32915 信息安全技术二元序列随机性检测方法

[14] GM/T 0051 密码设备管理对称密钥管理技术规范

[15] GB/T 20518 信息安全技术 公钥基础设施数字证书格式规范

[16] GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

[17] GM/T 0014 数字证书认证系统密码协议规范

[18] GM/T 0031 安全电子签章密码应用技术规范

[19] GM/T 0055 电子文件密码应用技术规范

[20] GB/T 17964-2021 信息安全技术 分组密码算法的工作模式

[21] GB/T 15852.1-2008 信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制

[22] GB/T 36624-2018 可鉴别加密功能的工作模式

[23] IEEE P1619, Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

[24] 基于国密算法的保留格式加密(FPE)研究，密码行业标准研究报告.

[25] 刘哲理, 贾春福, 李经纬. 保留格式加密技术研究[J]. 软件学报, 2012, 23(001):152-170.

[26] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[27] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. Advances in Cryptology. Berlin: Springer, 1999: 223-238.

[28] https://www.freebuf.com/articles/database/244536.html. 同态加密：实现数据的“可算不可见”.

[29] 李增鹏, 马春光, 周红生. 全同态加密研究[J]. 密码学报, 2017, 4(6): 561－578.

[30] 杨亚涛,赵阳,张卷美,黄洁润,高原.同态密码理论与应用进展[J].电子与信息学报,2021,43(02):475-487.

[31] Gentry C. Fully homomorphic encryption using ideal lattices. Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[32] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE[C]//Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on. IEEE, 2011: 97-106.

[33] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping[C]//Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. ACM, 2012: 309-325.

[34] Fan J , Vercauteren F . Somewhat practical fully homomorphic encryption [J]. Iacr Cryptology Eprint Archive, 2012.

[35] Gentry C, Sahai A, Waters B, et al. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based[C]. International Cryptology Conference, 2013: 75-92.

[36] Cheon J H, Kim A, Kim M, et al. Homomorphic Encryption for Arithmetic of Approximate Numbers[C]. International Conference on the Theory and Application of Cryptology and Information Security, 2017:409-437.

[37] HOWGRAVE-GRAHAM N. Approximate integer common divisors[C]. International Cryptography and Lattices Conference, Providence, USA, 2001: 51－56.

[38] https://homomorphicencryption.org/standard/.

[39] Song XD, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE Press, 2000. 44-55.

[40] Goh E J. Secure indexes. Cryptology ePrint Archive, 2003.

[41] Curtmola R, Garay J, Kamara S, et al. Searchable symmetric encryption: improved definitions and efficient constructions[J]. Journal of Computer Security, 2011, 19(5): 895-934.

[42] Agrawal R , Kiernan J , Srikant R , et al. Order preserving encryption for numeric data[C]// Proceedings of the ACM SIGMOD International Conference on Management of Data, Paris, France, June 13-18, 2004. ACM, 2004.

[43] 郭晶晶, 苗美霞, 王剑锋. 保序加密技术研究与进展[J]. 密码学报, 2018, 5(2): 182－195.

[44] BOLDYREVA A, CHENETTE N, LEE Y, et al. Order-preserving symmetric encryption[C]. In: Advances in Cryptology—EUROCRYPT 2009. Springer Berlin Heidelberg, 2009: 224－241.

[45] 程朝辉.数字签名技术概览[J].信息安全与通信保密,2020(7):48-62.

[46] 区块链密码技术体系框架研究，密码行业标准研究报告.

[47] 区块链密码使用指南，密码行业标准(草稿).

[48] Itakura K., Nakamura K. A Public-Key Cryptosystem Suitable for Digital Multisignatures. NEC Research and Development, 71: 1－8, 1983.

[49] Desmedt Y. Society and Group Oriented Cryptography: a New Concept. Advances in Cryptology-CRYPTO’87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg.

[50] Chaum D., van Heyst E. (1991) Group Signatures. Advances in Cryptology-EUROCRYPT’91. EUROCRYPT 1991. Lecture Notes in Computer Science, vol 547. Springer, Berlin.

[51] Mambo M., Usuda K., Okamoto E. (1996) Proxy Signatures: Delegation

of The Power to Sign Messages. IEICE Transactions Fundamentals, E79-A (9), 1338－1354.

[52] Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology. Springer, Boston, MA, 1983.

[53] Zheng, Y. "Digital signcryption or how to achieve cost(signature & encryption) cost(signature) + cost(encryption)." Lecture Notes in Computer ence 1294，1997.

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

[55] Blakley G R. Safeguarding cryptographic keys[C]. AFIPS Conference Proceedings, New York, 1979: 313-317.

[56] Fiat A., Naor M. Broadcast Encryption[c]. Proc of the 13th Annual International Cryptology Conference, Berlin Heidelberg: Springer，1993:480-491.

[57] 冯登国，Stinson，D.R,，密码学原理与实践（第三版），电子工业出版社，2009年。

[58] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers, 2001[C]. Springer.

[59] 冯登国，大数据安全与隐私保护，清华大学出版社，2018年12月。

[60] SAHAI A, WATERS B. Fuzzy Identity-based Encryption[C]//Springer. Annual International Conference on Theory and Applications of Cryptographic Techniques, May 22-26, 2005, Aarhus, Denmark. Heidelberg: Springer, 2005: 457-473.

[61] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data[C]. ACM. ACM Conference on Computer and Communications Security, October 30-November 3, 2006, Alexandria, Virginia, USA. New York: ACM, 2006: 89-98.

[62] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy Attribute-based Encryption[C]//IEEE. IEEE Symposium on Security and Privacy, May 20-23, 2007, Berkeley, USA. New York: IEEE, 2007:321-334.

[63] 冯登国, 陈成. 属性密码学研究[J]. 密码学报, 2014, 1(1): 1－12.

[64] 王建华, 王光波, 赵志远，密文策略属性加密技术，人民邮电出版社，2020年8月.

[65] 徐鹏，林璟锵，金海，王蔚，王琼霄，云数据安全，机械工业出版社，出版时间:2018年08月.

[66] 陈晓峰, 马建峰, 李晖, 李进，云计算安全，科学出版社，2016-02-01.

[67] M. Mambo, E. Okamoto. Proxy cryptosystems: Delegation of the power to decrypt ciphertexts[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1997, 80(1): 54-63.

[68] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography[A]. Advances in Cryptology-Eurocrypt'98[C]. Berlin: Springer-Verlag, 1998, 127-144.

[69] 王杰，Zachary A. Kissel, 孔凡玉，计算机网络安全的理论与实践（第3版），高等教育出版社，2017年11月.

[70] 黄勤龙, 杨义先，云计算数据安全，北京邮电大学出版社，2018 年 01 月.

[71] Ateniese G, Burns R, Curtmola R, et al. Provable data possession at untrusted stores[C]//Proceedings of the 14th ACM conference on Computer and communications security. 2007: 598-609.

[72] Juels, Ari , and B. S. K. Jr . "Pors: proofs of retrievability for large files." CCS '07: Proceedings of the 14th ACM conference on Computer and communications securityOctober 2007 Pages 584 - 597.

[73] Douceur J R , Adya A , Bolosky W J , et al. Reclaiming space from duplicate files in a serverless Distributed File System. Proceedings 22nd International Conference on Distributed Computing Systems, 617-624, 2002.

[74] Bellare M, Keelveedhi S, Ristenpart T. Message-locked encryption and secure deduplication[C]//Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2013: 296-312.

[75] Chen R, Mu Y, Yang G, et al. BL-MLE: block-level message-locked encryption for secure large file deduplication[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2643-2652.

[76] Halevi S, Harnik D, Pinkas B, et al. Proofs of ownership in remote storage systems[C]//Proceedings of the 18th ACM conference on Computer and communications security. 2011: 491-500.

[77] Atallah M J, Pantazopoulos K N, Rice J R, et al. Secure outsourcing of scientific computations[M]//Advances in Computers. Elsevier, 2002, 54: 215-272.

[78] Hohenberger S, Lysyanskaya A. How to securely outsource cryptographic computations[C]//Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2005: 264-282.

[79] Zhou K, Afifi M H, Ren J. ExpSOS: secure and verifiable outsourcing of exponentiation operations for mobile cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2518-2531.

[80] Chevallier-Mames B, Coron J S, McCullagh N, et al. Secure delegation of elliptic-curve pairing[C]//International Conference on Smart Card Research and Advanced Applications. Springer, Berlin, Heidelberg, 2010: 24-35.

[81] Chen X, Susilo W, Li J, et al. Efficient algorithms for secure outsourcing of bilinear pairings[J]. Theoretical Computer Science, 2015, 562: 112-121.

[82] Chen X, Huang X, Li J, et al. New algorithms for secure outsourcing of large-scale systems of linear equations[J]. IEEE transactions on information forensics and security, 2014, 10(1): 69-78.

[83] 多方安全计算技术研究，密码行业标准研究报告.

[84] Goldwasser S , Micali S , Rackoff C . The knowledge complexity of interactive proof systems[M]. Society for Industrial and Applied Mathematics, 1989.

[85] 零知识证明技术研究，密码行业标准研究报告.

[86] Blum M , Feldman P , Micali S . Non-Interactive Zero-Knowledge and

Its Applications (Extended Abstract)[C]// Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA. ACM, 1988.

[87] Goldreich O , Micali S , Wigderson A . Proofs that Yield Nothing But Their Validity for All Languages in NP Have Zero-Knowledge Proof Systems [J]. Journal of the ACM, 1991, 38(3):691-729.

[88] 《网络数据安全管理条例（征求意见稿）》

[89] 《商用密码管理条例（修订草案征求意见稿）》

[90] 《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》

[91] 《云计算服务安全评估办法》

[92] 《汽车数据安全管理若干规定（试行）》

[93] 通用数据保护条例 https://baike.baidu.com.

[94] 刘克佳，美国保护个人数据隐私的法律法规及监管体系. 全球科技经济瞭望. 第 34 卷第 4 期，4-11, 2019 年 4 月.

[95] 黄道丽，胡文华,后 GDPR 时代的美国数据隐私保护走向，http://www.mchz.com.cn/cn/about-us/industry-news/info_366.aspx?itemid=3012&ezeip=es515pfuwaihdff3mzwbdg==.

[96] 刘贤刚,孙彦,胡影,赵梓桐.数据安全国际标准研究[J].信息安全与通信保密,2018(12):33-49.

[97] 龚奇敏. 国际数据加密标准化工作现状[J].通信保密,1985(Z1):46-49.

[98] 中国电子技术标准化研究院、清华大学、四川大学、阿里云计算有限公司等，大数据安全标准化白皮书，2018.

[99] GB / T 35274-2017 信息安全技术 大数据服务安全能力要求

[100] GB/T 37932-2019 信息安全技术 数据交易服务安全要求

[101] GB / T 37973-2019 信息安全技术 大数据安全管理指南

[102] GB/T 35273-2020 信息安全技术 个人信息安全规范

[103] 徐羽佳,胡影,上官晓丽.我国数据安全标准化情况综述[J].中国信息安全,2019(12):56-59.

[104] 谢宗晓,董坤祥,甄杰.金融数据安全相关行业标准介绍[J].中国质量与标准导报,2021(06):9-11.

[105] 焦迪.详解政务信息共享数据安全国家标准[J].信息安全与通信保密,2021(06):11-15.