中国电信后量子隐私计算
白皮书

The White Paper on

Post-Quantum Privacy-Preserving Computation

of China Telecom

中国电信集团有限公司

2023 年 11 月

编写委员会

❖ **编写单位**（排名不分先后）：

天翼电子商务有限公司

天翼安全科技有限公司

中电信量子信息科技集团有限公司

中国电信科技创新部

中国电信网络和信息安全管理部

中国电信全渠道运营中心

中国电信研究院

中国电信数据发展中心

中国电信股份有限公司海南分公司

中国电信股份有限公司天津分公司

中国电信股份有限公司江苏分公司

中国电信股份有限公司上海分公司

中国电信股份有限公司河北分公司

中国电信股份有限公司广东分公司

中国电信股份有限公司重庆分公司

中国电信股份有限公司四川分公司

中国电信股份有限公司西安分公司

中电万维信息技术有限责任公司

上海交通大学网络空间安全学院

浙江大学网络空间安全学院

南京邮电大学信息智能与安全研究所

杭州趣链科技有限公司

杭州高新区（滨江）区块链与数据安全研究院

本源量子计算科技（合肥）股份有限公司

❖ **参与编写人员**（排名不分先后）：

李真、贺伟、徐潜、沈华杰、喻博、章庆、刘长波、张鑫、曹亮、于鹏超、方宇、罗俊、王波、陈国鑫、魏丫丫、仲籽彦、薛伟佳、王靖然、李锋、李娟、陈文思、白凡、李超凡、邓宗元、周一峰、陆晔、肖晴、王强、丁涛、韩家驷、刘鹰、向剑虹、秦国强、肖勇、张修权、杨小凡、李玮、齐文辉、王坤、张帆、范磊、董振江、董建阔、张帅、张珂杰、窦猛汉、李叶

前言

数据安全是国家安全、社会安全和经济安全的关键支柱，是数据要素市场健康发展的重要保障。2022 年 1 月，国务院办公厅印发《要素市场化配置综合改革试点总体方案》，提出探索“原始数据不出域、数据可用不可见”的数据交易新范式；2022 年 12 月，中共中央、国务院公布《关于构建数据基础制度更好发挥数据要素作用的意见》指出，要在保护个人隐私、商业秘密、维护国家数据安全的前提下，充分实现数据要素价值释放。由此可见，打破数据孤岛，实现数据资源的跨领域、跨组织域、跨区域的安全合规高质量汇聚利用，是推进数据要素市场化的重要基础。

隐私计算是一种数据流通技术，它可以在保证数据隐私安全的前提下实现数据的有效融通，以“可用不可见”的方式最大化释放数据价值。随着我国《网络安全法》、《数据安全法》和《个人信息保护法》相继出台，数据合规监管日益趋严，隐私计算已成为数据要素市场化进程中的关键技术之一，在各领域数据流通场景中发挥愈加重要的作用。为实现“原始数据不出域、数据不动价值流通”，以安全多方计算（Multi-Party Computation， MPC）、联邦学习（Federated Learning， FL）等为核心的隐私计算技术大量使用密码学原语进行协议的构建。然而，随着量子计算机的出现和发展，密码算法尤其是现有主流公钥密码体制的安全性受到极大的挑战，包括 Diffie-Hellman（DH）、RSA、椭圆曲线 ECC 等在内的一系列经典算法因其所基于的数论难题在量子计算时代变得不再“困难”而面临着较大的安全风险，这也进一步导致上层隐私计算协议的安全性问题日益凸显。如何保证隐私计算算法协议在量子计算时代的长效安全性，已成为隐私计算基础设施化以及数据要素市场化发展所必须考虑的关键问题。

当前全球公开渠道所公布的量子计算机制造仍未达到可用状态（大规模且容错：Large-scale and fault tolerant，即对于算法执行所需足够多的有效逻辑量子比特），对传统密码算法的安全威胁也更多的存在于理论上，但企业在量子计算机的研发进度上已出现加速态势。另一方面，诸如“现存后解”（Store Now and Decrypt Later，SNDL）攻击以及美国国家标准与技术研究所（National Institute of Standards and Technology，NIST）在后量子密码（Post-Quantum Cryptography，PQC）标准化方面的推进工作证明，实现后量子密码安全是一项长期且迫切的任务，我国应未雨绸缪，尽早布局并加快相关技术储备，以迎接即将到来的信息安全体制大变局。目前，为应对量子计算给密码算法以及数据安全带来的挑战，技术层面通

常依托后量子密码迁移,即将所采用的基于传统数论难题的公钥密码算法替换为可抵御量子计算攻击的新型密码算法，使其既能在传统的计算机上高效地运行，又能在有效时间内具备后量子安全能力。如今，国际社会对于后量子密码技术研究已广泛开展，但基于后量子密码的隐私计算理论研究与工程实践工作仍属于空白，亟待补充与加强。

本白皮书以中国电信在后量子隐私计算领域的初步实践探索为基础,介绍中国电信关于后量子隐私计算以及后量子密码迁移方面的重要思考、布局规划与实践成果经验，以期提升我国产业界对于后量子密码安全的关注度，为量子计算时代我国密码与隐私计算技术的发展、国家信息关基安全保障提出有益建议。

版权声明

目录

1 量子计算的威胁

量子计算是下一代计算体系的重要领域，也是当今全球科技界关注的热点。尽管量子计算发展仍处于起步阶段，技术成熟度有待提高，但其在特定计算问题上远超经典算法的强大计算能力，如在密码破译、气象预测、金融数据分析、材料制备等领域广阔的应用前景吸引了世界主要科技大国积极投入到“量子计算”发展的赛道。

量子计算机的突破使得量子计算算法的应用具备可行性，并可以以此解决特定的复杂数学问题。当前发展成熟且应用广泛的现代公钥密码体制其安全性大多建立在复杂数学难题基础之上，到目前为止，经典计算机尚无法解决这类困难问题，但量子计算机独特的并行计算能力结合基于量子叠加的计算算法对常规公钥算法底层的数学困难问题破解带来了可能，这也是现代安全体系的重大威胁与挑战。在量子信息时代来临之际，研究并建立能够抵御量子计算攻击的新型密码体制对于保障国家网络安全与信息安全至关重要。

1.1 量子计算机的发展

2022 年 10 月，法国物理学家阿兰•阿斯佩（Alain Aspect）、美国理论与实验物理学家约翰•弗朗西斯•克劳泽（John F. Clauser）以及奥地利科学家安东•塞林格（Anton Zeilinger）共同获得了诺贝尔物理学奖，以褒奖三位物理学家先后用实验方式证实了爱因斯坦所描述的纠缠态粒子间“鬼魅般的超距作用（Spooky action at a distance）”，这也为当代量子计算体系的持续发展奠定了坚实的理论基础。针对量子计算技术的发展路线，2013 年米歇尔•德沃雷提出了七阶段发展模型[1]：1）单物理量子比特操控；2）基于多个量子物理比特实现量子算法；3）量子纠错和控制所需的量子非破坏测量；4）实现逻辑量子比特；5）单个逻辑量子比特操控；6）基于多个逻辑量子比特实现量子算法；7）容错量子计算。2018 年，美国科学院在其发布的白皮书《量子计算：进展与展望》中，进一步对量子计算的发展作了评估，并给出详细的量子计算发展路线图（如图 1.1 所示），目前量子计算的发展基本遵循该路线。

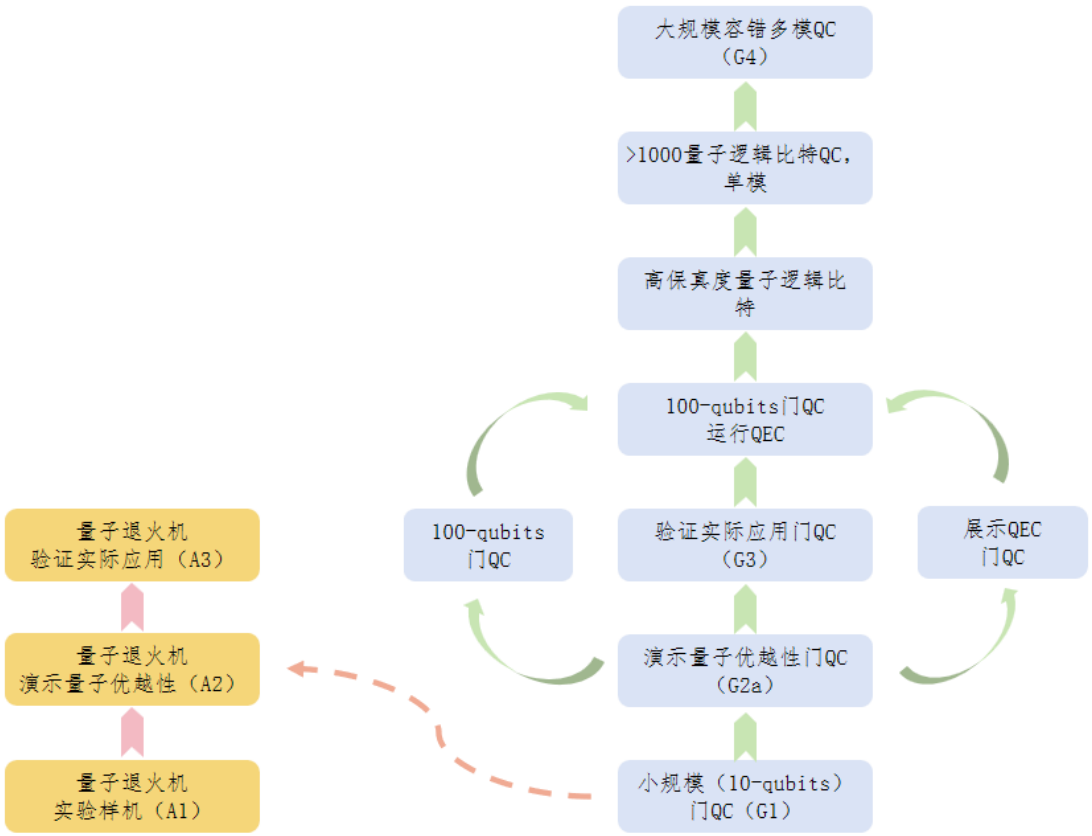

图 1.1 量子计算发展路线图

随着量子计算、量子通信、量子密码等的不断发展，量子技术近年来走上了大众视野，并快速走向成熟。作为量子领域最关键的技术之一，量子计算机具备运行速度快，解决特定问题处理能力强等优势，因而受到了各国政府以及国内外众多研究机构的关注，发展尤为迅猛。量子计算机可以看作是量子力学与计算机技术相结合的重要成果。早在 2001 年，IBM 公司就首次成功地建造了一个可操控 7 量子比特的实验性量子计算机。2007 年，我国科学家潘建伟的团队在量子计算机上实现了 Shor 量子分解算法[2]。随后在 2010 年，潘建伟团队与清华大学的联合小组通过量子隐形传态技术实现了世界最远距离的量子传输。根据 IBM 公司发布的量子处理器开发路线图（图 1.2），该公司计划在 2024 年发布 Flamingo 处理器，该处理器将能够整合量子通信链接，将三个 Flamingo 处理器组合成总计 1386 个量子位的量子系统，并计划在 2025 年通过多处理器模块化组合实现 4158 量子比特的处理器 Kookaburra。可以说，量子计算机已经由曾经虚幻的物理问题发展成当前一项具有重大现实意义的复杂工程问题。

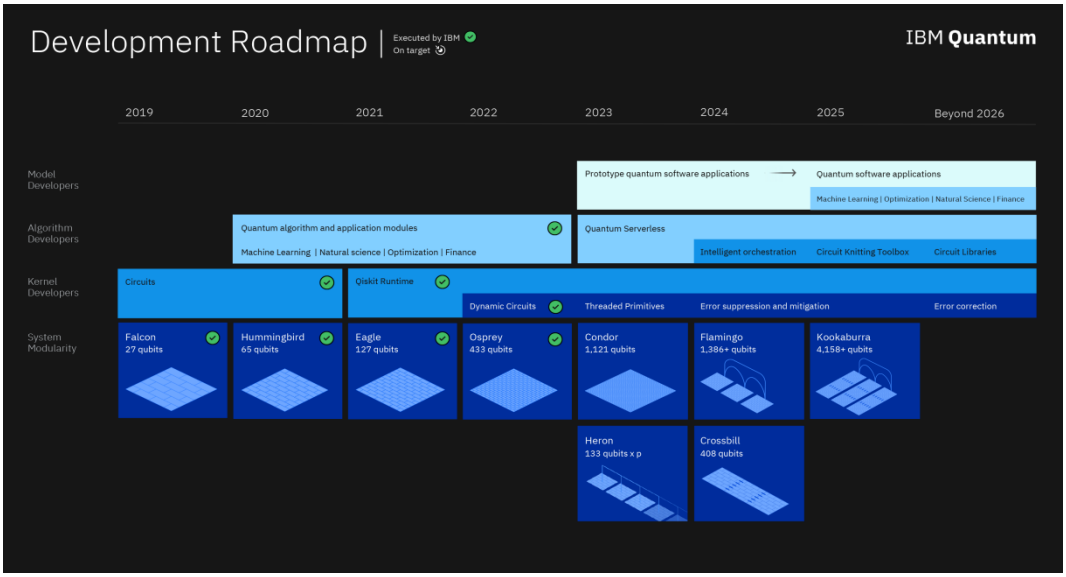

图 1.2 IBM 量子处理器开发路线[3]

1.2 量子计算时代的密码安全威胁

量子计算机的持续发展为人类社会未来算力的大幅提升带来可能性，但同时也对现有网络安全体系造成现实威胁。当前大多数（公钥）密码算法，如 Diffie-Hellman（DH）、RSA、ECC 等，其安全性所依赖的离散对数 Discrete Logarithm 和大整数分解 Integer Factorization 等传统数论难题将不再“困难”。早在 1994 年，美国 MIT 数学家 Peter W.Shor 提出了一种量子算法[2]，能够解决离散对数和大整数分解问题。理论上，破解经典 RSA-2048 算法仅需一台拥有 4098+个逻辑量子比特的计算机即可快速完成，但由于量子比特的噪声敏感性，现实环境需大量额外纠错物理量子比特以实现有效的逻辑量子比特。随着量子容错技术的不断进步以及 Shor 算法的突破性优化[27]，破解所需的海量量子比特数正逐步降低。

量子计算机及其所承载的量子计算算法给现代密码体系带来的威胁不是一个即时问题，而是一个持久挑战。攻击者完全可以由公开信道提前获取并大量存储由经典密码系统所保护的数据密文，以待量子计算时代，出现足够强大的量子计算机出现后再进行破解，即“现存后解”SNDL 攻击方法。在 2022 年 5 月《自然》杂志发表的《Transitioning organizations to post-quantum cryptography》[4]中，详细论述了 SNDL 攻击以及后量子密码迁移时间线（如图 1.3 所示）。概括来说，SNDL 攻击是将现在还无法破解的信息存储起来，等到日后时机成熟再进行破译。量子计算机的快速成熟加速了这一关键转折时间点的到来（即所称的 Q-Day），同步也对密码协议的前向安全性以及数据长期保密性造成了致命隐患。由于当前广泛使用的

互联网安全协议和密码系统大多基于 DH、RSA、ECC 等经典算法进行设计和构造，当这些底层算法在量子计算面前不再安全时，上层用来保护敏感数据（特别是金融、通信、政务、医疗、能源、国防等数据）的协议和系统也就存在被攻破的风险。这也是开展后量子密码理论研究与工程应用的迫切性与必要性。

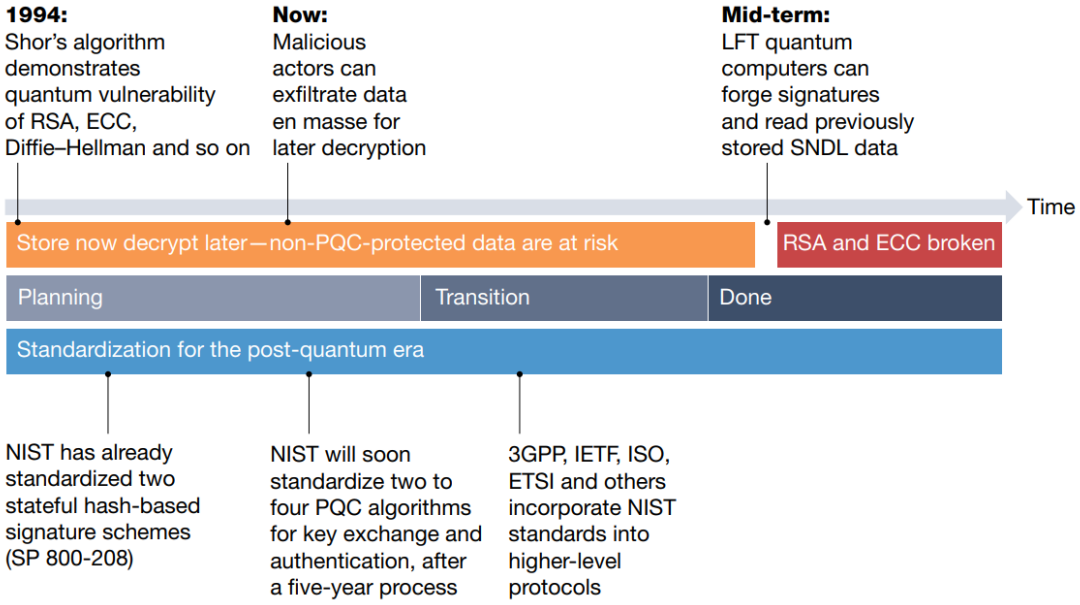

图 1.3 后量子密码迁移时间线[4]

现代密码体制分为公钥密码和对称密码两大部分，公钥密码算法（如 RSA 和国密 SM2）依赖于数学困难问题，在量子计算面前无法保证困难性，因此无法抵抗量子攻击。相比之下，对称密码仍然能够提供足够的后量子安全性。以著名的量子搜索 Grover 算法为例，因其可以实现对经典搜索效率的二次加速从而提高密码破译效率，被认为会对对称密码以及杂凑算法的安全性造成潜在威胁。对于理想的对称密码方案，基于 Grover 算法的量子穷举密钥攻击将使算法安全强度从 $O(2^n)$次经典计算变为 $O(2^{n/2})$次量子计算（攻击中运行 Grover 迭代的轮数）。尽管理论上对称或杂凑算法的安全强度可受量子攻击的显著影响，但由于 Grover 算法在搜索密钥时需要长时间运行的串行计算过程，即使在未来量子计算时代，这种攻击依然较难有效实现。在 NIST 正在进行的后量子标准化工作中，考虑拆分搜索空间来实现攻击中计算的并行化，但会显著增加量子比特和电路门数目。因此，后量子密码研究更多的关注于公钥密码领域。但对称密码的后量子安全性分析以及相关后量子对称密码算法设计依然是密码学的一个重要分支，也会为未来的后量子公钥算法研究提供基础。

1.3 后量子密码的行业进展

目前，学术界和工业界围绕 PQC 后量子密码算法的研究已持续多年，并提出了大量抗量子计算攻击新路径，按照不同的困难问题，一般可将主流后量子密码算法分为以下几类：

1）基于哈希（Hash based）的密码系统，其中，由 Merkle 设计的基于 Hash-Tree 的公钥签名方案[5]如 XMSS 是此类密码的典型方案。这一类方案的优势在于安全性可靠，安全哈希函数可以理解为任意布尔电路，其安全性可以归约到 NP 完全问题。其劣势在于，由于哈希过程的信息损失，只能用于构造签名方案，且签名体积往往较大，性能表现较低。

2）基于编码（Code based）的密码系统，例如 McEliece 公钥加密方案[6]；这类方案的安全性依赖于对应解码问题的困难性，部分解码问题可以归约到 NP 完全问题，也是一类安全性较好但性能表现较低的方案。

3）格基（Lattice based）密码是基于一种被称为“格空间”的数学结构上的困难问题构造的密码算法，这种结构在密码学和计算机科学中具有重要的应用，目前吸引了越来越多的关注。早期典型代表是著名的 NTRU 方案[7]，最新的方案有 Kyber、FrodoKEM 等，其中，Kyber 拥有较好的性能表现，FrodoKEM 则有更可靠的安全性。这类方案最大的优势在于可以选择恰当的格结构以达到安全性和性能的平衡兼顾。

4）多变量（Multivariate based）公钥密码，如 1999 年提出的 UOV（Unbalanced Oil and Vinegar）签名方案，这类方案的安全性所依赖的数学困难问题较为特殊，与哈希、格、编码问题相比得到的研究相当有限，因而没有成为各国政府和机构推荐的主流方案。

5）基于超奇异同源（Supersingular Isogeny based）的算法，提供基于特殊椭圆曲线代数结构上的后量子密钥交换算法；这类方案的安全性也有待更广泛地研究，目前也不能归约到 NP 完全问题。

6）其他密码算法和协议，如基于 MPC-in-the-head 的数字签名算法[24]、后量子安全的零知识证明协议（zk-STARK）、分组加密标准 AES 等。此外，信息理论安全的密码协议本身也是后量子安全的，比如基于秘密分享的 MPC 协议，一次一密等。

目前，对 PQC 算法本身的研究以及标准化工作的已有较多的成果。现有的信息系统为保证量子安全性，势必推动经典公钥算法向 PQC 算法的替换，该过程即后量子密码迁移（Post-Quantum Cryptography Migration，PQC Migration）。对后量子迁移的理论与工程研究

工作已在美国、欧盟成员国等科研机构与企业广泛开展，并成为基础安全领域的重要发展方向。由于密码和信息系统的理论与工程复杂性、标准规范与实践指南的缺失，以及迁移过程可能带来的系统性业务风险与成本增加，这一过程仍存在诸多挑战。美国国家标准与技术研究院 NIST 已启动对 PQC 算法迁移的研究项目以及迁移报告[8]，讨论识别 PQC 算法迁移对象的方法。欧洲电信标准化委员会 ETSI 也发布了 PQC 算法迁移报告[9]，并将迁移过程分为密码算法识别、迁移准备和执行等阶段。丁津泰教授团队[10]也详细探讨了 PQC 算法迁移过程中涉及的方法论和策略，并从安全性、可用性、敏捷性、普适性四个方面给出迁移原则和目标。

总之，后量子密码 PQC 的迁移是一项需要长期推进的工程，需尽早布局并尽可能提前完成易被量子计算攻击的传统密码体制向后量子版本的迁移工作，这将保证个人、企业以至国家核心数据在量子计算时代的持续安全。

1.3.1 国际

美国 NIST 于 2009 年发布了后量子密码算法综述，并于 2012 年正式启动了后量子密码算法标准项目，2016 年发布后量子密码算法征集公告，相关评估工作分为 3 轮进行，每轮 18 个月左右，预计 2024 年之前完成。初期征集共收到 82 种算法，经过长时间的评估以及同行之间的算法攻击测试，很多算法被发现存在安全漏洞。在 2022 年 7 月，NIST 公布了 4 项杀出重围并将完成标准化的算法提案，其中包括密钥封装算法 CRYSTALS-Kyber 以及三项数字签名算法 CRYSTALS-Dilithium、Falcon 和 SPHINCS+。同时，NIST 公布了四个第四轮候选的密钥封装算法：BIKE，McEliece，HQC 和 SIKE 算法（如图 1.4）。然而在 2022 年 7 月，比利时鲁汶大学团队公布的论文[11]中指出，当遇到特定类型的攻击时，SIKE 算法的 SIDH 安全假设可能会被破解。

NIST 2022标准算法

方案名称	方案结构	方案类型
CRYSTALS-Kyber	格密码	密钥协商/公钥加密
CRYSTALS-Dilithium	格密码	数字签名
Falcon	格密码	数字签名
SPHINCS+	基于哈希	数字签名

第四轮候选算法

方案名称	方案结构	方案类型
BIKE	基于编码	密钥协商/公钥加密
Classic McEliece	基于编码	数字签名
HQC	基于编码	数字签名
~~SIKE~~	同源椭圆曲线	数字签名

图 1.4 NIST 标准算法与候选算法

2022 年 2 月，美国政府公布《关键和新兴技术清单》，将后量子密码这一量子信息技

术列入了国家安全的考虑范围。2022 年 5 月，《自然》杂志发布的《Transitioning organizations to post-quantum cryptography》[4]指出，由于 SNDL 攻击的存在，向后量子密码迁移是一件现在就要开始做的事情。美国互联网工程任务组（IETF）也在制定改进的传输层（TLS）协议，以适配后量子密码算法。2022 年 10 月，美国现任总统拜登签署了《量子计算网络安全防范法案》。2022 年 11 月，白宫管理和预算办公室（OMB）发布了一份报告，督促联邦政府机构开始着手后量子密码迁移，并要求各联邦政府机构直到 2035 年之前，每年在 5 月 4 日前上传一份其系统中未进行后量子迁移的软硬件列表。著名咨询公司 Gartner 预计，在 2023 年将有 20%的组织开始筹备后量子密码迁移工作。欧盟通过资助 PQCRYPTO、SAFEcrypto 等研究项目来加快后量子密码的研究和应用。其中，SAFEcrypto 项目重点关注后量子安全的安全多方计算和全同态加密技术的研究。在标准化方面，ETSI 设有一个专门的后量子密码工作组，参与到国际后量子密码标准的制定中。IEEE、ISO、ITU-T、IETF 与 3GPP 等组织都先后发布了后量子密码相关草案及标准。韩国于 2022 年启动 KPQC 竞赛[12]，征集韩国本土的标准化后量子密码。目前已经收集到 16 个后量子的密钥协商和数字签名算法，其中，SOLMAE 签名算法计划启动标准化进程。德国联邦信息安全办公室（BSI）对后量子密码迁移给出了详细的技术指导文档[13]。在该文档中，官方特别推荐基于 LWE 问题的 FrodoKEM 以及基于编码的 Classic McEliece 方案，并建议将这些方案与经典公钥密码系统结合使用。

1.3.2 国内

在国际保守主义抬头，逆全球化趋势日盛的今天，为降低依赖外国技术所带来的风险，我国加快推进后量子密码领域的标准化工作，构建自主可控技术体系的迫切性已日益凸显。

中国密码学会在 2018 年启动了密码算法竞赛，征集了一系列后量子密码算法。其中，获奖算法 Aigis 算法分别基于模格上给对称学习问题个理想格问题提出加密算法 Aigis-enc 和签名算法 Aigis-sig，此外，获奖算法 LAC 算法成功进入 NIST 第二轮后量子密码候选算法名单；此外，很多的中国学者也参与进 NIST 标准算法的制定以及改进中。例如，丁津泰教授团队提出的 Rainbow 算法成功入选第三轮的 NIST 决赛算法，此外，他们也在新一轮的 NIST 签名算法征集中提交了 TUOV 算法。国内学者如郁昱教授团队也对 SPHINCS+、Dilithium 等算法进行了改进，在签名大小和签名时间方面相比 NIST 的标准算法有了 10%左右的提升。路献辉教授团队也一直在性能、安全性和工程实现角度对于格密码与基于哈希的密码进行优化。另外，在密码分析方面，来自中国的研究团队也分别发现了 NIST 候选算法中的 DRS、HK17、Compact-LWE 方案在特定攻击下不安全。

除此之外，中国密码学会也多次举办量子密码学术年会，探讨 PQC 以及 QKD 的研究进展。另外，雁栖湖国际后量子密码标准化与应用研讨会，专注于各国标准化现状以及最新研究进展。总体情况表明基于格的后量子密码由于其安全、平衡与灵活性，目前是 PQC 领域内最为活跃的路线，国内围绕格基密码的研究团队也较多。

尽管学术界在积极研究和探索后量子密码技术，我国企业对于后量子密码标准化与工程化方面的工作仍显滞后。当前产业界对后量子安全缺乏重视，仅有少数企业开始尝试从软件协议层面进行小范围的 PQC 预研，或者从硬件芯片层面提高后量子密码的运行效率。此外，部分初创公司开始关注后量子的区块链技术以保障量子计算时代链上数据的安全，如推动实现多重签名、环签名、门限签名、零知识证明等技术的抗量子攻击能力与区块链安全的融合。

在标准化方面，学术界对于国内是否需要有自己的 PQC 标准尚有争议，部分学者认为应该遵循国际公开标准，也有学者认为应该构建我国自有的算法和标准，从信任和国产自主可控的角度来确保后量子密码安全。总体上，国内的后量子密码标准化已在推进中，例如，全国信息安全标准化技术委员会（简称“信安标委”）2023 年第一次“标准周”活动期间开展了“后量子密码技术与创新实践研讨会”，这对未来后量子密码相关标准的设立及实施发挥了积极的促进作用。

2 隐私计算发展现状

如何兼顾数据流通与数据安全，在保障数据隐私安全的前提下实现数据的有效融通与价值释放已成为数据要素市场化要解决的重点问题。以安全多方计算、联邦学习等为核心的隐私计算技术遵循“数据可用不可见、数据不动模型动”原则，利用密码学、可信硬件实现敏感数据不出库的交互计算目的，保证参与方无法通过中间信息直接获得或推理出原始数据，进而在促进数据价值释放时保护数据隐私安全。

2.1 隐私计算概述

隐私计算[22]指在保护数据本身不对外泄露的前提下实现数据分析计算的一类信息技术，包含数据科学、密码学、人工智能等众多技术体系的交叉融合。隐私计算的底层技术覆盖密码学、分布式机器学习、可信硬件等多种技术，目前常见的技术路线主要包括安全多方计算MPC、联邦学习 FL、可信硬件等。其中，安全多方计算和联邦学习主要依赖丰富的密码学原语来构建计算或建模协议，以解决参与方间数据的隐私保护问题；可信硬件主要依靠硬件处理器安全域来解决多源数据的可信计算问题；隐私计算一体机则通过软硬件结合方式提供数据隐私安全防护、硬件加速等一系列解决方案。

安全多方计算的概念最早在上世纪 70 年代被提出，是密码学界重点研究方向之一，主要解决互不信任的实体之间协作完成计算任务的难题。安全多方计算包括通用和特定用途的协议，如隐私求交、隐私查询、零知识证明等。实现安全多方计算的核心技术主要包括秘密分享、不经意传输、混淆电路、全/半同态加密等，常用的底层密码算法涵盖 RSA、ECC、SHA3、Paillier，ElGamal 等国际密码算法以及 SM2、SM3、SM4 等国密算法。

联邦学习是一种特殊的分布式机器学习算法架构，其核心思想是在多数据源间完成分布式模型训练，不需要直接交换各自原始数据的前提下仅依赖中间参数构建全局模型，实现数据隐私安全和数据共享的平衡。根据数据的重叠程度，联邦学习可以分为横向、纵向和联邦迁移学习三种范式，常用的联邦学习算法包括树模型、回归模型、神经网络等。现阶段联邦学习算法协议多采用差分隐私、同态加密、秘密分享等方式保护中间参数和原始数据的安全。

可信硬件特指独立于不可信操作系统而存在的可信、隔离的独立代码执行环境，为不可信环境中的隐私数据和敏感计算提供一个安全而机密的计算空间。其安全性通常通过硬件安全域机制来保障。可信硬件主流技术路线包括 ARM TrustZone、Intel SGX 和 AMD SEV 等。

隐私计算一体机是融合计算、网络、存储等硬件资源，将软硬件技术融于一体，兼顾隐私计算安全性和计算性能，同时具备开箱即用、快速组网、稳定可靠、硬件加速等优势。目前国内主流隐私计算一体机架构体系需具备必要的硬件设备、算法支持能力、场景应用落地能力等，同时设备成本高，升级迭代能力较弱也是其主要问题。

2.2 隐私计算的应用

随着数字中国战略的部署与实施，数据要素已成为我国未来数字经济与实体经济发展的主要推动力。党和政府高度重视数据安全流通的发展应用，不断健全数据领域相关法律法规，已初步形成数据基础制度的“四梁八柱”。2021 年 5 月，《全国一体化大数据中心协同创新体系算力枢纽实施方案》明确提出，试验安全多方计算、区块链、隐私计算等技术模式，构建数据可信流通环境，提高数据流通效率；2022 年 10 月，《全国一体化政务大数据体系建设指南》提出探索利用模型分析、隐私计算等多种手段，有效支撑地方数据资源开发利用。隐私计算作为保障数据安全流通的有效手段，已经成为促进数据要素跨区域可信合规流通的关键技术，未来将在更多场景得到广泛应用，促进数据要素行业生态的发展。隐私计算的行业应用图谱如图 2.1 所示。

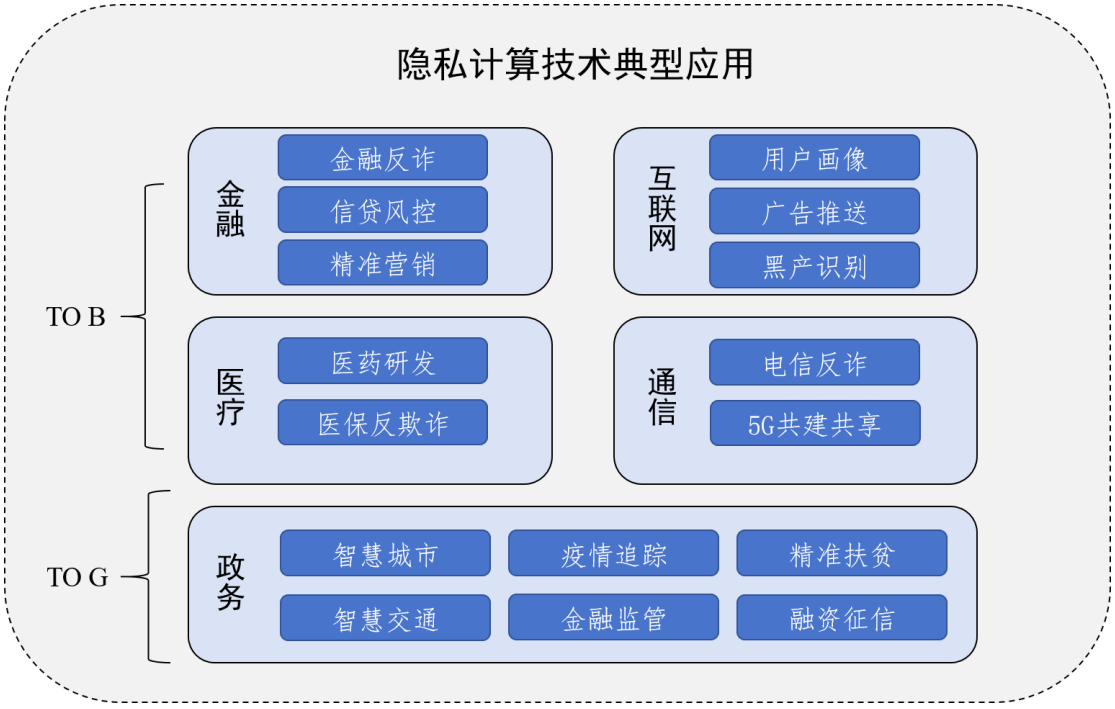

图 2.1 隐私计算技术在行业的主要应用领域

隐私计算的发展离不开市场的实践检验，不仅要确保数据的安全性，更重要的是在兼顾安全性的前提下，为业务和社会中各种场景进行赋能，真正发挥其应有的作用。在金融领域，隐私计算蓬勃发展，特别是在营销及风控应用中，其业务出发点是通过将金融机构内部的数据字段与外部的其他数据字段进行虚拟融合，进而达成多方之间的联合建模、联合统计、联合查询等任务；在医疗卫生领域，隐私计算的应用潜力巨大，例如医疗诊断、医药研发、医保反欺诈等；在政务领域，可联合多个委办局联合分析区域经济，助力解决民生问题；在互联网领域，可利用隐私计算实现更加精准的获客与广告推送。此外，隐私计算也可服务于跨领域跨行业的数据流通，如公共数据赋能银行业实现普惠金融，银行业数据也同时赋能政府部门实现定向扶持。

3 量子计算：对隐私计算的挑战与启示

3.1 挑战：量子计算带来的威胁

安全多方计算和联邦学习作为隐私计算的两条重要实现路径，其协议的安全性主要取决于底层密码算法的安全性。以广泛应用的隐私集合求交（Private Set Intersection，PSI）和联邦学习 XGBoost 算法为例，当前的 PSI 协议多采用基于 RSA 或 ECC 等公钥密码算法，或融合不经意传输（Oblivious Transfer，OT）及不经意伪随机函数（Oblivious Pseudo-Random Function，OPRF），并辅以对称密码算法进行构造。然而，RSA 和 ECC 等公钥密码算法无法满足后量子安全性，已成为后量子时代潜在的安全隐患。

另一方面，对于 XGBoost 来说，目前业界大多利用半同态 Paillier 算法加密梯度来保证中间传参的隐私性，而 Paillier 底层仍基于大整数分解困难问题，导致其无法抵御未来量子计算机的攻击。

此外，在可信硬件和密码芯片中，除了诸如证书验证、密钥协商、数字签名等协议因包括公钥密码算法而受到量子计算威胁外，传统密码硬件还提供硬件优化的加密算法指令集，如 AES 的 S 盒操作，大整数的模幂运算等。然而，此类硬件优化指令集并不能直接适用于后量子密码，需要在硬件指令集上进行额外调整来适配新的操作，比如数论变换（Number Theoretic Transform，NTT）及多变量的运算等。总之，通过后量子密码算法建立满足后量子安全的隐私计算协议，并构建适合于后量子密码的密码芯片或可信硬件，对于保障未来量子计算时代隐私计算技术安全性与可靠性具有十分重要的意义。

后量子密码迁移是保障量子计算时代密码长效安全的有效方法之一，同时也适用于隐私计算技术。以隐私集合求交和 XGBoost 算法为例，可以将普遍采用的公钥密码算法进行后量子密码算法替换，以提升整个协议的抗量子攻击能力。例如，可以将 PSI 的 OT 部分与联邦 XGBoost 中的 Paillier 算法用基于格的全同态加密来替代。当然，实现后量子安全的隐私计算并不仅是简单的算子替换，还涉及整个协议在量子攻击下的可证明安全性分析、相应算法与协议的后量子安全强度及资源消耗量化评估等问题，因而如前所述，后量子密码研究与工程迁移将是一项复杂且持续性任务。

隐私计算作为一项新兴技术，一方面其本身的安全性对于数据要素市场化、国家数据安全的保障具有重要意义；另一方面，相比于其他的传统信息系统，隐私计算系统本身刚起步，迭代空间较大，应用范围也还在逐步扩大，后量子密码迁移对其业务影响相对较小，成本较

低，且从业者的认知程度较高，是较为合适的后量子密码迁移实践场景。当前隐私计算相当一部分算法可以由后量子密码进行高效地实现，未来存在后量子隐私计算形成行业标准的可能。

因此，开展后量子隐私计算的研究，对于我国后量子密码领域的相关技术储备、人才储备与标准化都具有十分重要的示范意义。

3.2 启示：后量子隐私计算

后量子隐私计算：一类由经典计算机执行的隐私计算算法协议簇，可以抵御来自具有量子计算能力的其他参与方或窃听者的密码分析攻击；在量子计算的攻击下，仍能保证参与方私有数据的安全性和隐私性。

构建后量子隐私计算的整体目标是设计并采用既能抵抗量子攻击，又能支持多方协同计算的加密方案和计算协议，保障数据在传输过程以及计算过程中的后量子安全性，实现数据的最小暴露和最大利用。有效构建后量子隐私计算能力，可遵循以下步骤：首先，使用高效、可靠、安全的后量子密码及数据签名算法，替代或结合现有的基于数论难题的传统密码算法，以确保数据在计算和传输过程中的安全；其次，使用适用于量子计算环境的隐私增强技术，如差分隐私、全同态加密、后量子安全多方计算、后量子联邦学习等，以在量子计算环境下实现数据的“可用不可见”；最后，构建基于后量子密码算法和隐私增强技术的后量子隐私计算框架和平台，为各类应用场景提供可信赖的数据服务。

隐私计算体系复杂，覆盖面广，其后量子迁移也需要从多个层面进行框架设计（如图3.1），框架包含硬件层、算子层、传输层、计算层和应用层。无需进行迁移的模块用绿色表示，需要进行改造的模块为蓝色。在硬件层面，研发高效的后量子密码芯片、后量子安全的可信硬件；在算子层面，提供经典的对称密码算子、公钥密码算子和后量子密码算子；在传输层面，构建后量子的传输层安全协议（Transport Layer Security，TLS）来保证通信安全，能够防范具有量子计算能力的窃听者读取通信数据；在计算层面，研发各种后量子隐私计算算法和协议，如隐私集合求交、隐匿查询、安全电路运算、联邦学习及零知识证明等；在应用层面，基于底层能力开发后量子安全的数据流通实际应用。这五个层面的协同创新才可确保后量子隐私计算的整体框架基本完整。当前，后量子算法研究、标准

化及应用仍处于发展阶段，仍需要政府主管部门的有效引导以及产学研各界共同努力，该后量子隐私计算框架也会随着相关研究的进一步深入而做相应调整。

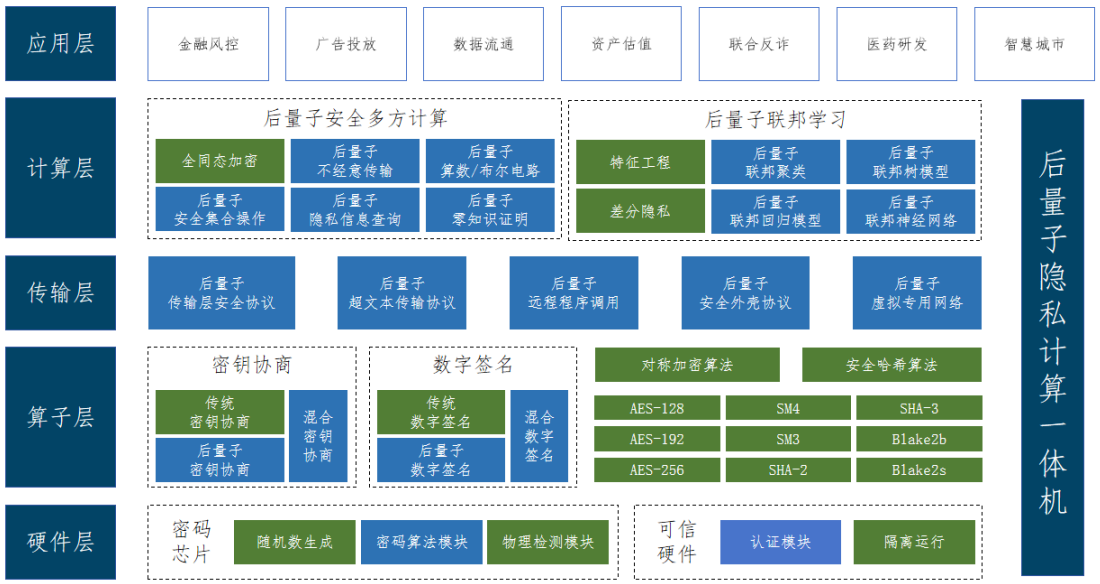

图 3.1 后量子隐私计算建设框架

3.2.1 硬件层

硬件层主要包含两方面，首先是依靠硬件手段实现后量子密码的基础运算操作，其次是使用后量子密码来增强硬件的安全性。为了实现后量子安全的硬件层，需要设计高效的芯片以提供后量子密码中的高速运算以及利用芯片的硬件属性来生成安全的随机数。

密码芯片是一种专门用于加密和解密数据的硬件设备，通过密码芯片实现的算法相比纯软件实现的密码算法具有更高的效率和安全性。后量子密码算法芯片需要包含多类密码学算法（如 CRYSTALS-Kyber、CRYSTALS-Dilithium、FrodoKEM、SHA2、SHA3、SM3、SM4 等）。此外，芯片需支持高效的基础运算操作（如大整数运算、模幂运算、数论变换、矩阵运算等），并提供定制化硬件架构、相关的密钥管理模块和密钥存储模块等基础功能。同时后量子密码芯片还需具备物理安全增强功能，如抗侧信道攻击（Side Channel Attack）和抗篡改攻击（Tampering Attack）等能力，以提升芯片的安全性。

可信硬件是一类基于硬件的芯片级安全技术，这种技术基于芯片内部特殊隔离的安全域，以确保在不受信环境下仍可执行敏感代码。可信硬件需经过深度改造才可满足后量子的安全性。一方面，可信硬件在证书验证、密钥协商、数字签名中使用传统的公钥密码算法，需要将这些算法替换为后量子密码算法；另一方面，可信硬件只支持有限的操作指令，若直接将可信硬件中这些有限的操作应用于后量子密码方案中将极大增加系统整体开销。可信硬件需

要解决的问题是如何通过增加或修改指令集的手段支持高效的后量子密码协议运算。

3.2.2 算子层

算子层提供基础的密码学算子供上层使用，主要包括对称密码算法、哈希算法、公钥（非对称）密码算法中的密钥封装（或密钥协商）和数字签名算法等。算子层的设计旨在提供高效的软件实现及调用接口，使上层应用可以轻松使用这些算法，以保护数据的机密性、完整性或用于构造上层计算协议。

对称密码算法和哈希算法：在后量子隐私计算中，对称密码算法和哈希算法是至关重要的基础密码工具。对称密码算法使用相同的密钥对数据进行加密和解密，由于速度快且密文扩张小（密文扩张表示加密后的数据相对于原始数据所占用的内存大小），常用于对传输的消息进行加密，而哈希算法则将任意长度的消息映射为固定长度的哈希值，常用于验证数据完整性，或作为其他密码学算法与隐私计算协议的基础算子。

目前量子计算整体上对于对称密码原语并无明显的影响。之前有观点认为 Grover 算法可在无序序列中以平方倍的速度搜索出特定数，因此需要在后量子密码中将对称密码的密钥大小翻倍，比如使用 AES-256 代替 AES-128，以保证相同的密钥安全强度。但当前业界对这一观点仍有争议，如果一个量子计算机运行 Shor 算法可以在几个小时内破解 RSA-2048，用同样的量子计算机运算 Grover 算法需要数十亿年才能破解 AES-128，这主要受制于 Grover 算法的高度串行特性，即使具备了量子计算集群，仍无法并行运行 Grover 算法来快速实现 $O(2^{64})$次对称密钥搜索。因而，在未来量子时代，AES 等对称密码原语相对于经典非对称密码原语将具有更长的安全有效期，受到量子计算的影响更小。NIST 已将后量子密码的安全等级设定为与破解相应对称密码的所需的计算资源相等的级别，从 1 级到 5 级分别对应 AES-128、SHA-256、AES-192、SHA-384、AES-256，证明业界对于 AES-128 的后量子安全性非常信任。简单来看，算子层所包含的对称密码是一系列常规国际或国内的对称密码算法，如 AES、SM4 以及哈希算法 SHA-2、SHA-3、SM3、BLAKE2 等。

公钥密码算法：公钥密码算法主要包括密钥协商算法和数字签名算法。这类算法通常基于数论算法构造，很容易受到量子计算攻击影响。因此需要寻找能抵抗量子计算攻击的替代算法，以保障敏感信息的安全。

1）密钥协商算法。密钥协商算法是一种用于在不安全的通信信道上建立共享密钥的方法。密钥协商算法的目的是在两方或多方间生成仅参与方可知的随机密钥，第三方无法猜测或截获该密钥。密钥交换和密钥封装是密钥协商的两种常见实现方式。具体来说，密钥交换

是指在不安全的通信渠道上，两个通信方之间通过一系列的加密和解密步骤来协商共享密钥的过程。该过程确保即使在通信被拦截的情况下，攻击者也不能轻易获取密钥，例如 Diffie-Hellman 和椭圆曲线 Diffie-Hellman 等常用的密钥交换协议。而密钥封装则是将一个密钥通过加密操作封装在一个安全的“信封”中，随后将其发送给接收方；接收方使用解密操作来提取出密钥。该过程可以用于在不安全的通信渠道上安全地传输密钥。密钥封装协议一般基于公钥密码来构造，比如 RSA，ECC 等。

Diffie-Hellman 密钥交换协议的安全性是基于离散对数问题或椭圆曲线的离散对数问题的，因此会被 Shor 算法轻易破解。可采用后量子的密钥封装协议来替代传统的密钥交换协议。目前后量子安全的密钥封装协议包括 Kyber、FrodoKEM 等算法。由于后量子密码算法尚未有国内标准，算子层保留接口给国内算法，未来插入符合未来国家标准的后量子密钥封装算法。

- Kyber 是一种被设计用来抵抗量子计算攻击的密钥封装机制（Key Encapsulation Mechanism，KEM），是 NIST 在 2022 年准备进行标准化的密钥封装算法，由 Regev 的容错学习（Learning With Error，LWE）加密方案演变而来，其安全性基于模块格上的 LWE 问题（Module Learning With Error，Module-LWE）。Module-LWE 问题比环上容错学习问题（Ring Learning With Error，Ring-LWE）问题具有更简单的代数结构，但效率接近 Ring-LWE，满足效率和安全性的均衡。Kyber 已经被工业界集成到库和系统中，被诸如 Cloudflare、Chrome 等公司所使用。
- FrodoKEM 也是一种基于 LWE 的密钥封装机制，不同于 Kyber 为提升效率对参数选择的安全性做妥协，FrodoKEM 的安全性更强。FrodoKEM 的核心是 FrodoPKE 公钥密码方案，满足选择明文攻击下不可区分的安全性。出于对 Frodo 安全性的信任，德国的联邦信息安全办公室 BSI 将 FrodoKEM 算法列为推荐算法[13]。

2）数字签名算法。数字签名算法用于保证消息的完整性和真实性，常见的包括 RSA、DSA、ECDSA 等，然而这些算法都会被 Shor 算法轻易的破解。因此要使用后量子的数字签名算法，如 Dilithium，LMS/HSS 等签名算法对经典数字签名进行替换。

Dilithium 是 NIST 列入 2022 标准计划中的一种基于 MLWE 的后量子数字签名方案，它可以抵抗选择消息攻击。这种安全性指即使敌手有签名算法的访问权限，也不能对他没有看过签名的消息进行签名，或是对他已经看过签名的消息产生不同的签名。Dilithium 基于“Fiat-Shamir with Aborts”技术实现，该技术使用拒绝采样来使基于格的 Fiat-Shamir 方案变得紧

凑和安全。Dilithium 是所有使用均匀采样的基于格的签名方案中公钥+签名尺寸最小的。

LMS/HSS 是 IETF 标准中的基于哈希的数字签名方案，可以抵抗量子计算的攻击。LMS 假设哈希函数的压缩函数是一个随机预言机，其安全性在随机预言模型和量子随机预言模型下已得到证明，但目前只支持 SHA-256 作为哈希函数。从国产化的角度考虑，目前已有论文论证将 LMS/HSS 中哈希函数替换为 SM3 的是可行的[25]。

3）混合密码体系：由于 PQC 算法正处于高速发展期，学术研究活跃，相关算法的安全性没有经过长时间的考验，目前主流的观点是采用后量子与经典密码的混合密码体系。具体来说，混合密钥协商是指密钥协商两方采用经典的 ECDH 生成一个随机数，并采用后量子密钥协商生成另一个随机数，将两个随机数合并放入密钥生成函数，并生成一个会话密钥。混合密钥协商的优势在于即使经典的密钥协商或后量子密钥协商其中一个被敌手破解，最终会话密钥仍然无法被敌手获得。混合的数字签名是指签名方分别采用传统的 ECDSA 签名和后量子签名协议对同一份数据进行签名。验证方需要同时验证两份签名的有效性，只有当两者均有效时，才能证明该消息是由签名方自己签署，而非敌手伪造。混合数字签名的优势在于即使敌手可以伪造经典签名和后量子签名中的一个，整体的签名仍然无法通过验证方的验证。

3.2.3 传输层

传输层负责数据的端到端传输，并使用后量子传输层安全（Transport Layer Security，TLS）协议来确保数据传输过程中的机密性、可靠性、完整性和不可抵赖性。在传输层安全协议的上层，应用 HTTPS 或远程程序调用（Remote Procedure Call，RPC）等协议或框架来具体管理数据在两个节点间传输的方式。

TLS 协议：TLS 协议是当今使用最广泛的安全传输协议，可保护世界各地的 Web 客户端和服务器之间交换的信息。尽管 TLS 协议在现有的经典计算机环境中是安全的，然而，其内部使用的非对称加密技术可能会面临量子计算的攻击。

具体来说，TLS 中的非对称密码在两个地方容易受到攻击（如图 3.2 所示）：

1）密钥交换：如前文所述，传统密钥交换协议中因融入了基于数论的密码算法而不满足后量子安全性。因此在后量子安全的传输层，最终目标之一是采用后量子的密钥封装算法替代诸如椭圆曲线 Diffie-Hellman 等密钥交换协议来进行对称密钥的共享。

2）身份验证：服务器（以及可选的客户端）使用其证书包含的公钥来证明其身份，涉及签名算法如 RSA 或 ECDSA。后量子安全的传输层需要采用后量子的数字签名方案替换

RSA 或 ECDSA 签名。

出于保守的安全策略考虑，初期可以采用混合的密钥协商以及混合签名方法来进行密钥交换和身份验证。后期待算法协议安全性经过深入评估以及国家与行业规范标准化成熟后，可逐步推进后量子密码的全面替换。

基于后量子安全的 TLS 协议，可以构造具体的数据传输规范或框架，并提供后量子的 HTTPS、RPC、FTP、SSH 等服务。

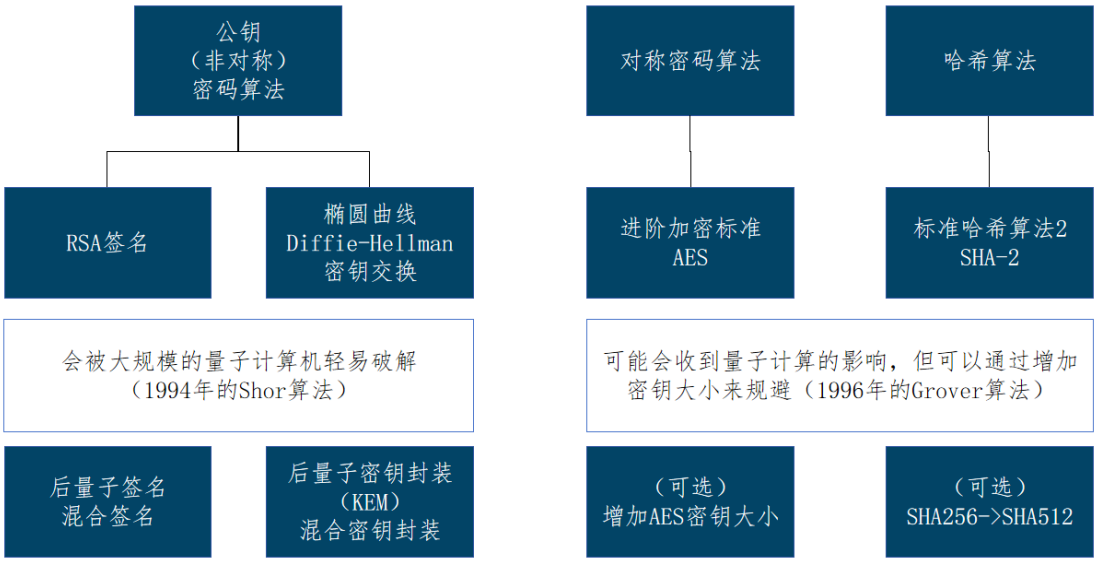

图 3.2 TLS 协议中使用的主要密码算法[29]

3.2.4 计算层

利用后量子密码能力构造后量子的数据安全计算方法，让多个参与方在不暴露本身数据的前提下与其他参与方共同完成某个计算任务并得到计算结果。计算层的协议涉及到多个参与方之间频繁的数据传输，其中数据大多以不可恢复的密文形式存在。后量子安全的计算层的主要目标是提供隐私计算协议的后量子安全版本，在不影响协议功能性的情况下，额外保证其可以抵抗量子计算的攻击。具体来说，计算层包括但不限于以下算法或协议：

1）**同态加密：**半同态加密（Partially Homomorphic Encryption，PHE）只支持乘法或加法中的一种的同态加密。如 Paillier、RSA、ElGamal 等。与 FHE 相比，PHE 的复杂性更低，执行速度更快，因此处理速度更快。半同态密码系统标准化较为成熟，如 Paillier 加密方案已广泛集成到各类数据保护解决方案中。全同态加密（Fully Homomorphic Encryption，FHE）是一种允许在密文上直接进行任意次数的加法和乘法运算的加密技术。全同态加密算法的核心思想是将明文空间和密文空间之间的运算映射为同态的关系，即在明文空间中相同的运

算，在密文空间中也有对应的运算，且解密后计算结果相同（或近似）。FHE 可以在不泄露任何关于明文或密钥的信息的前提下保证计算结果的正确性。FHE 的主要挑战是效率问题，为支持无限次数的运算，目前已知的全同态加密方案都需要很高的计算复杂度和存储空间，还存在着噪音增长和密钥管理等问题。但如果只在密文上进行有限次数的运算，现有的（Leveled）FHE 可以提供较好的计算效能，因此 FHE 可以被用于构造一些特定的安全计算协议。此外，FHE 的安全性基于 LWE 或 RLWE 困难问题，参数的选取需谨慎。一般来讲，特定参数的 FHE 方案所提供的安全性要比 NIST 标准提供的基于 LWE 的算法要强。因此，FHE 是一个构造后量子安全计算协议的优质工具。

2）不经意传输：不经意传输（Oblivious Transfer，OT）是一种基础密码学原语，它允许发送方向接收方传输一些信息，接收方获取其中一部分信息而无法得到任何其他信息。OT 有多种变体，例如 2 选 1-OT、n 选 1-OT、相关 OT、随机 OT、OT 拓展等。向量不经意线性关系（Vector Oblivious Linear Equation，VOLE）允许两个参与方在不泄露任何私密输入的情况下得到一对具有线性关系的向量。OT 和 VOLE 可以用于实现多种安全的多方计算协议，如隐私求交 PSI 或通用安全多方计算。后量子 OT 和 VOLE 都可以基于后量子安全假设如 LWE 或偏差学习问题（Learning Parity with Noise，LPN）来构造。通过实现后量子 OT 和 VOLE 原语，可以为其他后量子安全计算算法提供基础算子。

3）通用安全多方计算 MPC 协议：安全多方计算 MPC 协议是一种允许多个参与者在不泄露各自私密数据的情况下，共同计算一个函数结果的技术。安全多方计算的目标是保证参与者的数据隐私和计算正确性，即使有部分参与者是恶意的。MPC 可以分为通用的 MPC 协议或特定功能的 MPC 协议，通用的 MPC 协议是解决通用的计算问题，可以通过秘密分享、混淆电路等方式构造算数电路或布尔电路来构造。特定功能的 MPC 协议则包括隐私求交、隐匿查询或零知识证明等特定算法。对于通用的 MPC 协议，一般来说基于秘密分享的构造在加法和乘法运算上是信息论安全的，多方之间可以通过操作本地数据完成加法或使用乘法三元组来计算秘密分片上面的乘法。然而生成乘法三元组的过程或计算特定的非多项式运算比如比大小、激活函数、除法等运算需要使用 OT 或者 Paillier 算法，可能不满足后量子安全性，因此，后量子的通用 MPC 需要针对这方面进行改造。另一方面，混淆电路（Garbled Circuit，GC）的基本思想是将原始的布尔电路转换为一个加密的电路，每个参与者只能看到自己的输入对应的加密值，而不能推断出其他参与者的输入。通过使用 OT 交换加密值和解密表，参与者可以逐层计算出电路的输出，而不暴露中间结果。对于混淆电路的后量子改造

也主要涉及对于 OT 的替换。

4)隐私集合求交和隐匿查询：隐私集合求交 PSI 和隐匿查询（Private Information Retrieval，PIR）是两类典型的特定 MPC 算法。其中，PSI 可以让两个或多个参与者安全地计算他们的私有数据集的交集，而不泄露任何额外的信息；PIR 是一种允许用户从数据库中检索数据，而不泄露他们检索的内容的技术，PIR 的主要动机是保护用户的隐私，防止数据库所有者或其他观察者推断出用户的兴趣或偏好。PIR 有两种基本类型：信息论 PIR 和计算 PIR。信息论 PIR 可以在不信任数据库所有者的情况下实现完美的隐私，但需要多个不相互通信的数据库副本。计算 PIR 只需要一个数据库，但依赖于计算困难性假设，如 RSA 或学习有错误的假设。PSI 和 PIR 的实现方式有很多，像前文提到的基于 RSA、ECC 或者基于 OT、VOLE 的等等。目前行业内应用较多的方案基本都包括公钥密码部分，为满足后量子安全性，需要针对这些公钥模块进行 PQC 改造。

5）联邦学习：联邦学习 FL 是一种机器学习方法，允许多个参与者在保持训练数据隐私的同时，协同训练一个模型。FL 的基本思想是每个参与者使用自己的本地数据对模型进行更新，随后将更新的模型参数发送给中心服务器或某个计算方。服务器对所有参与者的模型参数进行聚合，得到一个全局的模型，并将其分发给所有参与者。每个参与者都可以从其他参与者的数据中学习，而不需要直接共享原始数据。FL 中的数据交互过程需要用（半）同态加密或者秘密分享来加密梯度以保护其隐私性，因此安全性同样容易受到量子计算攻击影响，需要仔细的评估 FL 中量子脆弱的部分，并进行后量子算法协议的改造。

6）零知识证明：零知识证明（Zero Knowledge Proof，ZK/ZKP）是一类密码学计算协议，其主要特征在于：遵循该协议的证明者可以向验证者证明某个陈述是真实的，而不需要透露任何其他信息。零知识证明的优点是可以保护证明者的隐私，同时也可以防止证明者伪造错误的证明。零知识证明应用领域广泛，例如身份认证、数字签名、资产证明等。在隐私计算中，ZKP 常用于将半诚实的安全计算协议扩展为恶意模型安全的协议。现有的 ZKP 体系大多数基于椭圆曲线密码体系，如何设计量子安全的通用 ZKP 或采用 ZKP 增强 MPC 的安全性仍是一项开放性课题。

3.2.5 应用层

推进利用后量子密码算法改进隐私计算中的多种算法，可以允许参与方在不暴露自己的数据的前提下实现量子计算时代的数据安全融通，助力上层多源数据的融合与应用。应用层支持的场景可涵盖金融风控、广告投放、数据流通、资产评估、联合反诈等。

后量子隐私计算及相关上层应用尚处发展阶段，需要产学研各界共同努力，完善技术体系、算法框架以应对未来量子计算带来的安全威胁。尽管面临诸多技术挑战，但后量子隐私计算无疑是量子计算时代保证数据安全的关键手段和必然趋势。业界需要从硬件、算法、协议等多个层面进行系统设计和技术创新，以构建长效安全且高效可靠的后量子隐私计算生态。

4 后量子隐私计算实践

后量子隐私计算对于确保量子计算时代的数据安全合规流通具有重要意义。目前中国电信基于自身在隐私计算和密码学方面的实践积累，在后量子隐私计算方面围绕上述框架进行了先期探索实践，重点关注如何使通用安全多方计算（MPC）、隐私集合求交集（PSI）、隐匿查询（PIR）、联邦学习（FL）等这些重要的隐私计算协议初步具备后量子安全性，主要路径是采用传统公钥密码的抗量子攻击算法迁移，以下针对相关技术探索进行简要论述。

4.1 隐私计算后量子改造

4.1.1 安全多方计算

OT 协议是构建安全多方计算的一个重要原语。在后量子 OT 的选取上，如果是基于随机预言机（Random Oracle Model，ROM）模型构建，比如基于 LPN 的 Ferret OT，其虽然在半诚实安全模型中因为没有用到 ROM 的历史查询而满足后量子安全，但在恶意模型中却无法在量子随机预言机模型（Quantum Random Oracle Model，QROM）下实现可证明安全性。因此，在实践中优先考虑使用不基于随机预言机模型的协议来构造后量子的半诚实 OT 或恶意 OT 协议，比如基于 RLWE 的 OT 协议。在后量子 OT 扩展的选取上，Bucher 等[14]证明了 IKNP03 的 OT 扩展协议在 Base OT 协议是后量子安全的情况下，OT 扩展协议也是后量子安全的，因此可基于 RLWE 构造 Base OT，并通过 IKNP 协议将其扩展为后量子的 OT 扩展协议。此外，对于 OT 扩展协议而言，实践证明将 Base OT 由基于 ECC 的 OT 替换为基于 RLWE 的 OT 对整体性能的损失不超过 0.5%。

FHE 是一项构造后量子安全多方计算的重要工具，其安全性基于 RLWE 问题。相比而言，量子计算对于解决格上困难问题并没有一个显著的加速，这使得 RLWE 问题往往只需要稍微调整参数，就可以由经典的安全强度，得到同样等级的后量子安全强度。根据不同算法对于全同态加密的不同计算性质需求，RLWE 的后量子参数选取也不同。参数的选取关系到整体协议的运行速度，如何通过谨慎的选取参数使协议整体保持高效是一个值得研究的问题。

对于通用的 MPC 协议，如果是采用基于秘密分享的信息论安全的 MPC 协议，只需在乘法三元组生成、比较大小、电路转换等需要 OT 参与的部分中将 OT 替换为（QROM 下安全或不基于 ROM 的）后量子的 OT 协议即可；若是基于 GC 的通用安全计算协议，同样可以将评价电路过程中的 OT 协议替换为后量子的 OT 协议以达到后量子的安全性。

在后量子 PSI 方面，通过 OPRF 或 ECC 的方式来构造平衡的两方 PSI 的比较典型的方案有 KKRT-PSI 和 ECDH-PSI。不过，对于 ECC 中涉及到的椭圆曲线点乘操作目前没有较好的替代，因此 ECDH-PSI 较难找到后量子替代；对于 KKRT-PSI 来说，基于 Bucher 等对 OT 扩展协议的后量子安全证明[14]可以推广得到后量子安全的 KKRT-PSI 协议。一般可以通过构造一个后量子安全的 Base OT 协议，再进行 OT 扩展得到后量子安全的 OPRF，或直接用后量子安全的 VOLE 协议来构造 OPRF，进而得到后量子安全的 PSI 协议。此外，还可以用 Oblivious Key-Value Store，即 OKVS 工具扩展 OPRF 得到后量子的 Oblivious Programmable Pseudo-Random Function，OPPRF 协议，通过 OPPRF 不仅可以实现恶意模型的 PSI 协议，也可以将两方 PSI 协议扩展到多方。此外，也可以直接使用 FHE 来实现 PSI，利用多项式运算来得出交集。具体来说，用户发送一个查询密文，服务器在密文上运算一个交集多项式，发送给用户解密，若解密后结果为 0 则表示用户数据在交集中。考虑到查询结果不在交集中的情况，多项式解密结果可能会暴露数据库的某些信息，因此还需要引入后量子的 OPRF 协议保护数据库的隐私。基于 FHE 的 PSI 协议在两方非平衡场景下有不错的性能表现。最后一种是可以不暴露交集 ID 的匿踪求交方案，这种方案的一种通用实现是通过构造 PSI 电路（Circuit PSI）来实现，可以采用通用后量子 MPC 协议来进行 PSI 电路构造。

PIR 有两种基本类型：基于索引的 PIR 和基于关键词的 PIR。基于索引的 PIR 要求用户知道自己所要查询的数据在数据库中的位置，这种基于索引的 PIR 可以由全同态加密 FHE 计算内积的方式来实现，由此可以轻易地具备后量子安全性质；另一种是基于关键词的 PIR，用户通过要查询数据的关键词从数据库中搜索想要查询的数据。基于关键词的 PIR 又有两种构造方式，第一种是通过全同态加密的 PSI 的方式构造，在密文计算一个求交多项式的时候也计算一个查询多项式，在求交多项式结果为 0 的时候，查询多项式的结果是 PIR 查询的值，可以较为轻松的得到后量子安全的协议；另一种是通过 PSI-PIR 的方式来构造，数据库在计算交集时，同步使用对称加密将所有数据都加密并发送给用户，用户通过 PSI 的方式查询对应数据的解密密钥。显然这种 PIR 的 PSI 部分需要首先满足后量子安全性。

在上述包括通用多方计算、隐私集合求交以及隐匿查询等安全多方计算协议中，可通过调整或替换已有的密码学算法来实现后量子安全方案的改造。然而，这仍然是一个快速发展和不断变化的领域，需要持续的关注和研究。

4.1.2 联邦学习

已有的联邦学习算法大多使用同态加密、秘密分享、差分隐私这三种技术中的一种或多

种技术的组合来保护参与方私有数据的隐私性。

基于同态加密的联邦学习算法利用明密文计算同态的性质，将隐私敏感的中间结果（梯度、模型参数等）加密，传输到不同的参与方进行密文计算，从而达到多个参与方在隐私保护的基础上联合训练模型的目的，如常见的纵向联邦逻辑回归[15]。目前应用于联邦学习中主流的同态加密算法是 Paillier 算法，其安全性基于大整数分解问题，由于 Shor 算法可以将 Paillier 的公钥 n 进行快速分解并推算出私钥，因此在隐私计算中所广泛应用的 Paillier 算法并不具备后量子安全性。

秘密分享的基本思想是将一个秘密分成多个碎片，每个参与者只持有一个碎片，只有当收集到足够多的碎片时，才能恢复出原始的秘密。基于这一特性，参与者可以将自己的隐私数据分成多个碎片并与其他参与者交换一部分碎片，随后所有的参与方基于自己获得的碎片并按照具体的联邦学习协议进行乘法或者加法运算，再将所得结果用于后续的迭代。在这一场景下，如果碎片化的数据单纯进行加法运算并将结果在可信第三方进行聚合，本身已经满足信息论安全，自然也满足后量子安全性；但如果算法协议的任一过程存在基于碎片数据的乘法运算或非多项式运算，就会涉及到后量子安全问题。例如，常见的基于同态加密、OT 等协议生成乘法三元组的方法、或基于 OT 的非多项式函数运算均会导致整个协议不具备量子安全性[16]。

差分隐私也是一种用于保护数据集中个体信息的隐私保护技术，其核心思想是在数据集中添加一定的随机性，使得对外部的查询结果不会因为数据集中某一条记录的改变而发生明显改变，从而保护被查询者的隐私。差分隐私通过在联邦学习的中间结果添加一些随机噪声（高斯、拉普拉斯等）来保护模型训练中间结果的隐私，使用差分隐私需要在数据的隐私保护程度和模型的准确性之间进行平衡。由于常用的差分隐私是直接对数据进行更改来增强隐私，其安全性通常不会受到量子计算的影响。

综上，目前在联邦学习后量子安全的协议改造上可将重点放在半同态加密算法替换以及非后量子安全的多方计算算法上。以常用的纵向联邦逻辑回归 [15]为例（如图 4.1），在不改变原始的算法协议流程基础上，通过引入后量子安全性的全同态密码算法 BFV 代替原始的 Paillier 加密，只需要将原始 Paillier 加解密的步骤直接替换即可。此外，在纵向逻辑回归中多次涉及到密文与明文的矩阵乘法，而基于 RLWE 的全同态加密技术结合多项式系数编码可极快地在两方之间运算密文上的矩阵乘法，实现在不损失训练结果精度的同时大幅提升训练速度。

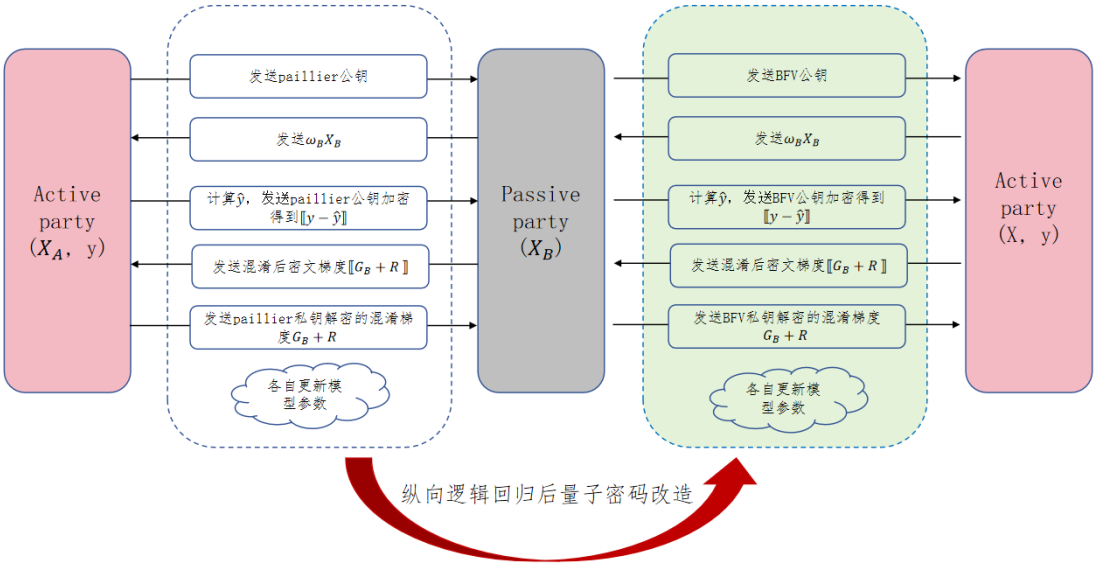

图 4.1 后量子安全纵向逻辑回归重构

4.1.3 其他依赖公钥密码学的算法

除了在隐私计算中直接应用到的密码算法外，其他一些可与隐私计算结合的密码学算法的后量子改造也在推进中。

群签名和环签名允许用户以群组的名义匿名地对消息签名，在支持身份认证等安全服务的同时保护用户隐私，在可信计算、车联网、电子投票、数字货币等场景有重要应用。目前在后量子密码改造方面，已经可以构建出在标准模型、随机预言机模型和量子随机预言机模型下安全的群签名和环签名方案[17]。但目前这些方案在设计上都尚未成熟，性能与传统的群签名和环签名相比仍有一定劣势。

在零知识证明方面，通用的零知识证明协议如 zk-SNARK[18]的安全性基于公钥 ECC，因此无法抵抗量子计算的攻击，其他的协议如基于哈希算法的 zk-STARK[19]达到了后量子安全性，但其证明的速度较慢，且空间复杂度较高。专用的零知识证明方面，如针对神经网络训练的零知识证明可以采用基于 LPN 构造的方案[20]，在满足后量子安全性的同时能达到较好的实用性。

4.1.4 后量子密码结合量子密钥分发

量子密钥分发（Quantum Key Distribution，QKD）技术基于量子力学原理，使用量子态来编码信息，通过对量子态的制备、传输和测量实现随机数的安全分发并作为密钥或密钥生成材料，其核心思想是利用非正交单量子态的不可克隆性来完成随机数的安全分发，且对分

发过程的任何窃听行为都会因扰动量子态而被及时发现。

相较于 PQC，QKD 主要适用于通信中的密钥交互场景，通过量子物理手段保证安全性，而 PQC 则基于数学上的困难问题提供一系列的密码算法。在实际应用中，可以融合量子密钥分发（QKD）和后量子密码（PQC）两种技术路线以实现更加安全的综合解决方案。比如，可以利用 PQC 解决 QKD 中的身份和消息认证问题，进一步提升如量子城域网、量子密话手机等一系列产品的安全性。而同时 QKD 从物理层面完善了 PQC 链路的安全性，两者融合可充分发挥量子技术的安全特性及优势，全面保障通信与计算网络的安全。

我国几家校企联合研究团队近期完成了全球首次量子密钥分发（QKD）和后量子密码（PQC）融合的城域网现网验证[23]，通过将 PQC 认证协议集成到 QKD 设备内部简化 QKD 设备之间原本采用的一对一的复杂认证方法，并在多用户、城域网现网通信条件下进行了长时间运行测试，在现网实际业务中验证了融合方案的可行性。

中国电信将基于量子通信领域先发优势，推进 QKD 与 PQC 在技术与多类产品层面的深度融合，以全面提升量子时代信息化系统的长效安全性。

4.2 密流量子盾

密流量子盾（PrivTorrent Quantum Shield）是中国电信基于新型后量子密码算法和隐私增强技术体系所自主构建的抗量子计算攻击的隐私计算试验型平台系统。该系统围绕量子计算可能引入的新型安全威胁，提供了可有效抵御量子计算以及传统计算机攻击的密码算法迁移方案，旨在实现既能抵御量子攻击，又能兼容多方协同计算的密码算法协议，确保隐私计算技术和数据融通基础设施在可预见未来的安全性，这也是建设面向未来的数据要素基础设施长效安全能力的必然要求与有力保障。密流量子盾系统架构如图 4.2 所示，其部分主要功能和特性包括：

(1) 通信层面支持基于格的全后量子密码的密钥封装机制及数字签名算法，以及国密混合的密钥封装和数字签名“双锁”或“多锁”机制；

(2) 全面覆盖后量子安全的数据流通能力，在保证数据隐私的前提下，实现不同参与方之间的协同计算，支持包括 PSI、PIR、LR、XGB、多方安全排序、统计等在内的多类隐私计算算法簇；

(3) 应用传统隐私保护增强技术，如差分隐私、匿名化等，通过算法的灵活组合，在数据利用和分析过程中提供额外的隐私增强保护，可按需配置不同等级的隐私保护策略；

(4) 通过密码算法和协议的替换与性能优化，获得高效的后量子安全算法计算性能，降

低算法迁移对业务的影响。性能测试表明，多数算法迁移导致的性能损失可忽略。值得注意的是，通过计算策略的综合优化，部分算法较经典算法获得了显著性能提升；

(5) 模块化和可插拔的系统框架设计，可根据应用场景需求定制不同的安全方案，同时支持不同安全机制的模块化集成。

密流量子盾系统通过前瞻性的技术布局，为后量子时代的数据要素流通提供安全保障，为建设面向未来的数据基础设施长效安全能力提供中国电信的实践范本。

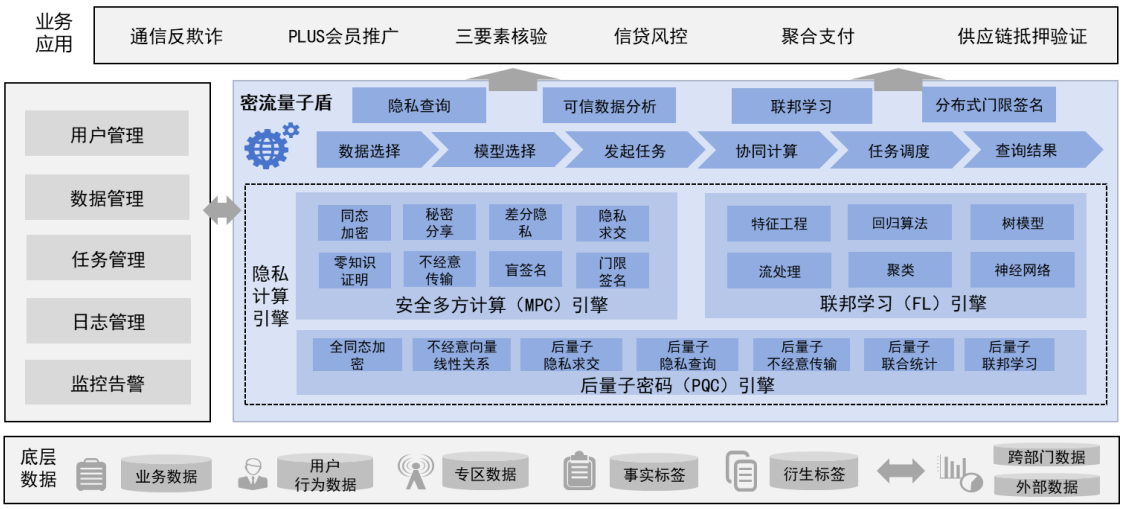

图 4.2 密流量子盾系统架构

5 后量子隐私计算的挑战

后量子密码迁移及其与隐私计算的深度融合是面向未来的数据要素关键信息基础设施安全的必要保障和发展趋势，但当前仍然存在包括性能衰减、安全评价、标准化缺失等方面诸多待解决的问题和挑战，以下简要论述。

5.1 性能

主流后量子密码大多基于格密码（Lattice based Cryptography）构造，格密码相比其它类别的后量子密码体系，从算法方面和密文大小方面具备一定优势。但相比传统的 ECC 等密码原语，后量子密码的密文和密钥的空间占用更大，计算性能也可能更低。表 5.1 展示了部分后量子密码相对于经典公钥密码的性能比较。后量子密码的签名大小导致其在一些计算存储资源有限的嵌入式设备中的使用将面临资源不足的问题，未来对于这类设备的后量子密码改造或迁移需将需要从硬件层面进行重新设计。

表 5.1 签名算法性能比较[28]

算法名称	量子安全等级	公钥大小 (bytes)	私钥大小 (bytes)	签名大小 (bytes)	签名时间 (ms)	验证时间 (ms)
RSA 3072	~0 bits	387	384	384	3.19	0.06
ECDSA 384	~0 bits	48	48	48	1.32	1.05
Dilithum II	91 bits	1184	2800	2044	0.82	0.16
Falcon 512	103 bits	897	1281	690	5.22	0.05
SPHINCS+	64 bits	32	64	16976	93.37	3.92
Dilithium IV	158 bits	1760	3856	3366	1.25	0.30
Falcon 1024	230 bits	1793	2305	1330	11.37	0.11

对于内存设计已达到性能极限的应用来说，将其中的密码原语替换为后量子密码往往需要更大内存空间存储中间计算结果。后量子密码的高计算复杂度会对需要实时或近实时响应的应用带来明显性能衰减。

观察到后量子密码算法在密钥或签名大小上远超于传统密码体制，所以后量子密码体制在总体性能方面仍弱于传统密码体制，因而适用于实时性要求不高且资源密集型场景。但随着基于后量子困难问题如 LPN、RLWE 等构造的更加高效的密码算法与隐私计算协议的不断成熟、理论和实践不断创新、软硬结合愈发紧密，后量子密码的应用场景将更加普适。

5.2 安全

在对密码学算法进行安全性证明过程中，通常需定义“预言机”来描述算法在理论上拥

有的能力。在传统情况下，允许敌手以比特串的形式向预言机输入信息并获得反馈。然而，当敌手拥有量子计算能力，他们可能会以量子叠加态的形式向预言机输入信息。因此，在考虑量子能力的敌手威胁模型时，往往需要允许预言机接收量子叠加态的输入。

Boneh 等[21]提出了量子随机预言机模型 QROM，并在论文中给出从 ROM 模型下的安全性推导到 QROM 模型下安全性的条件。从结论来看，存在一些在 ROM 下可以证明安全，但在 QROM 下不安全的算法。同时，一些在 ROM 下适用的证明技术，如 Rewinding 方法，在 QROM 中也需要重新考虑。因此，在后量子隐私计算中，仅仅将数论密码算法替换为后量子密码并不能完全确保协议整体上的后量子安全性，在进行隐私计算协议的后量子改造中，需谨慎考虑算法的可证明安全。

现有的后量子密码优化方法通常关注于提升算法的性能，忽略算法实现中的安全问题。侧信道攻击是密码分析中最常用的技术之一，后量子密码计算方案不仅面临 CPU 通用的侧信道攻击手段，例如时序攻击、电磁攻击等；还存在硬件带来的多线程并行、多层次内存等技术带来的新型攻击风险。近年来专门针对密码设备攻击的工作同样层出不穷，传统的基于掩码防护策略存在计算代价高、防护能力有限的问题。

此外，需要强调的是，目前的后量子安全算法仅能代表至今为止没有发现量子计算的攻击手段。Regev[26]在 2002 年发表了文章论证量子计算成功攻击格密码的概率非常小，但关于后量子密码的安全性问题还是受到很多的质疑。比如 SIKE 算法是基于椭圆曲线同源困难问题构建的，尽管椭圆曲线同源问题本身是困难的，但仍存在针对 SIKE 算法的量子攻击方法，以及侧信道攻击等非常规的攻击模式。因此，密码敏捷性也是需要考虑的重点因素，当发现某种算法不安全时，如何快速地切换系统中使用到的密码算法以保证整体安全性。密码敏捷性在算法与协议设计之初即需纳入规划。

5.3 工程复杂性

新型密码体制的研究、论证、筛选、工程化与普及是一个长期过程，涉及诸多环节，如探索可行的算法、可能攻击方式，论证算法的安全性，探索可靠安全的算法实现、算法性能提升、硬件设备层面实现以及拓展算法在现实场景应用等。这类改造与普及的复杂度导致新一代密码算法体制往往需要一个相当长的时间周期才能够被广泛地替换，比如 ECC 在 1985 年被提出，相较于 RSA 有着巨大的性能优势，但直到 2015 年可靠的 ECC 算法才正式接管 RSA 的地位。

对于已建成非后量子安全信息系统的机构，迁移改造也可能涉及到系统重建与业务迁移，

需要投入较高成本，且迁移过程可能会对现有业务产生不利影响，这需要前期做好全面评估，如考虑如何保证业务在过程中的不间断性以及如何尽可能降低迁移成本和周期。同时，在后量子密码总体性能弱于传统密码体制的情况下，如何安全高效地实现后量子密码算法，不仅要支持设备上的更新，还有考虑迁移的效率以保证不同的 PQC 数字签名算法或公钥加密算法在应用场景中的高适配度。

近年来随着以 IBM、谷歌、微软等为代表的企业在量子计算机制造领域突飞猛进，量子计算时代 Q-Day 正加速到来。后量子迁移进程将不得不进一步加速，尽可能地降低量子计算机所带来的一系列不可预知的安全风险。现存后解（SNDL）困境的存在也要求企业与政府信息化系统的后量子迁移工作必须尽早完成。

5.4 标准化进展

当前，全球后量子密码的标准化工作主要由美国国家标准与技术研究院（NIST）主导。NIST 早在 2016 年已正式启动全球后量子密码标准筛选，先后搜集全球高校或企业所提交的 82 项算法提案并筛选出 69 项进入首轮评估，涵盖格、哈希、同源、多项式等多种数学基础构建的方案。第三轮的标准化方案中已有部分算法生成 FIPS 草案，正在征集意见评论，总体标准化工作预计将在 2024 年完成。基于后量子密码的隐私计算迁移标准化工作目前还仅停留于学术研究阶段，尚无公开的标准化计划。隐私计算相较于传统的密码学，本身是一个较新的分支，其后量子迁移标准化工作将依赖于基础后量子算法的标准制定进程。随着 NIST 标准进入收尾阶段，隐私计算领域的后量子迁移已具备一定的算法基础。另一方面，提早布局后量子隐私计算研究与工程实践，将对相关标准化工作提供重要借鉴。

6 发展趋势

随着量子计算理论研究的成熟与量子计算机技术的飞速发展，量子计算时代即将来临。美国及欧盟已相继启动政府级的庞大后量子迁移推进项目，并公开宣布当项目进行到一定阶段后就不会再向全球公开其进展。这表明量子计算及后量子安全密码相关技术的研究将不再局限于科研与经济产业应用，而会首先应用于国家战略安全相关重大领域。

6.1 未来展望

随着量子计算时代的到来，向后量子密码体系迁移已成为所有基于公钥密码体系构建的信息系统所面临的当务之急。全球学术界对于量子计算对公钥密码体系的破坏作用已有充分认识，得益于学术界和产业界的共同努力，后量子密码相关的理论研究、标准化工作以及工程迁移尝试正加快推进中。

在初始阶段，后量子密码及后量子隐私计算将遵循保守策略，例如，利用混合密码体系或对算法细节进行保密的方式进行实施，主要应用于需要长期保护安全性和隐私的领域。

随着学术界与产业界对于后量子密码的关注度不断提升，相关算法的开发和优化将成为持续研究的重点，包括但不限于提高算法效率、优化资源消耗和增强安全性。

在相关标准逐步完善的同时，后量子密码与后量子隐私计算的应用领域将持续扩大。除涉密部门外，金融、政务、运营商等数据敏感的行业可能会进行早期的试点。

随着后量子密码和隐私计算相关的政策法规、制度标准日益明晰，尤其是随着量子计算机能力的逐步提升，量子计算相对于传统计算的优势将进一步显现，后量子密码与后量子隐私计算技术也将从少数领域或涉密部门转向大规模、商业化的广泛应用。

后量子密码技术的推广和普及必然会面临诸多挑战，包括技术难度、成本问题，甚至产业界对量子计算理解程度不足等问题。因此，未来各界需要在研发、应用、教育、公共意识、规范标准与法规等领域持续投入。随着后量子密码算法与隐私计算的普及，面向未来的可靠隐私计算技术体系将成为新一代数据要素流通基础设施的核心技术底座，也是数据在量子计算时代安全流通的重要保障。

6.2 中国电信的规划

随着信息化技术的发展，以及数字经济时代新兴技术的日益成熟，数据的价值已上升到前所未有的高度。数据已成为国家和企业具有战略价值的核心资产，数据安全也成为国家安

全、社会安全、经济安全和金融安全的关键支柱。为保证数据隐私合规、实现数据安全跨域融通以最大化释放数据价值，打破数据孤岛，对隐私计算、区块链、可信硬件等技术的深入研发意义重大，密码学作为核心技术底座，其长期的安全性更是对数据安全至关重要。

量子计算机技术的飞速发展，加速了现代密码学由公钥密码、数字签名等经典公钥算法进入到对数据融通进行全流程隐私安全保护的后量子时代。尽管传统的基于数论难题的密码算法受到量子计算的巨大挑战，但以格密码为代表的后量子密码算法却进一步推动现代密码学的演进。如何将目前广泛使用的密码算法迁移到更安全的后量子形态，如何将后量子安全算法与隐私计算、区块链、可信硬件等前沿信息技术进行融合，并基于其构建更安全、高效的计算协议，是后量子时代密码工作者与研究机构需要关注的核心问题之一，也是确保我国关键基础设施长期安全的重大科研与工程实践任务。

中国电信在网络安全、数据安全、基础密码学、隐私计算、区块链、大数据等领域持续投入，积累了丰富的技术实践经验。为应对即将到来的量子计算时代所引入的新型安全威胁，中国电信率先组建了后量子密码迁移与后量子隐私计算研究团队，跟踪全球后量子密码技术研发与标准化进程，同时积极吸收学术界和工业界对于后量子密码的优秀研究成果，不断从工程化、安全性、计算效率、功能性等多方面对后量子密码算法与隐私计算协议进行优化，并推进后量子密码迁移实践工作。中国电信在后量子密码领域开展了深入的工程探索，基于中国电信“密流安全计算平台”，构建了新一代“密流量子盾（PrivTorrent Quantum Shield）”隐私计算原型，这也是业界首款后量子安全的隐私计算试验产品，从理论到工程上积累了宝贵经验。

在后量子安全日益重要的当下，中国电信将积极承担央企责任，持续探索、推进后量子密码迁移、后量子安全密码算法/隐私计算协议构建等重点前沿技术创新。同时，中国电信也将跟踪后量子密码国密标准进展，并加快推进行业内、跨行业产学研生态协同，整合内外部资源与能力，依托数据要素市场化的趋势与数据要素流通基础设施建设，为后量子密码与后量子隐私计算拓展重要应用场景，为我国密码应用技术的发展、国家数据流通基础设施的安全保障做出应有贡献。

参考文献

1. Devoret M H, Schoelkopf R J. Superconducting circuits for quantum information: an outlook [J]. Science, 2013, 339(6124): 1169-1174.
2. 我国科学家率先实现量子分解算法 [EB/OL], 2007-12-24/2023-10-19. https://www.gov.cn/govweb/fwxx/kp/2007-12/24/content_841733.htm.
3. IBM Quantum Computing: Roadmap [EB/OL]. IBM Quantum Computing | Roadmap, 2015-10-01/2023-10-19. https://www.ibm.com/quantum/roadmap.
4. Joseph D, Misoczki R, Manzano M, et al. Transitioning organizations to post-quantum cryptography [J]. Nature， 2022, 605(7909): 237-243.
5. Merkle R C. Secrecy, authentication, and public key systems [M]. Stanford university, 1979.
6. McEliece R J. A public-key cryptosystem based on algebraic [J]. Coding Thv, 1978, 4244: 114-116.
7. Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem [C] // International algorithmic number theory symposium. Berlin， Heidelberg: Springer Berlin Heidelberg， 1998: 267-288.
8. Barker W, Souppaya M, Newhouse W. Migration to Post-Quantum Cryptography [J]. NIST National Institute of Standards and Technology and National Cybersecurity, Center of Excellence, 2021: 1-15.
9. European Telecommunications Standards Institute. Migration strategies and recommendations to quantum safe schemes [R/OL], 2023-10-19. https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
10. 胡希，向宏，丁津泰等. 后量子密码迁移趋势下应用于区块链的公钥密码安全 [J]. 密码学报，2023, 10(2): 219-245.
11. Castryck W, Decru T. An efficient key recovery attack on SIDH [C] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2023: 423-447.
12. KpqC Competition [EB/OL], 2023-10-19. https://www.kpqc.or.kr/competition.html.
13. Bundesamt für Sicherheit in der Informationstechnik. Cryptographic Mechanisms: Recommendations and Key Lengths [R/OL], 2023-01-24/2023-10/19. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html.
14. Büscher N, Demmler D, Karvelas N P, et al. Secure two-party computation in a quantum world [C] // Applied Cryptography and Network Security: 18th International Conference, ACNS 2020, Rome, Italy, October 19-22, 2020, Proceedings, Part I 18. Springer International Publishing, 2020: 461-480.
15. Yang S, Ren B, Zhou X, et al. Parallel distributed logistic regression for vertical federated learning without third-party coordinator [J]. arXiv preprint arXiv: 1911.09824, 2019.
16. Demmler D, Schneider T, Zohner M. ABY-A framework for efficient mixed-protocol secure two-party computation [C] // NDSS. 2015.
17. Esgin M F, Steinfeld R, Liu J K, et al. Lattice-based zero-knowledge proofs: new techniques for shorter and faster constructions and applications [C] // Annual International Cryptology Conference. Cham: Springer International Publishing, 2019: 115-146.

18. Gennaro R, Gentry C, Parno B, et al. Quadratic span programs and succinct NIZKs without PCPs [C] // Advances in Cryptology–EUROCRYPT 2013: 32nd Annual International Conference on the Th eory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings 3 2. Springer Berlin Heidelberg, 2013: 626-645.
19. Ben-Sasson E, Bentov I, Horesh Y, et al. Scalable, transparent, and post-quantum secure computation al integrity [J]. Cryptology ePrint Archive, 2018.
20. Weng C, Yang K, Katz J, et al. Wolverine: fast, scalable, and communication-efficient zero-knowledg e proofs for boolean and arithmetic circuits [C] // 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021: 1074-1091.
21. Boneh D, Dagdelen Ö, Fischlin M, et al. Random oracles in a quantum world [C] // Advances in C ryptology–ASIACRYPT 2011: 17th International Conference on the Theory and Application of Crypto logy and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings 17. Springer B erlin Heidelberg， 2011: 41-69.
22. 闫树, 吕艾临. 隐私计算发展综述 [J]. 信息通信技术与政策，2021，47(06): 1-11.
23. Yang Y H, Li P Y, Ma S Z, et al. All optical metropolitan quantum key distribution network with po st-quantum cryptography authentication [J]. Optics Express, 2021, 29(16): 25859-25867.
24. Beullens W, Delpech de Saint Guilhem C. LegRoast: Efficient post-quantum signatures from the Leg endre PRF [C] // International Conference on Post-Quantum Cryptography. Cham: Springer Internation al Publishing, 2020: 130-150.
25. 孙思维, 刘田雨, 关志等.基于杂凑函数 SM3 的后量子数字签名 [J].密码学报, 2023, 10(1): 46-60.
26. Regev O. Quantum computation and lattice problems [J]. SIAM Journal on Computing, 2004, 33(3): 738-760.
27. Regev O. An Efficient Quantum Factoring Algorithm [J]. arXiv preprint arXiv:2308.06572, 2023.
28. Sikeridis D, Kampanakis P, Devetsikiotis M. Post-quantum authentication in TLS 1.3: a performance study [J]. Cryptology ePrint Archive, 2020.
29. Post-Quantum TLS [EB/OL] // Microsoft Research. [2023-10-26]. https://www.microsoft.com/en-us/rese arch/project/post-quantum-tls/.

中国电信 天翼电子商务有限公司 数字科技事业群

联系邮箱：**tysk.bj@chinatelecom.cn**

联系电话：**021-66286813**

联系地址：北京市西城区复兴门南大街乙 **2** 号天银大厦 **A** 东座 **5** 楼