密码+应用推进计划
CRYPTOGRAPHY PLUS IMPLEMENTATION INITIATIVES

后量子密码应用研究报告

（2023 年）

“密码+”应用推进计划

2023 年 11 月

版权声明

编写委员会

❖ **编写单位**（排名不分先后）:

“密码+”应用推进计划、中国信息通信研究院云计算与大数据研究所、复旦大学、长春吉大正元信息技术股份有限公司、上海泓格后量子科技有限公司、华为技术有限公司、之江实验室、蚂蚁区块链科技（上海）有限公司、中国农业银行股份有限公司、银联商务股份有限公司、中国银行软件中心、中国金融认证中心、北京数字认证股份有限公司、中电科网络安全科技股份有限公司、北京信安世纪科技股份有限公司、兴唐通信科技有限公司、中国科学院信息工程研究所、四川轻化工大学、中国电信研究院、杭州量安科技有限公司、上海图灵智算量子科技有限公司、信通数智量子科技有限公司、浙江九州量子信息技术股份有限公司、郑州信大捷安信息技术股份有限公司、安徽华典大数据科技有限公司

❖ **编写人员**（排名不分先后）:

徐秀、何阳、马聪、武昱、赵运磊、韩璇、李健、梁志闯、李强、王贵林、刘亚敏、刘哲、戴望辰、蓝怡琴、余剑斌、刘邓、文黎明、祁玉琼、姜磊、李昀、李凯、孙冬旎、林立、郭智慧、高文华、李向锋、张小青、秦体红、朱桂桢、李帅钢、毕蕾、高媛媛、金贤敏、陈立权、王稀、魏瑛、王靖然、张峰、方黎明、於建江、黄大骏、刘为华、汪国航、叶辉、金凡、秘相友、张翼、胡军华、郭笑兵

前言

密码技术是国之重器，在当前复杂的国际形势下，密码技术作为网络空间安全关键技术的重要性更为凸显。但是随着量子计算的快速发展，现阶段部署的一些经典密码算法（特别是公钥密码算法）将受到巨大的安全性挑战。如果量子计算机到来，将对当前密码技术带来颠覆性影响，严重影响信息系统安全与稳定运行，甚至影响国家安全。因此，当前围绕抗量子计算的新一代密码技术——后量子密码成为全球竞争的焦点和战略抓手。本研究报告系统性分析了当前量子计算对经典密码的威胁、量子计算发展的进展以及后量子密码发展的必要性。

量子计算机的发展超过预期，后量子密码迁移必须尽早提上日程。当前美、欧各国都在密集地发布后量子密码相关的战略计划，后量子的国际标准化进程也在紧锣密鼓地推进。针对当前后量子密码的技术路线和后量子密码应用研究现状，本研究报告创新性地提出“两把锁、双保险”的混合式后量子密码迁移方案，并研究了行业迁移策略、预测了迁移时间、分析了迁移挑战。后量子密码迁移是一项庞大而紧迫的工程，会面临算法技术、法律合规、专利等方面的风险，还要消耗巨大的成本，必须提前考虑各种潜在风险，提早布局，安全设计，稳步迁移。

最后，本研究报告从顶层规划、自主技术储备、标准体系建设、构建迁移生态、健全密码人才队伍等方面给了后量子密码发展建议。

目录

缩 略 语

NIST National Institute of Standards and Technology 美国国家标准与技术研究院

BSI Bundesamt fÜr Sicherheit in der Informationstechnik 德国信息安全联邦办公室

BMI Bundesministerium des Innern 德国联邦内政部

BMBF Bundesministerium für Bildung und Forschung 德国联邦教育与科研部

NSTC United States National Research Council 美国国家科学与技术委员会

ANSSI Agence nationale de la sécurité des systèmes d'information 法国信息系统安全局

NLNCSA Netherlands National Communications Security Agency 荷兰国家通信安全局

EuroHPC JU European High-Performance Computing Joint Undertaking 欧洲高性能计算联合中心

NSA National Security Agency 美国国家安全局

NCSC National Cyber Security Centre 英国国家网络安全中心

NIST IR NIST Interagency Report NIST 内部报告

ISO International Organization for Standardization 国际标准化组织

CRYPTREC Cryptography Research and Evaluation Committees 日本密码学研究和评估委员会

ECC Elliptic curve cryptography 椭圆曲线密码学

QKD Quantum Key Distribution 量子密钥分发

QSDC Quantum Security Direct Communication 量子安全直接通信

PQC/PQCrypto Post-quantum Cryptography 后量子密码

LWE Learning with Errors 容错学习

RLWE Ring- Learning with Errors 环上的容错学习

SIDH Supersingular Isogeny Diffie-Hellman 超奇异同源密钥交换

SIKE Supersingular Isogeny Key Encapsulation 超奇异同源密钥封装

PKI Public Key Infrastructures 公钥密码基础设施

UEFI Unified Extensible Firmware Interface 统一可扩展固件接口

图 表 目 录

1.量子计算威胁现状

1.1 量子计算及其对经典密码的威胁

量子计算是结合了量子力学和计算机科学的一种新型计算方式，其基于量子力学原理、利用量子信息单元进行计算，与经典计算模式有很大差异。量子比特为量子计算的基本单元，具有叠加、纠缠等特性。量子计算机即利用量子比特进行信息处理和计算的非古典型计算机。早在 1980 年代，著名物理学家费曼便提出了基于量子力学规律制造计算机的设想。**通过利用量子比特的叠加和纠缠特性，量子计算机有可能高效率解决一些在经典计算模式下“指数”级困难的问题。**因此，量子计算机以其拥有强大的计算能力和在特定问题上的高效解决方案而成为了科学技术进程中备受关注的领域。

量子计算的发展对密码学带来了巨大威胁。1994 年 Shor[1]提出的量子算法，可以在多项式时间内快速分解大整数以及求解离散对数，理论上 Shor 算法可以彻底破解当前广泛应用的 RSA 和椭圆曲线公钥密码算法，因它们的安全基础分别为大整数分解和椭圆曲线离散对数问题。1996 年 Grover 提出的量子算法，对无序集中的搜索复杂度有开平方量级的降低，理论上也可以使对称密码算法例如分组加密、杂凑函数的安全强度减半。

目前，在量子环境下传统密码算法的安全强度如下表所示:

图表 1 量子环境下经典密码的安全强度[2]

密码体制	密码算法	密钥/输出长度	安全强度		量子算法
			传统计算	量子计算	

公钥密码	RSA-1024	1024bits	80bits	0bits	Shor 算法：破解
	RSA-2048	2048bits	112bits	0bits	
	ECC-256	256bits	128bits	0bits	
	ECC-384	384bits	192bits	0bits	
	SM2	256bits	128bits	0bits	
对称密码	AES-128	128bits	128bits	64bits	Grover 算法：安全性减半
	SM4	128bits	128bits	64bits	
	AES-256	256bits	256bits	128bits	
杂凑密码	SHA-256	256bits	128bits	64 bits	Grover 算法：安全性减半
	SM3	256bits	128bits	64bits	

从表 1 中可看出，量子计算的发展对公钥密码算法的威胁更为严重，因 Shor 算法可以将 RSA 或 ECC 等密码算法彻底破解，这些算法不是量子安全的；而对于对称密码或杂凑密码的影响在可控范围内，可通过配置加倍安全参数的长度，如对称密码的密钥长度加倍，杂凑密码输出长度加倍等方式应对量子计算的威胁。

1.2 量子计算发展现状

量子计算在各国及相关企业的投资和布局研究下取得了一些重要进展。在国家政策层面，多个国家都已经陆续推出了量子计算相关的政策，美国在 2018 年签署“量子科技发展战略”，欧盟在 2020 年发布“欧洲量子计算战略”，日本在 2017 年制定“量子科学技术战略”。**在生态方面**，2017 年 IBM 成立量子计算产业联盟，由世界 500 强企业、学术机构、初创公司和国家研究实验室组成的全球性团体；国内的量子计算生态也在逐渐构建，诞生一批如阿里巴巴达摩院量子实验室、本源量子、国盾量子、启科量子等企业，专门从事量子计算研究和开发工作，开展各种基础研究和应用实践。**在技术路线方面，**量子计算机的实现技术主要有超导量子比特技术、离子阱技术和光量子计算技术等三种技术，其中超导量子计算机是发

展最快的路线，2022 年 IBM 的超导量子处理器 Osprey 已经达到了 433 量子比特，预计未来 3 年将突破 1000 量子比特，到 2030 年实现 100 万量子比特。

(1) 超导量子比特技术：基于约瑟夫森结，有较高的可控性和比特寿命，代表企业与研究机构包括 IBM、谷歌和本源量子。

(2) 离子阱技术：利用离子阱陷住原子离子，并通过激光进行操作控制，实现较高的保真度，代表企业与研究机构包括 IonQ 和 Honeywell。

(3) 光量子计算技术：利用光子作为量子比特载体，具有较强的容错性和抗干扰力，代表企业与研究机构包括图灵量子、中国科学技术大学。

1.3 量子安全技术路线

目前实现量子安全的技术路线主要有两类：量子密码技术和后量子密码技术（又称抗量子密码技术）。

1.3.1 量子密码技术

量子密码技术是一种基于量子力学原理的加密方式，使用量子比特相互作用和测量来保证信息的安全性。量子密码技术中最实用的方案是量子密钥分发 QKD，已工程实用的 QKD 如基于诱骗态 BB84 协议、GG02 协议以及与一次一密结合的加密技术均具有可证明安全性；量子安全直接通信 QSDC 是另一种量子密码技术，可在量子信道中直接传输秘密信息。与传统密码不同的是，量子密码技

术的安全性基于量子物理的本质特性：量子测不准原理、量子力学的不确定性、测量坍缩、纠缠粒子的关联性和非定域性。

以量子密钥分发为代表的量子密码技术已经走向了实用化阶段。通过量子密钥和对称加密结合，利用 QKD 替代公私钥的密钥协商技术，是目前量子密码技术的核心方法，这种新型的量子密码技术在产业技术标准化、量子基础设施组网、量子应用创新等方面都有较快的发展。国际电信联盟电信标准化部门 ITU-T、欧洲电信标准化协会 ETSI、国际标准化组织与国际电工委员会第一联合技术委员会 ISO/IEC JTC1、电气与电子工程师协会 IEEE 等国际和区域性标准化组织布局开展量子密钥分发 QKD、量子密钥分发网络、量子计算、量子互联网等方面研究工作并取得阶段性成果。中国通信标准化协会 CCSA、密码行业标准化技术委员会 CSTC 和全国量子计算与测量标准化技术委员会 TC578 等国内标准组织积极布局和开展量子保密通信、量子计算和测量等领域标准研究。

1.3.2 后量子密码技术

后量子密码仍然使用经典方式处理信息，只是与传统的 RSA 和椭圆曲线密码相比，其安全性基于不同的数学困难问题。后量子密码的发展史最早可以追溯到 1978 年的 McEliece 加密、Merkle 哈希树签名等。但当时，量子计算机对密码算法的威胁并没有很明确，也没有“后量子”的概念。由于量子计算技术的快速发展，开始形成“后量子密码”或“抗量子密码”的概念，即抵抗量子计算攻击

的密码算法。后量子密码技术还处于测试验证阶段，产业化发展仍需一段时间。

2.后量子密码研究现状

2.1 后量子密码发展的必要性

在量子计算威胁的背景下，现阶段部署的一些传统密码算法将受到巨大的安全性挑战。这会严重影响到国家安全，破坏国家信用和国家主权。业界普遍认为后量子密码的研究和应用刻不容缓，应该尽早部署能够抵御量子威胁的后量子密码技术，从而将全球信息网络系统面临的总体风险降至最低。

首先，具有强大密码破解能力的量子计算机近年来已经不断取得实质性进展，其发展速度超过预期。2019 年，谷歌和瑞典斯德哥尔摩皇家理工学院公布的一项研究成果，分析了量子计算机如何用 2000 万个物理量子比特来计算，在 8 个小时内暴力破解 2048 位 RSA 密码。这给我们发出了警醒，量子计算发展的进度不可预见，其发展速度超出预期，如果量子威胁因为技术突变提前到来，将会导致量子危机。业界应比预想的时间要更早地实现从传统密码到后量子密码的升级换代。

其次，对于需要长久保护的国家高机密高敏感数据，存在前向安全风险，即未来的量子计算机可能会破译这些机密数据。一些恶意组织将当前无法破译的信息保存起来，等到量子计算机商业化之后再来破译和攻击，以获取商业机密。所以，即便量子计算机 10 年

或 20 年之后才具有实质威胁，如果当前传输的数据具有较长期限的机密性或敏感性要求，那么这些数据仍然具有前向安全风险。因此在关系国防安全、国计民生、商业机密的战略领域应该尽早开始部署后量子密码技术。

再者，后量子密码迁移是一项极为复杂的长期系统性工程，需要耗费相当长的时间，必须提前规划。密码迁移一般要全面考虑算法安全性、算法性能、实施的便利性、合规性等方面。以往密码安全体系的迁移工作历时往往达到 10 年以上，如 ECC 早在 20 世纪 80 年代就被提出，但它花了 20 多年才获得广泛的采用，目前我国的 SM 系列国密标准的推广时间也约为 10 年。相比之下，后量子密码的过渡更为复杂，周期可能更长。再考虑到未来不断增长的密码安全需求，每一类别的后量子密码都只适用于部分应用场景，因此需结合应用场景的实际需求具体选择，客观上增加了后量子迁移的复杂程度。

2.2 后量子密码发展政策

2.2.1 美国

后量子密码和迁移战略方面，美国发布和更新了诸多政策。2018 年 9 月，美国国家科学与技术委员会 NSTC 发布《量子信息科学国家战略总览》[3]。2018 年 12 月，美国政府发布《国家量子规划法案》，从法律上宣布成立国家量子规划 NQI[4]，以加速量子科技研发，促进美国经济发展和国家安全。2019 和 2020 年，美国通过《国

防授权法案》，由此美国国防部开展和支持量子信息科学和技术研发，以提升相关技术落地能力、增强人才培育能力和提高量子技术意识。2022 年 1 月，美国总统签署第 8 号国家安全备忘录 NSM-8，首次将后量子密码纳入国家安全备忘录。2022 年 5 月，美国签署总统政令，要求确保美国在量子计算领域的领先地位，并推进后量子算法迁移，减少量子计算带来的安全风险。2022 年 7 月，美国国众议院通过《量子计算网络安全防范法案》，鼓励联邦政府信息系统向后量子密码迁移，以抵抗量子计算机的攻击。2022 年 8 月，美国通过《芯片与科学法案》修正了 NQI 法案以授权开展量子网络基础设施、通信、计算资源和教育资源的研发与标准化。2022 年 9 月，美国 NSA 发布了含后量子密码算法推荐的 CNSA 2.0 套件[5]，给出政府信息系统 6 种场景在 2033 年前完成后量子迁移的时间表。2022 年 12 月，NSA 发布《2022 年网络安全年度回顾》强调抵御迫在眉睫的量子技术威胁的最佳方法是后量子密码学，NSA 的目标是到 2033 年为所有国家安全系统(NSS)实现后量子密码。2022 年 12 月 21 日，美国总统拜登签署了《量子计算网络安全防范法案》，使其正式成为一项法律，鼓励联邦政府机构采用不受量子计算影响的加密技术。2023 年 3 月 2 日，美国发布《国家网络安全战略》[6]，提出联邦政府将优先考虑将公共网络和系统过渡到抗量子密码的环境中，并要求私营机构效仿联邦政府，逐步完成相关网络和系统向抗量子密码的过渡。

2.2.2 欧盟

战略层面，2020 年欧盟宣布的网络安全战略中将量子计算与加

密作为最重要的安全相关技术之一单独提出来，以强调量子计算与加密技术对于确保关键基础设施安全的重要性。2021 年 2 月，欧盟网络安全局 ENISA 发布了《后量子密码学：现状和量子迁移》报告，并于 2022 年 10 月进一步发布《后量子密码：集成研究》报告，从技术角度介绍了两种基本的后量子迁移思路：将后量子算法集成到现有 ICT 系统，特别是 TLS 等重要的安全协议性中，或直接设计新的后量子安全协议。

经费层面，欧盟于 2018 年启动了欧盟量子旗舰研究规划，在该旗舰研究规划下目前已展开的研究项目 20 余个，包括构建量子计算机的 OpenSuperQ（第一期 100 量子比特，第二期 1000 量子比特）。2019 年，欧盟启动了创新框架项目 EuroQCI，其目标是在未来 10 年内研发和部署欧盟境内端到端安全的量子通信关键基础设施，项目包括地面和空间通信方案，且要求达到 EAL4+的高安全级别认证。同时，欧洲高性能计算联合中心 EuroHPC JU 表明，将在 2021-2033 年投资 80 亿欧元，进行量子计算和量子模拟的基础设施构建，以及与高性能基础设施的集成。欧盟地平线项目则重视在量子密码和后量子密码方面进行布局和投入，其后量子密码方面的 PQCRYPT 项目在 2015-2018 年期间投入经费 390 万欧元。

2.2.3 英国

英国国家网络安全中心 NCSC [7]在 2020 年 11 月发布了预备使用量子安全密码的白皮书，表达其对如何应对量子计算威胁进行安全迁移的观点，为技术决策者提供后量子迁移背景信息。

2.2.4 德国

战略层面，2015 年德国联邦教育与科研部 BMBF 发布了政策报告《2015-2020 年数字世界的自主和安全》[8]，其中声明将促进长效安全密码及其应用实现的研发作为作为联邦政府研究策略规划的一部分。2020 年 8 月，德国信息安全联邦办公室 BSI 发布了关于迁移到后量子密码的推荐建议。2021 年，德国联邦内政部 BMI 发布《德国网络安全战略》，指出通过量子技术保障 IT 安全的战略需要通过一系列措施来实现，包括在高安系统中进行量子安全密码的迁移等。2022 年 5 月，BSI[9]发布《量子安全密码—基础，现状和推荐》技术白皮书，积极推动安全系统的后量子迁移。

经费层面，BMBF 于 2018 年公布《后量子密码》研究申请指南，计划在 2019-2022 资助周期内遴选了七个研究项目，总研究经费为 2420 万欧元，其中德国 BMBF 负担大约 1610 万欧元。2018 年，BMBF 发布《量子技术-从基础研究到市场》[10]的研究规划，目标是在 2018-2022 年的周期内提供 6 亿 5 千万欧元经费，用于面向应用和有商业化潜力的量子技术研发。

2.2.5 法国

法国信息系统安全局 ANSSI[11]于 2022 年 1 月公布立场文件，为开发安全产品的工业界提供指导，并为法国安全认证计划“Security Visas”规划出迁移时间线。

2.2.6 加拿大

加拿大国防部和武装部队（DND/CAF）于 2023 年 3 月发布量

子科学和技术战略实施计划《Quantum 2030》，其中确定在国防和安全方面具有应用前景的量子技术任务。并提出为应对量子计算威胁，新型的后量子密码（PQC）标准正在制定，同时有必要考虑可选的、互补的安全解决方案，例如量子保密通信。

2.2.7 中国

中国在后量子密码研究项目中给与政策和资金支持，鼓励量子计算和后量子密码的技术创新和产业发展。2022 年，人民银行《深化金融科技应用、推进金融数字化转型提升工程》相关工作部署中把“探索量子技术金融应用”作为重要的工作任务，加快推进抵抗潜在量子计算攻击的能力研究。2022 年中央经济工作会议首次明确提出加快量子计算等前沿技术的研发和应用推广，但尚未发布后量子密相关政策文件。

2.3 后量子密码技术路线

根据后量子密码算法所基于的底层困难问题，主流后量子密码算法大致分为 5 类：基于格（Lattice-based）的、基于哈希（Hash-based）的、基于编码（Code-based）的、基于多变量（Multivariate-based）的以及基于同源（Isogeny-based）的后量子密码算法。

2.3.1 基于格

基于格的算法由于在安全性、公私钥尺寸、计算速度上达到了较好的平衡，被认为是目前最有应用前景的后量子密码算法之一。基于格的密码算法最早出现于 1996 年，它的安全性依赖于求解格中

问题的困难性，主要用于构造加密、数字签名、密钥交换、属性加密、陷门函数、伪随机函数、同态加密等。与基于数论问题的密码算法构造相比，在达到相同（甚至更高）的安全强度时，基于格的算法的公私钥尺寸更小，计算速度也更快，且能被用于构造多种密码学原语，因此更适用于实际应用环境。近年来，基于 LWE 问题和 RLWE 问题的格密码学构造发展迅速。

2.3.2 基于哈希

基于哈希的签名算法不依赖于具体数学困难问题，也不依赖于特定的哈希函数，是后量子密码中理论安全性最强的一类。基于哈希的签名算法从 Lamport 提出的一次性签名方案演变而来，最早由 Ralph Merkle 提出，并使用哈希树构造。基于哈希的密码算法仅限用于数字签名，至今学术界还没有专家提出基于哈希设计并实现的公钥加密或密钥封装的方案。基于哈希的数字签名方案的安全性依赖于哈希算法的一些安全性质，例如单向性（抗原像攻击）、弱抗碰撞性（抗第二原像攻击）和伪随机性等。如果使用的哈希函数被攻破，完全可以构造新的安全的哈希函数来替代，因此基于哈希的签名是后量子密码中理论安全性最强的一类。但是主要有以下两点缺点：一是签名体积大；二是对于有状态的基于哈希的签名，其所能支持的签名次数有限，增加签名数量也将降低计算效率，并进一步增加签名的体积。

2.3.3 基于编码

基于编码的密码算法被认为是后量子密码中相对具有竞争力的

密码算法。基于编码的算法 1978 年，McEliece 提出了首个基于编码的公钥加密方案 McEliece 方案，从而开创了基于编码的密码学这一研究领域。其核心在于将一定数量的错误码字引入编码中，纠正错误码字或计算校验矩阵的伴随式是困难的。著名的基于编码的加密算法是 McEliece，McEliece 使用随机二进制的不可约 Goppa 码作为私钥，公钥是对私钥进行变换后的一般线性码。基于编码的密码通常具有较小的密文，但其缺点是公钥大、密钥生成慢，在实用化方面有待提升。

2.3.4 基于多变量

基于多变量的密码算法适用于一些注重算法效率但不关心带宽的应用场景。基于多变量的公钥密码系统将有限域上一组二次多项式作为它的公钥映射，其主要安全假设为求解有限域上非线性方程组这个 NP 难问题，目前没有量子算法可以高效率求解，但是也没有安全性的形式化证明。多变量密码算法相比于其他后量子密码算法具有签名验签速度快、消耗资源少的优势，其缺点是公钥尺寸大，因此适用于无需频繁进行公钥传输的应用场景，例如计算和存储能力受限的物联网设备等。

2.3.5 基于同源

基于同源的密码算法优缺点明显，安全性问题不断被挑战。同源密码是基于椭圆曲线同源问题的后量子密码系统，它基于一个新的困难问题，即寻找任意两条椭圆曲线之间的同源。2011 年基于超奇异同源的 SIDH 算法被提出，该算法是一个 Diffie-Hellman 类型的

密钥交换算法，2017 年基于 SIDH 算法的高效实现 SIKE 算法被提出，随后一些新的基于同源的密码系统被提出，比如 CSIDH 和 SQIsign 算法等。基于同源的密码继承了椭圆曲线密码的底层运算，公钥和密文尺寸都非常小，可以在通信量受限的环境下运行，但是其运行效率非常低，其密钥生成、加密和解密速度几乎比基于格大两个数量级，这使其不易实现在一些计算性能不足的设备上。在 NIST 将 SIKE 进入第四轮不久，有专家利用 SIKE 的提示信息可以在数小时内恢复私钥信息，即 SIKE 被攻破，不过 CSIDH 和 SQIsign 算法仍未被攻破。

2.3.6 其他

NIST 在新的一轮数字签名算法征集中期望寻找不基于结构格的数字签名方案，新的一轮数字签名算法除了上述 5 种方案还有基于 MPC-in-the-head 的，基于对称的和其他类型。其中，MPC-in-the-head 是一种零知识证明，将零知识证明和单向函数组合在一起构造签名，MPC-in-the-head 签名密钥较小，但签名尺寸较大。基于对称的签名是指全部使用对称加密和哈希函数构造签名，因此这一类被认为是最可靠的。除了 Preon 外，其他的算法都已有不同程度攻击。Preon 是基于 zkSNARK 配合单向函数构造签名，其签名尺寸较大且计算效率较低。

2.3.7 总结

综合来看，上述 5 类主流的后量子密码算法的特点总结如表 2。

图表 2 各类抗量子密码算法特点总结

类别	优点	缺点
基于格	安全性高，性能优越，功能全	带宽较大
基于哈希	公钥很小，安全假设少	性能有待提升，功能上只能构造签名
基于编码	密文较小	公钥大，密钥生成慢，在实用化方面有待提升
基于多变量	签名验签速度快，消耗资源少	公钥大，安全性低
基于同源	带宽很小	计算速度慢，缺乏可证明安全性

2.4 后量子密码标准化进展

2.4.1 国际标准进展

(1) NIST 后量子密码标准化动态

NIST 发起的后量子密码标准化项目是当前影响力最大、参与范围最广的标准化项目。其目标是遴选出通用的抗量子算法攻击的公钥加密、签名和密钥封装/建立算法，以替代美国现有的 FIPS 186 和 SP 800-56A/B/C 标准中的 RSA 和椭圆曲线离散对数类公钥密码算法。

早在 2012 年，NIST 便开始了对后量子密码的研究，建立相关团队，跟进业界进展，联络工业和国际标准化组织，以筹备该标准化项目。2016 年，NIST 通过 PQCrypto、亚洲抗量子密码论坛等会议平台进行宣传，以呼吁全球密码学家积极参与；并于 2016 年 12 月发布了正式的算法征集公告 NIST IR 8105。截止到 2017 年 11 月底，共征集到来自全球 25 个国家的 82 个提案，其中 69 个算法满足 NIST 的“完整且合适”接受准则，进入第一轮评估。这包含了 3 个来自中国的算法，和 22 个来自欧盟的算法。

2019 年初，NIST 发布第一轮评估报告 NIST IR 8240，并宣布有 26 个算法进入第二轮评估。其评估报告主要从安全性、实现性能、设计灵活性等角度出发，参考其内部团队的分析、公开论坛的讨论和业内自发分析和实现研究等各方资讯，对各个候选算法进行评估、比较和筛选。2020 年 7 月，NIST 发布第二轮评估报告 NIST IR 8309，并宣布 7 个算法进入“决赛圈”以及 8 个算法进入“备选圈”。

2022 年 7 月，NIST 发布第三轮评估报告 NIST IR 8413[12]，宣布了第一批标准算法：基于有结构格的公钥加密/密钥封装算法 Crystals-Kyber，以及基于有结构格的公钥签名算法 Crystals-Dilithium、Falcon 与基于哈希的公钥签名 SPHINCS+。基于编码的 Classic McEliece、BIKE 和 HQC 以及基于超奇异椭圆曲线同源的 SIKE 进入第四轮评估，但是 SIKE 算法很快受到严重攻击，宣告退出。

同时，NIST 也宣布将继续征集额外的数字签名算法，尤其欢迎不同于有结构格技术路线的具有“签名短、验证快”优势的通用签名算法提案，这一征集独立于原项目第四轮评估进行。在 2023 年 7 月，NIST 公布了 40 个进入额外数字签名征集的算法。

NIST 于 2023 年 8 月 24 日发布第一批后量子密码算法标准草案，包括 Crystals-Kyber（FIPS.203）、Crystals-Dilithium（FIPS.204）和 SPHINCS+（FIPS.205），第四种 Falcon 的标准化草案将会在 2024 年发布。NIST 计划于 2024 年发布标准正式稿，NIST 后量子标准项目负责人 Dustin Moody 表示，“我们正在接近隧道尽头的曙光”。

（2）欧盟国家标准化动态

欧盟并没有公布单独的后量子密码标准化计划，而是通过其“地平线 2020”项目配合美国 NIST 的标准化项目。美国 NIST 遴选出的第一批标准 4 个算法中，其主提交人均来自欧洲。实际上，欧洲密码学研究团队实力强劲，过往由美国 NIST 组织的几个密码算法公开征集项目最终的优胜算法均为欧洲团队，例如分组密码 AES（原 Rijndael）、哈希函数 SHA-3（原 Keccak）和轻量级对称密码 ASCON。

在德国 BSI、法国 ANSSI、荷兰 NLNCSA 等欧盟国家的监管机构发布的后量子密码白皮书中，也均推荐使用 NIST 项目候选算法。尤其，德国 BSI 信任基于无结构格的加密 FrodoKEM 和基于编码的加密 Classic McEliece，认为它们虽然性能不及 Kyber，但安全性更可靠，可以用于需要长期保密的高安全场景，并在其技术规范（BSI TR-02102-1）中推荐。由于目前在 NIST 标准化项目中 FrodoKEM 已落选，而 Classic McEliece 也未能成为第一批标准，因此德国 BSI 正积极推动这两个算法在 ISO 的标准化（PWI 19541）。

（3）其他国家动态

日本. 日本密码学研究团队也积极参与了 NIST 的 PQC 标准化项目，有 3 个第一轮算法是日本团队主导设计的，但也均未进入第二轮。日本的密码学研究和评估委员会 CRYPTREC 持续关注国际标准化进展并发布相关报告。

韩国. 韩国密码学研究团队积极参与了 NIST 的 PQC 标准化项目，

有 5 个由韩国团队主导设计的算法进入了第一轮，但均未进入第二轮。随后，在 2021 年，韩国抗量子密码学研究中心宣布启动“抗量子密码学竞赛”，截止到 2022 年 11 月，共有 7 个公钥加密/密钥建立算法和 9 个数字签名进入第一轮评估。第一轮评估将于 2023 年 11 月结束。

（4）标准化组织动态

ISO. 2015 年 ISO/IEC JTC1 SC27 就开始筹备 WG2 工作组以为后量子密码标准化做准备。2017 年 WG2 启动了常备文档 SD8 的撰写，作为后量子密码学的综述，并于 2020 年 5 月正式发布。ISO 初期的标准化计划也会专注在加密、密钥建立和数字签名算法上，随后再开始考虑基于身份的加密、基于身份的签名、匿名签名、同态加密以及其它类型的密码算法。目前 ISO/IEC 正在进行 14888-4“有状态的基于杂凑的签名机制”规范的开发，并启动了 PWI 19541，将向 18033-2 AMD2 中增加 FrodoKEM、Classic McEliece 和 Crystals-Kyber 算法。此外，一类特殊的后量子密码——基于格的全同态加密的标准进展较快，WG2 正在开发相关标准 ISO/IEC 18033-8。

IETF. IETF 有多个工作组在推动密码协议纳入后量子密码算法的演进。

LAMPS 工作组. 2019 年发布了 RFC 8696，描述了在 CMS 规范中将密钥传输和使用预共享密钥的密钥协商的输出混合以抗量子攻击的方法。2020 年发布了 RFC 8708，描述了在 CMS 中使用

HSS/LMS 算法。2022 和 2023 年发布了一系列草案，例如：在 CMS 规范中使用密钥封装机制的草案，也可以支持后量子密钥封装机制；在 CMS 中使用 Kyber 和 SPHINCS+算法的草案；以及在 X.509 证书中使用 Kyber 和 Dilithium 算法的草案。

TLS 工作组. 2020 年发布了两份草案，分别讨论对 TLS 1.3 和 1.2 的扩展，使其支持混合使用传统和后量子密钥建立算法来进行密钥协商；发布了 RFC 8773，扩展了 TLS 1.3，使用外部预共享密钥来抗量子攻击。

IPSECME 工作组. 2020 年发布了 RFC 8784，在 IKEv2 中支持混合预共享密钥以抗量子攻击。2022 年发布了 RFC 9242，为 IKEv2 协议的后量子演进提供支持。2022 年扩展了 RFC 7296 使 IKEv2 支持多重密钥交换，包含后量子密钥交换。

COSE 工作组. 2023 年发布了一系列草案，分别描述了 Dilithium、Falcon 和 SPHINCS+算法的 JOSE 和 COSE 编码。

PQUIP 工作组. 2022 年底新成立的工作组，以专门支持 IETF 协议和文档的后量子演进。

IEEE. 2008 年 IEEE P1363.1 规范纳入了基于格的加密算法 NTRU。该算法也投向了 NIST 后量子标准化项目并进入了第三轮，但在第三轮结束时出局。2022 年 IEEE 发布了 P3172，讨论传统算法与后量子算法的混合机制的实现、密码学敏捷性等问题。

ITU-T. 2020 年发布了 ITU-T X.1811 (X.5GSec-q)，给出了对 5G 系统中的后量子安全方案的初步推荐。

ETSI. 2013 年起即联合加拿大滑铁卢大学举办量子安全密码学会议，到 2023 年已举办 9 届；2015 年成立了 TC CYBER WG QSC 工作组，已发布一系列关于量子安全密码算法的技术报告。

2.4.2 国内标准进展

我国在后量子密码领域一直积极跟进，广泛布局后量子密码安全技术应用与产业生态，目前后量子密码算法的研究和应用正在逐渐走向成熟与标准化。**在技术交流方面**，中国与日本、韩国等国家于 2016 年开始组织“亚洲抗量子密码论坛”，与亚洲以及欧美专家定期进行技术交流。2023 年 7 月，第三届雁栖湖国际抗量子密码标准化与应用论坛暨后量子技术成果发布会在北京雁栖湖应用数学研究院成功举办。

为了充分调动国内研究力量投入下一代密码算法标准设计工作，我国于 2018 年已经面向全国启动了密码算法设计竞赛活动，为制定我国的后量子密码标准做准备。竞赛活动共收到来自中国科学院信息工程研究所、密码科学技术国家重点实验室、清华大学、复旦大学等单位所提交的 38 个公钥密码方案。经过细致的评审筛选，最终有 14 个公钥密码方案进入第二轮并获奖。

国内相关企业和组织也在积极开展后量子密码应用标准的探索。特别是金融领域，各金融机构对后量子密码技术及应用的标准化工作越来越重视，如中国建设银行建信金融科技有限责任公司、上海扈民区块链科技有限公司、银联商务股份有限公司等机构联合撰写了《金融系统应用后量子密码技术指南》，以指导金融系统应用后量

子密码进行安全增强的技术规范问题，重点在数字证书、签名、密钥协商、应用迁移等环节指导如何进行改造和应用，同时确保兼容现有国家密码安全标准，合规合法，符合监管要求。CCSA 量子特设组由牵头单位阿里、中国信通院、科大国盾等开展了《量子密钥分发、量子随机数及后量子密码在信息安全中的融合技术研究》标准研究报告制定。中国电子信息协会 2020 年 12 月发布《量子安全技术白皮书》，其中对后量子密码技术的发展现状，从政策和规划、标准化及产业生态等方面进行了分析。

3. 后量子密码应用现状

3.1 后量子 PKI

PKI 是一种利用公钥密码体制建立起来的具有普适性的安全基础设施。PKI 的核心是数字证书，目前，数字证书一般采用 X.509 国际标准和相应的国内标准，证书采用的签名算法以及证书中包含的签名算法大多为 RSA、ECDSA、SM2，难以抵抗量子计算攻击。

实现后量子 PKI 最简单的方案是直接采用后量子签名算法对现有的 RSA 或 ECDSA 算法进行替换，定义新的后量子签名算法 OID，支持采用后量子签名算法进行 CA 自签名、证书签发、证书链签发和 CRL 签发，并对证书应用系统进行改造，支持新算法的识别和验证，达到数字证书的量子安全。

另一种方案是在保留原有 PKI 结构的基础上，在 X.509v3 数字证书格式下兼容后量子签名算法，构造支持经典算法和后量子算法的混合证书。在 X.509v3 证书扩展域中定义新引入的后量子签名算法 OID、后量子签名公钥和后量子签名，相应的在做证书验证过程中，需要验证经典签名值和后量子签名值。相比于简单的后量子算法替换，混合证书模式可以更好地支持 PKI 系统向后量子方向平滑过渡，并且兼顾了经典安全和后量子安全。但混合模式带来的证书尺寸的扩增也是显而易见的。

3.2 后量子 SSL/TLS

SSL/TLS 是实际中部署和应用最为广泛的密码协议，数据研究

表明，全球每天产生大约 2^{30} 个链接，超过 60% 的互联网数据是通过基于安全的 HTTPS 协议实现的[16]。公钥密码学为开放网络上的数字通信提供安全保障，它是包括 SSL/TLS 在内的所有互联网协议的安全基石。SSL/TLS 协议包括了双向认证、密钥协商、加密三个阶段以及定期的协商主密钥或加密会话密钥的更新维护。后量子 SSL/TLS 实现技术途径可包括，一是替换通信双方的双向认证算法；二是替换密钥协商算法；三是替换会话密钥加密算法；四是采用 QKD 技术或 QRNG 技术实现量子密钥安全增强。工程上可采用上述技术的一种或多种的组合实现后量子 SSL/TLS。

头部企业已开始尝试把后量子 SSL/TLS 相关产品作为一个可选项提供给用户。亚马逊已经将混合后量子 TLS 与 Amazon KMS 结合使用，Amazon KMS 支持对 TLS 网络加密协议使用混合后量子密钥交换选项，当用户连接到 Amazon KMS API 终端节点时可以使用此 TLS 选项。谷歌于 2023 年 8 月在其 Chrome 浏览器中部署了混合椭圆曲线 X25519 和后量子 Kyber 算法的 TLS 协议。这些混合后量子密钥交换功能与目前使用的传统 TLS 加密一样安全，但是在延迟和吞吐量性能方面存在一定影响。

3.3 后量子区块链

现有的区块链主要采用经典公钥加密体系保障区块链的安全性，因此并不能抵御量子计算的攻击。后量子区块链通常是指面对量子计算机攻击，仍然能够保证安全性和可靠性的区块链系统。其利用后量子密码实现量子安全的身份认证和数字签名，并利用量子密钥

加密实现量子安全的数据加密通信。蚂蚁链等国内企业已有后量子密码应用于区块链的实践，主要聚焦于区块链运行生命周期的交易、共识、通信三个场景，已经完成区块链全流程的后量子密码能力建设。并针对当前后量子密码签名尺寸问题，结合特定场景进行升级优化。区块链后量子密码迁移主要涉及以下三方面的工作。

一是评估量子计算对区块链带来的潜在安全风险。考虑到前提是区块链后量子密码迁移，这里只给出区块链中涉及公钥密码的风险评估:

- 一方面，区块链目前得到广泛应用来自于它给不同诉求方间的协作带来新的信任基础，而这种信任基础建立在底层密码学所提供的安全性保障之上。这其中涉及到公钥密码的用法可粗略分为：链上交易防篡改使用的数字签名机制，以及节点间通信使用的安全传输协议。受 Shor 算法的影响，上述公钥密码在使用上的安全性无法得到有效保障。
- 另一方面，在考虑专用密码破译量子计算机大规模应用所需时间的同时，还需考虑存储在区块链上的数据需要保存多长时间以及现有区块链系统升级到量子安全级别的时间。如果后两者相加的时间和大于前者，那么区块链上的数据就会受到量子计算带来的严重安全威胁。

二是选择适配区块链应用的后量子密码算法。理想情况下，将现有区块链使用的公钥密码算法升级为量子安全的后量子密码算法，

应尽可能满足以下特点：

- 密钥小且签名短：区块链上的每笔交易都会包含签名信息，而验证任意一笔交易的公钥也存储在链上。若密钥以及签名尺寸过大，都将大大加剧区块链的存储成本以及通信开销。
- 计算效率高：区块链运行时每一时间段可处理的交易数量很大程度上与算法的运行时间有关，特别是签名验签算法。算法更快的计算效率可以更好地支持高性能的区块链应用。

三是确定区块链后量子密码迁移的应用场景并进行迁移适配改造。结合链平台技术特点以及后量子密码应用，可将迁移重点聚焦在区块链运行生命周期的交易、共识、通信三个典型应用上：

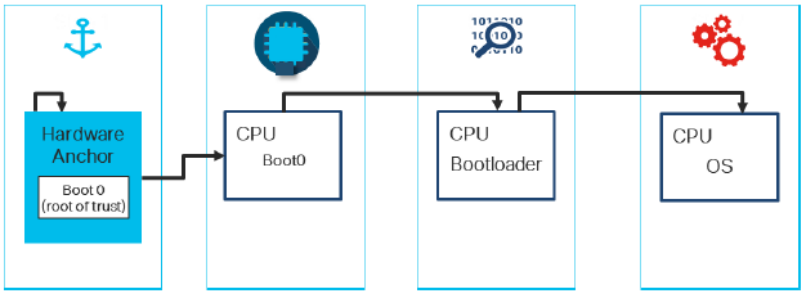
- 交易：用户对交易信息签名，发送交易请求到客户端后，客户端构造一笔有效交易并广播到链上的所有节点上。由于用户的公钥注册在链上，链上的各个节点都可以通过公钥验证这笔交易的合法性，交易合法才被允许上链。对于交易的迁移目标，需要做到目前运行传统签名算法的客户端，可与运行后量子密码签名算法的客户端兼容共存，并且预留出后量子密码算法的可扩展可插拔接口，以此快速应对未来后量子密码标准化的任何变化。
- 共识：共识机制本质上是用来验证添加到区块链上的交易数据。某一特定时间段，链上的某一节点会收到其它节点发送的共识消息和签名，该节点可通过其它节点的公钥信息进行

签名验证。与交易的迁移相似，共识的后量子密码迁移的重点也在后量子签名算法的适配上。

- 通信：区块链中各节点间通信使用 TLS 协议承载，节点既是客户端又是服务器。公钥密码算法在 TLS 通信上的使用范围集中在 TLS 的握手阶段。以 TLS1.3 为例，握手阶段主要包含两部分：密钥交换和认证。密钥交换方面，客户端和服务器通过询问得到通信双方支持的密码套件，以及使用密钥交换协议生成的预主密钥；认证方面，客户端和服务端会根据实际的认证需要，对对方的证书信息进行验证。对于通信的实际迁移应用，一方面要关注对 TLS 现用签名算法的迁移，这点与上述交易和共识同理；二要关注密钥协商算法的迁移，可以考虑使用后量子密钥封装机制来实现改造升级。

3.4 后量子可信启动

安全启动是一种用于保护设备系统正常加载、免受恶意软件攻击的技术。其基本原理是以一个信任根为基础，从设备加电起，至操作系统启动为止，逐步验证启动过程中每个阶段的数据和资源的数字签名，确保所有启动时加载的组件都是受信任的，并且没有被篡改或被恶意软件替换。安全启动的数字签名通常采用 RSA 等经典算法，难以抵抗量子计算机的攻击。安全启动过程如图所示。



图表 3 安全启动过程

思科提出将 HBS 后量子签名算法应用于 UEFI 安全启动的方案。HBS 后量子签名算法采用层级结构，多个层次结构对应多个级别的树。每个级别的树可以作为 UEFI 中平台密钥、密钥交换密钥或固件更新密钥的签名结构。每棵树的根作为 UEFI 允许签名数据库，用于验证固件和操作系统签名。每棵树用于对固件、固件包、平台密钥更新或者软件镜像做签名。

3.5 后量子安全存储技术

数据的可靠加密和有效访问控制是数据安全存储的重要环节，传统的数据加密存储和基于身份验证的访问控制技术，底层所依赖的对称加密算法和非对称加密算法均受到了量子计算技术飞速发展的巨大威胁，基于后量子加密算法并配合量子密钥体系构建的安全存储技术，成为了今后相当一段时间里提升数据抵御量子计算攻击能力和增强自身安全的有效措施。

后量子安全存储技术的涉及如下两点。一是通过量子随机数生成技术来生成所有加解密算法所依赖的加密密钥，并利用这些量子密钥来构建一个分级的加密密钥管理体系，对数据存储的身份识别，访问授权，数据加解密等操作提供分级保护的密钥源，通过分级密

钥保护机制来确保加密密钥的随机性和安全性。二是利用后量子算法来替换整套安全存储系统中所有的传统加解密算法，根据相应算法的需要配合上述加密密钥管理系统，共同构建一套数据加解密系统；确保数据在物理存储层和访问控制层的加密过程均能够有效抵抗量子计算的攻击。

目前后量子安全存储技术在后量子算法选择，后量子算法与量子随机数密钥结合以及后量子算法性能提升方面还处于摸索阶段，相信随着后量子算法自身的不断完善，后量子安全存储技术将在实用层面得到更大的应用和推广。

4. 后量子密码迁移研究

4.1 后量子密码迁移方案

后量子密码迁移不仅仅是替换密码算法，它还包括将密码协议、密码方案、密码组件、密码基础设施等更新为量子安全的密码技术，甚至还包括密码系统的灵活更新机制的能力构建及密码应用信息系统的迭代更新等，是将现有密码安全体系分阶段平稳过渡到后量子密码安全标准体系所需的一系列过程、程序和技术。

后量子密码迁移的整体工作基本包括:

- 后量子密码算法的理论研究及安全性评估工作
- 后量子密码算法及协议的标准化工作
- 后量子密码算法和协议的安全实现工作
- 后量子密码算法和协议与现有的密码产品或基础设施的集成工作
- 后量子密码算法的试点验证工作
- 后量子密码算法的部署及应用推广工作

考虑到后量子密码的复杂性以及稳定性，目前多数倾向于采用**“两把锁、双保险”**的混合模式进行过渡，而不是直接替换的模式。

4.1.1 混合方式

4.1.1.1 后量子密码与传统密码算法的混合

后量子密码与传统密码算法的混合使用，现阶段主要针对公钥密码算法的密钥交换和数字签名两种模式。

在后量子密码迁移早期采用混合密钥交换机制的方式，既能保留传统算法的安全性和监管约束力，又具备后量子安全的潜力。所以，混合密钥交换机制是在最终过渡到下一代算法之前的一个合适的方案。这个机制必须具备以下特点:

- **向后兼容性:** 具有“混合感知能力”的客户端和服务器;
- **高性能:** 使用混合密钥交换不需要过多的计算性能，这取决于所使用的特定加密算法的性能特征;
- **低延迟:** 使用混合密钥交换不应显著增加建立连接的延迟;
- **没有额外的交互:** 尝试协商混合密钥交换都不应该导致额外的交互;
- **最小的重复信息:** 尝试协商混合密钥交换不意味着必须发送多个相同类型的公钥。该方案同时基于 Diffie-Hellman 和某个候选的后量子密钥协商算法得到两个不同会话密钥，然后将两者混合推导出最终的会话密钥。这样可以显著降低潜在的风险，即使量子计算机成为现实，它也不可能攻破后量子部分的密钥，另外，如果在过渡期间发现后量子算法的安全问题，则 Diffie-Hellman 算法可以提供一层额外的保护。

对于真实性需求迫切，且使用数字签名算法的场景在后量子迁移早期采用混合签名的方式，再逐步过渡到纯后量子密码算法签名。同样的，混合签名机制也需具备向后兼容性、高性能、最小的重复信息等特点。并且针对混合机制的设计及实现时，要充分考虑密码的敏捷性和灵活性，进一步减小在迁移过程中的改造难度。

4.1.1.2 后量子密码与量子密钥分发的混合

QKD 和 PQC 是目前学术界公认的应对量子计算威胁的两个技术路径和方向。国际较为普遍的观点是 QKD 具有长效安全性，但缺少认证手段、应用成本相对较高；PQC 具有功能和应用体系与传统密码兼容的优势，但缺少安全性证明。将两个抗量子计算威胁的技术融合应用，可能是更为有效的方法。

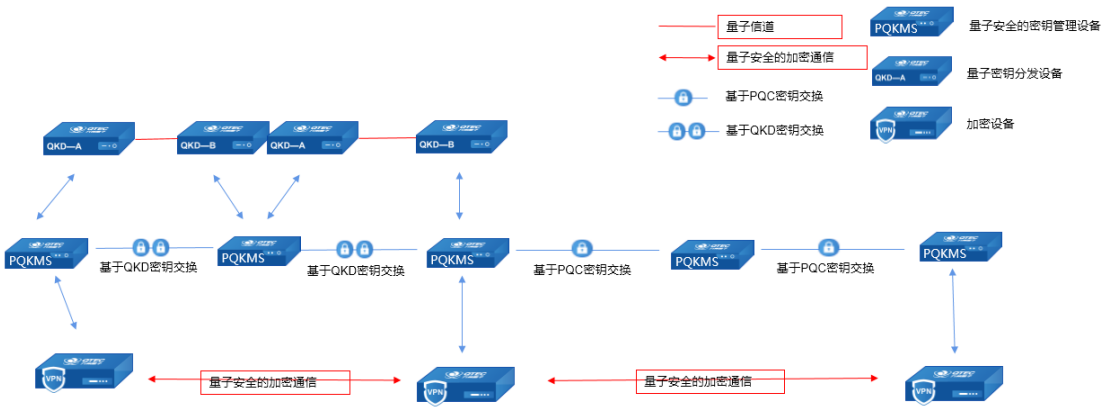
（1）QKD 增加基于 PQC 签名算法的设备认证

传统的 QKD 采用预共享密钥的方式来进行初始认证，每个配对 QKD 都需要存储其共享的身份验证密钥，面对规模网络中有大量节点需要相互认证的场景时，存在需预置大量密钥、管理维护不便的问题。**将基于格的 PQC 签名算法来实现 QKD 设备之间的认证，实现 QKD+PQC 的融合应用，进一步提升 QKD 网络的安全性和组网便利性。**采用哈希算法计算要认证的数据的摘要值，通信双方对摘要值根据 PQC 算法进行签名运算完成认证。将 PQC 认证协议集成到 QKD 设备内部，采用 PQC 认证后的成码率与原成码率相比误差保持在一定范围内，证明了融合方案对 QKD 性能并未产生明显影响。

（2）基于 QKD+PQC 的融合组网方案

QKD 大型组网使用需要光纤资源，受地理环境影响较大，应用成本相对较高，采用基于 QKD+PQC 融合组网的方式能有效降低成本。通过量子安全密钥管理设备将加密密钥传输从数据通道分离出来，并进入一个单独的密钥管理子系统，该子系统可以按需配置。

一个典型的融合网络配置由一系列的节点组成，其中一些节点与加密数据链路的加密设备通信，一些节点作为可信中继节点。存在成对 QKD 连接的量子安全密钥管理设备通过基于 QKD 完成密钥交换，不存在成对 QKD 连接的节点基于格的 PQC 密钥交换协议完成密钥交换。基于 QKD+PQC 的融合组网入下图表 4 所示。



图表 4 QKD+PQC 的融合组网方式

4.1.2 行业迁移策略

后量子密码迁移是一项庞大而紧迫的工程，这也就要求在后量子密码迁移工作中提早布局，安全设计，稳健迁移。后量子密码迁移与国密 SM2 算法升级有共同点，都是使用一种密码算法替换另外一种密码算法，可以借鉴前期 SM2 算法升级的策略进行迁移。后量子密码迁移与国密 SM2 算法升级也有明显的不同，SM2 升级时算法和标准均已经成熟，用户按照监管机构要求的时间点进行升级替换即可。而后量子密码算法的迁移动力，更多地来自于用户对自身业务系统安全性的考虑，而且目前算法和标准均未成熟，其推进过程

将会更加复杂。为了保证现有业务系统的安全性和合规性，试点机构进行后量子密码升级时需要制定出详细的迁移策略。

面对后量子迁移的紧迫形势，我们建议后量子迁移分三步走:

（1）**迁移准备**。 首先对业务系统的架构进行梳理，明确系统各部分所使用的加密算法类型，准确判断出后量子密码迁移所涉及的系统范围，包含所使用的密码技术特点（公私钥密文签名长度、安全参数等）、应用场景特点（数据包大小、关联关系、安全等级）等等，以此评估迁移的优先次序；然后是调研现有国内外主流的后量子密码算法，分析不同后量子密码算法安全性、密钥大小、延迟、带宽和适用场景，试验不同的后量子密码算法，并进行初步的功能和性能测试，以此评估后量子密码算法对系统运行的性能影响。

（2）**产品改造**。后量子密码算法标准颁布后，根据迁移的优先次序稳健迁移，并逐步引入后量子密码加密硬件，整体提升性能和安全性。待技术和标准成熟之后，在行业监管单位的带头下，先进行试点，再逐步推进推广，最终达成全产品、全系统的支持。

产品改造工作一：CA 发证机构数字证书基础设施改造

各 CA 发证机构首先需要对其数字证书相关的基础设施进行改造，使其底层支持后量子密码相关算法。只有这一步达成后，才具备面向全国推广新数字证书的基本条件。

产品改造工作二：发证类产品改造

需要 CA 发证机构与使用证书的单位密切配合，对证书发放类

产品进行调整，如电子签章类产品、证书发放管理类产品等。

产品改造工作三：证书应用类产品改造

在发证类产品兼容了后量子密码算法之后，再对证书应用类产品进行升级改造。例如，软件类的密码控件、加解密组件、通信组件、签名验签产品等，硬件类的网关、签名验签服务器、ukey 等，都需要支持存储和使用具备后量子密码功能的数字证书。

产品改造工作四：无证书公钥密码产品改造

证书相关产品改造完成之后，再对无证书公钥密码产品进行升级改造，确保所有涉及到公钥密码算法的产品全部支持后量子密码算法。

（3）**行业推广**。依据国密改造和信创改造的经验，行业可以首先在代表机构和典型场景进行试点推广，收集反馈信息，完善密码产品。在充分验证可行性后，再在各行业进行全面推广，以实现全方位的改造。

4.2 后量子密码迁移时间预测

目前能攻破当前在用的密码算法的量子计算机出现的时间仍然是未知的。美国兰德公司 2020 年的报告中“预测”平均情况下密码学相关量子计算机在 2033 年出现。德国 BSI“假设”密码学相关的量子计算机在 2030 年代中期出现。在 2023 年 2 月第 9 届 ETSI 量子安全密码学会议上，加拿大滑铁卢大学 Mosca 教授给出了其最新“预测”：RSA-2048 在 2030 年代初被攻破的乐观概率是 27%，与其

在 2016 年预测的 50%的概率相比，有所下调。尽管如此，业内的监管机构、标准化组织、企业等已对后量子迁移的必要性形成共识。如德国 BSI 在其 2020 年发布的后量子密码迁移指导中所阐述的：关于量子计算的“是否”与“何时”不再是问题，后量子密码将成为长期标准。**普遍认为后量子迁移将耗费 10 年以上，复杂 PKI 系统迁移时间或在 15 年以上。**

历史经验表明，密码系统的过渡需要较长的周期。ECC 早在 20 世纪 80 年代就被提出，尽管比 RSA 更高效，但它花了 20 多年才获得广泛的采用。NIST 的 SHA-3 密码早在 2007 年就宣布了，但到 2021 年仍然没有得到广泛采用。因此，密码系统的过渡（即使是比 PQC 简单得多的过渡）通常需要几年，甚至几十年。PQC 的过渡更为复杂，因为许多方法都是相对较新的，而且许多候选算法的性能与传统密码算法相比有很大差距。

目前，最为明确的迁移时间表为美国 NSA 发布的《商业国家安全算法套件 2.0》(简称 CNSA 2.0 或 CNSA 算法套件 2.0 版)。具体来说，对于软件和固件签名的场景，CNSA 2.0 推荐立即使用 NIST SP 800-208 所给出的基于 hash 的签名算法 LMS 和 XMSS。与基于格的后量子签名标准算法 Dilithium 和 Falcon 相比，这两个基于 hash 的签名算法的特点是私钥有状态，需要小心维护和更新。另外，单个私钥所支持的签名数量有限，而且签名和验签的速度慢。这使得它们可能不如无状态签名通用。关于对称算法，CNSA 2.0 推荐使用 AES 256，SHA384 或 SHA512。对于通用场景下的公钥算法，

CNSA 2.0 推荐用 Kyber 和 Dilithium 来代替 RSA、DH、ECDH 和 ECDSA，并且建议使用最高等级的 NIST Level 5 参数。但具体使用还涉及两个问题： 一是 Kyber 和 Dilithium 的正式规范还没有发布，所以最终标准化的参数和它们的第三轮文档有可能不一致，而且参数可能会增大以留出足够的安全边界。二是，按照 Kyber 和 Dilithium 第三轮文档，使用 Level 5 强度的参数会带来较高的成本，尤其是芯片面积/网络带宽等方面。不过 CNSA 2.0 针对的是美国国家安全系统，对于民用系统，特别是中、低安全的民用系统，可以根据安全需求和性能平衡选择更合适的参数。

对于不同场景下的后量子迁移时间线，CNSA 2.0 给出的要求如下：如表 5 所示，**美国政府将在 2033 年之前完成其信息系统中的后量子迁移**。其中，对于软件/固件签名场景的迁移，需立即启动，在 2030 年前完成；传统网络设备的迁移在 2025 年左右启动，也需在 2030 年前完成。

图表 5 美国 NSA 发布的 CNSA 2.0 迁移时间线

场景	支持和优先使用	完全使用
软件/固件签名	2025 年	2030 年
网络浏览器/服务器和云服务	2025 年	2033 年
传统网络设备（如 VPN、路由器）	2026 年	2030 年
操作系统	2027 年	2033 年
Niche 设备(如资源受限设备、大型 PKI 系统)	2030 年	2033 年
应用程序和遗留设备	2033 年前更新或替换	

在我国，金融行业是密码应用推广最早、重视程度最高的行业之一，当前我国的金融监管单位在推动金融机构的后量子密码迁移预研工作。**根据 SM2 证书体系迁移经验，在后量子密码算法相对成熟的基础上，从密码管理部门或者金融监管部门出具正式迁移通知开始到整个行业普及，总计时间预计需要 3 到 5 年。**详细时间预测如下:

（1）密码算法在理论上虽然可行，但实际应用到特定行业时，仍存在一些耗时的工作，比如技术实现方式、行业标准的统一以及各部门之间的协调沟通，这些迁移之前的准备工作预计持续 1 年以上。

（2）对于密码产品改造工作，由于产品体系庞大，密码和证书类产品在金融行业应用普遍且深入，而且还要考虑密码产品检测认证的时间周期，所以依据 SM2 改造的经验，整个过程可能持续 2 年以上。

（3）金融行业一般会采取先试点再全面推广的步调，预计从试点到基本普及（以核心业务 90%以上，非核心 60%以上）至少需要 3 年时间。不过，行业推广过程通常会与产品和系统改造同步进行，一般会存在轻微的滞后。

总体而言，以金融行业参考 SM2 证书体系迁移的经验为例，在后量子密码算法相对成熟后，从迁移准备到行业基本普及，最少需要 3 年，大概率是至少 5 年时间。

4.3 后量子密码迁移挑战

密码算法的推广部署总是充满挑战，涉及繁多场景和相互关联依赖的系统，往往新算法的部署和遗留算法的退出需要耗费数十年时间。在进行后量子密码迁移时需要全面考虑各种潜在风险，并制定相应的应对措施，以确保新系统的安全可靠性。

4.3.1 算法技术风险

首先，**在算法设计层面**，有些后量子密码只是当前尚不存在量子算法可以高效率地攻击它们，但是随着人们对量子算法的研究深入，未来是否会出现新的量子算法来攻破当前的后量子密码仍然是未知的。此外，由于目前的后量子密码算法大都是在近几年受标准化活动推动而设计的，密码分析的时间并不久，它们很多甚至还不能通过经典算法的攻击考验。例如，基于同源的 SIKE 算法在进入 NIST 标准化第四轮后一个月即受到严重攻击。类似情况对于其它算法也不能完全排除，这也是德国 BSI 力推基于无结构格的 FrodoKEM 和经历四十余年密码分析考验的 Classic McEliece 的原因。

其次，**在算法实现层面**，密码算法的实现和优化是一个复杂的问题，需要同时具备密码学专业知识和一定的工程能力，以避免在实现时引入漏洞。然而，后量子密码算法在数学结构上与传统的 RSA 和椭圆曲线离散对数类算法差异较大，引入了很多新型的、复杂的算子，因此，后量子密码算法的安全实现和优化有待继续探索。

最后，**在算法性能和兼容性层面**，实际应用中可能会遇到技术

成熟度不足、算法效率较低、加解密时间较长等问题，这些因素可能影响行业推进迁移的速度。在进行后量子密码迁移时，如果兼容性问题处理不当可能导致系统中断或数据丢失，给业务带来不稳定性，所以还需要兼顾现有密码体系和新体系之间的兼容性。

因此，在后量子迁移过程中，必须考虑到算法设计和实现带来的风险，以密码学敏捷的方式设计系统，以应对可能出现的突发情况。

4.3.2 法律合规风险

后量子密码在行业的应用涉及法规的变革，在电子签名上的迁移可能会带来法律合规方面的挑战。2005 年 4 月 1 日，我国正式颁布实施《中华人民共和国电子签名法》，其中明确规定，可靠的电子签名与手写签名或者盖章具有同等的法律效力。在日常生活中，电子签名拥有众多应用场景（电子保单、电子病历、电子成绩单和电子合同等）和庞大的应用规模。电子签名的安全性由公钥密码算法的安全性来保证，若广泛使用的公钥密码算法被破解，则基于这些算法的电子签名系统将完全崩溃，进而系统中被签名数据的完整性、签名行为的不可否认性均不能得到保证。为应对传统的公钥算法安全性问题带来的挑战，需对电子签名系统或应用进行 PQC 迁移。然而，在技术层面对长效电子签名进行 PQC 迁移，可能会面临法律纠纷或伦理方面的挑战。具体来说，若在迁移策略上采用“旧的旧办，新的新办”的策略，即旧签名证书继续支持已签署数据的有效性证明，新的数据则由新签名证书签署。那么以电子保险单为例，对于

一份由旧证书签名的电子保险单来说，由于旧签名算法已不再安全，电子认证机构无法判定保险单是否被篡改冒签过，所以无法出具认证证明并为此担责，进而可能会引起法律上的纠纷。若采用“以旧换新”的策略，即撤销算法不安全的证书，重新签发新证书，使用新证书重新签署旧证书已签名的数据，首先，无法保证毫无遗漏地将数以亿计的签名全部召回；其次，以电子病例为例，若一份电子病历的患者本人已去世或失联，家属是否有代签权、家属拒绝签署该如何处理，类似的很多问题目前都暂无答案，处理不当可能会引起法律上的纠纷或伦理问题。

4.3.3 迁移成本巨大

应用传统密码算法的产品及服务多种多样，已广泛应用并深刻影响着我们的生产和生活，产品及服务向 PQC 的迁移会面临迁移成本大的挑战。

首先，无法在线进行算法升级的大规模应用产品的 PQC 迁移面临迁移周期长、迁移成本大的挑战。比如我国的居民二代身份证中使用的是 SM2 算法，由于身份证的特殊性，对其进行平滑迁移是维护公共安全和社会稳定的基本要求。对二代身份证的 PQC 迁移需涉及到将数以亿计的二代身份证全部召回或者发布新一代身份证，对如此大规模的应用产品进行平滑的 PQC 迁移需要大力协调和组织，迁移周期和成本是一个巨大挑战。

其次，部分产品或服务的 PQC 迁移可能会使产品或服务面临性

能降低甚至不适用的的挑战。比如，对边缘计算来说，高价值边缘计算对时延以及带宽的要求相对较高，且部分边缘设备的硬件资源相对较弱。然而，PQC 算法与传统算法尤其是椭圆曲线离散对数类算法比较，具有更大的密钥、密文及签名，这将明显增大存储和传输开销，进而对边缘设备和云端之间数据的快速流动造成了一定的阻碍。此外，PQC 算法在硬件中部署时芯片面积和功耗的增加以及侧信道防护带来的成本使得其对边缘计算设备具有较高的要求，使边缘设备对 PQC 算法的兼容能力造成一定的挑战。

4.3.4 人员储备不足

PQC 迁移需要高度专业化的人才，然而目前我国密码学人才稀缺。2020 年，据统计我国每年培养的密码学专业人才仅上千人。2021 年，有网络媒体估计现阶段我国对密码人才需求人数 30 万人左右，实际人才缺口 20 万人。此外，目前密码人才供需仍存在层次上的不平衡，相关人才培养多集中于密码基础理论和算法协议设计方面，密码工程人才偏少，了解一个或多个行业信息化应用的密码工程人才则更为稀少。因此，在密码应用体系面临大规模 PQC 迁移的背景下，**密码人才的培养和需求不平衡问题对 PQC 迁移造成了一定的挑战**。

4.3.5 标准的专利风险

前期，我国积极参与国际后后量子密码标准的征集活动，但是国际上基础算法标准目前由美国 NIST 主导，并有欧盟大力配合，我国在国际密码标准组织上不占优势，很难取得主动权。

一是 NIST 选定的首批 PQC 标准算法中，几乎所有 LWE 技术路线的格密钥封装算法均有专利风险。LWE 技术路线的专利风险比较分散，分散在多个国家、机构和个人，极有可能存在尚未浮出水面的专利，也能对后续的 LWE 技术路线标准化构成威胁。首先提及的是，目前为止至少有 3 个专利对 Kyber 的应用产生阻力。

第一个是美国专利 9094189[14]，为法国国家科学院所持有，专利有效期持续到 2032 年。目前几乎所有 LWE 技术路线密码方案所使用的“带噪音 Diffie-Hellman+协调”的框架都受到该专利的影响，包括 Kyber、Saber、NewHope、Aigis、LAC、AKCN-MLWE 在内的国内外大部分 LWE 算法。事实上，不仅是 LWE 技术路线，NIST 第四轮评估的基于编码的 PQC 算法 BIKE/HQC/Classic McEliece 同样使用了类似的构造框架。在更广泛的范围之内，该专利对这些算法也存在着威胁。

第二个是美国专利 9246675[15]，为丁津泰教授所持有，专利有效期持续到 2033 年。该专利能够影响到 LWE 技术路线的密文压缩机制。事实上，为了降低通信带宽，包括 Kyber 在内的 LWE 算法会对两项密文进行压缩处理，不过每个算法所采用的压缩方法不同。谷歌曾于 2016 年开展 CECPQ1 实验，将 NewHope 算法嵌入到 TLS 1.2 测试性能，但几个月后因为该专利的原因，谷歌不得不终止 CECPQ1 实验。

第三个是中国专利 107566121[16]，为复旦大学赵运磊所持有，专利有效期持续到 2032 年。该专利提出一类高效的秘密共识方法，

而诸如 Kyber、Saber 等算法所采用的协调机制均是该专利的具象化。

专利风险对后量子密码应用造成迟滞和威胁。目前美国 NIST 的专利谈判仅取得如下进展:（1）专利授权仅对最终标准化的算法，对算法参数和结构的变化都不在授权范围之内。（2）NIST 主要关心 Kyber 等算法在美国应用的专利风险，无法确保 Kyber 在美国之外地区的使用不存在专利风险。（3）相关专利的授权是有条件的。在美国标准细节没有确定之前，商业领域不敢应用 Kyber，即便在标准公布后，在其它国家也有潜在专利风险，这导致在商业领域基于 LWE 技术路线的后量子密码应用存在严重的迟滞。

需要重视的是，LWE 技术路线的专利问题不仅影响到 PQC 算法的实际应用，可能也会对更大范围基于 LWE 技术路线的全同态加密 FHE 以及其它高级密码协议带来专利风险。

二是将现有的经典算法（例如 ECC）过渡到 PQC 算法的迁移路径也存在专利的影响。企业大规模应用的 CA 证书一般只应用某一种经典算法（例如 RSA 或 ECC），但是为应对量子计算的威胁，企业还需要一个支持 PQC 的证书，这就是混合证书方案，混合证书的关键特征之一是能够同时支持经典密码系统以及已升级的后量子密码系统。当使用者开始将其经典密码系统和应用程序迁移到后量子安全时，他们不需要支持两个单独的 PKI（一个用于传统证书，一个用于后量子安全证书），因为它们已经拥有二合一的混合证书。然而位于加拿大的 ISARA 公司将上述方案申请成 4 个专利，分别是美国专利 US9660978、美国专利 US9794249、国际专利

WO2018027300 和日本专利 JP6644894。目前，ISARA 公司已经将这 4 个专利授权给 NIST，并允许 NIST 合法合规地使用这些技术。但这也侧面反映了，即使 NIST 标准化某些 PQC 算法之后，从经典算法过渡到 PQC 算法的路径上也存有潜在的专利威胁或风险。

部分后量子路线的产品已受到出口管制。2018 年起，新版瓦森纳协议已经将基于格上困难问题、随机解码问题和同源困难问题这三类困难问题的密码技术列入出口管制清单。因此，在国内想要获取格、编码、同源密码算法相关的商业产品，或者与国外研究者进行商业合作，将受到出口管制的约束，需要申请相关的出口许可证。

5.后量子密码发展建议

5.1 强化政策顶层设计

呼吁国家及时制定向后量子迁移的顶层设计和规划。在全球大国战略竞争中，后量子密码技术产业已经成为全球关注的焦点。建议国家相关部门牵头制定后量子相关顶层规划和指导文件，负责统筹 PQC 项目规划、技术推动、标准制定、迁移方案研究和试点以及后续的产业落地等全方面的工作，制定后量子准备路线图、技术清单，组织产业链上下游共同推动后量子迁移事宜。

5.2 加强自主技术储备

加大对后量子密码理论研究和应用的投入。国内团队对后量子密码的研究起步较晚，清华大学王小云院士团队是国内较早开始研究的人员，大约在 2006 年启动了对格密码的研究。虽然经过国内研究者十几年的奋力追赶，国内的学术团队在算法设计、算法分析、安全性证明等方面出现了很多优秀的成果，并且在密码领域的国际顶会上发表。但是总体上，我国在后量子密码领域还缺乏引领领域发展的研究能力，需要继续加大对理论研究和应用实践的投入。

推动 PQC 各领域技术的研发和落地实用。在后量子密码技术领域，进行自主技术储备已成为非常迫切的任务。目前，欧美企业如英特尔、高通等已经部署了很多后量子密码硬件实现相关的专利和产品，国内相关企业也需要加大投入，尤其是在芯片领域。建议企业、高校科研院所组成研发联盟，共同研究 PQC 应用技术及其优化方法，从性能、存储、抗侧信道攻击等方面研发 PQC 算法的新型快

速安全实现技术，开发升级现有的密钥防护系统，克服技术与实际应用之间的融合问题，推动 PQC 各领域技术的落地实用。

5.3 推动标准体系建设

加快推进我国自主可控的后量子密码算法标准制订工作。目前我国还没有后量子密码相关的商密标准和监管规范或指导，亟需加快推进我国自主可控的后量子密码算法标准制订工作，完善后量子算法及配套应用的相关标准，使国内企业后量子迁移有规范可以参照。在后量子密码标准和迁移被美国列为制衡中国崛起的优先事项和战略抓手的背景下，我国应该有效反制甚至反超，中国的后量子密码标准制订坚持质量优先，同类型的算法应力争在安全及综合性能上具有国际竞争力，通过技术先进性引领实现国际上更大的采用率，避免发生中国的后量子标准主要由中国应用的局面。同时要注意避免把所有鸡蛋放在一个篮子里，鼓励多种技术路线，从而有效避开专利风险。

探索建设后量子密码相关的认证体系。目前国际上尚无后量子密码相关的认证，但法国 ANSSI 在其报告中提及未来在签发产品的 security visa 时将考虑到后量子算法的使用，TCG 组织也为英飞凌公司推出的含后量子签名 XMSS 算法的 TPM 芯片颁发认证。可以推测，在标准建设完成后，各国监管机构、国际行业组织将推出相关的认证体系。建设完善相关的认证体系，对后量子密码算法的产品化至关重要。

5.4 构建密码迁移生态

联合产业各方，逐步构建有序的后量子密码迁移生态，布局新的战略性蓝海产业。后量子迁移工作需要社会各方面的合作，只靠一家或少数企业解决迁移的所有技术问题是不现实的，需要监管部门的引导推动、供应商的支撑、客户迁移意识的培养、行业甚至全产业迁移生态的建立和完善，社会各界协调好步伐，才能进展到商用落地阶段。通过创建后量子迁移生态联盟的形式，集中后量子迁移生态产业链上下游的力量，建设好国内的后量子迁移生态圈，提前布局新的战略性蓝海产业。在算法标准化的同时，生态各方配合开发后量子密码算法开源库、自动分析和报告平台、后量子迁移项目验证落地等，以有序和自动化的方式推进迁移工程。

5.5 健全密码人才队伍

创新人才培养模式，推进产学研协同的人才培养模式。支持密码学科专业建设，开设后量子密码算法设计、分析等理论和工程课程，举行密码竞赛、攻防比赛等实践活动，鼓励企业与高校、科研院所进行项目落地合作，培养擅长理论懂算法设计的研究型人才、掌握标准熟悉技术开发的复合型人才、懂政策法规有密码知识背景的管理型人才、懂原理会操作的应用型人才等各类密码人才队伍。

参考文献

[1] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994: 124-134.

[2] Elaine Barker. National Institute of Standards and Technology Special Publication 800-57 Part 1,Revision 5,170 pages, May 2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5.

[3] National Strategic Overview for Quantum Information Science, Sept. 2018. https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf.

[4] The National Quantum Initiative (NQI). https://www.quantum.gov/about/.

[5]CANS 2.0: Announcing the Commercial National Security Algorithm Suite 2.0. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF.

[6]https://www.whitehouse.gov/wpcontent/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[7] Preparing for Quantum-Safe Cryptography, version 2.0. NCSC, Nov. 2020. https://www.ncsc.gov.uk/pdfs/whitepaper/preparing-for-quantum-safe-cryptography.pdf.

[8] Federal Ministry of Education and Research. Self-determined and Secure in the Digital World 2015-2020, The German Government's Research Framework Programme on IT security, March 2015.

[9] Quantum-safe cryptography - fundamentals, current developments and recommendations. Federal Office for Information Security, Germany, May 2022.

[10] Federal Ministry of Education and Research. Quantum Technologies – From Basic Research to Market, A Federal Government Framework Programme. September 2018.

[11] ANSSI views on the Post-Quantum Cryptography transition. Released on March 2022.https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf.

[12] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.

[13]

[14] https://patents.google.com/patent/US9094189B2.

[15] https://patents.google.com/patent/US9246675B2.

[16] https://patents.google.com/patent/CN107566121A.

联系方式：

中国信息通信研究院 云计算与大数据研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

邮箱：cpii@caict.ac.cn

网址：www.caict.ac.cn