美国加速推进后量子密码标准体系建设的战略启示

美国在后量子密码领域动作频频，显示出其正在加快推进后量子密码的标准化和应用进程，以应对量子计算带来的安全威胁。我国应当密切关注美国 PQC（后量子密码）标准化进程的特点与经验，加快布局标准体系、双线推进、应用试点，加速推进自身后量子密码标准体系建设。

文 | **高旖蔚 彭璐 樊炳辰** 中国电子信息产业发展研究院未来产业研究中心

一、美国布局后量子密码标准呈现三大突出特征

美国后量子密码标准化进程展现了卓越的前瞻性和严谨性。NIST（美国国家标准与技术研究院）后量子密码标准的制定过程可概括为“三步走”战略。第一阶段（2015—2017 年）着重前期布局，NIST 启动后量子密码学讨论，公布 PQC 标准化工作路线图，通过组织研讨会、发布报告和公开征集算法，广泛汇集全球智慧。第二阶段（2017—2021 年）聚焦评审筛选，采取多轮严格筛选和基准测试，历时近 5 年从初始征集的来自 25 个国家的 82 个算法中遴选出最具潜力的候选方案。第三阶段（2022—2024 年）致力于标准确定和发布，经过 4 轮筛选最终确定 4 种入选算法，截至 2024 年 12 月已发布 3 种算法正式标准。NIST 自 2016 年年末启动的标准化进程历时近 8 年，其系统化、长期性的科学评审过程展现了美国在密码学领域的战略前瞻性和科学严谨性，奠定了其在后量子密码中的引领地位。

美国的后量子密码标准涵盖多种技术路线。2022 年 7 月，NIST 经过对算法各种应用场景的全面考量，最终确定 4 种适合后量子加密迁移的算法，包括用于安全、网站加密的 CRYSTALS-Kyber 算法，以及 3 种专注于数字签名软件安全的 CRYSTALS-Dilithium、Falcon 和 SPHINCS+ 算法。CRYSTALS-Kyber 作为密钥封装机制（KEM）算法适用于安全网站加密等一般加密场景，具有相对较小的加密密钥，双方可以轻松交换，保证了较为高效的运行速度。对于适用于数字

表 1 美国后量子密码标准制定的“三步走”战略

阶段	年份	具体事项
阶段一：前期布局	2015	4 月：NIST 举行“后量子世界网络安全”研讨会，启动后量子密码学讨论。
	2016	2 月：NIST 首次宣布了其 PQC 标准化工作的路线图； 4 月：发布 NISTIR 8105 报告——《后量子密码学报告》，奠定后量子密码学研究基础； 12 月：NIST 向全球征集 PQC 算法提案，正式拉开了 PQC 标准化项目的序幕。
	2017	11 月：NIST PQC 标准化流程提交截止； 12 月：第一轮候选算法公布，开始公审和评选。
阶段二：评审筛选	2018	4 月：举办第一次 NIST PQC 标准化会议，推进标准化讨论。
	2019	1 月：第二轮候选算法公布，进一步缩小候选范围； 8 月：第二次 NIST PQC 标准化会议，深化标准化研究。
	2020	7 月：第三轮决赛候选算法和备选候选算法公布，开始公审和评选； 10 月：算法团队提供调整方案的最后期限。
	2021	4 月：发布后量子密码学采用挑战白皮书《为量子密码学做准备：探索采用与使用后量子密码算法的相关挑战》； 6 月：第三次 NIST PQC 标准化会议举行，NCCoE 发布项目描述草案。
阶段三：确立发布	2022	7 月：宣布将被标准化的候选算法及第四轮备选候选算法； 11 月：第四届 NIST PQC 标准化会议举行。
	2023	8 月：NIST 发布 3 种 PQC 算法标准草案：FIPS 203、FIPS 204、FIPS 205； 12 月：发布特别出版物（SP）1800-38B《量子就绪：密码发现》和 1800-38C《量子就绪：测试互操作性和性能标准草案》，提供测试计划和兼容性问题解决方案。
	2024	4 月：举办第五次 NIST PQC 标准化会议； 8 月：发布最终 PQC FIPS； 12 月：公布 Falcon 算法标准草案。

来源：中国电子信息产业发展研究院未来产业研究中心

签名的 3 种算法，CRYSTALS-Dilithium 和 Falcon 基于格密码学，后者主要作为前者的补充，适用于需要更小签名的应用；SPHINCS+ 基于哈希函数，比其他两种算法更大更慢，但作为一种备用算法很有价值，适用于对安全性要求高的场景。2024 年 8 月 13 日，NIST 发布了上述其中 3 种算法的标准，ML-KEM（以前称 CRYSTALS-Kyber）、ML-DSA（以前称 CRYSTALS-Dilithium）和 SLH-DSA（以前称 SPHINCS+）。美国多元化的标准选择确保了在不同应用场景下的适用性，同时为未来密码学发展提供多样化技术储备，有效降低单一算法可能存在的安全风险，为应对未来新型攻击方法预留技术空间。

美国后量子密码标准的制定展现了政府和产业间的全面协同与持续推进。在政府层面，NIST 作为主导机构与商务部、国土安全部、国防部等多个政府部门密切合作，共同推进标准的制定和实施，包括组建公开工作组、建立“向后量子密码学迁移项目”、开展跨部门指导和风险评估、制定量子准备路线图等措施。此外，美国出台多项政策推进政府信息体系向 PQC 迁移，并积极和产业

界合作促进PQC的商业化与产业化发展。在产业层面，大型科技公司、初创企业和安全行业公司积极投入研发力量，推动技术创新和产业化。IBM、微软等公司成立后量子密码学联盟，促进PQC在商业和开源技术中的全球采用；谷歌在Chrome中添加对后量子加密支持，并推出首个开源的后量子FIDO2安全密钥；初创公司QuSecure实现首个实时、端到端后量子加密通信星链，SandboxAQ推出端到端安全套件协助组织向PQC过渡。NIST发布首批后量子加密标准后，产业界迅速响应。2024年9月，微软立即在其开源核心加密库SymCrypt中引入ML-KEM算法，随后谷歌宣布将Chrome中的实验性Kyber替换为标准化的ML-KEM。政府的主导作用与产业界的积极响应形成良性互动，确保PQC标准的适用性和实施效果，为未来密码学标准的无缝更新奠定了基础。

二、当前推进后量子密码三条路径

秉持“PQC+QKD”双线并行推进策略，构建可靠的量子安全网络解决方案。为应对量子计算威胁，量子密钥分发（QKD）和PQC已成为量子加密通信的唯二解决路径，其中，PQC因其软件算法的简便性，相比QKD具有更高的经济性。目前，美国在PQC方面已展现一定应用先发优势，美大型科技公司和金融机构如谷歌和汇丰银行已开始采用PQC技术。2024年2月，谷歌采用NIST的PQC算法，推出首个开源量子弹性FIDO2密钥。综合来看，据美国电子电气工程学会IEEE Specturm观点，QKD提供了理论上的信息安全，而PQC实现了可扩展性，两者融合是未来量子安全网络最有可能的解决方案。为应对量子计算威胁，应立足QKD基础，最大程度秉持工程化、小型化原则，合理参考美国在PQC领域的低成本方案和实践经验，推动“PQC+QKD”双线并行和融合发展，促进全球量子加密通信技术的广泛应用。

加速标准制定，跟进后续发展进程。2024年8月，NIST正式发布PQC前3条标准，其时间跨度长，涵盖前置部署、审查、迁移等多阶段，逐步成为政府承包商的强制性标准。其中，IBM、Quantum Xchange等量子计算公司已宣布，将支持并采用NIST的最新PQC标准及迁移建议。在全球范围内，部分国家或地区的PQC研究较美国起步晚，若使用NIST的标准算法，存在巨大的专利成本，且易被“卡脖子”。基于此，应加快推动PQC标准化制定工作，探索迁移并入相关国际或区域通用的密钥标准体系，以促进全球量子加密通信技术在统一且合理的标准框架下不断发展演进，实现更广泛的应用与技术创新的协同共进，为全球量子安全网络的构建提供有力支撑与保障。

积极探索PQC迁移方法，加快推动试点应用。当前，诸多国际知名企业如IBM、谷歌、苹果等正逐步推进后量子密码产业化发展，并在实践中验证后量子密码的有效性。例如，IBM已将NIST前期征集的CRYSTALS-Kyber和CRYSS-Dilithium算法应用在Z16大型机中；

谷歌云在传统密码的基础上叠加使用了后量子密码NTRU-HRSS，强化云上数据安全；苹果引入后量子加密技术对其iMessage通信平台进行升级，成为迄今为止最大规模的后量子密码应用案例。目前，后量子密码落地场景尚有待进一步丰富拓展，亟须针对不同行业特点制定基于PQC的迁移安全策略，扎实推进后量子密码商业化落地，带动大规模应用，以点破面，撬动应用格局。

三、对我国的启示建议

完善顶层规划，系统布局PQC发展战略。一是组建专委会。在密码行业标准化技术委员会框架内，成立国家PQC标准制定专委会，汇聚政府、科研和产业界精英，统筹推进标准制定、技术研发和迁移部署工作。二是制定PQC标准前瞻性发展战略和实施路线图。制定短期（1～2年）、中期（3～5年）和长期（5～10年）的关键节点计划，循序渐进推进标准由推荐性到强制性演进，建立健全PQC标准实施的监督和评估机制，确保标准的有效落地。三是深化关键技术趋势研判与布局。聚焦国际前沿技术难题，突破高性能、高安全性的PQC核心算法，在国家重点研发计划中新增后量子密码相关专项，适时启动量子信息赛道未来产业创新任务揭榜挂帅工作。

双线并行，推进密码标准兼容与创新。一是深入研究美国NIST公布的PQC标准。组建专门的技术团队分析美量子标准的技术特点、安全性和实用性，开展仿真测试评估NIST标准在我国网络环境的实用性，在确保安全的前提下考虑适当兼容并制定兼容测试规范。二是坚持走出具有中国特色的PQC发展道路。加大对国产PQC算法的研发投入，融合QKD发展现状，研发适合我国国情的双线并行标准体系，充分考虑现有密码基础设施和应用环境，制定切实可行的过渡和迁移方案。三是加强与国际标准化组织（ISO）的沟通与合作，积极参与国际PQC和QKD标准制定，推进我国标准进入国际标准体系，提升我国在全球量子密码领域的话语权。

加快应用试点，促进产业化发展。一是推动后量子密码在多行业、多维度的应用落地。整合高校、科研院所和龙头企业优势资源，实施后量子密码应用推广计划，率先在金融、电信、能源、医疗等关键领域优先开展PQC应用试点，采取“边试验、边反馈、边完善”的迭代式发展模式，推进后量子密码技术基础设施迭代更新与应用部署。二是鼓励龙头企业牵头组建PQC产业联盟，参与标准制定和迁移工作。推动上下游企业协同创新，加快形成完整的产业链和生态系统。三是加强量子行业发展生态建设。支持PQC基础研究和应用开发，构建对PQC算法、终端产品和解决方案进行全方位审查的安全评估机制，构建高水平、多层次量子人才引培体系。

责任编辑：孙姗姗　投稿邮箱 zhouhl@staff.ccidnet.com