光子盒
QUANTUMCHINA

量子准备：向后量子密码的迁移

2024/06

目录

目录

图表目录

声明

01 本报告体现的内容和阐明的观点力求独立、客观，本报告中的信息或所表述的观点均不构成投资建议，请谨慎参考。

02 本报告旨在梳理和呈现2023年1月1日至2024年2月29日内全球与PQC产业领域发生的重要事件，涉及数据及信息以公开资料为主，以及对公开数据的整理。并且，结合发布之时的全球经济发展状态，对短期未来可能产生的影响进行预判描述。

03 本报告重点关注2023年1月1日至2024年2月29日间量子细分行业发生的相关内容，以当地时间报道为准，以事件初次发布之时为准。

04 本报告版权归光子盒所有，其他任何形式的使用或传播，包括但不限于刊物、网站、公众号或个人使用本报告内容的，须注明来源（2024量子准备：向后量子密码的迁移 [R]. 光子盒. 2024. 03）。
本报告最终解释权归光子盒所有。

05 任何个人和机构，使用本报告内容时，不得对本报告进行任何有悖原意的引用、删减和篡改。未经书面许可，任何机构和个人不得以任何形式翻版、复制、发表、印刷等。如征得同意进行引用、转载、刊发的，需在允许范围内。违规使用本报告者，承担相应的法律责任。

06 本报告引用数据、事件及观点的目的在于收集和归纳信息，并不代表赞同其全部观点，不对其真实性负责。

07 本报告涉及动态数据，呈现截至统计之时的情况，不代表未来情况，不够成投资建议，请谨慎参考。

引言

PQC，即Post-quantum Cryptography。这一密码体系，在美国国家标准技术研究所（NIST）的推动下，越来越多地受到来自各界的关注和重视。这一词汇，也预示着一个新信息时代即将到来。尽管当前量子计算机尚未颠覆现有密码体系，但考虑到潜在的量子计算威胁，信息可能在当下被存储，待未来量子计算技术发展到一定程度时将被解密。因此，现在就需要加强对PQC的关注，需要了解PQC的发展现状，以便在合适的时机做出正确的决定。

本报告主要针对近期全球PQC主要的参与国、参与研究单位等核心参与者的信息进行收集和梳理，力求呈现出当前PQC领域的发展现状。本报告覆盖密码算法、通信协议、硬件实现等领域，呈现全球PQC研究的多样性和创新点，助力读者理解PQC技术的发展方向。本报告还深入挖掘了PQC在各领域的具体应用案例，揭示其在解决实际问题中的独特价值。通过这些实际案例，为读者展现PQC技术在现实社会中的潜力和广泛应用。

通过这份报告，我们致力于为读者提供全球PQC领域的全景视角，提供更深入的理解，并把握这一快速发展的前沿技术领域。

Part 1

各方PQC标准化工作

PQC标准化制定的重要性在于，确保不同厂商PQC方案之间的互操作性和安全性，推动PQC技术的商业化应用和广泛采用，以便顺利地完成从经典密码体系向PQC的过渡。美国是诸国中，标准化进程走得最快的。除了美国，英国、德国、法国、中国、日本和韩国等国家在量子计算领域也相当重视，也开展了PQC相关工作，这也推动了PQC标准化制定。

美国NIST PQC标准化

早在2016年2月，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）在日本福冈举行的第七届后量子密码国际会议（PQCrypto 2016）上公布PQC标准化工作时间表。同年4月，NIST发布一项跨部门报告（NIST Interagency Report 8105，名为Report on Post-Quantum Cryptography），这份报告旨在获得更广的人士对这件事的评论。报告介绍了PQC发展现状、量子计算硬件发展现状，以及未来开展标准化工作的初步计划。随后，在2016年12月，NIST发布了PQC算法征集提案，正式启动PQC标准化项目。从2017年第一轮PQC算法征集至2022年第四轮候选人公布，经过四轮严格筛选，最终于2023年8月公布三种算法的标准草案，经过公众审查后预计于2024年7月正式公布第一批三项PQC算法标准。

图 1　NIST主导的PQC项目时间线

来源：NIST，光子盒

PQC标准草案的发布标志着在应对量子计算威胁方面有多种可供选择的解决方案。已发布标准草案的三种算法分别为CRYSTALS-Kyber、CRYSTALS-Dilithium和SPHINCS+，第四份PQC标准草案FALCON预计将在2024年公布。CRYSTALS-Kyber算法用于保证消息传输的安全性，而CRYSTALS-Dilithium和SPHINCS+则进一步保证消息的真实性与完整性。

CRYSTALS-Kyber是一种先进的密码算法，它是为了在未来保护我们的数据免受量子计算机的威胁而设计的。这种算法基于两个主要的数学概念：格理论[1]和多语言学习密钥封装机制[2]（Multilinear Learning Key Encapsulation Mechanism，ML-KEM），用于通过公共通道进行通信的两方之间建立共享密钥。NIST之前已经发布了一些密钥封装机制（KEM）的标准，比如SP-800-56A和SP-800-56B，而CRYSTALS-Kyber则是基于这些标准的首个具体的密钥建立方案。简而言之，它是一种新的技术，用来帮助人们在不安全的网络上安全地交换秘密信息。

CRYSTALS-Dilithium是基于格理论的数字签名[3]方案，其安全性基于在格中查找短向量的难度[4]。该算法在密钥和签名等方面具有较为平衡的安全性能[5]，并且其密钥生成能力、签名和验证效率在实际应用验证中表现较好。

SPHINCS+是基于无状态哈希[6]的数字签名方案，其安全性依赖于底层散列函数安全性的假设，即SPHINCS+的安全性依赖于其底层哈希函数的安全性。这意味着只要哈希函数是安全的，SPHINCS+也就是安全的。2023年8月，SPHINCS+算法更名为SLH-DSA，为便于理解、保持一致性，本报告仍称其为SPHINCS+。

表 1　2023年NIST发布标准草案中的算法及技术

算法名称	草案名称	技术
CRYSTALS-Kyber	FIPS 203草案	基于格理论的密钥封装机制标准
CRYSTALS-Dilithium	FIPS 204草案	基于格理论的数字签名标准
SPHINCS+	FIPS 205草案	基于无状态哈希的数字签名标准

注：FIPS是联邦信息处理标准（Federal Information Processing Standards）
来源：光子盒整理

在会议方面，美国于2023年8月召开第14届后量子密码学国际会议，此次会议包括以下主题：基于代码的密码学；同构密码学；基于格的密码学；多变量密码学；量子算法、密码分析和模型；后量子协议；以及密码侧信道分析和对策。

[1] 格理论是一种数学理论，涉及高维空间中的点阵结构。在密码学中，利用这些结构可以创造出很难被破解的密码系统，特别是对抗强大的量子计算机。
[2] 多语言学习密钥封装机制是一种用于安全地传输密钥（即密码的一部分）的方法。它让两个通信方在公共通道（如互联网）上交换信息时，能够建立一个只有他们知道的共享密钥，从而实现安全通信。
[3] 数字签名就像是电子版的个人签名或印章，用来证明信息的真实性和来源。在数字世界中，签名用来确保信息是由特定的人发送的，并且在传输过程中未被篡改。
[4] 这个算法的安全性基于一个特定的数学问题——在一个复杂的格中找到短向量的难度。这个问题被认为是非常困难的，即使是对于量子计算机来说。
[5] 在多个方面都表现出良好的安全性能。这包括它生成的密钥（用于验证签名的唯一代码）和签名本身的安全性。
[6] 哈希函数是一种算法，可以将任何数据转换成固定大小的值或字符串。在密码学中，哈希函数用于确保数据的完整性。无状态指的是在签名时，不需要维护关于之前签名的信息。

Part 1

各方PQC标准化工作

PQC标准化制定的重要性在于，确保不同厂商PQC方案之间的互操作性和安全性，推动PQC技术的商业化应用和广泛采用，以便顺利地完成从经典密码体系向PQC的过渡。美国是诸国中，标准化进程走得最快的。除了美国，英国、德国、法国、中国、日本和韩国等国家在量子计算领域也相当重视，也开展了PQC相关工作，这也推动了PQC标准化制定。

加拿大PQC标准化

加拿大于2023年3月举办了第一届PQC会议，就目前PQC所面临的算法、应用、性能、迁移等方面难题进行了讨论。会议就后量子密码学的许多最棘手的方面进行了各种演讲和小组讨论，包括算法、实现、性能和迁移。演讲人包括NIST计算机安全部门的科学家Rene Peralta，Entrust软件安全架构师Mike Ounsworth，ETSI量子安全密码学和安全主席、AWS的高级首席工程师Matthew Campagna，Bosch后量子密码学安全研究工程师Sebastian Paul，加拿大网络安全中心密码安全和系统开发总监Melanie Anderson等。

英国PQC标准化

英国国家网络安全中心（NCSC）于2020年发布了《准备量子安全密码学》（Preparing for Quantum-Safe Cryptography）。2023年9月，第二届牛津PQC峰会在英国牛津举办，会议聚集来自学术界、工业界和不同标准化机构的PQC领域的顶尖研究人员和从业者，举行两部分组成的峰会，讨论NIST的PQC标准草案及附加签明等的演讲。2023年11月，NCSC官网发表的白皮书，面向公共部门、大型组织、网络安全专业人员，旨在帮助商业企业、公共部门组织和关键国家基础设施提供商的系统和风险所有者思考如何为向后量子密码学的迁移做好最佳准备。

德国PQC标准化

德国联邦信息安全办公室（BSI）与承包商罗德与施瓦茨网络安全有限公司（Rohde & Schwarz Cybersecurity GmbH）开展了“通用密码库的安全实施”项目。该项目建设了Botan密码库，到2023年，Botan密码库已发展到3.0版本。德国政府决定启动对公共管理基础设施进行紧急的量子安全转型行动以及美国的量子准备指令（Quantum-Readiness Directives）政策的最新进展。

法国PQC标准化

第九届ETSI/IQC量子安全密码学活动于2023年2月在法国ETSI总部召开，此次会议汇聚了工业界、学术界和政府相关的量子密码学人才，并声明ETSI将继续向量子安全标准化历程努力。

Part 1

各方PQC标准化工作

PQC标准化制定的重要性在于，确保不同厂商PQC方案之间的互操作性和安全性，推动PQC技术的商业化应用和广泛采用，以便顺利地完成从经典密码体系向PQC的过渡。美国是诸国中，标准化进程走得最快的。除了美国，英国、德国、法国、中国、日本和韩国等国家在量子计算领域也相当重视，也开展了PQC相关工作，这也推动了PQC标准化制定。

美国

加拿大

英国

德国

法国

中国

日本

韩国

荷兰

国际机构

中国PQC标准化

在PQC研讨会议方面，中国多次举办PQC相关会议，强调PQC产业的发展以及推动国内PQC产业链上下游的共同努力。2023年3月，中国信通院“密码+”应用推进计划CPII量子计算组召开《后量子密码应用研究报告》研讨会，旨在探讨目前PQC算法、应用实现及迁移等多方面面临的难题。中国信息安全标准化技术委员会在2023年5月召开后量子密码技术与创新实践研讨会，围绕PQC领域前沿技术、研究动态及发展趋势等方面进行探讨，推动了PQC标准化设立以及应用实施。清华大学丘成桐数学科学中心、北京雁栖湖应用数学研究院主办的第三届雁栖湖国际后量子密码标准化与应用研讨会暨后量子技术成果发布会于2023年7月在北京召开，共同商讨国际PQC标准化进展与面向行业领域的PQC迁移工作。2023年8月，中国密码学会量子密码专业委员会举办中国密码学会2023年量子密码学术年会，旨在汇聚国内量子密码领域中专业人才，共同探讨量子密码领域各方向的主要问题、最新成果、技术动态及发展趋势等，促进量子密码学术科技领域相互交流与合作。2023年12月，2023 抗量子密码研究与工程实现技术论坛在京功举办。会议聚焦抗量子密码技术，分享抗量子密码技术的发展与经验，研讨抗量子密码工程实现与安全应用。

在PQC组织方面，2023年7月21日，后量子密码技术研讨会暨校企联合研究中心揭牌仪式在上海市静安区市北高新商务中心举行。中国复旦大学与格尔软件公司建立校企合作，成立“后量子密码技术校企联合研究中心”，聚焦后量子密码设计与软硬件实现、后量子密码云服务器和后量子VPN的研发、后量子密码应用示范和产业迁移、融合发展等6个研究方向。台湾于2023年8月1日成立量子安全迁移中心（Quantum Safe Migration Center，QSMC）。该研究中心将充当政府、工业界、学术机构和国际研究人员之间的桥梁，解决后量子安全以及相关的客户安全问题，预计很快将发布后量子安全蓝图。该研究中心得到了众多致力于信息安全加强的著名组织或利益团体的支持，包括数字台湾圆桌会议（Digital Taiwan Roundtable，DTR）、信息产业研究院（Institute for Information Industry，III）和工业技术研究院（Industrial Technology Research Institute，ITRI）等。中国抗量子密码战略与政策法律工作组于2024年1月成立，工作组将对抗量子密码技术、产业、业务的现状和相关国内外政策、法律法规进行研究，以公开或定向方式发表抗量子密码相关蓝皮书、要报、专题研究报告等成果。

日本PQC标准化

日本积极研究并推进PQC研究与分析，为应对未来量子计算机对经典密码学的挑战做准备。2023年3月，SandboxAQ及MITRE企业共同在日本东京举办主题为现实世界的PQC大会，此次大会汇集了产业、学术界与标准化机构，深入探讨PQC算法融入现有网络、协议和系统过程可能面临的挑战，并分享PQC最新研究、算法现状等。2023年3月，日本信息通信研究机构（NICT）发布消息称，NICT与日本凸版印刷株式会社正在合作研究PQC。双方在NICT运营的试验床——保健医疗用长期安全数据存储交换系统（H-LINCOS）中，建立了一个兼容PQC的私有证书颁发机构，验证了篡改检测功能的有效性。

韩国PQC标准化

2021年，国家安全研究所（NSR）和国家情报院（NIS）成立了韩国后量子密码学 （KpqC） 研究小组。旨在加强国家后量子安全，以对抗量子计算的兴起， 韩国有关PQC方案标准的KpqC竞赛自2022年4月开幕，2022年11月完成第一轮竞赛评选，共有7个密钥封装机制（KEM）候选者和9个数字签名候选者。2023年12月，4个KEM算法和4个数字签名算法已晋级第二轮。

此外，KpqC研究小组在2023年7月计10月分别举办了第六届和第七届PQC研讨会，共同探讨:KpqC竞赛算法分析结果及改进方法。2023年8月，KpqC研究小组举办了第二届PQC学术会议。

Part 1

各方PQC标准化工作

PQC标准化制定的重要性在于，确保不同厂商PQC方案之间的互操作性和安全性，推动PQC技术的商业化应用和广泛采用，以便顺利地完成从经典密码体系向PQC的过渡。美国是诸国中，标准化进程走得最快的。除了美国，英国、德国、法国、中国、日本和韩国等国家在量子计算领域也相当重视，也开展了PQC相关工作，这也推动了PQC标准化制定。

美国

加拿大

英国

德国

法国

中国

日本

韩国

荷兰

国际机构

荷兰PQC标准化

PKI联盟为举办机构的第二届PQC会议在2023年11月于荷兰举行，此次会议深入探讨了PQC的治理和监管框架；强调迁移到PQC算法对于保护关键数字基础设施、数据和通信的重要性；探索经典算法和PQC算法之间的差异等。

国际机构

互联网工程任务组（Internet Engineering Task Force，IETF）于2023年1月成立了后量子加密工作组（Post-Quantum Use In Protocols，PQUIP），旨在协调加密协议的使用。2023年7月，IETF批准英国网络安全公司Post-Quantum提出和设计的量子安全虚拟专用网络（VPN）的新标准。此标准规定了VPN如何在量子时代安全地交换通信，VPN新标准将互操作性放在首位，允许使用不同公钥加密算法的各方相互通信，使多种PQC和经典加密算法被纳入VPN成为可能。

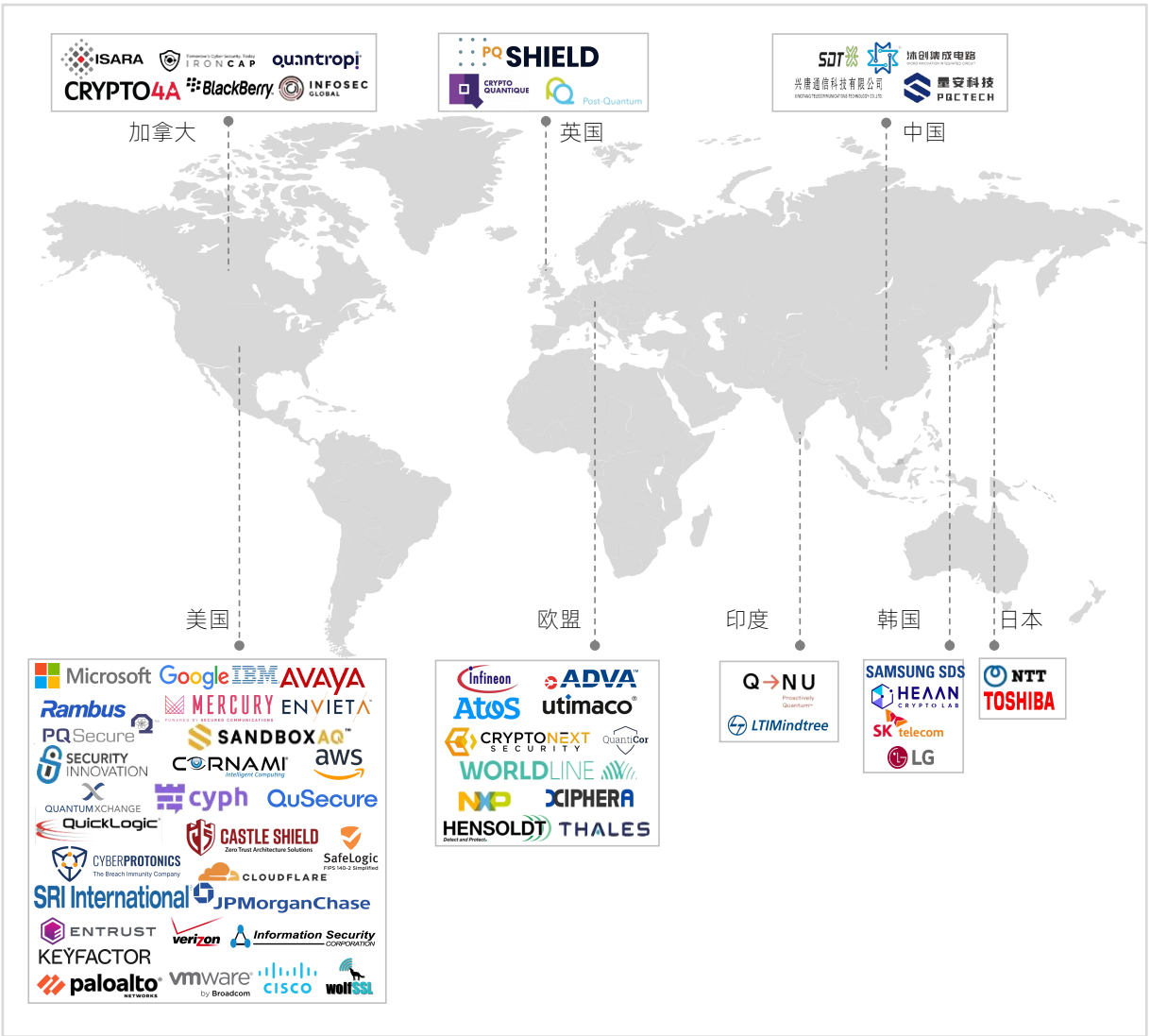
全球移动通信协会（GSMA）在2023年2月发布《后量子电信网络影响评估白皮书》（Post Quantum Telco Network Impact Assessment Whitepaper）概述了PQC算法、各机构迁移时间表以及如何在电信生态系统中引入和保持PQC的量子抗性和加密敏捷性。随后，GSMA又在2024年2月发布《后量子加密-电信用例指南》（Post Quantum Cryptography-Guidelines for Telecom Use Cases），此报告提出了一种分阶段的PQC迁移方法，允许对所需的操作进行优先排序，可用于支持电信生态系统中量子安全加密。

2023年9月，由PQC技术人员、研究人员和专家从业者组成的团体为推动美国NIST推行的PQC标准化算法理解及采用发起了PQC联盟（PQC Coalition）。创始联盟成员包括美国公司IBM Quantum、Microsoft、MITRE、SandboxAQ，英国PQShield以及加拿大滑铁卢大学。

欧洲International Cryptographic Module Conference 23（ICMC23）会议于2023年9月召开，会议由Cnxtd Event Media Corp.会议部门主办。此次会议聚焦于如何从RSA这类经典密码方法过渡到PQC，并讨论建立PQC标准的重要性以及公共和私人部门实施PQC迁移的具体策略。此外，在此次会议上专家们展示了PQC的首次实际应用，以及为端到端服务和硬件芯片实施PQC的方法，讨论了PQC领域的争议和未来发展趋势。

全球PQC公司总部地理分布在美国、欧盟、中国的公司分布较为密集。此外，加拿大、英国、日本、韩国、印度等国家也有公司参与PQC研究，并提供PQC产品或服务。从企业业务来看，美国IBM、Microsoft、Google等全球科技巨头将公司业务拓展至PQC领域，其中Google已应用PQC算法保护其旗下Chrome浏览器网络安全。印度QNu Labs公司以NIST的PQC标准工作为参考，开发基于格的PQC算法，提供Hodos产品服务。

图 2 全球PQC标准化参与者-公司



来源：光子盒整理

全球PQC科研机构以高校为主。中国参与PQC领域的科研机构较多，但实现商业化转型的机构仍然有限。主导PQC标准化的NIST机构位于美国，基于此优势，美国多个科研机构孵化出PQC初创公司，转型商业化。此外，欧盟、英国、加拿大、日本等国家也有较多PQC科研机构。

图 3 全球PQC标准化参与者-科研机构

来源：光子盒整理

为了迎接未来数字时代和量子计算相关的安全挑战，多地设立研究中心加强对数字时代中存在的各种安全威胁的研究与解决方案的开发。

表 2　2023年新建企业级PQC研究中心

时间	地区/区域	相关机构	标准工作
2023.07	中国	后量子密码技术校企联合研究中心	研究中心旨在通过格尔软件与复旦大学的校企合作，在后量子密码技术研究和产业落地这一事关国家安全的关键领域，共同打造下一代后量子密码技术产学研融合发展的“上海名。
2023.08	中国台湾	量子安全迁移中心	亚洲第一家提供可抵御量子计算机攻击的加密系统的机构，助力台湾过渡到后量子密码系统。

来源：光子盒整理

PQC相关的会议为学术界、产业界和政府部门提供了一个共同探讨PQC最新进展、研究动态和应用实践的平台。

表 3　2023年PQC研讨会议

时间	举办地点	会议名称	举办机构
2023.03	加拿大	后量子密码学会议 (Post-Quantum Cryptography Conference)	公钥基础设施联盟 (PKI consortium，PKI联盟)
2023.03	日本	现实世界的PQC (Real World PQC)	SandboxAQ、MITRE
2023.03	中国	《后量子密码应用研究报告》编写的启动会&第一次研讨会	中国信通院“密码+”应用推进计划CPII量子计算组
2023.08	中国	中国密码学会2023年量子密码学术年会	中国密码学会量子密码专业委员会
2023.08	美国	第14届后量子密码学国际会议 (The 14th International Conference on Post-Quantum Cryptography PQCrypto 2023)	Joint Center For Quantum Information And Computer Science（QuICS）、马里兰大学的研究所
2023.09	欧洲	ICMC23	Cnxtd Event Media Corp.
2023.09	英国	第二届牛津后量子密码学峰会 (2nd Oxford Post-Quantum Cryptography Summit 2023)	PQShield，牛津大学，巴里大学，内梅亨大学，马克斯普朗克安全与隐私研究所
2023.11	荷兰	第二届PQC会议	PKI联盟

来源：光子盒整理

Part 2

PQC政策及投融资分析

政策分析

投融资分析

政策分析

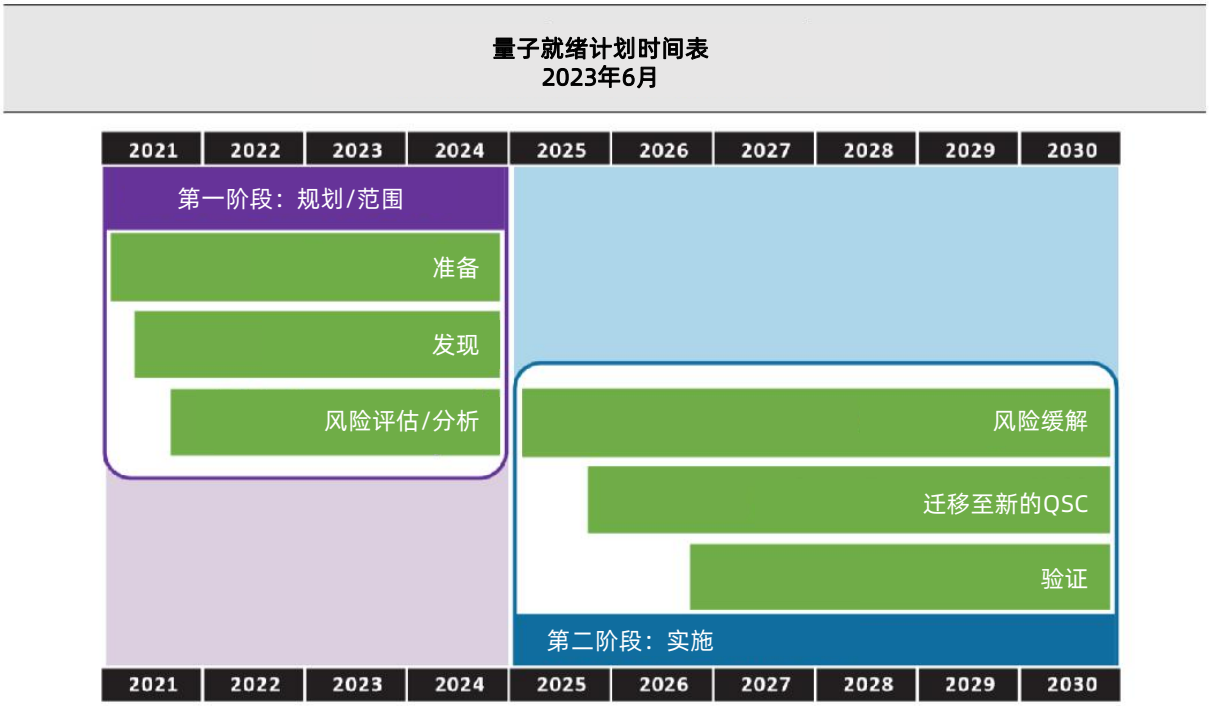
美国方面，在NIST公布第一批PQC标准算法之后，美国采取了量子时代以来最大的有关量子安全防范的工作，于2022年11月正式完成《量子计算网络安全方案法案》制定，为联邦政府提供PQC迁移支持。随后，相继出台多个政策推进政府信息体系向PQC迁移以及PQC相关技术的研发与应用。并且，美国政府积极与产业界合作，促进PQC在量子通信安全技术的商业化和产业化发展。2023年9月，国家网络安全中心（NCCoE）发布的《向后量子密码学迁移》文件中概述了PQC迁移面临的挑战及目标，并表明美国信息科技巨头IBM、微软、谷歌等公司均为政府PQC迁移的技术供应商。2023年12月，NIST发布的《迁移到后量子密码学量子准备：密码学发现》（Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery）草案概述了功能测试计划，要求使用加密工具查找数字网络中的错误安全配置。并且描述了用例场景，为演示成功的后量子系统迁移提供了使用场景。此草案表明支持PQC迁移第一步是确定在企业中使用公钥加密的位置和目的，然后识别并准备可迁移的资产（如硬件和软件）清单，这一部分网络安全框架的核心功能，也是任何组织有效管理网络安全风险的基本先决条件。另一个草案《迁移到后量子密码学量子准备：测试标准草案》（Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards）中强调了如何协调量子弹性算法与现有网络基础设施，并提供了受控的非生产环境中兼容性问题的解决方案，以及PQC算法与现有基础设施的协调融合问题并提供了兼容性的解决方案。该草案提出了两个专注于PQC迁移工作挑战的具体方面：识别易受量子攻击的系统和测试PQC算法的互操作性和性能。

中国方面，上海市科学技术委员会于2023年9月发布《2023年度“科技创新行动计划”区块链关键技术攻关专项项目指南的通知》。其中，一专项项目目标在于应对量子计算机对区块链等公钥密码系统带来的现实威胁，突破适用于区块链系统的后量子数字签名算法，完成后量子密码算法经典安全性和量子安全性量化评估的自动化工具。此项目包含两个研究内容：（1）设计并开源基于哈希的后量子数字签名算法，相较于国际上SPHINCS+等同类算法，在同等安全强度的提前下，签名大小改进不少于10%，满足区块链通用密码算法接口规范，适配多种典型共识算法并进行原型验证。（2）设计并开源基于格的后量子数字签名算法，相较于Dilithium等同类算法，在同等安全强度的前提下，公钥和签名大小改进不少于10%，计算效率提升不低于30%，满足区块链通用密码算法接口规范，适配多种典型共识算法并进行原型验证。该专项研究计划的执行期限为2023年12月1日至2025年11月30日，每项研究内容拟支持不超过1个项目，投入专项资助经费不超过200万元。企业牵头申报时，企业投入研发经费与申请资助经费之比不低于1:1。

荷兰国家通信安全局于2023年3月发布了《PQC迁移手册:迁移到后量子加密的指南》，指南中提供了开始制定迁移策略的具体及可操作的步骤。

加拿大方面，2023年1月创新、科学和经济发展部（ISED）发布加拿大国家量子战略，制定了三项关键使命。其中一项为通过国家安全量子通信网络和PQC计划，确保加拿大在量子时代中的隐私和网络安全。同时，加拿大学术界、工业界、非营利性机构以及政府部门高度重视PQC的开发和采用。量子准备工作组（QRWG）是加拿大数字基础设施弹性论坛（CFDIR）的五个工作组之一，于2023年发布了第三版《加拿大国家量子准备：最佳实践和指南》（Canadian National Quantum-Readiness: Best Practices and Guidelines）。该文件概述了三个PQC用例（通过KERBEROS、PKI/Cas、sFTP进行身份验证），以及PQC清单、加密性用例和PQC供应商路线图和第三方评估清单。

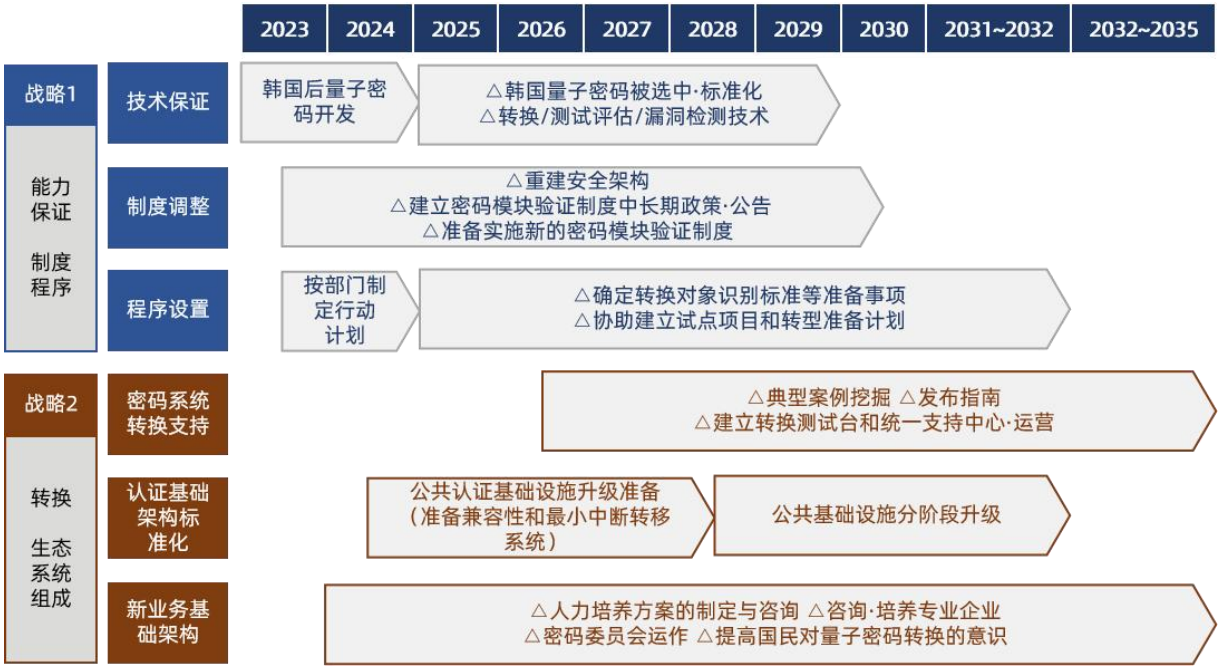
图 4 加拿大量子准备计划时间表



来源：Canadian National Quantum-Readiness: Best Practices and Guidelines [R], 2023.

韩国方面，由国家情报局（국가정보원과）和科学技术信息通信部（과학기술정보통신부）发布的PQC密码学总体规划《为量子转型时代做准备》表明，将在2035年之前将其国家密码系统转变为PQC。此规划包含三个总体目标：第一，在技术获取、制度完善、程序制定等六个方面制定详细的行动计划，为2024年向国家中长期密码系统过渡确立政策方向；第二，成立“泛国家密码系统过渡推进小组”，为到2030年实现向PQC系统过渡奠定基础；第三，到2035年建立向PQC过渡的技术和政策支持体系，并实施安全密码系统。

图 5 韩国国家密码向PQC的过渡规划



来源：信息通讯新闻

表 4　2023年全球主要PQC参与国发布的政策情况

时间	地区/区域	发布机构	政策名称	政策内容
2023.01	加拿大	加拿大创新、科学和经济发展部	国家量子战略（National Quantum Strategy，NQS）	国家量子战略（NQS）制定了三项关键使命，以确保加拿大保持在量子创新和领导地位的道路上。其中一项为通过国家安全量子通信网络和后量子密码学计划，确保加拿大人在量子世界中的隐私和网络安全。
2023.03	美国	白宫	国家网络安全战略（National Cybersecurity Strategy）	优先考虑后量子加密、数字身份解决方案和清洁能源基础设施等下一代技术的网络安全研发。
2023.03	荷兰	国家通信安全局	PQC迁移手册:迁移到后量子加密的指南（The PQC Migration Handbook: GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY）	提供了开始制定迁移策略的具体及可操作的步骤。
2023.06	加拿大	量子准备工作组	加拿大国家量子准备：最佳实践和指南（Canadian National Quantum-Readiness: Best Practices and Guidelines）	概述了三个PQC用例以及PQC清单、加密性用例和PQC供应商路线图和第三方评估清单。
2023.07	韩国	国家情报院和科学技术信息通信部	为量子转型时代做准备（양자대전환시대대비）	将在2035年之前将其国家密码系统转变为后量子密码。
2023.08	美国	美国网络安全与基础设施安全局、美国国家安全局、NIST	量子准备：迁移到后量子密码学（Quantum-Readiness: Migration to Post-Quantum Cryptography）	制定量子就绪路线图的建议、准备有用的加密清单的步骤、了解和评估供应链的注意事项、组织应如何与其技术供应商讨论后量子密码，并明确了技术供应商的责任。
2023.09	美国	国家网络安全中心	向后量子密码学迁移（Migration to Post-Quantum Cryptography）	概述了向后量子密码学迁移项目的背景、目标、挑战、好处和工作流程，此外NCCoE还列出了参与该项目的最新28家技术供应商名单。其中包含IBM、微软、亚马逊等头部企业。
2023.12	美国	NIST	迁移到后量子密码学量子准备：密码学发现 草案（Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery）	描述了用例场景，为演示成功的后量子系统迁移提供了使用场景。
2023.12	美国	NIST	迁移到后量子密码学量子准备：测试标准 草案（Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards）	强调了如何协调量子弹性算法与现有网络基础设施，并提供了受控的非生产环境中兼容性问题的解决方案

来源：光子盒整理

Part 2

PQC政策及投融资分析

政策分析

投融资分析

投融资分析

2023年共有4家PQC企业获得了不同程度的融资。包括瑞士QRCrypto、英国Crypto Quantique、杭州量安科技、法国Cryptonext Security，其中Crypto Quantique及量安科技未披露融资金额。

2023年获得投资的企业中，有两家均为A轮融资，表明PQC领域目前仍处于发展成长阶段，具有潜力和挑战并存的特点。通过研发和投资，这些企业已经开发出具有一定竞争力的PQC算法或产品，并开始在市场上进行推广和应用。这一阶段的成功融资将为企业进一步的技术研发和市场拓展提供资金支持。其次，A轮融资也表明PQC领域仍面临一些技术和商业上的挑战。虽然PQC被认为是防范“先存储，后解密”威胁以及应对未来量子计算威胁的关键技术，但目前其在实际应用中的效果和可靠性尚未得到充分验证。最后，PQC技术的标准化和产业化进程也需要进一步推进，以便更好地满足市场需求。未来随着技术的不断进步和市场需求的不断提升，PQC领域有望迎来更加广阔的发展前景。

表 5　2023年PQC企业投融资情况

时间	企业	国家	融资金额（万美元）	融资轮次	投资者
2023.05	QRCrypto	瑞士	50.00	Convertible loan	Toshiba Corporation
2023.07	Crypto Quantique	英国	未披露	Grant	European Innovation Council（EIC）
2023.09	杭州量安科技	中国	未披露	A	海越资管，余杭国投，银杏谷资本
2023.11	Cryptonext Security	法国	1199.00	A	AXA Venture Partners，Ventures

注1：由于该阶段汇率波动较大，本次换算按1：7进行
注2：本表仅统计在PQC领域的初创企业在2023年1月至2023年12月的投融资情况
来源：光子盒整理

Part 3

PQC商业化成果

PQC过渡方案

PQC产品

PQC过渡方案

多个量子通信公司相继提出PQC解决方案，定制并不断优化PQC解决方案，以满足不同行业和组织的特定需求。目前，IBM、WISeKey、SoftBank等公司均聚焦于PQC解决方案的研究，为企业及政府数据安全提供更高水平的保障。

日本软银公司于2023年2月成功完成经典密码与PQC算法的技术融合，并与美国SandboxAQ公司合作完成对此次混合技术的验证并确认此项混合技术可应用于现有商业网络，助力企业完成PQC过渡。

IBM在2023年5月年度Think大会上推出了量子安全路线图，以帮助政府和企业完成量子安全加密工作以及PQC迁移。IBM量子安全路线图概述了PQC过渡步骤并提供了三个独立产品帮助美国联邦机构及企业向量子安全过渡。IBM量子安全路线图中包括IBM Quantum Safe Explorer、IBM Quantum Safe Advisor、IBM Quantum Safe Remediator三个独立产品，帮助组织机构完成PQC过渡过程中的发现、观察和转换工作。

2023年6月，WISeKey子公司SEALSQ开发了基于人工智能的PQC量子解决方案，此方案在安全硬件平台MS6003上实现了NIST公布的Kyber和Dilithium CRYSTAL算法，创建了第一个抗量子演示器。

在PQC安全性评估方面，阿联酋技术创新研究所密码学研究中心推出了CryptographicEstimators开源软件库。CryptographicEstimators有助于公钥方案设计者选择安全参数，并支持密码分析专家对其研究结果与已建立的基准进行对比评估。此外，与仅评估单一类别的安全假设（例如基于格的假设）类似项目不同， CrypgraphicEstimators 的目标是全方位的PQC安全基础，目前包括多元和基于代码的问题及其一些变体。研究人员还可以轻松扩展该库，以适应各种其他类型的密码假设。

表 6　2023年1月至2024年2月期间的PQC过渡方案

时间	国家	相关机构	研究进展
2023.02	日本 美国	SoftBank Corp、SandboxAQ	软银（SoftBank）公司成功完成对以椭圆曲线密码（ECC）为代表的经典加密算法与PQC算法的技术混合。该公司通过与美国SandboxAQ的合作完成对该混合组合技术的概念验证，并确认它可以以最小的影响应用于现有网络，帮助企业进行PQC过渡。
2023.03	法国	Quandela、CryptoNext	两家公司利用量子计算和PQC方面的独特技术和专业知识，开发了完全集成的量子安全解决方案。
2023.04	美国	QuSecure、RedHat	QuSecure的后量子网络安全技术在Red Hat Enterprise Linux、Red Hat OpenShift和Red Hat Ansible自动化平台上得到支持支持应用，可以抵御现代网络威胁。
2023.05	美国	IBM	推出IBM Quantum SafeRoadmap以及技术组合，以简化并实现全面迁移，保护政府和企业关键数据安全。
2023.06	瑞士	WISeKey、SEALSQ	WISeKey子公司SEALSQ开发了基于人工智能的PQC量子解决方案，此方案在安全硬件平台MS6003上实现了NIST公布的Kyber和Dilithium CRYSTAL算法，创建了第一个抗量子演示器。
2023.09	阿联酋	阿联酋技术创新研究所密码学研究中心	推出了世界上第一个开源的CryptographicEstimators软件库，完全用于评估PQC方案的安全性，包括密钥交换方法、公钥加密和签名。

来源：光子盒整理

Part 3

PQC商业化成果

PQC过渡方案

PQC产品

PQC产品

由于PQC产品的使用与推广受到技术挑战、公众认知程度、标准化问题、安全性测试等多方面的影响，导致PQC产品的推进仍旧步履维艰。目前PQC产品处于初期发展和探索阶段，多为企业研发与测试。同时PQC产品应用也具有一定的局限性，主要为端到端的安全加密。

在完全基于PQC的产品方面，通过在硬件、算法等方面进行广泛的研究和实验，引领PQC技术的前沿。

法国Atos子公司Eviden于2023年4月发布首个“后量子就绪”（Post-quantum ready）数字身份解决方案，该方案包括两个产品，IDnomic PKI及Cryptovision GreenShield。IDnomic PKI是一个多用途公钥基础设施软件套件，用于生产和发布可信数字身份，符合最高安全标准。IDnomic PKI 采用加密敏捷设计，通过为传统和“后量子加密就绪”应用程序颁发混合证书，确保为客户提供顺畅的迁移路径。Cryptovision GreenShield为电子邮件和文件加密解决方案，获准用于交换机密信息（欧盟和北约限制，EUCI，VS-NfD 认证），由德国 BSI 认证并由欧洲理事会批准。该产品的架构是模块化和灵活的，基于加密敏捷开发。美国QuSecure公司于2023年6月推出QuProtect软件，并被亚马逊认定为合格软件，可以通过亚马逊品牌及其生态系统进行分销。2023年9月，QuSecure宣布其PQC产品已通过美国总务管理局（General Services Administration，GSA）提供的多重奖励计划（Multiple Award Schedule，MAS）。标志着QuSecure产品符合美国国家标准与技术研究院认可的标准和认证，并且可以通过PQC算法为政府用户提供抗量子保护，无缝集成到现有的政府IT基础设施中。GSA计划可以直接接触世界上最大的商品和服务买家美国联邦政府，并且使QuSecure能够更轻松地为州和地方政府以及公立学校、拥有领先的PQC技术。GSA的联邦服务计划可以使QuSecure直接接触世界上最大的商品和服务买家，即美国联邦政府，获得长期合作机会和简化的采购流程。并且QuSecure能够更容易地获取州和地方政府以及公立学校的PQC需求，从而提供相应服务。中国沐创在2022年7月就已推出抗量子攻击的商用密码芯片PQC 1.0，此芯片支持NIST发布的第三轮入选算法。基于此，沐创于2024年1月又推出了可迁的移抗量子密码芯片S20P。

在集成产品方面，2023年9月，芬兰公司Xiphera宣布与美国半导体公司QuickLogic建立合作伙伴关系，在QuickLogic的eFPGA（嵌入式的现场可编程门阵列）架构上实现Xiphera的xQlave®的PQC IP核以实现量子安全加密。2024年1月，英国EnSilica公司在其eSi-Crypto系列硬件加速器IP中增加两个PQC加速器。此次PQC加速器分别应用了CRYSTALS Dilithium和CRYSTALS Kyber两种算法。EnSilica的新型产品使用许可证现已授予一家大型半导体公司，用于制作高性能5纳米网络芯片。

在PQC安全评估方面，Thales与Quantinuum合作发布PQC入门套件，可加速在安全环境中测试量子弹性措施的过程。该套件将NIST的预标准化PQC算法与Quantum Origin结合，最终作为可信的Luna HSM解决方案。

量子计算领域企业也纷纷进入PQC领域，投身PQC研究与应用。中国图灵量子与其子公司天机量子共同推出抗量子加密芯片，此芯片是基于量子随机数、国密算法和抗量子算法的高性能抗量子加密芯片。专注于光量子芯片的国光量子基于公司已有的量子随机数芯片，推出了PQC+QRN抗量子算法应用新模式。

表 7　2023年1月至2024年2月期间的PQC产品

时间	国家	相关机构	内容
2023.04	法国	Eviden	发布首个“后量子就绪”数字身份解决方案，该解决方案由 PQC 驱动，包括 IDnomic PKI 和 Cryptovision Greenshield 两款网络安全产品
2023.06	美国	QuSecure、亚马逊	软件供应商QuSecure宣布其软件PQC已被Amazon Web Services (AWS)认定为合格软件；QuSecure还获得了称号，凭借这一称号，QuSecure现在可以利用AWS品牌和生态系统来加强其分销工作。
2023.09	美国、芬兰	QuickLogic、Xiphera	Xiphera宣布与QuickLogic Corporation建立合作伙伴关系，在QuickLogic的eFPGA架构上实现Xiphera的xQlave®量子安全加密IP核。
2023.09	中国	国光量子	结合自研量子随机数（QRN）芯片，推出PQC+QRN抗量子算法应用新模式。
2024.01	中国	沐创集成电路设计有限公司	沐创推出首款可迁移抗量子密码芯片RSP S20P。该芯片除了支持更多算法外，还可广泛应用于包括PCIE密码卡应用、SSL协议加速、IPSEC协议加速、安全网关、可信计算、安全存储等领域。
2024.01	英国	EnSilica	EnSilica公司在其eSi-Crypto系列硬件加速器IP中增加两个PQC加速器，包括：eSi-Dilithium（一款硬件IP），用于加速名为CRYSTALS Dilithium的NIST FIPS 204模块晶格数字签名算法；eSi-Kyber（一款硬件IP），用于加速名为CRYSTALS Kyber的NIST FIPS 203密钥封装机制（KEM）。
2024.01	法国、美国	Thales、Quantinuum	Thales与Quantinuum合作，推出PQC入门套件，可加速在安全环境中测试量子弹性措施的过程。该套件是通过功能模块将NIST的预标准化PQC算法与Quantinuum的Quantum Origin结合在可信的Luna HSM中的解决方案。
2024.01	中国	图灵量子、天机量子	图灵量子召开了2024年首场新品发布会并举办“量子安全 护航未来”主题沙龙。图灵量子及天机量子带来了自主研制的抗量子加密芯片，也展示了以自主研发基于量子隧穿效应的量子真随机数打造量子密钥系列产品，以抗量子密码及国产商用密码技术打造云、管、端全生态、多场景的下一代密码安全的软硬件产品矩阵。

来源：光子盒整理

Part 4

PQC实际应用

政府&国防

金融

通信

政府&国防

美国联邦政府、美国陆军、美国国防信息系统局、法国投资总秘书处等机构均开始寻求PQC服务，以确保敏感数据的安全性。并且在PQC领域，政府和军事机构开始倾向于与私营企业合作，私营企业通常拥有更快的创新速度和更灵活的研发能力，因此通过合作可以更快地获得最新的PQC解决方案。

在美国方面，QuSecure企业一直处于为美国政府提供PQC解决方案的最前沿。2022年7月，美国政府选择了QuSecure公司的QuProtect解决方案来保护美国空军、美国太空军和北美航空航天防御司令部使用的遗留系统中的加密通信数据。2023年6月，美国陆军授予QuSecure公司一份小型企业创新研究第二阶段合同，为陆军用户开发基于PQC的加密技术和解决方案，并确定如何在战术边缘使用量子技术。SandboxAQ企业也致力于为美国政府部门提供PQC解决方案。2023年6月，SandboxAQ企业获得美国国防信息系统局提供的合同，提供端到端的PQC管理解决方案。2024年1月，QuSecure又获得美国空军创新中心（AFWERX）授予的小型企业创新研究（SBIR）合同，空军部（DAF）将使用QuSecure的QuProtect™。

在法国方面，投资总秘书处（The General Secretariat for Investment，SGPI）于2023年6月与德国安全技术公司HENSOLDT签订PQC项目合同，该合同基于法国2030国家量子战略框架。通过其X7-PQC项目，HENSOLDT计划开发一种突破性的后量子技术，能够抵御涉及量子计算机的网络攻击。

表 8　2023年1月至2024年2月期间采用PQC技术的政府部门

时间	国家	部门	提供PQC服务企业/机构	内容
2023.06	美国	美国陆军	QuSecure	美国陆军授予QuSecure公司一项小型企业创新研究（SBIR）第二阶段的联邦政府合同，以开发量子弹性软件解决方案，确保敏感的军事数据和通信保持安全。
2023.06	法国	法国投资总秘书处（SGPI）	HENSOLDT	法国投资总秘书处（SGPI）授予法国公司HENSOLDT一份PQC技术开发合同，HENSOLDT打算通过其X7-PQC项目开发突破性的后量子技术，能够抵御涉及使用量子计算机的网络攻击。
2023.06	美国	美国国防信息系统局（DISA）	SandboxAQ	SandboxAQ公司获得由美国国防信息系统局（DISA）提供的合同，以实施该公司端到端的后量子加密管理解决方案。
2024.01	美国	美国空军创新中心（AFWERX）	QuSecure	获得AFWERX授予的小型企业创新研究（SBIR）合同，空军部（DAF）将使用QuSecure的QuProtect™。此次空军SBIR合同授予之前，QuSecure已从美国陆军 2023年（第二阶段SBIR）和美国政府2022年（第三阶段SBIR）获得类似的SBIR合同。

来源：光子盒整理

Part 4

PQC实际应用

政府&国防

金融

通信

金融

01 银行

金融银行逐渐意识到现有加密技术可能面临被量子计算机破解的风险，为了保护客户数据和交易安全，金融机构开始积极关注和投资量子安全通信，汇丰银行是首个加入英国开创性商业量子安全城域网络的金融机构。2023年5月，汇丰银行与Quantinuum签署一系列探索性项目，此次合作的目标是利用量子计算的力量来增强加密密钥，同时将其与PQC算法相集成，以减轻当前和未来的网络威胁。

此外，新加坡金融管理局（MAS）在2024年2月发布了一份指导建议，旨在敦促该国的金融机构为迎接量子计算时代的网络安全威胁做好充分准备。MAS明确指出，在未来，金融机构需要具备无缝集成PQC和量子密钥分发（QKD）技术的能力，以确保在面临潜在的量子攻击时，核心系统功能不会受到严重影响。这一指导旨在引导金融行业更好地理解并应对未来的量子计算安全挑战，确保整个金融体系在技术升级的过程中保持高度的安全性和韧性。

02 比特币

2023年7月，Quantum Resistant Ledger (QRL) 作为首个结合了企业级区块链与后量子安全技术的加密货币，正式面向区块链爱好者开放使用。QRL 超越了经典的安全椭圆曲线加密方式，转而采用了由NIST推荐的PQC算法，这一转变显著提升了其安全性。其核心安全措施为默克尔签名方案（XMSS），是NIST推荐的后量子安全数字签名方案，它能为每笔交易生成独一无二的一次性签名，即使面对量子计算机的强大计算能力，这些签名依然坚不可摧。不仅如此，QRL还通过结合链上格子密钥存储和层到节点间通信，构建了一个高度安全的消息传递系统。这一系统有效地屏蔽了量子威胁，使得QRL免受比特币和以太坊等传统加密货币所存在的无法修复的安全漏洞影响。

Part 4

PQC应用

政府&国防

金融

通信

通信

01 卫星

2023年3月9日，QuSecure推出首个具有量子弹性的实时端到端卫星加密通信链路，这一里程碑标志着美国卫星数据传输首次采用PQC来抵御经典和量子解密攻击，以保护卫星数据通信的安全性。QuSecure的量子弹性加密通信链路可以使任何联邦政府和商业组织都能够通过太空进行实时、安全、经典和量子安全的通信和数据传输。在星链网络上的安全卫星通信测试中，QuSecure成功地将量子弹性数据从Quark服务器通过科罗拉多州Rearden Logic的实验室发送到星链终端。然后通过上行链路将信号发送到Starlink卫星，再通过下行链路传回地球。所有这些通信均受到QuSecure的量子安全层（Quantum Secure Layer, QSL）的保护，通过PQC网络安全保护传输中的所有数据。同月29日，QuSecure宣布已与爱尔兰埃森哲（Accenture）公司合作开发并测试PQC保护的多轨道量子弹性卫星通信能力，这有效地结合了低地球轨道（Low Earth Orbit，LEO）卫星和地球同步赤道轨道（Geosynchronous Equatorial Orbit，GEO）卫星的优势，实现了数据在太空和地球之间的传输。

3月13日，美国纳米卫星服务提供商Sky and Space Company Limited （SAS）宣布与CyberProtonics建立合作伙伴关系。CyberProtonics将为SAS公司的纳米卫星和地面终端机群嵌入PQC技术，为2024年初的发射做准备。这一合作将确保卫星通信的安全性，并为未来的卫星网络提供了更强的数据保护。

谷歌作为全球科技巨头正积极应用PQC技术保护内部通信，且支持PQC密钥封装方法的谷歌浏览器普遍使用也标志这PQC在网络安全领域的应用。2023年8月，Chrome在其最新版本（版本116）中推出了一个量子混合密钥协商机制，该浏览器版本添加了抗量子攻击的X25519Kyber768算法。该算法是一种“混合机制”，它将两个加密算法的输出合并，以创建用于加密传输层安全协议（Transport Layer Security，TLS）连接大部分内容的会话密钥。所使用的两个算法分别是X25519（已经在使用中的椭圆曲线算法）和Kyber-768。从组织安全的角度来看，谷歌的举措代表了用户首次有机会在HTTPS网页上使用PQC。

法国企业Thales于2023年2月宣布在其移动安全应用和5G SIM卡中采用混合加密技术，为移动通信领域引入了PQC算法通信，不仅展示了量子安全技术在移动通信领域的前景，还为移动通信提供更高级别的安全性。QuSecure首次完成由后量子加密技术保障的多轨道数据通信测试，这一突破表明后量子加密技术已经进入实际通信场景，并具备可行性能进一步推动PQC在各个行业中的广泛采用。

美国Signal于2023年9月，升级了其端到端通信协议，采用PQC保护用户数据。升级后的协议称为PQXDH（Post-Quantum Extended Diffie-Hellman），融入了PQC算法CRYSTALS-Kyber。PQXDH可用于Signal的端到端加密（End-To-End Encryption，E2EE）规范。具体而言，PQXDH同时使用了X3DH的椭圆曲线密钥协议和CRYSTALS-Kyber的PQC密钥封装机制，适用于一般的加密以及需要快速交换小型加密密钥的高速操作。

苹果公司于2024年2月宣布对其iMessage通讯平台进行升级，此次升级采用PQ3加密技术，PQ3协议预计将在2024年内完全替代所有现有支持的对话协议。PQ3是一个开创性的抗量子加密协议，采取了一种混合设计策略，结合了目前的椭圆曲线加密技术（ECC）和新的PQC保护技术。因此，要想破解PQ3的安全性，攻击者必须同时克服传统的ECC加密技术和新的抗量子技术挑战。

表 9　2023年1月至2024年2月期间采用PQC技术的企业

时间	国家	企业/机构	内容
2023.02	法国	Thales	基于Thales的旗舰移动安全应用Cryptosmart以及5G SIM卡，采用NIST推荐的混合加密技术，实现后量子加密算法通信。
2023.08	美国	谷歌	从 Chrome 116开始，支持在 TLS 中建立对称密钥。Kyber768是抗量子，取得通用加密PQC获奖者。
2023.09	美国	Cloudflare	正式宣布对大部分入站和出站连接支持X25519+Kyber算法保护，此算法适用于源服务器和Cloudflare Workers fetch()。
2023.09	美国	Signal	Signal了“X3DH”（Extended Triple Diffie-Hellman）协议，升级后的协议PQC版本被称为PQXDH（Post-Quantum Extended Diffie-Hellman），融入了NIST发布的PQC算法，即CRYSTALS-Kyber。
2024.01	美国	Apple	苹果公司宣布推出PQ3，PQ3是一种后量子加密协议，具有防妥协的加密和对高度复杂的量子攻击的广泛防御，是第一个达到所说的3级安全性的消息传递协议，提供的协议保护超过了所有其他广泛部署的消息传递应用程序。PQ3采用混合设计，在初始密钥建立和重新密钥期间将椭圆曲线加密与后量子密码（Kyber）相结合。

来源：光子盒整理

Part 5

PQC市场规模预测

市场规模预测

市场规模预测

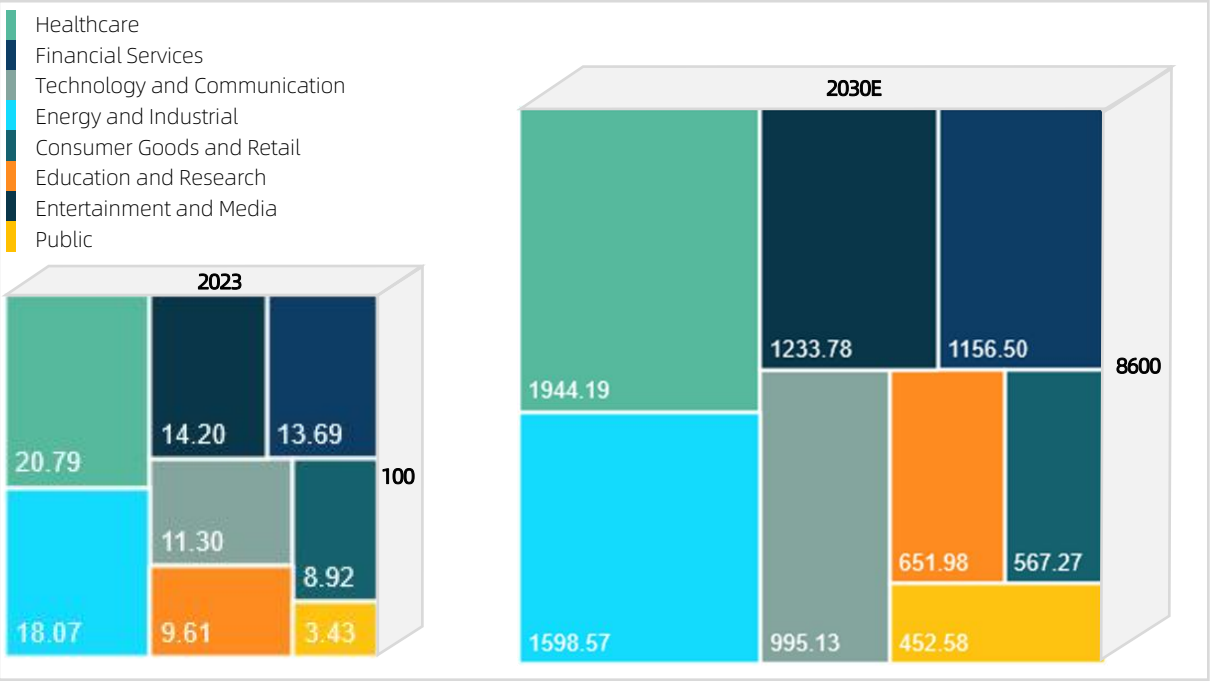
PQC市场增长与PQC标准化进程及量子计算机的实用化有较大关联。2023年，PQC产业规模仍处在初期成长阶段，约为1亿美元。根据NIST的PQC标准化工作预计完成的时间点（2024年），预计2024年后，行业将迎来小幅加速发展；预计到2030年，全球PQC产业规模将达到86亿美元。

据图6所示，在这段时间内，从2023年到2030年的复合年增长率（CAGR）预计为89%，凸显了PQC产业规模将经历迅猛的增长。各个领域的PQC产业规模，如医疗、金融服务、通信技术、能源工业、消费品和零售、教育与研究、娱乐和媒体和公共事业在2023到2030这段时间也预计都会出现迅猛增长。增长最快的领域为公共事业领域，2030年的该领域的PQC产业规模预测约为2023年的130倍。其次为医疗领域，其在2030年的PQC产业规模预测为2023年的94倍。消费品和零售、教育与研究、娱乐与媒体、通信技术、能源和工业以及金融服务这些领域的PQC产业规模也都显示出了积极的增长趋势，增长倍数显著。

在各个领域占比方面，2023年和2030年占比最多的领域均为医疗领域，所占比例均为20%左右。其次为能源和工业，所占比例均为18%左右，再其次为金融领域，占比均为13%左右。这预示着医疗、能源工业和金融服务领域存在着较高的加密需求。占比最少的为公共服务领域，占比均在5%以下，但也以101%的复合年增长率增长，在所有领域中拥有最高的增长速度。

总体来说，到2030年，各个细分领域对PQC解决方案的需求将急剧上升，以应对量子计算对现有加密技术的潜在威胁。因此可以预见，PQC产业将成为技术创新和投资的热点领域，推动相关企业和研究机构加大研发力度，加速产品开发和市场部署，以满足日益增长的市场需求。同时医疗、能源工业和金融服务领域存在着较高的加密需求。

图 6 全球PQC产业规模预测（2023-2030E）（单位: 百万美元）



Part 6

未来展望

PQC与经典密码的混合加密将推动密码学演进
PQC的量子安全性评估将成为未来研究焦点
PQC算法标准化工作仍需持续推进
PQC商业化与迁移计划逐步开启
量子领域公司业务扩张至PQC领域
PQC发展即将迎来成长期

01
PQC与经典密码的混合加密将推动密码学演进

PQC与经典密码相结合的混合加密策略将成为主导趋势，这一混合方法在发展过渡期提供了有效的安全保障和向后兼容性。具体而言，混合加密系统的设计将经典的RSA或椭圆曲线加密技术与PQC算法紧密融合。这种设计策略在确保系统安全性方面发挥着双重作用：一方面，运用PQC算法抵御潜在的量子计算威胁以及“先存储，后解密”风险；另一方面，通过经典加密技术，确保与现有系统的无缝兼容性。即便经典算法遭受破解，混合系统依然能够保持防御力。

在保证兼容性的同时，采用混合加密策略可以助力机构和组织平稳过渡至全面采用PQC时期。特别是面向消费者的应用（通信和支付平台），这种渐进过渡策略尤为重要。通过在现有使用经典密码的软件中逐步引入PQC算法，用户可以在不改变其现有使用习惯的情况下，享受到更高级别的数据保护。例如，谷歌浏览器（版本116）使用X25519Kyber768算法保护用户信息安全，该算法是由X25519（椭圆曲线算法）和Kyber-768（PQC算法）组成的混合加密算法。苹果公司同样利用经典加密算法及PQC算法混合的方式保护其iMessage通讯平台。

PQC技术与经典密码技术的融合、发展和实施是一个需要综合考虑安全性、兼容性和前瞻性的过程，以确保在量子时代过渡过程中，全球的数据通信依然能够保持安全。

02
PQC的量子安全性评估将成为未来研究焦点

PQC算法的核心设计目标在于对抗量子计算攻击，这一重要特性是经典加密算法无法达到的。然而，PQC算法已被破解四次。最近一次是在2023年年初，瑞典皇家理工学院仅利用神经网络便破解了NIST提名的Crystals-Kyber算法。因此，对于PQC算法的量子安全性需要进行深入的研究和全面的评估。

为了迎接这一挑战，阿联酋技术创新研究所的密码学研究中心于2023年9月推出了全球首个开源CryptographicEstimators软件库。该软件库旨在提供一个工具，协助研究人员评估PQC算法的安全性。尽管这一工具的推出对PQC领域需求做出了积极响应，但它目前仍处于早期阶段。CryptographicEstimators软件库尚未经历实际测试和长期验证，因此，关于其有效性和准确性的结论还需要更多的证据支持。该软件库为PQC算法的安全性评估提供了一个有用的起点，但在实际应用中仍需要基于更广泛的研究和实验数据来确认其可靠性。

此外，考虑到量子计算领域的快速发展，新的算法和潜在的量子攻击手段可能随时涌现。这些未来的发展可能会对现有的PQC算法构成挑战，或需求对算法进行调整和更新。因此，持续评估PQC算法是否能在这种不断变化的技术环境中保持量子安全性，是未来研究的一个重要方向。

03
PQC算法标准化工作仍需持续推进

PQC标准化是一个连续的、多阶段和迭代的过程。美国NIST在2016年便启动PQC算法标准化过程，通过广泛的算法征集、严格的安全性评估、开放的专业评审，以及全面的社区反馈征集。预计2024年，NIST将完成这一过程，并正式批准一系列PQC算法草案。然而，这并非标准化工作的终点，而是一个新的起点。

随着PQC技术的不断发展和新挑战的出现，标准的适用性和有效性将受到不断的监控和评估。这意味着标准化组织，包括NIST和其他国际标准机构，将致力于确保PQC标准在全球范围内保持协调和一致性。

该持续性的工作对于应对未来可能出现的技术变革和安全挑战至关重要。通过开放的专业评审和广泛的社区反馈，PQC算法标准将不断优化和更新，以适应动态的量子技术发展。确保全球通信系统在量子计算时代能够保持高水平的安全性，促进信息安全的全球共识。

04
PQC商业化与迁移计划逐步开启

企业在实施PQC迁移计划的过程中，需要寻找适用于其业务环境的PQC解决方案。这为PQC技术提供了商业应用的机会，推动了相关产业的发展。同时，商业领域对PQC的关注度提升促使企业开始考虑迁移计划。两者相辅相成，共同推动着PQC技术在实际应用中的发展。

随着科技企业推出基于PQC的软件，PQC商业化应用范围逐渐扩大。这些软件提供了易于集成和使用的PQC保护措施，为其他企业提供了一种简便而高效的方式来增强通信安全。IBM、QuSecure、WISeKey、Xiphera等公司均已推出PQC商业化产品。政府的积极参与在PQC的商业化推广应用中发挥了关键作用，为整个行业树立了示范标杆，促进了PQC商业化进程。PQC的商业化进程不断加速，使越来越多的企业能够轻松进行PQC迁移，建立更强大的安全防线，以保护企业和个人的重要信息免受量子计算攻击的威胁。

PQC迁移是一项关键的全球性举措，不同领域和机构正在逐步推进PQC的应用和迁移，为信息安全提供了多样化的解决方案和机会。政府和军事机构的需求对PQC迁移的推动作用尤为明显，这些机构拥有大量的敏感数据以及对通信的安全性要求较高，因此对高度安全的加密技术的需求非常迫切。美国、欧盟和韩国等国家都出台了相关政策以鼓励PQC研究和应用。其中美国政府通过与PQC私营企业合作，推动并完成PQC迁移工作。此外，谷歌、QuSecure等大型科技公司也开始采用PQC技术，未来PQC有望在各个行业广泛应用。在金融方面，汇丰银行正在积极参与并引领金融界在PQC安全领域的探索，在量子安全领域起到了维护金融安全和可持续性方面的关键作用，为量子时代的金融安全奠定坚实的基础。

05
量子领域公司业务扩张至PQC领域

在量子信息科技领域的不断创新和发展中，量子计算逐步崛起，经典加密面临的挑战愈发严峻，量子计算公司逐步拓展其业务范围，将目光投向了后量子计算时代的保密通信领域，即PQC。这种战略性的业务扩张将推动PQC技术在商业应用中的推广和深化，为用户提供更高级别的数据保护和通信安全。例如，中国图灵量子此前主要关注量子计算机的研发，但于2024年与其旗下天机量子推出了基于抗量子算法的高性能PQC加密芯片，并且实现万片以上量产。美国IBM同样为专注量子计算的科技公司，也于2023年发布量子安全路线图。

在未来，随着量子领域公司在PQC领域的投入和创新，可以看到更多基于新一代加密技术的产品和服务涌现。量子领域公司的业务扩张至PQC领域，必将为PQC领域带来新的动能，构筑更为坚固的数字防线。

06
PQC发展即将迎来成长期

随着美国NIST在PQC领域的标准化工作逐步推进，以及美国、加拿大及韩国相继发布多项关于PQC的文件，PQC技术即将告别起步期，步入成长期。标准化工作和政策文件的发布不仅扫清了PQC技术发展的政策障碍，也拓宽了对PQC技术的认知范围，为其进一步发展提供了有力的政策支持。

美国NIST领导的PQC标准化工作已经历八年，即将完成第一阶段PQC标准草案的制定，这标志着PQC技术将迈入商业化和潜在应用的探索阶段。尽管获得NIST提名的PQC算法仍存在安全性漏洞，但对网络信息安全和对量子计算破译能力的担忧将推动PQC技术不断升级。随着PQC算法的迭代与升级，PQC技术将逐步优化，有望应对各种实际应用场景的需求。

未来将有更多公司尝试进入PQC技术领域，积极研发和提供PQC解决方案，以迎接量子计算带来的“先存储，后解密”的挑战。PQC公司的涌现将深刻推动PQC领域的业务发展，逐渐完善PQC领域的产业链。

参考链接

https://pqcrypto2016.jp/

https://csrc.nist.gov/files/pubs/ir/8105/final/docs/nistir_8105_draft.pdf

https://csrc.nist.gov/projects/post-quantum-cryptography

https://csrc.nist.gov/pubs/fips/203/ipd

https://csrc.nist.gov/pubs/fips/204/ipd

https://csrc.nist.gov/pubs/fips/205/ipd

https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html

https://www.etsi.org/events/2117-2023-02-9th-etsi-iqc-quantum-safe-cryptography-workshop

https://www.tc260.org.cn/front/postDetail.html?id=20230616154140

https://www.ding-lab.com/archives/3rd-pqc-asia-forum

https://stcsm.sh.gov.cn/zwgk/kyjhxm/xmsb/20230927/8a0160510f484e9d88091988175f195c.html

http://www.legaldaily.com.cn/IT/content/2024-01/02/content_8945732.html

https://www.nict.go.jp/press/2023/03/14-1.html

https://www.koit.co.kr/news/articleView.html?idxno=114989

https://www.ietf.org/blog/pquip/

https://post-quantum.com/index.html

https://www.mitre.org/news-insights/news-release/post-quantum-cryptography-coalition-launches

https://www.gsma.com/newsroom/gsma_resources/post-quantum-telco-network-impact-assessment-whitepaper/

https://www.gsma.com/newsroom/wp-content/uploads//PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf

https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

https://www.hnftp.gov.cn/attach/2023/3/16/20220915183727e11deb2058a24b25a94835647a994eef.pdf

https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

https://www.congress.gov/bill/117th-congress/house-bill/7535

https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy

https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

https://www.datanet.co.kr/news/articleView.html?idxno=185202

https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
http://www.koal.com/news?id=64dd9821ff9295703e697584
http://www.koal.com/news?id=64dd9821ff9295703e697584
https://www.qsmc.org/zh
https://pkic.org/events/2023/post-quantum-cryptography-conference/
https://rwpqc.org/#about
https://mp.weixin.qq.com/s/PRw_JZXWt1Gu23_MD73UIQ
http://cacr2023.cacrnet.org.cn/fair/24
https://pqcrypto2023.umiacs.io/
https://icmconference.org/?page_id=19232
https://www.maths.ox.ac.uk/events/conferences/past-events/oxford-post-quantum-cryptography-workshop-2023
https://pkic.org/events/2023/pqc-conference-amsterdam-nl/#conference-details
https://www.softbank.jp/en/corp/news/press/sbkk/2023/20230228_01/
https://uploads-ssl.webflow.com/637deec5b8a2a6508d3d1159/6409fce19d51fcd809735ede_20230309-PR-Cryptonext%20Quandela-VDef.pdf
https://newsroom.ibm.com/2023-05-10-IBM-Unveils-End-to-End-Quantum-Safe-Technology-to-Safeguard-Governments-and-Businesses-Most-Valuable-Data
https://www.wisekey.com/press/wisekey-and-sealsq-develop-ai-based-quantum-solutions-demonstrator-for-post-quantum-cryptography/
https://www.qusecure.com/qusecures-post-quantum-cryptography-products-now-available-on-gsas-multiple-award-schedule/
https://castle-shield.com/castle-shield-holdings-llc-adds-post-quantum-cryptography-pqc-support-to-its-typhos-communications-app-for-audio-video-calls/
https://www.qusecure.com/qusecure-earns-validation-in-amazon-web-services-partner-network-apn-quprotect-awarded-aws-qualified-software-certification/
https://ir.quicklogic.com/press-releases/detail/672/securing-the-future-quicklogic-and-xiphera-partner-to
https://www.bita.org.cn/newsinfo/6340878.html
https://www.laoyaoba.com/html/share/news/892071?source=app_android_v115&news_id=892071&fromShare=android&utm_source=utm_source_sharewxm
https://www.ensilica.com/news/ensilica-adds-post-quantum-cryptography-support-to-esi-crypto-ip-library/
https://www6.thalesgroup.com/post-quantum-readiness-pqc-starter-kit
https://mp.weixin.qq.com/s/p4ulGKfNSxO2B-NvQ6DGtg
https://www.qusecure.com/post-quantum-cryptography-solutions-adopted-by-the-us-army/
https://www.hensoldt.fr/news/hensoldt-to-drive-forward-post-quantum-cryptography-in-france/

https://www.sandboxaq.com/press/defense-information-systems-agency-awards-sandboxaq-other-transaction-authority-agreement-for-prototype-to-provide-quantum-resistant-cryptography-solutions
https://www.qusecure.com/qusecure-awarded-u-s-air-force-contract-for-post-quantum-cybersecurity-solutions/
https://www.quantinuum.com/news/hsbc-and-quantinuum-explore-real-world-use-cases-of-quantum-computing-in-financial-services
https://www.qusecure.com/qusecure-uses-starlink-for-post-quantum-cryptography-in-satellite-to-earth-communications/
https://www.qusecure.com/qusecure-accenture-team-up-on-satcom-security-test-using-pqc/
https://www.einpresswire.com/article/621893832/sky-and-space-sas-to-embed-world-s-first-quantum-resistant-encryption-solution-for-its-satellites-and-ground-terminals
https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms?utm_source=substack&utm_medium=email
https://www.thalesgroup.com/en/worldwide/group/press_release/thales-pioneers-post-quantum-cryptography-successful-world-first
https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html
https://security.apple.com/blog/imessage-pq3/
https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum
https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook
https://kpqc.cryptolab.co.kr/
https://www.cisa.gov/news-events/alerts/2023/08/21/cisa-nsa-and-nist-publish-factsheet-quantum-readiness
https://eviden.com/insights/press-releases/eviden-to-launch-first-post-quantum-ready-solutions-for-digital-identity/
https://www.qusecure.com/inside-quantum-technology-qusecures-latest-partnership-gets-it-into-red-hat-platforms/
https://estimators.crypto.tii.ae/
https://signal.org/blog/pqxdh/
https://www.sansec.com.cn/news/132.html
https://www.theqrl.org/markets/
https://blog.cloudflare.com/zh-cn/post-quantum-cryptography-ga-zh-cn/

光子盒创立于2020年2月，作为一家量子产业服务平台，光子盒通过推送前沿量子科技新闻、科普量子知识、解读量子技术、发布年度和专题报告等形式，致力成为中国量子科技产业最值得信赖的服务机构。

光子盒不断扩充自有量子科技产业数据库的广度与深度，建立多维量子产业数据信息，提供客观、专业、深入及具有时效性的量子行业报道与咨询服务。

未来，光子盒将继续联合量子产业科技公司、金融行业投资公司、国家/省级量子相关科研院所、政策战略研究单位等共同促进量子产业持续向好发展。

Contact Us

光子盒
QUANTUMCHINA

北京市东城区朝阳门SOHO 1506

wangxin@quantumchina.com

https://www.quantumchina.com/

更多精彩内容，请关注：

光子盒微信公众号