后量子密码迁移白皮书

（2024）

2024 年 06 月

❖ **参与单位**:

西安电子科技大学广州研究院、广州链融信息技术有限公司、中国人民银行数字货币研究所、西安电子科技大学、北京理工大学、中国电信集团有限公司、华夏银行股份有限公司、中国科学院信息工程研究所、复旦大学、安徽问天量子科技股份有限公司、格尔软件股份有限公司、上海交通大学、暨南大学、天翼安全科技有限公司、龙盈智达(北京)科技有限公司、北京航空航天大学、广州大学、贵州大学、天翼电子商务有限公司、中国电信集团有限公司广州分公司、云上(江西)密码服务科技有限公司

❖ **指导委员会**:

马建峰、杨义先、曹珍富

❖ **编写人员**:

裴庆祺、王励成、宋玲娓、雷静、赵鹏、吴永飞、路献辉、赵运磊、谭武征、刘紫千、王彦博、朱浩瑾、祝烈煌、翁健、田志宏、樊迪、刘雪峰、马立川、刘樵、张宗洋、徐光侠、陈玉玲、刘长波、方宇、魏文术、蒋斌、肖阳、吕法科、郑向上、吴洋洋、马晓亮、姜林海、刘振、田翠翠、赵勇智、辛梓焜、贺伟、贾蒴、杨璇、王一多

前言

后量子密码（Post-quantum cryptography，PQC），国内又称抗量子密码（Quantum-resistant cryptography，QRC）。广义上，也可以将依赖量子力学特性的量子密码学（Quantum cryptography，QC）纳入后量子密码的范畴——因其具有抵量子攻击的能力；狭义上，后量子密码特指能够在现有电子计算机上实现的、具有抵抗未来量子计算机攻击能力的数学密码——本报告即取此义。

近年来，量子计算技术飞速发展，作为衡量量子计算能力的量子体积数呈“指数级”增长。传统基于数论难题的公钥密码算法及其协议和系统的安全性均面临量子计算的威胁。随着 NIST 后量子密码候选标准算法的推出，全球各主要国家的后量子密码算法迁移已经被提上议事日程。

后量子密码迁移不等同于“后量子密码算法标准的制定 + 后量子密码算法的实现及替换”，它至少包含了对现有网络和信息系统的量子脆弱性发现和相应的风险评估、后量子密码标准算法及安全协议的安全实现和有序部署、以及随之而来的兼容性、互操作性评测等，它是一个社会化的系统工程，必将涉及到各行各业乃至每一个人，因此也包含了相关技术链条上下游企事业单位共同参与的产学研用相结合的后量子密码迁移生态的培育和发展。

本报告简要回顾传统密码技术图景及其面临的量子威胁，详细梳理现有后量子密码的技术路线，重点关注 NIST 后量子密码算法的征集过程，通过解读 NIST 及相关国际化组织相继推出的后量子

密码迁移研究报告，给出后量子密码迁移路线图，包括现有密码体系量子脆弱性的发现和风险评估、现有后量子密码迁移的实现及性能评测、先行试点等，并提出我国后量子密码迁移的发展建议。

本报告虽然经过编写团队的不懈努力，但由于能力和水平有限，疏漏和不足之处在所难免，敬请广大读者和专家批评指正。

目录

第一章 传统密码面临的量子威胁

1.1 传统密码技术图景

密码学历史悠久，相关技术的应用日渐普及，从军事领域，逐步扩展到商业领域，并渗透到现代社会的各行各业，不断发展演进，为人们的生产和生活方式提供信息安全保障。传统意义上，密码学算法主要包括对称算法、非对称算法和杂凑算法等。表 1 给出了部分经典密码算法及其国际、国密标准。

- 对称密码算法，又称私钥密码算法，其特点为通信双方使用相同的密钥进行数据加密和解密，且由于对称密码加解密操作性能高效，常用于数据加密传输、数据库加密存储等场景，保障数据机密性。

- 非对称密码算法，又称公钥密码算法，其特点为通信双方使用一对不同的密钥（公/私钥对），其中公钥用于加密信息，私钥用于解密信息。虽然其加解密性能不及对称密码算法，但由于其私钥无需共享，因而给传统密码学带来了更多丰富应用，常用于生成短期的对称会话密钥、安全证书、数字签名等场景，实现身份验证、数据保密等关键功能。

- 杂凑算法（杂凑函数），又称散列函数或哈希函数，指将任意长度的数字消息映射成固定长度数字串的函数，常用于密码存储、数据完整性校验等功能。

表 1 现代密码算法及其标准[1-16]

	密码体系	算法分类	国际算法标准	国密算法标准
密码算法	非对称密码	加密算法	RSA (NIST SP 800-56B rev 1)	SM2-3 (GB/T 35276-2017)
		数字签名	RSA (FIPS 186-4)	SM2-1 (GB/T 35276-2017)
			ECDSA (FIPS 186-4)	
		密钥交换	DH (IETF RFC 3526)	SM2-2 (GB/T 35276-2017)
			ECDH (FIPS SP 800-56A)	
	对称密码	加密算法	AES (FIPS 197)	SM4 (GB/T 32907-2016)
				ZUC (GB/T 33133.2-2021)
		杂凑算法	SHA (FIPS 180-4)	SM3 (GB/T 32905-2016)

对称密码保障机密性和完整性。信息系统发展的早期，密码学应用的主要关注点在于保障安全的通信[17]。敏感信息在通过公共互联网进行传输时可能会遭到恶意攻击者的窃听，因而产生了机密性的需求，即数据通信过程中只被合法的通信方获取，而向未经授权的第三方隐藏。在这一背景下，密码学家设计了各种对称加密算法(例如 AES、ZUC、SM4 等)，通过将信息转化为只有授权方能解密的形式保障了机密性 (Confidentiality)。除此之外，实现机密性并不足以确保信息的安全，因为攻击者还可能对密文进行恶意篡改，如

直接删除部分信息，且接收方可能无法察觉这一恶意行为，因此，保障数据的完整性同样重要，其强调在通信过程中，可未经授权的第三方不得对数据进行非法篡改或伪造。杂凑算法（例如 SHA、SM3 等）使用密钥为数据生成固定长度的标识，由拥有相同密钥的另一方进行完整性验证，即可保障数据的完整性 (Integrity)。

公钥密码拓展身份的可认证性。对称密码算法的密钥需要一对一发放，因此在不安全的信道中安全传输对称密钥成为关键挑战。公钥密码算法应运而生（例如 RSA、ECC、SM2 等），建立在一系列数学困难问题所构成的陷门单向函数上。一方面，为对称密码学的广泛应用提供密钥交换等重要支撑；另一方面，通过将陷门设置为私钥，保障不掌握私钥中陷门信息的任何敌手都无法获得明文信息，拓展了更多应用场景。由于互联网信息的匿名性，恶意的中间人可冒充通信方身份窃取隐私，因此身份认证也同样重要。数字签名算法与公钥加密算法的原理类似，使用私钥用于签名，公开的密钥用于验证。结合可信的证书颁发机构（CA）提供的公钥、身份、有效期等信息，只要通信方能提供通过验证的经过 CA 签名的各自身份对应的证书，即可实现通信的可认证性 (Authenticity)。

综合运用上述密码算法，可以设计各种类型的密码协议（又称安全协议），完成两方或多方参与者的特定任务并满足数据机密性、完整性、不可否认性等安全需求。常见的密码协议，如 SSL/TLS、SSH、PKI 等，为数据安全和系统可靠性提供了不可或缺的保障。

TLS/SSL(Secure Sockets Layer) 协议综合使用加密算法、杂凑算法、数字签名算法等多种传统密码技术，为客户端和服务器之间的网络通信提供数据加密与身份认证的重要功能。其自身经过多次升级优化，最终更新并改名为 TLS (transport layer security)。TLS 传输协议位于不安全的 TCP/IP 等底层网络通信协议之上，其中握手协议进行身份认证与共享密钥的协商，记录协议保证通信数据的机密性与完整性。实际中，多种上层应用建立在 TLS 的服务之上。例如，HTTPS (HTTP over TLS) 基于 TLS 协议，为 HTTP 协议增加了安全性，已广泛应用于万维网服务器，Chrome、Internet Explorer 等常见浏览器都支持 HTTPS 协议[17]。

SSH(Secure SHell) 协议主要用于在不安全网络上实现安全远程登录和数据传输。在 SSH 协议出现之前，常用的远程连接协议，如 Telnet 和 Rlogin，主要使用基于口令的身份验证方式。谁拥有正确的用户名和口令，谁就可以登录到远程主机，因此，缺乏针对中间人攻击的有效保护。SSH 协议通过采用多种身份验证方式，包括密码认证、基于公钥的认证和基于证书的认证，确保用户的合法性并防止未经授权的访问。同时，它使用对称加密（如 AES）和非对称加密（如 RSA）技术，保障数据在传输过程中的机密性和完整性。SSH 协议一个广泛应用的开源实现是 OpenSSH，已被集成到各种 Linux 发行版中，用于系统管理和安全文件传输。通过提供对中间人攻击和数据篡改的防护，SSH 为远程登录和数据传输提供了可靠的安全保障，使其成为现代网络安全不可或缺的一部分。

PKI(Public Key Infrastructure) 是一种遵循公钥密码理论和技术为电子商务等业务提供普适性安全服务平台的基础设施。在 PKI 系统中，由 CA 签发数字证书、绑定用户的身份信息和公钥。PKI 依赖方 (Relying Party) 在使用 PKI 时，预先存储自己信任的根 CA 的自签名证书，以便验证由该 CA 签发的证书的真实性和有效性，可信地获得与之通信用户的公钥，用于各种安全服务。X.509 是公钥证书的格式标准。X.509 证书已应用在包括 TLS/SSL 在内的众多网络协议里，同时它也用在很多非在线应用场景里，比如电子签名服务。X.509 证书里含有公钥、身份信息（比如网络主机名，组织的名称或个体名称等）和签名信息（可以是证书签发机构 CA 的签名，也可以是自签名)。

1.2 量子计算对传统密码的威胁

1.2.1 量子计算对传统对称密码的威胁

传统对称密码（如 AES、ZUC、SM3/SM4 等）的安全性不依赖于特定的数学难题，其设计思路主要是基于香农 1949 年提出的“乘积密码”的思想，通过扩散和混淆两种基本步骤的多轮迭代，来提供更高的安全性。对称密码设计理念的一个通俗解释就是：尽可能破坏密文空间的代数结构，使得对称密码算法实现的映射尽可能与伪随机函数不可区分[1]。正因为如此，对于理想的对称密码来说，不存在快于穷尽搜索的攻击方法。从而，对称密码密钥的长

[1]尽管近十年来也有基于置换群、辫群、Cayley 图等非交换代数结构来设计对称密码的尝试，但这个方向目前仍未发展成对称密码设计的主流，不在本报告讨论范围之中。

度，直接决定了攻击的复杂度，我们也直接依此作为对称密码的安全强度。例如，AES-256 具有 256 位密钥，攻击搜索空间复杂度高达 2^{256}，其经典安全强度为 256 位。

量子计算对于传统对称密码也有一定的攻击优势，这主要归功于两类典型的量子算法：Grover 算法和 Simons 算法。前者是一个通用型量子算法，能够以 $O(\sqrt{N})$ 复杂度处理任意搜索空间为 $O(N)$ 的问题，即相对于经典计算来说，具有所谓的平方加速比。后者是一个专用型量子算法，可以在多项式时间内得到一个周期布尔函数的非平凡周期，且相对经典计算来说，具有指数加速比。近十年来，这两类量子算法被广泛应用于对称密码安全性研究领域，其典型应用范式为：首先利用 Grover 算法对密钥进行搜索，然后利用 Simon 算法来判断该密钥是否正确 [18]。例如，2018 年，董晓阳等人采用 “Grover+Simon” 量子攻击框架，设计了针对 r-轮 n-位 Feistel 结构的量子密钥恢复攻击，其量子查询次数为 $O(n2^{(r-3)n/4})$，攻击所需的量子比特数为 $O(n^2)$ [19]。

从目前研究来看，量子攻击对于对称密码安全性的影响相对较小[18]。一方面，原有的很多对称密码设计结构或模式，被证明是量子安全的；并且对于遭受量子攻击的方案，经过改造仍然可能达到量子安全性[18]。另一方面，针对具体的对称密码算法，现有 “Grover+Simon” 类型（及其改进版本）的量子攻击框架的量子资源总消耗（包括量子查询复杂度、量子计算复杂度、量子存储复杂度

等）仍然具有指数级复杂度，从而可通过增加密钥长度来有效抵抗此类量子攻击。此外，对于杂凑算法，面临同样的问题，通过增加杂凑函数输出长度，可以有效抵抗量子原象求解攻击。因此，本报告后续部分仅关注量子计算对公钥密码的威胁。

1.2.2 量子计算对传统公钥密码的威胁

理论上，相比于经典计算模型，量子计算对传统以数论难题为基础的公钥密码算法的威胁是本质性的。1994 年，Peter Shor 提出了分解大整数和求解离散对数的量子算法，其量子资源总消耗是多项式级的。Shor 算法及其后续发展起来的一系列量子算法都遵从了统一的量子计算框架——隐藏子群问题（Hidden Subgroup Problem, HSP）。现在人们已经知道，有限交换群上的隐藏子群问题，均存在多项式复杂度的量子求解算法。这一结论对目前仍然广泛使用的公钥密码系统——包括 RSA 公钥加密/签名、Diffie-Hellman 密钥交换、Elgamal 公钥加密/签名、Schnorr/DSA 签名、椭圆曲线加密和签名（如 ECDSA、ED25519、SM2）等常见公钥密码的底层数学问题均有效。换句话说，如果一定规模的量子计算机成为现实，那么当前互联网和区块链广泛使用的公钥密码体系都不再安全。在 2022 年 5 月，SandboxAQ 和谷歌的技术人员在 Nature 上联合发文[20]，指出了所谓的“现存后解”（Store-now-decrypt-later，SNDL）攻击对现有公钥密码系统的威胁。SNDL 攻击本质上是一种拖库攻击，即攻击者将今天尚不能破解的密文存储下来，等到大规模容错量子计算机可用的时候再来破解。

那么 SNDL 攻击的威胁有多么迫切呢？我们根据相关技术报道，简单估算一下。实践上，由于受限于与量子比特规模和量子门保真度等方面的限制，Shor 算法提出后近 20 年里，相关实验进展比较缓慢。2017 年，微软公司的技术人员提出了 Shor 算法的一个优化实现方案，分解 n 比特整数仅需 $2n+2$ 位（逻辑）量子比特，计算 n 比特的椭圆曲线离散对数也仅需 $9n+\log n^2$ 位（逻辑）量子比特[21] [2]。据此，对于破解模数为 2048 位的 RSA 密码和 256 位的 ECC 密码来说，大约需要 $2500\sim4000$ 位（逻辑）量子比特，这远远超出了今天的量子计算能力。

但是，考虑到近年来量子计算机研制方面的飞速发展，特别是作为衡量量子计算能力的量子体积数呈“指数级”增长态势，预计到 2035 年左右，就有可能出现百万级（物理）量子比特的计算机(见图1) [3]。2021 年，谷歌的技术人员估计：分解 2048 位的 RSA 模数，在 2000 万含噪（物理）量子比特的机器上仅需 8 个小时[4]。2024 年，IBM 最新的量子纠错技术展示了如何将 12 位逻辑量子比特编码到 288 位物理量子比特中，实际的逻辑量子比特对物理量子比特的编码率高达 1/48，并保持了近 100 万个指令周期[23]。既使不考虑今后十年间量子纠错技术的新突破，随着 IBM 这项量子纠错技术的成熟和大规模运用，百万级物理量子比特可编码实现的逻辑量子

[2]注：量子比特位数、量子线路深度、量子门个数是三个不同但相互关联的指标。Shor 量子算法的量子线路深度和量子门个数规模分别为 $O(n^3)$ 和 $O(n^2\log n)$。

[3]谷歌公司甚至宣布计划在 2030 年就实现百万级量子比特计算机的研制。

[4]谷歌这个方案估计的量子资源总消耗在复杂性量级上与微软的一致，但具体数值要略高于微软的，其所需要的逻辑量子位数、量子线路深度、量子门个数分别为 $3n+0.002\log n$、$0.3n^3+0.0005n^3\log n$、$500n^2+n^2\log n$。详见[22]。

比特位数将会超过两万。到那时，今天用 RSA 密码和 ECC 密码加密的东西将毫无秘密可言。也就是说，对于保密期超过 10 年的机密，今天已经不应该再用 RSA 密码和 ECC 密码加密了！甚至有专家断言：10 年时间太长，攻破现用 RSA 密码和 ECC 密码的量子计算机可能会更早到来！这种观点的依据主要是注意到了量子分解算法方面的最新进展。2023 年，格密码的领军人物之一 Regev 对 Shor 算法提出了近 30 年来的最大改进[5]：分解 n 比特整数的量子门个数由 Shor 算法的 $O(n^2\log n)$ 降低为 $O(n^{3/2}\log n)$，但所需要的逻辑量子比特位数由 Shor 算法的 $O(n)$ 上升为 $O(n^{3/2})$；很快，Regev 的改进再次被超越[6]，2024 年，MIT 的 Ragavan 和 Vaikuntanathan 提出了逻辑量子比特位数和量子门个数分别为 $O(n\log n)$ 和 $O(n^{3/2}\log n)$ 的分解算法。

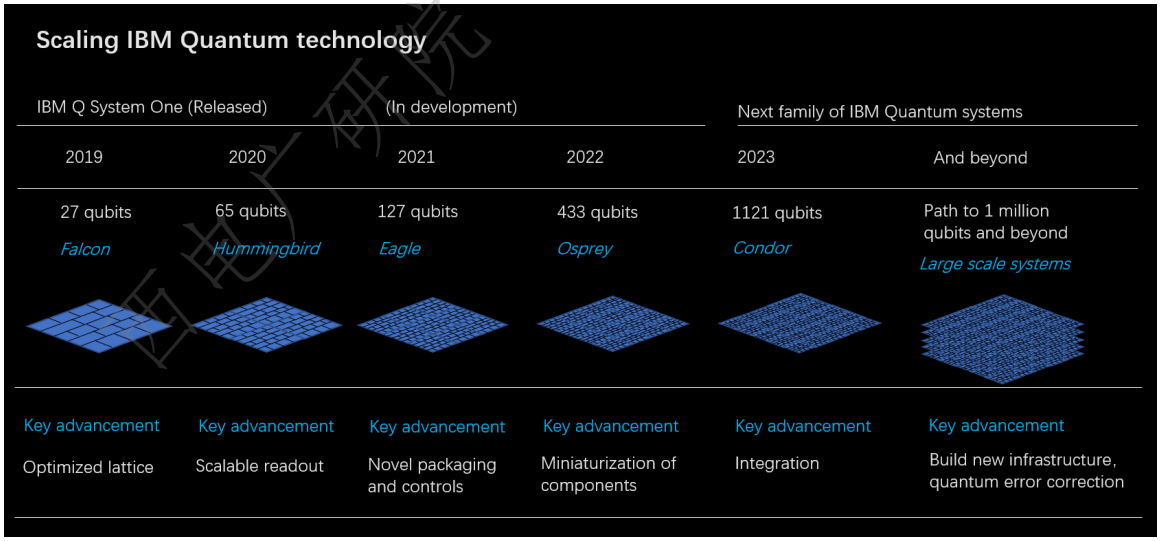

图 1 IBM 的量子技术路线图

[5]详见： https://arxiv.org/abs/2310.00899v3
[6]详见： https://arxiv.org/abs/2308.06572

第二章 后量子密码技术路线及标准化进程

2.1 后量子密码技术路线

为了应对量子计算机对现有密码算法的威胁，研究人员和密码学家已经着手开发新一代的密码算法，这些算法基于各种数学难题，旨在抵御量子计算的攻击。根据底层数学问题分类，后量子密码算法研究目前主要有 5 种技术路线，分别是基于格的密码、基于编码的密码、基于多变量的密码、基于哈希函数的密码以及基于曲线同源的密码。

基于格的密码：格（Lattice）俗称为“数的几何”（Geometry of numbers），是一种数与形相结合的代数结构，其本质是一个离散加法子群，定义为一组线性无关的非零向量（格基）的整系数线性组合。格密码基于格上问题的困难性，如最短向量问题（SVP）、最近向量问题（CVP）及其变种等。格最初多被用于某些密码问题的分析，直到 Ajtai 和 Regev 分别引入小整数解问题（SIS）和容错学习问题（LWE），开启了实用的可证明安全格密码研究。SIS 和 LWE 被广泛用于构造密码哈希函数、身份认证和数字签名等密码方案以及全同态加密、不可区分混淆等高等密码算法。目前主流的加解密格体制和数字签名个密码体制基本基于这两个问题，NIST 目前选择标准化的算法也多数是基于格的。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。

基于编码的密码：信道编码的目标是设计高效的冗余编码，以便在传输过程中纠正由信道噪声引入的错误，从而实现正确的译码。然而研究人员们发现某些编码的译码计算是困难的，这种译码的困难性为构造安全的密码算法提供了思路。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。1978 年 McEliece 提出了 Classical-McEliece，这是基于对称群隐藏子群问题的困难性，使用 Goppa 码设计的公钥加密方案。与现有公钥密码方案相比，加密速度更快，但由于公钥尺寸太大，实用性较低。随着后量子密码的提出，McEliece 等编码密码方案因具备后量子的特性，被认为可能成为基于数论的公钥密码体制的替代品，并成功通过了 NIST-PQC 前三轮评估，并入选了第三轮胜出算法集 Finalists。

基于多变量的密码：基于多变量的后量子密码算法是后量子密码算法最早的类别之一，这类密码算法基于求解高次多变量方程组这一 NP 难问题。通常，这些密码算法采用二次多项式，并将有限域上一组二次多项式作为公钥映射。代表性的基于多变量的密码算法包括 HFEv-类型的 GeMSS 签名体制和 UOV 类型的 Rainbow 签名算法。这两个算法都顺利通过了 NIST-PQC 评估的前三轮，并于 2022 年 7 月被分别选入第三轮的胜出集合 Alternates 集和 Finalists 集。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，虽然其具有公钥尺寸大的缺点，但适用于无需频繁进行公钥传输的应用场景。

基于哈希函数的密码：哈希函数是将任意长度的消息映射到固定长度输出的映射，其算法完全公开，没有密钥或任何秘密信息，设计的主要安全目标是使得找到各类碰撞最有效的方法是通用攻击。哈希函数的困难性可直接假设等同于理想的通用攻击的复杂度，其安全性并不会随着设计的优化而减弱。哈希函数多用于数字签名算法，其中最具代表性的由 Merkle 提出的数字签名方案 MSS 采用哈希树将多个一次性验证密钥的有效性降低到一个公钥的有效性。在后量子标准化过程中，取得重要进展的代表性算法包括 XMSS 和 SPHINCS+。XMSS 是一种有状态的签名，是在 MSS 基础上提出的一种具有更小签名的可证明安全的数字签名方案。SPHINCS+ 签名算法是一种无状态的签名，采用了一种在 Merkle 树和 Goldreich 树之间相折中的 SPHINCS 超树的结构进行构造。基于哈希函数的签名方案的理论安全性高，但也存在签名体积过大，有状态的哈希签名所能支持的签名次数有限等缺点。尽管目前基于 Hash 函数的数字签名方案成果并不多，但是由于 Hash 函数独特的属性及其实用性，在后量子时代，基于 Hash 函数的签名算法具有巨大的潜力。

基于曲线同源的密码：同源是指两条椭圆曲线之间存在一个映射，这个映射能够保持它们的群结构同态。同源密码包括超奇异同源 Diffie-Hellman（SIDH）和 CSIDH 等公钥密码算法，可用作传统的椭圆曲线密钥交换（ECDH）的后量子替代。2011 年 Jao 等人首次提出了超奇异同源 Diffie-Hellman 问题，并设计了基于超奇异同源的公钥密码系统 SIKE。与其他几类算法相比，其公钥和密文尺

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的算法低两个数量级，这使其不易实现在一些计算性能不足的设备上。SIKE 算法在 2022 年 7 月进入了 NIST-PQC 评估的第四轮，但仅 1 个月不到就遇到了致命性的攻击。但是，SIKE 的失败并不意味着同源密码的崩塌，同源问题本身并未被破解，仍是后量子密码的重要研究方向之一。

2.2 后量子密码算法的标准化进程

（1）美国 NIST-PQC 后量子密码算法候选标准征集工作

美国国家标准与技术研究所（National Institute of Standards and Technology，NIST）于 2016 年启动了全球征集后量子密码候选标准算法的工作[7]，目前已进入第四轮。其中，第一轮入选了 69 个算法，第二轮入选了 26 个算法，第三轮入选了 15 个算法且分为两组：Finalists 和 Alternates。前者在第三轮评估结束后即可进入标准化阶段，后者还要经过第四轮评估才有望成为潜在的标准候选者。Finalists 包括 7 个算法，其中密钥封装算法包括 Kyber、NTRU、SABER、Classic McEliece 共 4 个算法，而签名算法包括 Dilithium、Falcon、Rainbow 共 3 个算法。Alternates 包括 8 个算法，其中密钥封装算法包括 Bike、FrodoKEM、HQC、NTRUprime、SIKE 共 5 个算法，而签名算法包括 GeMSS、Picnic、Sphincs+ 共 3 个算法。

2022 年 7 月，NIST 发布第三轮评估报告 NIST IR 8413[24]，宣

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

布了第一批标准算法。同时 NIST 也宣布将通过一轮独立于原项目第四轮评估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。到 2023 年 6 月 1 日截止，共有 40 个新的后量子签名算法提交，目前正在第一轮评估中[8]。

2023 年 8 月，NIST 发布了后量子密码学的初始公开标准草案：基于有结构格的公钥加密/密钥封装算法 Crystals-Kyber[25]，以及基于有结构格的公钥签名算法 Crystals-Dilithium[26]、Falcon 与基于哈希的公钥签名 SPHINCS+[27]。最终标准预计将于 2024 年发布。随后 NIST 将发布弃用 RSA、Diffie-Hellman 和椭圆曲线加密技术的指南。

值得注意的是，NIST-PQC 标准化项目中，中国学者主导或参与提交了多个后量子密码算法，其中第一轮竞赛中有 7 个密码算法参与评选，其中由中科院信息工程研究所路献辉教授团队设计的 LAC 算法进入了第二轮。另外，目前正在进行的针对后量子数字签名算法展开的附加轮征集中，也有 8 个国人参与设计的密码算法。

表 2 中国学者参与 NIST 竞赛的后量子密码算法

算法名称	主要作者	挺进轮次
Ding Key Exchange	Jintai Ding、Xinwei Gao 等	第一轮
Gui	Jintai Ding、Ming-Shen Chen 等	第一轮

[8] https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures

KCL	Yunlei Zhao、Zhengzhong Jin 等	第一轮
LAC	Xianhui Lu、Zhenfei Zhang 等	第二轮
Lepton	Yu Yu、Jiang Zhang	第一轮
MQDSS	Ming-Shing Chen 等	第二轮
Rainbow	Jintai Ding、Ming-Shen Chen 等	第三轮
HuFu	Yang Yu、Xiaoyun Wang 等	签名附加轮
SNOVA	Lih-Chung Wang、Jintai Ding 等	签名附加轮
TUOV	Jintai Ding、Boru Gong 等	签名附加轮
UOV	Jintai Ding、Ming-Shen Chen 等	签名附加轮
SPHINCS-alpha	Yu Yu、Hongrui Cui 等	签名附加轮
Lepton	Yu Yu、Jiang Zhang 等	签名附加轮
Preon	Ming-Shing Chen、Yu-Shian Chen 等	签名附加轮
Xifrat1-Sign.I	Jianfang "Danny" Niu 等	签名附加轮

（2）欧盟后量子密码标准化工作

欧盟并没有公布单独的后量子密码标准化计划，而是考虑沿用但又不局限于 NIST 遴选出来的候选标准算法。事实上，欧盟通过其“地平线 2020”项目[28]，配合了美国 NIST-PQC 后量子密码候选标准算法的征集活动。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。在德国 BSI[7]、法国 ANSSI[12]、荷兰 AIVD[8] 等欧盟国家的监管机构发布的后量子密码白皮书中，均表示在使用 PQC 算法的过程中会重点参考 NIST 标准的评估结果。

德国联邦信息安全办公室（Bundesamt für Sicherheit in der Informationstechnik，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（BSITR-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，尽管德国 BSI 扔试图推动这两个算法在 ISO 的标准化（PWI19541），但现在改项目的状态似乎已经被取消[29]。法国国家信息系统安全局（Agence nationale de la sécurité des systèmes d'information，ANSSI）表示会严格遵循 NIST-PQC 流程，但认识到还有其他替代方案，所以其并不打算将推荐的后量子算法限制为 NIST 获胜者，并且可能会考虑其他算法。荷兰内政王国关系部情报安全总局 (Algemene Inlichtingenen Veiligheidsdienst, AIVD) 推荐使用 SPHINCS-256 作为无状态数字签名、XMSS 作为有状态数字签名。

（3）其它国家和国际化组织的后量子密码标准化工作

英国国家网络安全中心（NCSC）建议 ML-KEM-768 和 ML-DSA-65 为大多数用例提供适当级别的安全性和效率，在部署生产系统之前，用户应等待基于最终 NIST 标准的实施的可用性[30]；加拿大网络安全中心并未开发自己的 PQC 算法，而是与 NIST 合作开发 PQC。

在澳洲，澳大利亚网络安全中心（Australian Cyber Security Cen-

tre，ACSC）未开发 PQC 算法，选择将由 NIST 流程通知。新西兰政府通信安全局 (GCSB) 在选择 PQC 算法之前将审查 NIST 运行的 PQC 国际标准化计划的结果；

在亚洲，日本、新加坡等国表示将参考 NIST 的标准化方案。韩国 PQC 标准化项目 KpqC[9] 于 2021 年宣布启动[9]，遴选过程计划分两轮。第一轮评估已经于 2023 年底完成，共有 15 个算法提交，最终有 8 个算法胜出，进入第二轮评估——预计将于 2024 年 11 月结束。

欧洲电信标准化协会 (ETSI)、国际互联网工程任务组 (IETF)、美国电气和电子工程师协会 (IEEE)、国际标准化组织 (ISO) 等均在后量子标准化方面做了大量工程，制定了系列标准，如 ETSIGR QSC 001《量子安全算法框架》、IETF RFC 8391 《XMSS:eXtended Merkle Signature Scheme》、IEEE 1363.1-2008《IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices》等。

（4）我国后量子密码标准化的准备工作

我国后量子密码标准算法的公开征集工作尚未正式启动，但是已经做了一系列准备工作。2018 年 6 月，中国密码学研究会（CACR）启动了全面密钥算法设计竞赛[31]。该竞赛历时一年半，最终于 2019 年 12 月底遴选出了 14 个后量子公钥密码算法（见表3）。

[9] https://www.kpqc.or.kr/

表 3 全面密码算法设计竞赛优胜算法（后量子公钥密码部分）

所获奖项	算法名称	主要作者	算法种类
一等奖	Aigis-sig	张江	数字签名
	LAC.PKE	路献辉	公钥加密
	Aigis-enc	张江	公钥加密
二等奖	LAC.KEX	路献辉	密钥交换
	SIAKE	薛海洋	密钥交换
	SCloud	郑中翔	公钥加密
	AKCN-MLWE	赵运磊	公钥加密
三等奖	Piglet-1	王丽萍	公钥加密
	TALE	潘彦斌	公钥加密
	AKCN-E8	赵运磊	公钥加密
	木兰	赵运磊	数字签名
	FatSeal	潘彦斌	数字签名
	PKP-DSS	林东岱	数字签名
	SKCN-MLWE	赵运磊	密钥交换

2023 年，国家标准化管理委员会发布的《2023 年全国标准化工作要点》[32] 指出要开展后量子密码准的前瞻研究和规划布局。2024 年的前沿研究[33] 透露，一些后量子密码方案已在我国密码行业标准化技术委员会立项[34]。

第三章 后量子密码迁移计划及面临的挑战

过往密码算法更替的经验表明，向后量子密码的过度是一个艰巨的任务，制定完善的后量子密码迁移计划变得尤为重要。该计划的总体目标是确保所有应用中使用的密码算法能够抵抗后量子计算攻击。这一计划是综合性的，涵盖了从评估现有密码体系的脆弱性到实施后量子算法替代方案的整个过程。计划的成功依赖于政府、学术界和工业界之间的协同合作，以确保系统的高效和安全迁移。

3.1 后量子密码迁移计划

量子危机逐渐逼近的当下，国内外研究机构和学者们正在推进密码算法和安全协议的标准化进程，以应对量子计算带来的威胁。同时，各国逐步开始针对后量子密码迁移发布指导意见。此外，国防、金融、电信等领域也对后量子迁移展开部署计划。本节将介绍国内外后量子密码迁移研究进展。

3.1.1 国际后量子密码迁移计划概览

（1）各国后量子迁移规划及指南

美国：2023 年 5 月，NIST 发布一系列特别出版物的草案[1-3]：《NIST SP 1800-38A：向后量子密码学的迁移：考虑量子安全密码学的实现和采用的准备》、《NIST SP 1800-38B：迁移至后量子密码学的量子就绪：密码学发现》、《NIST SP 1800-38C：迁移至后量子密码学量子准备性：测试草案标准》，旨在指导行业有序进行后量子迁移。

加拿大：2023 年加拿大创新、科学和经济发展部 (ISED) 发布了第三版《加拿大国家量子就绪：最佳实践和指南》[35]。该文件概述了三个 PQC 用例、PQC 库存清单、加密敏捷性用例、PQC 供应商路线图以及第三方评估清单[35]，以指导企业解决密码学相关量子计算的威胁。

日本：2019 年 8 月，日本银行金融研究所（Institute for Monetary and Economic Studies Bank of Japan，IMES BOJ）发布了研讨论文《支持加密迁移以应对量子计算机带来的威胁》，为日本的后量子迁移给出了指导计划[10]。

韩国：2023 年 7 月，韩国国家情报局和科学技术信息通信部（The Ministry of Science and ICT，MSIT）发布的 POC 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[11]。

澳大利亚：2023 年 5 月，ACSC 更新了《后量子密码学规划》，并计划更新澳大利亚信息安全手册以解决 PQC[13]。

荷兰：2023 年 3 月，荷兰国家通信安全局（AIVD TNO CWI）发布了《PQC 迁移手册：迁移到后量子密码学的指南》以指导向 PQC 的迁移[36]。

（2）分领域后量子迁移计划

国防领域： 2022 年 5 月 4 日，白宫发布了一份国家安全备忘录，目的是“促进美国在量子计算方面的领导地位，同时减轻脆

弱加密系统风险”[37]。该备忘录确定了维持国家在量子信息科学(Quantum Information Science, QIS)中的竞争优势所需的关键步骤，并在美国开始将脆弱的计算机系统迁移到抗量子密码学的进程中指导各机构采取具体行动。2023 年 6 月 8 日 QuSecure宣布美国陆军授予该公司小企业创新研究 (SBIR) 第二阶段联邦政府合同，以开发量子弹性软件解决方案[38]。2023 年 6 月 27 日 SandboxAQ 宣布获得美国颁发的《量子抗性密码学公钥基础设施其他交易授权协议》[39]。2023 年 8 月 30 日 QuSecure 公司宣布被美国空军全球打击司令部 (AFGSC) 和小企业咨询公司 (SBCC) 评为年度商业能力展示奖竞赛的获奖者[40]。

金融领域： 2022 年 6 月，国际清算银行在其创新中心启动了一项关于后量子加密和支付的研究项目：“该项目将调查和测试能够承受量子计算机处理能力大幅提高的潜在加密解决方案。目标是测试各种支付系统中的用例，并研究引入后量子密码技术将如何影响其性能。”[41]。2022 年 9 月，存款信托和清算公司 (DTCC) 发布了一份白皮书，就 PQC 对银行间结算和支付的影响向清算银行成员和银行业提出了建议[42]。2022 年 9 月，法兰西银行（法国中央银行）称已于在其创新中心测试了 PQC 的实施情况[43]。世界银行将 PQC 列入银行需要采取行动的未来技术清单及其教育课程。

电信领域：2023 年 2 月 17 日，GSMA PQTN 工作组发布了《PQ.01：后量子电信网络影响评估白皮书》，分析了电信行业向量

子安全技术过渡的依赖性和时间表[4]；2023 年 9 月 22 日，GSMA PQTN 又发布了《PQ.02：电信公司量子风险管理指南》，旨在确保主要利益相关者和企业主拥有在正确的时间范围内做出适当的量子风险管理 (QRM) 决策所需的信息[5]；2024 年 2 月 22 日，GSMA PQTN 发布的《PQ.03：后量子密码学：电信用例指南》提供一组最佳实践指南，可用于支持电信生态系统背景下的量子安全加密路线图[6]。

3.1.2 我国后量子密码迁移研究现状

在国内，2023 年 4 月，赛迪智库发布的《应对量子计算挑战需积极推进后量子密码研发和迁移》中提出了一些建议，呼吁尽快在国家层面统筹开展为期 10-15 年的后量子密码研发和迁移计划[14]。信通院于 2023 年 11 月发布的《后量子密码应用研究报告》也提出后量子密码迁移必须尽早提上日程。同时报告中也研究了行业迁移策略、预测了迁移时间、分析了迁移挑战[15]。

在金融领域，2022 年，中国人民银行《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，指出要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。部分银行机构正在考虑《金融系统应用后量子密码技术指南》，以指导后量子密码的改造和应用，同时确保符合监管要求。

在电信领域，中国电信安全公司与北京大学、中国科学院大学、数盾科技等机构合作开展后量子密码产品研究，已经在电信“密评助手”密码服务管理平台上对基于 Kyber 算法的多个密码运算接口适配。2024 年 5 月，电信安全公司推出的安全网关设备融入了后量子密码卡，融合了国产 LMS/HSS-SM3 签名算法，集成了 Kyber 和 Dilithium 等国际后量子密码算法，实现了基于后量子密码的安全密钥协商、端对端身份认证，可通过灵活的选择加密方案，有效的抵御量子攻击。

在隐私计算领域，2023 年 11 月发布的《中国电信后量子隐私计算白皮书》[16] 提到，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。其中还介绍了基于后量子密码算法和隐私增强技术构建的试验型平台系统——密流量子盾（PrivTorrent Quantum Shield），围绕量子计算可能引入的新型安全威胁，提供有效抵御量子计算及传统计算机攻击的密码算法迁移方案。

3.2 后量子密码迁移的路线图

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：

（1）建立后量子密码迁移路线图

如图2所示，后量子密码迁移路线图是一个指导后量子密码就绪工作的多步骤方法。通过建立后量子密码迁移路线图可以更好的组织应对量子计算机带来的一系列工作。通过获取后量子密码迁移路线图的执行结果，可以进一步完善路线图，并获得后量子密码迁移推进过程中的重要工作范围、分布、特征和需求。

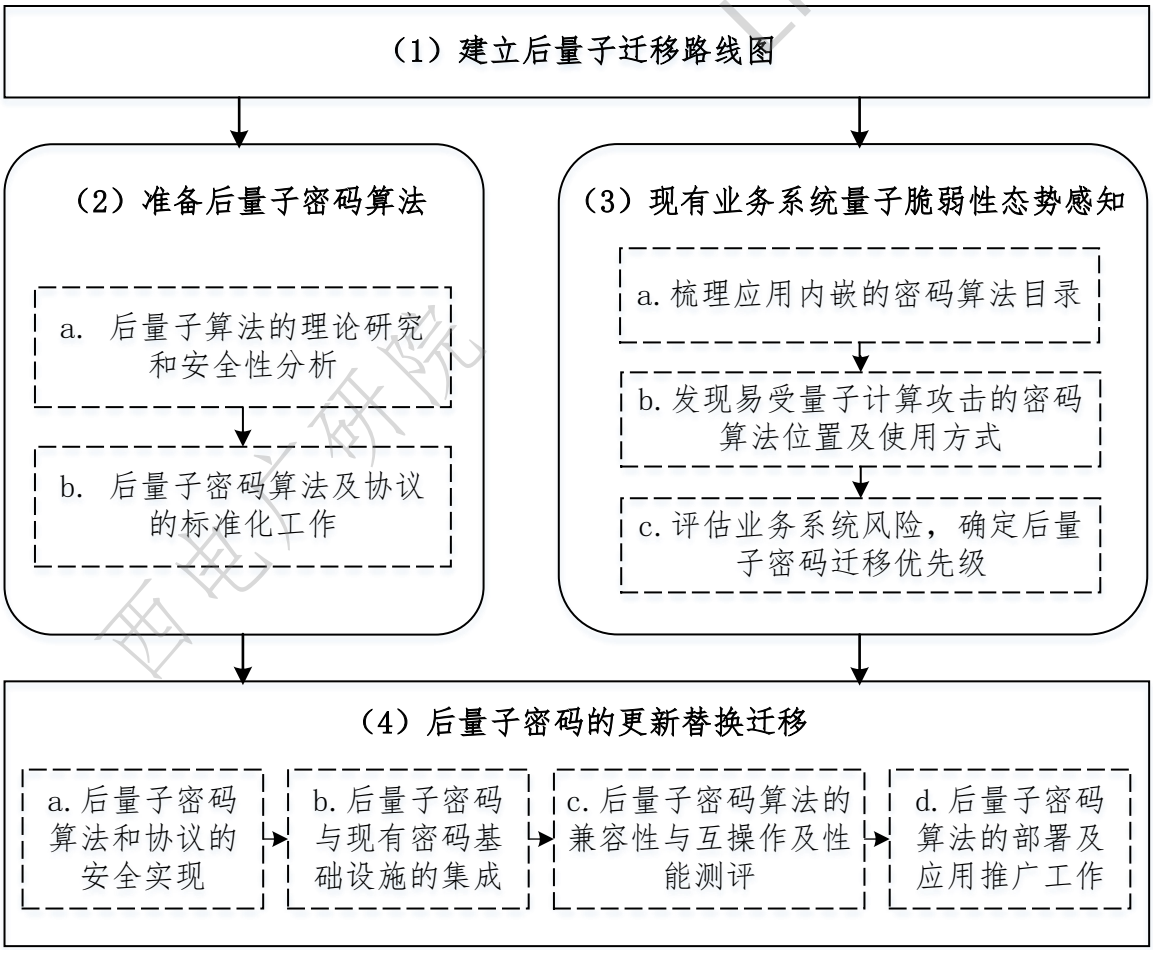

图 2 量子就绪路线图

（2）准备后量子密码算法

建立后量子密码迁移路线的首要任务是提供足够充足的后量子密码库存。完成这一任务的步骤需要经历以下两个过程：

a. 对后量子算法的理论研究和安全性分析。除了对上述各种技术路线的 PQC 算法的研究，还要关注于对算法的安全性评估，包括后量子攻击、数学问题的难度、侧信道攻击抵抗等多方面。

b. 后量子密码算法及协议的标准化工作。后量子算法及协议的标准化需要在行业或国家层面形成统一的算法共识，并通过一系列相关专利形成知识产权专利墙。

（3）现有业务系统量子脆弱性态势感知

进行后量子密码迁移的前提是对当前部署系统中的脆弱密码组件具有充足的了解。对密码系统脆弱性进行态势感知需要关注以下步骤：

a. 梳理应用内嵌密码算法目录。除了要梳理代码开发时所调用脆弱的密码算法，还需要对操作系统、依赖项目、网络组件中可能调用的密码算法进行梳理，以明确脆弱性发现的检测目标。

b. 发现系统易受量子攻击的密码算法所在位置及使用方式。应用系统内存在着多种密码组件，需要摸清这些易受量子攻击的密码算法在系统中的具体位置，以及这些密码算法的使用方式，实现对系统量子抗性的全盘摸底。

c. 评估业务系统风险，确定后量子密码迁移优先级。由于后量子密码算法的迁移是一个持续的过程，通过建立合理的风险模型并凭借风险优先级安排合理的迁移顺序。

（4）后量子密码的更新替换迁移

在最终推广后量子密码的迁移进程时，还要做好以下关键步骤，包括：

a. 后量子密码算法和协议的安全实现。需要产业界积极响应，推出后量子密码产品或开源项目。

b. 后量子密码与现有密码学基础设施的集成。在后量子密码迁移早期采用后量子密码与现有密码集成的方式，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。

c. 后量子密码算法的兼容性与互操作及性能测评。在不同单位完成 PQC 算法协议的实现后，对其成果进行充分的互操作性和性能测试，能够为密码算法的替代提供更充分的选取参考。

d. 后量子密码算法的部署及应用推广工作。完成上述一系列工作后，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。

3.3 挑战一：现有业务系统量子脆弱性发现及风险评估难

现有的业务系统错综复杂，内生安全模块的量子脆弱点位置及使用方式难感知。业务系统通常由多个子系统和模块组成，这些模块之间通过各种接口和协议进行通信。内生安全模块嵌入在这些复杂系统中，负责数据加密、身份验证、权限管理、日志记录等安全功能。多种传统密码算法被广泛使用以保障系统的安全性。底层硬件利用对称密码 AES 和公钥密码 RSA、ECC 等来提供安全服务；在应用层，签名认证则需要用到数字签名技术；而在通信过程中，使用的安全协议则是密码算法的综合运用，如 SSL/TLS 协议。基于场景的差异，即使是同一个系统，其内部的密码算法也需要进行修改和更新，这也是造成系统内部密码算法复杂的原因之一。如何及时准确地发现易受量子计算攻击的密码算法所在位置及使用方式是当前面临的关键挑战。

针对量子攻击的行业风险评估模型滞后，如何针对不同的场景对所发现的量子脆弱点进行风险评估并给出迁移的优先级也是一个重要挑战。在完成企业内部信息系统的后量子脆弱性发现后，一些企业可能更倾向于组建一个专门的技术团队，并持续安排和组织后续的改造任务。但由于人力物力成本的限制，同时对企业的所有系统进行改造是不现实的。根据安全风险的高低，依次对相应的组件进行改造，才能及时保障企业整体利益的最大化。

3.4 挑战二：现有后量子密码算法安全实现及热迁移难

迁移实施过程中首先面临的挑战是如何在不影响现有系统正常运行的同时完成密码算法的热迁移。后量子密码算法标准处于初步完成阶段，一些后量子密码的交互逻辑与旧系统不兼容，例如基于哈希函数的 SPHINCS+ 签名算法需要双方维护一个长期存在的密钥，而调用签名算法的旧系统则未必具有维护长期密钥的能力。还有一些后量子密码的性能开销导致无法在旧系统正常运行，Kyber768 在实现 TLS 的三次握手时，过大的 HelloClient 可能会超出旧有底层硬件的处理能力，进而导致协议的异常中断。后量子密码算法与传统密码算法有不同的交互和性能特性，如何在不影响现有系统正常运行的同时完成密码算法的热迁移成为迁移平稳过度的关键挑战。

另外，迁移实现还需要支持不同后量子密码算法的可插拔设计以及互联互通，并且当算法失效时，业务机制还需要支持回滚。这里的算法失效指的是：有可能选用的后量子密码在量子计算机出来之前就已经被经典电子计算机攻破，这种事情也有可能发生，比如 SIKE 算法在刚进入第四轮评估一个月就被攻破，这时，现阶段系统要有能力退回到之前不抗量子的系统，或者迅速切换到其他未被攻破的算法。

第四章 现有业务系统量子脆弱性发现

4.1 量子脆弱性发现的工作流及架构描述

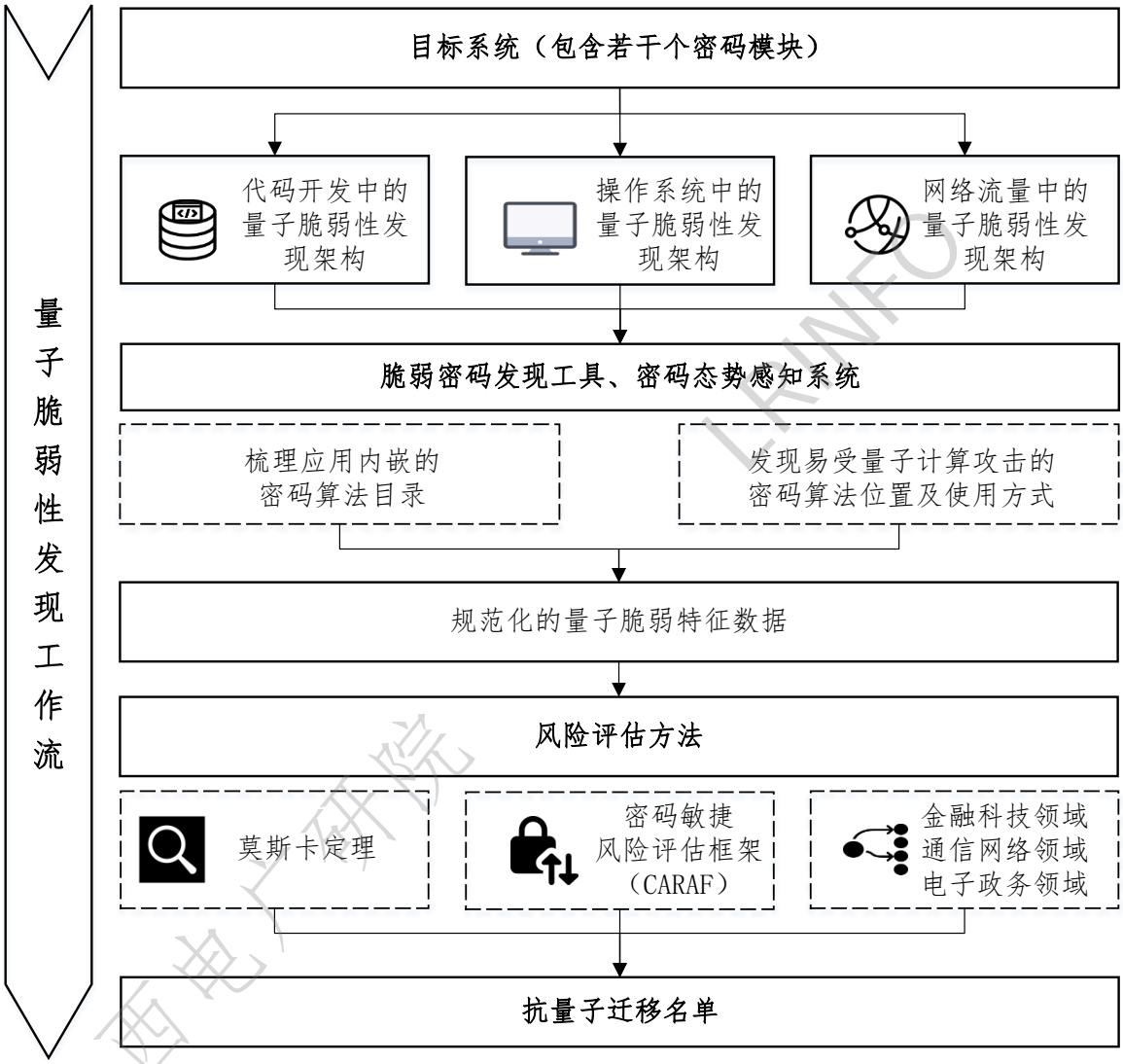

图 3 量子脆弱性发现总框架

图 3 是本节描述的现有信息系统量子脆弱性发现的整体工作流及具体架构。在该流程中，首先需要确定目标系统，目标系统可以是持续集成持续交付的代码开发系统、可以是终端或者服务器的操作系统、也可以是提供网络服务的传输系统。针对不同的目标系

统，可以通过以下三种后量子密码脆弱性发现框架，包括：源代码中的量子脆弱性发现架构、操作系统中的量子脆弱性发现架构，网络流量中的量子脆弱性发现架构。通过应用这些脆弱密码发现架构并部署相关的脆弱密码发现工具，可以梳理目标系统内嵌的密码算法目录，并发现易受量子计算攻击的密码算法位置及使用方式。随后，这些信息被规范化为量子脆弱特征数据，并被输入特定的风险评估框架中，最终根据风险管理策略给出后量子迁移名单。每个过程将在下面的小节具体描述。

4.1.1 代码开发中的量子脆弱性发现

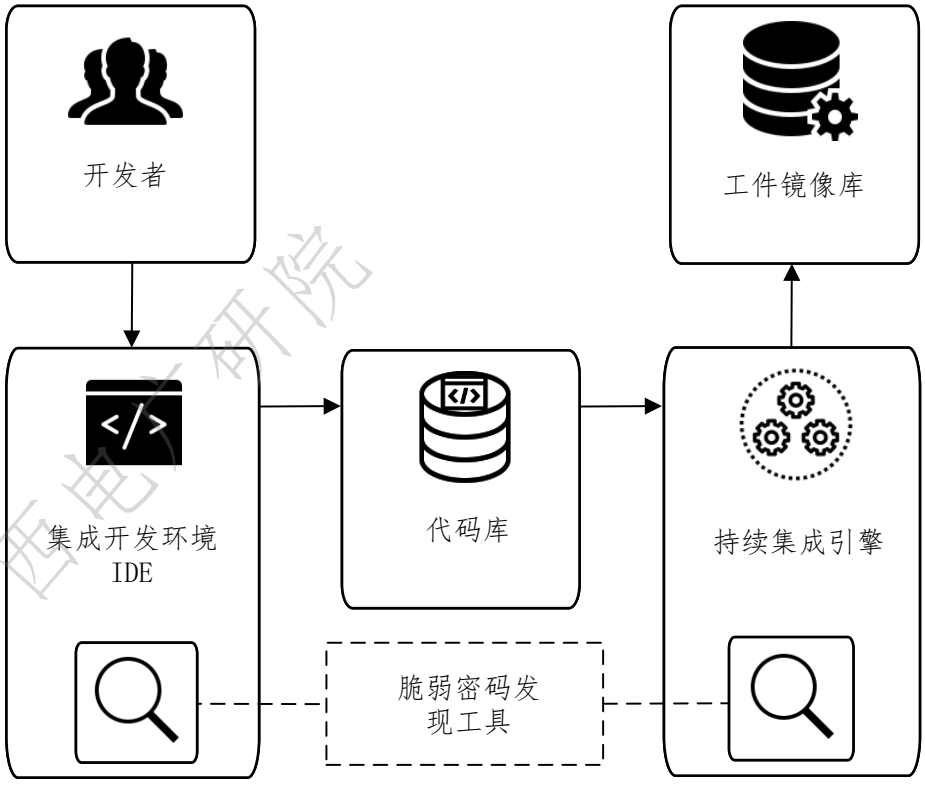

图 4 代码开发中的量子脆弱性发现架构

本节介绍代码开发中的量子脆弱性发现架构，该架构基于现有

的持续集成持续交付的代码开发系统。如图 4 所示，以一个用于持续集成的代码开发系统为例，该系统需要拉取代码并调用构建和测试工具，并将经过测试的工件存储到镜像库中。

在这个持续集成的过程中，存在两种触发脆弱密码发现活动的情况，第一类情况是开发者在本地部署的集成开发环境中直接调用静态应用安全检查工具，他们可以在代码构建的命令中手动添加运行发现工具的命令，或者直接在 IDE 插件中自动化运行；第二种情况是运行持续集成引擎的云平台在接收到对代码库的拉取请求时，触发内置的自动化静态应用安全检查工具。持续交付流水线中集成了脆弱密码发现功能的部分，在图 4 中以静态应用安全测试标出。

4.1.2 操作系统中的量子脆弱性发现

本节介绍操作系统中的量子脆弱性发现架构，该架构通过对终端设备或服务器中部署的操作系统的文件系统进行扫描来完成脆弱性发现。如图 5 所示，一个组织可以选择通过现有的自动化部署工具将文件系统扫描传感器部署到操作系统中。随后可以手动或者通过自动机制触发扫描，并将结果传输到后端分析引擎。

这种框架已在 x64Linux 和 Windows 主机上进行了验证，更多其它平台可能需要专门的发现平台进行支持。同时，一些解决方案还提供与端点检测和响应 (EDR) 平台的集成，结合了基于规则的自动化响应和分析能力，以实时连续监控和收集端点数据，能够充分利用现有的网络安全审阅和可视化能力。此外，扫描还会在二进

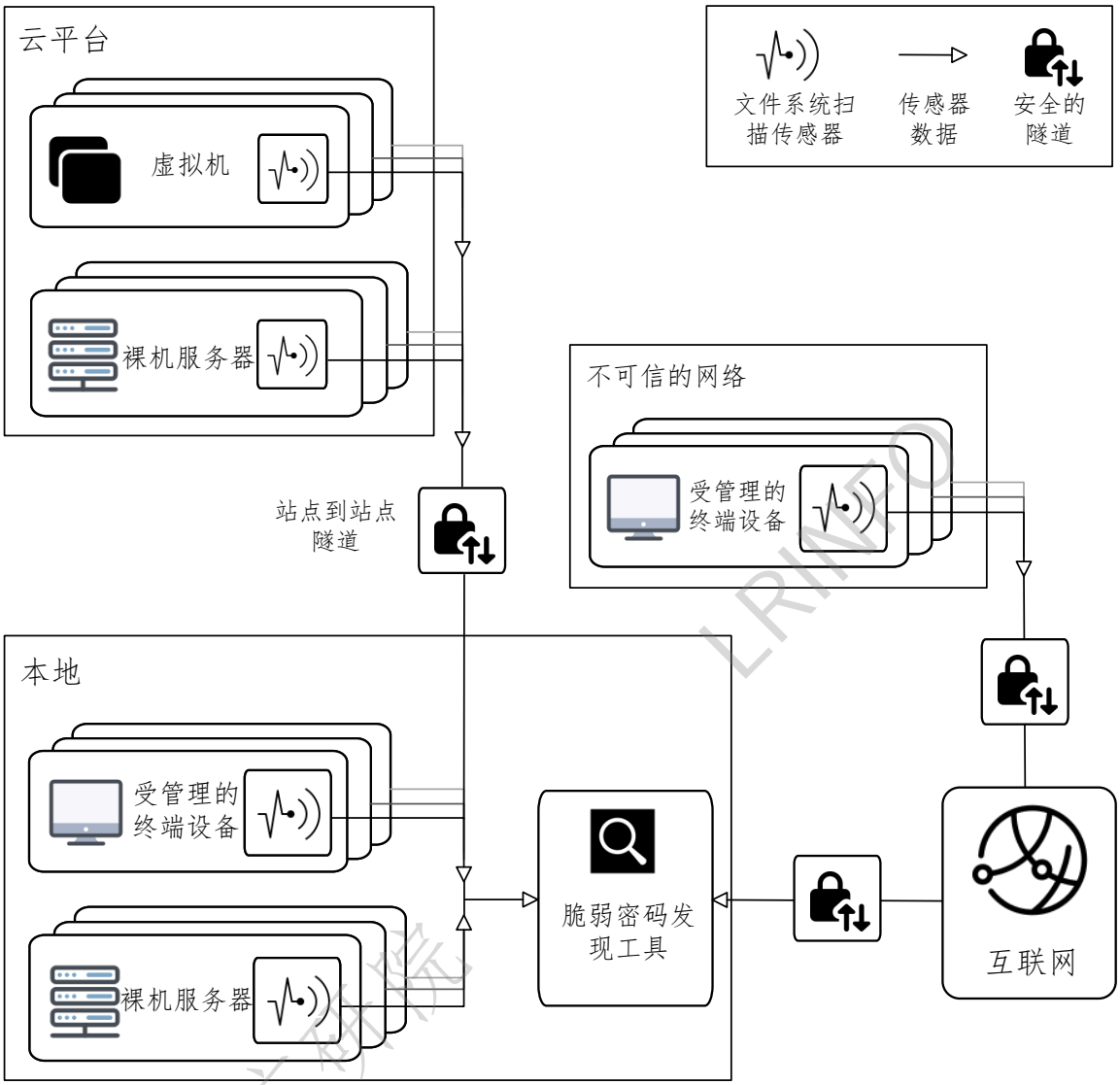

图 5 操作系统中的量子脆弱性发现架构

制文件中进行，以发现可能没有源代码的算法。

4.1.3 网络流量中的量子脆弱性发现

本节介绍网络流量中的量子脆弱性发现架构，该架构通过对本地及网络设备中部署的企业内部服务（例如人力资源、财务、信息技术等）的网络流量进行捕获以进行脆弱性检测。如图 6 所示，架构包括对云端、本地和不受信任网络三种不同的情况进行的讨论。

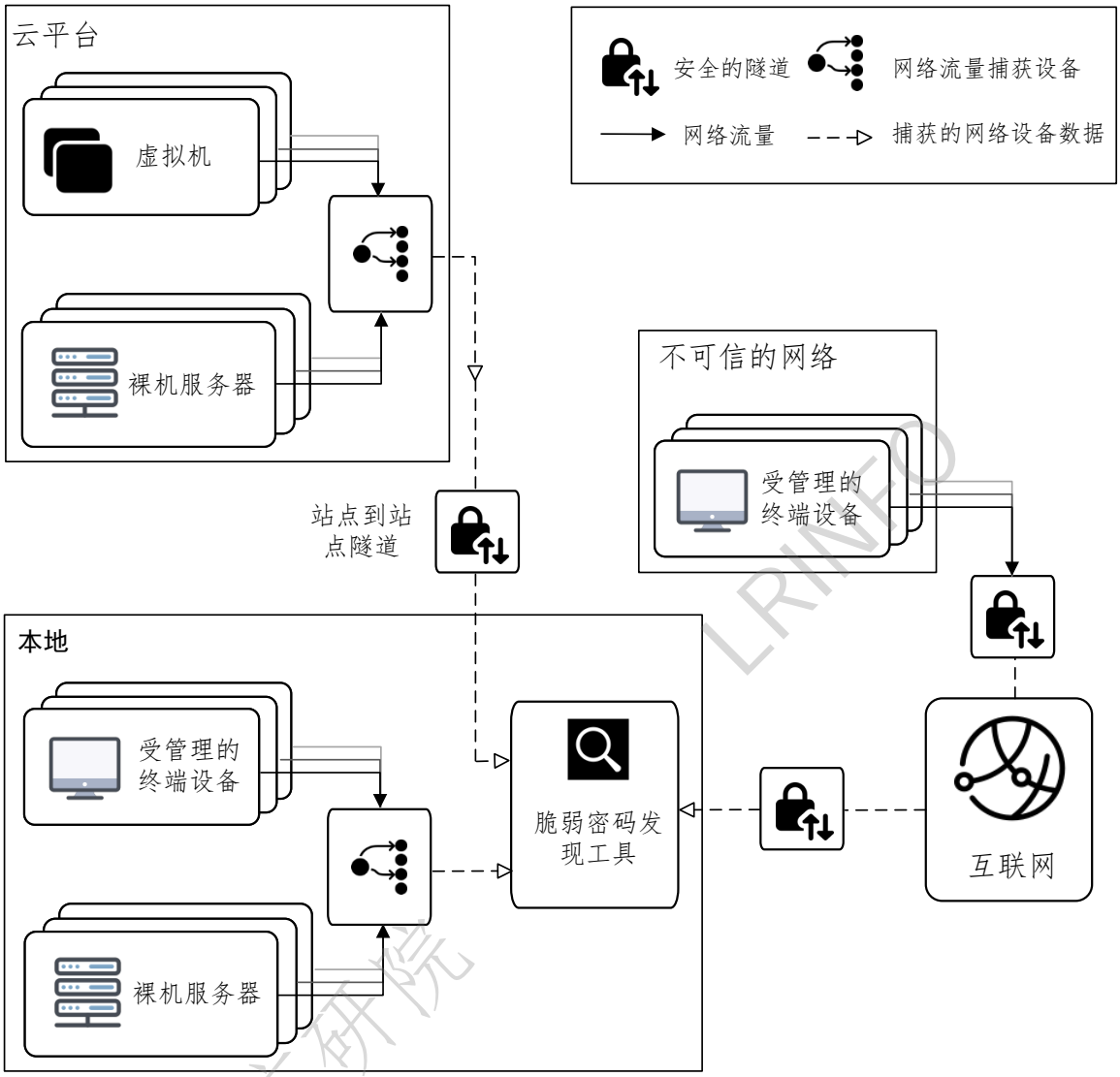

图 6 网络流量中的量子脆弱性发现架构

当内部服务托管于云端部署的裸机和虚拟系统时，其中的网络数据包将首先被镜像到基于云的网络流量捕获应用中，但这种捕获应用的实现取决于云服务提供商。随后被捕获的网络流量通过安全信道路由到本地部署的后量子脆弱发现工具中以完成脆弱密码发现。本地网络部分的系统除了负责托管公司的内部服务，还为用户使用的受公司管理的终端设备（如笔记本电脑）提供支撑。在这里，

网络流量可以直接由物理交换机捕获，并将其路由到本地的网络流量捕获设备。最后，一些以公司形式管理的终端设备会以远程用户形式进行操作，其中产生的网络流量无法直接实时转发到脆弱密码发现工具。在这种情况下，网络流量被捕获为文件，并通过安全隧道异步转发到发现工具。

4.2 量子脆弱性的密码态势感知工具及案例

为了能够及时发现现有密码体系中的量子脆弱性，国外各个研究团队都提出了自己的脆弱密码发现工具。同时，国内的许多组织和公司也具有能够完成脆弱密码发现任务的密码态势感知工具。本节将从国外和国内两个维度分别介绍其中一些工具和平台。

4.2.1 国外的密码态势感知工具

（1）IBM 系列

IBM 除了积极推动后量子密码算法的标准化实现外，在量子脆弱性发现上的工作也十分充分。其技术贡献包括对 IBMz16 大型机环境的 z/OS 镜像以及工作站服务器的远程访问技术、具备脆弱密码发现能力的软件、硬件和工具。该系统托管在 IBM 的一个设施中，可通过 VPN 从 NCCoE 实验室进行远程访问，允许合作者通过实际操作理解 IBM 的脆弱密码发现技术，这些技术可以在应用程序中（无论有无源代码）发现加密的使用情况以及网络连接情况。

表 4 IBM 的密码态势感知工具

产品或技术名称	介绍
IBM z/OS Integrated Cryptographic Service Facility (ICSF)	IBM z/OS ICSF 通过编写系统管理设施（SMF）活动日志记录来捕获与加密相关的信息，这些记录汇总了加密引擎、服务和算法的使用情况。这些信息在应用程序运行时动态捕获，既可用于汇总清单，也可用于在整个迁移过程中进行审计和观察。
IBM Application Discovery and Delivery Intelli-gence (ADDI) v.6.1	IBM ADD 是一个静态分析工具，用于分析 COBOL 应用程序源文件，捕获所有 ICSF 加密服务、与这些服务关联的参数以及有价值的元数据，并生成加密发现报告。
IBM Crypto Analytics Tool (CAT)	IBM CAT 是一种基于可配置的政策从 z/OS 环境中提取安全和加密信息，生成快照的工具。它提供了由 ICSF 和 RACF 管理的密钥详细信息，有助于识别不安全的密钥、算法和服务。该工具提供的信息有助于识别并解决与加密和安全相关的问题。
IBM zOS Encryption Readiness Technology (zERT)	IBM zOS zERT 收集并报告使用 TLS/SSL、SSH 和 IPSec 等加密网络安全协议的 IPv4 和 IPv6 连接的加密安全属性。该工具有助于提供链接密钥、证书和使用它们的应用程序的上下文。它能识别安全协议、加密算法、密钥长度等，这些都是在加密发现过程中需要掌握的重要信息。

（2）三星系列

三星数据科学研究所提供云和数字物流服务。三星数据科学研究所利用三星云平台构建优化后的云环境，并提供一体化管理服务以及在许多用例中已证明成功的 SaaS 解决方案。提供服务的核心

能力之一是网络安全，而密码技术对于增强安全性起着至关重要的作用。为此，三星数据科学研究所从事各种密码学研发活动，包括密码技术的设计、实施和架构设计，包括后量子密码学。

表 5 三星的密码态势感知工具

产品或技术名称	介绍
Samsung SDS Crypto Agility Platform for Enterprise (S-CAPE)	Samsung S-CAPE 是一个能够发现企业 DevSecOps 管道中易受 PQ 漏洞影响的算法的平台。它通过整合来自各种传感器的数据为企业提供对已识别 PQ 漏洞的可见性和风险评估分数。
Samsung SDS SECUI BLUEMAX NGF VE	NGF VE（Network Gateway Firewall Virtual Environment）是一个为检测量子后门漏洞的网络流量所配置的虚拟防火墙。

（3）Infosec Global (ISG) 系列

ISG 是一家快速增长的网络安全公司，在密码学敏捷管理、密码学发现和后量子密码学领域提供创新解决方案。ISG 在全球设有加拿大、瑞士和美国的办事处。ISG 团队汇集了最佳密码学专家（包括 SSL 之父）和经验丰富的业务领袖，他们在全球建立和增长新业务方面经验丰富。

表 6 ISG 的密码态势感知工具

产品或技术名称	介绍
InfoSec AgileSec Analytics Enterprise Server	InfoSec AgileSec Analytics Enterprise Server 是一个企业级安全解决方案，旨在帮助公司建立一个全面的、集中的库存，包括所有加密资产，如加密密钥、密钥库、X.509 证书、加密库、加密算法和加密协议。
InfoSec AgileSec Analytics Dashboard	InfoSec AgileSec Analytics Dashboard 是一个核心组件，它使公司能够根据自定义的加密策略来审查加密库存并主动识别加密弱点、合规差距或量子易受攻击的对象。
InfoSec AgileSec Sensors	InfoSec AgileSec Sensors 是 AgileSec Analytics 的核心组件，用于扫描数字足迹中部署的不同技术和系统。传感器可用于扫描主机（文件系统，二进制数据，运行进程，证书存储），网络接口，CI/CD 管道，应用程序仓库，密钥管理系统，PKI 系统，HSM 系统和其他技术。
AgileSec Analytics Vulnerability Response Connector	AgileSec Analytics Vulnerability Response Connector 允许公司使用他们现有的解决方案（如 ServiceNow）来处理在他们的数字足迹中发现的加密漏洞的修复工作。
AgileSec Agility SDK	AgileSec Agility SDK 是一个用于构建应用程序的软件工具包，它允许公司在敏感的业务应用中实现加密的灵活性。通过 AgileSec Agility SDK，开发者可以将加密操作从他们的工作中抽象出来，并通过策略进行管理，从而实现从经典到后量子、国家或任何其他未来加密标准的无缝迁移。

（4）其他

SandboxAQ 推出了 Security Suite，ISARA Corporation、微软和思科也都推出了自己的脆弱密码发现产品。

表 7 其他的密码态势感知工具

产品或技术名称	介绍
(SandboxAQ) Security Suite Discovery Modules	(SandboxAQ) Security Suite Discovery Modules 提供了加密的可观察性能力。这个模块分析了 IT 基础设施，并创建了一个加密库存，使利益相关者能够监控整个组织中谁/什么，在哪里，何时以及如何使用包括 PQC 的加密。
ISARA Advance® Cryptographic Discovery and Risk Assessment Tool	ISARA Advance® Cryptographic Discovery and Risk Assessment Tool 是一个用于分析和清点企业网络上加密的使用情况的平台。包括用于清点设备和服务器以及分析加密风险的功能，以帮助为加密迁移的资产排定优先级。结果可以在易于使用的仪表板上查看，或者导出到其他系统。
Microsoft CodeQL	Microsoft CodeQL 是 Visual Studio Code 和 GitHub 行动的一部分，它能够检测后量子时代的易受攻击的代码。
Cisco Mercury	Cisco Mercury 被用于后量子脆弱的网络数据包元数据捕获和分析。

4.2.2 国内的密码态势感知工具

国家密码管理局商用密码检测中心、国家信息技术安全研究中心、国家信息中心 (国家电子政务外网管理中心)、工业和信息化部

密码应用研究中心、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、中国科学院数据与通信保护研究教育中心、公安部第一研究所、公安部第三研究所、工业和信息化部电子第五研究所（中国赛宝实验室）、北京信息安全测评中心、北京银联金卡科技有限公司等 48 家商用密码应用安全性评估试点机构，以及国内信息安全等级保护测评单位，均提供各类密码态势感知服务。除此之外，一些公司也提供密码态势感知工具，如下表示例。

表 8 国内的密码态势感知工具

公司名称	产品或技术名称	功能
信安世纪	CSSP 全密码安全服务平台	结合客户需要和监管方面的要求，从前台业务接入到中台统一调度再到后台密码设备统一配置和管理以及整个业务态势的展示，提供了全方位的密码安全服务。
	NetCVM 密码安全可视化监管系统	提供统一、集中的密码应用设备集中监管服务，能够实时监控密码应用设备的状态、密码服务的状态以及代理状态的监控以及密码应用日志的集中审计。
	iCET 密评工具箱系统	提供合规的密评流程化管理，集成了信安世纪自主研发的专业的测评工具，为测评机构提供了流程引导、数字化管理以及专业的检测及分析工具。
纽创信安	密码态势感知平台	全天候不间断的监测网络流量和日志，检测安全漏洞。探测加密通信流量中可能存在的网络攻击、恶意软件威胁。

公司名称	产品或技术名称	功能
数盾科技	密码设备管理系统	提供统一设备监管能力，将上层管理应用的管理请求转换为标准的消息调用，实现管理应用与密码设备间的消息传递。
	密码态势感知平台	评估不同信息系统中的密码算法，检验其合规性、正确性及有效性，展示密码应用基本态势，确保密码应用的安全性。展示密码态势的关键指标，能够直观的监测运营情况，并可以对异常关键指标预警和挖掘分析。

4.2.3 量子脆弱性发现案例

为了更加具体的展示脆弱密码发现的工作流程，我们对三种脆弱密码发现架构各给出一个具体案例。以 Windows 开发环境下的代码开发业务小组的脆弱密码发现项目为例，根据前文给出的量子脆弱性发现框架，需要从代码、操作系统和网络流量三个方面进行量子脆弱性发现。

（1）代码开发中的量子脆弱算法发现示例

有关代码开发中的脆弱密码发现有两种方式：一是即时的通过集成开发环境（IDE）中的一些工具插件在代码开发过程中进行脆弱密码发现；二是滞后的在代码存入项目存储库后，在运行持续集成引擎时自动的完成发现。这里对两种方式的具体步骤展开介绍：

测试数据：

- 源代码
  - 使用 RSA 加密/解密应用的程序接口。
  - 使用 ECDSA 签名/验证应用的程序接口的使用。
- 依赖库、进程
  - KeyPairGenerator, KeyFactory, Signature, SignatureException 等 Java 类。

针对两种不同的场景，均可以采用上述数据集，但具体演示步骤及预期结果有所不同，具体而言，针对 IDE 的演示方式如下：

针对 IDE 的演示步骤：

1. 使用数据集的源代码在集成开发环境中创建一个开发项目。
2. 在集成开发环境中触发发现工具。

类似的，针对代码库进行检测时的演示方式如下：

针对代码库的演示步骤：

1. 克隆包含数据集源代码的存储库。
2. 更改代码库（例如，添加一条打印语句）。
3. 提交更改。
4. 在配置的远程版本库中创建拉取请求。
5. 自动触发代码扫描。

预期结果：发现工具会识别使用测试数据集中所述方法的文件

和代码行，并在版本库控制台中显示结果。

（2）操作系统中的量子脆弱算法发现示例

有关操作系统中的量子脆弱性发现主要针对两种文件：一是对操作系统中的应用程序进行脆弱性发现；二是对不可运行的文件，如证书、密码库等文件进行脆弱性发现。两种方式的具体设置如下：

测试数据：基于 Windows 11 的客户端，安装以下软件：
• 谷歌浏览器 • Java 运行环境 • OpenVPN 软件 • GRR 快速响应平台

针对可执行文件的检测：在 Windows 系统中，常见的可执行文件包括各种应用程序及其依赖库。具体在一个开发平台上，不可避免地需要用到浏览器应用以查找资料、编程应用以完成开发任务、网络应用以访问开发资源以及安全应用以保护开发环境。

针对应用程序的检测步骤：
1. 安装、配置和部署发现工具端点代理。 2. 根据发现平台的功能，记录发现的工件。

针对非可执行文件的检测：Windows 系统中潜在的量子脆弱非可执行文件主要包括各种密钥库。具体在一个开发平台上，需要包

括用于安全网络通信存储的密钥库、编程库中调用的密钥库、以及远程访问时创建的密钥库。

测试数据：使用量子脆弱算法的特定组件：
• 通过 OpenSSL 创建的 PKCS#12 密钥库 • 通过 keytool 实用程序创建的 Java 密钥库 • 通过 OpenSSL 创建的 PKCS#1 密钥库 • 通过 OpenSSL 创建的 PKCS#8 密钥库 • 通过 ssh-keygen 创建的 OpenSSH 密钥库

针对非可执行文件的检测步骤：
1. 创建一个完全更新的 Windows 10/11 虚拟机。 2. 安装发现工具传感器组件（如适用）。 3. 确认传感器组件与发现工具提供的后端系统之间的通信正常。 4. 将数据集文件移动到目标虚拟机的本地磁盘。 5. 触发发现传感器执行扫描

预期结果：发现工具传感器检测应用组件和数据集中的文件，并将结果记录在输出文件和（或）记录仪表板中，并将其传输到后端系统以供审查。

（3）网络流量中的量子脆弱算法发现示例

代码开发过程会不可避免的调用网络通信协议来访问企业内部的相关服务如人力、财务、业务对接等，这些业务往往会通过 TLS 进行通信层的保护。针对这种典型协议的脆弱性发现的具体步骤如下：

针对 TLS 协议流量的检测：

- **测试数据：**来自大型企业网络监控和主机监控的加密网络流量数据集。
- 步骤
  1. 配置发现工具以扫描第 4 层（传输）流量。此过程取决于个别发现工具的部署方法。
  2. 根据目标网络的需要修改测试数据包捕获 IP 地址。
  3. 使用 tcpreplay 等实用程序将 TLS 1.2 测试数据重放至已部署发现工具的网段。

预期结果：发现工具检测是否存在易受攻击的密钥交换/协议和身份验证算法，并在输出文件和/或仪表板中捕获结果。

此外，代码开发还会对企业内部或云上的服务器进行部署和配置，这时又会用到常见的 SSH 协议。针对这种情况的脆弱性发现的具体步骤如下：

针对 SSH 协议流量的检测：

- **测试数据：** AZSecure Data 和亚利桑那大学人工智能实验室提供的 AZSecure 数据。
- 步骤
  1. 配置发现工具以扫描第 4 层（传输）流量。此过程取决于个别发现工具的部署方法。
  2. 根据目标网络的需要修改测试数据包捕获 IP 地址。
  3. 使用 tcpreplay 等实用程序将 SSH 2.0 测试数据重放至已部署发现工具的网段。

预期结果：发现工具检测是否存在易受攻击的密钥交换算法，安全外壳 (SSH) 的密钥交换 (KEX) 方法更新和建议，并在输出文件和/或仪表板中捕获结果。

4.3 风险评估方法

在应用上述脆弱密码发现框架、部署相关的密码态势感知工具，并从目标系统中检测出具体的量子脆弱点后，需要将这些量子脆弱点以及相关的特征数据输入特定的风险评估模型中，并最终根据风险优先级给出一份量子迁移名单。

目前有两个广为人知的 PQC 风险评估框架可供使用：莫斯卡量子风险评估框架（QRA）和密码敏捷性风险评估框架（CARAF）。莫斯卡 QRA 采用基于时间的风险定义方法，取决于何时开始向量子安全状态迁移，并考虑“现在收获、稍后解密”攻击。CARAF 基

于莫斯卡 QRA，但侧重于“密码灵活性”，即能够快速将易受攻击的原始工件、算法、和协议替换为更安全的协议，并寻求为特定资产定义组织政策。以下是对这两个框架的详细介绍。

4.3.1 莫斯卡定理及密码敏捷风险评估框架

（1）莫斯卡定理

米歇尔·莫斯卡是量子信息处理和量子就绪理论和实践的主要贡献者，制定了一系列评估风险并采取主动措施以保障后量子安全的战略。风险评估的重点是在量子计算机可用的很长一段时间之前内迁移到量子安全状态，以避免“先存储后解密”类型的攻击。莫斯卡定理的基本内容如下：

如果在大规模量子计算机 (z) 建成之前，基础设施还没有被改造为量子安全型，并且信息安全的必要持续时间已经过去 (x+y)，那么加密的信息将不安全，容易受到敌手攻击。其中 x 是安全保质期，代表着加密结果需要在多长时间内保持安全。y 是迁移时间，代表着使 IT 基础设施变得量子安全需要花费的时间。z 是崩溃时间，指建成大规模量子计算机需要的时间。

基于莫斯卡定理的莫斯卡 QRA 所采用的方法学可以概括为 NIST 网络安全框架中[44] 用于进行风险评估的六个阶段，需要在完成常规风险评估之后进行。这些阶段具体如下：

莫斯卡量子风险评估框架

- 第一阶段：识别和记录具有价值的信息资产，明确其受加密保护的程度及所使用的加密技术类型。
- 第二阶段：研究新兴量子计算技术和量子安全加密技术的发展状况。
- 第三阶段：识别威胁行为者，估算其获取量子技术的时间。建议该值至少为两年。结合第 2 阶段的结果，可以确定估计的量子风险时间轴 “z”。
- 第四阶段：确定资产的使用寿命 “x”，并评估如果资产在第三阶段确定的时间框架 “z” 内变得脆弱，可能对业务造成的影响，以确定将组织的技术基础设施转变为量子安全状态 “y” 所需的时间。
- 第五阶段：通过计算"x + y > z " 来确定系统的量子风险，即业务资产是否会在组织采取行动保护它们之前变得脆弱。
- 第六阶段：确定活动的安全风险等级，以证系统能够对风险保持警觉，同时将系统的整体技术架构提升到能保障量子安全的等级。

(2) 密码敏捷风险评估框架（CARAF）

密码敏捷性[45] 是指实体以快速、低成本、无风险或可接受风险的方式用新的替代方案替换现有加密原语、算法或协议的能力。从一种加密解决方案过渡到另一种解决方案可能需要很长时间，并使组织面临不必要的安全风险。因此，CARAF 框架[46] 被创建来分析和评估由于缺乏加密灵活性而产生的风险。组织可利用该框架确定与其风险承受能力相称的适当缓解策略。该框架具体如下：

密码敏捷风险评估框架

- 阶段 1：识别威胁。识别会影响受加密敏捷性风险影响的资产的潜在威胁载体。
- 阶段 2：资产清单。编制受影响资产的清单，包括资产的性质和预期的安全风险暴露情况。
- 阶段 3：风险估计。根据暴露情况，需要对库存进行优先级风险缓解排序。与众所周知的“风险 = 影响 x 概率”的评估方法不同。CARAF 推荐的公式是“风险 = 时间表 x 成本”。时间表由莫斯卡定理的一二阶段得出。成本变量定义为在所需时间表内将资产更新为安全状态的成本。
- 阶段 4：通过风险缓解保护资产。当资产价值较高时，通过资源投入确保资产安全。当风险的预期价值较低时，接受风险并维持现状。当资产的的安全成本很高时，分阶段淘汰受影响的资产。
- 阶段 5：组织路线图。企业必须制定连贯的加密政策，支持和指导不同团队就其加密选择做出决策。

4.3.2 金融科技领域

金融服务信息共享和分析中心 (FS-ISAC) 是一个致力于降低全球金融体系网络风险的行业联盟。该组织为金融机构及其客户提供服务，利用其情报平台、弹性资源和值得信赖的点对点专家网络来预测、减轻和响应网络威胁。

FS-ISAC 最新成立的的后量子密码学工作组发布了《风险模型技术手册》[47]，在其中给出了一种风险管理策略，除了强调莫斯卡定理带来的紧迫性和 CARAF 框架指出的灵活性外，他们还建议

金融组织开发一个密码敏捷性指数（CAI）。CAI 被描述为一种整体观，反映了围绕优先级、控制、业务能力、供应商、缓解和实施计划的若干具体点。CAI 方法论的一个显着不同在于考虑密码资产是由组织开发的还是来自第三方供应商。换句话说，组织应在整体风险计算中纳入继续使用第三方软件的风险。CAI 还建议在迁移风险计算过程中仔细考虑特定于行业的服务，比如 SWIFT 银行系统。FS-ISAC PQC 小组还创建了一份潜在供应商问题清单，以帮助机构了解供应商的 PQC 状况。

FS-ISAC PQC 的供应商问题清单

- 公司的首席信息官是否参与了后量子密码学相关标准的制定？
- 公司是否清点了量子计算到来后必须保护的数据集？
- 公司是否意识到数据可能会在今天被采集，并在加密相关的量子计算机可用时被解密？
- 公司是否清点了所有使用加密技术的系统，以促进未来平稳过渡？
- 公司是否确定了需要更新以反映后量子时代要求的数据安全标准？
- 公司是否正在确定公钥密码学被用于何处，为何目的，以及标记这些系统为量子脆弱的？
- 公司是否有办法考虑资产价值、密钥存储、通信、与其他实体的联系、关键基础设施或数据受保护的时间长短等因素，确定加密过渡系统的优先级？
- 公司是否制定了用于在发布新的后量子密码学标准后进行系统过渡的路线图？

4.3.3 通信网络领域

英国的一份名为《通用 CPS 设置上的量子计算威胁建模》的报告[48] 详细阐述了一种针对通信网络领域的风险评估方法论。该方法论基于攻击模拟和威胁分析 (PASTA) 流程，旨在将业务目标、业务影响以及技术要求相结合，为威胁建模提供混合风险分析和攻击者视角，并生成基于资产的输出。

PASTA 七个阶段:

- 阶段一：确定业务目标、安全与合规性要求，分析业务影响。
- 阶段二：捕获技术环境的边界、基础设施、应用和软件依赖。
- 阶段三：识别用例，定义应用程序、入口和信任级别，确定资产、服务、角色和数据源，确定数据流图和信任边界。
- 阶段四：分析概率攻击场景、安全事件回归，并关联威胁情报。
- 阶段五：查询并跟踪现有漏洞报告，使用威胁树进行威胁映射，使用用例和滥用案例设计流程分析。
- 阶段六：分析攻击面，开发攻击树，管理攻击库，使用攻击树和 STRIDE 进行漏洞攻击和利用分析。
- 阶段七：限定和量化业务影响，识别对策，确定风险缓解策略。

4.3.4 电子政务领域

在电子政务领域，美国国土安全部提出了评估迁移路线图时需要考虑的因素，其关于过渡到后量子算法的路线图[49] 建议组织在评估系统时考虑因素。这些因素主要针对美国联邦政府的系统所有者，但也适用于私营部门，特别是支持关键基础设施运行的组织。

美国国土安全部给出的考虑因素：

- 因素 1：系统是否基于组织要求的高价值资产。
- 因素 2：系统正在保护的内容（例如密钥存储、密码、根密钥、签名密钥、个人可识别信息、敏感个人可识别信息）。
- 因素 3：系统的通信对象。
- 因素 4：系统是否基于组织要求的高价值资产。
- 因素 5：系统在多大程度上与联邦实体分享信息。
- 因素 6：系统在多大程度上与组织之外的其他实体分享信息。
- 因素 7：系统是否支持关键基础设施部门。
- 因素 8：数据需要得到多长时间的保护。

第五章 现有后量子密码算法迁移及评测

5.1 后量子密码算法及应用的实现

目前，美国 NIST 主导的后量子密码标准化计划是全球范围内最为知名和广泛参与的标准化项目。于 2022 年 7 月，NIST 发布了第三轮评估报告 NIST IR 8413，正式宣布了首批后量子标准算法，包括基于结构化格的公钥加密/密钥封装算法 Crystals-Kyber（FIPS.203）、基于结构化格的公钥签名算法 Crystals-Dilithium（FIPS.204）、以及 Falcon 与基于哈希的公钥签名算法 SPHINCS+（FIPS.205）。

欧盟国家并未单独制定后量子密码标准化计划，而是与美国 NIST 的标准化项目保持密切合作。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，也一致推荐采用 NIST 项目候选算法。尽管德国 BSI 认为基于无结构格的加密 FrodoKEM 和基于编码的加密 Classic McEliece 的性能稍逊于 Kyber，但其安全性更为可靠，特别适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）中予以推荐。然而，由于目前 FrodoKEM 在 NIST 标准化项目中未获通过，Classic McEliece 也未能成为首批标准，德国 BSI 正在积极促使这两个算法在 ISO 标准化（PWI 19541）方面取得进展，以加强后量子密码技术的全球标准化与应用。

表 9 国外选定的后量子密码算法

	后量子密码算法	类别	算法类型
美国	Crystals-Kyber	基于格	密钥封装
	Crystals-Dilithium	基于格	数字签名
	Falcon	基于格	数字签名
	SPHINCS+	基于哈希	数字签名
德国	FrodoKEM	基于格	密钥封装
	Classic McEliece	基于编码	密钥封装

亚马逊、AWS、Crypto4a、CryptoNext、Entrust、IBM、ISC、微软、三星、泰雷兹、Utimaco、wolfSSL 等公司积极跟进后量子算法的演进并贡献了表 10 中的算法实现。在诸多安全协议和机制中，SSH、TLS 和 PKI 是被广泛应用的技术。在下一节分别对这些密码协议进行测试，包括互操作性和性能的测试。

表 10 国外公司及机构的后量子产品

公司或机构	产品名称	产品简介
CryptoNext	量子安全库 C-QSL	提供全面的 PQC 算法封装以及常见操作平台的优化实现
	量子安全加密服务 C-QSC	启用 PQC 的混合协议和加密对象实现，涉及通信协议，证书等
	量子安全工具 C-QST 及件 C-QSA	加密敏捷、支持混合方案、量子安全的集成工具和应用插件

公司或机构	产品名称	产品简介
Microsoft	开放量子安全(OQS)项目	开源项目，包括 liboqs 开源 C 库以及在协议和应用程序的集成
AWS	aws-lc 软件库	实现用于 AWS 用例的 PQC 算法软件库
	s2n-quic 软件库	实现 QUIC 协议的软件库，用于 AWS 的使用场景
	AWS SSH 实现	实现 SSH 协议的软件库，用于 AWS 的使用场景
	s2n-tls 软件库	实现 TLS 协议的软件库，用于 AWS 的使用场景
Crypto4a	QxHSMTM 密码模块	基于 Crypto4A 的 FIPS 3+QASM 模块构建的 HSM
	QxEDGETM 密码模块	将 FIPS 3+QASM 和通用计算处理引擎结合的 HSP
三星	s-qpc-tls 软件库	实现 TLS1.3 和支持 PQC 算法进行混合密钥交换的 Java 软件库
worfSSL	wolfSSL 软件库	实现 TLS 和 DTLS1.3, 支持 NIST 标准化 PQC 算法的软件库
	wolfSSH 软件库	实现支持 ecdh-nistp256-kyber-512r3-sha256-d00 的 SSHv2
	wolfMQTT 软件库	实现多个版本 MQTT 协议的软件库，在 wolfSSL 上运行
	wolfSSL-Nginx 发行版	使用 wolfSSL 加密库编译的高性能、高并发的 NGINX 版本
	wolfSSL-cURL 发行版	使用 wolfSSL 加密库编译 cURL 版本

公司或机构	产品名称	产品简介
Thales	Thales Luna A/S790 HSM	提供一个可定制的功能模块，支持多种 PQC 算法
	Thales TCT Luna T5000 HSM	专用的防篡改加密处理器，安全的管理和存储加密密钥
	Thales CN 系列网络加密器	经过 FIPS 验证的网络加密解决方案，用于加密关键网络通信
	CipherTrust Manager & Connectors	细粒度访问控制，可配置安全策略的企业密钥管理方案
Entrust	PQ 启用的 nShield HSM	启用 PQ 支持在安全的 HSM 中测试和实施 PQC
	PKIaaS PQ Beta，量子安全 Java 工具包	支持复合和纯量子证书 CA，可用于测试多证书和复合证书
PQShield	PQCryptoLib 通用软件库	使用多种算法提供后量子安全，支持混合密钥派生
	PQSDK 加密 SDK	后量子和经典密码原语易于使用的软件实现
ISC	ISC CDKpqc 可链接库	提供经典和 NIST 选定的量子安全算法的可链接库
	ISC CertAgent	支持 PQC 的 X.509 证书颁发机构
	ISC SecretAgent 应用程序	支持 PQC 的文件加密和数字签名的应用程序
Kudelski IoT	Kudelski IoT 实验室服务	算法安全性的评估，执行针对量子安全密码的攻击和分析
	Kudelski IoT Key-Stream	物联网设备安全生命周期和密钥管理平台

公司或机构	产品名称	产品简介
	Kudelski IoT KSE	提供全方位安全和密码服务的硬件安全隔离环境组合产品
Keyfactor	Bouncy Castle 密码库	支持经典和量子安全算法，各种围绕 X.509 证书管理的协议
Utimaco	u.trust Anchor	支持容器化环境，提供高安全性，灵活性和完整控制

5.2 后量子安全外壳协议（PQ-SSH）的评测

SSH 是一种被广泛使用的管理、配置和安全文件传输协议，用于在计算机系统之间建立安全连接。在 SSH 的安全性测试中，特别关注对抗立即收集、以后解密的攻击。在一系列测试中，涉及 PQC 密钥交换方法，以便全面了解它们的性能差异和可能存在的问题。值得注意的是，保护 SSH 认证相对而言并不是当务之急，因为对 SSH 的攻击通常需要利用量子计算机在会话建立期间执行，这提供了更多的时间来评估和应对潜在的安全威胁。

SSH 的测试使用组件包括：OQS-OpenSSH v8，wolfSSH，以及 AWS-SSH。

SSH 的测试算法参数包括：Kyber-512、kyber-768、kyber-1024；P256+Kyber-512、x25519+Kyber-512、P384+kyber-768、P521+Kyber-1024。

在每次测试中，使用不同的 SSH 测试组件构建客户端和服务器，在每个算法上测试成功的 SSH 连接。表 11 是互操作性测试的结果[3]（仅展示测试成功的组件组合）。表 11 显示，所有支持的算法实现在组件之间实现的互操作性。

表 11 SSH 互操作性测试结果[3]

算法参数	测试客户端	测试服务器	互操作结果
Kyber-512/768/1024	OQS-OpenSSH	OQS-OpenSSH	成功
P256+Kyber-512	任意	任意	成功
x25519+Kyber-512	AWS SSH	AWS SSH	成功
P384+Kyber-768	OQS-OpenSSH/AWS SSH	OQS-OpenSSH/AWS SSH	成功
P521+Kyber-1024	OQS-OpenSSH/AWS SSH	OQS-OpenSSH/AWS SSH	成功

从表 11 中可以看出，主流的 SSH 组件对于纯 PQC 算法的兼容性并不完善，仅 OQS-OpenSSH 完整支持 Kyber 算法，但是由于各组件对于 P256 算法的完全支持，所以 P256+Kyber-512 的混合方案在任意的测试组件之间都可以实现互操作，这也说明了使用混合方案进行 SSH 的后量子迁移是可行的方案，另外 AWS SSH 组件相比其他组件对于混合方案的支持性更好。

与 TLS 1.3 设计为在一次数据往返后启动加密不同，SSH 作为

协议在建立隧道并交换数据之前需要进行多次往返的消息交换。这意味着大多数 PQC 算法对整体握手时间的影响不大，因为大部分时间都花在往返消息上。即使认证发送更多数据，也不会对 SSH 产生显著影响，特别是因为大多数 SSH 连接传输的数据量相当可观。Sikeridis 等人在 2020 年评估了 PQC 算法对 SSH 的影响[50]。他们的研究证实了 Kyber-512、Kyber-768 和 Dilithium-4 对 SSH 握手影响都在个位数百分比内，这也证实了在 SSH 使用 PQC 算法替换传统密码算法并不会对 SSH 产生显著影响。

5.3 后量子传输层安全协议（PQ-TLS）的评测

确保传输层安全（TLS）协议支持后量子安全至关重要，因为它是目前最广泛部署的在线安全协议之一。随着其广泛使用，TLS 成为了攻击者的主要目标，因此保障其安全性尤为重要。在 PQC 原型化工作甚至 NIST PQC 标准化工作之前，已有许多学术研究和大规模的工业实验对 TLS 进行了后量子保护的探索和研究。自那时以来，许多开源和商业的 TLS 1.3 实现已经添加了对 PQC 和混合密码套件的支持，甚至在最终的 PQC FIPS 标准以及它们被包含在 TLS 规范中之前就已经实现。大多数实现（包括所有 NCCoE 协作参与者的实现）都遵循了 IETF 草案 draft-ietf-tls-hybrid-design-05 规范，用于实现混合 TLS 1.3 密钥交换。测试的主要目标是验证符合规范的实现之间的互操作性，并测量各种算法之间的性能，以便了解它们对性能的影响。

需要指出的是，目前主要关注的是 PQC 和混合密钥交换，而不是认证部分（除了商业国家安全算法套件 CNSA 2.0 配置文件，该配置文件测试了 Dilithium-5 认证）。这是因为“现在存储、以后解密”的问题主要影响加密部分，而不是认证部分（取决于会话建立的密钥交换部分）。此外，目前尚未就如何执行混合认证或是否有必要进行混合认证达成共识。

TLS 测试中使用以下协作组件的客户端和服务器功能：Open Quantum Safe（OQS）OpenSSL Provider，wolfSSL，AWS s2n-tls，三星 SDS PQC-TLS（s-pqc-tls，OQS NGINX。

互操作测试总包括对 TLS 进行了两种算法配置的测试：第一种仅使用协议的密钥交换部分（PQC 和混合）Profile 1，而另一种遵循了 CNSA Suite 2.0 的规范 Profile 2。测试配置中使用由 NIST 选择进行标准化的第一个密钥交换机制的 Kyber 方案，其要么单独使用，要么与相应强度的 NIST 椭圆曲线相结合。

具体测试的密钥交换算法组合包括：Kyber-512、kyber-768、kyber-1024；P256+Kyber-512、P384+kyber-768、P521+Kyber-1024。

在每次测试中，使用不同的 TLS 测试组件构建客户端和服务器，在每种密钥交换算法上都测试了 TLS 1.3 连接。表 12 包含了互操作性测试的结果[3]（仅展示测试成功的组件组合），表中展示了所有支持的算法实现在组件之间的互操作性。

在表 12 所示的测试结果中，除了涉及 AWS s2n-tls 组件的测试

组合不支持 Kyber 方案，其余测试组件间的组合均支持通过 Kyber 方案实现互操作，混合方案的测试结果基本和 Kyber 方案的测试结果一致，除了由于 AWS s2n-tls 方案对于 P256 算法的支持使得在 P256+Kyber-512 的混合方案测试中涉及 AWS s2n-tls 组件的测试组合同样可以实现互操作性。

第二种符合 CNSA Suite 2.0 规范的配置测试中，使用 Kyber-1024 和 Dilithium，并排除了混合方案，表 13 中包含了互操作性测试结果[3]（仅显示测试成功的组件组合）。

表 12 Profile 1 配置下 TLS 互操作性测试结果[3]

算法参数	测试客户端	测试服务器	互操作结果
Kyber-512/768/1024	OQS-OpenSSL/ wolfSSL/ SDS PQC-TLS	OQS-OpenSSL/ wolfSSL/ PQC-TLS/ OQS-NGINX	成功
P256+Kyber-512	OQS-OpenSSL	任意	成功
	wolfSSL/ SDS PQC-TLS	OQS-OpenSSL/ wolfSSL/ SDS PQC-TLS/ OQS-NGINX	
	AWS s2n-tls	wolfSSL/ AWS s2n-tls/ SDS PQC-TLS/ OQS-NGINX	

P384+Kyber-768	OQS-OpenSSL/ wolfSSL/ PQC-TLS	OQS-OpenSSL/ wolfSSL/ SDS PQC-TLS/ OQS-NGINX	成功
P521+Kyber-1024	OQS-OpenSSL/ wolfSSL/ PQC-TLS	OQS-OpenSSL/ wolfSSL/ SDS PQC-TLS/ OQS-NGINX	成功

表 13 Profile 2 配置下 TLS 互操作性测试结果（CNSA Suite 2.0 规范）[3]

算法参数	测试客户端	测试服务器	互操作结果
Kyber-1024/ Dilithium5	OQS-OpenSSL/ wolfSSL	OQS-OpenSSL/ wolfSSL/ OQS-NGINX	成功

OQS-OpenSSL 性能测试: OQS OpenSSL 上对 Profile 1 和 Profile 2 进行性能测试[3]。(Intel Xeon Platinum 8259CL CPU @ 2.50 GHz，2 个 CPU 和 8 GB 内存)。测试结果见图7。

表中数据可以表示测量 TLS 连接是服务器的负载。结果显示，PQC 混合方案可能会对负载较重的服务器的最大连接吞吐量产生显著影响。我们可以看到，Kyber 在所有安全级别下的性能都很高。与具有 P384 和 P521 的 ECDH 相比，Kyber-768 和 Kyber-1024 的性能要高得多。与高度优化的 P256 相比，Kyber-512 的效率略低，但性能类似。在组合的 PQC 混合密钥交换中，Kyber-512 和

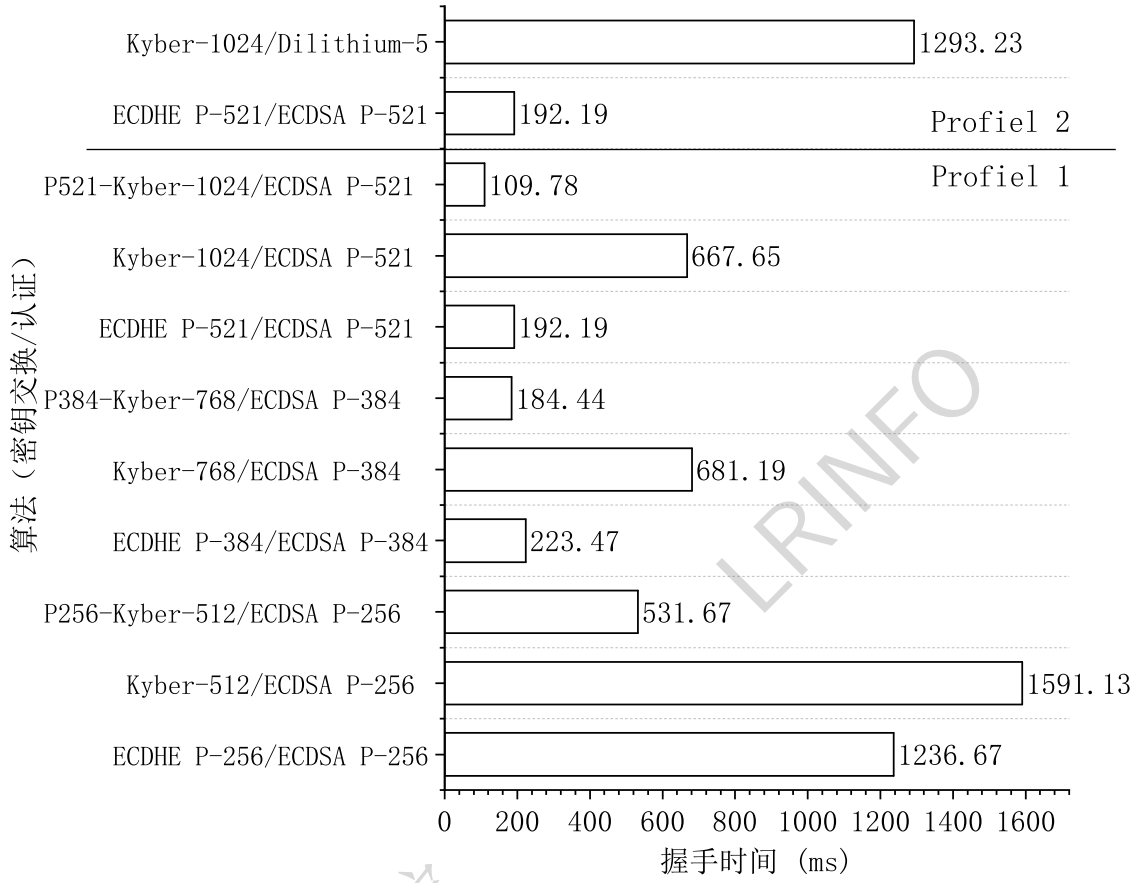

图 7 Profile 1 和 Profile 2 下 TLS1.3 中 PQC 密钥交换和认证的性能测试结果[3]

ECDH P256 结合使用时，握手吞吐量减半，因为使用了性能类似的两种算法。当与未优化的 P384 和 P521 结合使用时，Kyber-768 和 Kyber-1024 对效率的影响很小。

在 Profile 1 配置下，测试了三星 SDS PQC-TLS 在 TLS1.3 中进行 PQC 密钥交换和身份验证的性能测试[3] (Intel Xeon Gold 6126 CPU @ 2.60 GHz (2 Core) 32 GBRAM)，结果见图 8。

在图 8 上可以观察到与 OQS OpenSSL 类似的规律。Kyber 效率

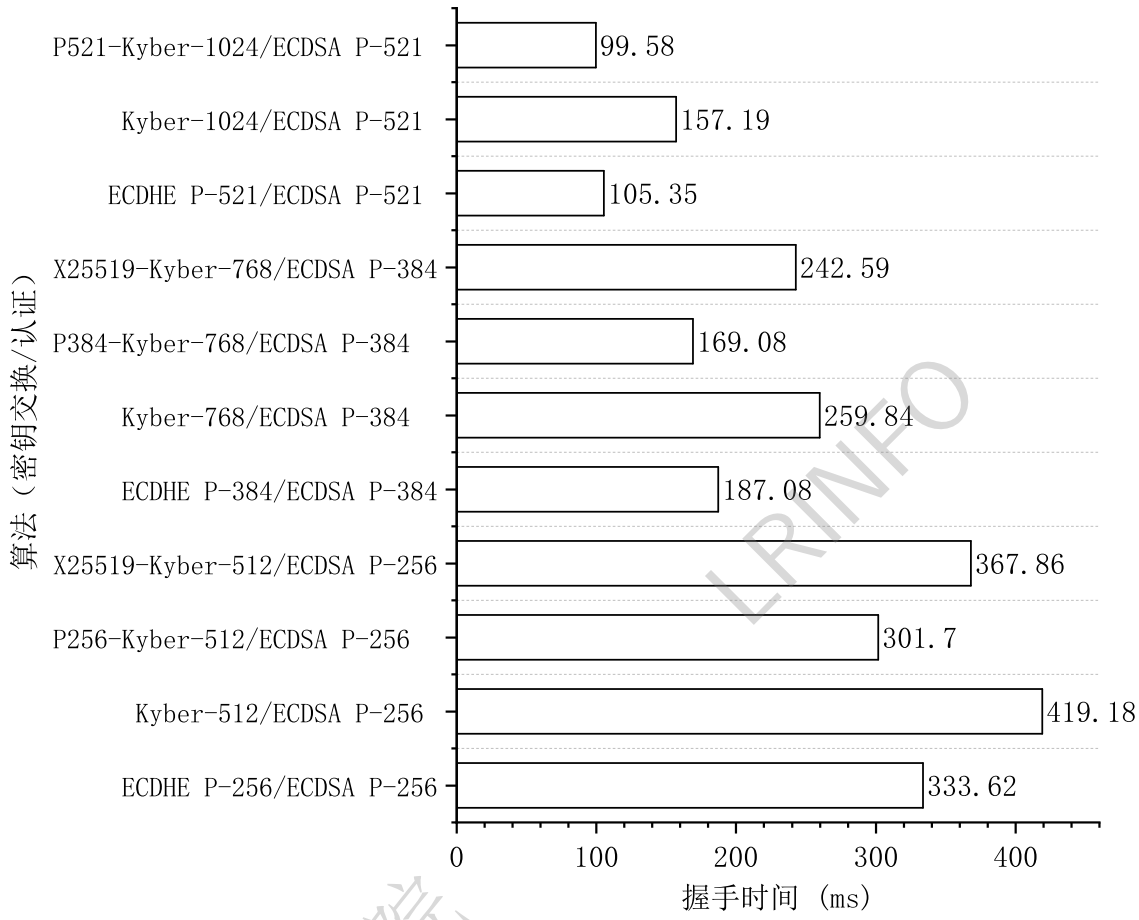

图 8 Profile 1 下 s-pqc-tls 中 TLS 1.3 进行 PQC 密钥交换和认证的性能测试结果[3]

高，特别是对于更高安全性的曲线 P384 和 P521。将 ECDH 与 Kyber 结合会降低吞吐量，但并不会造成明显的性能损失。将 X25519 与 Kyber 结合比将 ECDH 与 Kyber 结合效率略有提升。需要注意的是测试环境的改变可能会影响实际使用中的性能。

在 s2n-tls 客户端和 QOS OpenSSL 服务器 test.openquantumsafe.org 之间测试了 TLS1.3 中使用 P256 和 Kyber-512 的 PQC 混合密钥交换和 X25519 密钥交换之间的性能测试[3]，测试结果见图 9。

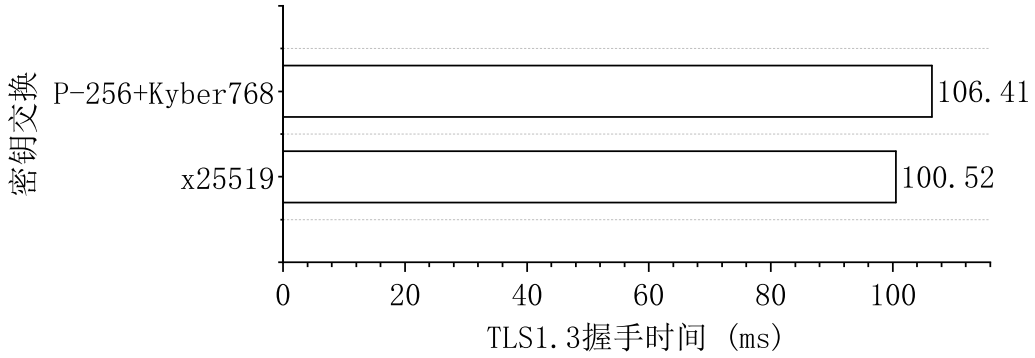

图 9 TLS1.3 中 PQC 混合密钥交换性能[3]

图 9中可以看到，使用 ECDH P256 和 Kyber-768 的 PQC 混合密钥交换方案比传统的 X25519 稍慢几毫秒。由于使用 Kyber 而导致的减速在标准差范围内，所以即使混合方案稍慢于传统方案，混合方案也是一种高效的替代算法，对于一般的互联网连接，Kyber 导致的时间延迟是微不足道的。这意味着对于普通的网络或机器之间的通信来说，PQC 连接的性能是可以满足使用需求的。

通过本地连接的 s2n-tls 客户端和服务器测试更高安全级别的 PQC 混合密钥交换方案，并与传统的 P256 和 P384 密钥交换方案进行对比[3]，如图 10 所示，每个方案的平均握手时间中包括了模拟实现的 133ms 的往返延迟。

结果显示，不同密钥交换方案的握手时间基本上没有太大差距。即使是使用 Kyber-1024 的 PQC 混合交换，也只比非常高效的 P256 慢了几毫秒。这样的性能差异不会对用户体验造成明显影响。但是在考虑额外损耗的条件下可能会受到更多影响，因为

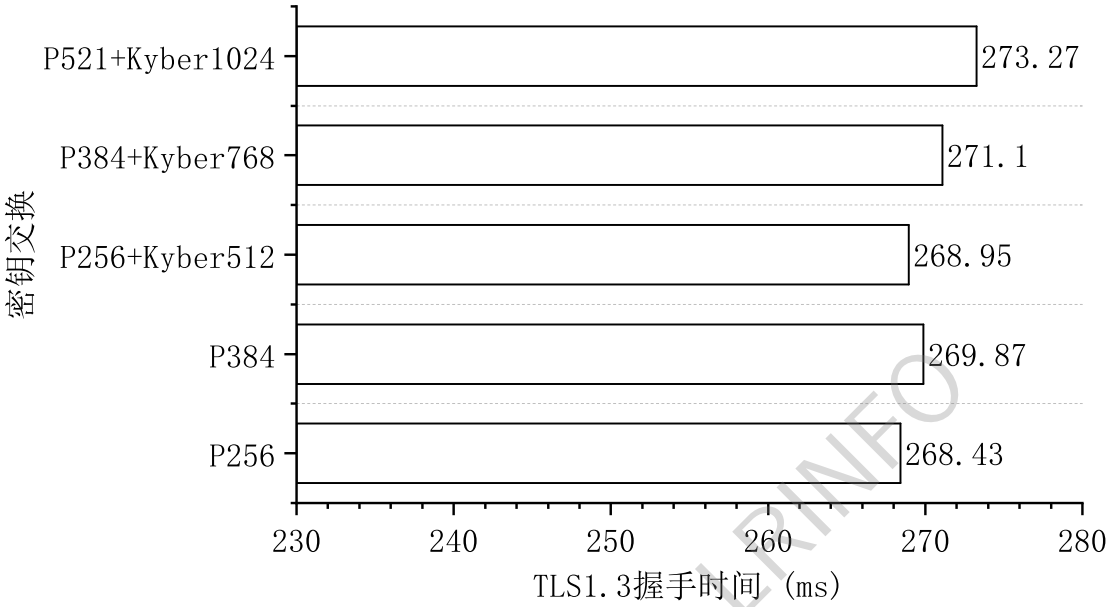

图 10 模拟延迟情况下，更高级别 PQC 混合密钥交换方案性能[3]

Kyber-1024 或 Kyber-768 将包含更多的 TCP 分段，这意味着丢包对性能的影响将更为显著。

为了测试更高丢包率对 PQC 混合密钥交换方案的影响，通过将客户端和服务器之间的丢包概率调整到 3%，重复上面的实验[3]，测试结果如图 11 所示。

3% 的丢包概率造成的影响相当于一次额外的往返延迟。并且 Kyber768 和 Kyber1024 中更长的密钥和更大规模的密文导致了更高的丢包率和平均握手时间。总体而言，测试中所有密钥交换方案中的连接都明显受到更高的丢包概率的影响。实验结果表明 PQC 混合密钥交换方案相较于传统密钥交换方案在更高丢包率的条件下并没有受到更显著的影响。在更高的网络丢包率的情况下，各方

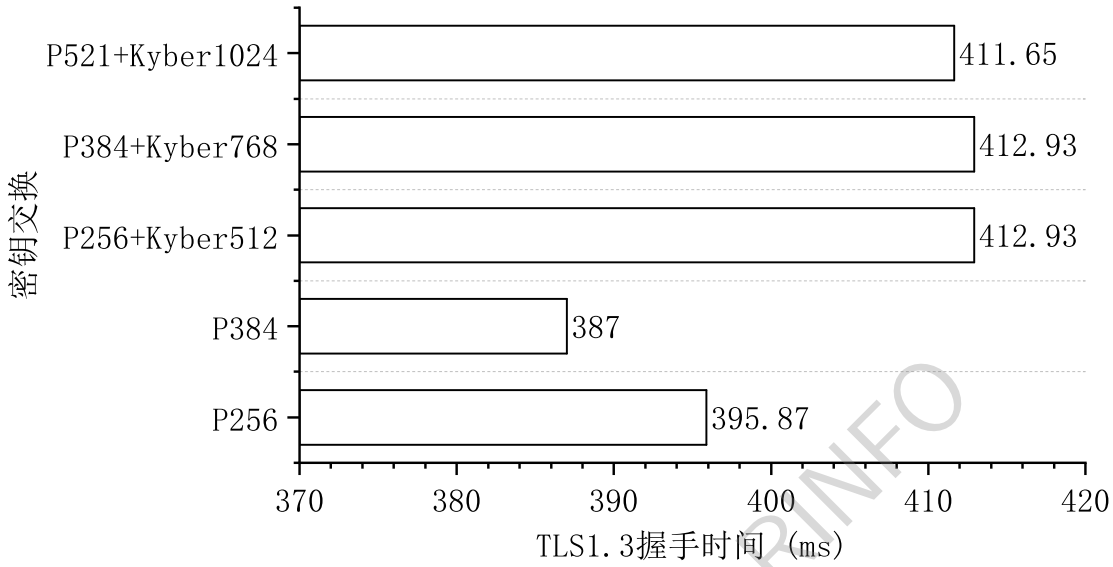

图 11 3% 丢包率下，更高级别 PQC 混合密钥交换方案性能[3]

案的密钥交换性能将更“随机化”。

综上的性能测试表明，Kyber 非常高效，当单独使用 Kyber 比单独使用 ECDH，可以略微加快握手速度。当将 Kyber 与 ECDH 结合使用时，会略有减慢，但对于大多数网络连接来说，这种减慢可以忽略不记。由于 Kyber-768 或 Kyber-1024 可能携带两个 TCP 数据包，更高的丢包率将会对 Kyber 造成更大的影响。

一种实现后量子 SSL/TLS 的方法是通过替换通信双方的双向认证算法，密钥协商算法以及会话密钥加密算法，或者采用 QKD 技术或 QRNG 技术来增强量子密钥的安全性。在工程实践中，可以采用这些技术的组合来实现后量子 SSL/TLS。一些领先企业已经开始将相关产品作为可选项提供给用户。例如，亚马逊已将混合后量子 TLS 与其 Amazon KMS 结合使用，以支持对 TLS 网络加密

协议的混合后量子密钥交换选项。通过这种 TLS 选项，用户连接到 Amazon KMS API 终端节点时可以使用混合后量子密钥交换功能。谷歌在其 Chrome 浏览器中也已于 2023 年 8 月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提供了与传统 SSH 加密相当的安全性，但在延迟和吞吐量性能方面可能会有一定影响。2024 年 4 月默认启用，由于兼容性问题导致部分用户无法正常访问网站和连接服务器，目前正在收集错误报告中。综上所述，后量子密码应用及测试在保障网络通信和数据安全方面具有重要意义。

5.4 后量子公钥基础设施（PQ-PKI）的评测

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，难以抵后量子计算攻击。X.509 证书在向后量子密码 (PQC) 迁移过程中将是重要的工具，因为它们是在终端之间传输和交换公钥的主要方式。X.509 证书可用于携带签名或加密密钥，因此在 TLS/SSL、QUIC、S/MIME 和 IPsec 等协议中被广泛使用。X.509 证书格式有：

- 纯 PQC 证书 (PURE PQC)：这个 X.509 证书是一个纯 PQC 证书，意味着它只包含 PQC 数据 (PQC 密钥和 PQC 签名)。使用传统的 X.509 结构，并用量子安全的对象替换了传统对象。

- 混合串联证书（HYBRID CONCATENATED）：这个 X.509 证书是一个混合证书。它使用特定的 OID 来表示传统 + 后量子算法组合，并且密钥和签名遵循通常的 ASN.1 语法。

- 混合边界证书（HYBRID BOUND）：这个 X.509 证书是一个混合证书。它使用两个证书，一个是传统的，一个是后量子的。传统证书按照通常的方式构建，而后量子证书则按照 PURE PQC 模型构建。此外，后量子证书包含一个扩展，将其链接到传统证书。传统证书可能包含类似的扩展，将其链接到后量子证书，这样每个证书都有一个经过验证的指向另一个证书的指针。

- 混合复合证书（HYBRID COMPOSITE）：这个 X.509 证书是一个混合证书。这个版本是之前的 HYBRID CONCATENATED 格式的一个改进，它使用 ASN.1 编码来分隔传统和后量子对象。

- 使用拓展的混合证书（HYBRID USING EXTENSIONS (Catalyst)）：这个 X.509 证书是一个混合证书。这种格式将后量子对象存储在 X.509 扩展中。除了这些扩展，证书看起来与传统的 X.509 证书完全相同，因此，假设它将未知的非关键扩展视为不透明的数据，那么未经修改的工具便能够解析和验证它。原理上来说，这种证书格式是向后兼容的。

- 混合增量证书（HYBRID DELTA EXTENSIONS (Chameleon)）：这个 X.509 证书是一个混合证书。该格式将两个证书之间的差异编码为单个扩展。一个证书是“基础”或外部证书，第二个

是“增量”或内部证书。扩展中仅包含基础和增量证书之间的差异。除了扩展之外，该证书看起来完全像传统的 X.509 证书，因此，只要将未知的非关键扩展项视为不透明数据，未经修改的证书解析工具就能够正确地解析和验证这种混合证书。从原理上来说，这种证书格式是向后兼容的。基础证书可以通过增量证书重建为一个完全可验证的次要证书。

PKI 的互操作性测试旨在验证：1) X.509 证书中包含的所有公钥都可以被其他供应商应用程序提取和使用。2) X.509 证书中包含的所有签名都可以由另一个供应商应用程序进行验证。

应用程序 A 和 B 之间最基本的互操作性测试包括以下步骤：

- SIG 签名算法：1) 应用程序 A 生成一个根 CA 证书（自签名）。2) 应用程序 B 验证根 CA 证书。通过该测试检查 PQC 公钥的可用性和 PQC 签名的正确性。
- KEM 公钥算法：1) 应用程序 A 生成一个持有 KEM 密钥的终端实体证书。该证书由在签名算法测试用例中生成的根 CA 证书的私钥进行签名。2) 应用程序 B 验证持有 KEM 密钥的终端实体证书的有效性。

针对 X.509 不同证书格式的互操作性测试算法配置如下文所示：

纯 PQC 签名测试配置文件测试传输 PQC 签名密钥的 PURE

PQ X.509 证书。该测试配置文件见表14中列出的算法配置:

表 14 纯 PQC SIG 测试配置文件中包含的算法配置

X.509 公钥算法	X.509 签名算法
Dilithium-2/3/5	Dilithium-2/3/5
Falcon-512/1024	Falcon-512/1024
SPHINCS+-SHAKE-128f/192f/256f	SPHINCS+-SHAKE-128f/192f/256f
SPHINCS+-SHA2-128f/192f/256f	SPHINCS+-SHA2-128f/192f/256f

纯 PQC 密钥封装测试配置文件测试传输 PQC KEM 密钥的 PURE PQ X.509 证书。该测试配置文件见表15中列出的算法配置:

表 15 纯 PQC KEM 测试配置文件中包含的算法配置

X.509 公钥算法	X.509 签名算法
Kyber-512/768/1024	Dilithium-2/3/5

混合串联证书、混合边界证书、混合复合证书、使用拓展的混合证书（CATALYST)、混合增量证书（CHAMELEON）使用相同的测试配置文件来测试传输 PQC SIG 密钥的各自类型的 X.509 证书。测试配置文件见表16中列出的算法配置:

表 16 混合证书测试配置文件中包含的算法配置

X.509 公钥算法	X.509 签名算法
RSA(3072)+Dilithium-2	RSA_PKCSv1.5_SHA256 (3072)+Dilithium-2

ECDSA(P-256)+Dilithium-2	ECDSA_SHA256(P-256)+Dilithium-2
ECDSA(P-521)+Dilithium-5	ECDSA_SHA512(P-521)+Dilithium-5

以上针对每种证书类型的互操作性测试都在 IETF PQC X.509 Hackathon 中，具体的互操作性测试结果见：IETF Hackathon Results。

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。

第六章 先行试点：后量子区块链

密码技术是区块链系统运行与安全的基石，因而，量子计算对传统公钥密码的安全威胁，也自然而然地传递到了区块链系统。特别是，目前仍然被大多数区块链系统广泛使用的基于椭圆曲线的数字签名算法 ECDSA 和 ED25519 在大规模量子计算机面前将毫无安全性可言。或许行业级的后量子密码迁移不可能马上出现，但一些新兴的技术领域因为历史负担少而可以先行试点。特别是，区块链技术又是密码密集型的。因此，基于传统密码技术的区块链（以下简称传统区块链）向基于后量子密码技术的区块链（以下简称后量子区块链）的迁移已经被提上议事日程。

6.1 国外后量子区块链研究现状

下面我们将按照时间线，简要介绍目前能够公开查询到的具有代表性的后量子区块链系统或平台[10]。

(1) **IOTA**。早在 2014 年，德国柏林的一个团队就发布了 IOTA，并为此专门成立一个非盈利的组织 IOTA Foundation 来运维 IOTA，目前已经演进到 2.0 版（https://wiki.iota.org/）。由于 IOTA 使用了 Winternitz 一次性签名算法（WOTS），该签名算法是基于密码学哈希函数构造的，具有抵抗量子攻击的特点，因此 IOTA 也成为最早的后量子区块链系统。IOTA 是一种分布式账本技术（DLT），使个人能够控制自己的私人数据，运行防篡改程序，并无需中介机构即

[10]我们不得不放弃按国别对已有后量子区块链进行归类的努力：不少链是完全开源的，代码贡献者众多，而且他们似乎也在不约而同地隐去了他们的国别、身份等信息。

可参与资产所有权和交易。与集中式系统不同，DLT 需要独立节点之间达成共识才能就账本的状态达成一致。这就带来了保护网络免受恶意行为者侵害的挑战。IOTA 基于有向无环图 DAG 设计，这是一种新交易验证先前交易的结构，与大多数 DLT 使用的典型区块链不同：在基于区块链的系统中，交易被分组为块并链接在一起，从而产生了天然的瓶颈；然而，IOTA 通过利用所谓的纠缠 (Tangle) 机制绕过了这一限制，从而实现了更具可扩展性和高效的网络，它消除了集中验证的需要，并为交易和数据交换提供了分散且安全的环境。

(2) **QRL**。发布于 2016 年 QRL 宣称是第一个工业级的后量子区块链系统。QRL 是抗量子账本（Quantum Resistant Ledger）一词的缩写，它是一个开源项目（https://www.theqrl.org/），由 Peter Waterland、Kaushal Kumar Singh 和 James Gordon 共同领导，到目前为止，已有来自 80 多个不同开源库的近 60 位代码贡献者的超过 12000 次的迭代。QRL 得到了 Open Quantum Safe (OQS) 项目（https://pqca.org/）的支持，使用了 IETF 推荐的后量子签名算法 XMSS，这也是一个基于密码学哈希函数的且具有前向安全性的后量子签名方案，它也获得了 NIST 的认可。QRL 使用了由链接的 XMSS 树组成可伸延状态非对称超树的方法，这个方法的优点是使用已核实的签名方法，并且容许生成可以签名交易的账本地址，避免了庞大 XMSS 结构的预先计算延迟。在使用了基于哈希的抗量子签名算法 XMSS 以外，QRL 还兼容多种后量子签名方案（Sphincs、

Falcon 等）以及扩展账户地址，通过地址格式的更新，并支持不同的哈希函数（SHA256、SHAKE128, SHAKE256 等）。在共识方面，QRL 使用了低功率 POS 算法，该算法使用了迭代哈希链和可证实的基于哈希的伪随机数函数，摆脱了对传统签名依赖性，更好的保障了区块链的安全性。

（3）**Algorand**。发布于 2016 年的 Algorand 是由美国图灵奖得主 Silvio Micali 团队设计的，其核心技术特征是使用了可验证随机函数 VRF 来实现所谓的密码抽签（Cryptographic Sortition）功能，并以此从一群大范围的验证者中选取一部分验证者运行他们自己设计了一类 BFT 算法，从而达到提高共识效率的效果。尽管 Algorand 系统目前的硬件钱包还使用了不抗量子的签名算法 ED25519，但是 Algorand 的框架设计中对所使用的签名算法并不指定具体的实例化，这就是说，它自然而然具有抗量子特性，只要实例化时采用了抗量子的签名算法即可。Algorand 在其官网上宣称：在 NIST-PQC 后量子签名算法候选标准确定之前，拟选定 Falcon 作为自己的签名算法，以提供量子安全性[11]。

（4）**Mochimo**。发布于 2018 年的 Mochimo 是由 Matt Zweil 领导的 Mochimo 基金会所开发（https://mochimo.org/）。Mochimo 是一个致力于提供抗量子安全性、可扩展性和高吞吐量的加密货币系统，它采用基于哈希的 Winternitz 一次性签名方案的改进版本（WOTS+）以确保交易签名的抗量子安全。Mochimo 还支持自定义

[11] Algorand 的 Github 项目上集成 Falcon 的时间是 2021 年 12 月，见 https://github.com/algorand/falcon。

地址标签功能，允许用户使用只有 12 字节的简短标签来标记尺寸庞大的抗量子账户地址。在可扩展性方面，Mochimo 使用了一种专有算法 ChainCrunch 大幅提高了交易吞吐量，并支持压缩账本技术以实现区块链节点的快速建立。该项目的源代码已在 github 上开源（https://github.com/mochimodev/mochimo），并在 MPL 2.0 派生的开源许可证下获得授权。

（5）**Bitcoin PQ**。2018 年，Bitcoin 的抗量子版本发布（https://www.bitcoinpq.org/），它是由 Noah Anhao，Domef Fd，Serhiy Khvashchuk，Oleksandr Kravchenko 和 Oleg Lavronov 共同研发实现的。Bitcoin PQ 从比特币的第 555000 个区块开始进行硬分叉，是比特币主链的一个抗量子实验性分支，在保持比特币的所有基本功能不变的情况下，Bitcoin PQ 提供了更强的抗量子特性和隐私保护特性。Bitcoin PQ 采用了基于密码学哈希函数的且具有前向安全性的后量子签名算法 XMSS，以支持量子安全新特性。在运行初期，Bitcoin PQ 同时支持经典签名方案 ECDSA 和抗量子签名方案 XMSS。但在主链运行一年后，Bitcoin PQ 已弃用 ECDSA 签名方案，仅支持抗量子签名方案 XMSS。在传统比特币中，出于隐私和安全的考虑，建议每进行一次交易就使用一个新地址。与比特币不同，Bitcoin PQ 推荐有限次的重用单一地址。在共识方面，采用了抗量子工作量证明算法 Equihash96x3。此外，Bitcoin PQ 采用了基于后量子安全的零知识证明来实现匿名交易，从而保护用户的隐私。

(6) **QANplatform**。从其官网（https://www.qanplatform.com/en）看，这个项目最早是 2019 年就启动的，开发团队来自 10 多个国家的 30 多位成员构成，总部注册在爱沙尼亚。QANplatform 从其架构上看是一个混合链：一方面，它可以被用作类似 Corda 或 Hyperledger 的私有链；另一方面，它也可以被用作类似于 Solana、Cardano 和 Polkadot 这样的公有链。从其白皮书看，QANplatform 的抗量子特征很丰富：首先，它在其交易签名中使用了后量子签名算法 Glyph（这是一个基于 RLWE 问题的抗量子签名算法），并且还提供了一个称之为 QAN XLINK 的面向客户端的交叉签名协议，这个协议能够支持兼容以太坊的钱包（如 MetaMask 和 Trust Wallet）与抗量子签名密钥对的无缝集成[12]；其次，它借鉴使用了 Algorand 的共识机制，并在机制实现（如 VRF）中使用了基于格上 SIS 问题的累加器技术，在其合约地址的生成中也嵌套使用了基于 SIS 的哈希函数和标准的 SHA 哈希函数；最后，为了进一步增强其智能合约的表达能力，QANplatform 的虚拟机居然提供了支持格基全同态加密算法（GSW 类型）和基于身份的加密（IBE）的操作码（opcodes）。

(7) **TideCoin**。发布于 2020 年的 TideCoin 是一种抗量子安全的加密货币系统（https://tidecoin.co/）。Tidecoin 采用基于格的后量子签名算法 Falcon，该算法具有签名尺寸小、运行高效、可扩展性强等特点，适用于需要快速处理大量交易的应用环境。在共识方

[12]从 QANplatform 官网上的最新信息看，它已经通过 QAN XLINK 来使用了 NIST-PQC 第三轮推荐的候选后量子签名算法 CRYSTALS-Dilithium。

面，Tidecoin 使用对 CPU 友好的 PoW 算法 yespower，让使用普通计算机的个人也能参与挖矿。此外，Tidecoin 支持包括电脑端、移动端等多种类型的钱包，确保用户体验友好。Tidecoin 也支持根据网络需求动态调整区块大小。这一点对于处理大量交易与优化网络拥堵具有重要作用。目前，Tidecoin 在 github 上开源了项目的源代码（https://github.com/tidecoin），鼓励社区参与其开发和治理，以促进项目的更新迭代。

（8）**PQFabric**。这是加拿大滑铁卢大学的量子信息领军人物 Michele Mosca 团队于 2020 年提出的一个基于 Hyperledger Fabric 的后量子区块链架构，其后量子特征的集中体现是它集成了一个开源的后量子密码库 LibOQS 0.4.0（而不仅仅是某个单一的后量子密码算法），因而提供了完备的密码敏捷性（crypto-agility）。由于 LibOQS 是用 C 语言写的，而 Hyperledger Fabric 是用 Go 语言写的，因此 PQFabric 的核心是对 LibOQS 写了一个接口（称之为 CGO wrapper）。为了支持交易的后量子迁移，PQFabric 使用了证书系统 X.509 的一个经典-后量子混合版本，在其中首次明确提出了所谓的对偶组合签名思想：将待签名的消息 m 拆分为对偶的两部分 (m_1, m_2)，先用后量子签名算法 Σ_1 对原始消息生成签名 σ_1，再用经典签名算法 Σ_2 对组合的消息 $m_1 \| \sigma_1 \| m_2$ 生成签名 σ_2，最后令 $\Sigma = (\sigma_1, \sigma_2)$ 为最终输出的签名。这样做的好处是提供了对不支持后量子密码算法的节点的后向兼容（签名生成时只需令 m_1 和 σ_1 为空串即可）。PQFabric 在其官宣论文[51] 中还提供了详细的

使用不同的后量子签名算法（如 Falcon-512/1024、Dilithum-2/3/4、qTesla-p-1）后的出块延迟时间和系统的吞吐量的测试结果。

(9) **Cellframe**。这是由俄罗斯圣彼得堡国立信息技术机械与光学大学的 Dmitry Gerasimov 和第聂伯彼得罗夫斯克国立大学 Mira Brezhinskaya 两人于四年前共同建立的一个面向服务的后量子区块链开源项目（https://gitlab.demlabs.net/cellframe）[13]，现有近 20 位主要贡献者。Cellframe 的抗量子特性主要体现在两个方面：首先，它选择了 NTRU、Frodo、SIDH 等诸多后量子加密算法；其次，它宣称选择后量子密码算法 Crystal-Dilithium 作为平台默认的签名算法，同时也宣称使用另一个零知识后量子签名算法 Picnic。与已有区块链不同的是，Cellframe 宣称的设计目标居然不是成为一个区块链（协议），而是成为一个通用的构建区块链生态的基础架构层（infrastructure layer），并计划重建 OSI 模型第 3 层至第 7 层的一切，以使得所有现存的区块链都能够迁移到 Cellframe 上并获得前所未有的性能和安全水平。为此，Cellframe 宣称完全基于 C 语言开发，不使用任何第三方代码，甚至强调不能依赖于任何操作系统内核，从而能够高效地和主机或者智能冰箱一起运行（be efficient in working with both mainframes and smart refrigerators）。Cellframe 还引入了所谓的零级协议的概念（Zero level protocol）作为其共识机制，根据该协议，在零级链上只需要验证 1% 的创始区块，每个创始区块也仅包含 1 个数据项（通常是元数据和根公钥的集合），创

[13]从其官网看（https://cellframe.net/），现在 Cellframe 由 Demlabs 公司运维。

始区块后的每个数据项都必须由一个根密钥进行签署。

(10) **Qoin**。根据我们的调研，现在有两个区块链系统都叫 Qoin。第一个 Qoin（https://qoin.world/）是 2020 年 1 月在澳大利亚推出的以密码货币为主体的平台，具有桥接到以太坊区块链的能力，其生态系统已经拥有超过 60,000 个注册用户，其中包括超过 30,000 家注册企业，并且从 2020 年 1 月到 2023 年 12 月，Qoin 用户在 554,000 笔交易中交易了超过 25 亿澳元的 Qoin。但是，从其官网看，这个 Qion 平台跟后量子区块链没有关系。

第二个 Qoin 是 2024 年 1 月才发布的，其白皮书 1.0 版中表明（https://twitter.com/PostQuantumQoin）：Qion 在提供了一个去中心化的抗量子 AI 超级计算网络（Decentralized Quantum-resistant AI Supercomputing Network, DQASN）。Qion 可以使用多种 NIST-PQC 征集的后量子密码算法，并在区块链钱包和区块链验证节点上使用了多重签名的机制。例如，它使用 Falcon 和 Dilithium 生成密钥对，分别用私钥对交易进行签名，然后验证时使用对应的公钥验证签名的合法性。此外，Qoin 也在其共识机制中使用抗量子安全的可验证随机函数生成可验证的工作量证明。DQASN 也使用了一个称之为量子纠缠的协议（Quantum Entanglement Protocol, QEP）——但其本质上是个经典协议，而非量子的——在每一轮的区块生成时进行收集，并且计算他们的权重，分析区块的重要性，这样就能使区块链达到快速收敛，提升整条链上的吞吐量。

6.2 国内后量子区块链研发现状

(1) **ABCCoin**。早在 2016 年，丁津泰团队就提出过一种在比特币架构上更换签名算法，以期达到抗量子的效果的抗量子区块链。在 2018 年，抗量子区块链 ABCCoin 正式发布，但目前该区块链并未向社会发行数字货币。整个算法的基础是建立在比特币 0.8.6 版本上的，将比特币的椭圆曲线签名算法替换为了基于多项式的彩虹签名算法 Rainbow。此外，ABCCoin 更新了 PoW 公式算法：不再使用基于哈希函数的 SHA-256 作为挖矿算法，而是使用了求解多元多项式的新式挖矿程序 ABCardO，这种这种解多项式的挖矿方式将会在不同的难度等级时，使数学家们了解到不同的多项式时间内能解决多大算力数学题等有意义的数学问题。

(2) **Hcash**。2017 年，由上海交通大学和香港理工大学团队联合发布了 Hcash (https://h.cash/)。Hcash 使用了 BLISS 和 MSS/LMS 两个抗量子签名方案。BLISS 是一种基于格的抗量子签名方案，对比现有的抗量子签名算法，其拥有最小的公钥和签名尺寸，而 MSS/LMS 则是一种基于哈希的高效抗量子签名方案。另外，Hcash 与传统的 ECDSA 签名兼容。在隐私保护方面，Hcash 改进和优化了 zk-snarks，采用了基于格的抗量子环机密交易 (RingCT) 来保护用户隐私。在架构方面，Hcash 采用并生的双链构架，此架构由原有的 Hshare 链升级后的 HyperCash (HC) 主链以及由 Hcash 孵化出的 HyperExchange (HX) 主链组成。两条主链互相协作，共同组成 Hcash 双链双币生

态系统。在共识机制方面，Hcash 采用 PoW+PoS 混合共识机制，所有基于 PoW 共识所生成的区块均须经过 PoS 共识的验证，才能成为合法区块。即 PoW 共识负责生成区块，PoS 共识负责投票决定区块的有效性，矿工与权益持有者共同参与区块生成，能够减轻算力过于集中的问题。

（3）**树图链**。树图链（Conflux）是我国唯一合规、公共和无需许可的区块链，由首位华人图灵奖获得者、著名计算机科学家姚期智担任首席科学家，并获得国家认可，于 2021 年 1 月 12 日获得上海市科学技术委员会筹集的 500 万美元的融资。Conflux 链采用了与常规区块链单链结构完全不同的结构，采用了高效的树状图链，并借鉴了一种名为“GHOST”的规则确定主链，根据主链和引用链接确定区块顺序和交易顺序。Conflux 链还能够完全兼容以太坊的智能合约，同时在共识上引入了一条独立运行的 PoS 链，不仅提升了链上信息数据处理速度，还大大提升了安全性能。虽然采取了这种 PoW+PoS 的机制，Conflux 链仍然坚持去中心化的性质，并予以安全性的增强。目前为止，Conflux 链没有公开宣布使用任何特定的抗量子密码算法，但是他们在 Github 中的代码库却显示已经做好了 Dilithium 抗量子签名算法的适应性改造，相信在不久的将来会通过版本更新将 Dilithium 算法集成到链中。总体来说，目前国内的研究还处于初步探索阶段。

（4）**长安链**。2022 年，由北京微芯区块链与边缘计算研究院牵

头，清华大学、腾讯公司等多家校企联合参与的长安链宣布集成了 Dilithium 抗量子签名算法，能够在量子安全下保证交易的真实性与可信度。作为国内首个可控区块链软硬件技术体系，长安链携手央行数研所，共同推进数字人民币企业级应用；联合国家公共信用信息中心与北京市大数据中心协同探索“区块链 + 信用”的创新应用。同时，长安链为了保证其上层应用的加密过程也能抵抗量子攻击，提出了基于 NTRU 格的抗量子多方安全计算方案，此算法输出向量短、拥有高效的运算能力。相比于传统多方门限解密依赖大整数分解、离散对数求解等困难问题，在量子计算机的攻击下已无法保证其安全性，这种方案提供了一种抗量子多方门限解密能力，采用了基于格构造的密码算法，在量子计算机的攻击下仍然是安全的。

(5) **天翼链**。天翼链是由中国电信自主研发，具备高可用底层存储、支持跨集群组网及隐私增强的区块链即服务 (BaaS) 平台。天翼链已广泛应用于物联网、政务、数据要素流通领域，提供了功能强大的分布式可信计算能力。2022 年，天翼链提供 Dilithium+SM2 混合签名作为可选签名组件，构建了量子安全的链上交易签名及身份验证类服务；2023 年，在数据融通中，基于 LPN、RLWE 格设计的安全多方计算算法簇保障了数据要素流通中的底层密码原语的量子安全性；2023 年，在通信传输方面，天翼链支持通过 PQC 及 QKD 两种量子安全密钥协商方式进行部署，从而为各类复杂场景提供安全可靠的传输信道。目前，天翼链与中国电信后量子隐私计

算系统-密流量子盾正推进实现抗量子组件融合，以构建具备长效安全性的数据要素流通可信计算基础框架。

(6) **趣链**。趣链科技是由中国工程院陈纯院士担任首席科学家的区块链领域首家独角兽企业，在数字政务方面拥有电子档案管理、数字身份服务、公检法司联盟链等能力，使其和住建部、科技部等部委，北京市人民政府、杭州市人民政府等人民政府达成合作。从 v2.16 版本趣链区块链平台已经支持了抗量子账户以及账户交易的签名和验签部分的抗量子密码算法，由于 Dilithium 抗量子签名算法具有较高的安全性和较短的密钥和签名大小，而被趣链最终选择，同时趣链还提供了密码算法在线升级和切换功能，方便用户选择经典密码和抗量子密码。

(7) **蚂蚁链**。蚂蚁链是蚂蚁集团代表性的科技品牌，其在数据要素、金融、数字政府等应用场景拥有巨大的用户群，为了抵抗量子计算机的攻击，也紧跟技术潮流，在交易签名中集成了 Dilithium 抗量子签名算法，同时因为其在多种场景的广泛应用，为了保证所传输的数据不受到量子计算机的攻击，在 TLS 通信模块集成了抗量子机制，保障了数据在传输中的安全。

(8) **ROTA**。2024 年，布比科技联合北京理工大学、中国科学院信息工程研究所与北京航空航天大学，在原布比链的基础上，集成了由中国科学院信息工程研究所王鲲鹏团队提出的后量子签名算法 Dilithium R，推出了布比后量子区块链 ROTA。Dilithium R 是

在 NIST-PQC 优胜算法 Dilithium 的基础上，引入了基于基座旋转 (Rotation) 操作的改进，相比原算法性能有近 20% 的提升。ROTA 同时支持 ED25519 签名和 Dilithum R 签名，支持传统账户和后量子账号之间的交易，也支持传统账户、交易、智能合约的后量子迁移。

第七章 后量子密码迁移发展建议

为了推动我国后量子密码迁移工作，提升我国各行各业的量子威胁防护能力，我们提出以下几点发展建议。

7.1 加快我国后量子密码标准体系建设

积极推动我国后量子密码算法的遴选和标准制定。目前我国还没有后量子密码相关的商密标准和监管规范，亟需加快推进国内的后量子密码算法遴选和标准制定工作，尝试多种技术路线，从工程开发的角度，围绕性能、存储、抗侧信道攻击等方面给出后量子密码算法标准化规范。

加速推进后量子公钥基础设施的构建。公钥基础设施是信任建立的根源，完成具有量子抗性的公钥基础设施的改造对现有安全协议及应用至关重要。持续推进密码基础设施的标准化进程，结合国密算法在证书迁移中的经验，逐步建立从传统密码证书，过渡到后量子密码证书的规范。

加快后量子密码向安全协议规范的推广。基于密码学的安全协议为丰富的互联网应用建立基础，但也最容易受到先存储后解密攻击，因此将后量子密码推广到广泛的安全协议尤为重要。亟需从传输层安全协议（如 SSL、SSH、QUIC 等）出发，推进其他后量子密码协议标准与规范的体系建设。

7.2 加快现有系统量子脆弱性发现与评估

加快量子脆弱性发现工具的研发。在经典密码算法面临被量子计算攻破的背景下，能够对各类信息系统完成量子脆弱性感知，才能有的放矢，从容应对后量子迁移工程上的挑战。需要在现有后量子脆弱性发现工作流和量子脆弱性发现框架下，结合我国商密算法迁移的经验，扩展更多的发现场景、开发更丰富的密码态势感知工具，梳理更全面的量子脆弱点。

加快建立各行业的风险评估模型。有限的迁移资源和能力使得立即对各个行业所有的量子脆弱组件进行改造是不现实的，需要围绕具体细分行业的业务需求，建立和维护风险评估样本库，并推出有行业针对性的风险评估模型。然后，根据各个业务系统的后量子风险评估模型，获得后量子迁移任务的优先级列表。

7.3 培育后量子密码迁移生态

优先推进后量子密码混合迁移模式。在后量子密码迁移早期采用混合密码机制的方式，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。法国 ANSSI，德国 BSI，荷兰 AIVD，电信领域的 GSMA，以及标准化组织 IETF 均推荐在迁移前期采用混合模式。优先设计具备向后兼容性、高性能且具有最小重复信息的后量子密码迁移替换方案，充分考虑密码敏捷性和灵活性在后量子迁移中的重要作用。

支持后量子密码可插拔实现和回滚机制。量子计算机和量子算

法的研究仍处于学术界的前沿，现有的后量子密码算法仍存在被攻破的可能。成熟且稳定的后量子迁移生态应当推动对后量子密码的可插拔实现，这意味着新的迁移系统要允许用户根据需要选择不同的后量子密码算法。此外，迁移还需要考虑回滚机制，一旦迁移的后量子算法被攻破，需要具有回滚到以前的版本或状态的机制。

全面开展后量子密码迁移工程测评。在后量子密码迁移过程中，需要在不同系统和应用环境下进行全面评测，主要包括：性能测试，评估后量子密码算法在实际应用中的处理速度和资源消耗，确保其能够满足业务需求；兼容性测试：检查后量子密码算法与现有系统和协议的兼容性，确保在迁移过程中不会破坏现有的功能和服务；互操作性测试：测试后量子密码算法在不同厂商和平台之间的互操作性，确保其能够在多样化的环境中正常运行。为后量子密码强制迁移做好准备。

健全产学研协同的人才培养模式。参考世界各国各领域的后量子迁移规划，结合量子计算技术日新月异的发展趋势，后量子迁移工作预计会在六到十年内完成，时间之紧迫使得仅靠一家或少数企业无法解决所有技术问题，需要产业、学校和科研机构间的通力合作。产业界应当协调步伐，通过创建后量子迁移生态联盟，集中产业链上下游力量，建设国内后量子迁移生态圈。企业、科研院所之间可以组成研发联盟，国内高校则需创新人才培养模式，推进产学研协同的人才培养模式。

参考文献

[1] NIST. Migration to post-quantum cryptography:preparation for considering the implementation and adoption of quantum safe cryptography[R]. Maryland, Virginia: U.S. Department of Commerce, 2023.

[2] NIST. Migration to post-quantum cryptography quantum readiness: Cryptographic discovery[R]. Maryland, Virginia: U.S. Department of Commerce, 2023.

[3] NIST. Migration to post-quantum cryptography quantum readiness: Testing draft standards[EB/OL]. U.S. Department of Commerce, 2023. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf.

[4] GSMA. Quantum telco network impact assessment whitepaper version 1.0[EB/OL]. GSMA, 2023. https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf.

[5] GSMA. Guidelines for quantum risk management for telco version 1.0[EB/OL]. 2023. https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/09/Guidelines-for-Quantum-Risk-Management-for-Telco-v1.0.pdf.

[6] GSMA. Post quantum cryptography-guidelines for telecom use

cases version 1.0[EB/OL]. 2024. https://www.gsma.com/newsroom/wp-content/uploads/PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf.

[7] BSI. Cryptographic mechanisms:recommendations and key lengths [R]. Germany: Bundesamt für Sicherheit in der Informationstechnik(BSI), 2024.

[8] AIVD. Bereid je voor op de dreiging van quantumcomputers[R]. Dutch: Algemene Inlichtingenen Veiligheidsdienst (AIVD), 2021.

[9] Korea Post Quantum Cryptography Research Group. National Post Quantum Cryptography Contest[EB/OL]. 2021. https://www.kpqc.or.kr/competition.html.

[10] Institute for Monetary and Economic Studies, Bank of Japan. On mitigation to PQCs[EB/OL]. 2019. https://www.imes.boj.or.jp/research/abstracts/japanese/19-J-15.html.

[11] The Ministry of Science and ICT. The commemoration ceremony of the 12th Information Security Day is held[EB/OL]. 2023. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=830.

[12] ANSSI. Anssi views on the post-quantum cryptography transition[R]. French: Agence nationale de la sécurité des systèmes d'information(ANSSI), 2022.

[13] ACSC. Planning for post-quantum cryptography[EB/OL]. Aus-

tralian Cyber Security Centre(ACSC), 2023. https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography.

[14] 赛迪研究院. 应对量子计算挑战需积极推进后量子密码研发和迁移[R/OL]. 中国电子信息产业发展研究院, 2023. https://report.ccidgroup.com/.

[15] 中国信通院. 后量子密码应用研究报告[EB/OL]. “密码 +”应用推进计划, 2023. https://www.wosign.com/Docdownload/20231130.pdf.

[16] CHINATELECOM. 中国电信后量子隐私计算白皮书[EB/OL]. 2023. http://www.chinatelecom.com.cn/news/02/202311/t20231111_77827.html.

[17] 任奎, 张秉晟, 张聪. 密码应用: 从安全通信到数据可用不可见[J]. 密码学报, 2024, 11: 22-44.

[18] 梁敏, 罗宜元, 刘凤梅. 抗量子计算对称密码研究进展概述[J/OL]. 密码学报, 2021, 8: 925-947. DOI: 10.13868/j.cnki.jcr.000488.

[19] DONG X, WANG X. Quantum key-recovery attack on feistel structures[J/OL]. Sci. China Inf. Sci., 2018, 61(10): 102501:1-102501:7. https://doi.org/10.1007/s11432-017-9468-y.

[20] JOSEPH D, MISOCZKI R, MANZANO M, et al. Transitioning organizations to post-quantum cryptography[J/OL]. Nat., 2022, 605

(7909): 237-243. https://doi.org/10.1038/s41586-022-04623-2.

[21] HÄNER T, ROETTELER M, SVORE K M. Factoring using $2n+2$ qubits with toffoli based modular multiplication[J/OL]. Quantum Inf. Comput., 2017, 17(7&8): 673-684. https://doi.org/10.26421/QIC17.7-8-7.

[22] GIDNEY C, EKERÅ M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits[J/OL]. Quantum, 2021, 5: 433. https://doi.org/10.22331/q-2021-04-15-433.

[23] BRAVYI S, CROSS A W, GAMBETTA J M, et al. High-threshold and low-overhead fault-tolerant quantum memory[J/OL]. Nat., 2024, 627(8005): 778-782. https://doi.org/10.1038/s41586-024-07107-7.

[24] NIST. Pqc candidates to be standardized and round 4[EB/OL]. 2022. https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.

[25] NIST. Module-lattice-based key-encapsulation mechanism standard: 203 (Draft)[EB/OL]. Washington, DC: U.S. Department of Commerce, 2023. https://doi.org/10.6028/NIST.FIPS.203.ipd.

[26] NIST. Module-lattice-based digital signature standard: 204 (Draft) [EB/OL]. Washington, DC: U.S. Department of Commerce, 2023. https://doi.org/10.6028/NIST.FIPS.204.ipd.

[27] NIST. Stateless hash-based digital signature standard: 205 (Draft)

[EB/OL]. Washington, DC: U.S. Department of Commerce, 2023. https://doi.org/10.6028/NIST.FIPS.205.ipd.

[28] European Commission. Horizon 2020[EB/OL]. 2020. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en.

[29] European Commission. ISO/IEC PWI 19541: Inclusion of key encapsulation mechanisms for Post-Quantum Cryptography in ISO/IEC standards[EB/OL]. 2023. https://genorma.com/en/standards/iso-iec-pwi-19541.

[30] National Cyber Security Centre. Next steps in preparing for post-quantum cryptography[EB/OL]. 2024. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography.

[31] 中国密码学会. 全国密码算法设计竞赛通知[EB/OL]. 2019. https://sfjs.cacrnet.org.cn/site/content/309.html.

[32] 国家标准化管理委员会. 2023 年全国标准化工作要点[EB/OL]. 2023. https://www.sac.gov.cn/xw/tzgg/art/2023/art_80c53d6e4b064ec0b64b3a1e2980fe3e.html.

[33] 魏汉玉, 郑婕妤, 赵运磊. 基于 Cortex-M4 的 CNTR/CTRU 密钥封装高效实现[J]. 计算机学报, 2024, 47: 589-607.

[34] 密码行业标准化技术委员会. 2023 年度密码行业标准制修订任务 (商用密码领域)[Z]. 北京, 2023.

[35] GROUP Q R W. Canadian national quantum-readiness best prac-

tices and guidelines[EB/OL]. Canadian Forum for Digital Infrastructure Resilience (CFDIR), 2023. https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf.

[36] ADVISORS A C S. The pqc migration handbook: Guidelines for migrating to post-quantum cryptography[R/OL]. Applied Cryptography and Quantum Algorithms(TNO) and Cryptology Group(CWI) and Netherlands National Communications Security Agency(AIVD), 2023. https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf.

[37] NSM. National security memorandum on promoting united states leadership in quantum computing while mitigating risks to vulnerable cryptographic systems[EB/OL]. 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[38] QUSECURE. Qusecure awarded u.s. army contract for post-quantum cybersecurity solutions[EB/OL]. 2023. https://www.qusecure.com/qusecure-awarded-u-s-army-contract-for-post-quantum-cybersecurity-solutions/.

[39] SANDBOX. Defense information systems agency awards sandboxaq other transaction authority agreement for prototype to provide quantum-resistant cryptography solutions[EB/OL]. 2023. https://www.sandboxaq.com/press/defense-information-systems-agency-awards-sandboxaq-other-transaction-authority-agreement-for-prototype-to-provide-quantum-resistant-cryptography-solutions.

[40] QUSECURE. Qusecure named commercial capabilities showcase winner by air force global strike command and small business consulting corporation[EB/OL]. 2023. https://www.qusecure.com/qusecure-named-commercial-capabilities-showcase-winner-by-air-force-global-strike-command-and-small-business-consulting-corporation/.

[41] Bis innovation hub announces new projects and expands cyber security and green finance experiments[EB/OL]. The Bank for International Settlements, 2022. https://www.bis.org/press/p220617.htm.

[42] CORPORATION D T C. Post-quantum security considerations for the financial industry[EB/OL]. 2022. https://www.dtcc.com/dtcc-connection/articles/2022/september/21/post-quantum-security-considerations-for-the-financial-industry.

[43] The banque de france has successfully experimented with cryptonext security post-quantum security technologies[EB/OL]. The

Banque de France, 2022. https://www.banque-france.fr/en/espace-presse/communiques-bdf/la-banque-de-france-realise-avec-cryptonext-security-une-experimentation-de-securite-post-quantique.

[44] MOSCA M, MULHOLLAND J. A methodology for quantum risk assessment[EB/OL]. 2020. https://globalriskinstitute.org/mp-files/a-methodology-for-quantum-risk-assessment-pdf.pdf.

[45] BARKER W, POLK W, SOUPPAYA M. Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms: NIST CSWP 15[R]. Gaithersburg, MD: National Institute of Standards and Technology, 2021.

[46] MA C, COLON L, DERA J, et al. Caraf: Crypto agility risk assessment framework[J]. Journal of Cybersecurity, 2021, 7(1): 1-11.

[47] P.-Q. C. W. Group. Risk model technical paper[R]. FS-ISAC Post-Quantum Cryptography Working Group, 2023.

[48] LEE C C, TAN T G, SHARMA V, et al. Quantum computing threat modelling on a generic cps setup[C]//Applied Cryptography and Network Security Workshops: ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, June 21–24, 2021, Proceedings. Springer, 2021: 171-190.

[49] C. I. S. Agency and N. S. Agency and N. I. of Standards and Tech-

nology. Quantum readiness: Migration to post-quantum cryptography[R]. Arlington, Virginia: CISA, 2023.

[50] SIKERIDIS D, KAMPANAKIS P, DEVETSIKIOTIS M. Assessing the overhead of post-quantum cryptography in tls 1.3 and ssh [C/OL]//2020. DOI: 10.1145/3386367.3431305.

[51] HOLCOMB A, PEREIRA G C C F, DAS B, et al. Pqfabric: A permissioned blockchain secure from both classical and quantum attacks[C/OL]//IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021, Sydney, Australia, May 3-6, 2021. IEEE, 2021: 1-9. https://doi.org/10.1109/ICBC51069.2021.9461070.

联系方式：

西安电子科技大学广州研究院

广州链融信息技术有限公司

邮箱：ly@lianrongtech.com

电话：吕洋 13641449825（微信同号）

网址：https://www.lianronginfo.com/about/