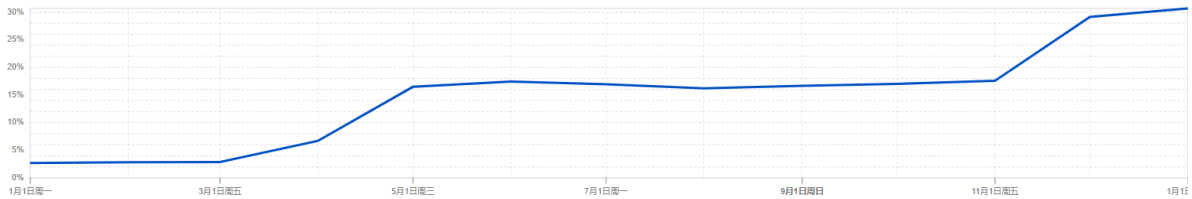
后量子密码已来，传统密码死期已定

密码算法对于保护机密信息免受未经授权的访问至关重要。几十年来，无论是国际算法还是国密算法都已被证明足够强大，可以抵御使用传统计算机试图破解密码算法的攻击。然而，未来的量子计算可能会秒破这些算法，使数据和信息变得脆弱。对抗这种未来的量子能力需要新的密码算法，这些算法可以保护数据免遭使用当前传统计算机和未来的量子计算机发起的攻击。这些算法称为后量子密码(Post-Quantum Cryptography，简称 PQC)。

尽管向后量子密码的过渡在量子计算机问世之前就开始了，但仍然存在紧迫的威胁。攻击者现在收集加密数据，目的是在量子技术成熟后解密数据，这就是“先收集-后解密”的安全威胁，因为许多机密数据的价值往往会持续多年，有些个人机密数据会伴随人的一生，因此现在开始过渡到后量子密码，对于防止未来发生机密数据被解密至关重要。这种威胁模型是迫切过渡到后量子密码的主要原因之一。

一、后量子密码已来，来势迅猛

根据 Cloudflare 发布的 2024 年度报告，Cloudflare 已于 2022 年 10 月开始在其服务网络上默认启用了后量子密码算法，2024 年 4 月 17 日发布的谷歌浏览器 Chrome 124 版本默认启用后量子密码协议后，PQC 密码算法流量在一个月内从略高于 2% 的请求迅速增加到 12% 左右，并在 11 月末达到 13%, 2025 年 1 月 1 日达到 30%，这是由于其他基于 Chromium 的浏览器升级到 124 版本后，再加上火狐浏览器的默认支持和苹果 Safari 浏览器的初步测试导致了继续不断上升中。



这就是本文题目所讲的“后量子密码已来”，并且来势迅猛，在 HTTPS 加密中普及应用后量子密码将有效解决“先收集-后解密”的安全威胁。大家可以使用谷歌浏览器查看一下 ztbro.com 的安全概览，其中网络连接部分显示：与此网站的连接已使用 TLS 1.3、

X25519MLKEM768 和 AES_128_GCM 进行加密和身份验证，这个 X25519MLKEM768 就是一种后量子密码算法-混合后量子密钥交换协议，用于非对称密钥算法的密钥封装，而网站部署的是传统密码 ECC 算法 SSL 证书。

ML-KEM-768 是美国国家标准技术研究院(NIST)于 2024 年 8 月 13 日发布的 FIPS 203 基于模块格的密钥封装机制标准，这是密钥封装机制(KEM)的一组算法之一，通讯双方可以使用这些算法在公共通道上建立共享密钥。使用 KEM 建立的共享密钥可以与对称密钥加密算法一起使用，以执行安全通信中的基本任务，如加密和身份验证。该标准指定了一种称为 ML-KEM 的密钥封装机制，ML-KEM 的安全性与 Module Learning with Errors 问题的计算难度有关。目前，ML-KEM 被认为是安全的，即使面对将来的量子计算机也是安全的。该标准指定了三个参数集，按安全强度增加和性能降低的顺序，分别是 ML-KEM-512、ML-KEM-768 和 ML-KEM-1024。

二、传统密码算法死期已定，必须提前做好相应准备

为了应对“先收集-后解密”的安全威胁，美国国家标准技术研究院(NIST)于 2024 年 11 月 12 日发布了 NIST IR 8547《过渡到后量子密码标准》的公开征求意见草案，该报告描述了 NIST 从易受量子攻击的密码算法过渡到后量子数字签名算法和密钥建立方案的预期方法，确定了现有的易受量子攻击的密码标准以及信息技术产品和服务需要过渡到的抗量子密码标准，旨在促进与行业、标准组织和相关机构的合作，以促进和加速后量子密码的采用。

NIST 在 8 月份发布了三个 PQC 标准，以开始向后量子密码过渡的下一个重要阶段：基于模块格的密钥封装机制 [FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism]，就是

上面讲的已经开始使用的 ML-KEM 算法，基于模块格的数字签名算法 [FIPS 204, Module-Lattice-Based Digital Signature Algorithm] 和 基于无状态哈希的数字签名算法 [FIPS 205, Stateless Hash-Based Signature Algorithm]。NIST 认为，从算法标准化到完全集成到信息系统中使用可能需要 10 到 20 年时间，这个时间表反映了产业界将算法构建到产品和服务中、采购这些产品和服务以及将这些产品和服务集成到技术基础设施中的复杂性。

一旦 PQC 算法标准化，就需要修改相关应用程序以使用它们。许多应用程序包括基于标准化协议和安全组件，这些组件需要进行修改以支持 PQC 算法的使用。此外，应用程序构建在软件加密库之上，这些库要么提供加密算法的实现，要么提供硬件加密模块(HSM)的接口，这些软件加密库和硬件加密模块也需要修改以支持 PQC 算法。应用程序还可能依赖于基础设施组件，如公钥基础设施(PKI)，这些组件也需要更新以支持 PQC 算法，应用程序才能使用 PQC 算法。

三个 PQC 标准中的 FIPS 204 和 205 为抗量子数字签名算法，FIPS 203 是抗量子密钥封装算法，现有的数字签名算法 ECDSA、RSA、EdDSA 以及基于 ECC 和 RSA 算法的密钥封装算法都是容易被量子计算机破解的算法，但现有的对称密码算法则不易被量子计算机破解。

也就是说，现有的基于 RSA 和 ECC 算法的网络协议和安全技术标准，如：传输层安全(TLS)、安全套接层(SSL)、SSL VPN、安全外壳(SSH)、互联网协议安全(IPsec) 和 加密消息语法(CMS)等等，都依赖于易受量子攻击的传统密码算法，必须升级更新它们，以支持 PQC 算法，这对于维护数据机密性和完整性至关重要。

公钥基础设施(PKI)系统包括 CA 系统、RA 系统、密钥管理系统和目录服务等都必须更新 PKI 组件，以签发、分发和管理使用 PQC 算法的数字证书，并使用 PQC 算法签发证书吊销列表，确保过渡期间的向后兼容性和互操作性，这对于维护全球互联网的信任和安全至关重要。

IT 应用程序和服务涵盖组织使用的各种软件和平台，包括 Web 应用程序、数据库、通信工具、云服务和企业软件。这些应用程序依靠密码技术来保护数据、验证用户身份并确保交易安全。必须修改应用程序和服务以支持用于加密、数字签名和密钥交换的 PQC 算法。这需要更新底层加密实现，适应密钥大小和算法性能的变化，并确保与更新的协议和库兼容。开发人员需要重构代码、进行大量测试，并可能重新设计用户界面以适应这些变化。

为此，NIST 列出了迈向 PQC 标准过渡时间表，目标是到 2035 年尽可能低降低量子风险。如下表所示，目前正在广泛使用的安全密码算法 RSA-2048 和 ECC-256 将在 **2030 年弃用，2035 年禁用**，这就是传统密码算法的死期，要求业界必须提前做好所有相关系统和产品向 PQC 算

法的迁移工作。

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

三、我国应尽快出台后量子商用密码标准及相应的 PQC 迁移计划

NIST 发布的《过渡到后量子密码标准》草案目前处于公开征求意见阶段，截至日期为本周五(2025 年 1 月 10 日)，笔者特在周一撰文的目的是希望我国密码产业界高度重视这个由美国 NIST 制定的传统密码算法死期即将到来的紧迫性，因为我国正在大力推广普及应用的商用密码算法 SM2 也属于 ECC-256 算法类，属于 NIST 报告中计划 2030 年弃用的同类算法，只剩下 5 年时间了。国际 CA 都已经纷纷启用 ECC-384 算法的根证书和用户证书，虽然 ECC-384 仍然属于传统密码算法，但这是 5 年后允许继续使用到 2035 年的过渡算法，这些允许使用的过渡算法还包括 RSA-3072 和 RSA-4096 算法。

我国不仅必须尽快出台后量子商用密码标准，也必须尽快出台向后量子密码过渡的行动计划，而且也应该抓紧升级现有传统密码算法，早日启用 5 年后还允许使用的等同于 ECC-384 的 SM2-384 算法，这也是平稳过渡到 PQC 算法的必要措施，否则 5 年后将没有安全的商用密码算法可用！而一旦我国 PQC 商密算法标准确定，则相关产业界就必须立即行动起来，开始着手 PQC 商密算法迁移工作，因为这个迁移工作可能需要 10-20 年的时间才能完成，必须抢在量子计算机可用之前完成所有相关系统的 PQC 算法迁移工作，并且彻底禁用所有传统密码算法，任重道远。

王高华

2025 年 1 月 6 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 200 篇(共 58 万 1 千多字)和英文 84 篇(10 万 9 千多单词)。