量子安全技术-PQC 和 QKD 科普

PQC 是后量子密码的英文缩写，QKD 是量子密钥分发的英文缩写，这两个技术都与量子安全有关，但这是两个完全不同的容易搞混的技术名词，本文尝试用通俗易懂的语言科普一下这两个名词，尽量能客观地介绍这两个技术的长处和短处。

一、 什么是量子计算、量子密码、后量子密码？

量子计算(Quantum Computing)，是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式。与传统计算不同，量子计算遵循量子力学规律，它是能突破传统算力瓶颈的新型计算模式。量子计算令人难以置信且快速增长的功率和能力已经改变了我们使用计算机解决问题、分析信息和保护数据的方式。

量子密码(Quantum Cryptography)，是把量子计算的不可预测性用于加密和解密数据，信息直接编码在量子比特本身中。最常见的量子加密是使用量子比特的属性来保护数据，如果有人试图在未经许可的情况下解密信息，则会产生量子比特错误。

后量子密码(Post-Quantum Cryptography, PQC)，是能够在现有计算机上实现并抵抗未来量子计算机攻击的数学密码系统，其算法基于量子计算难以破解的数学难题，如基于格密码学、多变量多项式等，可通过混合密码机制兼容现有系统。

二、 QKD 不能直接加密数据

量子密钥分发 QKD 属于量子密码范畴，一种利用量子力学原理进行密钥分发的密码技术，它通过量子信道传输加密密钥，确保通信双方能够检测到任何窃听行为，从而保证密钥的安全性。即使攻击者拥有无限算力，也无法破解密钥，适合需要长期保护的高度机密数据。

QKD 需要专用的量子通信设备(如单光子源、探测器、量子信道)，成本高且部署复杂，有通信距离限制，并且必须安全稳定的物理环境(如低温、真空)和专用光纤或卫星通信支持。QKD 仅用于密钥分发，不能直接加密数据，需结合传统密码算法使用，但是传统密码算法已经不能抗量子了，QKD 也必须采用 PQC 算法来加密数据。QKD 适合于对安全性要求极高的场景(如国家安全)，其信息理论安全性无与伦比，但受限于硬件和部署成本，应用范围较窄。

(C) 2025 零信技术（深圳）有限公司

三、 PQC 不属于量子密码

后量子密码 PQC 与 QKD 最大的不同是：与量子密码没有任何技术关系，是这个名称误导了大家，准确地说：它就是现有传统密码算法的一个能抗量子攻击的升级算法，就像 RSA 密码算法从 512 位升级到 1024 位后再到现在的 2048 位一样。后量子密码同现在的密码算法唯一不同的是：理论上，现在的传统密码算法能被量子计算机秒破，而后量子密码则能抵御量子计算机的破解，属于抗量子密码算法，不属于量子密码算法。

之所以要发展后量子密码，因为这是一个低成本的解决方案，一个可以基于现有设备系统基础之上的只需相关的软硬件升级密码算法的解决方案，因为不可能丢弃现有网络系统和所有设备重新建设一套全新的量子系统。这就是后量子密码的优势：兼容性强、高效且通用和抗量子攻击。PQC 更适合广泛的商业和民用场景，易于部署且成本低，但安全性依赖于数学难题的长期可靠性，存在一定的不确定性，因为现在还没有量子计算机能真正验证其安全性，只是理论上的量子安全。

四、 目前最紧迫的是普及 PQC 算法 HTTPS 加密

最紧迫的需要升级到后量子密码的是 HTTPS 加密，因为攻击者已经开始采用“先收集后解密”的策略，先把 HTTPS 加密流量收集起来保存好，一旦量子计算机可用时就可以解密这些传统密码加密的数据了。为了防止这个攻击，必须现在就开始启用后量子密码 HTTPS 加密。

根据 Cloudflare 的统计数据，全球互联网流量中已经有 38%的流量实现了传统密码+后量子密码混合协议加密，这是基于现有的传统密码算法签发的 SSL 证书，采用现有密钥交换协议(X25519)和后量子密码密钥封装协议(ML-KEM)实现双协议封装共享密钥实现 HTTPS 加密。也就是说，全球互联网流量中的 38%的数据在量子时代也是安全的，即使是将来的量子计算机也无法破解，有效解决了“先收集后解密”的安全威胁。

(C) 2025 零信技术（深圳）有限公司

零信技术已经发布了后量子密码 HTTPS 加密全生态产品就绪时间表，明确告诉用户一个非常清晰的量子安全之路，只有现在就做好双算法 SSL 证书自动化管理，才能实现将来无缝迁移到后量子密码 HTTPS 加密，从而切实保障用户数据在现在和在量子时代的持续安全。

五、 一次改造同时完成商用密码改造和后量子密码改造

我国目前处于从 RSA 密码体系向国产密码体系迁移的关键阶段，这是一个要在已经深入到各种系统中的使用了 30 多年的 RSA 密码算法的替代改造工作，是要改造整个生态，一定是一个非常艰难的工作，所以大家都在喊“国密改造”难。

但是，随着量子计算的发展，国产 SM2 密码体系在量子计算面前也是不安全的算法，可以参考国际上对于 RSA/ECC 算法的迁移要求，一样必须在 2030 年之前完成迁移到后量子密码。也就是说，我国关键信息基础设施系统面临两次密码算法迁移工作，商用密码迁移工作还没有完成就要准备后量子密码迁移工作了，这是我国面临的独有技术问题。

零信技术创新解决方案是一次技术改造完成 HTTPS 加密的两次密码算法迁移—商用密码迁移和后量子密码迁移，同时完成了 SSL 证书自动化管理，这是最佳解决方案，省投资，省时间，省劳力。SSL 证书自动化管理是顺利完成商用密码改造和后量子密码改造的技术基础，原 Web 服务器零改造，只需在服务器端增加部署一个零信国密 HTTPS 加密自动化网关，就可以实现传统密码算法(RSA/ECC/SM2) SSL 证书和后量子密码算法 SSL 证书的自动化管理。同时在用户电脑上安装使用完全免费的、干净无广告的、支持商用密码和后量子密码的零信浏览器，就可以实现两次密码算法迁移工作一次完成，不仅采用商用密码来保证关基系统安全，而且能切实保障政务数据、商业数据和个人数据在现在和在量子时代的始终安全。

王高华

2025 年 8 月 25 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 225 篇(共 67 万 1 千多字)和英文 99 篇(13 万 4 千多单词)。

(C) 2025 零信技术（深圳）有限公司