量子霸权和后量子密码平权：通向公平的数字未来

量子计算正在叩响未来的大门。谷歌 Sycamore 和我国“九章”用 200 秒完成经典计算机需数千年甚至 6 亿年的任务，这就是“**量子霸权**(Quantum Supremacy)”。但当量子计算机威胁到传统密码体系安全时，谁将拥有数据安全的钥匙？是少数科技巨头，还是每个人？笔者在本文全球首次提出“**后量子密码平权**(Post-Quantum Cryptography Equity)”，让后量子密码技术能像 Wi-Fi 一样普及，惠及全球所有人。

一、 量子霸权：突破与隐忧

量子霸权标志着量子计算的飞跃。基于量子叠加和纠缠，量子计算机能在特定任务上实现指数级加速。谷歌 Sycamore 和我国“九章”的成功，证明了量子计算的潜力，不仅吸引了全球投资，也预示着供应链、金融和数据安全领域的革命。

然而，量子霸权并非没有隐忧。虽然当前完成的任务多为理论验证，实用性有限。但更重要的是，量子技术集中在少数国家和企业手中，可能加剧技术鸿沟。若只有巨头能驾驭量子之力，中小企业和个人的数据安全将面临风险，因为传统密码已经无法保障这些商业数据和个人隐私数据的安全。

二、 后量子密码：量子安全的基石

量子计算的崛起对传统密码体系构成了威胁。Shor 算法可轻松破解 RSA、ECC 和 SM2 密码算法，而这些算法支撑着今天的全球互联网安全。后量子密码(PQC)应运而生，这是基于格密码、哈希签名等新数学难题开发的抗量子攻击的新密码算法。美国国家标准与技术研究院(NIST)已于 2024 年 8 月发布了首批 3 个 PQC 算法标准，这些 PQC 标准的发布快速推动了后量子密码算法在各种产品和服务中的应用。

然而，后量子密码的部署面临挑战，所有系统都需要升级改造，其算法复杂性可能增加 50%的计算需求，中小型企业或物联网设备难以负担。迁移成本高、周期长，可能让发展中国家和小型组织的数据在量子时代等同于原始明文时代。如何确保量子计算不成为少数人的特权或霸权？答案在于“**后量子密码平权**”。

三、后量子密码平权：公平的数字未来

笔者提出的“后量子密码平权”，是一个让抗量子密码技术普惠化的愿景：无论企业规模、

资源多少，每个企业都应享有企业数据在量子时代的始终安全，每个人都应享有个人数据在量子时代的始终安全，以防止现在已经存在的“先收集后解密”安全威胁，保障企业商业数据和个人隐私数据安全。全球网络安全领导者 Cloudflare 已迈出了重要一步，其官方博客 2025 年 3 月 17 日文章宣称：“隐私是基本人权，高级密码技术应向所有人开放，不应为后量子安全额外付费”，Cloudflare 秉承这个平权理念，其 CDN 服务不仅实现了 SSL 证书自动化管理，而且已经为每一个用户免费升级支持后量子密码 HTTPS 加密。笔者非常赞同这个理念，并为 Cloudflare 联合谷歌浏览器在全球率先实现“后量子密码平权”点赞。

要想实现“后量子密码平权”这一伟大愿景，需要多方共同努力：

(1) 开源算法：如 Open Quantum Safe 项目、OpenSSL 项目、铜锁 SSL 项目、openHiTLS 项目等，提供免费的后量子密码库，降低技术门槛。

(2) 全球标准化：NIST 和 ETSI 的努力需全球企业参与，确保标准兼容各种系统和服务。

(3) 自动化实施：提供零改造支持后量子密码的免费无缝升级解决方案。

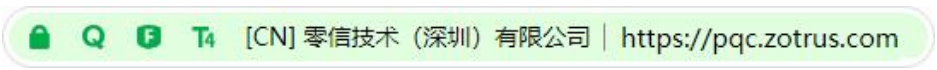
(4) 教育普及：通过培训和科普，让企业和公众了解普及应用后量子密码的重要性和紧迫性。

“后量子密码平权”不仅是技术目标，更是企业社会责任的体现。技术进步不应以牺牲公平为代价，企业的使命是让安全惠及每一个人，切实保障每个人的个人隐私数据和企业商业数据在量子时代的始终安全，而不应该是拥有“量子霸权”的少数组织的特权。

四、零信技术是“后量子密码平权”的行动派

零信技术非常重视后量子密码的研发工作，早在 2023 年 2 月就正式成为国际 PKI 联盟的成员单位，也是最早加入其后量子密码工作组的成员之一。2025 年 8 月 8 日公开发布了后量子密码 HTTPS 加密全生态产品就绪时间表，这是迈出了“后量子密码平权”的第一步。

零信技术后量子密码 HTTPS 加密应用生态中的一个最重要的产品是零信浏览器，不仅仅是一个完全免费的、支持商用密码的、干净无广告的浏览器，即将发布的 137 版本将支持后量子密码 HTTPS 加密，不仅优先采用后量子密码算法实现 HTTPS 加密，而且全球独家创新地在浏览器地址栏加密锁标识后面增加显示后量子密码标识(Q)，如下图所示，让普通网民也能一眼就知道正在访问的网站是否实现了后量子密码 HTTPS 加密，了解自己的个人隐私数据是否能在量子时代也是安全的。



所有零信浏览器用户都会免费自动升级支持后量子密码，因为零信技术同 Cloudflare 一样

认为用户不应该为后量子安全额外付费，零信浏览器秉承完全免费支持商用密码一样继续免费支持后量子密码。同时，零信浏览器这个创新 UI 就是一个后量子密码的科普工作，让高大上的后量子密码真正走进大众视野，从而带动更多的网站积极拥抱后量子密码技术，切实保障用户数据在现在和将来量子时代的始终安全。

零信技术后量子密码 HTTPS 加密应用生态中的另一个重要的产品是零信国密 HTTPS 加密自动化网关，这是一个端云一体的原 Web 服务器零改造的实现双算法(ECC 和 SM2)SSL 证书自动化管理的创新解决方案，双算法 SSL 证书自动化管理是下一步无缝升级迁移到后量子密码 HTTPS 加密的技术基础，所有部署了零信国密 HTTPS 加密自动化网关的用户都将免费无缝无感迁移到后量子密码 HTTPS 加密，因为零信技术同 Cloudflare 一样认为用户不应该为后量子安全额外付费。

五、行动铸就未来

量子霸权点燃技术革命，后量子密码平权决定其普惠程度；量子霸权就像高铁技术突破，后量子密码平权则是让每个人都能乘坐高铁。Cloudflare 通过 CDN 免费提供后量子 HTTPS 加密服务，零信技术通过浏览器和自动化网关创新，聚焦自动化和用户直观体验，填补了平权生态的空白。Cloudflare 和零信技术的实践证明，公平的数字安全未来可期。笔者呼吁更多企业加入这一使命：投资后量子密码技术，支持开源和标准化，拥抱 SSL 证书自动化管理，积极准备和实施后量子密码迁移。

零信技术作为 SSL 证书自动化管理的领导者，其责任不仅是追逐技术前沿，更是确保其成果普惠大众。让我们携手，实现后量子密码 HTTPS 加密普惠应用，打造一个安全公平的量子未来，让量子安全的钥匙掌握在每个人手中！

王高华

2025 年 8 月 18 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 224 篇(共 66 万 9 千多字)和英文 99 篇(13 万 4 千多单词)。