

决胜未来，从浏览器支持后量子密码开始

—这是一场关乎未来十年数据安全的战略抢滩

本文由 AI 辅助完成，因为今天这个话题极具未来感——**后量子密码 (PQC)**。当我们的注意力还停留在日常的业务竞争时，一场重塑互联网安全基石的革命，正从我们最熟悉的工具软件——**浏览器**——中无声地开始了。

如果您是四大浏览器(Chrome、Firefox、Safari 或 Edge)的用户，您已经不知不觉地参与了这次革命。当您在访问很多常用大流量网站时，您的浏览器正自动使用一种能抵御未来量子计算机攻击的新型密码技术-后量子密码。这标志着一个历史性转折：后量子密码已从实验室的理论，走向了全球数亿用户的规模化应用。据 Cloudflare 统计，全球互联网流量中已经有 47% 流量采用了后量子密码 HTTPS 加密，这是四大浏览器全面支持后量子密码的功劳。

一、为何是“决胜未来”？量子威胁并非危言耸听

许多人会问：“量子计算机不是还很遥远吗？”是的，实用的量子计算机或许还需五年、十年。但安全专家的警示是：“**先收集后解密**”的风险真实存在。这意味着，今天被加密传输的交易数据、商业机密、客户数据、知识产权等，正在被攻击者收集并留存。一旦量子计算成熟，这些看似安全的锁在“铁柜”里的数据都将成为明文数据。

因此，向后量子密码的迁移，不是等到量子计算机问世才开始的“升级”，而是一场必须提前布局的“安全军备竞赛”。四大浏览器巨头的行动，拉响了这场竞赛的号角。

二、浏览器为何它成为后量子密码普及的先锋？

浏览器(包括采用浏览器技术的 APP)是所有用户连接互联网的入口，HTTPS 加密是数据安全的基石。因此，浏览器的支持是 PQC 生态落地的最关键一环。目前采用的核心技术是“**混密模式**”——在 HTTPS 加密握手时，同时运行传统密码算法和后量子密码算法实现 HTTPS 加密共享密钥的加密。

这是一种极具智慧的策略：

- 保障平稳过渡：即使新型 PQC 算法存在未知漏洞，传统密码算法仍能提供保护。
- 彰显务实精神：它告诉我们，通向未来的道路不是颠覆，而是稳健的演进。

目前，全球主流四大浏览器已全部 PQC 就位。这是一次罕见的、由科技巨头们共同推动的快速技术迭代，其背后的共识与紧迫性不言而喻。

三、全球已起跑，我国处在什么位置？

当我们审视我国浏览器市场时，情况呈现出有趣的“二元格局”，这种格局给出了一个清晰的信号：浏览器市场需要更多的引领者和 PQC 教育者。

1. **主流国产浏览器**：目前都仍处于观望状态。它们的首要任务或许是满足当前其营收需要和抢占国密合规市场。这种状态可以理解，但必须认识到，PQC 是面向未来的、全球性的安全基石，与国密合规并非二选一，而是需要融合和更加紧迫的课题。
2. **后起之秀—零信浏览器**：国内唯一一个完全免费的、干净无广告的、同时支持商用密码算法和后量子密码的国产浏览器，新生力量已经走在了前面。已经实现国际算法+国密算法+后量子密码混合，这为我们提供了一条既符合国情、又能与国际接轨的可行路径。这充分证明了零信技术在密码创新上的决心与技术实力。



四、致每一个组织的决策者：行动指南

PQC 对政府和企业意味着什么？这意味着，数据安全战略的规划周期必须拉长到“量子时代”。笔者建议立即思考以下几步：

1. **意识先行**：将 PQC 纳入政府 IT 主管和企业 CTO、CISO 的技术雷达中。这不再是可选的前沿技术，而是必须的优先考量事项。
2. **清单评估**：梳理您的组织中最核心、生命周期最长的数字资产（例如：数据库、长期归档的机密文档）。这些是 PQC 保护的最高优先级。

3. **咨询供应商：**向您的云服务商、软件供应商、安全合作伙伴询问他们的 PQC 迁移路线图。您的供应链安全同样至关重要。
4. **关注整体方案：**积极探索如何将传统密码(RSA/SM2)与后量子密码相结合，打造兼顾合规性与前瞻性的“双保险”安全体系。不仅关注浏览器的 PQC 支持，更需要同时关注服务端的 PQC 迁移解决方案。

五、拥抱变化，方能掌控未来

全球浏览器们的这一步，看似微小，实则宏大。它宣告了一个新时代的序幕已经拉开。在商业世界，我们常常关注眼前的季度报表，但真正的战略家，永远会为那些即将改变游戏规则的“慢变量”留出席位。

后量子密码，正是这样一个“慢变量”。它不会在明天就改变一切，但它将从根本上决定谁能在未来的十年、二十年里，牢牢守住数据价值的核心。现在，正是思考、规划并行动的黄金窗口期。让我们一起，为组织的长远未来，筑起一道坚不可摧的安全防线。

王高华

2025 年 10 月 11 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 232 篇(共 69 万 3 千多字)和英文 99 篇(13 万 4 千多单词)。

