后量子密码迁移比商用密码改造更为紧迫

在确定本文题目时，笔者几经斟酌，最终仍决定采用当前这一可能引发争议的文章标题。恳请读者耐心阅读全文，并深入思考文中所阐述的观点。

过去十年，笔者始终致力于商用密码 HTTPS 加密产品的研发与推广应用，重新创业四年多以来，仅 CEO 博客就已撰写 228 篇，超过 68 万多字。欣喜的是，我国商用密码改造与密评工作正全面推进，并已取得阶段性成果。然而，随着对后量子密码（PQC）研究的不断深入，笔者愈发意识到，后量子密码迁移的实际紧迫性远超当前广泛开展的商用密码改造。遗憾的是，目前整个网络安全与密码产业界似乎尚未形成同等程度的共识。因此，笔者特撰文呼吁我国应高度重视并加速推进后量子密码迁移工作，其优先级甚至应高于传统商用密码改造。最优策略是：将两类密码算法改造同步完成。

一、美国高度重视后量子密码迁移，并已进入实施阶段

美国在国家战略层面已全面布局后量子密码迁移。2022 年 5 月 4 日，拜登总统签署了《关于促进美国在量子计算领域的领导地位，同时降低易受攻击的密码系统风险》的国家安全备忘录，明确要求美国国家标准技术研究院（NIST）牵头 PQC 算法的开发与标准化，国家安全局（NSA）指导国家安全系统（NSS）进行 PQC 迁移，总统管理与预算办公室（OMB）则负责清查关键信息系统中的密码使用情况并制定迁移预算。该备忘录突出强调了密码分析相关量子计算机（CRQC）对传统密码体系的严峻威胁，以及转向抗量子密码的紧迫性。

2024 年 8 月 13 日，NIST 正式发布三项 PQC 标准：FIPS 203（基于模块格的密钥封装机制，ML-KEM）、FIPS 204（基于模块格的数字签名算法，ML-DSA）及 FIPS 205（基于无状态哈希的数字签名算法，SLH-DSA）。NIST 预计，从算法标准化到全面集成至信息系统，仍需 10 至 20 年时间，反映出产业化落地的复杂性。

PQC 技术落地方面进展迅速：2024 年 11 月 12 日，谷歌 Chrome 131 版本正式支持在 TLS 1.3 协议中使用混合后量子密钥交换算法 X25519MLKEM768；2025 年 3 月 17 日，Cloudflare 宣布为所有 CDN 用户免费提供混合 PQC 算法的 HTTPS 加密服务；2025 年 4 月 8 日，OpenSSL 3.5.0 原生支持上述三项 PQC 标准。

政策推进亦未停步：2025 年 6 月 6 日，特朗普总统签署行政令，要求 **2025 年 12 月 1 日**前公布 PQC 产品目录，各联邦政府机构必须尽快启动 PQC 迁移，最晚于 **2030 年 1 月 2 日**前

全面完成。2025 年 8 月，美国政府网站、国务院网站及多项政务服务系统、互联网关键基础设施（如重要互联网服务、网银系统）已陆续启用后量子密码 HTTPS 加密。

可见，美国已在 PQC 领域确立领先地位，政府推动坚决、标准制定领先、科技企业集群实力雄厚，形成了多层次、全体系的快速行动网络，旨在迅速占据后量子密码的战略高地。

二、我国商用密码改造成效显著，为后量子密码迁移奠定基础

我国在量子密钥分发（QKD）领域国际领先，量子科技，包括后量子密码，已被明确列为国家战略重点。当前商用密码改造工作法规体系健全、产业链条完整、应用规模庞大，为 PQC 迁移提供了坚实支撑。

1. 法律法规体系健全，国家高度重视

我国已出台四部国家大法（《密码法》《网络安全法》《数据安全法》《个人信息保护法》）和三部国务院条例（《商用密码管理条例》《关键信息基础设施安全保护条例》《网络数据安全管理条例》），构建起全球罕有的严密制度体系，强制性、系统性远超一般国际实践。

此外，多项部委联合规章进一步细化要求。如 2024 年 7 月 1 日实施的《互联网政务应用安全管理规定》（网信办、中央编办、工信部、公安部联合发布），明确要求政府网站与政务服务系统必须实现商用密码 HTTPS 加密；2025 年 8 月 1 日实施的《关键信息基础设施商用密码使用管理规定》（国密局、网信办、公安部联合发布），则强制要求关基运营者使用商用密码保护核心数据、重要数据与个人信息。

2. 标准与产业链完备，人才储备充足

我国已发布百余项商用密码国家标准与行业标准，覆盖密码算法、产品应用、检测评估，形成完整标准与认证体系。目前全国已有 174 家密评机构，支撑密码改造的合规评估。

产业链方面，我国已实现从密码芯片、密码板卡、密码整机、密码系统、密码网关等的全链条覆盖，服务多类关基保护场景。经过十余年发展，密码改造实施、检测评估与运维人才梯队也已成熟。

尤其值得肯定的是，通过多年来持续的政策宣传与科普教育，关键信息基础设施运营单位的密码合规意识和网络安全防护意识显著提升。越来越多单位认识到密码合规不仅是法律要求，更是保障业务连续性和可持续运营的重要举措，正在主动、积极推进商用密码改造工作。

三、为何后量子密码迁移更为紧迫？

我国自 2018 年推动国产密码全面应用以来，商用密码改造虽进展稳健，但 PQC 迁移已刻不容缓。大国密码自主已成共识，俄乌冲突中 SSL 证书断供事件更凸显了密码算法自主的迫切性。

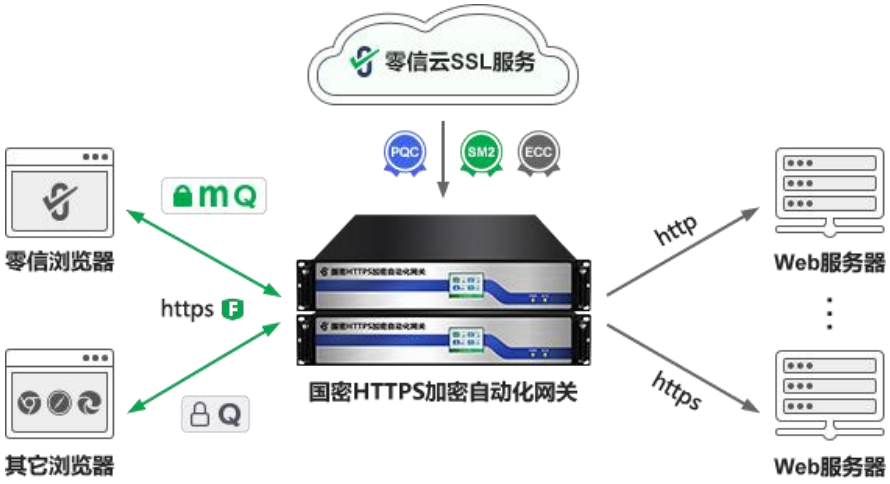
美国 PQC 战略表明，这是一场“输不起的竞赛”。现行加密数据面临“先收集后解密”的量子威胁—今日收集的加密流量，待量子计算机成熟即可被破解。因此，关键信息基础设施系统每延迟一天启用 PQC，就多一天机密数据将来被解密的风险，所有现在已用传统密码算法加密的机密数据将来都会成为明文数据，这可能是灾难性的巨大风险。即便现在已完成全部系统商用密码改造，但传统密码算法（包括 SM2）不仅仅是在量子时代不安全，现在就已经存在数据安全威胁。美国行政令要求 2025 年 12 月 1 日前启动 PQC 迁移，但其政府网站与金融系统已经提前在 2025 年 8 月就已启用 PQC 加密，正是因为“以天为单位”的时间紧迫性。

我国虽尚未发布自主 PQC 算法标准，但产业界不应等待。建议先尽快采用国际成熟 PQC 算法实现 HTTPS 加密，快速提升我国互联网流量安全等级，待自主 PQC 算法标准发布后再平滑替换为国产 PQC 算法。值得明确指出的是，后量子密码算法已被明确为新一代商用密码算法，现有密码法律法规与“三同步一评估”机制（同步规划、建设、运行，加安全性评估）同样适用于后量子密码改造，这将极大加速我国的后量子密码迁移进程。

四、上策：双改造同步实施，一次升级两类算法

既然商用密码改造与后量子密码迁移皆势在必行，且后者更为紧迫，我们应借助当前商密改造之势，将两类算法改造合并实施，遵循“密码敏捷”原则协同推进。

两项密码改造的核心皆在于实现互联网流量安全，即 HTTPS 加密算法改造，而 HTTPS 加密的关键在于 SSL 证书的自动化管理。因 PQC 迁移需要，SSL 证书有效期将缩短至 47 天，没有自动化证书管理机制，两类密码改造将无法顺利完成。



零信技术提出了端云一体化创新方案：一端为零信浏览器，同时支持商用密码与后量子密码算法，并优先采用 PQC 算法；另一端为零信国密 HTTPS 加密自动化网关，部署于 Web 服务器前，自动对接零信云 SSL 服务系统，支持自动化申请和部署双算法证书（SM2/ECC）、实现混合 PQC 算法 HTTPS 加密，使得原 Web 服务器无需改造即可自动化、低成本完成商用密码和后量子密码改造，实现 HTTPS 加密量子安全，保障关基数据在现在与量子时代的持续安全。

王高华

2025 年 9 月 22 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 229 篇(共 68 万 3 千多字)和英文 99 篇(13 万 4 千多单词)。