

2025第十八届中国密码学会年会 (ChinaCrypt 2025)

后量子密码HTTPS加密 研究与实践

王高华 Richard Wang | CTO

零信技术 (深圳) 有限公司

ZoTrus Technology Limited

2025.11.08



研究背景与威胁现状

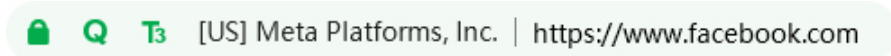
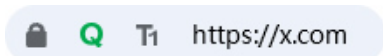
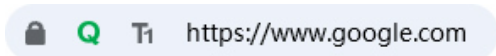
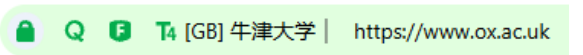
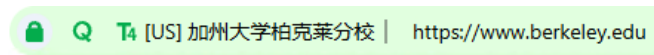
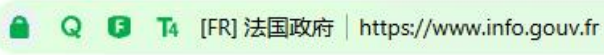
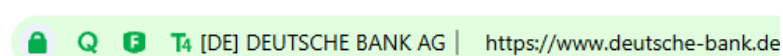
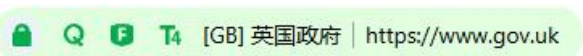
- **重新定义威胁：这不是科幻，是现在的、中长期的、确定的风险。**
 - **核心风险：** Shor算法可破解RSA/ECC/SM2传统密码算法，“**先收集后解密**”，今天已加密的核心机密、客户数据、交易数据等，正在被攻击者收集，等待量子计算机可用时解密。
 - **战略影响：** 直接威胁一个国家的**核心竞争力** 和 **机密信息安全**。
- **研究结论：** 向后量子密码(PQC)迁移不是技术升级，而是关乎未来十年生存与发展的“**战略必需品**”。



PQC应用现状：一场无声的技术革命已经开始

- **核心信息：** 当我们的目光还聚焦于当下业务时，全球互联网的安全基石正在发生**根本性**重塑。
- **震撼事实：**
 - **全球主流浏览器（Chrome, Firefox, Safari, Edge）已全部默认开启后量子密码(PQC)支持。**
 - 全球前8大流量网站（Google、X等）已经启用后量子密码HTTPS加密
 - 8月份开始，美欧政府网站、网银系统、大学官网等都纷纷支持后量子密码HTTPS加密
 - 这标志着**PQC从理论课题迈入规模化部署阶段。**
 - 因为“**先收集后解密**”安全威胁已被攻击者大规模实施，早一天支持PQC就早一天安全。
- **我国差距：** 没有一个互联网流量网站、**没有一个**政府网站、没有一个网银系统支持PQC！

国外后量子密码HTTPS加密应用情况



核心原理：稳健的“混密模式”是成功关键

- 现阶段技术路线：混密模式—传统RSA/ECC/SM2算法+PQC算法
- 技术隐喻：这不是更换发动机，而是为汽车增加第二套冗余动力—“混电”

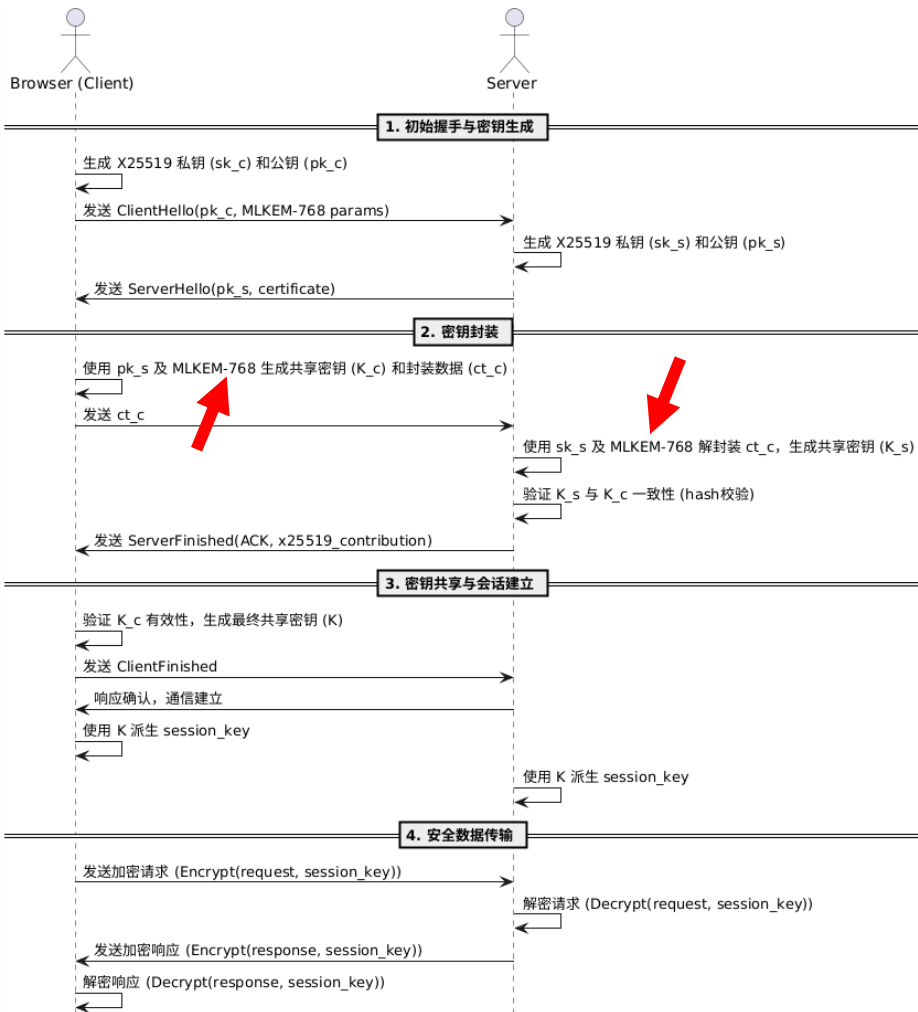


核心原理：稳健的“混密模式”是成功关键

- **现阶段技术路线：混密模式—传统RSA/ECC/SM2算法+PQC算法**
- **技术隐喻：**这不是更换发动机，而是为汽车增加**第二套冗余动力—“混电”**
- **“混密模式”：**
 - **工作原理：**在HTTPS握手时，**并行**使用传统密码算法（ECC）和PQC算法（MLKEM）。
 - **战略智慧：**
 - **风险对冲：**即使PQC算法未来发现漏洞，传统密码算法依然有效。
 - **平稳过渡：**确保与旧系统的兼容性，极大降低迁移风险。
 - **务实路径：**体现了从当前走向未来的稳健策略。
- **商业价值：**该模式降低了采用PQC的技术门槛和不确定性，使快速部署成为可能。

核心原理：混密模式

26	1.403203	192.168.1.32	116.198.201.35	TLSv1.3	1874 Client Hello (SNI=pqc.zotrus.com)
Transmission Control Protocol, Src Port: 50249, Dst Port: 443, Seq: 1, Ack: 1, Len: 1820					
Transport Layer Security					
[Stream index: 4]					
TLSv1.3 Record Layer: Handshake Protocol: Client Hello					
Handshake Protocol: Client Hello					
Handshake Type: Client Hello (1)					
Length: 1811					
Extension: supported_versions (len=7) TLS 1.3, TLS 1.2					
Extension: key_share (len=1263) X25519MLKEM768, x25519					
Type: key_share (51)					
Length: 1263					
Key Share extension					
Client Key Share Length: 1261					
Key Share Entry: Group: Reserved (GREASE), Key Exchange length: 1					
Key Share Entry: Group: X25519MLKEM768, Key Exchange length: 1216					
Group: X25519MLKEM768 (4588)					
Key Exchange Length: 1216					
Key Exchange [...]: b3d489e27b1115f4ab54b5cec0d0c2a4b5bb8d6281cb50cd808589820aa49d197263226bbc05					
Key Share Entry: Group: x25519, Key Exchange length: 32					
Group: x25519 (29)					
Key Exchange Length: 32					
Key Exchange: 466b5b05fb07cb9fe5c2243d81b3b5ef162cb70cb505228c6605d9d2d23c145e					



如何查看网站是否启用后量子密码HTTPS加密？

零信浏览器展示Q标识



谷歌浏览器 开发者工具-隐私与安全 查看PQC算法



全球格局：科技巨头已构建“先行者优势”

- **现状：统一行动，规模化部署。** 四大浏览器巨头步调高度一致，在最新版本中为数亿用户默认开启混合PQC算法HTTPS加密。国际云巨头-亚马逊、Cloudflare提供了服务端的**零改造**方案。
- **深度分析：这不仅仅是技术升级，更是：**
 - **生态主导权的巩固：** 通过定义下一代密码算法标准，强化其平台地位。
 - **数据主权壁垒：** 为其全球用户数据建立面向未来的安全护城河。
 - **产业号召力体现：** 展示了顶尖科技公司协调重大技术变迁的能力。
- **对我国的启示：** 全球技术演进路径已清晰，必须马上采取行动，早一天普及应用PQC HTTPS加密，早一天保障我国互联网数据安全。

本土洞察：机遇窗口与战略抉择

• 客户端格局分析：

- **主流国产浏览器：**处于**战略观望期**。优先级在于国密合规与市场运营，对PQC的跟进滞后。
- **后起之秀--零信浏览器：**处于**战略引领期**。专注于实现“国际+国密+PQC混合”，提供了可行的技术路径。

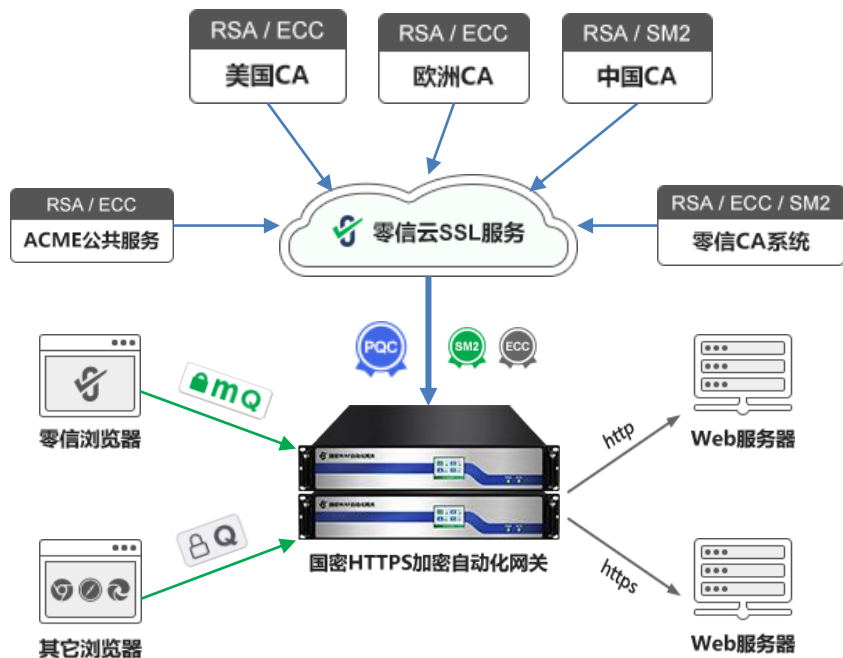
• 服务端格局分析：

- **主流云平台厂商：**处于**战略观望期**。优先级还是市场运营，对PQC的跟进滞后。
- **后起之秀--零信技术：**处于**战略引领期**。专注于实现“国际+国密+PQC混合”，**浏览器+云SSL服务+HTTPS加密自动化网关** 提供了可行的技术路径。

密码敏捷 与 迁移路径

- **密码敏捷原则：**
 - 系统设计支持算法灵活替换
 - 无需重构协议或基础设施
 - 无需硬件替换，仅需自动升级软件
 - SSL证书自动化管理
- **密码敏捷原则，保障(1)密码改造不影响现有业务系统的持续运营；
(2)密码改造须确保现有业务系统的持续安全。**
- **无感PQC迁移路径：**
 - 当前：混合模式（传统密码+后量子密码）
 - 未来：纯后量子密码模式（ML-DSA / ML-KEM /中国PQC算法）

后量子密码HTTPS加密实践--证书自动化、商密改造、PQC迁移

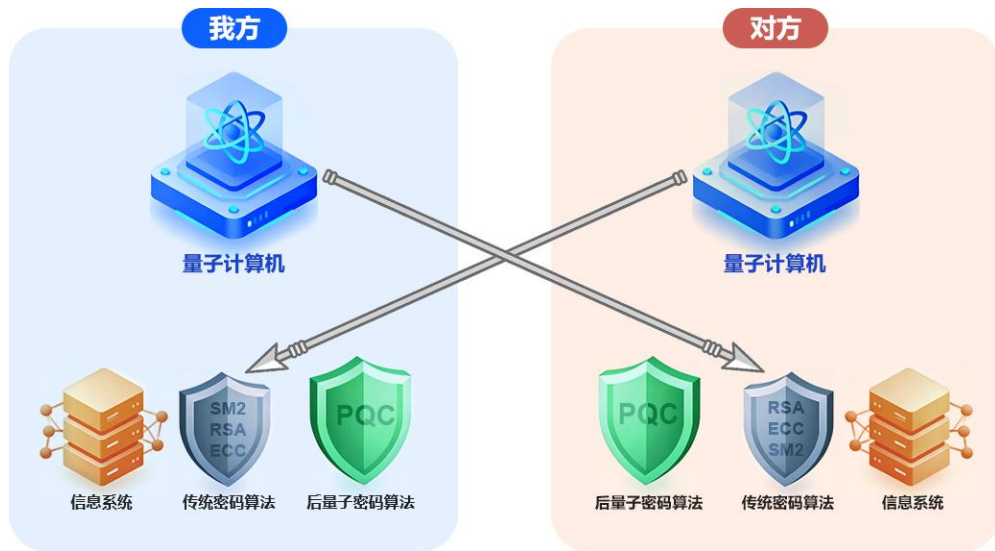


- **SSL证书自动化改造**是实现密码敏捷的基础
- **商用密码改造**和**后量子密码迁移**都需要客户端和服务端支持商用密码算法和后量子密码算法
- **零信浏览器**全球独家同时支持商用密码和后量子密码
- **零信国密HTTPS加密自动化网关**，让服务端零改造，Web服务器不用动！
- 所有网站系统都**自动化**申请和部署SSL证书，**无需**向CA购买和申请SSL证书，**无需**手动安装SSL证书
- **支持**自动切换的多CA签发通道，保证证书可靠供给
- 只需**部署**多台网关，所有网站系统都能**自动化**实现不间断的国密PQC HTTPS加密和WAF防护，保障业务数据安全和用户账户安全
- **支持**多达255个网站系统5年自动化提供HTTPS加密服务，商密合规、全球信任，轻松完成PQC迁移！

用户端-服务端-云端，三端一体，PQC迁移方案首选

- **再次强调：** 国际业界已经行动起来，宣告量子时代的安全竞赛已经开始！
- **整体方案：** 需要浏览器和服务端都支持PQC，核心基础是SSL证书自动化
- **市场教育：** 多多宣传“密码敏捷原则”和“后量子密码HTTPS加密”
- **期待：** 早日出台我国后量子密码算法、等效TLS1.3及相关支持协议
- **呼吁：**
 - 不再观望，立即启动战略评估，行动滞后意味着未来更高的风险和成本。
 - 必须将后量子密码纳入政府和企业核心安全架构的蓝图，构建面向未来的韧性政府和企业。

总结：量子计算机与后量子密码，磨砺利矛与铸牢坚盾



坚持“矛利盾坚”战略思想，同步推进量子计算机(矛)和后量子密码(盾)发展。 加快后量子密码技术的研发和应用，切实筑牢国家网络安全的坚固底座。只有在“盾”的建设上取得实质性突破，我国才能在这场与量子计算赛跑的安全竞赛中赢得主动，切实保障数字时代的国家安全。

迎接后量子密码时代，现在正当时！



预祝2025第十八届中国密码学会年会精彩圆满！