双混合 PQC 算法双端支持，意义重大

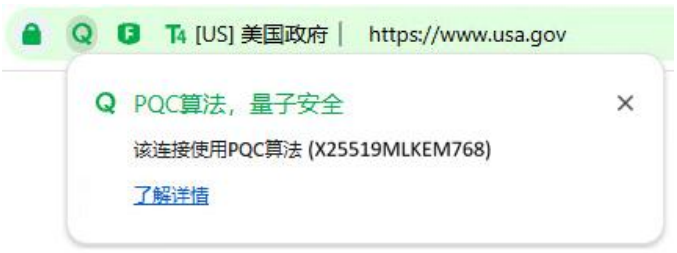
2025 年 12 月 15 日

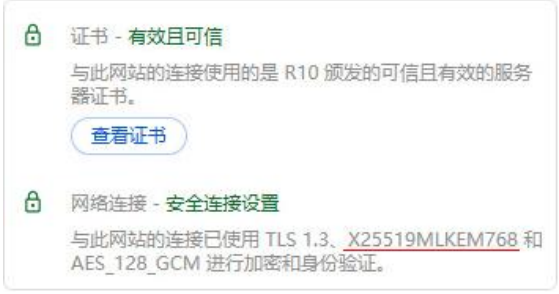
零信浏览器于 12 月 12 日发布了支持商用密码和后量子密码混合算法-SM2MLKEM768 的更新版本-V2601，这事距离 11 月 14 日国际组织 IANA (互联网号码分配机构)正式为 SM2MLKEM768 分配了 TLS 支持组算法编号-4590 不到一个月时间，零信技术就实现了全线产品支持。而这事距离 10 月 11 日零信浏览器发布支持 ECC 算法和后量子密码混合算法-X25519MLKEM768 也就两个月时间，零信浏览器和零信 HTTPS 加密自动化网关就实现了双产品双支持双国际标准后量子密码混合算法：X25519MLKEM768 和 SM2MLKEM768，这充分展现了零信技术非凡的尖端密码产品研发实力，这是我国量子科技的国之大器产品。本文好好讲讲这件大事。

一、 PQC 迁移国际方案是普及应用 X25519MLKEM768 混合算法

根据 Cloudflare 雷达发布的统计数据，截止到今天，全球互联网流量中已有 51%流量实现了后量子密码 HTTPS 加密，证明全球业界正在快速应用混合 PQC 算法解决已经存在的“先收集后解密”安全威胁，确保了这些流量数据在现在和量子时代的持续安全。这个快速应用方案采用的技术是基于传统 ECC/RSA 算法 SSL 证书实现密钥封装混合算法 X25519MLKEM768，这是传统密码算法 X25519 和后量子密码算法 MLKEM768 的混合算法，X25519 确保当前兼容和速度，MLKEM768 则是抵抗量子攻击。

用户可以通过浏览器的开发者工具查看正在访问的网站是否已经支持 X25519MLKEM768，当然也可以直接使用零信浏览器查看地址栏是否显示 Q 标识，点击“Q”标识，会提示“PQC 算法，量子安全”，并且会显示 PQC 混合算法为 X25519MLKEM768。





这个混合算法 PQC 技术落地方面进展非常迅速：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码算法 X25519MLKEM768，微软 Edge 浏览器、苹果 Safari 浏览器和火狐浏览器都陆续支持。2025 年 3 月 17 日，Cloudflare 宣布为所有 CDN 用户免费升级支持混合 PQC 算法；2025 年 4 月 8 日，OpenSSL 3.5.0 原生支持三项 PQC 算法标准。2025 年 8 月开始，美国政府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）已陆续使用 X25519MLKEM768 启用后量子密码 HTTPS 加密。欧洲国家也纷纷启用，G20 国家中已有 7 个国家门户网站启用，包括：美国、英国、法国、日本、澳大利亚、沙特阿拉伯、阿根廷，欧美著名大学如牛津、剑桥、伯克利等也已启用。

二、 现阶段 PQC 迁移中国方案是普及应用 SM2MLKEM768 混合算法

我国在后量子密码 HTTPS 加密这块起步较晚，目前没有一个政府网站和政务系统启用了 PQC 混合算法 HTTPS 加密，没有一个银行网站和网银系统启用，只有几个高校官网如清华已启用国际方案 X25519MLKEM768。这也许与我国还没有自己的后量子密码算法有关，也与后量子密码迁移的重要性宣传不够有关，这就是笔者已经连续发布了十几篇后量子密码 HTTPS 加密相关文章的主要原因。

其实，我国密码业界早就行动起来了，不仅密码学会已经召开过多次后量子密码相关的学术会议，最关键的是产业界已经拿出了实际行动，主要有四件大事：

(1) 铜锁密码开源社区早在 2025 年 1 月起草了《用于 TLS 1.3 的混合后量子密钥交换协议 SM2-ML-KEM》的 RFC 草案，并 2025 年 7 月实现铜锁 SSL 开源项目支持 SM2MLKEM768 混合后量子密码算法，这是里程碑的工作。

(2) 零信浏览器从 2025 年 4 月开始开发支持后量子密码混合算法，于 2025 年 10 月发布了 137 版本，全球率先实现同时支持商用密码 SM2 算法和后量子密码混合算法 X25519MLKEM768，并创新地在地址栏加密锁标识后增加显示后量子密码标识“Q”，让用户一眼就能知道网站是否支持后量子密码。

(3) 零信浏览器于 2025 年 10 月联合铜锁密码开源社区向国际组织 IANA (互联网号码分配机构)申请为 SM2MLKEM768 算法分配了 TLS 支持组编号，此申请于 2025 年 11 月 14 日正式批准获得编号-4590，标志着我国密码研究团队推出的商用密码算法和后量子密码算法混合协议获得了权威的国际标准组织认可，正式成为国际标准 TLS 协议组的四个后量子密码混合协议之一。

(4) 2025 年 12 月 12 日，零信浏览器和零信 HTTPS 加密自动化网关全球独家率先正式发

布升级版本支持 SM2MLKEM768 算法实现后量子密码 HTTPS 加密。

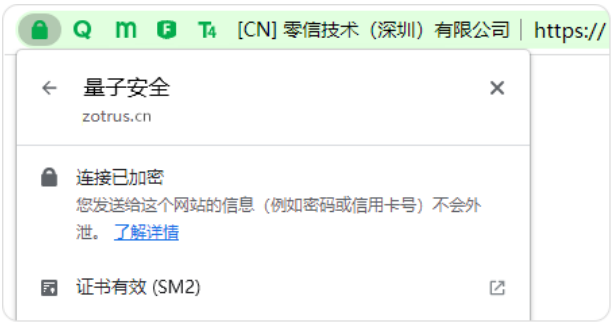
至此，我国就真正有了可落地应用的、同时支持实现商用密码 SM2 算法和后量子密码算法 MLKEM768 的完整产品线，可用于我国关键信息基础设施系统急需的商密 HTTPS 加密改造和后量子密码迁移。这是我国现阶段 PQC 迁移 HTTPS 加密的最佳方案，待后续国产后量子密码算法正式发布后只需升级算法就可以实现最终 PQC 迁移方案-SM2 算法和国产后量子密码算法混合算法。

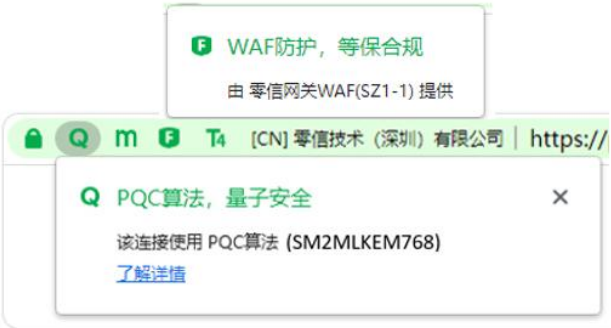
三、 零信技术全球率先同时支持两个国际标准 PQC 混合算法

零信技术本次发布的两个产品更新是：零信浏览器在已经支持 X25519MLKEM768 的基础上升级支持 SM2MLKEM768，零信 HTTPS 加密自动化网关也同步升级支持，这是全球唯一同时支持 IANA 批准的四个后量子密码混合算法之两个算法的产品和厂商。

Value	Description
4587	SecP256r1MLKEM768
4588	X25519MLKEM768
4589	SecP384r1MLKEM1024
4590	curveSM2MLKEM768

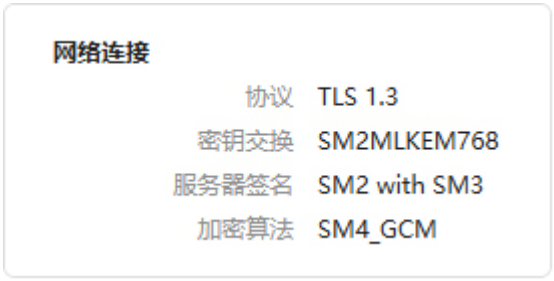
用户使用零信浏览器访问零信技术官网，点击加密锁标识，会显示 SSL 证书是 SM2 算法的国密 SSL 证书，提示“量子安全”，如下左图所示。点击后量子密码“Q”标识，会显示“PQC 算法，量子安全”，同时显示“该连接使用 PQC 算法(SM2MLKEM768)”，如下右图所示。

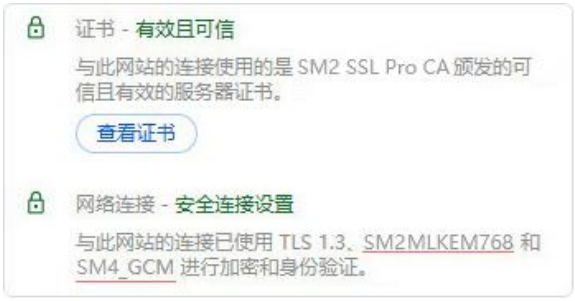




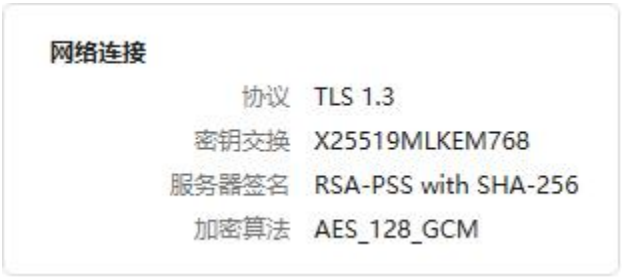
用户还可以使用零信浏览器的开发者工具查看 SSL 证书信息和网络连接信息，如下左图所示，网络安全连接采用了 TLS 1.3 协议、密钥交换采用了 SM2MLKEM768 算法、服务器签名(SSL 证书)采用了 SM2 和 SM3 算法，加密算法采用了 SM4_GCM，HTTPS 加密所需的三种算法都是商用密码算法。如下右图所示，SSL 证书是贵州 CA 根签发的国密 SSL 证书。这是

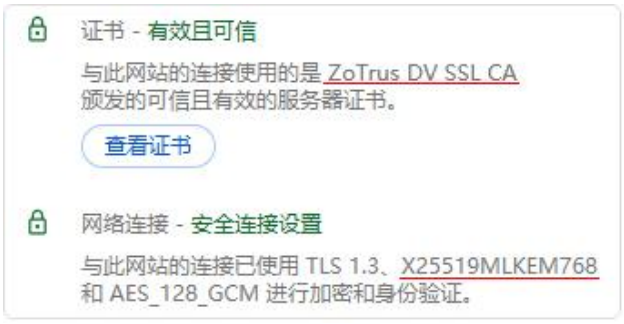
HTTPS 加密全栈实现了商用密码算法和后量子密码算法。如上右图所示，点击 WAF 防护标识“F”，则会显示“由 零信网关 WAF( )提供” WAF 防护服务，这也能证明正是零信网关同零信浏览器的密切配合才无缝实现了部署的是传统密码 SM2 算法的国密 SSL 证书但实现了 SM2 算法和后量子密码算法 MLKEM768 的混合算法密钥交换，这是一箭双雕同时完成了商密改造和后量子密码迁移。





如果用户使用谷歌浏览器访问零信官网，则使用了 RSA/ECC 算法 SSL 证书实现 HTTPS 加密，如左下图所示的服务器签名算法(SSL 证书算法)。使用开发者工具查看就能看到网络连接采用了 TLS 1.3 协议、X25519MLKEM768 密钥交换和 AES_128_GCM 加密，如下右图所示。这充分证明了零信 HTTPS 加密自动化网关是同时支持 IANA 分配编号为 4588 和 4590 的两个后量子密码混合算法-X25519MLKEM768 和 SM2MLKEM768。





当然，用户也可以使用零信浏览器访问其他支持 X25519MLKEM768 算法的网站验证零信浏览器也是一样同时支持 X25519MLKEM768 和 SM2MLKEM768 两个国际标准后量子密码混合算法。零信浏览器优先采用 SM2MLKEM768 算法，如果网站仅支持 X25519MLKEM768，则零信浏览器采用 X25519MLKEM768 算法实现 HTTPS 加密。如下图所示，通过抓包软件可以看出，零信浏览器同时支持常用的传统密码算法(X25519, SM2)和两个后量子密码混合算法(X25519MLKEM768, SM2MLKEM768)。

```
▾ Extension: key_share (len=2755) X25519MLKEM768, SM2MLKEM768, curveSM2, x25519,
    Type: key_share (51)
    Length: 2755
  ▾ Key Share Entry: Group: X25519MLKEM768, Key Exchange length: 1216
      Group: X25519MLKEM768 (4588)
      Key Exchange Length: 1216
      Key Exchange […]: 8034c87eab36a6431f58f63c254756abc8802a26c0187a4c4bd0
  ▾ Key Share Entry: Group: SM2MLKEM768, Key Exchange length: 1249
      Group: SM2MLKEM768 (4590)
      Key Exchange Length: 1249
      Key Exchange […]: 043e4eceb1efe7a53676a620f3a746e66d209370508ba3576615
  ▾ Key Share Entry: Group: curveSM2, Key Exchange length: 65
      Group: curveSM2 (41)
      Key Exchange Length: 65
      Key Exchange: 04c2d90e25a640ed496f2e412c854eaff60a18837563ba196a4115d6
  ▾ Key Share Entry: Group: x25519, Key Exchange length: 32
      Group: x25519 (29)
      Key Exchange Length: 32
      Key Exchange: 45579ee5f74014f7d187c97ab6d43f5d82ba602f4b091e0b595a12c5
```

四、 后量子密码混合算法中国方案不仅是中国的，也是世界的

上面较为详细地讲了后量子密码迁移国际方案和现阶段的中国方案，这样分开讲就是为了方便讲解，由于 SM2MLKEM768 已经是 IANA 列出的 4 个可选方案之一，所以，实际上这两个解决方案都是全球用户可以选用方案，只是 X25519MLKEM768 方案是最早提出的方案，并且已经得到了常用浏览器的支持，也得到了 OpenSSL 等开源密码组件的支持，使得云服务厂商如 Cloudflare、亚马逊等也就可以为用户提供支持了，这才形成了全球 51%的 HTTPS 加密流量都已经采用了 X25519MLKEM768 算法实现了抗量子保护，虽然这个算法目前还是 RFC 草案阶段。

X25519MLKEM768 算法 RFC 草案是 2024 年 8 月提出的，2025 年 3 月正式成为 TLS 工作组的草案，预期 RFC 标准状态是拟议标准(Proposed Standard)。SM2MLKEM768 算法目前还没有正式成为 TLS 工作组的草案，而推动这个标准进程的唯一力量是 SM2MLKEM768 算法也能像 X25519MLKEM768 算法一样大量部署使用，这个力量就一定首先来自我国国产浏览器、网络安全企业、密码企业和互联网巨头们的广泛部署和使用。零信技术本次发布的两个核心产品升级就一个证明：SM2MLKEM768 算法是可行的，浏览器是可以支持的，SSL 网关也是可以支持的。笔者在此再次感谢铜锁 SSL 开源社区为此做出的开源贡献。

正如我们向 IANA 申请 SM2MLKEM768 算法的 TLS 支持组编号时所讲的，全球互联网 TLS 生态需要多种算法提供更好的韧性和更多的选项，因为谁也无法保证传统的密码算法和后量子密码算法在未来的量子计算机面前是安全的，多一个选择就多了一份安全保障，这个观点也已经得到了零信技术香港合作伙伴的支持，虽然 SM2 算法在香港不是强制项。

为了全球互联网在未来更加安全，呼吁全球业界，特别是我国网安业界和密码业界，一起

行动起来，在支持后量子密码混合算法 X25519MLKEM768 的同时也积极支持 SM2MLKEM768 算法，为全球互联网流量安全提供更好的韧性和安全性，因为全球只有一个互联网，一起共筑全球互联网安全命运共同体。

王高华

2025 年 12 月 15 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 244 篇(共 72 万 3 千多字)和英文 105 篇(14 万 2 千多单词)。