美英法政府门户网站已启用后量子密码 HTTPS 加密

笔者最近正在内测零信浏览器 137 版本支持后量子密码 HTTPS 加密，发现美国政府官网上周还不支持后量子密码 HTTPS 加密，本周就已经支持了，同时发现英国政府和法国政府门户网站也已经支持后量子密码了，可见后量子密码 HTTPS 加密来势很猛。本文讲一讲为何不仅仅是走在技术前沿的美国互联网巨头都纷纷启用后量子密码 HTTPS 加密和提供后量子密码 HTTPS 加密服务，而且欧美政府网站也纷纷启用。我国政府网站和政务服务系统怎么办？本文有创新思路。

一、 美英法政府门户网站纷纷启用后量子密码 HTTPS 加密

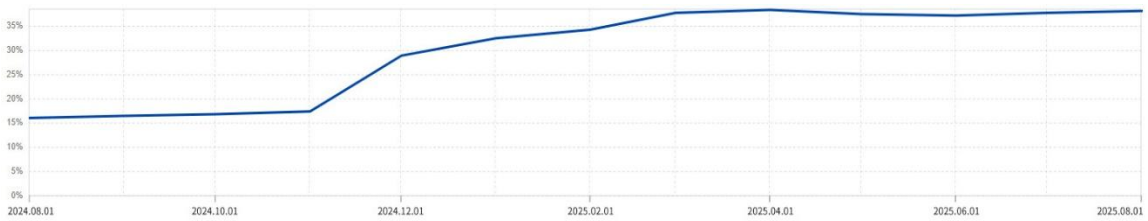
眼见为实，如果网站采用了后量子密码算法实现 HTTPS 加密，零信浏览器 137 版本在原先显示商密标识 **m** 的位置显示后量子密码标识 **Q**，如下图所示，点击 **Q** 标识，则提示“PQC 算法，量子安全”。

也许马上有读者会问：如何能让我相信零信浏览器这个 **Q** 标识是正确的呢？如何验证这个网站的确是采用了后量子密码算法实现了 HTTPS 加密呢？很好的问题！如下图所示，点击“开发者工具”-“隐私与安全”查看网站的“安全性概览”，在“网络连接”部分显示“与此网站的连接已使用 TLS 1.3、X25519MLKEM768 和 AES_128_GCM 进行加密和身份验证”，这就能证明零信浏览器正在使用后量子密码混合封装协议(X25519MLKEM768)实现后量子密码 HTTPS 加密。当然，大家也可以使用谷歌浏览器和微软 Edge 浏览器验证，而零信浏览器所做的创新是让后量子密码 HTTPS 加密可视化—在地址栏展示 **Q** 标识。

再看看英国政府和法国政府门户网站，零信浏览器一样会显示 Q 标识，当然大家还是可以用开发者工具查看和验证。

二、 全球互联网流量中已有 38%流量采用后量子密码加密

根据 Cloudflare 发布的统计数据，最近一年来的全球互联网流量中采用混合后量子密码密钥封装协议实现 HTTPS 加密的流量已经从去年的 8 月 1 日的 16%增长到今年 8 月 1 日的 38%，翻了一倍多，如下图所示。2024 年 11 月份之后的后量子密码加密流量的快速增长得益于谷歌浏览器 131 版本正式支持混合后量子密钥交换算法 X25519MLKEM768，随后微软 Edge 浏览器、火狐浏览器也相继支持后量子密码 HTTPS 加密。



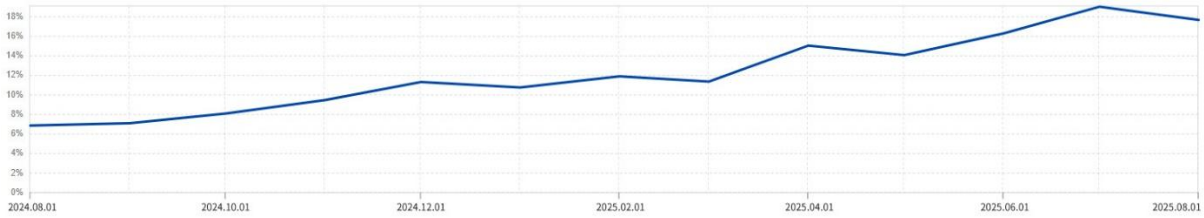
这么大比例的后量子密码 HTTPS 加密流量，当然不仅仅来自上面所说的美英法政府官网，全球前十大流量网站中前 8 个网站包括谷歌、油管、Facebook、Instagram、OpenAI、X.com 等都已经实现了后量子密码 HTTPS 加密，这就是 38%后量子密码加密流量的来源。

还有，Cloudflare 已经免费为其所有 CDN 用户升级支持后量子密码 HTTPS 加密，而不仅仅是其官网支持。作为学术研究前沿的美英高校官网如伯克利、牛津、剑桥等也都实现了后量

子密码 HTTPS 加密，著名的支付公司 Visa 官网也实现了后量子密码 HTTPS 加密。

三、 我国政府网站没有一个支持后量子密码 HTTPS 加密

笔者同时对比查询了中国大陆地区的数据，去年 8 月 1 日为 7%，今年 8 月 1 日为 18%，不到全球数据的一半，导致这个低的原因当然是在国内大量使用的国产浏览器、主流云服务商、CDN 服务商目前都不支持后量子密码 HTTPS 加密。而这 18%的流量来自中国用户使用支持后量子密码 HTTPS 加密的浏览器访问国外的大流量网站。



到目前为止，笔者没有发现一个政府网站支持后量子密码 HTTPS 加密，也没有发现我国的互联网巨头们的官网采用了后量子密码 HTTPS 加密，也没有发现我国高校官网实现了后量子密码 HTTPS 加密，更没有发现最需要实现后量子密码 HTTPS 加密的网银系统支持后量子密码 HTTPS 加密！这就是差距，值得反思！

也许读者又要提问了：为何网站必须启用后量子密码 HTTPS 加密呢？为何不启用就是差距呢？这又是一个好问题！因为最新的互联网安全威胁是“先收集后解密”，全球互联网流量已经有 83%的流量实现了 HTTPS 加密，这些流量在现在就是安全流量。所以，攻击者现在就开始收集这些加密流量，等将来量子计算机可用时就可以解密这些加密数据，这个时间点估计是 2030 年，不到 5 年时间了！所以，美国政府要求所有政府网站系统现在就要启用后量子密码 HTTPS 加密，以防止“先收集后解密”攻击。

简单讲就是：如果现在不启用后量子密码 HTTPS 加密，那现在的所有系统的登录口令、网银交易数据、移动支付数据等所有已加密的机密信息在量子时代就会被解密为明文，则将是一个巨大的信息安全灾难！所以，必须马上启用后量子密码 HTTPS 加密，以确保已加密的机密数据在量子时代的持续安全。这就是为何欧美政府网站、高校网站、网银系统等纷纷启用后量子密码 HTTPS 加密的根本原因，早一天启用就早一天保护了机密数据在将来的安全！

但是，由于纯后量子密码 HTTPS 加密的实现需要整个生态的所有元素都支持后量子密码算法，这需要时间和实验验证。所以，目前各大网站已经实现的后量子密码 HTTPS 加密采用的技术路线是基于现有密码算法混合后量子密码算法实现，用户网站不用更换 SSL 证书，只

需升级 Web 服务器和浏览器支持后量子密码混合协议即可，这是最小的升级改造。

四、 我国政府网站面临商用密码改造和后量子密码迁移双重技改压力

美国政府网站早在 2016 年就已经完成所有网站系统的 HTTPS 加密工作，并且已于 2023 年实现了 SSL 证书自动化管理。所以，现在实现后量子密码混合协议 HTTPS 加密的技术难度很小，只需简单升级 Web 服务器软件即可，这就是为何现在能快速实现后量子密码 HTTPS 加密的根本原因。

而我国政府网站系统则面临两次密码算法技术改造的双重压力，一次是正在如火如荼进行中的商用密码改造，这就要求从 RSA 算法 HTTPS 加密改造支持商密 SM2 算法 HTTPS 加密。而 SM2 算法同属于椭圆曲线算法，在量子计算面前一样是不安全的，所以，另一次技术改造就是要后量子密码改造，以保障政务数据在量子时代的安全，这就要求 HTTPS 加密支持后量子密码。两次都是密码算法支持改造，最理想和最经济的方案是一次技术改造搞定两次密码算法迁移工作，这应该成为所有单位密改和密评的工作重点和最低要求，用户应该优先选择可以一次完成的密改方案，技术前提是同时支持双算法 SSL 证书自动化管理。

零信技术拥有客户端浏览器、服务端网关、云端 PKI 系统三个必须的商用密码和后量子密码支持的全生态产品，使得原 Web 服务器零改造，只需在 Web 服务器前增加部署零信国密 HTTPS 加密自动化网关，使用完全免费的支持商用密码算法和后量子密码算法的零信浏览器，即可同时完成商用密码和后量子密码双改造工作，这是目前国内唯一一个最完美的、最省钱的、最省事的解决方案，开创双密码算法迁移新思路和新路线。

五、 后量子密码是下一个网络安全产业制高点

全球网络安全产业的基座是密码体系，RSA 密码体系保障了全球互联网的网络通信安全、数据传输安全、软件系统安全、文档安全和用户身份安全。但是，这个体系中赖以保障安全的密码算法在量子时代还没有到来之前就已经无法保障数据安全了，只有后量子密码才能保障量子时代的数据安全，所以，全球网络安全产业参与者就已经开始抢占这个新的制高点。

大家应该能从上面的后量子密码 HTTPS 加密应用情况可以看出：目前美国已经处于绝对领先地位，不仅率先制定了后量子密码算法标准，发布了总统行政令要求联邦政府机构加快向后量子密码迁移。最重要的是已经真正开始落地应用，实现了政府网站、高校网站、银行网站、CDN 服务等支持后量子密码 HTTPS 加密，这非常值得我国政府决策部门、网络安全产业界和密码产业界学习借鉴和深思。

笔者非常高兴地看到上周二(8 月 26 日)国务院发布的《关于深入实施“人工智能+”行动的意见》指出了“加强人工智能与**量子科技**等领域技术的协同创新”。后量子密码是量子科技的最重要组成部分之一，是目前唯一确定的能有效保障数据在现在和量子时代安全的密码技术，需要像后量子密码混合协议 HTTPS 加密应用一样得到全面的创新应用，从而带动量子科技的创新突破；需要有我国自己的后量子密码算法标准，更需要政府网站系统带头实现商用密码和后量子密码 HTTPS 加密应用，切实保障政务数据的现在和将来的始终安全。

王高华

2025 年 9 月 1 日于深圳
