零信浏览器让后量子密码看得见

2025 年 12 月 16 日更新

全球互联网数据正在面临一个新的安全威胁-“先收集后解密”，攻击者正在全球范围收集 HTTPS 加密数据，以备将来量子计算机可用时解密这些加密数据。轻松应对此安全威胁的唯一可靠方法就是网站系统马上支持后量子密码(PQC) HTTPS 加密，这样才能确保机密数据在现在和量子时代的始终安全。

为了让用户能直观感知正在访问的网站是否支持后量子密码 HTTPS 加密，零信浏览器本次发布的升级版本(137 版本)不仅支持后量子密码 HTTPS 加密，而且在原有的展示网站已经实现了商用密码 HTTPS 加密标识(m)的基础上增加了一个新的后量子密码 HTTPS 加密标识(Q)，让用户可以非常直观地了解正在访问的网站是否采用了后量子密码 HTTPS 加密，是否能保护机密数据的长期安全，这是全球独家创新。本文讲一讲零信浏览器 137 版本增加的这个全球独家匠心设计。

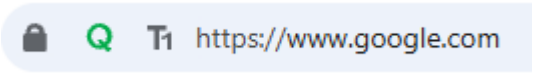
一、 眼见为实，Q 标识独家匠心设计

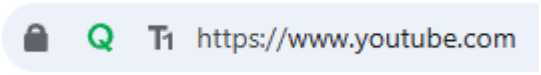
为了防止“先收集后解密”安全威胁，后量子密码 HTTPS 已经成为网站安全的必须。根据 Cloudflare 统计数据，全球互联网流量中，已经有 51%的流量采用了后量子密码加密，全球十大流量网站中前 8 大都支持 PQC HTTPS 加密，Cloudflare 正在为其保护的网站全面实现 PQC HTTPS 加密，美英法政府网站、美欧银行网站、大学官网都已经纷纷启用 PQC HTTPS 加密。但是，目前所有介绍如何查看网站是否支持后量子密码的文章都是要求用户使用非常复杂的开发者工具去查看，这对于普通网民来讲有一定的技术门槛，如何让所有互联网用户一眼就能知道网站是否支持后量子密码加密，这是一个普及后量子密码 HTTPS 加密的一个迫切工作。

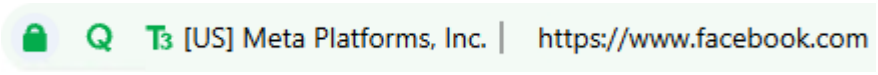
凡是使用过零信浏览器的用户都已经熟悉了地址栏的 **m** 标识，这个设计得到了国内密码界专业人士的高度评价，密评专业人士都说已经离不了这个善器了，即刻知道待检查的网站是否部署了商密 SSL 证书，是否采用商密 SM2 算法实现 HTTPS 加密，是否商密合规和密保合规，真的很好用！

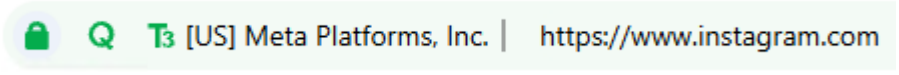
沿着这个思路，本次零信浏览器发布的 137 版本不仅支持后量子密码 HTTPS 加密，而且在原 **m** 标识位置又增加了一个 **Q** 标识，代表 HTTPS 加密采用的是后量子密码算法。用户可以放心地访问此网站，因为此网站的数据传输安全保护采用了后量子密码技术，确保了用户数据不仅现在安全，而且在量子时代也是安全的。如果网站支持 PQC 算法 HTTPS 加密，零信浏览器地址栏的加密锁标识后就会显示 **Q** 标识，用户点击 **Q** 标识，提示“PQC 算法，量子安全”和“该连接使用 PQC 算法”。

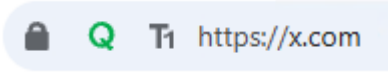
全球 10 大流量网站中，只有两个网站不支持后量子密码加密，大家可以使用零信浏览器访问一下这些网站，看看地址栏是否会显示 **Q** 标识。请注意，零信浏览器会同时展示网站可信身份标识(T1/**T2**/**T3**/**T4**)和 WAF 防护标识(**F**)，以帮助用户了解更多网站安全防护措施。

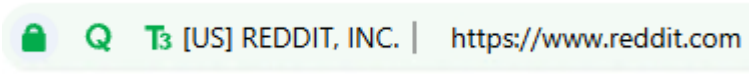




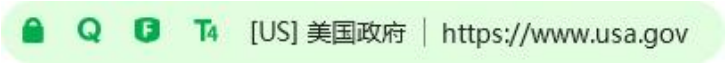


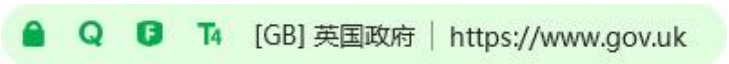


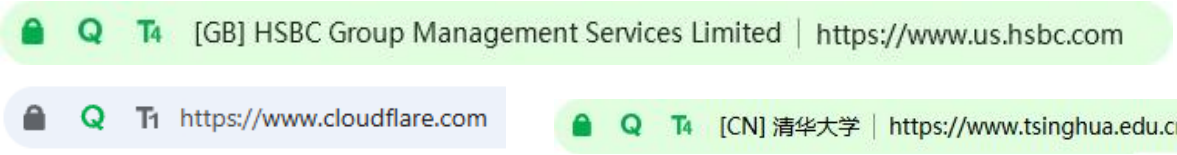




当然，还有很多网站都已经实现了后量子密码 HTTPS 加密，笔者在此再展示 5 个，更多网站需要你自己使用零信浏览器去发现。

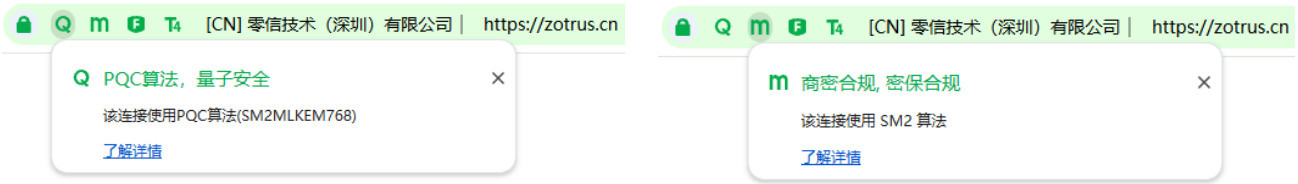




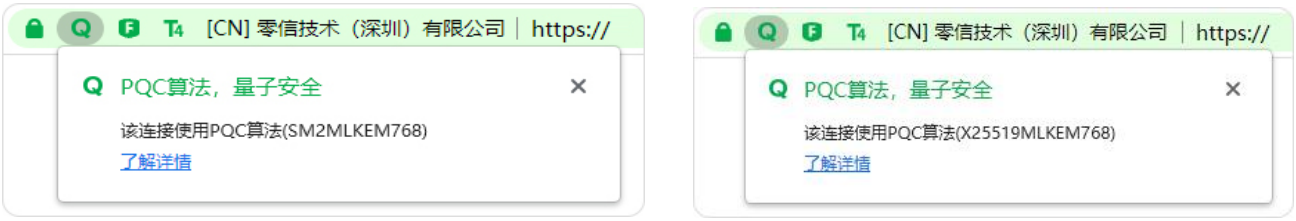


二、 零信浏览器优先采用 TLS1.3 协议支持双混合 PQC 算法

零信浏览器从 V2601 版本开始，全球率先支持已获 IANA 分配 TLS 支持组混合 PQC 算法编号-4590 的商密 SM2 算法和后量子密码算法 MLKEM768 的混合 PQC 算法-SM2MLKEM768，零信 HTTPS 加密自动化网关也同步支持，这样用户使用零信浏览器访问零信官网就会在地址栏加密锁标识后面同时显示“Q”标识和“m”标识，表示此网站已经完成后量子密码迁移和商密合规改造，这是我国商密合规和后量子密码迁移的最佳解决方案。



如果网站仅支持 SM2MLKEM768 算法实现密钥交换，则零信浏览器仅显示“Q”标识，而不会显示“m”标识，仅网站同时支持 SM2MLKEM768 算法密钥交换、SM2 算法服务器签名和 SM4 算法加密，零信浏览器才会同时显示“Q”标识和“m”标识。当然，如果网站支持 X25519MLKEM768 算法实现密钥交换，则零信浏览器一样会显示“Q”标识。



三、共同努力，让 Q 标识普及可见

目前全球都在大力推广后量子密码混合协议 HTTPS 加密应用，这是防止“先收集后解密”的数据安全威胁唯一有效技术手段，而实现后量子密码 HTTPS 加密当然离不开浏览器的支持。但是，这个高大上的加密技术对普通用户来讲是不可见的，用户根本对此无感，这不利于后量子密码技术的普及应用推广。

零信浏览器全球独家率先实现在地址栏显示后量子密码 Q 标识，让网站访问者非常容易地了解正在访问的网站是否支持后量子密码，了解网站是否能切实保护用户数据在量子时代的

持续安全，这对于普及后量子密码应用非常重要，欢迎全球用户一起努力推动这个创新 UI 在所有浏览器的普及采用，只有这样才能真正推动后量子密码的快速普及应用，才能真正保障全球互联网数据的持续安全。

让我们共同努力，普及使用支持后量子密码算法和后量子密码 Q 标识的零信浏览器，共同推动后量子密码的普及应用，切实保障全球互联网数据安全，让 Q 标识一直停留在浏览器地址栏上。

王高华

2025 年 10 月 11 日于深圳
2025 年 12 月 16 日更新

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 233 篇(共 69 万 4 千多字)和英文 100 篇(13 万 6 千多单词)。