零信浏览器让后量子密码看得见

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

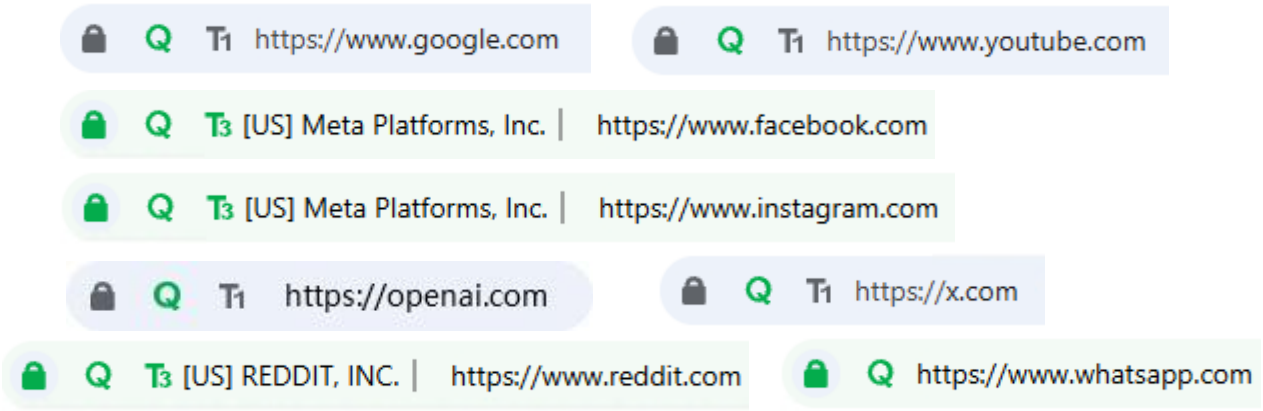
为了防止“先收集后解密”安全威胁，后量子密码 HTTPS 已经成为网站安全的必须。根据 Cloudflare 统计数据，全球互联网流量中，已经有 38%的流量采用了后量子密码加密，全球十大流量网站中前 8 大都支持 PQC HTTPS 加密，Cloudflare 正在为其保护的网站全面实现 PQC HTTPS 加密，美英法政府网站、美欧银行网站、大学官网都已经纷纷启用 PQC HTTPS 加密。但是，目前所有介绍如何查看网站是否支持后量子密码的文章都是要求用户使用非常复杂的开发者工具去查看，这对于普通网民来讲有一定的技术门槛，如何让所有互联网用户一眼就能知道网站是否支持后量子密码加密，这是一个普及后量子密码 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！

(C) 2025 零信技术（深圳）有限公司

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 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。

(C) 2025 零信技术（深圳）有限公司

二、 再增加 RSA/ECC 算法标识(R/E)，了解网站是否量子安全

沿着这个思路，零信浏览器 137 版本继续增加了两个密码算法标识-R/E，分别代表网站部署的是 RSA 算法或 ECC 算法 SSL 证书，因为 ECC 算法密钥更短(256 位)，加密算法更快，所以已经成为混合后量子密码 HTTPS 加密的默认配置，而 RSA 算法 SSL 证书(2048 位)不仅密钥长而且存在某些安全问题，所以，现在主流网站 TLS 堆栈已经弃用 RSA 算法。这就也有必要告诉网站访问者网站部署的是何种算法的 SSL 证书，并且告诉用户这些算法是“不支持量子安全”的，告诉网站运营者必须尽快支持后量子密码。

根据这个设计理念，如果网站部署的是 ECC 算法 SSL 证书，如下图所示，显示 E 标识，点击 E 标识，显示“ECC 算法，全球信任”。点击加密锁标识-连接已加密(ECC)，则会显示“不支持量子安全”。这个设计改变了 Chromium 默认的显示为“安全”，意在突出网站须迁移到后量子密码的紧迫性和必要性。

如果网站部署的 SSL 证书是 RSA 算法 SSL 证书，如下图所示，显示 R 标识，点击标识，显示“RSA 算法，全球信任”。点击加密锁标识-连接已加密(RSA)，则会显示“不支持量子安全”。

对于已经支持后量子密码的网站，点击加密锁标识-连接已加密，则会显示“量子安全”，无论网站部署的是 ECC/RSA/SM2 算法 SSL 证书，SSL 证书算法显示在“连接已加密”后面。

(C) 2025 零信技术（深圳）有限公司

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

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)。

(C) 2025 零信技术（深圳）有限公司