神秘密码是时候进入大众视野了

2025 年 11 月 3 日

本文所指的“密码”是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务，不是大家平时所讲的“银行卡密码”的“密码”，这个“银行卡密码”的正确叫法应该叫“银行卡口令”。密码非常重要，因为大家日常上网每一秒都是密码在保护数据安全和网络安全，但又很神秘，看不见摸不着。零信浏览器全球独家创新在地址栏展示用户正在访问网站时所采用的密码算法标识，把高深莫测的神秘技术带进了大众视野，这对于现在全球范围如火如荼进行中的从传统密码算法迁移到抗量子密码算法的技术革命科普非常重要，零信浏览器的“可视化”就是搭建了技术精英与公众认知的桥梁，只有公众了解和支持才能真正在全球范围快速完成后量子密码(PQC)迁移。

一、 为何神秘的密码现在需要现身大众视野？

密码技术自诞生以来，一直是互联网安全的隐形守护者。从早期的 DES 算法到如今的 AES、RSA、ECC 和 SM2，使得“银行卡口令”通过复杂的数学变换，确保了机密数据在传输和存储过程中不被非法窃取或篡改。然而，这种神秘性也带来了双刃剑：用户享受着安全的上网体验，却对背后的算法一无所知。这在当下量子计算浪潮来临之际，显得尤为危险，因为谁也不能保证这些密码算法是否真能抗住未来量子计算机的攻击。

量子计算机的崛起，将彻底颠覆传统密码体系。经典的 RSA/ECC/SM2 算法依赖于大数因子分解或离散对数问题的计算难度，但量子算法如 Shor's 算法能在多项式时间内破解它们。所以，攻击者无需现在就能立即解密，只需“先收集后解密”—今天加密的数据，明天在量子时代即可被轻易破解。所以，全球顶尖密码专家和顶尖科技巨头已经快速行动起来，采用了后量子密码算法基于现有的 SSL 证书实现了后量子密码混合算法加密。根据 Cloudflare 11 月 1 日的统计数据，全球互联网流量中已有 47%采用了混合 PQC 算法加密，全球前十大互联网流量网站中前 8 家已支持 PQC 算法 HTTPS 加密，美英法政府网站、美欧银行以及顶尖大学官网也纷纷启用 PQC。但这个快速更换密码算法的高科技，如何让普通互联网用户知道呢？互联网用户有权知道自己访问的网站是否已“量子安全”，因为用户自己的所有关乎到身家性命的数据都在网上，用户有知情权！

但是，很遗憾的是，常用的浏览器如谷歌 Chrome 或微软 Edge，仅显示一个简单的 Tune

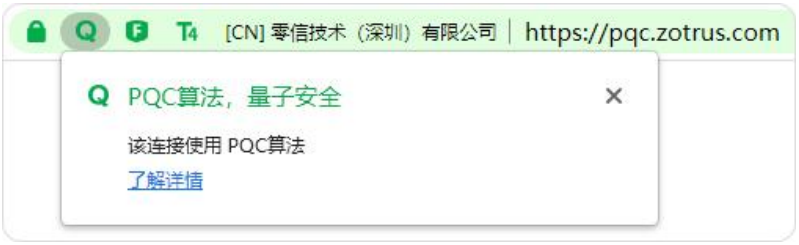
或锁标识，声称“连接安全”，却不透露底层算法。这让 PQC 迁移缺乏公众动力：网站管理员不愿投资，用户不知其益处，整个生态停滞不前。神秘的密码需要现身大众视野，正是因为只有让技术透明化，才能激发全民参与。想象一下，如果每个人都能一眼看出网站是否使用抗量子算法，就能推动网站加速升级，形成从用户到企业的倒逼机制。这不仅是技术革命，更是科普革命—让密码从幕后走向台前，让安全成为日常常识。

也就是说：安全不应该只是黑箱里的魔法，而应是透明可验的公共服务，必须从“信任某机构”到“人人可验证”的安全范式转移。所以，密码必须从隐式保护变成显式安全，密码技术必须赋能公众，以更开放透明的方式来保护公众数据安全。

二、 零信浏览器是如何让神秘密码走进大众视野的？

零信浏览器作为零信技术的拳头产品之一，遵循公司定位—“基于零信任原则的密码技术提供商”，在最新发布的 137 版本中全球独家创新地址栏 UI，将 HTTPS 加密的密码算法可视化。这不是简单的图标堆砌，而是基于深度技术解析的直观设计，帮助全球互联网用户一目了然地了解每次网站访问的连接是否真的安全，是采用何种密码算法实现的安全。这就是“零信任原则”的具体体现，不信任浏览器告诉我的“连接安全”，而是要浏览器同时告诉我真正采取的密码算法，从而让用户自己判断是否真的是安全的连接。

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”，明确告诉用户正在访问的网站能保证用户数据在现在和量子时代的持续安全，如下左图所示；而不是像其他浏览器那样简单显示“连接安全”，如下右图所示。零信浏览器这一匠心设计全球首创，让用户无需专业工具，无需专业密码知识就能验证网站的抗量子攻击能力。



此外，为全面揭示传统密码算法的风险，零信浏览器在原先已有 SM2 算法(**m** 标识)的基础上新增了 RSA 算法(**R** 标识)和 ECC 算法(**E** 标识)。如果网站使用 RSA 算法(2048 位密钥，存在风险，已被弃用)，显示“**R**”标识，点击提示：“RSA 算法，全球信任，但不支持量子安全”，

意在建议网站迁移 PQC。而网站如果采用 ECC 算法(256 位密钥，加密高效，已成 PQC 混合方案默认)，显示“**E**”标识，点击提示：“ECC 算法，全球信任，但不支持量子安全”，意在建议网站迁移 PQC。对于现在普遍采用的混合 PQC 算法连接，不仅明确告知“量子安全”，并标注网站连接认证所采用的传统密码算法（如 ECC/RSA/SM2）。这些标识不仅直观，而且还集成了网站可信身份（T1/**T2**/**T3**/**T4**）和 WAF 防护（**F**）标识，形成一站式安全仪表盘，让用户对网站所采用的所有安全保护措施一目了然。

零信浏览器通过修改 Chromium 底层 UI 逻辑，摒弃了默认的模糊“安全”标签，通过告知用户目前连接加密采用的是传统密码算法还是后量子密码而明确强调 PQC 迁移紧迫性。这项 UI 创新源于零信技术对 SSL 证书和 TLS 协议的深度分析，并优先采用 PQC 算法，不仅保障了用户的上网浏览安全，而且帮助用户在上网浏览中自然学习密码知识，增强自身上网安全保护能力。

三、 只有广泛科普后量子密码，才能顺利快速完成后量子密码迁移

后量子密码迁移不是技术精英的独角戏，而是全球范围的大工程，需要全民共识与行动。当前，PQC 标准化已由美国 NIST 主导完成，算法如 Kyber、Dilithium 等已集成进 OpenSSL、BoringSSL 和铜锁 SSL，美欧国家已经快速启动 PQC 迁移，但是中国等发展中国家及所有不发达或欠发达国家都还没有开始，这就要求从科普入手，让神秘密码真正走进大众视野。

零信浏览器的 **Q** 标识正是这一科普利器，它将抽象的密码算法转化为可见符号，推动互联网用户行为变革：当用户看到“**Q**”时，会主动选择能保障自己的数据在量子时代也是安全的网站；看到“**R**/**E**/**m**”时，会主动反馈给网站管理员，要求支持后量子密码。每一位互联网用户都能成为这场 PQC 迁移的见证者和参与者，当用户能够“**看见**”量子安全时，他们就会更有意识地“选择”量子安全，从而形成推动全球互联网 PQC 迁移的市场力量。类似地，其他浏览器也应效仿这一 UI 设计，全球互联网用户可通过推荐零信浏览器或呼吁标准化（如在 W3C 提案中加入 PQC 可视化 UI 规范 或者 在 CA/浏览器论坛中推动浏览器增加 PQC 可视化 UI 提案），从而加速 PQC 生态演进。

只有广泛科普，才能化解阻力。教育用户理解“先收集后解密”的安全威胁，就能激发需求；让企业看到用户偏好，就能投资 PQC。最终，全民支持将驱动从传统密码到抗量子密码的无缝迁移，确保互联网数据在量子时代的始终安全。零信浏览器以此为使命，作为一座桥梁，通过技术透明化，连接密码专家与大众用户，连接中国与全球。呼吁全球开发者、用户与监管者携手，让 **Q** 标识成为地址栏的标配，让密码革命惠及全球每一个人。

四、 美中 PQC 标准算法可互为备胎，协同保障全球互联网安全

美国国家标准技术研究院(NIST)已于 2024 年 8 月发布了三个 PQC 算法标准：(1) FIPS-203：基于模块格的密钥封装机制(ML-KEM)，该机制能够生成用于数据加密的安全密钥(如 HTTPS)，能够抵御量子攻击。包含：ML-KEM-512、ML-KEM-768 和 ML-KEM-1024。(2) FIPS-204：基于模块格的数字签名算法(ML-DSA)，采用 Fiat-Shamir with Aborts 来抵御量子攻击，其密钥和签名大小适中，签名较快，验签更快。(3) FIPS-205：基于哈希的数字签名算法(SLH-DSA)，采用 HORST 和 W-OTS 来抵御量子攻击，具有更短公钥和私钥的优势，签名值比 ML-DSA 长。其中，目前被广泛使用的 PQC 算法是 ML-KEM-768 算法，用于 HTTPS 密钥交换协议的混合 PQC 算法 X22519MLKEM768，这是美国 PQC 标准为保障全球互联网安全率先做出的贡献，值得高度肯定。

中国商用密码标准研究院(NICCS)已于 2025 年 10 月发布了全球正式开始接收下一代商用密码算法(NGCC)包括公钥密码算法、杂凑算法和和分组密码算法的后量子密码算法标准提案，这是在前期国际密码研究工作取得的成果基础上做出的新探索，希望进一步促进密码算法设计与分析技术发展创新，进一步丰富密码算法特别是抗量子计算公钥密码算法的新颖性、多样性，进一步推动国际密码学术交流、 繁荣密码学科发展，以期形成相互适配的新一代商用密码算法体系，推动新一代商用密码算法标准制定。按照《密码算法提交要求》，NGCC 不排斥之前参与国际标准化活动但未被选中的算法提案，同时期待收到有进一步创新的算法提案，但明确不接受已经成为由美国 NIST 标准的相同或类似算法提案。

鉴于目前的后量子密码算法只是理论上的抗量子攻击，无法真正验证，因为可用于验证算法是否可靠的量子计算机还没有研究出来。所以，笔者认为，为了保障全球互联网安全，全球互联网不仅应该尽快启用已有的美国主导的 PQC 标准算法来保障全球互联网安全，同时也期待中国的 PQC 标准算法能早日出台并成为保障全球互联网安全的可选算法之一，并呼吁 IANA、IETF 和 CA/浏览器论坛等国际组织能积极支持把中国现有商用密码算法和下一代商用密码算法(PQC 算法)纳入相关国际标准中，及时分配相关协议号，以便正式在相关协议(如 TLS)中启用中国 PQC 标准，让美国主导的 PQC 国际标准和中国主导的 PQC 标准互为备胎，同时也都是全球互联网用户可选的 PQC 算法之一，共同为保障全球互联网安全做贡献，因为量子计算对传统密码算法的威胁是全球无国界的威胁，全球只有一个互联网。

王高华

2025 年 11 月 3 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 236 篇(共 70 万 1 千多字)和英文 101 篇(13 万 8 千多单词)。