科普：只有后量子密码才能真正保障数据安全

2026 年 1 月 12 日

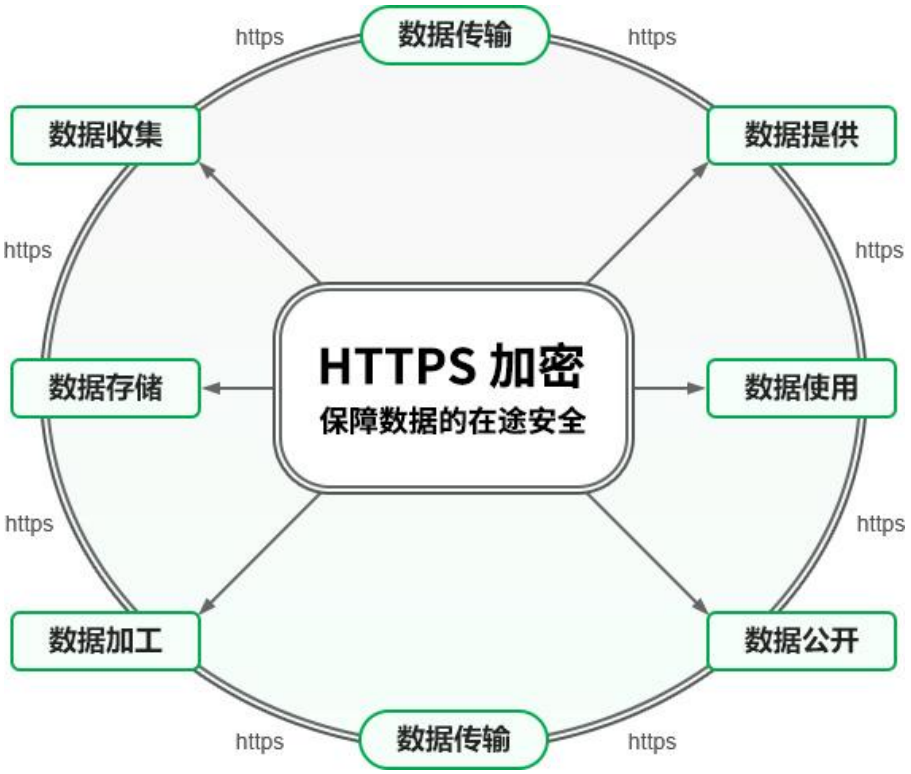
日前，国家数据局印发了《**关于加强数据科技创新的实施意见**》，《意见》中 3 次提到“**数据安全**”，充分体现了数据安全在整个数据科技创新中的重要性。但是，如何保障数据安全，非常值得认真探讨。

随着量子计算的快速发展，用于保护数据安全的传统密码技术正面临前所未有的挑战。令人瞩目的是，美欧国家在普及后量子密码（PQC）方面进展迅速，不到一年时间，全球互联网流量中采用混合 PQC 算法加密的占比从 28%跃升至 56%，整整翻了一倍。然而，我国互联网的后量子密码 HTTPS 加密流量却几乎为**零**。这与我国作为数字应用大国的地位以及“数据安全是国家安全的重要组成部分”的战略定位极不相称。本文将系统阐述，为何只有普及应用后量子密码，才能真正筑起坚不可摧的数据安全长城。

一、 HTTPS 加密：保障数据流通安全

数据要创造价值，就必须流通。而数据一旦开始流动，其安全的核心就聚焦于“**在途**”阶段，数据安全的关键在于保障其在传输过程中的安全。HTTPS 加密正是现代互联网保障数据传输的基石，它利用 SSL/TLS 协议，在用户端和服务器之间建立一个加密的安全通道，确保数据在传输过程中既无法被窃取，也无法被篡改。

依据《数据安全法》第三条对“数据处理”的定义，数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等。在这七个数据处理环节中，其他六个环节都离不开数据传输，所以，数据安全的“七寸”是数据传输，必须保护数据的传输安全，不做好这个安全保护，其他任何安全措施都是空中楼阁，这就是数据的“在途”安全保障，唯一可靠的技术方案就是 HTTPS 加密，数据在全生命周期中的流通传输都必须是通过 HTTPS 加密通道传输。HTTPS 加密是数据安全的最低要求，也是所有数字信任的前提，当然也是人工智能应用的最低要求。



当然，依据《密码法》必须采用商密算法实现 HTTPS 加密，也就是必须部署国密 SSL 证书来实现 HTTPS 加密，只有这样，才能有效保障每一个数据处理过程中的数据处于有效保护中，使得数据从生产到销毁的全生命周期都处于持续安全状态。这就是《数据安全法》所定义的“数据安全”要求，指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

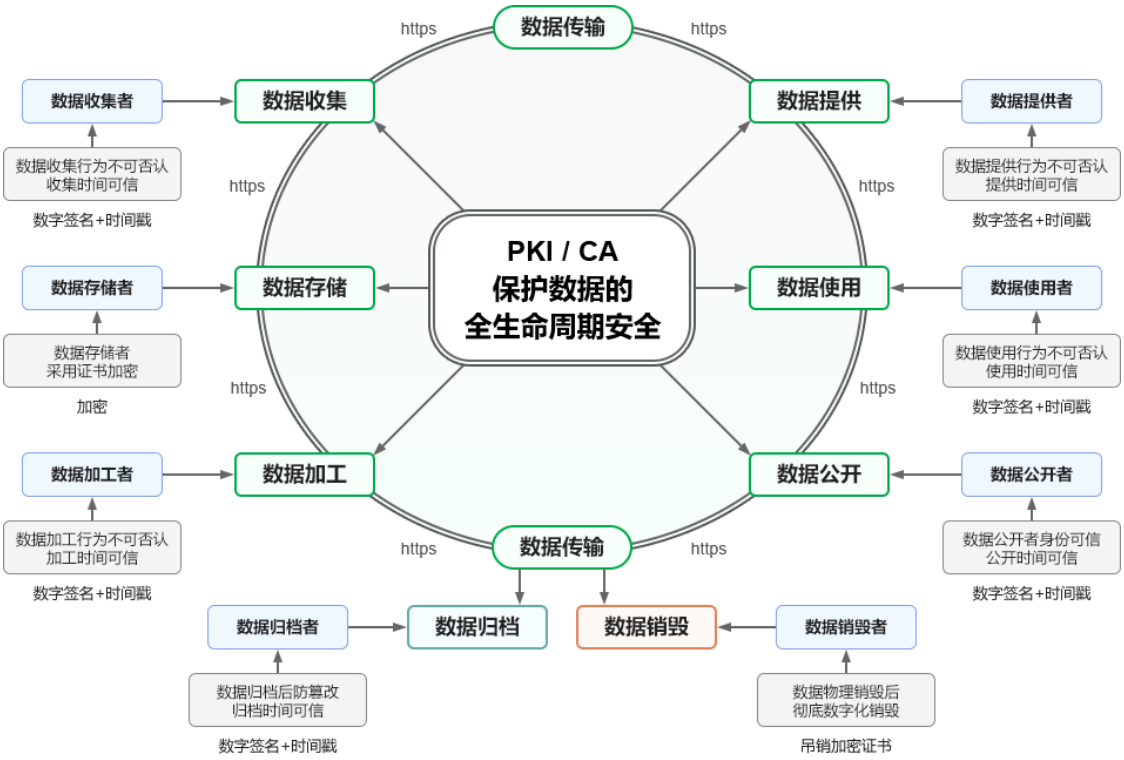
二、 数字签名认证：保障安全使用数据

如果说 HTTPS 加密解决了数据“怎么传”的安全问题，那么以 CA（证书颁发机构）为核心的 PKI（公钥基础设施）体系，则解决了数据“从哪来”、“谁处理”以及“是否可信”的身份认证与责任认定问题。《密码法》明确指出，密码是用于加密保护与安全认证的技术。CA 机构作为依法设立的可信第三方，其签发的数字证书是实现这两大功能的关键载体。它贯穿于数据的全生命周期：

- **在途加密**：签发 SSL 证书，是实现 HTTPS 加密的信任起点。
- **身份认证**：为数据处理者和数据使用者签发数字身份证书，证明其真实、合法的可信身份。
- **行为确权**：无论是数据的收集、存储、加工、提供、公开、使用，通过数字签名和时

间戳技术，可以确保任何数据处理行为都不可否认、可追溯、且具备法律效力，这就是《电子签名法》提供的法律保障。

- **存储、归档与销毁安全：**用数字证书加密存储的数据，即使发生泄露，只要私钥安全，数据依然安全。当数据需要销毁时，吊销对应的加密证书即可实现数据先逻辑销毁再物理销毁。而当数据需要归档时，其数字签名和时间戳保证了归档数据的不可篡改和归档时间可信。



数字签名利用非对称密码技术，实现对数据发布者身份的强认证，并确保数据自签名后不被篡改，为每一次数据交互提供不可否认性。它确保了在复杂的网络环境中，我们可以信任数据的来源，并追溯处理过程，从而构建起可信的数字秩序。离开了数字签名，数据的真实性与可信度将无从谈起。可以说，CA/PKI 体系及数字签名是数据安全体系的“保护神”，它建立的信任链条，是整个数字社会得以有序运行的底层逻辑。

三、 HTTPS 加密和数字签名认证面临量子计算安全威胁

但是，无论是保障“在途”安全的 HTTPS 加密，还是实现数字签名认证的 PKI 体系，其安

全根基都依赖于 RSA/ECC/SM2 算法的经典数学难题的计算复杂性。然而，量子计算的崛起，对这些数学难题构成了“降维打击”式的根本性威胁。一旦实用化的量子计算机问世，它能够在极短时间内破解当前广泛使用的公钥密码，导致灾难性后果。这意味着：

(1) **加密通道被穿透**：量子计算机可以解密截获的采用传统密码算法实现的 HTTPS 加密通信历史数据，这就是已经存在的“先收集后解密”安全威胁，用户隐私、商业秘密和国家机密将完全暴露。

(2) **信任体系被瓦解**：可以伪造数字签名，冒用任何个人或机构的身份，整个基于 PKI 的信任链条的数字世界身份认证体系和信任链将瞬间崩塌。

(3) **威胁具有“追溯性”**：今天用传统密码算法保护的高度敏感数据（如国家机密、医疗档案、知识产权等），可能因其需长期保密（如 30 年）的特性，暴露在未来量子计算机的威胁之下。

因此，量子计算带来的并非一种增强的威胁，而是关乎现行数据安全体系存亡的范式危机。它击中的正是我们现有数据安全体系的“七寸”。 对于需要长期保密（数十年）的数据而言，量子计算的威胁已迫在眉睫，这并非遥远的前瞻担忧，而是正在发生的现实安全危机。

四、 只有普及应用后量子密码，才能真正保障我国数据安全

应对这场迫在眉睫的数据安全危机，必须立刻行动起来实施后量子密码迁移工作，快速采用后量子密码算法替换现有密码体系中脆弱的环节。这要求我们：

(1) **快速普及混合 PQC 算法 HTTPS 加密**：基于现有的传统密码算法(SM2/RSA/ECC)签发的 SSL 证书，采用混合 PQC 算法（如 SM2MLKEM768 或 X25519MLKEM768）实现密钥交换，替换当前 TLS 协议中易受量子攻击的密钥协商部分。这将确保即使面对未来的量子计算机，数据传输通道的保密性和完整性依然牢不可破。这是全球业界推行的“混合模式”过渡方案，即在现有 HTTPS 加密中同时结合传统密码算法和后量子密码算法，是当前平滑、安全地向后量子密码 HTTPS 迁移的最佳路径。

(2) **采用传统密码和后量子密码算法双数字签名**：改造现有传统密码算法数字签名应用，实现传统密码算法和 PQC 算法双数字签名，不仅兼容传统密码算法验签，而且同时支持 PQC 算法验签，为各种电子文档和身份认证等应用重建一个能抵御量子攻击的长期信任基础，确保数据的真实性、完整性和签署行为的不可否认性在未来依然有效。

普及这两大同时兼容传统密码和后量子密码的解决方案不仅是技术升级，更是国家数据安全战略的必然要求。《**意见**》要求“加快数据流通利用基础设施体系建设，推动建设数据安全防护平台，促进跨地域、跨领域、跨主体数据资源可信流通与高效利用，保障数据安全。”这就要求我国在标准制定、算法研发、产品实现、生态建设等多个层面加速布局，特别是在作为信任核心的证书签发体系（CA）、浏览器、操作系统、服务器和关键业务系统中率先推动支持后量子密码算法和协议栈。唯有如此，我们才能在加固当前数据流通与使用安全的同时，筑牢面向量子时代的终极防线，真正掌握数据安全的主动权。

数据安全是数字时代的生命线。当守护这条生命线的 HTTPS 加密与数字签名两大核心技术面临量子计算颠覆性威胁时，被动防御毫无胜算。唯有主动出击，通过实施后量子密码 HTTPS 加密以保障数据流通安全，采用后量子密码数字签名以维护数字信任体系，才能系统性地化解危机。这是一场关乎未来数字主权和网络安全根基的战略行动，只有赢得这场密码算法的代际升级，才能真正实现“数据供得出、流得动、用得好、保安全”、“进一步激活数据要素乘数效应，更好赋能数字中国建设”，才能为数字中国的发展奠定坚实、可信、面向未来的安全基石。

王高华

2026 年 1 月 12 日于深圳
