量子计算威胁与应对白皮书

——“先收集后解密”攻击：今天的威胁，必须今天应对

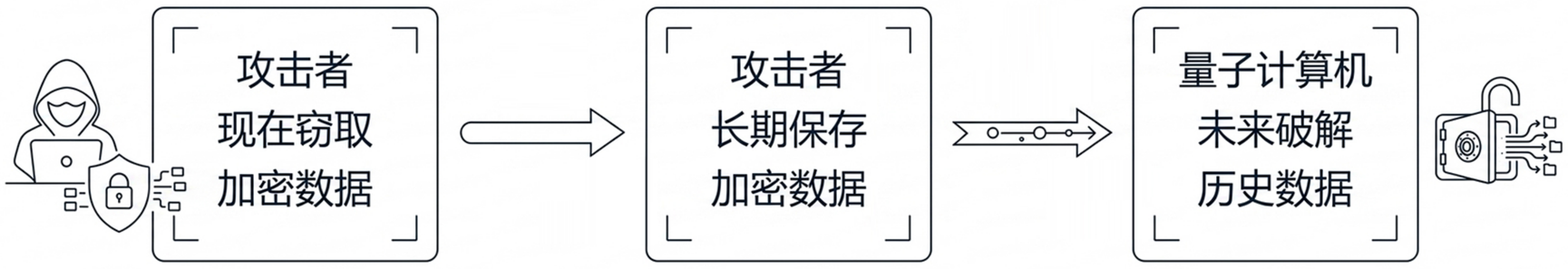
一 引言：被低估的现实威胁

当人们谈论“量子计算威胁”时，常常将其视为一个遥远的未来问题。然而，**这个未来已经到来，**但不是以量子计算机已经破译密码的形式，而是以“先收集后解密”（Harvest Now, Decrypt Later）攻击的形式，成为今天就必须面对的严峻现实。

“先收集后解密”攻击：攻击者现在收集加密数据并长期保存，等待未来量子计算机成熟后，再批量破解这些数据。这意味着，今天通过互联网传输的敏感信息，可能在3-5年后被大规模泄露。

二 威胁解析：“先收集后解密”如何运作？

2.1 攻击链路



2.2 哪些数据面临风险？

数据类型	保密周期	风险说明
政府机密文件	数十年	外交、国防、情报信息一旦泄露，后果不可估量
银行交易记录	10-30年	账户信息、交易流水、客户身份信息
医疗健康档案	50年以上	患者病历、遗传信息、健康隐私
企业核心知识产权	长期	研发数据、商业机密、专利信息
个人隐私数据	终身	身份证号、通讯记录、社交媒体内容

2.3 为何是“今天”的威胁？

- **攻击成本低：**攻击者现在大规模收集加密数据，成本极低，包括敌对国家行为
- **数据价值高：**政府、银行、医疗机构的数据具有长期价值
- **等待成本低：**攻击者只需存储数据，等待量子计算机成熟(估计2030年-2035年)
- **破解收益大：**一次破解，可获得多年积累的海量数据

美国国家安全局（NSA）、英国国家网络安全中心（NCSC）等机构均已发布警告，明确指出“先收集后解密”是当前最紧迫的后量子安全威胁之一。

三 多CA高可用的核心价值

3.1 全球PQC迁移进展

根据Cloudflare雷达统计，截至2026年4月，**全球互联网流量中已有68%实现了后量子密码HTTPS加密**。这意味着接近70%的全球互联网流量，现在就已经受到后量子密码保护。

区域/组织	进展
美国政府	2025年8月起，政府网站及多项政务服务系统已陆续启用后量子HTTPS加密
美国银行业	主要银行网银系统已完成后量子迁移试点
欧洲国家	英国、法国、德国等纷纷启动政府网站后量子改造
G20国家	已有7个国家门户网站启用后量子HTTPS加密（美国、英国、法国、日本、澳大利亚、沙特阿拉伯、阿根廷）
顶尖高校	牛津大学、剑桥大学、加州大学伯克利分校等已启用
云服务商	Cloudflare、亚马逊AWS等已为所有用户免费提供后量子加密支持

3.2 我国现状：仍为空白

对比项	欧美	中国
政府网站后量子加密	已大规模部署	**0个**
银行网站后量子加密	主要银行已完成	**0个**
高校网站后量子加密	顶尖高校已启用	仅个别高校（如清华）启用国际方案，非国密方案
浏览器支持	Chrome、Edge、Safari、Firefox已支持国际混合PQC	**零信浏览器**全球独家支持国密混合PQC和国际混合PQC

差距警示：当我国政府、银行、高校、医院的数据仍然使用传统密码保护时，这些数据实际上已经暴露在“先收集后解密”的威胁之下。而欧美同行的同类数据，已开始受到后量子密码的保护。

四 应对之道：双混合PQC算法，数字认证的领先方案

4.1 什么是混合PQC算法？

混合PQC算法是指**传统密码算法与后量子密码算法的组合**。它在保证当前兼容性和性能的同时，提供抗量子攻击能力：

- **传统密码算法部分**（如X25519、SM2）：确保与现有系统的兼容性，保障当前业务正常运行
- **后量子密码算法部分**（如MLKEM768）：提供抗量子攻击能力，保护数据在未来量子计算机面前依然安全

4.2 全球两大混合PQC算法标准

算法名称	传统部分	后量子部分	适用场景
X25519MLKEM768	X25519（ECC）	MLKEM768（Kyber）	国际主流方案，已在欧美大规模部署
SM2MLKEM768	SM2（国密）	MLKEM768（Kyber）	**中国方案**，同时满足国密合规与量子安全

4.3 SM2MLKEM768的国际认可

◆**2025年11月14日**：国际组织IANA（互联网号码分配机构）正式为SM2MLKEM768分配了TLS支持组算法编号：**4590**
◆这是我国密码研究团队推出的商用密码算法与后量子密码算法混合协议，首次获得权威国际标准组织认可
◆SM2MLKEM768已成为IANA列出的四个后量子密码混合协议之一，与X25519MLKEM768并列

4.4 数字认证 SSL自动化网关：全球率先支持双混合PQC算法

数字认证 SSL自动化网关是全球率先**同时支持SM2MLKEM768和X25519MLKEM768双混合PQC算法**的商用产品。

能力	说明
双算法支持	同时支持X25519MLKEM768（国际方案）和SM2MLKEM768（中国方案）
智能协商	自动与客户端协商最优算法，优先采用SM2MLKEM768（如客户端支持），确保国密优先
向后兼容	如客户端不支持混合PQC，自动降级至传统算法（X25519或SM2），保障业务连续性
国密合规	支持国密SM2算法SSL证书，满足等保2.0、密评GM/T 0054要求
后量子密码就绪	无需更换SSL证书，即可为所有网站开启后量子密码HTTPS加密

4.5 配套支持：零信浏览器——端到端的后量子密码HTTPS加密生态

仅有网关支持是不够的。后量子密码HTTPS加密需要客户端（浏览器）与服务器端（网关）的双重支持，才能实现完整的加密通道。

零信浏览器是全球首款同时支持SM2MLKEM768和X25519MLKEM768双混合PQC算法的浏览器，与数字认证 SSL自动化网关形成**端到端的完整后量子密码HTTPS加密生态：**

组合	效果
数字认证网关 + 零信浏览器	**国密混合PQC：**采用SM2MLKEM768算法，同时满足国密合规与量子安全
数字认证网关 + 谷歌Chrome	**国际混合PQC：**采用X25519MLKEM768算法，与国际生态对齐
数字认证网关 + 传统浏览器	**传统算法加密：**自动降级，保障正常访问

用户使用零信浏览器访问由数字认证 SSL自动化网关保护的网站时，地址栏会显示“Q”标识，提示“PQC算法，量子安全”，让用户一眼即可确认该连接已受到后量子密码保护。

五 为什么选择双混合PQC算法？——韧性即安全

5.1 单一算法的风险

如果只依赖一种后量子算法，存在以下风险：

◆**该算法在未来被发现存在安全漏洞**
◆**该算法的标准化进程受阻**
◆**该算法与某些客户端不兼容**

5.2 双算法的韧性优势

优势	说明
算法冗余	两种算法同时部署，即使一种算法出现问题，另一种仍可提供保护
生态兼容	X25519MLKEM768兼容国际主流浏览器，SM2MLKEM768兼容国密生态，双管齐下
合规保障	SM2MLKEM768满足国内国密合规要求，X25519MLKEM768满足国际互认需求
面向未来	无论未来后量子算法如何演进，双算法架构提供了更长的技术生命周期

全球互联网TLS生态需要多种算法提供更好的韧性和更多的选项，因为谁也无法保证传统的密码算法和后量子密码算法在未来的量子计算机面前是安全的，多一个选择就多了一份安全保障。

六 部署效果：一台网关，三重保障

部署数字认证 SSL自动化网关后：

访问场景	加密效果	说明
用户使用零信浏览器访问	国密算法+后量子密码混合加密（SM2MLKEM768）	同时满足国密合规与量子安全
用户使用Chrome/Edge/Firefox/Safari访问	国际算法+后量子密码混合加密（X25519MLKEM768）	与国际主流生态对齐
用户使用不支持PQC的浏览器访问	传统算法加密（SM2或RSA/ECC）	自动降级，保障正常访问

一台网关，同时覆盖国密合规、国际兼容、量子防护三大需求。

七 行动建议：现在就开始后量子密码迁移

7.1 立即评估风险

- ◆ 您的单位是否传输需要长期保密的敏感数据（政务、金融、医疗、科研）？
- ◆ 这些数据的保密期是否超过10年?
- ◆ 您能否承受数据在未来被批量破解的后果?

7.2 选择后量子迁移路径

路径	方案	适合场景
国际方案	X25519MLKEM768	仅需国际兼容，无国密合规要求
中国方案	SM2MLKEM768	同时需要国密合规与量子安全
双方案（推荐）	同时支持两种算法	政府、银行、高校、医院等需要同时国密合规、国际兼容与数据长期安全的机构

7.3 立即部署

数字认证 SSL自动化网关，是当前市场上**唯一能同时实现国密合规、证书自动化、双混合PQC后量子密码加密**的一体化解决方案。部署网关后，您的所有网站即刻获得：

◆ 证书全生命周期自动化（多CA高可用）
◆ 国密改造一键完成（满足等保、密评）
◆ **双混合PQC后量子加密（X25519MLKEM768 + SM2MLKEM768）**
◆ 内置A级WAF，证书自动联动
◆ 与**零信浏览器**形成端到端后量子密码HTTPS加密生态

一次投资，同时解决国密合规、证书自动化、量子威胁三大难题。

八 结语

后量子密码迁移不是“未来时”，而是“**现在时**”。“先收集后解密”攻击已经让今天的数据面临明天的风险。当欧美政府、银行、高校、医院已经大规模部署后量子密码HTTPS加密时，我国相关领域仍是空白。

数字认证 SSL自动化网关与**零信浏览器**配套，提供全球独家支持双混合PQC算法的端到端后量子密码HTTPS加密解决方案，帮助中国关键信息基础设施单位，**今天完成国密改造，同时实现后量子密码就绪**，保障数据在量子时代的持续安全。

时不我待，立即行动。

数字认证·双混合PQC算法支持，为您的数据提供面向未来的双重保障

北京数字认证股份有限公司　国有控股上市企业（300579）·北京数据集团核心成员 ·数字认证，SSL证书自动化领导者
联系我们：官网 ssl.bjca.cn　服务热线 4009-197-888　邮箱 ssl@bjca.org.cn