我国云平台密码应用差距正在拉大，未来三年或决定生死

2026 年 3 月 9 日

在数字化转型浪潮席卷全球的今天，云平台已成为国家数字经济的核心基础设施。企业客户数据、政府政务信息、个人隐私资料、AI 数据——这些构成数字社会基石的宝贵资产，如今绝大多数都存储在云平台上。然而，在这看似坚固的云存储和云计算的背后，一道关键安全防线正在出现令人担忧的裂缝：密码技术应用的严重滞后。

当国际云服务巨头已在量子时代到来之前重构密码体系时，我国云服务平台仍在传统密码技术的舒适区中缓慢前行。这种差距不是简单的技术代差，而是关乎未来数字主权和数据安全的战略隐患。如果不能立即行动，今天加密存储在云端的所有机密数据，都可能在未来 3-5 年内的某个时刻变成“透明的裸数据”。

一、国际竞争：从证书自动化到后量子密码的全面领先

纵观全球云服务市场，国际领先云平台厂商在密码技术上的布局已形成清晰的战略路径。亚马逊云平台 AWS 拥有全球信任根 CA，其证书管理服务实现了 SSL 证书全生命周期自动化管理，用户只需简单配置，系统即可免费自动完成证书的申请、验证、部署和续期，彻底消除了因证书过期导致服务中断的风险。更值得关注的是，AWS 已投入巨资建立后量子密码研究中心，并在其 CDN 服务中支持混合 PQC 算法，其密钥管理服务中开始支持后量子密码算法。

谷歌也拥有全球信任根 CA，谷歌所有系统仅信任自家 CA 签发的 SSL 证书。谷歌云平台更是展示了另一种极致体验——在负载均衡器配置中仅需选择“Google 托管证书”，系统便会自动处理所有繁琐证书管理流程。这种“零配置”安全理念，让 HTTPS 加密从专业运维任务变为基础服务功能。与此同时，谷歌在量子安全领域的布局更为超前，其全球网络节点正逐步升级支持后量子密码算法，包括用于 HTTPS 加密的混合 PQC 算法和用于数字签名的 PQC 算法。其占据全球 70%以上市场份额的 Chrome 浏览器（含开源 Chromium）更是全球率先支持混合 PQC 算法 HTTPS 加密，形成了端云一体的全生态 PQC 迁移战略。

微软云平台 Azure 的策略体现了企业级市场的深度思考，通过 Key Vault 与 Active Directory 的深度集成，为企业客户提供证书自动化和平滑的后量子密码升级路径。在量子计算应对方面，微软云已为政企客户提供混合 PQC 算法 HTTPS 加密方案，并制定了清晰的迁移路线图。

Windows 操作系统和 Edge 浏览器也都已经支持后量子密码算法，形成了端云一体的全生态 PQC 迁移战略。

最引人注目的是 Cloudflare 的实践。作为全球最大的边缘网络服务商，Cloudflare 默认为所有用户免费自动化配置 SSL 证书，默认对所有流量启用混合 PQC 算法 HTTPS 加密。这意味着通过其网络的每一比特数据，都已获得面向未来的量子安全防护。这种前瞻布局，让 Cloudflare 在全球网络安全格局中占据了独特位置。

二、国内现状：三重差距叠加的严峻现实

相比之下，我国云平台在密码技术应用上面临着三重差距叠加的挑战。

第一重差距：自动化程度落后整整一代。

当国际厂商实现“零干预”证书管理时，国内平台几乎全部仍依赖手工操作。证书申请和部署需要人工申请和部署，续期需要手动触发。这种落后不仅增加了运维负担，更导致证书过期事故频发，直接影响服务可用性。在容器化和微服务架构成为主流的今天，传统的手工证书管理方式已无法适应动态、弹性、规模化的云环境需求。

第二重差距：后量子密码布局基本空白。

这是最危险的技术代差。目前，国内没有一家主流云厂商正式支持后量子密码 HTTPS 加密，甚至缺少公开的技术路线图和实验性部署。在量子计算快速发展的背景下，这种空白意味着所有使用传统密码算法保护的机密数据都面临“先收集后解密”安全威胁——攻击者现在截获加密数据，等待量子计算成熟后解密。一旦量子计算机实现实用化突破，基于 RSA/ECC/SM2 传统密码算法的 HTTPS 加密体系和数字签名体系将瞬间瓦解，而缺乏防护的云端数据将完全暴露。

第三重差距：国密算法支持不完整且应用受限。

虽然国家推动商用密码算法已有十余年，但实际落地情况远未达到预期。目前仅阿里云、华为云等少数厂商在部分产品中支持国密算法，且大多存在使用门槛高、兼容性差、性能不佳、API 功能不全等问题。更重要的是，没有一个云平台支持高性能的 TLS 1.3 协议国密算法，更别提支持国密混合 PQC 算法(SM2MLKEM768)了，无法满足中国企业出海和跨国企业在华业务的密码合规需求。这种“推而不广”的局面，既制约了国密算法的实际应用效果，也影响了我国密码技术的国际竞争力。

三、三重危机：技术、商业与安全的连锁反应

我国云平台面临三重差距相互叠加，产生乘数效应，形成系统性的三重安全危机。

第一危机：技术方面

密码技术的滞后正在拖低整个云平台生态的安全水位。云平台作为数字基础设施，其安全能力决定了上层应用的防护上限。当基础平台存在密码应用短板时，所有构建其上的 SaaS 服务、行业应用都将面临先天不足的安全风险。在量子计算渐行渐近的背景下，这种风险呈现出“时间累积效应”，越早迁移到后量子密码，防护成本越低，安全性越高；越晚行动，风险越大，代价越高。

第二危机：商业方面

安全能力正在成为云服务竞争的关键维度。越来越多的大型企业、金融机构、政府部门在选择云服务时，将供应商的密码技术路线作为重要评估指标。缺乏前瞻性安全布局的云平台，不仅难以争取高端客户，还可能在国际市场竞争中丧失机会。当全球主要经济体开始要求关键基础设施具备量子安全能力时，不符合要求的云服务将面临市场准入障碍。

第三危机：安全方面

密码技术的落后直接威胁国家数字主权。在数字时代，密码算法和标准制定权等同于数据控制权。如果我国云平台不能建立起自主可控、面向未来的密码体系，就意味着将数据安全的主动权拱手让人。特别是在地缘政治复杂多变的国际环境下，密码技术的自主性已成为国家网络安全的核心要素。

四、未来三年：决定生死的战略窗口期

从全球技术演进趋势看，未来三年将是我国云平台弥补密码技术差距的最后窗口期。

美国国家标准技术研究院（NIST）于 2024 年 8 月正式发布了三个后量子密码算法标准，开启全球密码体系升级的序幕。按照密码学界的普遍预测，从标准发布到规模化应用通常需要 3-5 年时间。这意味着，如果我国云平台不能在 2027 年前完成基础补课和前瞻布局，就可能错过量子安全迁移的最佳时机。

这个窗口期之所以“生死攸关”，是因为密码技术的升级不是简单的功能迭代，而是涉及算法替换、协议升级、系统重构的复杂工程。特别是向后量子密码的迁移，需要重新设计整个密码体系架构，更新硬件加速设备，改造软件协议栈。这些工作需要充足的准备时间和缜密的实施规划。

更紧迫的是，密码技术的升级存在“协同效应”——只有当云平台、操作系统、浏览器、应用程序等各个环节同步升级时，新算法才能真正发挥作用。这要求云平台必须尽早启动后量子

密码迁移工作，现在就开始支持混合 PQC 算法 HTTPS 加密，特别是 CDN 和 WAF 服务，为整个生态系统的演进提供平滑迁移实践经验，并为向纯后量子密码迁移留出足够时间。

五、三场硬仗：证书自动化、国密算法、后量子密码算法并行推进

面对时间窗口的紧迫性，我国云平台需要在三条战线上同时发力。

第一战线：打赢证书自动化攻坚战。

必须马上行动起来，彻底改变当前手工管理 SSL 证书的落后模式，构建智能化的证书全生命周期管理体系，而且必须是双算法(SM2+RSA/ECC) SSL 证书自动化管理。这不仅仅是开发几个自动化工具，而是要将密码管理深度集成到云原生架构中，实现双算法 SSL 证书申请、部署、更新、吊销的完全自动化。同时要建立智能监控预警机制，实时发现和处置证书异常。自动化不仅是效率问题，更是安全问题——减少人为错误，提高防护一致性。

第二战线：打赢国密算法深度支持战。

要推动国密算法从“有支持”到“好用易用”的根本转变。这需要在云平台的每个层级——从基础设施到平台服务再到软件应用——全面集成国密算法。全面支持 TLS 1.3 协议国密算法，切实优化国密算法性能，解决实际部署中的兼容性问题。更要推动国密标准的国际化，使中国密码技术能够在全球范围内获得认可和应用。国密算法的深度应用，是构建自主可控安全体系的基石。

第三战线：打赢后量子密码破局战。

这是最具战略意义的一战。云平台需要立即启动混合 PQC 算法 HTTPS 加密的全面部署，不仅需要支持国际云平台广泛支持的国际混合 PQC 算法(X25519MLKEM768)，在关键网络通道和核心数据服务中，特别是政务云平台，必须同时支持国密混合 PQC 算法(SM2MLKEM768)。要积极参与国际标准制定，推动中国方案纳入全球标准体系。要研发过渡时期的国密混合后量子密码 HTTPS 加密方案，确保技术演进过程中的业务连续性。后量子密码布局的早晚，决定了未来数据防护的强度。

六、行动路线：从紧急止血到全面领先

要在有限时间内打赢以上三场战役，我国云平台需要有一个清晰务实的实施路线。

第一阶段（未来 6-12 个月）：紧急止血与快速补课。

云平台应全面评估现有密码应用体系的风险点，立即引入成熟的自动化证书管理方案，如：

零信技术 HTTPS 加密自动化解决方案，解决最紧迫的 HTTPS 自动化运维安全问题。应该率先在 CDN 服务中启动双算法 SSL 证书自动化，支持国际混合 PQC 算法和国密混合 PQC 算法 HTTPS 加密，积累初步经验。这一阶段的目标是遏制与国际云平台的差距的进一步扩大，建立基础密码保障能力框架。

第二阶段（1-2 年）：系统加固与深度整合。

在 SSL 证书自动化方面，建成统一的证书管理平台，实现跨产品线的一致体验。在国密算法支持上，完成全栈深度集成，使 TLS1.3 国密算法成为默认选项而非特殊配置。在后量子密码布局上，开始在实际业务场景中部署使用混合 PQC 算法，并制定详细的后量子密码迁移路线图。这一阶段的核心是构建完整的密码技术体系，形成内部协同能力。

第三阶段（2-3 年）：全面领先与生态引领。

此时的目标应转向建立竞争优势。构建全球一流的双栈算法(国产密码算法+国际密码算法)密码应用自动化体系，比其他国外云平台的单栈密码体系更有韧性，让双栈密码安全能力成为产品核心竞争力。推动国密算法在国际标准中获得广泛认可，为中国技术全球化铺路。在后量子密码的实际部署上达到国际先进水平，在某些关键领域实现领先。最终目标是形成中国云平台在密码安全领域的双栈算法独特优势。

七、时代召唤：安全能力决定云平台的未来价值

在数字时代，数据已成为最宝贵的资产，而密码技术就是守护这些资产的终极防线。云平台的密码安全能力，不仅关系到自身商业成败，更关系到千行百业的数字化转型安全，关系到国家数字主权的完整性。

当前，我们正站在一个关键的历史节点上。量子计算的突破虽时间未定但可预期，密码防御必须提前布局已成全球共识。国际云平台已在这场关乎未来的竞赛中抢先起跑，我国云平台若不能奋起直追，就可能在新一轮技术变革中掉队。

密码技术的升级不仅是技术挑战，更是战略抉择。它考验的是云平台的前瞻视野、技术勇气和责任担当。在价格战、规模战之外，中国云平台需要开启一场“**密码能力战**”——这可能是决定未来十年行业格局的关键战役。

八、紧急呼吁：行动起来，构筑量子时代的加密防线

在此，零信技术向国内所有商业云平台、政务云平台发出紧急呼吁：

立即行动起来，全面升级密码技术体系！

首先，请立即部署 SSL 证书自动化管理系统。 不要让证书过期成为服务中断的原因，不要让手工操作成为安全漏洞的来源。自动化不是可选项，而是现代云服务的标配。请为用户提供简单、可靠、全自动的证书管理体验，让 HTTPS 加密成为无缝的基础服务。

其次，请深度支持国密算法体系。国密算法是我国密码自主可控的核心，不仅要“有支持”，更重要的是要让国密算法真正“好用”——优化其性能，简化其配置，完善其生态，推动其国际化。国密算法的广泛应用，是构建国家网络安全和数据安全屏障的基石。

最重要的是，请立即启动后量子密码布局。时间不等人，量子计算的脚步日益临近。请现在就开始研究、实验、部署后量子密码算法，默认为用户提供国密混合 PQC 算法 HTTPS 加密，提供面向未来的合规保护。不要等到量子计算机成为现实时才匆忙应对，那时必定为时已晚。

云平台的运营商们，你们托管的不仅是客户的数据，更是数字经济的未来。每一份加密的数据，都是对用户信任的承诺；每一次算法升级，都是对安全责任的践行。

零信技术愿助力云平台快速行动起来，在量子时代到来前筑起坚固的加密防线。让我们证明，中国云平台不仅能够提供高效的计算和存储，更能够提供面向未来的密码安全保障。这是技术的竞赛，更是责任的担当。

数据安全无小事，密码防线是基石。未来三年，行动与否，将决定我国云平台是引领时代，还是被时代抛弃。选择就在此刻，行动必须现在开始！

为中国云平台的安全未来，为我们共同的数字明天，请立即行动！

王高华

2026 年 3 月 9 日于深圳

王高华 Digitally signed by 王高华 Date: 2026.03.09 08:58:30 +08'00'

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 265 篇(共 77 万 9 千多字)和英文 117 篇(16 万 1 千多单词)。