量子安全之路：我国应该大力发展 PQC，而非 QKD

2026 年 4 月 17 日

一、量子安全的两条道路

量子计算机的脚步声越来越近。2026 年 3 月 25 日，谷歌正式宣布将在 **2029** 年底前完成其所有系统、产品与服务向后量子密码（PQC）的迁移。然而，在通往“量子安全”的道路上，一直存在着两条技术路线之争：一条是**后量子密码（PQC）**，依靠数学算法抵抗量子攻击；另一条是**量子密钥分发（QKD）**，依靠量子物理原理实现密钥的安全传输。

面对这两条路，我国应该如何选择？谷歌的两位技术专家在一篇题为《Google’s Commitment to a Quantum-Safe Future: Why PQC is Google’s Path forward and not QKD》的官方博客中，给出了清晰而坚定的答案：**PQC 是通往量子安全未来的正确道路，而 QKD 对于谷歌这样规模的基础设施几乎没有价值**。这一立场与美国国家安全局（NSA）、英国国家网络安全中心（NCSC）、德国联邦信息安全办公室（BSI）等多家国家级安全机构的建议高度一致。

本文将从谷歌技术专家的详细评估出发，分析 PQC 与 QKD 的技术优劣，并结合我国国情，阐述为什么我国应该大力发展国密混合 PQC，而非押注 QKD。

二、谷歌为什么选择 PQC 而非 QKD？

谷歌技术专家对 QKD 进行了深入的技术评估，既承认其理论上的优势，更指出了实践中无法克服的局限。以下是谷歌博客原文中的核心观点。

1. QKD 的理论优势：窃听检测与无数学假设

谷歌技术专家指出，QKD 在理论上具有两个显著优势：

(1) 能够检测窃听。 量子力学的基本原理（不可克隆定理）保证：如果第三方试图窃听通信信道，测量光子的量子态会导致该态坍缩，从而被通信双方以高概率检测到。窃听者无法复制未知的量子态并转发给另一方。

(2) 不依赖数学难题假设。 当前大多数密码算法（如 RSA、ECC）属于“计算安全”，其安全性依赖于某些数学问题的难解性（如大整数分解、离散对数）。一旦这些数学难题被攻破（例如出现高效的量子算法或 P=NP 的突破），这些算法将瞬间失效。而 QKD 在理论上提供了“信息论安全”，即使攻击者拥有无限计算资源，也无法破解。

2. QKD 的现实劣势：谷歌技术专家列举的六大问题

然而，理论上的优美无法掩盖工程实践中的致命缺陷。谷歌技术专家明确指出 QKD 存在以下 6 大劣势：

(1) 缺乏认证机制（致命缺陷）

部署 QKD 的前提是，通信双方（Alice 和 Bob）必须已经拥有一个经过认证的经典信道。QKD 本身不提供任何认证手段。这意味着：要么使用非对称密码（这又回到了依赖数学难题的老路，失去了 QKD 的“无假设”优势），要么依赖预共享对称密钥（带来巨大的运营复杂度）。谷歌技术专家一针见血地指出：“如果你已经有了预共享密钥，那么使用信息论安全的认证码就足够了，何必再用 QKD？”

(2) 成本高昂且无法扩展

QKD 总是在两个端点之间进行。迁移到 QKD 需要完全替换所有网络硬件，每一个需要保护的链路两端都必须部署对应的 QKD 设备。添加任何新设备都需要与其他所有设备进行物理连接，这在大规模网络中是不可扩展的。对于谷歌这样的全球网络，“用专门的 QKD 设备替换数据中心中的现有硬件，不是一种实用或可扩展的解决方案”。端到端用户安全更是无从谈起，每个用户设备都需要与每个服务器建立直接链路，这在运营上完全不可行。

(3) 距离限制严重

所有商用 QKD 解决方案的有效距离被限制在约 100 公里以内，安全性仅在两个端点之间得到保证。要扩展距离，必须使用**可信中继**，而每个中继节点都必须被信任，这引入了极高的拦截或后门风险。对于高度分布式的网络（如谷歌的全球基础设施），迁移到 QKD 基础设施在当前看来是不可行的。自由空间密钥协商和量子中继器虽然可能解决部分问题，但在可预见的未来不会有商用产品。

(4) 吞吐量极低

当前商用 QKD 设备只能达到每秒千比特(kbps)的密钥生成速率，这使其无法用于绝大多数实际应用。虽然可以用对称密码扩展密钥材料来提高效率，但谷歌技术专家反问：“如果这样，一开始为什么要用 QKD？你再次需要依赖额外的安全假设。如果双方已经有预共享密钥，直接用该密钥派生更多密钥材料就能提供相当的安全保障。”谷歌技术专家甚至用了一个生动的比喻：以当前 QKD 的速率，一个价值不到 100 美元的 5TB 硬盘（存储随机比特）足够使用 1000 年。

(5) 仅解决密钥协商问题

QKD 只解决了密钥协商问题。在大规模基础设施中，仍然需要哈希函数、数字签名等密码原语，而这些原语的安全性仍然依赖于数学假设。因此，部署 QKD 并不能实现“对抗无界攻击者的安全性”，其实际风险降低效果令人怀疑。

(6) 实现安全性存疑

QKD 的安全性质仅对**理论协议**有保证。在实际实现中，硬件必须满足极其严格的要求。如果不满足，整个实现可以被认为完全不安全。侧信道攻击的防护在这些设备中尚未得到很好理解。测试和认证流程也不成熟。现实中，已有多种攻击成功攻破了商用 QKD 系统（谷歌技术专家在文章中引用了相关文献）。

3. 谷歌技术专家的结论：PQC + 加密敏捷性

基于上述评估，谷歌技术专家给出了明确的结论：

“我们目前认为 QKD 对谷歌的基础设施价值非常有限。QKD 解决的问题很窄，所有实际实现都有严重的局限性。QKD 的主要好处是降低数学突破影响我们当前密码算法的风险，但这种风险很小，而且由于 QKD 的诸多局限性，部署 QKD 极不可能充分应对这一风险。”

因此，谷歌**既不**在生产环境中部署 QKD，**也不**探索 QKD 与现有系统的共存。谷歌的道路是：**广泛采用 PQC 并实现加密敏捷性，**即能够在不大幅修改工程的情况下更换算法或参数集的能力。这一立场与 NSA、NCSC、BSI 等多家国家安全机构的建议完全一致。

三、国际权威机构的共识：PQC 优先，QKD 不适用

谷歌技术专家在博文中引用了多家国家级安全机构的立场：

- **美国 NSA**：优先采用 PQC 而非 QKD
- **英国 NCSC**：明确认为 QKD 不适合政府或军事应用
- **德国 BSI**：同样建议优先发展 PQC
- **法国 ANSSI、荷兰 NCSA 等**：联合立场文件支持 PQC

这些机构的一致判断是：QKD 的理论优势在实践中难以兑现，而 PQC 可以运行在经典硬件上，具备可扩展性、可管理性和加密敏捷性，是应对量子威胁的主要手段。

四、我国的战略选择：大力发展国密混合 PQC

面对谷歌技术专家和国际权威机构的明确结论，我国应该做出怎样的战略选择？答案已经

清晰：**大力发展 PQC，并以“国密混合 PQC”为战略路径，为平滑迁移至国产 PQC 算法做好战略储备。**

1. 为什么不能只做国密改造？

我国在密码领域取得了显著成就，国产密码算法体系（SM2/SM3/SM4）实现了技术自主可控。然而，一个严峻的事实是：包括 SM2 在内的当前所有公钥密码算法，在未来的量子计算机面前都显得非常脆弱。仅满足于完成国密改造，无异于为数字大厦安装了自主设计的门锁，却忽略了有人正在打造能熔化所有金属的火焰。

2. 为什么不能只采用国际 PQC？

目前全球互联网流量中的 68%已经实现了国际混合 PQC 算法（X25519MLKEM768）HTTPS 加密保护，但是如果我国也仅采用国际 PQC 混合方案，理论上能抵御量子威胁，但它将核心安全命脉再次系于他人制定的标准之上。在最终的国际 PQC 算法与我国 PQC 算法标准博弈未定之时，全面押注单一外部技术路线，将失去战略主动权，并可能在未来面临二次改造的巨额成本与安全风险。

3. 国密混合 PQC：最佳战略路径

最明智的战略路径是：**全面普及并优先采用“国密 SM2 与国际 PQC 算法 ML-KEM-768 的混合算法 SM2MLKEM768”**，以此构建面向未来的核心战略储备。

这一方案具备多重战略价值：

(1) **双重安全**：融合中国自主 SM2 密码技术与国际抗量子算法，形成“双重安全”防线；

(2) **全球互认**：此算法已获得国际号码分配机构 IANA 授予的官方编号 **4590**，意味着该方案已被纳入全球互联网的基础协议体系，成为可全球互认的通行信号；

(3) **平滑过渡**：在国产 PQC 标准尚未正式出台之前，为未来平滑迁移至国产 PQC 算法提供关键战略储备；

(4) **应对即时威胁**：标准制定是需要时间的，但是数据安全等不起，我国应该立即大力推广国密混合 PQC，以应对已存在的“先收集后解密”威胁，保障关基数据在量子时代的持续安全。

五、国密混合 PQC 生态已完整成熟

值得骄傲的是，支持 SM2MLKEM768 的国密混合 PQC 方案的完整国产技术产品线已经成熟落地，为大规模部署提供了坚实可靠的实施基础。

1. 底层密码库：铜锁 SSL

蚂蚁集团旗下的铜锁 SSL（Tongsuo）开源密码库，作为国产密码技术的基石，已率先实现并开源了 SM2MLKEM768 混合密钥交换算法。在 3 月 23 日发布的 Tongsuo 8.5.0-pre1 版本中，铜锁 SSL 全面支持国际 PQC 算法（ML-KEM、ML-DSA 和 SLH-DSA），同时支持双 PQC 密钥协商机制 SM2MLKEM768 和 X25519MLKEM768。铜锁为整个生态提供了核心密码学能力，使开发者能够基于这一开源密码库构建支持国密混合 PQC 的应用。

2. 客户端：零信浏览器

零信浏览器已于 2025 年 12 月 12 日发布了 V2601 版本，成为全球首个支持 SM2MLKEM768 国密混合 PQC 算法 HTTPS 加密的客户端。其地址栏能同时向用户直观展示代表量子安全的“**Q**”标识和代表国密合规的“**m**”标识。零信浏览器优先采用国密混合 PQC 算法实现 HTTPS 加密，国内强制国密，海外完美兼容，为后量子密码迁移提供了坚实的客户端支持。

3. 服务端：零信 HTTPS 加密自动化网关

零信 HTTPS 加密自动化网关为企业端部署提供了便捷的、原生 Web 服务器零改造的、支持证书自动化的后量子密码迁移解决方案。网关自适应支持混合 PQC/SM2/ECC/RSA 四种算法，能根据客户端能力自动选择最优加密方案，实现从国密合规到量子安全的一次性平滑升级与证书自动化管理。

4. 国际开源密码库：OpenSSL

OpenSSL 开发团队在 2 月 21 日已完成 Issue #1855 (支持 TLS 1.3 商密算法和商密混合 PQC 算法)的代码开发、审核和测试工作，预计不久的将来 OpenSSL 正式版本也会支持 SM2MLKEM768，这将为全球范围的生态支持又近了一大步。

5. Java 生态：Bouncy Castle 已经支持

在国际 IETF 第 125 届大会上，有国际厂商代表明确表示将尽快在其维护的 Java 平台开源

密码库 Bouncy Castle 中支持 SM2MLKEM768，推动该算法在 Java 生态中落地。最新的情况是已经完成 1.84 版本的正式支持，就待官方发布新闻了。

6. 国际标准推动：IETF 草案进展

由我国密码团队主导的《TLS 1.3 商密混合 PQC 算法》RFC 草案已在 IETF 积极推动。在深圳举办的 IETF 第 125 届大会上，零信技术成功主持了专题研讨会，向全球展示了 SM2MLKEM768 算法的完整生态系统，获得了国际同行的广泛关注和认可。

六、时不我待，加速部署

谷歌技术专家在博文最后写道：“我们致力于确保用户和客户当前及未来的安全。我们认为，后量子密码与加密敏捷性的结合是应对量子计算机威胁最有效、可扩展的方式。”这一判断得到了全球多家国家级安全机构的背书。

而在我国，支持国密混合 PQC 的完整技术生态已经就绪，从铜锁 SSL 到零信浏览器，从零信 HTTPS 加密自动化网关到 IETF 标准草案。现在需要的是决心和快速行动。

量子倒计时的钟声已经敲响。全球超过 68%的互联网流量已启用混合 PQC 算法 HTTPS 加密，欧美关基系统已大规模部署 PQC。我国不应该在 QKD 这条窄路上徘徊，正如谷歌技术专家所说，QKD 解决的问题很窄，所有实际实现都有严重局限，不适合大规模基础设施。

正确的选择是：**大力发展国密混合 PQC，以 SM2MLKEM768 为战略储备，以证书自动化降低迁移门槛，为数字中国构筑量子时代的安全基石。**

王高华

2026 年 4 月 17 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 270 篇(共 79 万 9 千多字)和英文 119 篇(16 万 6 千多单词)。