普及国密混合 PQC：为平滑迁移至国产 PQC 算法做好战略储备

2026 年 2 月 25 日

一场静默但决定性的全球安全升级竞赛正在进行。根据行业监测，全球超过 65%的互联网流量已启用能抵御量子计算攻击的“后量子密码（PQC）HTTPS 加密”。与此同时，另一个关乎未来十年数字主权的竞争也在标准制定层面展开：我国密码团队提出的“国密 SM2+国际 PQC”混合算法方案，已正式获得国际互联网号码分配机构（IANA）授予的官方编号 4590。

这并非一个遥远的技术话题。它意味着，一套融合了中国自主密码技术与国际抗量子算法的“双重安全”方案，已被纳入全球互联网的基础协议体系，成为浏览器、服务器和设备间可全球互认的“通行信号”。对我国互联网安全而言，这揭示了一条清晰的战略路径：我国必须马上开始全面部署国密混合 PQC 算法 SM2MLKEM768。这不仅是应对“量子威胁”的盾牌，更是为平滑、无感地迁移至未来国产 PQC 算法所做的关键战略储备。

一、现状反思：为什么“完成国密改造”和“采用国际 PQC”都非终极方案？

首先，我们必须对我国在密码领域取得的成就——国产密码算法体系（SM2/SM3/SM4）——报以最高的敬意。完成国密改造，是实现技术自主可控的关键一步。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，无异于为我们的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。

但是，为了应对已经存在的“先收集后解密”安全威胁，保障我国关基数据在量子时代的持续安全，就必须马上采用混合 PQC 算法。那么，是直接采用国际标准的 PQC 混合方案（如 X25519MLKEM768）还是一直等到我国后量子密码算法出台呢？显然不能等。而如果仅采用国际混合 PQC 方案，理论上确实能抵御量子威胁，但它将我们核心的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，将让我们失去战略主动权，并可能在未来面临二次改造的巨额成本与安全风险。

二、战略路径：以“国密混合 PQC”构建战略储备，赢得平滑迁移主动权

最明智的、必须立即采取的战略路径是：全面普及并优先采用“国密 SM2 与国际 PQC 算法 MLKEM768 的混合算法 SM2MLKEM768，以此构建面向未来的核心战略储备。

这绝非纸上谈兵或远景规划，值得特别强调的是，从底层密码库到终端应用，支持这一战略的完整国产技术产品线已经成熟落地，为我们提供了坚实可靠的实施基础。**阿里铜锁 SSL** 开源密码库作为国产密码技术的基石，率先实现并开源了 SM2 算法与国际 PQC 算法 MLKEM768 的混合密钥交换算法-SM2MLKEM768，为整个生态提供了核心密码学能力。在此基础之上，**零信浏览器**已成为全球首个支持 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。而在服务器端，**零信 HTTPS 加密自动化网关**可与之无缝协同，为网站提供一键式支持，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。

这条从基础算法、客户端到服务端的完整产品链，确保了“国密混合 PQC”方案已具备大规模部署的成熟条件。它让我们今天的战略储备，拥有了可立即落地的技术载体。这一战略储备的核心价值体现在：

(1) **构建当下的“安全与能力”双重储备**：在每次 HTTPS 连接中，系统将同时运行 SM2 和 MLKEM768 两套密钥交换算法。只要其中任何一套算法是安全的，整个通信连接就牢不可破。这既为我国互联网数据储备了当下的“双重安全”，也为我国储备了运营下一代加密系统的实战能力。更重要的是，我们有现成的国产工具链来实现它，将能力储备落到实处。

(2) **储备宝贵的“实战经验与数据”**：通过利用现有成熟产品大规模应用 SM2MLKEM768，关基单位的技术团队将在真实业务压力下，提前掌握后量子时代加密系统的运维、故障排查和性能调优能力。这些在真实战场上积累的经验与数据，是任何模拟测试都无法获取的、最具价值的战术储备。

(3) **储备决定性的“无缝切换基础设施”**：这是此战略储备最核心的一环。今天基于成熟产品线进行部署，不仅仅是在应用一个算法，更是在建设和固化一套支持密码算法敏捷替换的基础设施和能力框架。这套框架，就是我国未来实现“平滑迁移”的核心基础设施储备。当我国自主 PQC 算法标准正式出台时，无需再次伤筋动骨地进行全网改造，而是可以依托现有框架，像升级标准件一样，平滑、无感地将混合 PQC 模式中的 MLKEM768 算法替换为国产 PQC 算法，最终形成“SM2+国产 PQC”的混合自主安全形态，直至最终的纯国产 PQC 算法完成平滑无缝迁移。今天的部署，是为明天的终极迁移储备了最关键的“转换器”和“高速公路”。

三、关键支撑：SM2MLKEM768 的国际标准地位——编号 4590

选择 SM2MLKEM768 作为战略储备的核心技术，并非权宜之计，而是在采纳一项已获得国际权威组织背书的成熟资产。国际互联网号码分配机构（IANA）是管理全球互联网核心协议参数的顶级权威，其为“SM2MLKEM768”混合算法分配的专用编号 4590，是一个具有分水岭意义的里程碑。这标志着：

(1) **资产权威性**：该方案的设计获得了国际标准组织的技术认可，是具备长期互操作价值的标准化资产。

(2) **生态通行证**：IANA 编号确保了该协议能在全球遵循同一标准的网络中无障碍通行，避免了私有方案可能带来的“资产孤岛”风险，保障了我国战略储备的广泛适用性。

(3) **战略主动权**：这是在由国际主导的后量子密码过渡方案中，成功纳入“中国方案”的关键一步。它为我国在量子时代的国际标准制定中储备了话语权资产，也为未来国产 PQC 算法升级铺平了国际接轨的道路。

因此，部署获得 IANA 编号 4590、且有完整国产产品线支撑的 SM2MLKEM768，不仅是关基运营单位当下务实、高效的安全决策，更是在为关基运营单位的未来系统性地储备关键的技术资产与基础设施。

四、行动呼吁：将战略储备转化为核心竞争优势

现在，网络安全和数据安全已从成本中心演进为竞争力乃至生存力的核心。当成熟的混合 PQC 产品链已经铺就，国际的通行证已经获取，等待就是最大的风险。所以，零信技术呼吁：

(1) **立即启动能力储备计划**：要求组织的技术团队立即利用现有的铜锁 SSL、零信浏览器、零信 HTTPS 加密自动化网关等成熟产品，对核心业务系统进行 SM2MLKEM768 混合加密的兼容性测试与试点部署，并将此过程定义为关键的“未来安全能力储备项目”，尽快形成全面部署路线图。

(2) **将“可平滑迁移”纳入采购核心标准**：在未来的所有 IT 基础设施、云服务及安全产品采购中，必须将“支持 TLS 1.3 协议的国密混合 PQC 算法（SM2MLKEM768）及未来向国产 PQC 算法的平滑迁移能力”作为不可妥协的技术门槛。确保每一次采购，都是向未来安全架构的一次投资和储备。

(3) **一次投资，储备多重战略价值**：正如成熟产品所验证的，一次正确的技改，可以同步、高效地完成“国密合规改造”、“证书自动化改造”和“后量子密码迁移”三大刚需任务的战略储备。这是一项能够立即执行、并为未来节省巨大成本的战略性投资。

量子计算的威胁倒计时已然响起，而国家间技术主导权的竞争也日趋激烈。此刻，选择由完整国产产品线支撑的“国密混合 PQC”道路，并系统性地将其转化为核心战略储备，是每一个关基运营单位为保障组织的长治久安、掌握升级主动权所必须履行的责任。这更是一条已经铺就的、能将当下投资转化为未来优势的务实道路。

让我们行动起来，将技术资产、实战经验和基础设施的储备，转化为无可替代的核心竞争优势。**今日之储备，决定未来之疆域。新春伊始，此时不进，更待何时？全面进发才是真！**

王高华

2026 年 2 月 25 日于深圳
