后量子密码是下一个网络安全产业制高点

笔者在博文《美英法政府门户网站已启用后量子密码 HTTPS 加密》的最后一段抛出了本文标题这个观点，受到了大量的反馈。笔者认为有必要专门针对这个话题写一篇文章，展开阐述一下这个观点，抛砖引玉，以期待业界达成共识，共同努力拿下这个产业制高点。

一、量子计算带来的“断崖式”安全威胁

当前全球网络安全和数字经济所依赖的公钥密码体系(RSA、ECC、SM2)的安全性是基于某些数学难题的“计算复杂性”，例如大整数分解和离散对数问题。然而，Shor 算法等量子算法证明，一旦量子计算机问世，这些数学难题将被秒破，这意味着现有的数字签名、密钥交换等安全机制将彻底失效，现在已经加密的所有机密信息都会成为明文信息。

这种威胁不是渐进式的，而是**“断崖式”** 的。它威胁到的不仅是个人隐私，更是国家安全、金融体系、关键基础设施（电网、水坝、交通）的根基。因此，研发能够抵抗量子计算攻击的新一代密码技术—**后量子密码** (Post Quantum Cryptography, **PQC**) 已成为全球共识。这绝非简单的技术升级，而是一场关乎未来网络空间主导权的战略争夺，是制高点。

二、为什么说后量子密码是“制高点”？

这绝对不是危言耸听和哗众取宠！“制高点”意味着具有全局性、战略性的控制地位。后量子密码符合制高点的所有特征，具体体现在以下 3 个方面：

1. 基础性与全局性

密码是网络空间安全的“基石”，几乎所有数字交互都建立在密码之上。更换密码算法是一项极其复杂、昂贵且漫长的系统性工程，涉及硬件(芯片、设备)、软件(操作系统、浏览器、应用软件)、协议(TLS、SSH)、标准和组织流程的全栈更新。

谁掌握了下一代密码标准，谁就事实上制定了未来数十年全球数字安全的“游戏规则”，其影响深度和广度无与伦比。现在是 RSA 国际密码体系在保障全球网络空间安全，鉴于地缘政治原因，我国网空安全必须有自己的密码体系，这就是目前正在如火如荼进行中的商用密码改

造，要把整个生态改造支持商用密码体系。但是，SM2 算法在量子时代也是不安全的密码算法，必须尽快制定我国自己的后量子密码算法(新一代商用密码算法)，不仅有力保障我国网空安全，而且为保障全球互联网安全提供中国方案。

2. 国家安全与战略自主

无论现在采用的是国际密码体系还是商用密码体系，都存在“先收集后解密”的数据安全威胁，攻击者现在就已经开始收集加密数据，等到量子计算机问世后再进行解密，所有数据在量子时代都成为了明文数据，这个时间点是 2030 年，这就要求必须马上迁移到 PQC，具有极端紧迫性。

(1) **技术主权**：依赖国外（尤其是战略竞争对手）的 PQC 技术和标准，将使本国在数字时代处于危险的境地。自主可控的 PQC 能力是未来国家网络主权的核心组成部分。

(2) **军事与情报优势**：军队和情报机构是密码技术的最大使用者之一。拥有更安全、更高效的 PQC 方案，意味着在未来的量子时代享有绝对的通信和安全优势。

3. 巨大的经济产业价值

后量子密码迁移是一个所有系统都必须实施的刚需，将带来巨大的经济产业价值，具体体现在如下三个方面：

(1) **市场规模巨大**：全球所有联网设备、软件和服务都需要升级或集成 PQC 功能。这将催生一个价值数千亿美元的新兴市场，涵盖芯片、安全模块、硬件产品、软件产品、咨询、迁移服务和合规认证等。

(2) **产业链带动效应**：从底层的半导体（需要支持 PQC 算法的指令集和协处理器）、到中间的网络安全产品（防火墙、VPN、HSM、网关），再到顶层的云服务和应用程序，整个产业链都将被重塑和激活。

(3) **先发优势与标准红利**：主导国际标准（如 NIST 遴选）的企业和机构，将通过专利许可、技术方案和生态建设获得巨大的商业回报和行业领导地位。

4. 技术领先的标志

后量子密码是数学、计算机科学和工程学的深度交叉领域。能否提出优秀、安全、高效的 PQC 方案，是一个国家或公司基础科研实力和工程化能力的试金石。在 PQC 领域的领先，也代表着在更广阔的量子科技竞赛中占据了有利位置，为未来“量子互联网”等更前沿的布局打下基础。

三、 后量子密码主要参与者与竞争格局

就国家层面来讲，美国在后量子密码已经是绝对领先者。通过 NIST 主导标准制定，拥有最强的科技公司集群（谷歌, 微软, IBM, 亚马逊等）和科研实力。政府层面推动力度极大（如总统行政令要求联邦机构向 PQC 迁移）。

中国在量子密钥分发(QKD)处于领先地位，但是在后量子密码则是积极追赶者，量子科技（包括 PQC）已列为国家战略重点。中国密码学界在 NIST 标准进程中表现活跃，提交了多个 PQC 方案，也正在推动制定中国自己的 PQC 算法标准，产业界包括零信技术也正在推动商用密码和 PQC 的混合算法应用。市场潜力巨大，政府主导力强（如《密码法》等相关法律和规定）。

欧盟也是后量子密码的重要力量。拥有深厚的数学和密码学底蕴（如法国、荷兰、德国），在 NIST 中有多项方案入选最终轮。通过《网络安全法案》等政策推动 PQC 发展，强调“数字主权”。其他国家和地区，如日本、韩国等也在积极布局，力争在特定领域或市场占据一席之地。

最值得注意的是美国科技巨头与初创企业，所有科技巨头都在推动 PQC 标准制定和落地应用，如谷歌、苹果、Cloudflare 等。而一批专注于 PQC 的初创公司（如 Isara, PQShield）已经成为被收购或合作的对象。

四、面临的挑战与不确定性

要想夺取制高点，当然不会是一帆风顺的事情，面临各种挑战和不确定性，具体体现在如下 4 个方面：

(1) **技术成熟度**：PQC 算法普遍比现有算法更慢、更大（密钥和签名更长）。在资源受限的物联网（IoT）设备上实现难度大。其长期安全性也仍需长时间的持续检验。

(2) **迁移的复杂性与成本**：全球数字生态系统的 PQC 迁移将是一个持续 10-15 年的漫长过程，协调成本极高，且存在新旧系统兼容的巨大挑战。

(3) **“窗口期”的紧迫性**：虽然不确定量子计算机何时到来，但“先收集后解密”的安全已经存在，这就要求现在就要普及应用后量子密码 HTTPS 加密，而不是等到 2030 年完成 PQC 迁移。这是一场与时间的赛跑。

(4) **标准不统一的风险**：如果未来出现美国、中国、欧盟等多套标准并存的“碎片化”局面，将增加全球互联互通的复杂性和成本。

五、决胜未来网络空间的“核武器”

综上所述，后量子密码绝非一次普通的技术迭代，而是重构网络空间安全基座、决定未来数字世界格局的战略性技术。它集基础性、战略性、经济性和时代性于一身，完全符合“产业制高点”的定义。

对于国家层面而言，掌握 PQC 意味着保障了未来的国家安全和战略自主；对于产业层面而言，率先布局 PQC 意味着抓住了下一代网络安全市场的命脉，占据了价值链的顶端；对于整个社会而言，平稳过渡到 PQC 是抵御“量子世界”未知风险、保障数字经济持续繁荣的基石。

因此，无论是从国家战略还是产业发展视角，都必须以前所未有的重视程度和资源投入，全力抢占后量子密码这一至关重要的制高点。这场竞赛的结果，将深远影响未来几十年的全球网络安全格局。

王高华

2025 年 9 月 29 日于深圳
