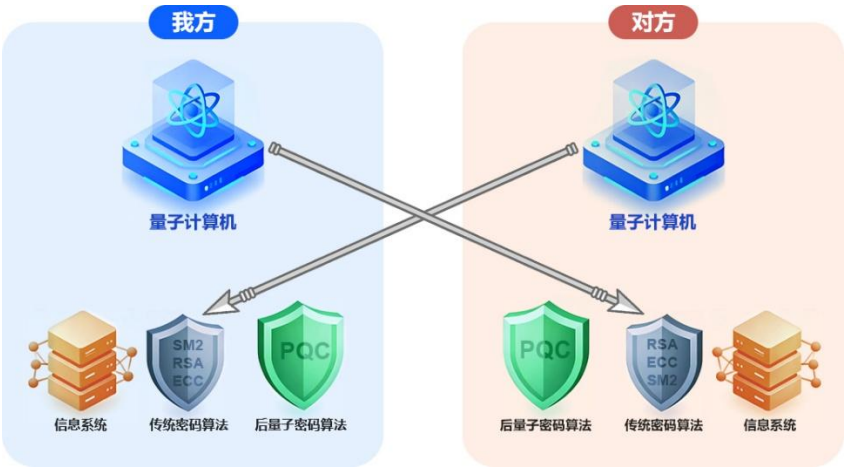
量子计算机与后量子密码：磨砺利矛与铸牢坚盾

2025 年 10 月 27 日

在现代数字时代，密码体系是保障网络空间安全和数据安全的基石。然而，随着量子计算技术的迅猛发展，这一基石正面临被颠覆的威胁。据可靠预测，到 2030 年，足够破解当前密码体系的量子计算机有超过 50%的概率出现，这意味着今天被加密的所有机密数据，都可能在未来某个时刻被轻易破解，这就是**“先收集后解密”**安全威胁，而解决这一威胁的唯一可靠技术就是后量子密码。本文讲一讲这两者的“矛”与“盾”的关系，重点论述我国必须加强“盾”的建设。

一、 新说“矛”“盾”：可同世而立

《韩非子 · 难一》载：“夫不可陷之盾与无不陷之矛，不可同世而立。” 然而，在当今的数字安全领域，我们却必须追求“矛”之利与“盾”之坚的统一。量子计算机正是那把能刺穿传统密码体系的“无不陷之矛”，而后量子密码则是那面必须铸就的“不可陷之盾”，这个统一并不矛盾，因为这个量子计算机的“矛”是用于攻击对方的传统密码体系的，而这个后量子密码的“盾”是用于防止对方用量子计算机的“矛”来攻击我方的传统密码体系的，“矛”和“盾”针对的都是对方的传统密码体系，而不是“矛”“盾”双方。



但是，我国在量子科技领域的投入明显严重偏向于量子计算这一"攻击之矛"，而对后量子密码这一"防御之盾"的重视严重不足。根据调研数据，仅 2023 年我国在量子计算领域的直接投资超过 150 亿元，而在后量子密码领域的直接投资非常少，这种严重的战略失衡正在累积成为巨大的国家安全风险，非常值得高度重视。

二、"盾"的缺失：系统性安全代差正在形成

后量子密码的紧迫性建立在严密的数学论证基础上。Shor 算法能够在多项式时间内解决大整数分解问题，这意味着当量子计算机达到足够规模时，RSA/ECC 公钥密码算法将被秒破，这一安全威胁同样存在于基于椭圆曲线的国产密码算法(SM2)。也就是说，即使我国现在已经完成了所有系统的国密改造，一样存在“先收集后解密”安全威胁。

正是基于后量子密码的紧迫性，美国率先发布了后量子密码算法标准，美国互联网巨头和浏览器巨头都迅速行动起来，美国政府网站、政务系统、网银系统、主要互联网服务系统和高校网站都纷纷启用了后量子密码 HTTPS 加密，在不到一年的时间内使得全球近半数的互联网流量已启用后量子密码 HTTPS 加密，这就是在快速铸造“防御之盾”。而我国的互联网流量仍处于完全依赖传统密码算法加密，我国在后量子密码应用-也就是“盾”的铸造方面已经严重滞后，并已经形成明显的安全代差。

这种滞后主要体现在三个层面：首先，在标准制定方面，美国在 2024 年 8 月发布了首批后量子密码标准，而我国后量子密码算法标准才刚刚开始征集；其次，在产业支撑方面，国内没有一家互联网巨头能像亚马逊和 Cloudflare 那样免费为其用户升级支持后量子密码 HTTPS 加密，能够提供完整后量子密码解决方案的企业屈指可数；最后，在实践应用方面，除少数试点项目外，我国关键信息基础设施尚未启动系统的后量子迁移计划，没有一个政府网站、政务系统、网银系统、互联网服务系统等关键信息基础设施系统实现了后量子密码 HTTPS 加密。

三、　信任基石：数字签名体系面临重构

相比 HTTPS 数据传输加密，数字签名机制的安全危机更为深远。研究表明，当前使用的 RSA/ECC/SM2 数字签名算法在量子计算环境下完全失效。这意味着：首先，金融领域的数字签名验证机制将形同虚设。研究表明，一个具备 4000 个量子比特的计算机就足以在一天内伪造数以万计的金融交易数字签名。其次，电子合同和电子公文的法律效力将面临根本性崩溃。因为基于传统密码算法的数字签名一旦被破解，其不可否认性将不复存在，电子合同和电子公文的法律效力也将不复存在，其灾难性后果也是不可想象的。

还有基于传统密码算法的安全认证体系，一样是依赖数字签名的不可否认性，一样面临被假冒身份签名而面临根本性的崩溃。这些都需要重新采用后量子密码算法实现数字签名和验签，数字签名体系急需重构。

四、 铸盾之路：系统性推进四维建设

既然我们认识到了我国铸建“防御之盾”的差距，那就需要赶紧行动起来，抓紧追赶，快速缩短差距。后量子密码属于新一代商用密码算法，我国现有成熟的商用密码改造体系，包括法律、技术和人才都将是快速推进后量子密码普及应用的利器，可以从以下四个方面推进铸建“防御之盾”。

1. 完善标准体系架构

亟需加快建立后量子密码国家标准体系。建议在现有商用密码标准框架下，加快推进后量子密码相关标准的研制和发布，为产业应用提供技术依据。

2. 分领域实施合规改造

按照网络安全等级保护制度要求，应当优先在第三级及以上信息系统中实现后量子密码 HTTPS 加密，可以同商用密码改造同步完成。采取"重点先行、分步推进"的策略，首先在政务、金融、能源等关键领域开展示范应用，不仅要尽快实现后量子密码 HTTPS 加密，而且还需要尽快实现后量子密码数字签名。可以先实现美国标准的 PQC 算法 HTTPS 加密，即刻保障关键数据在量子时代的安全，后续我国 PQC 算法标准出台后就可以快速替换。

3. 构建密码敏捷体系

在新系统设计中应贯彻“密码敏捷原则“，为未来密码算法升级预留灵活性。在 HTTPS 加密实现方面，最佳方案是一次改造同时完成证书自动化改造、商用密码改造和后量子密码改造。研究表明，具备良好密码敏捷性的系统在后量子迁移时的成本可降低 70%以上。

4. 强化产业生态培育

在量子科技产业政策引导下，需要加快培育从密码芯片、安全设备到系统应用的后量子密码完整产业链，还需包括后量子密码人才培养。尤其是急需实施的后量子密码 HTTPS 加密，不仅需要国产浏览器的支持，还需国产 Web 服务器和所有 SSL 网关产品的支持，更需要 CDN/WAF 等互联网服务的支持。这是一个产业生态的全面升级，需要国内互联网巨头以前所未有的重视程度和资源投入，共同全力拿下后量子密码这一至关重要的制高点。

五、 坚持“矛利盾坚”战略思想，同步推进两项技术发展

古人论“矛”与“盾”，意在揭示逻辑矛盾；今日论量子计算机与后量子密码，则是要把握对立统一的辩证法则。在国家安全层面，我们既要重视“矛”的研发，以免在计算革命中落后；同时更不能忽视“盾”的建设，以免在量子攻击面前门户大开。这不仅仅是一场技术竞赛，更是一

场关乎国家安全的战略博弈。只有坚持“矛利盾坚”的战略思想，同步推进量子计算机和后量子密码的技术发展，才能在新一代技术革命中掌握主动权，筑牢数字中国的安全防线。

笔者呼吁各方共同努力，在相关量子科技和商用密码政策指引下加快推进后量子密码技术的研发和应用，切实筑牢国家网络安全的坚固底座。只有在"盾"的建设上取得实质性突破，我国才能在这场与量子计算赛跑的安全竞赛中赢得主动，切实保障数字时代的国家安全。

王高华

2025 年 10 月 27 日于深圳