

卷首语

抗量子计算密码迁移：认识与思考

实用的密码技术与计算能力密切相关,随着计算技术的发展,密码技术从适应于手工计算的古典密码,到适应于机械计算的机械密码,再到适应于电子计算的现代密码不断演化和发展。今天,计算技术迎来量子计算时代,不得不发展适应于量子计算的密码技术,人们把这种密码称为抗量子计算密码,也称为后量子密码(post-quantum cryptography, PQC)。密码应用无处不在,要将传统密码替换为 PQC 不是一件容易的事情,是一个复杂工程、系统工程,先前的历史,例如从 DES (Data Encryption Standard) 到 AES (Advanced Encryption Standard)、从 RSA (Rivest-Shamir-Adleman) 到 ECC (Elliptic Curves Cryptography),表明它也是一个耗时工程,需要 10 年或更长的时间。国际上将其称为 PQC 迁移。PQC 迁移不仅是密码的迁移,而且是信息技术的迁移。我们要高度重视这项工程,深刻认识其重大意义。

1 PQC 迁移是一项国家战略工程

PQC 迁移涉及面极广,不仅涉及政府机构、行业应用部门、学术界和工业界等,也涉及政策法规、标准、技术、产品和测评等,这就需要从国家层面进行顶层设计和推动。美国、欧盟等国家和组织都从顶层进行设计和部署,并积极

密码是网络与信息安全的基因即 DNA,密码这个基因从传统密码升级为 PQC,必然要求重塑信息安全(当然也包括网络空间安全、数据安全等)体系,PQC 迁移加速了这一重塑进程。

推进 PQC 迁移法规和指导性文件的制定以指导、规范和简化 PQC 迁移工作。例如,美国国家标准技术研究院下属的国家网络安全卓越中心于 2023 年 12 月发布了指导性文件《向抗量子计算密码迁移》(Migration to post-quantum cryptography),美国总统特朗普于 2026 年 6 月 22 日签署了行政令《保护国家免受高级密码攻击》(Securing the nation against advanced cryptographic attacks);欧盟委员会于 2025 年 6 月发布了《关于向抗量子计算密码迁移协同实施路线图的建议》(A coordinated implementation roadmap for the transition to post-quantum cryptography)。同时,PQC 迁移还要积极推进国际合作和行业合作与协同。

2 PQC 迁移牵引密码创新发展

PQC 迁移需要新理论和新技术支撑。首先,基础理论和设计方法需要不断创新,包括底层困难问题的深入刻画与挖掘,安全模型与安全性定义等;新的设计范式、思想与理念,如低通信量抗量子计算密码、非结构格数字签名;高效的算法、协议和方案等的创新设计。其次,高效能实现需要不断优化和突破,包括软硬件快速实现方法与技术,以及基础算法的优化实现方法等。再次,测评分析方法与工具需要不断发



冯登国
中国科学院院士
网络与信息安全专家

现任中国科学院软件研究所研究员。研究方向为网络与信息安全、数据安全和隐私保护、可信计算与机密计算。

中国科学院软件研究所,北京 100190

展和完善,包括数学问题的量子复杂度模型和评估方法,科学、系统的分析评估方法及自动化智能化工具,如实际环境中的攻击、侧信道攻击,发现和评估抗量子计算密码应用情况的自动化工具等。最后,迁移方法需要不断拓展和创新,包括科学、合理的迁移方法和策略,以及密码敏捷性等。

3 PQC 迁移加速信息安全体系重塑

密码是网络与信息安全的基因即 DNA,密码这个基因从传统密码升级为 PQC,必然要求重塑信息安全(当然也包括网络空间安全、数据安全等)体系,PQC 迁移加速了这一重塑进程。重塑内容包括政策法规和指导性文件、基础理论与关键技术、基础设施(如 PKI(Public Key Infrastructure)、RPKI(Resource Public Key Infra-

structure))、算法和协议、标准、产品、应用和测评等多个方面。

4 PQC 迁移带动信息技术产品升级换代

PQC 迁移不仅是密码的迁移,而且是信息技术的迁移,因此,必将带动信息技术产品升级换代,从而推动网络和信息系统的迭代发展。PQC 尤其是抗量子计算公钥密码的密钥生成速度比较慢、密钥/签名规模比较大、处理过程比较复杂,难以像现用密码那样与计算机和通信相关软硬件、应用程序、通信协议、访问控制机制和关键信息基础设施相匹配,因此,需要从代码、软硬件模块、设备、操作系统、数据库、应用、协议、测评工具等实现 PQC 的全方位更新;推进在信息技术产品、协议和服务中采用 PQC,推动信息技术产品和服务转型;推动

标准化组织、产品供应商、服务提供商、检测认证机构等协同发展。

5 PQC 迁移促进密码复合型人才培养

PQC 迁移涉及密码、计算机、通信、网络、微电子、工程管理等多门学科,亟需一批懂密码、懂信息技术、懂工程的复合型人才,因此,需要通过国家政策引导和意识培养,让全社会认识到培养密码复合型人才的重要性;通过对国家、社会和行业的精准需求分析,凝练出人才培养类别及需求结构;科学、合理设置课程,编写理论与实践紧密结合的高质量教材;鼓励各行各业为密码复合型人才提供实践锻炼机会。不仅要加强高质量密码专业人才培养,而且要积极推动“密码+专业或行业”和“专业或行业+密码”人才培养。