DOI 10.15302/J-SSCAE-2025.11.014

抗量子公钥密码技术的现状、挑战与应对

朱桂桢*，吴江，范爱兵，施焕生，李鸿利，于宗文

（数据通信科学技术研究所，北京 100191）

摘要：密码作为保障国家信息安全、数字经济健康发展的核心战略资源，是维护关键基础设施、政务数据、金融交易等领域安全的核心防线。当前，量子计算技术快速发展对现有公钥密码体系带来颠覆性挑战，对全球信息安全格局构成致命威胁，开展抗量子公钥密码技术的研究与部署必要且紧迫。本文详细阐述了抗量子公钥密码中格、编码、杂凑签名、多量、同源5条主流技术路线的发展现状，并发现5条技术路线各有侧重但都处于持续迭代与验证阶段。研究发现，抗量子公钥密码技术发展存在的主要问题包括性能瓶颈、生态兼容性差以及安全评估困难等，我国抗量子公钥密码发展面临理论研究基础薄弱、标准制定滞后、产业生态不完善以及人才短缺等挑战。为保障我国在量子计算时代的信息安全，研究建议，加强基础研究、提升自主创新能力，加速标准制定、提升国际话语权，完善产业生态、推动抗量子分阶段迁移，强化人才培养，打造专业人才队伍，助力我国构建起多维度、强韧性的数字安全新生态，推动我国网络空间安全能力实现从经典安全向量子安全的能力跃升。

关键词：抗量子公钥密码；格；编码；杂凑签名；多变量；同源

中图分类号：TN918.2　**文献标识码：**A

Research Status, Challenges, and Future Development of Post-Quantum Cryptography

Zhu Guizhen*, Wu Jiang, Fan Aibing, Shi Huansheng, Li Hongli, Yu Zongwen

(Data Communication Science and Technology Research Institute, Beijing 100191, China)

Abstract: As an important strategic resource for safeguarding national information security and the healthy development of digital economy, cryptography is the cornerstone of protecting the security of critical infrastructure, government affairs data, financial transactions, and other fields. Currently, the rapid development of quantum computing poses a disruptive challenge to the existing public-key cryptosystems and a fatal threat to the global information security landscape, making research on post-quantum public-key cryptography (PQC) both necessary and urgent. This study expounds on the current development status of five mainstream technical routes in PQC: lattice-based, code-based, hash-based signature, multivariate, and isogeny-based cryptography, and finds that each of these five routes has its own focus yet is in a stage of continuous iteration and verification. The study identifies the existing issues of the development of PQC including performance bottlenecks, insufficient ecological compatibility, and difficulties in security evaluation. Meanwhile, the development of PQC in China is confronted with challenges such as a weak foundation in theoretical research, lagging standards formulation, an imperfect industrial ecosystem, and a shortage of professional talents. To safeguard China's information security in the quantum computing era, we propose the following suggestions: strengthening basic research to enhance the independent innovation capability of the industry; accelerating standards formulation to boost international discourse

收稿日期：2025-11-13；**修回日期：**2025-12-26

通讯作者：*朱桂桢，数据通信科学技术研究所正高级工程师，研究方向为抗量子密码；E-mail: zhuguizhen.2008@tsinghhua.org.cn

资助项目：中国工程院咨询项目“网络空间安全新技术新应用风险研究”(2023-JB-13)

本刊网址：sscae.engineering.org.cn

power; improving the industrial ecosystem to promote the phased migration to PQC; intensifying talent cultivation to build a professional talent team. These measures are expected to help China construct a multi-dimensional and highly resilient digital security ecosystem, and drive the leap-forward development of China's cyberspace security capability from classical to quantum security.
Keywords: post-quantum cryptography; lattice-based cryptography; code-based cryptography; hash-based signature; multivariate cryptography; isogeny-based cryptography

一、前言

密码技术是信息安全的基石，在保障网络信息机密性、真实性、完整性和不可抵赖性方面发挥着核心作用。大整数因子分解、离散对数求解被认为是经典计算不能有效解决的问题，这也是现役公钥密码如RSA加密算法、椭圆曲线加密算法（ECC）的安全基础。1994年，受Simon算法的启发，研究人员提出了最具影响力的量子算法——Shor算法[1]。该算法可以在多项式时间内分析大整数或求解离散对数问题，使现役公钥密码如RSA、ECC加密算法在量子计算下毫无安全性。除大整数因子分解、离散对数问题外，其他许多密码设计中常用的数论难题也可以用类似的量子傅里叶分析方法设计出有效的量子算法。

一旦大规模通用量子计算机研制成功，利用Shor量子算法及其变种，现役的ECC、RSA等公钥密码体系将完全被攻破。2022年，有关研究指出，若使用配备量子存储器的量子计算系统破译RSA-2048加密算法，所需的物理比特数可以从百万级别降低为1.3万个[2]。按照当前每年翻一番的增速来看，到2029年左右就可能破译达上万量子比特的量子计算机。按照国际商业机器公司（IBM）在2023年发布的新路线图[3]，2029年之后，逻辑量子比特将不再成为制约量子计算规模增长的瓶颈，量子计算机将进入大规模通用发展的第三阶段；计划在2033年研制出2000位逻辑量子比特、运算门数达到10亿的大规模通用量子计算机。以破译RSA-2048加密算法为例，如果用逻辑量子比特衡量，估计大约需要1024位[4]，属于千位级逻辑量子比特规模。破译密钥长度为n比特的ECC算法所需的量子比特数为（$9n+2\log_2 n+10$），因此，ECC密码也同样有被破译风险[5]。

假设抗量子密码系统的部署需要X年完成，能破译现役公钥密码的量子计算机Y年后研制出来，对于保密期限为Z年的秘密信息，如果$Y<X+Z$，现役公钥密码将存在被破译的风险。机密级信息的典型保密期限Z=20，乐观估计X=10，即便2050年才出现破译当前密码的量子计算机，都可能对数据安全造成威胁。此外，攻击者可采用“先存储后解密”策略来威胁当前的信息系统，这将对需要长期保密且易于被攻击者截获存储的秘密信息造成不可控的风险。

目前，公钥密码已被广泛应用于我国网络信息体系中。一方面，在网络互联层被用于保障信息传输安全，另一方面，在服务供给层为网络信任体系提供核心支撑。大规模通用量子计算机一旦研制成功，攻击者可快速实现“通过公钥推导私钥”，使我国网络信任体系的安全性面临颠覆性冲击，而仅依赖公钥密码的信息传输将面临致命威胁。因此，抗量子公钥密码研究迫在眉睫。

Shor算法的提出激发了密码学家研究抗量子公钥密码的极大热情。2016年，美国国家标准与技术研究院（NIST）已开展抗量子公钥密码全球算法标准的征集工作（简称NIST PQC征集），吸引了全球密码领域人才的积极参与。为更好地了解抗量子公钥密码技术，本文梳理抗量子公钥密码主流技术路线的发展情况，分析抗量子公钥密码技术发展存在的问题，总结我国抗量子公钥密码发展面临的挑战，针对性地提出发展建议，为我国抗量子公钥密码技术研究提供参考。

二、抗量子公钥密码技术的发展现状

目前，抗量子公钥密码主要依托5类量子难解的数学难题构建：基于格的密码、基于编码的密码、多变量密码、基于杂凑的签名和基于同源的密码，各路线呈现差异化的技术特性。NIST PQC征集过程中各技术路线的数量情况如表1所示。

（一）基于格的密码

基于格的密码是当前最成熟的主流路线，在NIST PQC征集中占技术主力。基于格的算法在安全性、公私钥尺寸、计算速度方面可以实现较好的

表1 NIST PQC征集过程中各技术路线方案数量

（单位：个）

征集过程	基于格的密码	基于编码的密码	多变量密码	基于杂凑的签名	基于同源的密码
第一轮评估	28	20	10	2	1
第二轮评估	12	7	4	2	1
第三轮决赛	5	1	1	0	0
第三轮候补	2	2	1	2	1
第四轮评估	0	3	0	0	1
进入标准化	3	1	0	1	0

平衡。

基于格的密码具有的强安全性来自于在最差情况下的困难性保证。1996年，Ajtai首次提出了格的单向陷门函数这一思想[6]，给出了格中困难问题最坏情况的最短向量问题（SVP）到平均情况的小整数解问题（SIS）的归约[7]，使基于格的密码算法具有可证明安全的性质。这一开创性的结果引起了密码学界的广泛关注，也吸引了越来越多的学者投入到格基密码算法的设计与分析中。2005年，Regev提出一个基于错误学习问题（LWE）的密码算法[8]，并且证明了作为一种平均情况的实例，它在量子归约下至少与格中最坏情况的求解近似最短向量问题（SVPγ）和求解近似最短线性无关向量组问题（SIVPγ）的变种一样困难。目前，基于格的密码算法主要基于SIS、LWE问题或其变种开展研究。基于格的密码算法可以基于已有的安全证明技术，实现算法方案安全性到格困难问题的安全归约，显著增强了人们对格密码安全的信心。

基于格的密码算法主要使用小整数的模加和模乘运算，无需使用诸如模指数运算、双线性对等复杂、耗时的密码运算，因此计算复杂度低，具有潜在的计算效率优势。此外，格上的运算还便于采用并行运算等计算方法。1998年，NTRU算法被提出，成为目前比较实用的格密码算法之一[9]。与传统的RSA、ECC加密算法相比，NTRU运算简单，加/解密速度更快，且随着安全参数的提高，速度优势更加明显。2008年，在IEEE 1363.1—2008标准中，制定了基于格的密码算法标准，主要是NTRU加密算法的标准。2010年，NTRU加密算法被纳入ANSI X9.98标准。2014年，基于NTRU格的陷门生成和求逆算法被提出[10]，并给出了高效的签名方案。2017年，有研究利用新的快速离散傅里叶变换方法，改进了Ducas签名方案的效率和实现代码，设计出了新的高效签名方案Falcon[11]，提交至NIST PQC征集并进入标准化阶段。

基于标准LWE问题的密码算法密钥量较大。2010年，基于环上的错误学习问题（RLWE）的加密算法被提出[12]，与基于标准LWE问题的算法相比，运算效率有了大幅提升。此后，多个基于RLWE、基于模上错误学习问题（MLWE）的方案均是在此基础上进行的改进和优化，典型代表如算法CRYSTALS系列，可以在效率与安全性上实现最优平衡。其中Kyber[13]的1024位参数版本密钥长度仅为1.1 KB，加密延迟低至微秒级，可直接嵌入现有传输层安全协议（TLS）栈中。目前，密钥封装算法Kyber已正式成为NIST标准FIPS 203，数字签名算法Dilithium[14]成为NIST标准FIPS 204。

基于格的密码算法是目前功能最为齐全的技术路线，可以实现加密、数字签名、密钥交换、属性加密、函数加密、全同态加密等各类功能的密码学构造。国内外对基于格的密码算法普遍认可度高，对格的研究也是最活跃、最全面的，密码技术相对成熟。在NIST PQC征集、韩国PQC征集以及我国密码算法设计竞赛中，基于格的密码均是提交算法最多的类型。

（二）基于编码的密码

基于编码的密码是历时最为悠久的抗量子密码类型，目前多用于构造密钥封装算法；其设计基于一般线性码的陪集重量问题、子空间重量问题、伴随式译码问题等量子难解问题。1978年，第一个基于编码的公钥加密方案被提出[15]，称为McEliece公钥加密（MC-PKE），开创了对基于编码理论的公钥密码体制的研究。2022年，NIST公布的进入NIST PQC第四轮评估的Classic McEliece就是基于MC-PKE设计的。到目前为止，MC-PKE在经典计

算及量子计算条件下仍是安全的。需要指出的是，由于原始的MC-PKE使用戈帕（Goppa）码，虽然很有效，但公钥非常大且达几百千字节，严重限制了在实际应用场景中的使用。

1986年，另一个基于纠错码的公钥密码体制NC-PKE[16]被提出，该体制是一个背包型公钥密码体制。NC-PKE的公钥为随机产生的线性分组码校验矩阵，与MC-PKE不同的是，NC-PKE隐藏了具有快速译码算法的线性分组码的校验矩阵。2022年，NIST公布的进入NIST PQC第四轮的BIKE就是基于NC-PKE设计的[17]。近年来，受基于格的密码算法思想的启发，基于编码的ElGamal型加密方案（EC-PKE）被提出，该方法不直接隐藏码结构，为编码算法提出了一个新思路。进入NIST标准化的算法HQC[18]就是基于EC-PKE设计的。

由于基于编码的密码算法公钥量较大，减少公钥量一直是国内外学者研究的热点。有学者尝试利用准循环低密度校验（QC-LDPC）码代替Goppa码，从而可以接近香农界。该方法具有良好的译码算法，在密码体制构造时可获得更小的公钥量和更高的加／解密效率，但存在严重的安全问题，如对偶码攻击和消息集译码攻击。2013年，一种基于准循环中密度奇偶校验码（QC-MDPC）的公钥密码体制被提出[19]。该公钥密码体制保持了基于准循环码的公钥量小的特点，并且给出了一种针对QC-MDPC码的比特翻转译码算法，降低了解密的复杂度，可抵抗对偶码攻击和消息集译码攻击，具有公钥存储量小、加／解密复杂度低、安全性高等优势。HQC和BIKE算法都是基于QC-MDPC码设计的，其公钥长度和基于格的密码相当，约为几千字节。

（三）基于杂凑的签名

基于杂凑的签名算法安全性基于底层对称组件，是安全性假设最少的技术路线，其典型特点是功能单一，只能构造签名算法且签名尺寸较大。基于杂凑的签名算法方案的安全性基于基础函数的抗原像性（即单向性）和杂凑函数的抗碰撞性，每一对新的单向函数和杂凑函数都可以产生一个新的基于杂凑的签名方案。因此，基于杂凑的签名方案具备可以基于可用的硬件和软件资源进行选择的显著优势。例如，为了在芯片上使用签名方案，可以选择在芯片上实现基于AES的单向函数和杂凑函数。

基于杂凑的签名算法可以分为带状态的和无状态的，前者速度相对较快，但是需要维护密钥状态，可用于对软件固件的更新，以XMSS[20]为典型，目前该算法已正式成为NIST SP 800-208标准；后者则不需要维护密钥状态，可适应标准的应用程序编程接口（API），但是效率相对较低，其中以Sphincs+[21]最为著名，目前该算法已正式成为FIPS-205标准。

基于杂凑构造抗量子公钥密码只能构造数字签名算法，签名尺寸较大（与基于ECC的签名相比，大约相差3个数量级）；与基于格的数字签名算法相比，计算开销大（大约相差2个数量级），不利于在通用场景中应用。在256比特安全级别下，基于格的数字签名算法Dilithium和基于杂凑的数字签名算法Sphincs+实现性能对比情况如表2所示，实现平台为Intel i7处理器，未使用指令集加速。

（四）多变量密码

一般情况下，多变量公钥密码系统的公钥是由两个仿射变换和中心映射复合而成，其私钥为两个随机生成的仿射变换。多变量公钥密码的优点在于可以在较小的有限域上实现，具有较高的计算效率，而缺点是密钥量较大，且随着变量个数的增加及多项式次数的增加，密钥量增长较快。

多变量公钥密码系统的研究始于20世纪80年代中期。1988年，第一个多变量公钥方案被提出[22]，即著名的MI加密体制，并将“小域–大域”思想引入到了多变量公钥密码方案的设计当中。然而，原始的MI加密体制于1995年被一种线性化方程的攻击方法破解[23]。1997年，研究人员受线性化方程攻击的启发，提出了“油–醋”签名体制[24]。

表2　Sphincs+和Dilithium数字签名算法性能对比

算法	公钥长度/B	签名长度/B	密钥生成速度／时钟周期	签名速度／时钟周期	验签速度／时钟周期
Sphincs+	64	49 856	72 503 094	1 467 095 732	39 555 542
Dilithium	2592	4595	819 475	2 856 803	871 609

在原始的多变量公钥密码体制基础上，通过变形的方法，可设计出使安全性有所提高的多变量方案。较为典型的变形方法有：加方法、减方法、醋变量方法以及内部扰动方法等，其中减方法和醋变量方法主要用于设计数字签名方案如彩虹（Rainbow）签名体制[25]等，内部扰动方法则是一种系统化的增强多变量公钥密码安全性方法。此外，有研究人员提出了一种与内部扰动方法类似的Piece in Hand（PH）方法，用来加强多变量公钥密码的安全性[26]，其使用的思想与内部扰动方法类似。近年来，还出现了概率化多变量密码体制，即在多变量公钥体制中应用概率验证的思想以及利用多变量多项式构造哈希函数等。

目前，从严格的理论上来说，并没有公认的既安全又高效的多变量公钥加密体制，对多变量签名算法的信心较加密稍强，但随着进入NIST PQC第三轮评估的Rainbow方案2022年2月被攻破，学者对多变量签名的安全信心有减弱趋势。2022年，NIST开启了新一轮的签名算法征集工作，MAYO[27]、UOV[28]、QR_UOV[29]、SNOVA[30]等4个多变量的签名算法进入了第二轮评估。

（五）基于同源的密码

基于同源的密码的典型特点是参数尺寸小，但安全性信心有待加强。1996年，首个同源密码方案被提出[31]，即CRS方案。然而，CRS方案效率低下且存在亚指数时间的量子攻击算法[32]。经过一系列的改进，与CRS方案类似但相对高效的密钥交换方案CSIDH被提出[33]；与CRS方案不同的是，CSIDH利用了理想类群在超奇异椭圆曲线上的作用。基于CSIDH可以构造公钥加密方案，如SiGamal[34]、SimS[35]、数字签名方案SeaSign[36]、CSI-FiSh[37]。此外，利用虚二次域理想类群在超奇异椭圆曲线上的作用，CSIDH的变种OSIDH[38,39]被提出，但因效率低下，目前仅停留在理论层面。

超奇异同源图的研究进一步推动了密码学家们对同源密码算法的研究工作。2011年，研究人员提出了基于超奇异同源图的密钥交换方案SIDH[40]，基于SIDH构造的密钥封装算法SIKE[41]是NIST PQC征集过程中唯一一个基于同源的加密算法。但SIDH的公钥泄露了扭点在同源作用下的像，2022年8月，通过利用扭点信息，完成了对SIDH的彻底攻破[42~44]。Deuring对应[45]给出了超奇异椭圆曲线（几何世界）与四元数代数（代数世界）之间的对应，并可用来构造新的密码算法。2020年，研究人员在此基础上构造了目前最为紧凑的后量子签名算法SQISign[46]。2022年，Decru在构造可验证延迟函数时发现，高维同源有可能被用来攻击SIDH系统，从而将同源的高维表示带入了大众的视野。随后，高维表示被迅速应用到算法构造上，如SQISignHD[47]、QFESTA[48]、SQISign2d-West[49]、SQISign2d-East[50]、SQIPrime[51]。目前SQISign及其优化版本是基于同源的密码算法中最具竞争力的算法。同源密码的密钥量和签名尺寸在几百字节，在规模上占据较大优势，但其计算效率较低，多为几百毫秒至秒级，计算性能是制约其大规模应用的主要因素。

三、抗量子公钥密码技术发展存在的问题分析

（一）性能瓶颈：效率与资源矛盾突出

抗量子公钥密码技术路线呈现多样性，但各技术路线都难以兼顾效率与存储资源的平衡。传统ECC算法的参数尺寸在几十字节到上百字节，目前抗量子公钥算法普遍参数尺寸较大，多为几百至几千字节（见表3和表4）。例如，基于格的密码虽然效率较高，但与传统的公钥密码相比，其密钥、密文、签名尺寸、带宽占用等方面是传统ECC算法

表3 典型抗量子签名算法参数尺寸

技术路线	算法名称	公钥长度/B	签名长度/B
基于格的密码	ML-DSA（Dilithium）	2592	4595
	Falcon	1793	1280
基于杂凑的签名	XMSS_SHA2_10_256	64	2500
	XMSS_SHA2_10_512	128	9092
	LMS_SHA256_M32_H10	64	1452
	SLH-DSA（Sphincs+）	64	29 792
基于同源的密码	SQISign2.0	129	292
多变量密码	UOV	447 000	260
基于编码的密码	CROSS	106	36 000
	LESS	197 000	7116

表4　典型抗量子密钥封装算法参数尺寸

技术路线	算法名称	公钥长度/B	密文长度/B
基于格的密码	ML-KEM（Kyber）	1568	1568
	Frodo	21 520	21 632
基于编码的密码	McEliece	1 357 824	240
	HQC	7245	14 469
基于同源的密码	POKE	544	768

的10倍以上，从而导致存储与传输成本激增，难以满足资源受限场景的需求。同源密码的带宽约为传统公钥密码ECC算法的2~5倍，为目前尺寸相对较小的抗量子公钥密码技术路线，但运算效率为几百毫秒至秒级，难以满足物联网等场景的实时性要求。此外，抗量子密码普遍存在硬件资源消耗大的问题，如Kyber算法的硬件实现需消耗20 kB的内存，是ECC算法的5倍，在8位微控制器等极简设备中难以部署。抗量子公钥密码技术路线存在性能瓶颈的根源在于抗量子公钥密码算法基于的数学问题本身具有较高的计算复杂度或存储复杂度，而现有的优化技术无法弥补与传统算法的差距。

（二）生态兼容性：新旧系统协同难度大

现有信息系统多是基于传统密码构建，抗量子密码的引入需与硬件、软件、协议进行尝试适配，面临升级成本高、兼容性差的问题。一是硬件适配问题，传统密码协处理器不支持抗量子算法的特殊运算，需重新设计硬件架构。例如，服务器的可信平台模块（TPM）若要支持Dilithium签名算法，需增加专用多项式乘法单元，使每台设备的系统升级成本将增加50美元，全球服务器市场的总升级成本预计超过100亿美元。二是软件与协议的兼容问题，现有人工智能、网络协议未预留抗量子算法的扩展字段，如TLS记录协议的长度限制是16 384 kB，而Sphincs+签名长度超过该限制，因此，需修改协议规范，而这可能导致与旧版本客户端的兼容性冲突。同时，抗量子公钥密码算法缺乏DH协议类似的密钥协商算法，密钥协商需要通过密钥封装完成，协议抗量子迁移直接进行算法原位替换不现实。抗量子密码公钥算法的带宽开销大、可能与现役密码协议不适配，会引起网络拥塞、丢包率提升、握手延迟增加等问题。三是“混合加密”的过渡存在额外风险，当前主流方案是“传统密码算法+抗量子密码算法”混合使用，但混合机制可能引入新的漏洞。

（三）安全评估困难：缺乏成熟的方法和工具

抗量子密码算法的安全性基于一些新型的数学难题，但目前对这些数学难题的研究还不够深入。此外，抗量子密码算法技术路线众多，其安全评估缺乏成熟的方法和工具。例如，在当前的抗量子密码算法设计中，为保证算法的实现效率，往往会采用较强的代数结构，但目前的分析技术尚未利用代数结构。此外，随着量子计算技术的不断发展，新的攻击方法可能不断涌现，这进一步增加了抗量子算法安全性评估的难度。例如，Grover搜索算法和量子随机游走算法都可以对SVP筛法实现一定的量子加速，近年来随着量子随机游走技术的发展，SVP问题的量子安全性有所降低[52~56]。由于缺乏统一的评估标准，不同机构对同一抗量子密码算法的安全评估结果可能存在差异，从而影响了企业和用户对这些算法的信任度。

四、我国抗量子公钥密码技术发展面临的挑战

国际上，抗量子公钥密码技术的发展逐步形成“美国主导、欧洲跟随”的态势，国际标准化组织积极推进算法标准化，初步形成了抗量子密码算法的基础体系。客观来讲，我国抗量子密码研究起步较晚，目前在抗量子公钥密码技术领域仍面临一些挑战。

（一）理论研究基础薄弱

虽然我国在抗量子公钥密码技术领域已开展了一些研究工作，但与国际先进水平相比，理论研究基础仍相对薄弱。在核心算法的原创性研究方面，我国缺乏具有国际影响力的原创成果。目前，国际上的抗量子密码算法主要由欧美国家的科研团队提出，我国在算法设计、安全性证明等方面的研究深度和广度有待提高。

在对新型数学难题的研究方面，我国投入的研究力量相对不足。抗量子公钥密码技术依赖于一些新型的数学难题，如格理论、编码理论等领域的难

题，对这些数学难题的深入研究是设计高效、安全抗量子密码算法的基础。然而，我国在这些领域的研究起步较晚，研究团队规模较小，与国际前沿研究存在一定差距。

此外，我国在抗量子公钥密码技术理论研究方面的国际合作也相对较少。抗量子公钥密码技术是一个全球性的研究课题，国际合作对于共享研究成果、共同攻克难题具有重要意义。但目前我国在该领域与国际顶尖科研机构和团队的合作不够紧密，限制了我国抗量子公钥密码技术理论研究水平的提升。

（二）标准制定滞后

标准化是抗量子公钥密码技术规模化应用的前提。当前，以美国NIST主导的抗量子公钥密码标准化进程为核心，全球形成了多区域协同推进的格局。2024年8月，NIST正式发布全球首批3项抗量子公钥密码标准（FIPS 203/204/205），标志着PQC进入实用化阶段。其中，CRYSTALS-Kyber（基于格密码）被选为密钥封装机制（KEM）标准，用于TLS协议密钥协商等场景；CRYSTALS-Dilithium（基于格密码）和Sphics+（对称签名）被指定为数字签名标准，适配身份认证、固件校验等需求。这3类算法均通过多轮严苛评估，可以在安全性、效率与可扩展性方面实现平衡，已初步形成抗量子公钥密码算法体系。国际标准化组织也在加速推进抗量子公钥密码算法标准工作。互联网工程任务组（IETF）有多个工作组在推动密码协议纳入后量子密码算法的演进。IETF建议在TLS1.2、TLS1.3、IKEv2协议中添加抗量子密钥封装算法（ML-KEM、FrodoKEM）以构造抗量子融合密钥协商协议，从而抵抗未来可能的量子计算机的攻击。目前，我国在抗量子公钥密码技术标准制定方面相对滞后，刚刚启动抗量子密码算法的全球征集工作，尚未形成国家抗量子密码算法标准。标准制定滞后导致我国企业在研发抗量子密码产品时缺乏统一的规范和指导，增加了产品研发的成本和风险。不同企业研发的产品可能在算法选择、参数设置、接口规范等方面存在差异，难以实现互联互通和互操作，阻碍了抗量子公钥密码技术的产业化推广。同时，由于我国在国际抗量子密码标准制定中的参与度不高，缺乏话语权，可能导致未来我国在该领域的国际竞争中处于被动地位。

（三）产业生态不完善，抗量子迁移难度大

我国抗量子公钥密码技术的产业生态尚不完善，产业链各环节之间的协同合作不够紧密。在芯片制造、算法实现、系统集成等关键环节，存在技术瓶颈和资源分散的问题。① 在芯片制造方面，抗量子密码算法对芯片的计算能力和功耗有较高要求。目前，我国的芯片制造技术在满足抗量子密码算法需求方面仍存在一定差距，制约了我国抗量子公钥密码技术产业的自主可控发展。② 在算法实现方面，虽然我国在抗量子密码算法研究方面取得了一些成果，但在算法的工程化实现和优化方面还存在不足。算法的实现效率、稳定性和安全性等需要进一步提高，以满足实际应用的需求。③ 在系统集成方面，抗量子公钥密码技术与现有信息系统的集成难度较大。现有信息系统大多基于传统密码体系构建，引入抗量子公钥密码技术需要对系统进行大规模改造，涉及硬件、软件、网络等多个层面的适配和升级。由于缺乏成熟的集成方案和经验，系统集成过程中容易出现兼容性问题，增加了应用推广的难度。此外，公钥密码在我国部署广泛，抗量子迁移工程面临存量巨大、产业纵深、演进敏捷、国际性强等难点，再加上抗量子迁移面临诸多管理和技术问题尚未解决且并非短时间可以完成。目前，抗量子公钥密码技术主要在一些对信息安全要求极高的领域进行试点，在金融、医疗、能源等其他领域的应用还处于起步阶段。

（四）人才短缺

抗量子公钥密码技术是一门交叉学科，涉及数学、密码学、计算机科学、量子物理学等多个领域。目前，我国在抗量子公钥密码技术领域的专业人才短缺，难以满足技术研发和产业发展的需求。高校和科研院所在抗量子公钥密码技术人才培养方面的课程设置、研究方向相对滞后，在相关专业的课程体系中，对抗量子公钥密码技术的教学内容覆盖不足，缺乏系统性和深度。企业在抗量子公钥密码技术人才招聘和培养方面也面临挑战。由于该领域人才稀缺，企业难以招聘到具有丰富经验和专业技能的人才；同时，企业内部缺乏完善的人才培养机制，难以对现有员工进行有

效的培训和提升，进一步加剧了人才短缺的问题。整体来看，人才短缺不仅限制了我国抗量子公钥密码技术的创新能力和研发水平，也影响了产业的发展速度和规模。

五、我国抗量子公钥密码技术的发展建议

（一）加强基础研究，提升自主创新能力

加大对抗量子公钥密码技术基础研究的投入，鼓励高校、科研院所和企业开展联合攻关。设立国家级专项科研基金，支持核心算法的原创性研究、新型数学难题的探索以及算法安全性证明等基础研究工作。加强与国际顶尖科研机构和团队的合作与交流，积极参与国际学术会议和合作项目，学习借鉴国际先进的研究经验和技术成果。同时，吸引国际优秀人才来华开展合作研究，提升我国抗量子公钥密码技术研究团队的国际化水平。建立抗量子公钥密码技术基础研究平台，整合国内优势研究资源，形成协同创新的研究格局。平台可以提供先进的实验设备、计算资源和数据共享服务，为科研人员开展研究工作提供良好的条件。

（二）加速标准制定，提升国际话语权

加快我国抗量子公钥密码技术标准的制定工作，建立完善的标准体系。组织国内相关领域的专家学者、企业代表和标准化机构，共同开展标准的研究和制定工作。标准应涵盖算法规范、性能指标、接口标准、安全评估等多个方面，为企业研发和产品认证提供统一的依据。积极参与国际抗量子公钥密码技术标准的制定工作，提升我国在国际标准制定中的话语权。加强与国际标准化组织的沟通与协调，提出我国的标准建议和技术方案，推动我国自主研发的抗量子密码算法和技术纳入国际标准。建立标准动态更新机制，及时跟踪国际抗量子公钥密码技术的发展动态和研究成果，对我国的标准进行修订和完善，确保我国的标准始终与国际先进水平保持同步，适应技术发展和市场需求的变化。

（三）完善产业生态，推动抗量子分阶段迁移

加强产业链上下游企业的协同合作，形成完整的抗量子公钥密码技术产业生态。鼓励芯片制造企业加大研发投入，突破高性能抗量子密码芯片的关键技术，提高芯片的国产化率。支持算法研发企业与芯片制造企业、系统集成企业开展合作，实现算法与芯片、系统的深度融合。积极拓展抗量子公钥密码技术的应用场景，培育市场需求。加强与金融、医疗、能源、交通等行业的合作，推动抗量子公钥密码技术在这些领域的应用示范。通过应用示范，分级、分类、分阶段开展迁移工作。尽快开展密码识别与脆弱性发现研究工作，对现役密码的应用情况和安全威胁进行全面梳理，分析重点和难点、制定迁移方案、开展演示验证，为实现各类密码应用平滑升级和体系能力整体跃升打好基础。

（四）强化人才培养，打造专业人才队伍

高校和科研院所应优化相关专业的课程设置，增加抗量子公钥密码技术相关的教学内容。开设专门的课程和研究方向，培养具有扎实理论基础和实践能力的专业人才。加强与企业合作，建立实习实训基地，为学生提供实践机会，提高学生的实际操作能力。企业应建立完善的人才培养机制，加强对现有员工的培训和提升。与高校、科研院所合作，开展定制化培训项目，根据企业的实际需求，培养具有专业技能的人才。同时，积极引进国际优秀人才，提升企业的技术创新能力和研发水平。建议政府出台相关政策，鼓励人才投身抗量子公钥密码技术领域，通过政策倾斜等措施，提供良好的发展环境，吸引国内外优秀人才回国创业和工作。建立人才激励机制，对在抗量子公钥密码技术领域取得突出成果的人才给予表彰和奖励，激发人才的创新积极性。通过“产学研”联动，构建综合创新的抗量子公钥密码的人才队伍与创新团队。

六、结语

抗量子公钥密码技术对保障我国在量子计算时代的信息安全具有重要战略意义。我国在该领域取得了一定进展，但在理论研究、标准制定、产业生态和人才培养等方面仍面临诸多问题。通过加强基础研究、加速标准制定、完善产业生态和强化人才培养等一系列措施，我国有望提升抗量子公钥密码技术的自主创新能力和产业发展水平，在全球抗量子密码战略博弈中争取主动权，为国家信息安全提

供坚实的保障。抗量子公钥密码作为应对量子计算威胁的核心技术手段，正从标准制定向规模化落地加速迈进，未来将构建起多维度、强韧性的数字安全新生态，为推动我国网络空间安全能力实现从经典安全向量子安全的能力跃升发挥巨大作用。

利益冲突声明

本文作者在此声明不存在任何利益冲突或财务冲突。

Received date: November 13, 2025; **Revised date:** December 26, 2025

Corresponding author: Zhu Guizhen is a professor-level senior engineer from Data Communication and Technology Research Institute. Her major research field is post-quantum cryptography. E-mail: zhuguizhen.2008@tsinghua.org.cn

Funding project: Chinese Academy of Engineering project “Research on Risks of New Technologies and Applications in Cyberspace Security” (2023-JB-13)

参考文献

[1] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring [R]. Santa Fe: The 35th Annual Symposium on Foundations of Computer Science, 2002.

[2] Gouzien É, Sangouard N. Factoring 2048-bit RSA integers in 177 days with 13436 qubits and a multimode memory [EB/OL]. (2021-03-10)[2025-05-12]. https://arxiv.org/abs/2103.06159.

[3] IBM quantum submit 2023 [EB/OL]. [2025-05-20]. https://www.ibm.com/quantum/summit-2023.

[4] Chevignard C, Fouque P A, Schrottenloher A. Reducing the number of qubits in quantum factoring [R]. Santa Barbara: The 45th Annual International Cryptology Conference, 2025.

[5] Roetteler M, Naehrig M, Krysta M S, et al. Quantum resource estimates for computing elliptic curve discrete logarithms [EB/OL]. (2017-06-21)[2025-05-08]. https://doi.org/10.48550/arXiv.1706.06752.

[6] Ajtai M. Generating hard instances of lattice problems (extended abstract) [R]. Philadelphia: STOC96: ACM Symposium on Theory of Computingx, 1996.

[7] Ajtai M, Dwork C. A public-key cryptosystem with worst-case/average-case equivalence [R]. El Paso: The Twenty-Ninth Annual ACM Symposium on Theory of Computing—STOC '97, 1997.

[8] Regev O. On lattices, learning with errors, random linear codes, and cryptography [R]. Baltimore: The Thirty-Seventh Annual ACM Symposium on Theory of Computing, 2005.

[9] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem [R]. Portland: Third International Symposium, 1998.

[10] Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices [R]. Kaoshiung: The 20th International Conference on the Theory and Application of Cryptology and Information Security, 2014.

[11] Prest T, Fouque P A, Hoffstein J, et al. Falcon [EB/OL]. [2025-08-20]. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions.

[12] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings [R]. French Riviera: The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2010.

[13] Schwabe P, Avanzi R, Bos J, et al. Crystals-kyber [EB/OL]. [2025-08-20]. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions.

[14] Léo D, Tancrède L, Vadim L, et al. CRYSTALS—Dilithium: Digital signatures from module lattices [EB/OL]. [2025-08-20]. https://cryptojedi.org/papers/dilithium-20170627.pdf,2017.

[15] McEliece R. A public key cryptosystem based on algebraic coding theory [R]. Pasadena: California Institute of Technology, 1978.

[16] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory [J]. Problems of Control and Information Theory, 1986, 15(2): 159–166.

[17] Aragon N, Barreto P, Bettaieb S, et al. Bike [EB/OL]. [2025-08-20]. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions.

[18] Melchor C A, Aragon N, Bettaieb S, et al. HQC [EB/OL]. [2025-08-20]. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions.

[19] Misoczki R, Tillich J P, Sendrier N, et al. MDPC-McEliece: New McEliece variants from moderate density parity-check codes [R]. Istambul: The 2013 IEEE International Symposium on Information Theory, 2013.

[20] Buchmann J, Dahmen E, Hülsing A. XMSS-a practical forward secure signature scheme based on minimal security assumptions [R]. Taipei: The 4th International Workshop, PQCrypto 2011, 2011.

[21] Bernstein D J, Hülsing A, Kölbl S, et al. The SPHINCS+ signature framework [R]. London: The 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019.

[22] Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption [R]. Davos: Workshop on the Theory and Application of Cryptographic Techniques, 1988.

[23] Patarin J. Cryptanalysis of the matsumoto and imai public key scheme of eurocrypt’88 [R]. Santa Barbara: The 15th Annual International Cryptology Conference, 1995.

[24] Patarin J. The oil and vinegar signature scheme [R]. Dagstuhl: Dagstuhl Workshop on Cryptography, 1997.

[25] Ding J T, Schmidt D. Rainbow, a new multivariable polynomial signature scheme [R]. New York: Third International Conference, ACNS 2005, 2005.

[26] Tsujii S, Tadaki K, Fujita R. Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: without containing all the information of secret key [EB/OL]. (2004-12-20)[2025-05-23]. https://eprint.iacr.org/2004/366.

[27] Beullens W, Campos F, Celi S, et al. MAYO specification document [EB/OL]. [2025-08-20]. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/mayo-spec-web.pdf.

[28] Beullens W, Chen M S, Ding J T, et al. UOV: Unbalanced oil and vinegar: Algorithm specifications and supporting documentation version 1.0 [EB/OL]. [2025-08-20]. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/UOV-spec-

web.pdf.

[29] Furue H, Ikematsu Y, Kiyomura Y, et al. A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV [R]. Singapore: The 27th International Conference on the Theory and Application of Cryptology and Information Security, 2021.

[30] Wang L C, Tseng P E, Kuan Y L, et al. A simple noncommutative UOV scheme [J]. IACR Cryptol EPrint Arch, 2022, 2022: 1742.

[31] Couveignes J W. Hard homogeneous spaces [EB/OL]. (2006-08-24)[2025-05-26]. https://eprint.iacr.org/2006/291.pdf.

[32] Childs A, Jao D, Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time [J]. Journal of Mathematical Cryptology, 2014, 8(1): 1–29.

[33] Castryck W, Lange T, Martindale C, et al. CSIDH: An efficient post-quantum commutative group action [R]. Brisbane: The 24th International Conference on the Theory and Application of Cryptology and Information Security, 2018.

[34] Moriya T, Onuki H, Takagi T. SiGamal: A supersingular isogeny-based PKE and its application to a PRF [R]. Daejeon: The 26th International Conference on the Theory and Application of Cryptology and Information Security, 2020.

[35] Fouotsa T B, Petit C. SimS: A simplification of SiGamal [R]. Daejeon: The 12th International Workshop, PQCrypto 2021, 2021.

[36] Luca De F, Steven D G. Seasign: compact isogeny signatures from class group actions [R]. Darmstadt: The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2019.

[37] Beullens W, Kleinjung T, Vercauteren F. CSI-FiSh: Efficient isogeny based signatures through class group computations [R]. Kobe: The 25th International Conference on the Theory and Application of Cryptology and Information Security, 2019.

[38] Colò L, Kohel D. Orienting supersingular isogeny graphs [J]. Journal of Mathematical Cryptology, 2020, 14(1): 414–437.

[39] Onuki H. On oriented supersingular elliptic curves [J]. Finite Fields and Their Applications, 2021, 69: 101777.

[40] Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies [R]. Taipei: The 4th International Workshop, PQCrypto 2011, 2011.

[41] Jao D, Azarderakhsh R, Campagna M, et al. Supersingular isogeny key encapsulation [EB/OL]. [2025-08-20]. https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/SIKE-spec.pdf.

[42] Castryck W, Decru T. An efficient key recovery attack on SIDH (preliminary version) [J]. IACR Cryptol EPrint Arch, 2022, 2022: 975.

[43] Maino L, Martindale C. An attack on SIDH with arbitrary starting curve [EB/OL]. (2022-08-08)[2025-05-24]. https://eprint.iacr.org/2022/1026.

[44] Robert D. Breaking SIDH in polynomial time [R]. Cham: Advances in Cryptology—EUROCRYPT 2023, 2023.

[45] Deuring M. Die typen der multiplikatorenringe elliptischer funktionenkörper [J]. Abhandlungen Aus Dem Mathematischen Seminar der Universität Hamburg, 1941, 14(1): 197–272.

[46] De Feo L, Kohel D, Leroux A, et al. SQISign: Compact post-quantum signatures from quaternions and isogenies [R]. Daejeon: The 26th International Conference on the Theory and Application of Cryptology and Information Security, 2020.

[47] Dartois P, Leroux A, Robert D, et al. SQIsignHD: New dimensions in cryptography [R]. Zurich: The 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2024.

[48] Nakagawa K, Onuki H. QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras [R]. Santa Barbara: The 44th Annual International Cryptology Conference, 2024.

[49] Basso A, Dartois P, De Feo L, et al. SQIsign2D-West:The fast, the small, and the safer [R]. Kolkata: The 30th International Conference on the Theory and Application of Cryptology and Information Security, 2024.

[50] Nakagawa K, Onuki H, Castryck W, et al. SQIsign2D-East: A new signature scheme using 2-dimensional isogenies [R]. Kolkata: The 30th International Conference on the Theory and Application of Cryptology and Information Security, 2024.

[51] Duparc M, Fouotsa T B. SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies [R]. Kolkata: The 30th International Conference on the Theory and Application of Cryptology and Information Security, 2024.

[52] Nguyen P Q, Vidick T. Sieve algorithms for the shortest vector problem are practical [J]. Journal of Mathematical Cryptology, 2008, 2(2): 181–207.

[53] Becker A, Ducas L, Gama N, et al. New directions in nearest neighbor searching with applications to lattice sieving [R]. Arlington: SODA '16: Symposium on Discrete Algorithms, 2016.

[54] Chailloux A, Loyer J. Lattice sieving *via* quantum random walks [R]. Singapore: The 27th International Conference on the Theory and Application of Cryptology and Information Security, 2021.

[55] Bonnetain X, Chailloux A, Schrottenloher A, et al. Finding many collisions *via* reusable quantum walks: Application to lattice sieving [R]. Lyon: The 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2023.

[56] 向宏, 胡希, 付皓玥. 美国标准与技术研究院后量子密码分析及制标工作研究 [M]. 北京: 电子工业出版社, 2025.
Xiang H, Hu X, Fu H Y. Research on post-quantum cryptanalysis and standardization work at the National Institute of Standards and Technology (NIST) [M]. Beijing: Publishing House of Electronics Industry, 2025.