后量子密码学研究：从传统公钥体系到后量子安全方案

莫文涛[1,2]，陶伟[1,3]，洪振厚[1]，查高密[1]，张旭龙[1]，瞿晓阳[1]，宋歌[2]，王健宗[1]
1. 平安科技（深圳）有限公司，广东 深圳 518063；
2. 清华大学，北京 100084；
3. 华中科技大学，湖北 武汉 430070

摘要
随着量子计算技术的发展，基于大整数分解与离散对数问题的传统公钥密码体系面临安全挑战。为系统梳理后量子密码的研究进展，对其理论基础、算法体系、工程实现与部署问题进行了综述。首先分析传统密码体系在量子攻击模型下的脆弱性及协议迁移约束；随后分类比较格基、哈希基、编码基、多变量及同源映射等后量子密码方案，并结合CPU、FPGA与嵌入式平台讨论硬件适配、实现优化和实现安全问题。在统一测试环境下，对传统、后量子、混合及部分国内研究团队提出并公开实现的签名与KEM方案进行了性能和通信开销评测。结果表明，不同技术路线在安全性、计算效率与通信成本之间存在明显权衡。最后归纳长期安全验证、实现安全、系统迁移与工程部署等挑战，为后量子密码研究与应用提供参考。

关键词
后量子密码；量子攻击模型；公钥密码；密码标准化；性能评测

中图分类号：TP391　　文献标志码：A　　doi：10.11959/j.issn.2096–0271.2024xxx

Post-quantum cryptography: from classical public-key systems to post-quantum secure schemes

MO Wentao[1,2], TAO Wei[1,3], HONG Zhenhou[1], CHA Gaomi[1], ZHANG Xulong[1], QU Xiaoyang[1], SONG Ge[2], WANG Jianzong[1]
1. Ping An Technology (Shenzhen) Co. , Ltd. , Shenzhen 518063, China；
2. Tsinghua University, Beijing 100084, China；
3. Huazhong University of Science and Technology, Wuhan 430070, China

Abstract
With the development of quantum computing, traditional public-key cryptographic systems based on integer factorization and discrete logarithm problems face security challenges. To systematically review the research progress of post-quantum cryptography, its theoretical foundations, algorithmic systems, engineering implementation, and deployment issues were surveyed. First, the vulnerabilities of traditional cryptographic systems under quantum attack models and the constraints of protocol migration were analyzed. Then, post-quantum cryptographic schemes, including lattice-based, hash-based, code-based, multivariate, and isogeny-based schemes, were classified and compared, and

hardware adaptation, implementation optimization, and implementation security were discussed in combination with CPU, FPGA, and embedded platforms. Under a unified testing environment, the performance and communication overhead of traditional, post-quantum, hybrid, and selected signature and KEM schemes proposed and publicly implemented by domestic research teams were evaluated. The results show that different technical routes involve obvious trade-offs among security, computational efficiency, and communication cost. Finally, challenges in long-term security validation, implementation security, system migration, and engineering deployment were summarized, providing a reference for post-quantum cryptography research and application.

Key words
post-quantum cryptography, quantum adversary model, public-key cryptography, cryptographic standardization, performance evaluation

0 引言

量子计算的发展对现代公钥密码体系构成了直接挑战。RSA、Diffie–Hellman和椭圆曲线密码（Elliptic Curve Cryptography, ECC）等传统公钥密码方案主要依赖大整数分解和离散对数问题，而Shor算法[1]表明这些问题在量子计算模型下可被多项式时间求解，从而使传统公钥密码的安全基础面临根本性失效[2][3]。Grover算法[4]主要对对称密码和哈希函数的穷举搜索复杂度产生平方级加速，使其等效安全强度下降。因此，后量子密码研究的核心任务是构建可在经典计算平台上部署、并能抵抗量子攻击的公钥密码原语与算法体系[5]。

为系统推进后量子密码技术的评估与标准化，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）[6]于2016年正式启动了后量子密码标准化项目。2024年，NIST正式发布三项后量子密码联邦信息处理标准，分别为FIPS 203（ML-KEM）、FIPS 204（ML-DSA）和FIPS 205（SLH-DSA）[7][8][9]。在此基础上，NIST继续推进后续算法标准化工作，其中Falcon已被选定用于后续数字签名标准化，后续标准名称为FN-DSA。2025年3月，NIST进一步选择HQC作为第五个进入标准化体系的后量子密码算法，用于补充密钥封装机制标准化流程[10][11]。截至目前，NIST后量子密码标准化进程已形成以ML-KEM、ML-DSA和SLH-DSA等已发布标准为基础，并以FN-DSA和HQC等后续标准化对象为补充的算法体系，覆盖密钥封装机制（key encapsulation mechanism，KEM）与数字签名两类主要公钥密码原语。与此同时，为进一步丰富后量子数字签名算法组合，NIST于2026年5月14日公布了“后量子密码附加数字签名方案”第三轮候选算法[12]，共有9个签名方案进入后续评估，包括4个多变量签名方案（MAYO、QR-UOV、SNOVA、UOV）、2个MPC-in-the-Head签名方案（MQOM、SDitH），以及同源签名方案SQIsign、格基签名方案HAWK和对称基签名方案FAEST各1个。该进展表明，在已发布和推进标准化的主线算法之外，NIST仍在通过附加签名方案遴选机制持续扩展数字签名算法的技术多样性。该标准化过程不仅关注算法在理论模型下的安全证明，也高度重视其

在不同软硬件平台上的实现代价与潜在风险。

在算法标准化之外，后量子密码迁移也逐渐成为国内外研究与工程部署中的重要议题。国际方面，相关迁移指南[13]强调应尽早开展密码资产清点、量子就绪路线图制定、风险评估与迁移优先级排序，以降低长期敏感数据面临的“先收集、后解密”风险。国内方面，相关研究主要围绕后量子密码算法设计、公开实现、性能优化、硬件适配与迁移评估展开，并已有部分算法方案和开源密码库[14]为后续性能评测与工程部署研究提供支撑。由此可见，后量子密码研究正在从单一算法安全性分析，逐步转向算法标准化、迁移策略、工程实现与系统部署相结合的综合研究阶段。

本文围绕后量子密码学的理论基础、算法体系与工程实现展开系统综述。全文首先分析传统密码体系在量子算法攻击下所面临的安全挑战，随后对主流后量子密码算法类别进行分类与比较，并进一步讨论其在实际硬件平台上的实现与优化问题。在此基础上，本文总结现有评测方法与测试数据体系，对不同方案的性能特征进行系统分析，最后归纳当前研究中仍待解决的关键问题，并展望未来的发展方向。

本文的主要贡献如下：

● 本文从传统公钥密码的数学假设出发，简要梳理其在量子计算模型下面临的安全脆弱性，并进一步分析传统密码体系在协议层与系统层迁移中的现实约束，为后续讨论后量子密码算法体系、工程实现与部署评估提供必要背景。

● 本文从算法范式出发，系统分析主流后量子密码（格基、哈希基、编码基、多变量等）的安全假设、性能特征与实现代价，并结合硬件平台差异（CPU、现场可编程门阵列（field-programmable gate array，FPGA）、嵌入式设备）讨论其工程适配问题，形成算法—实现—部署的整体分析框架。

● 在统一硬件与软件环境下，本文对国际主流签名算法与KEM方案，以及国内研究团队提出并公开实现的相关后量子密码方案进行性能评测与通信开销对比，分析不同安全等级下的计算与存储特征，并讨论评测公平性与Benchmark差异问题，为实际部署提供数据支撑与决策依据。

1 传统公钥密码体系及其量子脆弱性

1.1 传统公钥密码的数学基础

传统公钥密码体系主要建立在经典计算模型下的计算困难性假设之上，典型包括大整数分解问题、有限域离散对数问题和椭圆曲线离散对数问题。RSA依赖大整数分解难题[15]，Diffie - Hellman[16]、ElGamal[17]及相关签名方案依赖离散对数问题，ECC[18]则通过椭圆曲线群在较短密钥长度下实现较高效率。尽管这些体系在数学结构和工程性能上存在差异，但其共同特征是安全性均依赖于经典计算模型下相关问题的不可行性[19]。一旦攻击者计算模型发生变化，这些基础假设便可能整体失效。

1.2 量子攻击模型下的安全性分析

量子攻击模型假设攻击者能够利用量子叠加、量子并行性和量子干涉等机制运行量子算法，从而改变传统密码分析中对计算资源和攻击复杂度的基本假设[20]。在该模型下，传统公钥密码所依赖的大整数分解和离散对数问题需要重新评估，其安全性不再仅取决于经典计算条件下的求解

难度。

Shor 算法[21]表明，大整数分解问题和离散对数问题均可在量子计算模型下于多项式时间内求解。这一结果直接破坏了 RSA、Diffie - Hellman 和 ECDSA 等传统公钥密码组件的安全基础[15][16][18]。如图 1 所示，量子算法首先突破大整数分解、离散对数和椭圆曲线等数学假设，随后导致公钥机制与认证机制失效，并进一步影响 TLS 密钥交换、PKI 传统体系和数字签名基础等协议与系统层安全。因此，对于依赖上述问题的公钥密码体系，量子攻击会从根本上改变其底层困难问题的计算复杂度，使参数放大等传统加固手段难以继续发挥作用。

相比之下，Grover 算法主要对无结构搜索问题提供平方级加速。在对称密码和哈希函数场景中，这意味着穷举搜索或碰撞相关攻击的复杂度下降，等效安全强度被削弱。该影响通常表现为安全裕度降低，并不会直接导致底层安全假设整体失效。因此，量子攻击对传统密码体系的影响具有明显差异：公钥密码面临由数学假设失效引发的结构性风险，对称密码和哈希函数主要面临参数安全强度下降问题。

综上，后量子安全研究的重点集中于构建能够替代传统公钥密码的算法体系，即在经典计算平台上可部署，并在经典与量子攻击模型下均保持计算安全性的密钥封装机制和数字签名方案。

1.3 传统体系在后量子场景下优化的局限性

在经典密码分析中，参数放大是增强安全性的常见手段，例如增加密钥长度、模长或群阶规模以提升攻击成本。然而，在后量子场景下，该策略难以继续适用于传统公钥密码体系。对于基于大整数分解或离散对数问题的方案，量子算法直接改变其底层困难问题的计算复杂度等级，单纯增加参数规模已无法恢复计算安全性[3][5][21]。这表明，参数放大策略只有在底层安全假设仍然成立时才具有意义。一旦数学假设被量子计算突破，局部参数调整便难以构成有效防御[4][5]。

进一步来看，传统公钥密码体系在协议与系统层面也存在迁移局限。大量安全协议在设计时默认使用 RSA、Diffie - Hellman 或椭圆曲线密码等基础组件，其安全证明、协议流程和实现接口均与这些算法的结构特性相关。后量子场景下，若直接以新算法替换传统公钥算法，往往难以保持原有协议的安全性质与性能表现[22]。一方面，后量子算法在密钥长度、通信负载和计算模式上与经典方案差异显著，可能改变协议的效率假设和实现约束；另一方面，部分协议安全证明依赖特定代数结构或数学性质，而后量子算法通常采用不同的困难问题与构造方式，导致协议级安全性需要重新分析[10]。此外，现有基础设施、硬件加速模块和标准接口长期围绕传统公钥算法构建，实际迁移还涉及系统兼容性、性能开销和实现安全等问题[23][24]。

综上，传统密码体系在后量子场景下的局限性具有结构性特征：其安全性难以通过简单参数放大维持，协议设计与系统实现也对传统公钥算法存在深度依赖。因此，后量子安全需求难以通过局部修补解决，需要在算法设计、协议架构和系统部署层面进行协同重构。

2 后量子安全密码算法体系

在明确传统密码体系在量子攻击模型

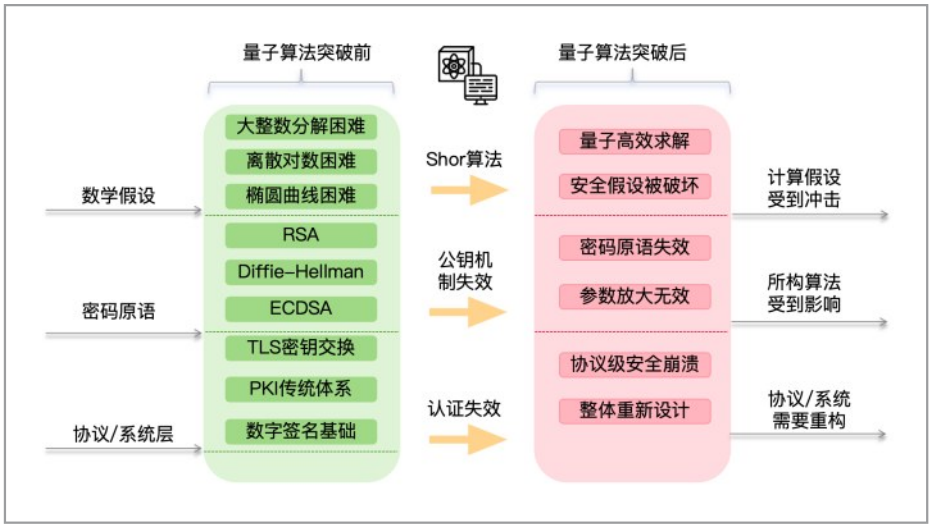

图1　量子场景下传统公钥密码挑战。上层为数学假设层，基于大整数分解与离散对数等计算难题；中层为密码原语层，包括公钥加密、密钥交换与数字签名等核心机制；下层为协议与系统层，如安全通信协议与网络安全架构，其安全性依赖于密码原语与数学假设的支撑。

下的结构性局限之后，后量子密码算法成为替代传统公钥密码的重要方向。后量子安全密码算法不依赖大整数分解或离散对数问题，而是基于当前尚未被量子算法高效求解的数学困难问题。本章从算法范式出发，对主流后量子公钥密码类别进行比较分析，相关范式对比如表1所示。

2.1 基于格的密码方案

基于格的密码是当前研究最活跃、工程化程度较高的后量子密码方向，主要建立在学习带噪声问题[25]（Learning With Errors, LWE）及其结构化变体之上。LWE问题可与若干最坏情况下的格问题建立归约关系，因此具有较强的安全理论基础。为降低计算与存储开销，Ring-LWE[26]和Module-LWE[27]等结构化变体被提出，并通过引入环或模格结构提升实现效率。其中，Ring-LWE利用多项式环结构降低密钥尺寸并加速多项式运算；Module-LWE在标准LWE与Ring-LWE之间取得折中，兼顾安全假设与实现效率。

基于格的方案已广泛用于构造密钥封装机制与数字签名算法[28]。其主要优势在于计算效率较高、实现路径清晰，并且适合通用处理器和硬件平台部署。然而，这类方案通常具有较大的公钥、密文或签名尺寸[29]，同时对参数选择、随机采样、恒定时间实现和侧信道防护较为敏感。

2.2 基于哈希的签名方案

基于哈希的签名方案是较早被系统研究的后量子数字签名技术，其安全性主要依赖密码哈希函数的抗碰撞性和单向性。该类方案通常以Merkle树结构为基础[30]，通过组合一次性签名或少次使用签名实现可扩展签名能力，代表性方案包括XMSS[31]及无状态的SPHINCS+[32]。

该类方案的优势在于安全假设简单、理论基础清晰，且不依赖复杂代数结构。然而，其局限也较为明显[33]：有状态方案需要严格维护签名状态，状态复用可能导

表1 主流后量子公钥密码算法范式对比

算法范式	核心假设	密码原语	性能特征	主要局限	标准化状态
基于格 LWE Ring-LWE Module-LWE	学习带噪声问题(LWE)及其最坏情况格问题	KEM、签名	计算效率高,适合软件与硬件实现	公钥/密文尺寸较大,对实现安全敏感	NIST已进入标准化流程
基于哈希 Merkle XMSS SPHINCS+	哈希函数的抗碰撞性与单向性	签名	安全假设简单,结构清晰	签名尺寸大,有状态管理问题	NIST已进入标准化流程
基于编码 McEliece	一般线性码译码问题	KEM	安全性稳定,长期未被攻破	公钥尺寸极大	NIST已进入标准化流程
基于多变量多项式 MQ	多变量二次方程组求解问题	签名	签名速度快	历史攻击频繁,参数设计敏感	部分方案进入NIST附加签名第三轮
基于同源映射 Isogeny-based	椭圆曲线同源映射问题	KEM、签名	公钥与密文尺寸小	部分构造受攻击影响,实现复杂度高	KEM方向受攻击影响,SQIsign进入NIST附加签名第三轮

致安全失效；无状态方案避免了状态管理问题，但通常带来较大的签名尺寸和计算开销。因此，基于哈希的签名方案更适合长期安全性要求高、签名频率相对有限的应用场景。

2.3 基于编码理论的密码方案

基于编码理论的密码方案以McEliece体系[34]为代表，其安全性建立在一般线性码译码问题的计算困难性之上。该问题在经典和量子计算模型下均未发现有效的多项式时间算法，因此具有较长时间的安全分析积累。

McEliece方案的优势在于安全稳定性较高，自提出以来长期未被实质性攻破。其主要不足是公钥尺寸极大，通常达到数百KB甚至更高，对存储、通信和协议集成提出较高要求[10]。尽管结构化编码可在一定程度上降低公钥规模，但也可能引入新的代数结构和安全分析负担。因此，基于编码的方案更适合对带宽不敏感、但强调长期安全性的场景。

2.4 基于多变量多项式的密码方案

基于多变量多项式的密码方案以多变量二次方程组（Multivariate Quadratic, MQ）问题[35]为安全基础。该问题要求在有限域上求解非线性多项式方程组，被证明为NP-hard问题，在量子模型下也缺乏高效通用解法[36]。

多变量方案在数字签名场景中通常具有较高效率，尤其在签名生成阶段表现突

出。然而，该方向的安全稳定性较为敏感，历史上多次出现方案提出后被有效攻击的情况[37][38]。相关攻击通常与隐藏结构泄露或参数设计不当有关。因此，多变量密码方案需要更严格的参数选择和公开安全分析，其长期可靠性仍需持续验证。

2.5 基于同源映射的密码方案与算法选型权衡

除上述主要类别外，研究者还探索了若干其他后量子密码方向[39]，其中较具代表性的是基于同源映射[40]（Isogeny）的密码方案。该类方案利用椭圆曲线之间的同源映射构造公钥密码，其突出特点是公钥和密文尺寸较小[41]。然而，近年来部分同源密码构造受到有效攻击[42]，显示出该方向在参数设计、构造选择和安全分析方面仍需持续验证。这一发展反映出，在后量子密码设计中，结构紧凑并不必然意味着更高的安全性。

进一步来看，不同后量子密码算法在安全性、计算效率与通信开销等方面呈现出明显差异。例如，格基方案在计算效率上具有优势，但通信成本相对较高；哈希基方案安全假设较为简洁，但在签名尺寸与计算开销方面代价较大；而同源映射方案虽然在密钥尺寸上具有优势，但其安全性稳定性仍存在不确定性。这些差异表明，各类算法在不同性能维度之间形成了显著的权衡关系。

从工程角度看，后量子密码算法的选型不宜依赖单一指标，而应在安全性、计算性能、通信开销以及实现复杂度等多个维度之间进行综合权衡。不同应用场景对上述因素的关注重点存在差异，例如在带宽受限环境中更关注通信成本，而在高安全需求场景中则更强调安全假设的稳健性。上述分析从算法层面对不同技术路径的特征进行了初步抽象，也为后续章节中关于实现与性能评测的系统分析提供了基础。

3 后量子密码与硬件平台的适配与优化

在前文对后量子密码算法体系进行分类与分析的基础上，可以进一步看到，不同算法范式在计算结构、数据表示和参数规模方面存在显著差异。这些差异不仅影响算法性能，也直接决定其在实际硬件平台上的实现方式与优化路径。为刻画这种差异，本文在表2中对格基、哈希基、编码基、多变量及同源映射方案在CPU、FPGA以及专用集成电路（application-specific integrated circuit，ASIC）/嵌入式平台上的实现特征进行归纳对比。

从表2可以看出，各类算法在并行性、存储访问模式、资源占用和实现复杂度等方面存在明显差异。例如，格基方案具有较强的数据并行性，适合向量化与流水线加速；编码基方案则更容易受到公钥尺寸和内存带宽的约束。因此，后量子密码的工程实现本质上涉及算法计算模式、存储结构与硬件架构之间的协同优化。本章将从计算与存储特性出发，分析后量子密码在不同硬件环境下的实现问题，并讨论侧信道安全与软硬协同优化趋势。

3.1 后量子算法的计算与存储特性

与传统公钥密码相比，多数后量子密码算法以向量和多项式运算为核心计算单元。基于格的方案通常依赖大规模模运算、多项式乘法和采样操作[43]，而基于编码和哈希的方案则涉及高维线性代数或大量哈希计算。这类运算呈现出明显的数据并行性，但同时带来了较高的内存访问压力[5]。

表2 硬件平台与后量子密码算法范式对照表

算法范式	CPU(AVX/NEON)	FPGA	ASIC/嵌入式设备	实现关注点
基于格 LWE Ring-LWE Module-LWE	适配性强，向量化效果好	并行度高，吞吐量优势明显	资源占用较高，需参数裁剪	多项式乘法、采样、恒定时间实现
基于哈希 Merkle XMSS SPHINCS+	实现简单，性能稳定	易于流水线实现	计算与存储开销偏大	哈希吞吐率、签名尺寸
基于编码 McEliece	计算高效，内存压力大	存储需求高	公钥尺寸限制明显	公钥存储、内存访问
基于多变量多项式MQ	签名生成速度快	结构复杂，利用率有限	参数敏感，安全风险高	结构隐藏、实现安全
基于同源映射 Isogeny-based	计算开销大	设计复杂	实现难度高	长时运算、实现稳定性

在存储方面，多数后量子公钥密码方案需要显著大于传统算法的密钥或中间状态空间。尤其是基于编码的方案，其公钥规模可达数百KB，这对缓存层级、片上存储以及数据搬移效率产生直接影响[33]。因此，后量子密码的实现往往受到存储带宽而非纯计算能力的限制。上述计算与存储特性的组合，使得后量子密码在硬件实现中必须同时考虑并行度设计与内存层级优化。这一特征也决定了不同硬件平台在支持后量子密码时呈现出明显差异。

3.2 通用处理器平台上的实现挑战（CPU）

在通用处理器平台上，后量子密码实现的主要目标是充分利用指令级并行能力。针对x86架构，AVX指令集可用于加速向量和多项式运算；在ARM架构中，NEON指令提供了类似的并行支持[44]。然而，后量子算法往往具有复杂的控制流和非规则内存访问模式，这限制了自动向量化的效果。高性能实现通常需要对数据布局、参数表示和运算顺序进行手工优化。若实现不当，不仅性能提升有限，还可能引入可观测的时序差异。

此外，通用处理器平台上的实现还需要兼顾恒定时间执行要求[45]。为避免侧信道泄露，部分条件分支和内存访问必须被消除或替换，这在一定程度上抵消了向量化带来的性能优势。因此，CPU平台上的后量子密码实现往往在性能与实现安全性之间进行权衡。

3.3 FPGA与专用硬件实现

FPGA[46]具有高度可重构性，能够灵活构建并行数据通路与深度流水线结构，特别适用于后量子密码中具有规则计算模式的核心算子加速。在格基密码中，多项式乘法与数论变换（number theoretic transform，NTT）等操作具有良好的数据并行性，可通过并行乘法单元与流水线设计实现高吞吐率执行。此外，FPGA片上资源（如BRAM和DSP单元）可用于缓存中间结果并加速模运算，从而降低访存

延迟。

然而，FPGA 实现通常需要针对算法结构进行定制化设计，例如数据布局优化与流水线调度，这使得开发复杂度较高。同时，在资源受限情况下（如逻辑单元或存储块不足），需要对参数规模进行裁剪，从而在性能与安全性之间进行权衡。因此，FPGA 更适用于算法原型验证、中等规模部署以及对能效有一定要求的场景。

ASIC 通过定制化电路实现算法级优化，能够针对后量子密码中的关键运算（如模乘、多项式乘法、哈希函数计算）设计专用硬件模块，从而在延迟、吞吐率与能效比方面达到最优水平。例如，可通过专用 NTT 加速单元或哈希流水线实现低时延计算，并通过电路级优化减少功耗。

然而，ASIC 设计[47]具有较高的前期开发成本和较长的设计周期，其硬件结构在流片后基本固定，缺乏灵活性。当后量子密码标准仍处于演进阶段时，参数调整或算法替换可能导致现有设计失效，从而带来额外成本。因此，ASIC 更适用于标准已稳定、需求规模较大且对性能和能耗要求严格的长期部署场景。

嵌入式设备通常面临严格的资源约束[48]，包括有限的计算能力、存储空间与功耗预算，这使得后量子密码的部署面临较大挑战。具体而言，部分后量子算法（如码基方案）由于公钥尺寸较大，会对片上存储与内存带宽造成显著压力；而格基方案中的多项式运算则对计算能力提出较高要求。

需要指出的是，不同后量子算法范式在专用硬件上的适配性差异明显。基于格的方案更易映射为并行数据通路，而基于编码的方案则更容易受到存储瓶颈的制约。这种差异直接影响算法在资源受限场景中的可行性。

3.4 侧信道攻击与物理安全问题

后量子密码算法在硬件实现中同样面临侧信道攻击风险[49]，包括时序分析、功耗分析和电磁泄露等[50]。近期研究进一步表明，PQC 虽然面向量子攻击设计，但其具体实现仍可能受到传统物理攻击威胁[51]，因此实现层防护不能被忽视[52]。由于许多后量子方案涉及随机采样、条件分支和多阶段计算，其实现若缺乏防护，容易泄露与密钥相关的信息。

与传统公钥密码相比，后量子算法的数据结构更为复杂，中间状态更多，这扩大了潜在的攻击面。研究表明，即使在理论上安全的后量子算法，在实现层面仍可能因侧信道泄露而被有效攻击[53]。因此，后量子密码的安全评估必须同时覆盖算法层和实现层。在实践中，实现者通常通过恒定时间执行、随机掩码和噪声注入等手段降低侧信道风险。然而，这些防护措施往往会带来额外的性能和能耗开销，使得实现安全性与效率之间的平衡成为长期挑战。

3.5 软硬协同优化趋势

后量子密码算法在计算复杂度与数据规模上的显著提升，使得单一软件或硬件优化难以同时满足性能与安全需求。因此，近年来的研究逐渐转向软硬协同优化策略[54]。

从动机上看，一方面，后量子算法涉及大量多项式运算与内存访问，软件优化难以充分挖掘底层硬件并行能力；另一方面，纯硬件实现缺乏灵活性，难以适应标准演进与参数调整。因此，软硬件协同成为在性能、灵活性与安全性之间取得平衡的有效途径。

在软件层面，通过数据布局优化、向

量化指令（如AVX2）以及算法流程重构，可以显著减少计算冗余。例如，在Kyber实现中，通过优化NTT数据排列可减少缓存未命中率，从而提升整体性能。

在硬件层面，研究者开始探索针对后量子密码的专用指令扩展和加速模块[55]，以提升关键操作的执行效率。这种协同设计方式有助于在保证实现安全性的同时缓解性能瓶颈。通过软硬件协同设计，可以在保证恒定时间执行等安全要求的前提下，实现更高性能与更低能耗。因此，该趋势不仅源于性能需求，也源于实现安全与算法灵活性的综合考虑。

4 后量子评测方法、测试数据与性能对比

后量子密码的工程可行性不仅取决于理论安全性[56]，还取决于实际运行开销与通信成本。本章基于统一测试环境，对传统签名算法、后量子签名算法、混合签名方案以及主流后量子KEM进行系统评测分析。测试平台为Intel i9-14900K（24核）、Ubuntu 22.04，采用OpenSSL[57]3.5.0与liboqs 0.15.0及oqs-provider 0.12.0-dev实现。对于国内研究团队提出并在公开密码库中提供实现的后量子密码方案，本文基于PQMagic[14]完成测试。由于不同算法依赖的实现库存在差异，本文尽可能统一硬件环境、操作系统与测试流程，以降低实现差异对评测结果的影响。

4.1 安全级别与参数集匹配原则

在比较后量子签名算法与KEM算法性能之前，需要首先明确安全等级与参数集之间的对应关系。不同算法家族通常通过调整参数规模来匹配不同的对称安全强度等级，例如Module-LWE类方案提供L1至L5等级的参数配置，哈希基或码基方案则通过扩展结构规模提升安全强度。如果跨安全等级直接比较计算时间、签名长度、公钥大小或密文大小，所得结论将缺乏公平性。因此，本文的性能分析均以安全等级近似一致为前提，并采用系列区间统计方式进行趋势性讨论。

安全等级的提升通常会同时影响计算复杂度与通信成本。在签名算法中，安全等级提升可能带来签名长度、签名时间和验签时间的增加；在KEM算法中，则通常对应公钥尺寸、密文尺寸以及封装/解封装开销的变化。不同算法范式的增长趋势并不相同：格基方案在高等级参数下通常仍能维持较低延迟，传统RSA类算法的计算代价随模数扩展迅速增加，码基方案则更容易表现出公钥尺寸膨胀。基于上述原则，本文后续分别对签名算法与KEM算法的计算和通信开销进行分析，以揭示不同技术路线在实际部署中的性能权衡。

4.2 签名算法的计算与签名开销分析

如表3所示，传统签名算法在安全等级提升时呈现明显的性能扩展代价。RSA系列的密钥生成时间范围为4.42至185720 ms，签名时间范围为0.05至356.07 ms。随着模数长度增加，其计算时间呈数量级增长，说明RSA依赖参数放大提升安全强度，性能代价随之迅速累积。相比之下，DSA与SM2的计算时间保持在较低区间，签名时间多处于十毫秒量级，签名长度维持在几十字节范围内，在经典计算模型下具有较高通信效率。传统体系中，椭圆曲线类算法在计算效率与签名长度之间实现较好平衡，RSA则表现出更明

显的参数扩展成本。

在后量子签名算法中，基于格问题的Falcon与ML-DSA系列呈现较为均衡的性能特征。Falcon系列的签名时间为14至18 ms，验签时间为10至16 ms，签名长度为658至1280字节，其计算性能接近传统椭圆曲线算法，但签名长度明显增加。ML-DSA系列的签名时间为8至18 ms，验签时间为6至15 ms，签名长度为2420至4627 字节。虽然通信开销高于Falcon，其计算时间仍控制在几十毫秒范围内。在相近安全等级条件下，格基签名方案在计算效率与签名长度之间实现较为稳定的平衡，因此成为当前后量子签名标准化的核心方向。

基于哈希函数的SLH-DSA系列在性能分布上表现出不同特征。其密钥生成时间为9至124 ms，签名时间为20至882 ms，签名长度为7856至49856字节。部分高安全等级参数集的签名时间接近800 ms，签名长度接近50 KB，显著高于格基方案。这种高计算与通信开销源于哈希树结构设计。该类方案仅依赖哈希函数抗碰撞性这一安全假设，安全基础相对简洁且稳健，因此更强调长期安全性，对通信效率的要求相对次要。

混合签名方案在性能上体现出明显叠加特征。其密钥生成时间范围为22至205 ms，签名时间为11至108 ms，签名长度为729至35771字节。由于同时包含经典与后量子算法结构，其计算与通信成本高于单一方案。混合签名在量子计算能力尚未成熟的阶段提供双重安全保障，适用于迁移过渡场景。但其计算复杂度和通信负担较高，不利于长期高效部署。

如表4所示，总体来看，在相近安全等级条件下，格基签名算法在计算效率与签名长度之间取得较为合理的折中。哈希基方案以更高通信代价换取安全假设的简洁性。混合方案强调过渡阶段的安全冗余。不同技术路径在安全性、性能与通信成本之间形成清晰的权衡结构，这一结构构成当前后量子签名设计与标准化进程的重要特征。

4.3 KEM算法的计算与通信开销分析

在密钥封装机制的评测中，性能与通信成本同样必须建立在安全等级近似匹配的前提之上。与签名算法类似，不同KEM算法通过参数规模调节对应不同对称安全强度等级。Kyber与ML-KEM系列覆盖L1、L3与L5三个典型安全等级。BIKE、FrodoKEM与NTRU等方案则代表不同安全假设和候选/研究路线，其成熟度和标准化状态存在差异。性能比较应在相近安全强度条件下进行，否则不同安全等级之间的直接对比难以反映算法结构本身的效率差异。

从表5可以观察到，不同算法家族在计算效率与通信开销方面呈现出明显分化。基于Module-LWE的Kyber与ML-KEM系列在性能上表现最为突出。其密钥生成时间稳定在0.01毫秒量级，封装与解封装时间同样维持在0.01毫秒区间，公钥与密文尺寸分别处于800至1568字节范围内。该系列在计算延迟与通信开销之间实现了高度均衡，体现出良好的工程优化程度和硬件适配能力。这一结果与其已进入NIST标准化阶段的成熟度相一致。

基于标准LWE的FrodoKEM在性能上呈现不同特征。其密钥生成时间范围为0.17至1.88毫秒，封装与解封装时间处于0.23至2.01毫秒区间。虽然计算时间仍保持在毫秒级，但公钥与密文尺寸显著扩大，达到数千至两万字节以上。相比Module-

表3 传统、后量子与混合签名算法的计算开销与签名尺寸对比

算法类别	算法名称	代表算法	密钥生成时间范围	计算速度（签名/验签）	签名大小范围
传统签名算法	DSA系列	DSA1024DSA2048	0.29 - 25.00 ms	签名:0.21 - 14.00 ms验签: 0.13 - 17.00 ms	40 - 139 B
	RSA系列	RSA512RSA1024RSA2048RSA4096	4.42 - 185720.00 ms	签名:0.05 - 356.07 ms验签: 0.00 - 1.49 ms	64 - 1920 B
	SM2系列	SM2	19.00 ms	签名: 12.00ms验签: 14.00ms	71 B
后量子签名算法	Falcon系列	Falcon512Falcon1024	9.00 - 31.00 ms	签名: 14.00 - 18.00 ms 验签: 10.00 - 16.00 ms	658 - 1280 B
	ML-DSA系列	ML-DSA-44ML-DSA-65ML-DSA-87	7.00 - 21.00 ms	签名:8.00 - 18.00 ms验签: 6.00 - 15.00 ms	2420 - 4627 B
	SLH-DSA-SHA2系列	SLH-DSA-SHA2-128sSLH-DSA-SHA2-128fSLH-DSA-SHA2-192sSLH-DSA-SHA2-192fSLH-DSA-SHA2-256sSLH-DSA-SHA2-256f	13.00 - 83.00 ms	签名: 20.00 - 505.00 ms 验签:5.00 - 11.00 ms	7856 - 49856 B
	SLH-DSA-SHAKE系列	SLH-DSA-SHAKE-128sSLH-DSA-SHAKE-128fSLH-DSA-SHAKE-192sSLH-DSA-SHAKE-192fSLH-DSA-SHAKE-256sSLH-DSA-SHAKE-256f	9.00 - 124.00 ms	签名: 30.00 - 882.00 ms 验签: 5.00 - 7.00 ms	7856 - 49856 B
混合签名算法	混合签名系列	p256_mldsa44rsa3072_mldsa44p256_falcon512rsa3072_falcon512p256_falconpadded512rsa3072_falconpadded512p256_sphincssha2128fsimplersa3072_sphincssha2128fsimplep256_sphincsshake128fsimplersa3072_sphincsshake128fsimple	22.00 - 205.00 ms	签名: 11.00 - 108.00 ms 验签:7.00 - 15.00 ms	729 - 35771 B

表4 签名算法安全性与成熟度对比表

算法类别	算法名称	安全性/成熟度
传统签名算法	DSA系列	基于离散对数问题,经典算法,成熟度高
	RSA系列	基于大整数分解,经典安全假设,成熟度高
	SM2系列	基于椭圆曲线密码,国家商用标准,成熟度高
后量子签名算法	Falcon系列	基于格问题(NTRU),NIST选定用于标准化,成熟度高
	ML-DSA系列	基于格问题(L2 - L5安全),NIST标准化,成熟度高
	SLH-DSA-SHA2系列	基于哈希函数安全性(L1 - L5安全),NIST标准化,成熟度高
	SLH-DSA-SHAKE系列	基于哈希函数安全性(L1 - L5安全),NIST标准化,成熟度高
混合签名算法	混合签名系列	经典算法 + 后量子算法组合,提高过渡期安全性,工程复杂度较高

LWE结构，标准LWE方案在通信开销上付出更高代价。其设计强调安全假设的简洁性，因此在尺寸上做出权衡。

NTRU系列在性能分布上具有一定波动性。密钥生成时间范围为0.02至2.56毫秒，封装与解封装时间集中在0.01至0.12毫秒区间。公钥与密文尺寸控制在数百至两千字节范围内，整体通信成本较低。该系列在计算效率与通信效率之间保持相对均衡，但安全等级标注尚不统一，其工程成熟度主要来源于长期研究与实现积累。

BIKE系列属于码基密码方案，其密钥生成时间为0.14至0.72毫秒，封装与解封装时间为0.39至3.07毫秒。其公钥与密文尺寸处于一至五千字节区间。与格基方案相比，其计算时间略有增加，但通信开销仍保持在可接受范围内。BIKE仍处于NIST候选阶段，其长期部署稳定性尚需进一步验证。

Classic-McEliece作为码基方案的代表，在性能与通信特征上呈现出显著差异。其密钥生成时间范围为16.92至118.08毫秒，远高于其他家族，同时公钥尺寸达到261120至1357824字节区间。密文尺寸则维持在百字节级别。这种结构体现出典型的公钥膨胀特征。虽然封装与解封装时间仅为0.08至0.12毫秒，计算效率较高，但其极大的公钥尺寸在带宽受限环境中构成明显压力。该方案历史悠久，安全基础稳固，但通信代价成为其主要约束因素。

综合表5与表6可以看出，后量子KEM算法在结构上形成三种典型模式。基于Module-LWE的方案在计算与通信之间取得较好平衡。基于标准LWE的方案在尺寸上代价较高但安全假设更直接。基于码理论的方案在计算效率与通信尺寸之间呈现明显结构分离。不同技术路线在性能与安全假设之间形成清晰的权衡关系。

4.4 国内研究团队后量子密码方案的性能评测与分析

前文主要围绕国际主流后量子密码方案展开了系统评测，但从实际研究与工程应用角度看，对国内研究团队提出并公开实现的后量子密码方案进行性能分析同样具有必要性。为此，本小节进一步选取若干由国内研究团队提出、并已在公开密码库中提供实现的后量子签名与KEM方案进行测试。

根据表7可以看出，上述国内公开实现的后量子密码方案在性能分布上同样呈现出明显的家族差异，其总体规律与前文对国际主流方案的分析基本一致。具体而言，基于格的AIGIS系列在计算效率上表现突出，而基于哈希的SPHINCS-Alpha

表5 主流后量子KEM算法的计算开销与通信开销对比

算法家族	代表算法	公钥大小范围	密文大小范围	密钥生成时间范围	计算速度（封装/解封装）
BIKE	BIKE-L1BIKE-L3BIKE-L5	1541 - 5122 B	1573 - 5154 B	0.14 - 0.72 ms	封装:0.39 - 3.07 ms解封装:0.39 - 3.07 ms
FrodoKEM	FrodoKEM-640-AESFrodoKEM-640-SHAKEFrodoKEM-976-AESFrodoKEM-976-SHAKEFrodoKEM-1344-AESFrodoKEM-1344-SHAKE	9616 - 21520 B	9720 - 21632 B	0.17 - 1.88 ms	封装:0.23 - 2.01 ms解封装:0.23 - 2.01 ms
Kyber	Kyber512Kyber768Kyber1024	800 - 1568 B	768 - 1568 B	0.01ms	封装:0.01 ms解封装:0.01 ms
ML-KEM	ML-KEM-512ML-KEM-768ML-KEM-1024	800 - 1568 B	768 - 1568 B	0.01 ms	封装:0.01 ms解封装:0.01 ms
NTRU	NTRU-HRSS-701NTRU-HPS-4096-1229NTRU-HRSS-1373NTRU-HPS-4096-821NTRU-HPS-2048-677NTRU-HPS-2048-509	699 - 2401 B	699 - 2401 B	0.02 - 2.56 ms	封装:0.01 - 0.12 ms解封装:0.01 - 0.12 ms
Classic-McEliece	Classic-McEliece-348864Classic-McEliece-348864fClassic-McEliece-460896Classic-McEliece-460896fClassic-McEliece-6688128Classic-McEliece-6688128fClassic-McEliece-6960119Classic-McEliece-6960119fClassic-McEliece-8192128Classic-McEliece-8192128f	261120 - 1357824 B	96 - 208 B	16.92 - 118.08 ms	封装:0.08 - 0.12 ms解封装:0.08 - 0.12 ms

表6 主流后量子KEM算法安全基础与成熟度分析

算法家族	安全基础	安全等级汇总	成熟度说明	一致性错误总数
BIKE	基于码基问题	覆盖多个安全等级	NIST第四轮候选	0
FrodoKEM	基于标准LWE问题	覆盖多个安全等级	非标准化方案工程实现较成熟	0
Kyber/ML-KEM	基于Module-LWE问题	L1 (≈AES-128)/L3 (≈AES-192)/L5 (≈AES-256)	NIST已标准化	0
NTRU	基于NTRU格问题	覆盖多个安全等级	研究与工程实现较成熟	0
Classic McEliece	基于Goppa码译码问题	覆盖多个安全等级	历史悠久,公钥较大	0

系列则在计算与签名开销上更为显著。这表明，相关国内研究方案在算法设计思路上与当前后量子密码主流技术路线具有较高一致性，不同方案之间同样体现出安全性、计算效率与通信开销之间的结构性权衡。

在签名算法方面，AIGIS-SIG系列表现出较为均衡的综合性能。其密钥生成时间范围为0.053 - 0.079 ms，签名时间范围为0.164 - 0.240 ms，验签时间范围为0.035 - 0.069 ms，整体均保持在较低水平；同时签名大小范围为1852 - 3046 B。相比之下，SPHINCS-Alpha系列的密钥生成时间范围扩大至0.499 - 37.894 ms，签名时间范围达到12.79 - 523.749 ms，验签时间范围为0.668 - 2.319 ms，签名大小范围也增至7856 - 49856 B。可见，AIGIS-SIG在计算效率与签名长度之间实现了较好的平衡，更适合对实时性和资源开销较为敏感的应用场景；而SPHINCS-Alpha则延续了哈希基签名方案安全假设简洁但开销较高的典型特征，更适用于对长期安全性要求较高、但对通信与计算代价相对不敏感的场景。

在KEM算法方面，AIGIS-ENC系列表现出较高的效率与较低的通信开销。其公钥大小范围为672 - 1440 B，密文大小范围为736 - 1568 B，密钥生成时间范围为0.032 - 0.123 ms，封装时间范围为0.044 - 0.067 ms，解封装时间范围为0.037 - 0.083 ms，整体均维持在较低水平。这说明AIGIS-ENC在计算延迟与通信成本之间取得了较为理想的平衡，体现出格基KEM方案良好的工程适配能力。综合来看，国内公开实现的后量子密码方案在性能表现上已具备一定实用潜力：AIGIS系列更突出效率优势，SPHINCS-Alpha系列则更强调安全基础的稳健性。该结果不仅补充了前文对国际主流方案的分析，也说明国内研究团队在后量子密码设计与实现方面已经形成了较为清晰的技术路线。

需要指出的是，上述国内研究方案的性能结果应结合其安全等级与标准化成熟度进行理解。一方面，AIGIS系列与SPHINCS-Alpha系列在参数设计上同样面向后量子安全需求，但其安全级别划分、参数集对应关系及评测体系与NIST标准方案并不完全等同，因此与国际主流算法的性能对比更适合用于趋势分析，而不宜

简单视为严格的一一对应比较。另一方面，相较于已进入国际标准体系的ML-KEM、ML-DSA和SLH-DSA等方案，上述国内研究方案在标准化成熟度、生态支持与公开评测积累方面仍存在阶段性差异。因此，对相关方案的评估除了关注计算效率与通信开销外，也应结合其安全分析充分性与工程成熟度进行综合判断。

表7 国内后量子签名与KEM算法性能评测结果

国内后量子签名算法				
算法家族	代表算法	签名大小范围	密钥生成时间范围	计算速度（签名/验签）
AIGIS-SIG	AIGIS_SIG_1AIGIS_SIG_2AIGIS_SIG_3	1852 – 3046 B	0.053–0.079 ms	签名:0.164–0.240 ms 验签:0.035–0.069 ms
SPHINCS-Alpha	SPHINCS_Alpha_SHA2_128f SPHINCS_Alpha_SHA2_192f SPHINCS_Alpha_SHA2_256f SPHINCS_Alpha_SHA2_128s SPHINCS_Alpha_SHA2_192s SPHINCS_Alpha_SHA2_256s	7856 – 49856 B	0.499 – 37.894 ms	签名:12.79–523.749 ms验签:0.668 – 2.319 ms

国内后量子KEM算法					
算法家族	代表算法	公钥大小范围	密文大小范围	密钥生成时间范围	计算速度（封装/解封装）
AIGIS-ENC	AIGIS_ENC_1AIGIS_ENC_2 AIGIS_ENC_3 AIGIS_ENC_4	672 –1440 B	736 –1568 B	0.032 –0.123 ms	封装:0.044 – 0.067 ms 解封装:0.037 – 0.083 ms

4.5 Benchmark框架、评测公平性与综合分析

性能评测结果高度依赖具体实现环境。即使在相同硬件平台上，不同库版本、编译选项以及是否启用向量指令优化都会对测试结果产生影响。本章所有评测基于统一的软件框架和实现环境，以减少实现层差异带来的干扰。然而，不同算法在底层优化程度上仍可能存在差异。例如，部分格基算法已针对AVX2等指令集进行深度优化，而部分码基方案的优化程度相对有限。这种差异可能影响绝对时间数值，但通常不会改变整体性能分布趋势。对于物联网（internet of things，IoT）[58]和嵌

入式设备，PQC的部署成本更加敏感，真实场景下的评测需要同时考虑计算延迟、内存占用、网络接口与证书链大小。

公平比较应满足安全等级一致、硬件平台一致以及实现优化程度相近三个基本条件。如果缺乏上述前提，性能数据只能反映特定环境下的表现，而不能推广为普遍结论。因此，对评测结果的解读必须建立在明确测试环境和参数设定的基础之上。

在统一评测条件下，综合表3至表7的数据可以观察到清晰的结构性差异。基于格问题的签名与KEM方案在通用处理器平台上表现出较好的均衡性，计算延迟与通信开销均控制在合理范围内。基于哈希的签名方案在通信成本方面压力较大，尤其在高安全等级参数下签名尺寸显著增加。基于码理论的KEM方案在封装和解封装时间上具有优势，但公钥尺寸膨胀问题突出。混合签名方案在计算与通信开销上体现叠加效应，更适合迁移阶段部署。从表7所示的国内公开实现方案结果来看，这一总体规律在相关国内研究方案中同样成立。具体而言，基于格的AIGIS-SIG与AIGIS-ENC系列在签名、验签、封装与解封装时间上均保持在较低区间，同时其签名、公钥与密文尺寸处于相对可控范围，体现出较好的综合均衡性；而基于哈希的SPHINCS-Alpha系列则呈现出签名时间较长、签名尺寸显著增大的特征，表现出与国际主流哈希基签名方案相一致的性能分布趋势。

这些结果表明，后量子密码的部署决策不能仅依赖理论安全性评价，而应同时考虑安全等级、计算代价与通信资源约束。同时，对国内公开实现后量子密码方案的补充评测结果说明，不同技术路线之间的结构性权衡并非局限于国际标准候选方案，而是后量子密码设计中的普遍现象。性能评测为系统架构设计与标准选择提供了量化依据，也强调了评测环境透明性与参数匹配原则的重要性。在未来标准演进与大规模部署过程中，这种综合评估框架将成为算法选择的重要参考基础。

5 后量子密码的挑战、开放问题与统一评估框架

5.1 当前面临的主要挑战

后量子密码已经从理论研究阶段进入标准化与工程部署阶段[59][60]。然而，从算法设计到系统落地，仍存在一系列关键挑战[61]。首先，尽管部分后量子算法已进入标准化阶段，其长期安全性仍需持续验证。部分密码范式在历史上曾出现参数失效或结构漏洞问题，这表明后量子算法的安全评估仍需依赖长期的公开分析、持续审查与参数修正机制。

其次，理论安全性并不等同于实现安全性。后量子算法通常涉及复杂的数据结构、随机采样过程以及大规模中间状态，这增加了侧信道攻击和实现缺陷的风险。在高性能实现与恒定时间执行之间如何取得平衡，仍是工程实践中的核心问题。特别是在CPU、FPGA、ASIC与嵌入式平台上，不同算法家族在并行性、存储访问模式和资源占用方面差异显著，使实现安全成为部署中的关键约束。

再次，后量子算法在密钥长度、签名尺寸和计算模式上与传统算法存在明显差异，直接影响带宽消耗、存储需求和协议结构。现有系统大多围绕RSA或ECC构建，直接替换算法往往需要同步调整协议流程和基础设施。因此，后量子迁移不仅是密码原语替换问题，也涉及系统级重构、兼容性维护与综合成本评估。

5.2 面向部署的多维评估框架

基于前文对算法体系、硬件实现和统一评测结果的讨论，后量子密码算法的选型可进一步抽象为一个面向部署的多维评估问题。与传统密码主要围绕安全性和计算效率进行评估不同，后量子密码的实际应用需要同时考虑多个维度。

第一是安全性维度，包括对经典与量子攻击的抵抗能力、安全假设的简洁性、历史分析深度以及长期稳定性。不同方案在这一维度上差异明显，例如格基方案具有较强的理论基础与工程活跃度，哈希基方案的安全假设相对简洁，而部分结构紧凑的方案可能在后续分析中暴露新的风险。

第二是计算性能维度。密钥生成、签名、验签、封装与解封装的时间开销直接影响系统吞吐率与响应延迟。前文评测表明，格基签名与KEM方案通常表现出较好的效率均衡性，而哈希基签名方案在签名阶段开销更大。国内公开实现方案的测试结果也体现出类似趋势：AIGIS系列保持较低时延，SPHINCS-Alpha则表现出较高的签名时间。

第三是通信与存储开销维度。后量子密码普遍存在密钥、密文或签名尺寸增大的问题，这不仅影响带宽占用，也会影响缓存利用、内存访问和协议报文设计。前文结果显示，码基KEM方案在公钥尺寸上膨胀明显，哈希基签名在高安全等级下的签名长度也显著增加，而格基方案通常在通信与效率之间实现较平衡的折中。

第四是实现复杂度与工程成熟度维度。后量子算法的硬件适配能力、恒定时间实现难度、对随机数质量和侧信道防护的敏感程度，都会影响其部署难度。同时，算法的标准化成熟度、生态支持程度以及公开实现与测试积累，也直接影响工程落地风险。相比已进入国际标准体系的主流方案，国内公开实现的后量子密码方案在性能上已表现出一定潜力，但在公开评测积累、生态兼容性和标准化成熟度方面仍需进一步发展。

综合来看，后量子密码算法不存在能够在所有维度上均占优的统一最优方案，其选型本质上是面向具体应用场景的多维权衡过程。在高安全场景中，应优先强调安全假设的稳健性与长期验证基础；在实时通信场景中，应更关注计算时延；在资源受限环境中，则需重点考虑通信与实现成本。因此，后量子密码的部署决策应从单指标比较转向多维框架评估。

5.3 未来研究方向与总结

在过渡阶段，混合密码机制为兼容性与安全性提供了一种折衷方案。通过同时使用传统与后量子算法，可以在短期内降低迁移风险，但也会带来额外的计算与通信开销。因此，如何在安全冗余与系统效率之间取得更合理的平衡，仍是后量子部署中的重要问题。与此同时，后量子迁移不仅涉及算法选择，还涉及协议结构调整与安全证明更新。如何在传输层安全协议（transport layer security，TLS）[62]、虚拟专用网络（virtual private network，VPN）及身份认证框架中实现平滑升级，并通过密码敏捷性设计支持算法快速替换、参数更新与版本演进，将是实际部署中的关键方向。

此外，后量子密码需要在开放评估环境中持续接受密码分析与实现审查。随着分析结果与计算能力的发展，参数集可能不断调整，因此构建可演进的参数体系与长期验证机制，是保证未来安全性的必要条件。对于国内研究团队提出并公开实现的后量子密码方案而言，除继续优化性能

与实现效率外，还需要在公开安全分析、标准化推进、工程生态支持及跨平台评测体系建设方面进一步完善，从而推动其走向更成熟的系统部署。

总体而言，后量子密码研究的重点已逐步从替代传统公钥算法的构造，转向面向真实系统约束的部署与优化问题。本文从传统体系的量子脆弱性出发，系统综述了主流后量子密码算法范式、硬件适配问题、性能评测方法以及国际与国内研究方案的性能特点，并进一步归纳了面向部署的多维评估视角。后量子密码的未来发展，不仅取决于算法本身的理论安全性，也取决于安全、性能、通信与实现之间能否形成合理平衡。

参考文献：

[1] Monz T, Nigg D, Martinez E A, et al. Realization of a scalable Shor algorithm [J]. Science, 2016, 351(6277): 1068-1070.

[2] Joseph D, Misoczki R, Manzano M, et al. Transitioning organizations to post-quantum cryptography[J]. Nature, 2022, 605(7909): 237-243.

[3] Mosca M. Cybersecurity in an era with quantum computers: Will we be ready? [J]. IEEE Security & Privacy, 2018, 16 (5): 38-41.

[4] Grover L K. A fast quantum mechanical algorithm for database search[C]//Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996: 212-219.

[5] Bernstein D J. Post-quantum cryptography[M]//Encyclopedia of Cryptography, Security and Privacy. Cham: Springer Nature Switzerland, 2025: 1846-1847.

[6] Chen L, Chen L, Jordan S, et al. Report on post-quantum cryptography[M]. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.

[7] Alagic G, Dang Q, Moody D, et al. Module-lattice-based key-encapsulation mechanism standard[S]. 2024.

[8] Dang T, Lichtinger J, Liu Y K, et al. Module-lattice-based digital signature standard[S]. 2024.

[9] Cooper D. Stateless hash-based digital signature standard[S]. 2024.

[10] Alagic G, Alagic G, Apon D, et al. Status report on the third round of the NIST post-quantum cryptography standardization process[R]. 2022.

[11] Alagic G, Barker E, Chen L, et al. Recommendations for key-encapsulation mechanisms[M]. US Department of Commerce, National Institute of Standards and Technology, 2025.

[12] Alagic G, Bros M, Ciadoux P, et al. Status Report on the Second Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process[R]. NIST Interagency/Internal Report (NISTIR) 8528. National Institute of Standards and Technology, 2024.

[13] Barker W, Souppaya M, Newhouse W. Migration to post-quantum cryptography [J]. NIST National Institute of, Standards and Technology and National Cybersecurity, Center of Excellence, 2021: 1-15.

[14] He Y, Hao X, Li J, et al. PQMagic: Towards Secure and Efficient Post Quantum Cryptography Implementations[C]// International Conference on Applied Cryptography and Network Security. Cham: Springer Nature Switzerland, 2025: 152-172.

[15] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[16] Diffie W, Hellman M E. New directions in cryptography[M]//Democratizing cryptography: the work of Whitfield Diffie and Martin Hellman. 2022: 365-390.

[17] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE transactions on information theory, 1985, 31(4): 469-472.

[18] Koblitz N. Elliptic curve cryptosystems [J]. Mathematics of computation, 1987, 48(177): 203-209.

[19] Goldreich O. Foundations of cryptography: volume 2, basic applications[M]. Cambridge university press, 2001.

[20] Nielsen M A, Chuang I L. Quantum computation and quantum information[M]. Cambridge university press, 2010.

[21] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994: 124-134.

[22] Bindel N, Herath U, McKague M, et al. Transitioning to a quantum-resistant public key infrastructure[C]//International Workshop on Post-Quantum Cryptography. Cham: Springer International Publishing, 2017: 384-405.

[23] Ott D, Peikert C. Identifying research challenges in post quantum cryptography migration and cryptographic agility [EB]. arXiv preprint arXiv: 1909.07353, 2019.

[24] Stebila D, Fluhrer S, Gueron S. Hybrid key exchange in TLS 1.3[J]. IETF draft, 2020.

[25] Regev O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 1-40.

[26] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM (JACM), 2013, 60(6): 1-35.

[27] Langlois A, Stehlé D. Worst-case to average-case reductions for module lattices[J]. Designs, Codes and Cryptography, 2015, 75(3): 565-599.

[28] Liu Z, Choo K K R, Grossschadl J. Securing edge devices in the post-quantum internet of things using lattice-based cryptography[J]. IEEE Communications Magazine, 2018, 56(2): 158-162.

[29] Alkim E, Ducas L, P ppelmann T, et al. Post-quantum key {Exchange—A} new hope[C]//25th USENIX security symposium (USENIX Security 16). 2016: 327-343.

[30] Merkle R C. A certified digital signature [C]//Conference on the Theory and Application of Cryptology. New York, NY: Springer New York, 1989: 218-238.

[31] Buchmann J, Dahmen E, Hülsing A. XMSS-a practical forward secure signature scheme based on minimal security assumptions[C]//International Workshop on Post-Quantum Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 117-129.

[32] Bernstein D J, Hülsing A, K lbl S, et al. The SPHINCS+ signature framework [C]//Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. 2019: 2129-2146.

[33] Fathalla E, Azab M. Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations[J].

IEEE Access, 2024.

[34] McEliece R J. A public-key cryptosystem based on algebraic[J]. Coding Thv, 1978, 4244(1978): 114-116.

[35] Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988: 419-453.

[36] Ding J, Gower J E, Schmidt D S. Multivariate public-key cryptosystems[C]//International conference on the Algebra and its application. 2005: 79-94.

[37] Patarin J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms[C]//International conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996: 33-48.

[38] Patarin J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt' 88[C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995: 248-261.

[39] Alagic G, Bros M, Ciadoux P, et al. Status report on the first round of the additional digital signature schemes for the nist post-quantum cryptography standardization process[R]. 2024.

[40] Galbraith S D. Constructing isogenies between elliptic curves over finite fields [J]. LMS Journal of Computation and Mathematics, 1999, 2: 118-138.

[41] Peng C, Chen J, Zeadally S, et al. Isogeny-based cryptography: A promising post-quantum technique[J]. IT Professional, 2019, 21(6): 27-32.

[42] Castryck W, Decru T. An efficient key recovery attack on SIDH[C]//Annual international conference on the theory and applications of cryptographic techniques. Cham: Springer Nature Switzerland, 2023: 423-447.

[43] Peikert C. A decade of lattice cryptography[J]. Foundations and TrendsŴ in Theoretical Computer Science, 2016, 10 (4): 283-424.

[44] Nejatollahi H, Dutt N, Ray S, et al. Post-quantum lattice-based cryptography implementations: A survey[J]. ACM Computing Surveys (CSUR), 2019, 51(6): 1-41.

[45] Barenghi A, Pelosi G. Constant weight strings in constant time: a building block for code-based post-quantum cryptosystems[C]//Proceedings of the 17th ACM International Conference on Computing Frontiers. 2020: 132-141.

[46] Agrawal R, Bu L, Ehret A, et al. Open-source FPGA implementation of post-quantum cryptographic hardware primitives[C]//2019 29th International Conference on Field Programmable Logic and Applications (FPL). IEEE, 2019: 211-217.

[47] Xie J, Basu K, Gaj K, et al. Special session: The recent advance in hardware implementation of post-quantum cryptography[C]//2020 IEEE 38th VLSI Test Symposium. Piscataway, NJ, USA: IEEE, 2020.

[48] Manifavas C, Hatzivasilis G, Fysarakis K, et al. Lightweight cryptography for embedded systems - a comparative analysis[C]//International Workshop on Data Privacy Management. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013: 333-349.

[49] Ravi P, Chattopadhyay A, D'Anvers J P, et al. Side-channel and fault-injection attacks over lattice-based post-

quantum schemes (Kyber, Dilithium): Survey and new results[J]. ACM Transactions on Embedded Computing Systems, 2024, 23(2): 1-54.

[50] Alioto M, Giancane L, Scotti G, et al. Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2009, 57(2): 355-367.

[51] Delgado-Vargas K A, Mancillas-López C, Gallegos-García G. A look at side channel attacks on post-quantum cryptography[J]. Computación y Sistemas, 2024, 28(4): 1879-1896.

[52] Huang Z, Wang H, Cao B, et al. A comprehensive side-channel leakage assessment of CRYSTALS-Kyber in IIoT[J]. Internet of Things, 2024, 27: 101331.

[53] Guo Q, Nabokov D, Nilsson A, et al. Scaldpc: A code-based framework for key-recovery side-channel attacks on post-quantum encryption schemes[C]//International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, 2023: 203-236.

[54] Cheng H, Gro sch dl J, Marshall B, et al. SoK: Instruction Set Extensions for Cryptographers[EB/OL]. Cryptology ePrint Archive, 2024.

[55] Brohet M, Valencia F, Regazzoni F. Instruction Set Extensions for Post-Quantum Cryptography[C]//2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD). IEEE, 2023: 1-6.

[56] Alagic G, Bros M, Ciadoux P, et al. Status report on the fourth round of the nist post-quantum cryptography standardization process[R]. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2025.

[57] Stebila D, Mosca M. Post-quantum key exchange for the internet and the open quantum safe project[C]//International Conference on Selected Areas in Cryptography. Cham: Springer International Publishing, 2016: 14-37.

[58] Hanna Y, Bozhko J, Tonyali S, et al. A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices[J]. Internet of Things, 2025, 33: 101650.

[59] Moody D, Perlner R, Regenscheid A, et al. Transition to post-quantum cryptography standards[R]. National Institute of Standards and Technology, 2024.

[60] Moody D. Advancing Post-Quantum Cryptography: NIST's Standardization Efforts[C]//Proceedings of the 2025 1st Workshop on Quantum-Resistant Cryptography and Security. 2025: 5-5.

[61] Von Nethen N, Wiesmaier A, Alnahawi N, et al. PMMP-PQC Migration Management Process [C]//Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference. 2024: 144-154.

[62] Montenegro J A, Rios R, Lopez-Cerezo J. A performance evaluation framework for post-quantum TLS[J]. Future Generation Computer Systems, 2025: 108062.

作者简介

莫文涛（2000– ），男，清华大学深圳国际研究生院硕士生，主要研究方向为人工智能安全、量子计算安全等。

陶伟（1999– ），男，华中科技大学博士生，主要研究方向为模型量化、云边协同、大模型时序数据应用、大模型长文本推断优化等。在体系结构方向国际顶级会议DATE发表论文2篇，在人工智能方向国际顶级会议ACL、ICASSP、ICME、IJCNN、AAAI等发表论文多篇。

洪振厚（1991–），男，硕士，平安科技前沿机器学习算法分组成员。长期从事深度学习和模型推理加速的工作。已发表论文6篇，授权国家发明专利4项，译著1本。联系邮箱:zhenhouhong@gmail. com

查高密（1991–），男，硕士，平安科技前沿机器学习算法分组数据高级分析师，普林斯顿大学硕士学位。主要研究方向包括人工智能应用、机器学习及密码学。

张旭龙（1988– ），男，博士，平安科技（深圳）有限公司，算法研究员，复旦大学计算机理学博士，2023年入选上海市东方英才计划青年项目。兼任清华大学深圳研究院及中国科学技术大学先进技术研究院校外导师，以及中国指挥与控制学会具身智能专业委员会委员、中国自动化学会联邦数据与联邦智能委员会委员、中国电子音响行业协会声音与音乐技术专委会常务委员。目前是IEEE、中国自动化学会以及中国计算机学会会员。主要研究方向包括大模型、具身智能、跨模态智能计算等。发表学术论文80余篇，获得国家发明专利授权20余项。联系邮箱：zhangxulong@ieee. org

瞿晓阳（1988–），男，博士，平安科技前沿机器学习算法分组负责人，华中科技大学博士，兼任清华大学深圳国际研究院、中国科学技术大学先进技术研究院、哈尔滨工业大学校外研究生导师，以及美国中佛罗里达大学访问学者。长期从事机器学习、大数据与计算体系结构方向的研究，在大模型推理加速、具身智能、联邦学习、持续学习、高性能计算与存储等领域具有丰富的研究与实践经验。近年来，在体系结构方向（如INFOCOM、DAC、TPDS、IPDPS）和人工智能方向（如NeurIPS、AAAI、ACL、ICCV、IJCAI）等国际顶级会议及期刊上发表论文60余篇，多篇论文获评最佳论文奖；担任多家国际顶级期刊审稿人。已授权国家发明专利100余项，出版专著2本，译著1本。联系邮箱：quxiaoy@gmail. com

宋歌（1976– ），女，硕士研究生，清华大学计算机科学与技术系在读工程博士；现任平安银行金融科技部云数据运营中心总经理，及中国银行业协会信息科技与数字金融专业委员会委员、深圳市金融科技协会信息安全专委会副主任、北京金融科技产业联盟专家库专家、ISC 智库专家。主要研究方向为大数据、信息安全等。近年来，主持多个银行重大网络安全项目建设，并在人民银行金融科技发展奖获奖 5 次，其中 1 次二等奖，3 次三等奖，1 次四等奖。作为出品人，组织金融行业安全专家编纂《安全村文集金融行业专刊》，已刊印发行 2022 和 2023 两期。联系邮箱：1079890039@qq. com

王健宗（1983– ），男，博士，正高级工程师，平安科技（深圳）有限公司，智能金融前沿技术研究院院长。美国佛罗里达大学人工智能博士后，美国莱斯大学和华中科技大学联合培养博士，中国计算机学会杰出会员，IEEE Senior member, 中国计算机学会大数据专家委员会委员，中国自动化学会联邦数据和联邦智能专业委员会副主任。主要研究方向为具身智能、大模型、联邦学习和深度学习等。荣获中国专利优秀奖、广东省科技进步二等奖、吴文俊人工智科技进步一等奖、人民银行金融发展一等奖、深圳高层次专业人才领军人才、福田英才等奖项。联系邮箱：jzwang@188. com

收稿日期: XXXX–XX–XX
通信作者: 王健宗，jzwang@188.com
基金项目: 深港联合资助项目（A 类）（No. SGDX20240115103359001）
Foundation Items: Shenzhen–Hong Kong Joint Funding Project (Category A) under Grant No. SGDX20240115103359001