

特色专题

格基后量子密码算法安全分析进展

丁津泰^{1,2}, 赵子瑜³

摘要 后量子密码(post-quantum cryptography, PQC)作为抵御量子计算潜在威胁的关键技术,已成为新一代密码安全体系的基石。当前,全球信息产业已进入密码迁移的实质性落实阶段,多国标准化机构正在推进新一代标准遴选与制度建设。格基密码算法凭借其优异的计算效率、较小的密钥尺寸成为通用场景下的主流选择。安全分析作为密码算法设计与评估的核心环节,对于确保 PQC 的可靠性至关重要。聚焦于格基密码算法的安全分析,回顾了格密码攻击技术的发展脉络及其理论背景,针对目前最优的格攻击算法——筛法在密码学规模下频繁凸显的访存瓶颈进行深入研究。通过算法优化与高效实现,展示了一系列刷新公开记录的攻击成果。实践证明,先前在格密码安全评估中将访存效能视作关键的观点存在显著偏差。基于此,对包括银行业等关键基础设施在 PQC 迁移与部署过程中的密码参数选择提出建议。

关键词 后量子密码;格密码;信息安全

公钥密码是数字社会建立身份认证、密钥协商、数字签名与可信互联能力的基础支撑,也是政务系统、金融交易、云服务、工业互联网等关键信息基础设施得以安全运行的核心技术环节。目前广泛用于加密和数字签名的传统公钥密码算法,其安全性普遍建立在大整数分解问题与离散对数问题的计算困难性之上,典型代表包括 RSA(Rivest-Shamir-Adleman)加密和椭圆曲线数字签名算法(elliptic curve digital signature algorithm, ECDSA)等。1994 年, Peter Shor 提出著名的 Shor 算法^[1],证明量子计算机能够在多项式时间内完成整数分解。该算法可进一步推广到对离散对数问题的高效求解,从而从根本上动摇了传统公钥密码安全性所依赖的困难性假设。这意味着,一

旦能够稳定运行、具备足够规模与纠错能力、具有密码学意义的实用量子计算机(cryptographically relevant quantum computer, CRQC)真正出现,大量建立在传统公钥密码之上的安全机制都将面临系统性失效风险。

为应对量子计算带来的挑战,密码学研究者试图寻找在量子计算模型下仍被认为难以求解的数学问题,并据此构造新的公钥加密与数字签名方案,这类方案通常统称为后量子密码(post-quantum cryptography, PQC)。在众多候选路线中,包含最短向量问题(shortest vector problem, SVP)和容错学习问题(learning with errors, LWE)在内的格问题,为构造抗量子攻击的密码设计提供了最重要的理论基础之一。人们相信这类问题即使在量子计算机上依旧难以高效求解,而且基于格的 PQC 算法在运算效率、密钥与签名尺寸等方面都较为平衡,因而逐步成为通用场景下的主流方案。例如,美国国家标准与技术研究院(National Institute of Standards and Technology,

1. 西交利物浦大学后量子迁移交叉实验室(PQC-X), 苏州 215123
2. 江苏省金融学会抗量子计算迁移专业委员会, 苏州 215123
3. 清华大学数学科学系, 北京 100084

收稿日期: 2026-05-13; 修回日期: 2026-08-20

作者简介: 丁津泰, 教授, 研究方向为抗量子计算密码学, 电子信箱: jintai.Ding@xjtlu.edu.cn

引用格式: 丁津泰, 赵子瑜. 格基后量子密码算法安全分析进展[J]. 科技导报, 2026, 44(16): 57-63; doi:10.3981/j.issn.1000-7857.2026.05.00053

NIST)已将基于格的 ML-KEM^[2]和 ML-DSA^[3]分别确立为密钥封装和数字签名的核心标准。

安全是 PQC 迁移和部署的核心问题。虽然由于量子计算的迫在眉睫的威胁,这些格类算法已经或即将被部署,但对它们的安全分析仍然是一个活跃的研究领域。本文将介绍在格基密码安全分析方面的最新研究进展。

1 PQC 标准化与格基算法

在当前量子计算技术持续进步的背景下,PQC 标准化与部署已经成为全球信息安全领域的紧迫任务,而非可以无限期后延的长期规划。值得注意的是,量子威胁并不只在大规模容错量子计算机真正出现的那一刻才开始发挥作用。考虑到“先存储、后解密”的现实攻击模式,攻击者完全可能在今天先收集和保存高价值密文,待未来量子能力成熟后再集中解密,因此部分

需要长期安全的数据可能已经暴露在量子威胁之下。

NIST 在其迁移路线初步公开草案 NIST IR 8547^[4]中进一步给出了具有明确时间约束的政策信号:112 比特(bit)安全级别的 RSA 和 ECDSA 应在 2030 年前进入弃用阶段(deprecated),所有易受量子攻击的密码算法应在 2035 年之前被移除(disallowed)。与此同时,产业界也开始提出更激进的内部迁移节点,例如,Google 公司近期已将 2029 年定为其 PQC 迁移的截止日期。在中国,围绕 PQC 算法和应用规范的标准化和征集工作也正在同步推进。

迄今为止,在全球范围内影响最大、参与最广的 PQC 算法标准化工作,仍然是由美国 NIST 主导的 PQC 标准化进程^[5]。该项目于 2016 年正式启动,面向全球公开征集能够替代传统公钥密码的候选方案。在最初收到的 82 个完整提案基础上,经过第 3 轮筛选及第 4 轮补充评估,历经近 10 年,最终选定了 5 个候选算法进入标准制定阶段,详细信息见表 1。

表 1 NIST PQC 标准化入选算法

算法	底层安全问题	算法描述
ML-KEM	模格	通用场景下推荐
ML-DSA	模格	通用场景下推荐
SLH-DSA	哈希函数	签名长,最少的安全假设
FN-DSA	NTRU 格	实现困难,签名明显短于 ML-DSA
HQC	循环码解码	尺寸稍大于 ML-KEM,作为备份

基于格的算法在 NIST PQC 标准化项目中占据了主导地位,目前选中的 5 个算法有 3 个是基于格的,综合性能显著优于其他候选算法。然而,标准的建立不代表相关密码算法的安全性被研究透彻。相反,NIST 标准化进程本身已经多次展示出 PQC 候选方案在进入大规模部署之前仍可能遭遇突发性安全风险。在第 3 轮评审阶段,基于有限域多变量方程的数字签名候选 Rainbow^[6]和 GeMSS^[7]都突然受到新型攻击^[8-9],安全性被显著削弱。甚至在第 4 轮,原本被寄予多样化希望的基于超奇异椭圆曲线同源的 SIKE^[10]方案被彻底攻破^[11]。此类事件往往具有高度的不可预测性。如果类似级别的攻击发生在已经完成大规模部署的算法上,将直接导致全球数字基础设施、认证体系和长期保密数据面临集中失效的系统性事件。

NIST 在密钥封装方向继续保留并最终推进了基

于编码的 HQC^[12],以避免所有核心标准都集中在同一类数学假设之上。对于数字签名,基于哈希构造的 SLH-DSA^[13]在安全上更为保守,仅依赖于对称密码学的假设。但该方案签名长度较长,签名时间可达百毫秒级,难以在所有应用中直接替代格基签名方案。因此 NIST 于 2022 年额外启动了补充数字签名征集^[14],希望寻找非格路线的候选方案,目前该进程已经进入第 2 轮评审阶段。NIST 在密码底层安全问题的多样性上做出了一定努力,但新算法在安全分析的成熟度上也很难与被研究数十年的格类算法媲美。

因此,在当前时间节点,对即将成为主流部署对象的格类密码算法开展及时而关键的安全分析,既是理解其真实安全边界的必要工作,也是为参数选取、风险预判与性能安全权衡提供依据的前提。被 NIST 优先推进的基于格的方案在底层困难问题上具有较

强的相似性,主要建立在容错学习问题的结构化变体之上。这意味着,虽然这些方案在用途、实现方式和具体参数上存在差异,但它们在安全分析上往往共享类似的攻击面,目前这3种格密码算法的安全评估都直接依赖格上SVP的求解复杂性估计。

为系统评估各类SVP求解算法在密码学规模下的实际效能,德国达姆施塔特工业大学(TU Darmstadt)建立并持续维护了公开的SVP挑战赛^[15]。该挑战通过生成一系列维度不断提升的随机格实例,真实模拟攻击场景下的最短向量求解任务。相关实测数据已成为学术界和工业界制定PQC安全边界的重要参考依据。尽管NIST标准化的格基密码算法从未出现突发性的大幅安全削弱,但一个事实是,目前被实际求解的SVP实例的难度约为10年前记录的百万倍。

2 格基密码安全性分析

对最短向量问题及其近似版本的算法研究,可以追溯到20世纪80年代提出的LLL(Lenstra-Lenstra-Lovász)算法^[16]与随后发展的BKZ(Block Korkin-Zolotarev)算法^[17]。LLL能够在多项式时间内将输入的格基转化为一个质量尚可的约化基,因此直到今天仍是几乎所有格攻击流程中不可缺少的预处理步骤。BKZ则将格约化组织为一系列局部块上的SVP子问题求解,通过调节块大小在运行时间与输出质量之间提供平滑而可控的折中。现代格密码安全估计中常用的根Hermite因子、块大小以及局部投影格等概念,基本都建立在这一路线之上。从这个意义上说,虽然近年来最受关注的是更快的SVP子问题求解算法,但LLL与BKZ依然构成了当代格密码分析的基础骨架。

在相当长一段时期内,实践中求解SVP的主导方法是枚举。其核心思想是在Gram-Schmidt正交基下按系数逐层回溯搜索,并借助剪枝规则尽可能提前截断不可能通向最优解的分支。在原始的BKZ算法中,SVP子问题的求解就是通过枚举实现的。在2008年前后,Gama等^[18]在此基础上进一步提出了极限剪枝(extreme pruning)等方法,利用高斯启发式对搜索树进行更激进而精细的裁剪,使得枚举在保持多项式空间复杂度优势的同时,显著降低了实际运行时间。

枚举类算法的复杂度为 $2^{O(d \cdot \log(d))}$,其中 d 为被枚举的格的维度。此类枚举算法易于大规模并行,实现简单,直至2017年长期主导了公开的SVP求解记录。

另一类求解SVP的算法是筛法(sieving)。与枚举不同,筛法的基本思想不是在一棵搜索树上系统遍历候选,而是维护一个指数规模的短向量数据库,并不断寻找可以相互约化的向量对,使数据库整体逐步“收缩”到包含最短向量的状态。该思路可以追溯到更早的二维Gauss约化,并在21世纪初被推广为适用于高维SVP的通用算法框架^[19]。筛法在渐近时间复杂度上明显优于枚举,属于单指数时间算法,因此在理论上一直极具吸引力;但它必须保存和访问指数规模的中间向量集合,空间复杂度同样呈指数增长。由于实践中筛法的复杂度曾具有较大的常数因子,它在很长时间内仍被认为在真实密码学攻击中未必比经过高度优化的枚举更快。

这一判断在近10年中逐渐被改写。欧洲Léo Ducas和Martin Albrecht的研究团队围绕筛法提出了一系列相互叠加的改进,包括更高效的近邻搜索策略、渐进式筛法、免费维数(dimensions for free)等^[20-21],推动筛法从“渐近最优但工程上受限”的方法,转变为公开记录中的主导路线。2018年前后,基于通用筛法框架的工作首次将公开SVP记录推进到155维,标志着筛法在实践上超过了枚举。此后,该团队进一步利用基于图形处理器(graphics processing unit, GPU)的异构并行硬件和更系统的工程调优,将公开记录持续提升,最终在2021年达到了180维^[22]。此后,其他研究团队又于2024年将公开记录进一步推进至190维。当前主流的安全评估框架(如NIST PQC标准化所采用的Core-SVP模型)在理论上已经以筛法的渐近复杂度作为估计基准,而非枚举算法;然而,这类估计通常将筛法复杂度中的指数系数与单位运算成本视为一个固定的常数,未能充分反映筛法在工程实现上的持续进步。安全评估不仅需要依据筛法的理论复杂度,还必须考虑其在真实攻击中不断演进的实际能力。

3 筛法的最新进展

尽管筛法已经成为公开记录中的主导路线,但直

到最近,人们对其在密码学规模下的真实攻击能力仍然存在一个重要争议:最优的筛法虽然在逻辑运算上很快,却需要在一个指数规模的向量数据库上执行大量不可预测的访存操作。在采用局部敏感过滤(locality-sensitive filter)策略的筛法框架中,算法首先将大量短向量按过滤条件分配到许多桶中,使得桶内的向量互相距离更近,出现可约化向量对的概率更高,再在桶内进行搜索。此前最优的分桶策略可以把理论时间复杂度降到非常理想的水平,但代价是每个向量都可能被写入指数多个位置之一,产生海量随机访存。

对于密码学攻击涉及的问题规模,这些随机访问的代价常常远高于一次内积或一次向量更新,并且会随着问题规模的增大而增长。因此,一段时间内,学界和工业界普遍认为,筛法在理论上的速度优势会被访存瓶颈大幅拖慢,进而在具体安全估计中额外“补”上相当可观的安全余量。例如,对于 ML-KEM-512 参数,长期存在一种观点:虽然按门电路或理想化运算模型计算,它们已接近 NIST Level 1 的比特安全门槛,但真实攻击会因随机访存、主机与加速器带宽以及大容量内存成本而再增加 20~40 bit 的实际难度。如果这一判断成立,那么部分看似偏紧的参数在工程上仍可能拥有较大安全缓冲。在实际 SVP 问题的求解中,内存的大小和带宽确实一度成为限制更大规模筛法计算的主要因素,计算资源并不总是能够被充分利用。

为解决访存瓶颈问题,采用连续分桶(successive bucketing)的筛法路线,该技术原型最早由 Becker-Gama-Joux 提出^[23]。其核心思想不是一次性把整个数据库散写到大量桶中,而是对同一批向量连续施加多层过滤:先根据第 1 层过滤生成较大的一级桶,再在每个一级桶内部继续施加第 2 层过滤,得到更小的二级桶,必要时再进入第 3 级。这样做的关键收益在于,桶的规模会随着过滤层数增加而迅速缩小,常常呈现出数量级上的下降,因此不同层级的中间数据可以自然映射到不同速度、不同容量的存储介质之上。

与一次分桶相比,连续分桶虽然在纯理论运算数上并非绝对最优,但它显著减少了大规模随机写入,主存中的主要访问模式从“把向量打散到全局随机位置”转变为“按桶顺序流式扫描并局部处理”。从算法

机制上看,连续分桶并没有放弃高维近邻搜索的基本收益,而是把原本难以承受的全局随机访存,重构为层次化、局部化的筛选过程。在前期进行的一个仅基于 CPU 和系统内存的实现中,已经能观测到明显的获益,在一次 140 维筛法的运行过程中,部分性能数据如表 2 所示。可以看出,几乎所有的计算都在缓存内被完成,而少量需要访问主存的分桶步骤没有对总运行时间造成明显影响。

表 2 Becker-Gama-Joux 筛法 CPU 实现的部分性能数据

步骤	计算吞吐/ TOPS	平均桶大小/ GB	数据位置	运行时间/s
Filter-0	11.81	278.8	RAM	544.7
Filter-1	11.10	3.386	RAM	451.4
Filter-2	39.19	80.75×10^{-3}	L3缓存	762.4
搜索	116.4	556.7×10^{-6}	L2缓存	3397

注:读写存储器(random access memory, RAM)。

基于此基本思想,在工程实现层面,进一步把这一算法结构与异构存储体系相结合,构造出一个面向大规模筛法的高性能分层实现框架。具体而言,最大的主数据库不再强行驻留在系统 RAM 中,而是放置在外部固态硬盘(solid state drive, SSD)或磁盘阵列上;当前正在处理的一级桶放在系统 RAM 中;更小的二级和三级桶则下沉到 GPU 显存中完成密集计算。这样一来,容量最大的慢速存储负责保存全局状态,带宽较高的 RAM 负责承接中等粒度的数据搬运,而最昂贵但最快的显存只处理已经被过滤到足够小的热点数据。

要让这一架构真正奏效,关键不只是“把数据分层存放”,而是把整个程序组织成大块顺序 I/O、批量传输、流水化调度和充分重用缓存的形式,尽可能隐藏外存延迟,避免将小粒度随机访问暴露给 SSD。我们的实现经验表明,只要分桶结构设计得当,外存 I/O 并不会成为主瓶颈;真正决定速度的,重新回到了内积计算等算术密集步骤上。与此同时,现代 GPU 基于 Tensor Core 的低精度计算路径在筛法中同样有效,筛法并非数值精度敏感型任务。

基于上述算法与实现^[24],得到了一系列具有直接安全含义的实验结果。首先,基于连续分桶的筛法在实际攻击中显著优于原有的筛法实现,在安全评估时

应将其纳入考虑。其次,在公开 SVP 挑战上,新的实现已经把记录从原先的 190 维继续推高,进一步求解了 200 维及 210 维的实例,其中 210 维实例使用了数十 TB 的外部存储,运行时间约为 78 d。不但打破了内存大小带来的瓶颈,也获得了 1~2 个数量级的可观加速。与 10 余年前 SVP 挑战创立之初的约 130 维记录相比,这一实例对应的计算难度提升已达到数千万到上亿量级——目前理论上最优的 SVP 算法的求解复杂度为 $2^{0.292d+o(d)}$ 。一个明确的事实是,实践中格攻击算法的能力至今仍在稳步提高,其幅度即使对于密码分析来说也不可忽略。如果格攻击算法的能力继续以过去 15 年的速度提升,在 20~30 年后目前被 NIST 标准化的如 ML-KEM-512 参数将会面临被实际破解的风险。除此之外,该实现也在更贴近实际密码算法攻击的问题上被证明有效,比如,可以在数周内破解密钥大小减半的“ML-KEM-256”实例,超出基于之前所有的公开实现的预期。

综合这些大规模实验结果,把访存瓶颈视作格密码安全估计中的稳定附加保护层,并不可靠。随着算法结构、存储层次利用方式和实现细节持续改进,这部分所谓的“安全余量”正在被不断压缩。访存瓶颈几乎不能给基于格的 PQC 带来更多的安全性。

4 结论

本文对筛法最新进展的分析和一系列公开记录表明,过去被广泛认为会显著抬高攻击成本的访存瓶颈,并不是一个稳定、可靠且可以长期依赖的安全来源。随着密码分析技术的不断进步,目前格密码标准化参数中预留的工程性安全余量正在持续被压缩,而且这一趋势至今没有停滞。对于如银行业等关键基础设施而言,这一点尤其重要。

在后量子威胁日益逼近的大环境下,银行业关键基础设施正面临紧迫的迁移压力。银行信息系统部分涉及高价值资产与敏感数据,其中相当一部分——如期限长达数十年的贷款与抵押合同数据、核心密钥材料与长有效期数字证书、客户身份与征信数据等——极易受到“先存储、后解密”攻击模式的影响。因此,迁移工作具有明确的时间紧迫性。比如美国白宫于 2026 年 6 月发布的第 14412 号行政令^[25],要求联邦所

有高价值资产(high value asset, HVA)与高影响系统在 2030 年 12 月 31 日前完成密钥建立的 PQC 迁移,并在 2031 年 12 月 31 日前完成数字签名的 PQC 迁移。

银行业众多核心业务场景对密码算法的性能同样有着严苛要求。以客户接入类场景为例,其业务特点是高并发与终端硬件受限并存:短时间内需要处理海量身份认证与转账请求,同时相当一部分接入终端计算与存储资源有限,属于典型的资源受限环境,密码运算必须在有限时间窗口内完成,任何延迟累积都会直接影响响应时延与系统吞吐。这些技术难点既源自抗量子密码算法自身的时空效率特征,也植根于金融业务场景高并发、终端环境多样与硬件资源受限并存的复杂性。在当前各类后量子候选路线中,格类密码算法的标准化程度与实现成熟度相对最高,在运算效率、密钥与签名尺寸等方面综合性能无明显短板,预计将在这一轮迁移中承担主要角色之一,其安全性的可靠程度直接关系到整个迁移的成败。

因此,在未来数年即将进行的 PQC 迁移和部署过程中,对于格类密码算法,更稳妥的策略是在满足业务性能要求的前提下,优先采用对标等级高于常规 128 bit 安全性的参数配置。这与银行业自身的特点密切相关:银行业的业务数据保密周期通常以数十年计,系统服役时间长、跨机构互联复杂、升级替换成本高,一旦完成部署便难以频繁更换参数,这意味着今天选定的安全等级,有必要能够抵御未来 20~30 年间攻击能力的持续增长。需要指出的是,目前 NIST 标准化中较低一档的参数(如 ML-KEM-512)在今天的比特安全性上大致对标 AES-128,本身已处于安全门槛的临界状态;而格攻击算法的能力至今仍是活跃的研究话题,本文展示的公开记录持续刷新,较 10 余年前对应的计算难度提升已达数千万到上亿量级。在这种攻击能力仍在稳步提高且未来不排除出现新的突破性分析方法的背景下,对于银行业这类不容有失的场景,并不推荐采用此类临界参数。具体而言,可采用对应 ML-KEM-768、ML-DSA-65 安全等级的方案,为长期安全留出更充足的裕量。这类更保守参数带来的性能代价通常只是有限的,不会造成数量级上的系统开销上升,却能够显著降低由于安全估计偏乐观而带来的部署风险。与此同时,PQC 标准化进程中 GeMSS、Rainbow、SIKE 等方案遭遇突发性攻

击的经验也说明,密码算法在进入大规模部署之前,其安全性未必已经被完全摸清。在这种背景下,预留更高参数等级的意义不仅在于应对已知攻击能力的持续增强,更在于当未来出现新的突破性分析方法时,系统仍有希望避免被迅速彻底攻破,从而为风险评估、标准修订、系统改造和业务切换争取必要的缓冲时间。

参考文献(References)

- [1] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society, 1994: 124–134.
- [2] National Institute of Standards and Technology. FIPS 203 Module–lattice–based key encapsulation mechanism standard[S]. Washington, DC: Department of Commerce, 2024.
- [3] National Institute of Standards and Technology. FIPS 204 Module–lattice–based digital signature standard[S]. Washington, DC: Department of Commerce, 2024.
- [4] Moody D, Perlner R, Regenscheid A, et al. Transition to post–quantum cryptography standards[R]. Gaithersburg, MD: National Institute of Standards and Technology, 2024.
- [5] Moody D. Post–quantum cryptography: NIST's plan for the future[C]//Proceedings of the 7th International Conference on Post–Quantum Cryptography. Cham: Springer, 2016.
- [6] Ding J, Schmidt D. Rainbow, a new multivariable polynomial signature scheme[C]//Proceedings of the Third International Conference on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer, 2005: 164–175.
- [7] Patarin J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms [C]//International Conference on the Theory and Application of Cryptographic Techniques. Berlin, Heidelberg: Springer, 1996: 33–48.
- [8] Beullens W. Breaking rainbow takes a weekend on a laptop [C]//42nd Annual International Cryptology Conference. Cham: Springer, 2022: 464–479.
- [9] Tao C, Petzoldt A, Ding J. Efficient key recovery for all HFE signature variants[C]//41st Annual International Cryptology Conference. Cham: Springer, 2021: 70–93.
- [10] Jao D, De Feo L. Towards quantum–resistant cryptosystems from supersingular elliptic curve isogenies[C]//Post–Quantum Cryptography. Berlin, Heidelberg: Springer, 2011: 19–34.
- [11] Castryck W, Decru T. An efficient key recovery attack on SIDH[C]//International Conference on the Theory and Application of Cryptographic Techniques. Cham: Springer, 2023: 423–447.
- [12] Gaborit P, Aguilar–Melchor C, Aragon N, et al. Hamming quasi–cyclic (HQC)[EB/OL]. (2025–08–22) [2026–04–22]. https://pqc-hqc.org/doc/hqc_specifications_2025_08_22.pdf.
- [13] National Institute of Standards and Technology. FIPS 205 Stateless hash–based digital signature standard[S]. Washington, DC: Department of Commerce, 2024.
- [14] 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]. Gaithersburg, MD: National Institute of Standards and Technology, 2024.
- [15] Schneider M, Gama N. Darmstadt SVP challenges[EB/OL]. [2026–04–22]. <https://www.latticechallenge.org/svp-challenge/>.
- [16] Lenstra A K, Lenstra H W, Lovász L M. Factoring polynomials with rational coefficients[J]. Mathematische Annalen, 1982, 261: 515–534.
- [17] Schnorr C P. A hierarchy of polynomial time lattice basis reduction algorithms[J]. Theoretical Computer Science, 1987, 53: 201–224.
- [18] Gama N, Nguyen P Q, Regev O. Lattice enumeration using extreme pruning[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer, 2010: 257–278.
- [19] Ajtai M, Kumar R, Sivakumar D. A sieve algorithm for the shortest lattice vector problem[C]//Symposium on the Theory of Computing. New York: Association for Computing Machinery, 2001: 601–610.
- [20] Ducas L. Shortest vector from lattice sieving: A few dimensions for free[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2018: 125–145.
- [21] Albrecht M R, Ducas L, Herold G, et al. The general sieve kernel and new records in lattice reduction[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2019: 717–746.
- [22] Ducas L, Stevens M, van Woerden W. Advanced lattice sieving on GPUs, with tensor cores[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2021: 249–279.
- [23] Becker A, Gama N, Joux A. Speeding–up lattice sieving without increasing the memory, using sub–quadratic nearest neighbor search[EB/OL]. (2015–05–31) [2026–04–22].

- <https://eprint.iacr.org/2015/522>.
- [24] Zhao Z, Ding J. Towards large-scale lattice attack: New lattice records by disk-based sieving[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2026: 154–182.
- [25] The White House. Securing the Nation against advanced cryptographic attacks: Executive Order 14412[EB/OL]. (2026–06–22) [2026–07–06]. <https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/>.

Cryptanalysis advances in lattice-based post-quantum cryptography

DING Jintai^{1,2}, ZHAO Ziyu³

1. Post-Quantum Migration Interdisciplinary Laboratory (PQC-X), Xi'an Jiaotong-Liverpool University, Suzhou 215123, China
2. Special Committee on Post-Quantum Cryptography Migration, Jiangsu Provincial Society for Finance and Banking, Suzhou 215123, China
3. Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

Abstract Post-quantum cryptography, as a key technology against possible threats from quantum computing, is now becoming the foundation of next-generation cryptographic systems. The global migration to PQC is underway, with many countries actively developing new standards. Among the various candidates, lattice-based cryptography algorithms are popular due to their efficiency and small key sizes. Security analysis is crucial for ensuring the reliability of PQC. This paper focuses on the security analysis of lattice-based cryptography. We first review the development of lattice attacks and their theoretical background. Then, we study the main memory bottleneck in the best current attack method, called sieving, especially when used at cryptographic scales. By improving both the algorithm and its implementation, we achieved some new record results. Our tests show that the previous view of memory efficiency as a critical factor in lattice cryptography security estimation is significantly flawed. Based on this, we provide recommendations for choosing parameters in PQC migration and deployment, especially for critical infrastructure like banking.

Keywords post-quantum cryptography; lattice-based cryptography; information security ●



(责任编辑 王志敏)