赛题二:RLWE 问题和 MLWE 问题的求解

摘要: 随着量子计算技术的快速发展, 传统公钥密码体制面临严峻安全威胁. 本文针对 NIST 后量子密码标准化中的核心问题, 深入研究环学习带错误 (RLWE) 和模学习带错误 (MLWE) 问题的求解方法与安全性分析. 首先, 基于分圆多项式理论精确计算了环 $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ 中主理想 $(a(X)) = R_q$ 的概率. 其次, 提出完整的 RLWE 问题求解框架: 通过旋转矩阵构造将 RLWE 转化为标准 LWE 问题, 利用 q-ary 格理论约化为最近向量问题 (CVP), 再通过 Kannan 嵌入技术转换为最短向量问题 (SVP). 实验成功恢复多种参数设置下的 RLWE 实例中的秘密多项式 $\mathbf{s}$ 与错误多项式 $\mathbf{e}$, 其中第 1-5 问求的解均满足题目模长要求. 本研究为评估基于格的后量子密码方案 (如 NIST 标准 ML-KEM 和 ML-DSA) 的实际安全强度提供了理论基础与实用工具.

关键词: 格密码; RLWE; 格基约化; 最短向量问题

引言

大规模量子计算机的潜在威胁对传统公钥密码学的安全性构成根本性挑战. 为应对此挑战, **后量子密码学** (Post-Quantum Cryptography, PQC) 应运而生, 其核心在于构建基于**量子计算下困难数学问题**的密码体制, 旨在替代当前广泛依赖的传统公钥密码学, 实现密钥封装, 数字签名等核心功能.

在此背景下, 美国国家标准与技术研究院（NIST）于 2016 年启动全球性后量子密码标准化进程. 经过多轮严格评估, NIST 于 2024 年 8 月正式发布首批后量子密码标准:

- **FIPS 203**(基于模格学习带错误问题的密钥封装机制 ML-KEM)
- **FIPS 204**(基于模格学习带错误问题的数字签名 ML-DSA)
- **FIPS 205**(无状态哈希数字签名 SLH-DSA)

其中,**FIPS 203**（Crystals-Kyber）与 **FIPS 204**（Crystals-Dilithium）均基于**模格学习带错误问题** (Module Learning With Errors, MLWE). 这些方案的理论安全性本质依赖于底层 MLWE 及其变种（如环学习带错误问题 RLWE）的计算困难性. 因此, 深入理解 LWE 问题家族的计算复杂度并优化其求解算法, 构成评估后量子密码方案安全性的理论基础.

相关工作

近年来关于攻击 LWE 以及其变体的相关研究大致如下:

格基约简与基础攻击框架. 格基约简算法构成了几乎所有 LWE 攻击的理论基础, 其核心是通过系统性地投影向量到线性子空间来缩小尺寸并寻找短向量. LLL 算法[1] 作为多项式时间算法, 能生成近似正交的短格基, 但其解的质量仅达到指数级近似. Block Korkine-Zolotarev (BKZ) 算法[2] 虽能获得更短向量, 却以指数时间复杂度为代价. 其改进版本如 BKZ2.0[3] 和渐进式 BKZ[4–6] 显著提升了效率. 值得注意的是, BKZ 的子程序需在低维子格中求解最短向量问题, 筛法[7,8] 因其能在短时间内生成指数级短向量而成为重要选项, 但其内存消耗同样呈指数增长. 最新提出的 Flatter 算法[9] 通过精细的精度管理技术, 在保持 LLL 级别解的质量的同时实现了更快的格基约简.

多样化攻击范式. 针对 Search-LWE 的攻击主要分为四类: uSVP 攻击[10]、机器学习攻击[11], Cool&Cruel 攻击[12] 以及针对 Decision-LWE 的对偶攻击[13,14]. uSVP 攻击通过构造特殊格结构, 将秘密向量恢复问题转化为寻找格中唯一最短向量问题[10]. 对偶攻击则通过寻找对偶格中的短向量来解决 Decision-LWE 问题[15], 其核心变种包括: 混合对偶攻击[16]: 将矩阵 $\mathbf{A}$ 分割为两部分, 分别进行格基约简和猜测计算, 特别适用于稀疏秘密. 中间相遇攻击 (MitM)[14]: 通过构建部分秘密猜测表来提升成功率, 但需指数级内存. 机器学习攻击以 SALSA 框架为代表[11,17–19], 通过训练 Transformer 模型从约简样本 $(\mathbf{A}, \mathbf{b})$ 中预测 $\mathbf{b}$ 并构建预言机, 最终在维度 $n \leq 1024$ 下成功恢复稀疏二元/三元秘密[11]. Cool&Cruel 攻击[12] 则利用格基约简后矩阵的" 悬崖现象"——前部列保持未约简状态 ("Cruel" 位), 后部列显著缩小 ("Cool" 位), 先通过暴力破解恢复 Cruel 位, 再用贪心算法高效恢复 Cool 位.

本研究主要工作

具体研究工作涵盖:

1. 计算环 R_q 中均匀随机元素 $a(X)$ 满足主理想 $(a(X)) = R_q$ 的概率;
2. 基于 **Primal Attack** 求解不同参数下的搜索 RLWE 问题, 成功恢复短模长的秘密向量 $\mathbf{s}$ 与错误向量 $\mathbf{e}$ (攻击流程见图 1, 图中 Search-RLWE 和 Search-LWE 分别简写为 S-RLWE 和 S-LWE).

图 1: 本研究规约流程图.

一、前置知识及符号说明

$\mathbb{Z}$ 和 $\mathbb{R}$ 分别表示整数环和实数域. 对于奇素数 q, 令 $\mathbb{Z}_q$ 表示模 q 的整数集, 如 $\mathbb{Z}_q = \mathbb{Z} \cap [-\frac{q}{2}, \frac{q}{2})$. 对于两个向量 $\mathbf{v} = (v_1, \ldots, v_d)$, $\mathbf{w} = (w_1, \ldots, w_d) \in \mathbb{R}^d$, 令 $\langle \mathbf{v}, \mathbf{w} \rangle$ 表示内积 $\sum_{i=1}^{d} = v_i w_i$. 我们用 $\|\mathbf{v}\|$ 表示定义为 $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$ 的欧氏范数, $\mathbf{A}^\top$ 表示矩阵 $\mathbf{A}$ 转置.

定义 1 (搜索 LWE 问题)**.** *固定一个秘密向量 $\mathbf{s} \in \mathbb{Z}_q^n$. LWE 分布 $A_{\mathbf{s},\chi}$ 生成样本对 $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, 其中向量 $\mathbf{a}$ 在 $\mathbb{Z}_q^n$ 上均匀随机选取, 且 $b = \langle \mathbf{a}, \mathbf{s} \rangle + e \mod q$, 噪声项 e 采样自分布 χ. 给定任意独立样本, 搜索 LWE 问题要求恢复秘密向量 $\mathbf{s}$.*

定义 2 (搜索环 LWE 问题)**.** *固定一个秘密元素 $s(X) \in R_q$. 环 LWE 分布 $A_{s,\chi}$ 生成样本对 $(a(X), t(X)) \in R_q \times R_q$, 其中多项式 $a(X)$ 在商环 R_q 上均匀随机选取, 且 $t(X) = s(X) \cdot a(X) + e(X)$, 噪声多项式 $e(X)$ 采样自分布 χ. 给定任意独立样本, 搜索环 LWE 问题要求恢复秘密 $s(X)$.*

旋转操作. 环 R（或 R_q) 中的任意元素均可表示为系数属于 $\mathbb{Z}$（或 $\mathbb{Z}_q$) 的 $n-1$ 次多项式. 对于元素 $f(x) = f_0 + f_1 X + \cdots + f_{n-1} X^{n-1} \in R$（或 R_q), 其系数向量记为 $\mathbf{f} = (f_0, f_1, \ldots, f_{n-1}) \in \mathbb{Z}^n$（或 $\mathbb{Z}_q^n$). 定义 $\mathbf{f}$ 的旋转操作为:

$$\mathrm{rot}(\mathbf{f}) = (-f_{n-1}, f_0, f_1, \ldots, f_{n-2}). \tag{1.1}$$

该向量即对应环 R 中元素 $xf(x)$ 的系数表示. 进一步, 对任意 $1 \le i \le n$,i 次旋转向量 $\mathrm{rot}^i(\mathbf{f})$ 对应元素 $x^i f(x)$ 的系数表示. 特别地, 由 R 中关系 $x^n = -1$ 可得 $\mathrm{rot}^n(\mathbf{f}) = -\mathbf{f}$.

格. 格是欧几里得空间 $\mathbb{R}^d$ 中的离散加法子群. 任意格 L 可由 $\mathbb{R}^d$ 中线性无关的行向量组 $\mathbf{b}_1, \ldots, \mathbf{b}_h$ 生成:

$$L = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_h) = \left\{ \sum_{i=1}^{h} z_i \mathbf{b}_i \mid z_i \in \mathbb{Z} \right\}. \tag{1.2}$$

向量组 $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_h)$ 称为 L 的格基, 生成格 L 的极大线性无关向量数称为格的维度

(或秩), 记为 $\dim(L)$. 当 $\dim(L) = d$ 时, 称 L 为 $\mathbb{R}^d$ 中的满秩格. 定义 $\lambda_1(L)$ 为格 L 的第一逐次极小值, 即 L 中最短非零向量的范数.

q 元格. 设 q 为奇素数, 若满秩格 $L \subset \mathbb{R}^d$ 满足包含关系 $q\mathbb{Z}^d \subseteq L \subseteq \mathbb{Z}^d$, 则称 L 为 q 元格. 基于 LWE 实例, 文献[20] 构造了若干 q 元格以规约至 SVP, CVP 等格难题. 对于给定 LWE 实例, 可构造如下 q 元格:

$$\Lambda_q(\widehat{\mathbf{A}}) = \left\{ \widehat{\mathbf{z}} \in \mathbb{Z}^d \mid \widehat{\mathbf{z}} \equiv \mathbf{s}\widehat{\mathbf{A}} \pmod{q},\ \exists \mathbf{s} \in \mathbb{Z}^n \right\}. \tag{1.3}$$

该 q 元格由 $(d+n) \times d$ 矩阵 $\begin{pmatrix} \widehat{\mathbf{A}} \\ q\mathbf{I}_d \end{pmatrix}$ 的行向量生成, 其中 $\mathbf{I}_d$ 为 d 维单位矩阵.

Lenstra-Lenstra-Lovász (LLL) 约化基. 对于参数 $\delta \in (\frac{1}{4}, 1)$, 格 $L \subset \mathbb{R}^m$ 的基 $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$ 称为 δ-LLL 约化基需满足: (i) **尺寸约减性**: 对任意 $i > j$ 满足 $|\mu_{ij}| \leq \frac{1}{2}$, 其中 $\mu_{ij} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle$ 为 Gram-Schmidt 系数; (ii) **Lovász 条件**: 对任意 $2 \leq k \leq d$ 满足 $\delta \|\mathbf{b}_{k-1}^*\|^2 \leq \|\mathbf{b}_k^* + \mu_{k,k-1}\mathbf{b}_{k-1}^*\|^2$, 其中 $\mathbf{b}_i^*$ 为 Gram-Schmidt 正交化向量. 该约化基满足重要上界: 设 $\alpha = (4\delta - 1)^{-1/2}$, 则

$$\|\mathbf{b}_1\| \leq \alpha^{d-1}\lambda_1(L) \quad \text{且} \quad \|\mathbf{b}_1\| \leq \alpha^{(d-1)/2}\mathrm{vol}(L)^{1/d}.$$

LLL 算法通过迭代执行尺寸约减和向量交换实现约化: 当违反 Lovász 条件时, 交换 $\mathbf{b}_k$ 与 $\mathbf{b}_{k-1}$ 并重新正交化. 其时间复杂度关于维度 d 为多项式级, 可有效消除基向量间的线性相关性, 为格密码学基础工具.

Block Korkine-Zolotarev (BKZ) 约化基. 对于格 $L \subset \mathbb{R}^m$ 的基 $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$, 定义正交投影算子 π_j 为向量在子空间 $(\mathbf{b}_1, \ldots, \mathbf{b}_{j-1})^\perp$ 上的投影.

令 $\mathbf{B}_{[j:k]} = (\pi_j(\mathbf{b}_j), \pi_j(\mathbf{b}_{j+1}), \ldots, \pi_j(\mathbf{b}_k))$ 生成子格 $L_{[j:k]} = \mathcal{L}(\mathbf{B}_{[j:k]})(j < k)$. 对块大小 $\beta \geq 2$, 若基 $\mathbf{B}$ 满足尺寸约减条件, 且对所有 $1 \leq j \leq d-1$ 有:

$$\|\mathbf{b}_j^*\| = \lambda_1(L_{[j:k]}), \quad k = \min(j + \beta - 1, d)$$

则称其为 β-BKZ 约化基. 特别地, 当 $\beta = n$ 时即为 Hermite-Korkine-Zolotarev (HKZ) 约化基.

BKZ 算法通过迭代处理投影子格构造约化基: 对每个块 $\mathbf{B}_{[j:k]}$ 先进行 LLL 约化, 再调用精确 SVP 算法（如枚举法）求解最短向量. β-BKZ 约化基满足长度上界 $\|\mathbf{b}_1\| \leq \gamma_\beta^{\frac{d-1}{2(\beta-1)}}\lambda_1(L)$, 其中 γ_β 为维度 β 的 Hermite 常数. 增大块尺寸 β 虽可降低 $\gamma_\beta^{1/(\beta-1)}$ 以获取更短向量, 但显著增加计算开销——其复杂度由子格 $L_{[j:k]}$ 上 SVP 算法的复杂度主导.

二、环 R_q 中主理想 $(a(X)) = R_q$ 的概率计算

1. 理论基础与计算方法

考虑分圆环 $R_q = \mathbb{Z}_q[X]/(X^n + 1)$, 其中 $n = 256$, $q = 3329$ 为质数. 需计算均匀随机选取元素 $a(X) \in R_q$ 满足主理想 $(a(X)) = R_q$ 的概率 p.

$(a(X)) = R_q$ 当且仅当 $a(X)$ 是 R_q 中的可逆元. 在商环结构 $\mathbb{Z}_q[X]/(f(X))$ 下,$a(X)$ 可逆的充要条件为:

$$\gcd(a(X), f(X)) = 1 \quad \text{于多项式环} \quad \mathbb{Z}_q[X]$$

其中 $f(X) = X^n + 1 = X^{256} + 1$.

由分圆多项式理论, $X^{512} - 1 = (X^{256} - 1)(X^{256} + 1) = \prod_{d|512} \Phi_d(X)$. 因 $512 = 2^9$ 且 $n \times 2 = 512$, 有:

$$f(X) = X^{256} + 1 = \Phi_{512}(X) \tag{2.1}$$

$\Phi_{512}(X)$ 的次数为欧拉函数值 $\phi(512) = 512 \times (1 - \frac{1}{2}) = 256$.

在有限域 $\mathbb{Z}_q$ 上 (q 为奇质数), $\gcd(q, 512) = 1$ 保证 $\Phi_{512}(X)$ 的不可约因子次数由 q 模 512 的乘法阶决定:

$$q \equiv 3329 \equiv 257 \pmod{512}$$
$$257^2 = 66049 \equiv 1 \pmod{512} \quad (\text{因} 512 \times 129 = 66048)$$

故乘法阶为 2, $\Phi_{512}(X)$ 在 $\mathbb{Z}_q[X]$ 中分解为 $\frac{\phi(512)}{\mathrm{ord}_q(512)} = \frac{256}{2} = 128$ 个互异首一不可约二次多项式:

$$X^{256} + 1 = \prod_{i=1}^{128} p_i(X), \quad \deg p_i = 2$$

由概率独立性,$a(X)$ 与所有 $p_i(X)$ 互素的概率为:

$$p = \left(1 - \frac{1}{q^2}\right)^{128} \tag{2.2}$$

2. 数值结果

代入参数 $q = 3329$, 得具体概率值:

$$p = \left(1 - \frac{1}{3329^2}\right)^{128} \tag{2.3}$$

三、RLWE 和 MLWE 问题的求解

1. RLWE 到 LWE 的规约

从 RLWE 分布 $\mathcal{A}_{\mathbf{s},\chi}$ 中获取采样 $(a(X), t(X))$ 后, 对于 $a(X)$ 的系数向量 $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$, 可构造对应的 $n \times n$ 矩阵:

$$\mathbf{A} = \begin{pmatrix} \mathbf{a} \\ \mathrm{rot}(\mathbf{a}) \\ \mathrm{rot}^2(\mathbf{a}) \\ \vdots \\ \mathrm{rot}^{n-1}(\mathbf{a}) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & \cdots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \cdots & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \cdots & a_0 \end{pmatrix} \tag{3.1}$$

此时成立同余关系 $\mathbf{t} \equiv \mathbf{sA} + \mathbf{e} \pmod{q}$, 其中 $\mathbf{t}$, $\mathbf{s}$, $\mathbf{e}$ 分别为多项式 $t(X)$, $s(X)$, $e(X)$ 的系数向量. 环 LWE 关系 $t(X) = s(X)a(X) + e(X)$ 可转化为矩阵形式:

$$\mathbf{t}\mathbf{X}^\top = t(X) = s(X)a(X) + e(X) \tag{3.2}$$

$$= \mathbf{s}\mathbf{X}^\top a(X) + \mathbf{e}\mathbf{X}^\top \tag{3.3}$$

$$= \mathbf{s} \begin{pmatrix} \mathbf{a} \\ \mathrm{rot}(\mathbf{a}) \\ \mathrm{rot}^2(\mathbf{a}) \\ \vdots \\ \mathrm{rot}^{n-1}(\mathbf{a}) \end{pmatrix} \mathbf{X}^\top + \mathbf{e}\mathbf{X}^\top \tag{3.4}$$

$$= (\mathbf{sA} + \mathbf{e})\mathbf{X}^\top \tag{3.5}$$

此处 $\mathbf{X} = (1, X, X^2, \ldots, X^{n-1})$ 构成环 R（或 R_q）作为 $\mathbb{Z}$-模（或 $\mathbb{Z}_q$-模）的基. 因此, 单个环 LWE 样本可生成大小为 $n \times n$ 的 LWE 实例 $(\mathbf{A}, \mathbf{t})$, 其秘密向量为 $\mathbf{s}$, 错误向量为 $\mathbf{e}$.

1.1 多样本扩展

考虑从 $\mathcal{A}_{\mathbf{s},\chi}$ 获取 $m \geq 1$ 个独立 RLWE 样本 $(a_1(X), t_1(X)), \ldots, (a_m(X), t_m(X))$. 令 $\mathbf{A}_i$ 表示按式 (2) 构造的, 对应 $a_i(X)$ 的 $n \times n$ 矩阵, 则由前述推导可得 m 个关系式:

$$\mathbf{t}_i \equiv \mathbf{s}\mathbf{A}_i + \mathbf{e}_i \pmod{q}, \quad 1 \leq i \leq m \tag{3.6}$$

将这些关系式拼接可得尺寸为 $n \times d$ 的 LWE 实例:

$$(\widehat{\mathbf{A}}, \widehat{\mathbf{t}}), \quad \widehat{\mathbf{t}} \equiv \mathbf{s}\widehat{\mathbf{A}} + \widehat{\mathbf{e}} \pmod{q} \tag{3.7}$$

其中 $d = mn$, 且满足:

$$\widehat{\mathbf{A}} = (\mathbf{A}_1 \mid \cdots \mid \mathbf{A}_m), \quad \widehat{\mathbf{t}} = (\mathbf{t}_1 \mid \cdots \mid \mathbf{t}_m), \quad \widehat{\mathbf{e}} = (\mathbf{e}_1 \mid \cdots \mid \mathbf{e}_m) \tag{3.8}$$

为保证秘密向量 $\mathbf{s}$ 的唯一可恢复性, 系统需满足超定条件 $m \geq 2$（即 $d > n$）.

2. LWE 到 CVP 的规约

我们可将 LWE 实例自然地视为 q 元格 $\Lambda_q(\widehat{\mathbf{A}})$ 上的最近向量问题 (CVP) 实例, 其中目标向量为 $\widehat{\mathbf{t}}$. 特别地, 当错误向量 $\widehat{\mathbf{e}}$ 足够短时 (在标准 LWE 设定中, 错误向量的范数远小于模数 q), 目标向量 $\widehat{\mathbf{t}}$ 与格点 $\mathbf{s}\widehat{\mathbf{A}} \in \Lambda_q(\widehat{\mathbf{A}})$ 的最小距离等于 $\|\widehat{\mathbf{e}}\|$. 从技术角度看, 这是**有界距离解码问题 (BDD)** 的实例——一种特殊的 CVP 问题, 其要求目标向量与格点的距离存在上界.

当条件化 RLWE 问题要求 $s(X)$ 为短多项式时, 可构造如下 $2n$ 阶整数矩阵:

$$\mathbf{A}^{\mathrm{ex}} = \begin{pmatrix} \mathbf{A} & -\mathbf{I}_n \\ q\mathbf{I}_n & \mathbf{0} \end{pmatrix} \in \mathbb{Z}^{2n \times 2n} \tag{3.9}$$

令 Λ 为 $\mathbf{A}^{\mathrm{ex}}$ 列向量张成的格, 定义目标行向量:

$$\mathbf{t}^{\mathrm{ex}} = \begin{pmatrix} \mathbf{t}^* & \mathbf{0} \end{pmatrix} \in \mathbb{Z}^{2n} \tag{3.10}$$

则存在整数向量 $\mathbf{s}^{\mathrm{ex}} = \begin{pmatrix} \mathbf{s}^* & \mathbf{r} \end{pmatrix} \in \mathbb{Z}^{2n}$, 使得格点 $\mathbf{s}^{\mathrm{ex}}\mathbf{A}^{\mathrm{ex}}$ 与目标向量 $\mathbf{t}^{\mathrm{ex}}$ 的差向量为:

$$\mathbf{t}^{\mathrm{ex}} - \mathbf{s}^{\mathrm{ex}}\mathbf{A}^{\mathrm{ex}} = \begin{pmatrix} \mathbf{t}^* & \mathbf{0} \end{pmatrix} - \begin{pmatrix} \mathbf{s}^* & \mathbf{r} \end{pmatrix} \begin{pmatrix} \mathbf{A} & -\mathbf{I}_n \\ q\mathbf{I}_n & \mathbf{0} \end{pmatrix} \tag{3.11}$$

$$= \begin{pmatrix} \mathbf{e}^* & \mathbf{s}^* \end{pmatrix} \in \mathbb{Z}^{2n} \tag{3.12}$$

其中 $\mathbf{e}^*$ 和 $\mathbf{s}^*$ 分别为目标错误向量和秘密向量.

3. CVP 到 SVP 的规约

Kannan 's embedding. 至此, 问题已转化为在格 $\mathcal{L}(\mathbf{A}^{\mathrm{ex}})$ 中寻找距离目标向量 $\mathbf{t}^{\mathrm{ex}}$ 最近的格点, 并恢复错误向量 $\mathbf{e}$. 为求解此 CVP 问题, 我们采用 *Kannan* 嵌入技术[21] 将其转化为最短向量问题 (SVP). 构造如下 $(2n+1) \times (2n+1)$ 维嵌入格矩阵:

$$\mathbf{A}^{\circledast} = \begin{pmatrix} \mathbf{A}^{\mathrm{ex}} & \mathbf{0} \\ \mathbf{t}^{\mathrm{ex}} & M \end{pmatrix} \in \mathbb{Z}^{(2n+1)\times(2n+1)} \tag{3.13}$$

其中 M 为标准嵌入常数 (通常取 $M = 1$). 对格 $\mathcal{L}(\mathbf{A}^{\circledast})$ 应用 LLL 或 KZ 格基约简算法, 可提取其最短向量. 该最短向量包含错误向量 $\mathbf{e}^*$ 和秘密向量 $\mathbf{s}^*$ 的关键信息. 上述过程完整实现了 RLWE 问题到 SVP 问题的规约与求解框架.

Kannan 嵌入的扩展方法. 通过引入旋转操作和扩展参数 k, 可在格中嵌入多个等长短向量, 显著提升 BKZ 算法的求解成功率[22]. 给定 LWE 实例 $(\hat{\mathbf{A}}, \hat{\mathbf{t}})$, 构造扩展矩阵:

$$\mathbf{A}^{\circledast} = \begin{pmatrix} \hat{\mathbf{A}} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \hat{\mathbf{t}} & \eta & 0 & \cdots & 0 \\ \mathrm{rot}(\hat{\mathbf{t}}) & 0 & \eta & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{rot}^{k-1}(\hat{\mathbf{t}}) & 0 & 0 & \cdots & \eta \end{pmatrix} \tag{3.14}$$

其中 $\hat{\mathbf{A}}$ 为 q-ary 格基, $\hat{\mathbf{t}}$ 为目标向量, η 为小常数, $\mathrm{rot}^i(\cdot)$ 表示向量循环移位. 该矩阵生成维度 $d + k$ 的新格 $\bar{\Lambda}_k$, 其包含 k 个等长短向量:

$$\left\{ (\hat{\mathbf{t}}, \eta, 0, \ldots, 0),\ (\mathrm{rot}(\hat{\mathbf{t}}), 0, \eta, \ldots, 0),\ \ldots,\ (\mathrm{rot}^{k-1}(\hat{\mathbf{t}}), 0, 0, \ldots, \eta) \right\}.$$

通过调整右下块结构, 可增大格体积而不增加错误向量长度, 从而优化求解过程.

实验表明 (参数: $n = 32, q = 577, d = 96, \sigma = 11.0, \beta = 65$), 扩展方法显著提升成功率: 当 $k = 1$（原始嵌入）且 $\eta = 1, \lceil\sigma\rceil, 2\lceil\sigma\rceil$ 时, 成功率分别为 $55\%, 69\%, 62\%$; 而 $k = 2, 3, 4, 5$ 时成功率最高可达 $75\%, 78\%, 76\%, 79\%$（较原始最大提升 23%）[22]. 需注意, 成功率随 k 增加呈波动性, 且受误差标准差 σ 和 BKZ 块大小 β 等因素影响, 但合理选择 k 可稳定获得显著增益.

4. SVP 问题的求解

格上最短向量问题 (SVP) 的计算困难性是评估格基密码协议安全性的核心基础, 其求解效率直接影响密码体制的实际安全性. 当前主流求解方法包括 BKZ 算法框架, 枚举算法及筛法, 其中枚举与筛法常作为关键子算法嵌入 BKZ 以提升整体效率. 枚举算法通过穷举以原点为中心, 半径为 R 的 n 维超球体内所有格点来求解 SVP, 实际执行过程可视为遍历枚举树结构. 剪枝技术作为其核心优化手段, 通过预设参数对子树进行剪枝, 显著缩小搜索空间, 但会引入有限失败概率. 该算法在低维场景表现优异, 常被用作 BKZ 子程序; 然而在高维情况下, 因其超指数时间复杂度 $\left(2^{\Theta(n \log n)}\right)$ 导致性能急剧下降, 成为算法优化的主要瓶颈.

筛法作为另一类重要求解技术, 自 2001 年 AKS 筛法[23] 提出后持续演进. 早期理论算法包括结构相异的 MV 筛法和列表筛法 (ListSieve)[24], 研究者随后发展出启发式版本如 NV 筛法[25] 和高斯筛法 (GaussSieve)[24]. 近十年来的优化突破主要体现在三个维度: (1) 算法结构创新: 包括基于 NV 筛法的层级筛法 (Level Sieve)[26,27], 基于列表筛法的元组筛法 (Tuple Sieve)[28], 以及线性筛法 (Linear Sieve)[29]; (2) 搜索加速技术: 运用局部敏感哈希[30], 局部敏感过滤[31] 及量子 Grover 搜索[32] 优化遍历过程; (3) 工程实践优化: 涵盖渐进筛法[33], 子筛法[34], 基于秩约简的 G6K 框架[7], 以及低存储需求的 k-筛法[35]. 特别值得关注的是, 启发式算法中具有最优渐进复杂度的 LDSieve[31] 代表了当前技术水平. 作为 BKZ 的高效子程序[6], 现代筛法通过上述多维优化显著提升了格基密码分析能力.

经过上述规约, 问题被转化为 $N = 2n + 1$ 维格上的最短向量问题 (SVP). 典型参数配置为 $n = 64, 96, 128, 256$, 对应的格维度分别为 $129, 193, 257, 513$ 维. 在 257 维和 513 维格上求解精确 SVP 具有显著计算难度——当前 `SVPChallenge` 记录显示, 已求解的最高维度仅为 200 维 (近似因子 1.05). 为此, 我们调用 `SGAE` 框架中的 LLL, BKZ 以及 G6K 算法进行 SVP 求解实验, 具体结果如表 1所示.

表 1: 解题结果

题目	n	N	$\|\|\mathbf{e}\|\|$	$\|\|\mathbf{s}\|\|$	SVP-Solver	是否满足条件
2.1	64	129	8.54	7.99	LLL	是
2.2	64	129	1.73	1.41	BKZ	是
2.3	96	197	9.38	9.27	BKZ	是
2.4	128	257	11.1	11.44	BKZ	是
2.5	128	257	13.74	2.82	BKZ	是
2.6	256	513	13.71*	4.00*	LLL	是
2.7	256	513	10.58*	4.00*	LLL	是
2.8	256	513	-	-	G6K	-

注:“-”表示受设备限制无法在短时间内求解, “*”表示时间限制下求取的近似解.

实验环境: CPU: i9-13900H@2.6 GHz, RAM: 32GB.

四、结论

本文深入研究了 RLWE 问题的求解方法, 旨在推进后量子密码学的安全性评估. 基于分圆多项式理论, 我们精确计算了环 $R_q = \mathbb{Z}_q[X]/(X^n+1)$ 中主理想 $(a(X)) = R_q$ 的生成概率, 在标准参数 $n = 256$, $q = 3329$ 下得到 $(1 - \frac{1}{q^2})^{128}$ 的理论结果, 这为理解 RLWE 问题的代数结构和评估相关密码方案安全性提供了理论基础.

我们构建了一个完整的 RLWE 求解框架: 首先通过旋转矩阵构造将 n 维 RLWE 问题转化为 $n \times n$ 维 LWE 问题; 接着利用 q-ary 格理论将 LWE 约化为格中的最近向量问题 (CVP); 最后通过 Kannan 嵌入技术将 CVP 转化为最短向量问题 (SVP). 这种系统化的约简方法为求解各类 LWE 变体提供了统一的理论基础. 在算法实现层面, 我们比较了多种格基约简技术: LLL 算法 (时间复杂度 $n^6(\log B)^3$)[1], BKZ 算法 (时间复杂度 $O(n^{c\cdot\beta}\cdot\mathrm{poly}(\log n))$)[2] 以及基于 G6K 求解器的 3-sieve 算法 (时间复杂度 $2^{0.396N+o(N)}$, 其中 $N = 2n+1$)[36]. 实验尝试求解了 (1)-(7) 题的 RLWE 实例, 成功恢复了秘密和错误多项式, 验证了方法的有效性.

本研究为评估基于格的后量子密码方案（特别是 NIST 标准化的 ML-KEM 和 ML-DSA）的实际安全强度提供了关键工具. 通过分析 RLWE 求解复杂度, 研究结果有助于: 评估现有参数安全边界, 指导未来参数设计, 并为密码学界提供实用分析方法. 总而言之, 我们在 RLWE 问题求解和后量子密码安全性评估方面取得了实质性进展, 所建立的理论框架, 求解方法和实验结果, 为领域研究者和工程实践提供了有价值的理论基础和

实用工具.

附录 I　解题结果

1. 题目 (2.1)

s = [1, -2, 0, 0, 1, 0, -1, 1, 1, -1, 1, 2, 1, 1, -1, -1, 0, 1, 0, -1, -1, 0, 0, 2, 1, -1, 0, -1, 0, 2, 0, 1, 1, -1, 0, 0, -1, 2, -1, -1, 0, -1, -1, 2, 1, -1, 1, -1, 2, 1, 1, 0, -1, 1, -1, 0, -2, 1, 0, 1, -2, 0, 0, 1]

s.norm=8.54400374531753

e = (-1, 1, 0, -1, 1, 0, -1, 0, -1, -1, 0, 1, -1, -1, -2, -2, -1, -1, 0, 0, -1, 1, 2, 2, -1, -1, 0, 0, -1, -1, 0, 1, -1, -1, -2, -1, 1, 0, -1, 0, 0, -1, 1, 0, 1, -2, 0, 1, 0, -1, -1, -1, 1, 1, -1, -1, 1, 1, 0, 1, 0, -1, 0, -1)

e.norm=7.999999999999999

2. 题目 (2.2)

s= [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

s.norm= 1.73205080756888

wt(s(x))=3

e= [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0]

e.norm= 1.41421356237310

3. 题目 (2.3）

s = [-1, 0, 0, 1, 0, 1, 0, 2, 0, 0, 0, 1, 1, -1, 1, 0, 1, -2, 0, -1, 0, 0, -1, 0, 1, 1, -2, 0, 0, -2, 1, 1, 1, -1, 1, -1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 2, 0, 1, 1, -1, -1, -1, 1, -1, 1, -1, 0, 0, 0, 0, -1, 0, 0, -1, -1, 0, 1, 0, -1, 0, 2, 1, -2, -2, -1, 0, 1, 0, 1, 0, 0, -1, 0, 0, 0, 0, 1, 0, 0, -1, -2, 0, -2, -2, 0]

s.norm = 9.38083151964686

e = [-1, 0, 1, 0, 0, 1, -1, -1, 0, 0, 0, -1, 1, 0, 0, -1, 1, 0, 0, -2, 0, -1, -1, 1, -2, 0, 0, -1, 0, 0, -1, 0, 2, -1, 1, -2, 0, 0, 1, -1, 1, 0, 0, 2, 0, 1, -1, 0, 1, -1, 1, 1, 1, -1, 0, -1, 0, 0, -1, -1, 0, -1, 0, -1, -1, 0, 0, -1, 0, 0, 0, -2, -2, 1, -1, -1, 0, -2, 0, 0, -2, 0, 0, -1, 2, 0, 0, 0, 0, 0, 1, 2, -1, 0, 1, 1]

e.norm = 9.27361849549571

4. 题目 (2.4)

s=[0, 0, 0, 0, -1, 1, 1, -1, -1, 0, 0, -1, -1, -1, -2, 1, -1, -1, 1, -1, 1, 0, 1, -1, -1, 0, 1, -1, -1, -2, 1, 0, 0, 0, 0, -1, 1, 0, -2, 0, -1, 0, 0, 1, 0, 2, -1, 1, 0, 0, 0, 2, -2, 2, -1, 0, 1, 0, 1, 2, 0, 0, -2, -1, 0, 0, -1, 0, -1, 0, 2, -2, 0, 0, -1, 0, -1, 2, -1, -1, -1, 1, 1, -1, 0, -1, 0, -1, -1, -1, 0, 1, -1, 0, 0, -1, 0, 2, -1, 0, 0, 0, -1, 0, -2, 1, 0, 0, 0, -2, 0, 1, 1, 1, 1, 0, 0, -1, -1, 0, -2, 0, -2, 0, 0, 0, 0, 0]

s.norm=11.1803398874989

e=[0, -2, 1, 1, 1, 0, 1, 0, 0, -1, -1, -1, 0, 0, 0, 1, 0, 0, 1, -2, 0, -2, 0, -1, 0, -1, -1, 0, 1, -1, 1, -1, -1, 2, -1, 0, 0, 1, 1, 2, 0, 2, -1, 0, 0, -1, 0, 2, 2, 1, 1, 0, -1, 1, -1, -1, -1, 0, -2, 0, -1, -1, 1, 1, 0, 0, 0, 1, 0, 2, 0, 2, 0, -1, -1, -1, 1, -1, -1, -1, -1, 0, -1, 1, 0, 1, 2, 0, -1, -2, 1, 0, 0, 0, 1, -1, 0, 0, 1, -1, 0, 0, 1, -1, 1, 0, 1, 0, 1, 1, 1, 0, 0, -1, 0, -1, -1, 1, 0, 0, 2, -2, -1, -1, 1, -2, -1, -1] e.norm=11.4455231422596

5. 题目 (2.5)

s=[1, -1, 0, 0, -1, 1, -1, -1, 1, 1, 2, -1, 0, -1, -1, 0, 0, -2, -1, 1, 0, 0, 2, 1, 2, 0, -2, 1, 0, -2, 0, -1, 1, 0, 1, 0, 0, 1, 0, 0, -1, 0, 0, 0, -1, -1, 1, -1, -2, 0, -2, 1, -1, -2, -1, -1, 1, -1, 1, 0, 1, 3, -1, 1, -1, 0, 0, 2, -1, 1, 2, 1, 2, 2, 2, -1, 1, -2, -1, 0, 0, 1, 0, 1, 1, 1, 1, 0, -1, 1, 0, 0, -1, -1, -2, 0, 1, -2, 1, 1, -1, 1, -1, 2, 2, 1, -2, 3, 0, 0, -2, 1, 1, 0, -2, 0, 0, 1, -2, -1, 1, -1, -1, -3, -2, 1, 0, -1]

s.norm=13.7477270848675

e=[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0]

e.norm=2.82842712474619

6. 题目 (2.6)*

s=[0, -1, -1, -1, -1, -1, 0, 0, -2, 0, 2, 0, 0, -1, -1, -1, 2, -2, 0, 0, 0, 0, 1, 1, 0, -1, -1, -2, 1, 1, 1, -1, 0, -1, 1, 1, 0, 0, 0, -2, 0, -1, 0, 0, 0, -2, -1, -2, 0, -2, 1, 2, 0, 0, 1, 1, 0, 0, 1, 2, 0, 1, 1, 1, 0, 1, 2, 0, -1, 0, 0, 0, 0, 0, 1, -2, -1, 0, 0, -1, -1, -1, 2, 1, -2, -1, -2, 0, 0, 0, -2, -1, 1, 0, 1, 0, 0, 2, 0, 1, -1, 1, -1, 0, 1, 0, -1, 0, 0, -2, 1, -2, 1, 1, 0, 0, -2, 0, 0, -2, 1, 1, -1, 1, 1, 2, -1, 0, -1, 2, 0, 0, 2, -1, -1, 0, -2, 1, 1, 1, -1, 1, 0, -1, 1, 0, 1, 0, 0, 1, -1, 1, 2, 0, 0, 1, 0, 0, 0, -1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0]

s.norm(): 13.7113092008021

e=[4, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

e.norm=4.00000000000000

7. 题目 (2.7)*

s=[2, 0, -1, 0, -2, 0, 0, 0, 0, 0, 1, -1, -1, -1, 1, 0, 0, 0, 0, 1, -1, 0, 0, 1, 0, 1, 0, 0, 0, 2, 1, -1, 0, 0, -1, -1, 0, 0, 0, 1, 0, 0, -1, 1, 1, 0, 0, 1, 0, 0, 0, 1, -1, -1, 0, 0, 0, 0, -1, -1, 0, 0, 1, -1, 0, -2, 0, 1, 0, 1, -1, 1, 0, -1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, -1, -1, -1, 2, 1, -1, 0, -1, 2, -1, 0, 2, 0, 0, -1, 0, 0, 0, 0, 0, -1, 1, 1, 0, -1, 0, 0, 0, 0, -1, 0, -1, 1, 0, 0, 1, -1, 0, 1, 0, -1, 0, -1, 1, -1, -1, 0, 1, 1, -1, 0, 0, -1, -1, 1, 2, 0, 0, 0, -1, 0, -2, 0, 1, -1, 1, -1, 0, 1, 1, 1, 0, -1, 0, -1, 0]

s.norm=10.5830052442584

e=[4, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

e.norm=4.00000000000000

注: “*” 为时间与设备限制下求取的近似解

附录 II

1. 代码

```
#sage
n =
q =
A = # a(x)的多项式各项系数
B = # t(x)的多项式各项系数

# 将A转换为矩阵形式
poly_mul_mat = Matrix(ZZ,n,n)
for i in range(n):
    for j in range(i+1):
        poly_mul_mat[j,i] = A[i-j]
    for j in range(n-i-1):
        poly_mul_mat[j+i+1,i] = A[-(j+1)]*(-1)

# 将RLWE问题规约为SVP问题
I = identity_matrix(n)
B_mat = Matrix(ZZ,B)
O = diagonal_matrix([0]*n)
O_vec = Matrix(ZZ,1,n)
O_vec_T = Matrix(ZZ,n,1)
L = block_matrix(ZZ,[[p*I,O,0],[poly_mul_mat,I,O_vec_T],[B_mat,O_vec,1]]) # kannan embedding

# 格基规约,LLL或BKZ
# L_LLL = LLL()
L_LLL = L.BKZ()
```

```
26
27 # 得到s(x)和e(x)的各项系数
28 s = res[n,2n]
29 e = res[0,n]
```

2. 各题解题参数

(1) LLL(default)

(2)(3) BKZ(block_size=20)

(4)(5) BKZ(algorithm='NTL',fp='qd',prune = 10,block_size=20)

(6)(7) LLL(algorithm='NTL:LLL',fp='qp',transformation = true)

注: 由于设备与时间限制, 未尝试使用更高的 blcok_size 进行求解, 若使用更高的 block_size, 可以显著提高格基规约质量.

参考文献

[1] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," 1982.

[2] C.-P. Schnorr, "A hierarchy of polynomial time lattice basis reduction algorithms," *Theoretical computer science*, vol. 53, no. 2-3, pp. 201–224, 1987.

[3] Y. Chen and P. Q. Nguyen, "Bkz 2.0: Better lattice security estimates," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 1–20, Springer, 2011.

[4] Y. Aono, Y. Wang, T. Hayashi, and T. Takagi, "Improved progressive bkz algorithms and their precise cost estimation by sharp simulator," in *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I 35*, pp. 789–819, Springer, 2016.

[5] L. Wang, W. Xia, G. Wang, B. Wang, and D. Gu, "Improved pump and jump bkz by sharp simulator," *Cryptology ePrint Archive*, 2022.

[6] W. Xia, L. Wang, D. G. GengWang, D. Gu, and B. Wang, "Improved progressive bkz with lattice sieving.," *IACR Cryptol. ePrint Arch.*, vol. 2022, p. 1343, 2022.

[7] M. R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. W. Postlethwaite, and M. Stevens, "The general sieve kernel and new records in lattice reduction," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 717–746, Springer, 2019.

[8] L. Ducas, M. Stevens, and W. van Woerden, "Advanced lattice sieving on gpus, with tensor cores," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 249–279, Springer, 2021.

[9] K. Ryan and N. Heninger, "Fast practical lattice reduction through iterated compression," in *Annual International Cryptology Conference*, pp. 3–36, Springer, 2023.

[10] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, *et al.*, "Homomorphic encryption standard," *Protecting privacy through homomorphic encryption*, pp. 31–62, 2021.

[11] S. Stevens, E. Wenger, C. Li, N. Nolte, E. Saxena, F. Charton, and K. Lauter, "Salsa fresca: angular embeddings and pre-training for ml attacks on learning with errors," *arXiv preprint arXiv:2402.01082*, 2024.

[12] N. Nolte, M. Malhou, E. Wenger, S. Stevens, C. Li, F. Charton, and K. Lauter, "The cool and the cruel: separating hard parts of lwe secrets," in *International Conference on Cryptology in Africa*, pp. 428–453, Springer, 2024.

[13] M. R. Albrecht, S. Bai, P.-A. Fouque, P. Kirchner, D. Stehlé, and W. Wen, "Faster enumeration-based lattice reduction: root hermite factor time," in *Annual International Cryptology Conference*, pp. 186–212, Springer, 2020.

[14] J. H. Cheon, M. Hhan, S. Hong, and Y. Son, "A hybrid of dual and meet-in-the-middle attack on sparse and ternary secret lwe," *IEEE Access*, vol. 7, pp. 89497–89506, 2019.

[15] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-quantum cryptography*, pp. 147–191, Springer, 2009.

[16] M. R. Albrecht, "On dual lattice attacks against small-secret lwe and parameter choices in helib and seal," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 103–129, Springer, 2017.

[17] E. Wenger, M. Chen, F. Charton, and K. E. Lauter, "Salsa: Attacking lattice cryptography with transformers," *Advances in Neural Information Processing Systems*, vol. 35, pp. 34981–34994, 2022.

[18] C. L. J. S. E. Wenger, Z. Allen-Zhu, F. Charton, and K. Lauter, "Salsa verde: a machine learning attack on learning with errors with sparse small secrets,"

[19] C. Y. Li, J. Sotáková, E. Wenger, M. Malhou, E. Garcelon, F. Charton, and K. Lauter, "Salsapicante: a machine learning attack on lwe with binary secrets," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2606–2620, 2023.

[20] D. Micciancio and O. Regev, "Lattice-based Cryptography," in *Post-Quantum Cryptography* (D. J. Bernstein, J. Buchmann, and E. Dahmen, eds.), pp. 147–191, Berlin, Heidelberg: Springer, 2009.

[21] R. Kannan, "Minkowski's convex body theorem and integer programming," *Mathematics of Operations Research*, vol. 12, no. 3, pp. 415–440, 1987.

[22] S. Nakamura and M. Yasuda, "An extension of kannan's embedding for solving ring-based lwe problems," in *Cryptography and Coding* (M. B. Paterson, ed.), (Cham), pp. 201–219, Springer International Publishing, 2021.

[23] M. Ajtai, R. Kumar, and D. Sivakumar, "A sieve algorithm for the shortest lattice vector problem," in *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, STOC '01, (New York, NY, USA), p. 601 - 610, Association for Computing Machinery, 2001.

[24] D. Micciancio and P. Voulgaris, *Faster exponential time algorithms for the shortest vector problem*, pp. 1468–1480.

[25] P. Q. Nguyen and T. Vidick, "Sieve algorithms for the shortest vector problem are practical," *Journal of Mathematical Cryptology*, vol. 2, no. 2, pp. 181–207, 2008.

[26] X. Wang, M. Liu, C. Tian, and J. Bi, "Improved nguyen-vidick heuristic sieve algorithm for shortest vector problem," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 1–9, 2011.

[27] F. Zhang, Y. Pan, and G. Hu, "A three-level sieve algorithm for the shortest vector problem," in *International Conference on Selected Areas in Cryptography*, pp. 29–47, Springer, 2013.

[28] S. Bai, T. Laarhoven, and D. Stehlé, "Tuple lattice sieving," *LMS Journal of Computation and Mathematics*, vol. 19, no. A, pp. 146–162, 2016.

[29] P. Mukhopadhyay, "Faster provable sieving algorithms for the shortest vector problem and the closest vector problem on lattices in p norm," *Algorithms*, vol. 14, no. 12, p. 362, 2021.

[30] T. Laarhoven, "Sieving for shortest vectors in lattices using angular locality-sensitive hashing," in *Advances in Cryptology–CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I 35*, pp. 3–22, Springer, 2015.

[31] A. Becker, L. Ducas, N. Gama, and T. Laarhoven, "New directions in nearest neighbor searching with applications to lattice sieving," in *Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms*, pp. 10–24, SIAM, 2016.

[32] T. Laarhoven, M. Mosca, and J. Van De Pol, "Solving the shortest vector problem in lattices faster using quantum search," in *Post-Quantum Cryptography: 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings 5*, pp. 83–101, Springer, 2013.

[33] T. Laarhoven and A. Mariano, "Progressive lattice sieving," in *International Conference on Post-Quantum Cryptography*, pp. 292–311, Springer, 2018.

[34] L. Ducas, "Shortest vector from lattice sieving: a few dimensions for free," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 125–145, Springer, 2018.

[35] A. Chailloux and J. Loyer, "Classical and quantum 3 and 4-sieves to solve svp with low memory," in *International Conference on Post-Quantum Cryptography*, pp. 225–255, Springer, 2023.

[36] M. R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. W. Postlethwaite, and M. Stevens, "The general sieve kernel and new records in lattice reduction." Cryptology ePrint Archive, Paper 2019/089, 2019. https://eprint.iacr.org/2019/089.