Pure Mathematics 理论数学, 2025, 15(6), 104-108
Published Online June 2025 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2025.156194

Hans汉斯

LWE问题的代数求解方式

范晨涛

成都理工大学数学科学学院，四川 成都

收稿日期：2025年5月23日；录用日期：2025年6月19日；发布日期：2025年6月27日

摘　要

本文研究了基于错误学习(LWE)问题的密码学构造，重点探讨了通过Kannan嵌入方法将其转化为代数问题的理论框架。我们系统分析了Kannan嵌入在LWE实例中的应用，证明了该转化过程的严谨性及其在密码分析中的有效性。具体而言，本文展示了如何将LWE的搜索问题嵌入到格结构中，并利用代数工具(如最短向量问题，SVP)求解，同时严格论证了转化后的代数形式与原问题的等价性。此外，我们讨论了该方法在参数选择、计算复杂度及安全性证明中的优势，为基于LWE的密码方案设计提供了理论支撑。实验结果进一步验证了该方法的可行性与效率。

关键词

LWE，Kannan嵌入

The Algebraic Way to Solve LWE

Chentao Fan

School of Mathematical Sciences, Chengdu University of Technology, Chengdu Sichuan

Received: May 23rd, 2025; accepted: Jun. 19th, 2025; published: Jun. 27th, 2025

Abstract

This paper studies cryptographic constructions based on the Learning With Errors (LWE) problem, with a focus on exploring the theoretical framework of transforming it into an algebraic problem through Kannan's embedding method. We systematically analyze the application of Kannan's embedding in LWE instances and prove the rigor of this transformation process and its effectiveness in cryptographic analysis. Specifically, this paper demonstrates how to embed the search problem of LWE into a lattice structure and solve it using algebraic tools (such as the Shortest Vector Problem, SVP), while strictly proving the equivalence between the transformed algebraic form and the original problem. Additionally, we discuss the advantages of this method in parameter selection, computational complexity, and security proof, providing theoretical support for the design of LWE-

文章引用: 范晨涛. LWE 问题的代数求解方式[J]. 理论数学, 2025, 15(6): 104-108.
DOI: 10.12677/pm.2025.156194

based cryptographic schemes. Experimental results further validate the feasibility and efficiency of this approach.

Keywords

LWE, Kannan's Embedding

1. 引言

LWE (Learning With Errors)问题由 Oded Regev 于 2005 年提出[1]，是一个基于格理论的数学难题。其核心思想是在线性方程组中引入随机误差，使得即使已知部分信息，恢复秘密值也变得极其困难。LWE 问题的困难性不仅在经典计算模型下成立，而且在量子计算模型下也被认为是难以解决的。这一特性使得基于 LWE 问题的密码学方案成为后量子密码学中的重要组成部分。基于 LWE 问题的重要性，已经开发出了多种解法。其中一种方法是将 LWE 问题重新表述为一个优化问题，其解向量由私钥和误差向量组成。假设这两个向量的元素具有较小的绝对值，因此这些问题被称为短向量问题(SVP)。与 LWE 问题不同，SVP 的解是在整数环上的向量，这使得解法的设计更为简单，因为无需模运，仅需使用标准整数运算即可。

但目前尚无有效算法能求解实际规模的 SVP。为了简化 SVP 的求解，常使用诸如 Lenstra-Lenstra-Lovász 基约简算法(LLL 算法) [2]或 Block Korkine-Zolotarev 算法(BKZ 算法) [3]。这些算法将 SVP 的解视为格中的元素，并将格基转换为几乎正交且由短向量组成的新基。借助这样的基，可以更便捷地计算或逼近 SVP 的解。在某些情况下，格基本身就可能包含 SVP 的解。故在本研究中，将针对不同规模的 LWE 问题去选择更合适的格基约化算法。

LWE 问题的研究具有深远的实际意义。首先，它为构建抗量子攻击的密码学原语提供了坚实的理论基础。基于 LWE 问题，可以设计出安全的公钥加密，数字签名，伪随机函数等多种密码学工具。这些工具不仅能够抵御量子计算攻击，还能在经典计算环境下保持高效性。其次，LWE 问题的困难性可以归约到格理论中的最坏情况假设，这意味着破解 LWE 问题等价于解决格理论中的某些困难问题(如最短向量问题，SVP)。这种归约为 LWE 问题的安全性提供了强有力的理论支持，使其成为密码学研究中备受信赖的难题[4]。

本文主要是通过数学角度来去证明如何将 LWE 问题重新表述为一个优化问题，其解向量由私钥和误差向量组成。并与短向量问题联系起来，通过代数学的角度来去简化问题。

2. 理论基础

2.1. 格理论以及格上的数学问题

格(Lattice)是一个在向量空间中由一组线性独立的基向量生成的离散集合。形式上，一个格 $L(b)$ 可以定义为：

$$L(B)=\left\{\sum_{i=1}^{n} c_i v_i : \forall i \in [n], c_i \in Z\right\}$$

其中 B 为 n 维空间中的一组基[5]。

格的最短向量问题(SVP)：给定一个格 $L(b)$，其由一组线性无关的向量 $B_1, B_2, \cdots, B_n$ 生成，目标是找到格中一个非零的最短向量 u，使得其欧几里德范数最小。我们称 u 为该格 $L(b)$ 中的最短向量，记作 $\lambda_1(L)$。

在实际问题当中，有时我们并不需要找出真正的最短向量而只需要找出一个“足够短”的向量即可。这样我们就得到了近似最短向量问题。

近似最短向量问题(aSVP)：给定一个 n 维的格 L 和一个目标向量 $v \in R^n$ 以及近似参数 $\gamma \geq 1$，目标是找到格中一个向量 $v \in R^n$，使得其满足 $\|u\| \leq \gamma\lambda_1(L)$。

2.2. LWE 问题

在 2005 年，Regev 提出了一种基于 LWE 的加密算法。与之前的基于格的密码系统相比，基于 LWE 的密码系统的密文大小和密钥大小大大减少。因此，LWE 开始被应用于许多密码原语，例如 Key-Dependent Message (KDM)，完全同态加密等等。

n 是正整数，q 为奇素数，X 是在上服从离散高斯分布的 Z_q 错误分布。s 是 Z_q^n 上的秘密向量，秘密向量服从均匀分布，$L_{s,x}$ 是 $Z_q^n * Z_q$ 上的可能分布，通过随机地在 Z_q^n 上选择 a 和 Z_q 上服从 X 分布的错误 e，最终得到 $Z_q^n * Z_q$ 上的：

$$(a, z) = (a, \langle a, s\rangle + e)$$

LWE 问题就是利用 $L_{s,x}$ 中给出的大量的例子也就是方程，找到秘密向量 s [6]。

3. 理论证明

现有 LWE 问题的分析方法可以分为组合方法、代数方法、格方法和穷举搜索。组合方法主要指的是高斯消元法的扩展应用，但它需要大量的样本。代数方法指的是 Arora-Ge 算法，其复杂度也与 LWE 维度的数量呈指数关系。主要有三种格方法：对偶方法用于通过解决对偶格上的短整数解问题来攻击决策——LWE 实例；解码方法用于直接解决原始格上的有界距离解码问题(BDD)；最主要也是最常用的方法是将有界距离解码(BDD)问题进一步简化为唯一最短向量问题。由于穷举搜索的时间复杂度较高，所以它不适合实际应用[7]。

本文主要是从代数角度给出求解 LWE 问题的一种可行方法并予以证明。

LWE 问题就是利用 $L_{s,x}$ 中给出的大量的例子也就是方程，找到秘密向量 s。如何去通过代数学的角度去处理 LWE 问题，可以采用 Kannan 嵌入法将 LWE 问题放入更高维的格中去考虑。

将 LWE 问题表述为矩阵形式

$$b = A \cdot s + e \in Z_q^m$$

其中矩阵 $A \in Z_q^{m \times n}$ 为随机公开矩阵，$s \in Z_q^n$ 是秘密向量，$\mathrm{e} \in Z^m$ 是小误差向量。

目标是从 (A, b) 中恢复 s 或 e。

构建如下形式的格基矩阵 B

$$B = \begin{pmatrix} I_m & A \\ 0 & qI_n \end{pmatrix} \in Z^{(m+n)\times(m+n)}$$

现在我们去证明在 $L(b)$ 中必定存在一向量 $v = (-e, s)$。并且由于 e 是小范数向量，此时 $v = (-e, s)$ 还是 $L(b)$ 中的短向量。

证 矩阵 $A \in Z_q^{m \times n}$ 为随机公开矩阵，通过嵌入法将其放到一个更高维度的矩阵 B 当中。此时我们通过观察，因为矩阵 B 是相当于矩阵 A 和单位矩阵扩充而成，所以矩阵 A 的秩不会影响到矩阵 B 是一个满秩矩阵。

此时矩阵 B 是一个满秩矩阵，由格的定义我们可知，可以将矩阵 B 可以视作一组基，其整系数线性组合构成了一个格 $L(B)$。

现在我们需证明在格 $L(B)$ 中必定存在一向量 $v=(-e,s)^{\mathrm{T}}$。

对于格中任一向量 ν，可以将其表示成

$$\begin{aligned}\nu &= \begin{pmatrix} I_m & A \\ 0 & qI_n \end{pmatrix}\begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} \\ &= \begin{pmatrix} Z_1 + AZ_2 \\ qZ_2 \end{pmatrix}\end{aligned}$$

其中 Z_1, Z_2 为任意整数。

若存在向量 $\begin{pmatrix} -e \\ s \end{pmatrix} = \begin{pmatrix} Z_1 + AZ_2 \\ qZ_2 \end{pmatrix}$，则需满足

$$Z_1 = -e - AZ_2,$$

$$Z_2 = \frac{s}{q},$$

由于 $\mathrm{s} \equiv qZ_2$，不妨设 $Z_2 = s - kq$，k 为整数。此时

$$\begin{aligned}Z_1 &= -e - AZ_2 \\ &= -e - A(s - qk) \\ &= -b + kqA.\end{aligned}$$

当取 $k=0$ 时，有

$$Z_1 = -e - As = -b,$$

$$Z_2 = s.$$

故我们可知，当 $Z_1 = -b, Z_2 = s$ 时，在格 $L(B)$ 中存在向量 v，满足 $v=(-e,s)$。由于 $\mathrm{e} \in Z^m$ 是小误差向量，且秘密向量 s 长度较小，故我们可知向量 v 是一个近似短向量。这样我们就将 LWE 问题转化为一个代数学问题，其解向量由私钥和误差向量组成。然后我们通过 LLL 算法与 BKZ 算法来进行其解向量的求解。

Kannan 嵌入是一种简单通用但效率受限的求解工具，其优势在于理论直观和算法复用性，可以将 LWE 问题转化成代数学问题，但在高维或高精度需求场景下表现不佳。实际应用中，常需与其他技术(如预处理基规约、参数调优)结合，以平衡效率和解的质量。

参考文献

[1] Regev, O. (2005) On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, Baltimore, 22-24 May 2005, 84-93. https://doi.org/10.1145/1060590.1060603

[2] Lenstra, A.K., Lenstra, H.W. and Lovász, L. (1982) Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, **261**, 515-534. https://doi.org/10.1007/bf01457454

[3] Schnorr, C.P. and Euchner, M. (1994) Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. *Mathematical Programming*, **66**, 181-199. https://doi.org/10.1007/bf01581144

[4] 王旭阳, 胡爱群. 格困难问题的复杂度分析[J]. 密码学报, 2015, 2(1): 1-16.

[5] 张平原, 蒋瀚, 蔡杰, 等. 格密码技术近期研究进展[J]. 计算机研究与发展, 2017, 54(10): 2121-2129.

[6] Budroni, A., Guo, Q., Johansson, T., Mårtensson, E. and Wagner, P.S. (2020) Making the BKW Algorithm Practical for LWE. In: Bhargavan, K., Oswald, E. and Prabhakaran, M., Eds., *Progress in Cryptology—INDOCRYPT* 2020, Springer International Publishing, 417-439. https://doi.org/10.1007/978-3-030-65277-7_19

[7] Lv, L., Yan, B., Wang, H., Ma, Z., Fei, Y., Meng, X., *et al*. (2022) Using Variational Quantum Algorithm to Solve the LWE Problem. *Entropy*, **24**, Article No. 1428. https://doi.org/10.3390/e24101428