第六届（2021）全国高校密码数学挑战赛
赛题三

一、赛题名称

错误学习问题（LWE）

二、赛题描述

2.1 符号说明

Z：整数集

Z_q：整数模 q 剩余类环

χ_α：整数上的离散高斯分布，中心点为 0，标准差为α

2.2 问题描述

给定(**A**, **b**=(**As**+**e**) mod q)，求解 **s**，其中 **A** 为Z_q上$m \times n$维均匀随机矩阵，**s** 为Z_q上均匀随机 n 维秘密向量，**e** 为χ_α上的 m 维噪声向量。

注：上述问题被称为“错误学习问题”，若将 s 看作未知数，则该问题可以看作一个带错误多维线性方程求解问题；若将 s 和 e 一起看作未知数，则该问题可以看作一个不定方程求解问题。

2.3 成绩评判标准

本赛题固定模数 q=256，固定噪声向量的标准差为$\alpha = 0.5$，问题的难度通过 s 的维数 n 来调整，具体评判标准如下：

n	分值
40	60
45	65
50	70
60	80
65	85
70	90

75	100
80	110
90	120

三、密码学背景及相关问题的研究进展

错误学习问题（Learning with Errors Problem）是设计格密码算法的基础数学困难问题之一，可用于设计公钥加密、数字签名、密钥交换、全同态加密、基于身份的加密等各类密码算法。在密码学领域，错误学习问题由 Regev 于 2005 年提出,其理论安全性可以由格上的基础困难问题 SIVP（Short Independent Vector Problem）问题保证。

求解 LWE 问题的主要方法包括穷搜索[1]、优化搜索 BKW 算法[2]、格基约化算法[3]等。穷搜索方法可以穷举所有秘密向量 s 的可能取值，验证（b-As）mod q 是否符合错误向量的分布来求解 s；BKW 算法通过对 s 进行分组，优化搜索任务的计算复杂性；最近平面算法将 As 看作一个超平面，寻找 b 在超平面上的投影来求解正确的 s；格基约化方法基于 b 和 A 构造一个格，并使得格上的短向量包含 s 和 e 的信息，从而将 LWE 问题转化为格基约化问题。

给定一组线性无关向量$\mathrm{B}=\{\mathrm{b}_1,\cdots \mathrm{b}_\mathrm{n}\}$，集合 $\mathrm{L}=\{\mathrm{v}=\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{a}_\mathrm{i}\mathrm{b}_\mathrm{i}:\mathrm{a}_\mathrm{i}\in \mathrm{Z}\}$称为格，B 称为格基。 给定一组格基 B，求解格上最短向量的问题称为最短向量问题（SVP）。给定一组格基 B，和空间中的向量 t，求解距其最近的格点的问题称为最近向量问题（CVP）。SVP 和 CVP 是格上最基础的计算困难问题，是格密码算法安全性的根本保证，即使在量子计算环境下，目前最好求解算法的计算复杂性也是指数级。

格基约化算法在密码算法分析中具有广泛的应用，例如 Knapsack 和 RSA 密码算法的安全性分析。给定一组格基 B，格基约化算法通过向量之间的约减输出长度更短的格基。若能将待求解的问题转化为求解格上的短向量问题，则可以通过格基约化算法进行求解。目前，格基约化算法主要包括 LLL 算法和基于其改进的 BKZ 算法。

错误学习问题定义了一类特殊的格，称为 q 元格（q-ary lattice）。给定$A \in Z_q^{m\times n}$, 由向量$z \equiv As \bmod q$构成的格称为 A 定义的 q 元格，由满足$rA \bmod q \equiv 0$的向量 r 构成的格称为 A 定义的 q 元垂直格。错误学习问题可以看作 A 定义的 q 元格上的噪音向量有界的最近向量问题。

目前，求解 LWE 问题计算性能最好的算法是格基约化算法，具体地，给定 LWE 问题(A, b)可以构造一个 q 元垂直格：

$$[\mathbf{A} \mid \mathbf{I}_m \mid \mathbf{b}]\mathbf{z} = 0 \bmod q,$$

并将格基输入 BKZ 算法计算最短向量。可以验证，$[\mathbf{s},\mathbf{e},\text{-}1]$是上述格的向量，若其长度足够短，则可以使用 BKZ 算法求解该向量，从而得到 s。

四、参考文献

1. Martin R. Albrecht, Rachel Player, Sam Scott: On the concrete hardness of Learning with Errors. J. Math. Cryptol. 9(3): 169-203 (2015).
2. Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, Ludovic Perret: On the complexity of the BKW algorithm on LWE. Des. Codes Cryptogr. 74(2): 325-354 (2015).
3. Martin R. Albrecht, Florian Göpfert, Fernando Virdia, Thomas Wunderer: Revisiting the Expected Cost of Solving uSVP and Applications to LWE. ASIACRYPT (1) 2017: 297-322.