赛题二

作者 1 作者 2 作者 3 …老师 1（指导老师）

暨南大学　邮箱

摘要：在此处输入摘要内容，约 300 500 字。应说明工作的目的、研究方法、结果和最终结论。要突出本论文的创造性成果或新的见解，语言力求精炼。为便于文献检索，应在本页下方另起一行注明本文的关键词（3 5 个）。

关键词：关键词 1；关键词 2；关键词 3；关键词 4；关键词 5

引言

在论文正文前，应简要阐述对赛题的分析、解题使用的主要方法和解题结果等内容。解题思路为将通过构造格将 RLWE 转化为 CVP 问题，再通过 Kannan embedding 将问题转化为 SVP 问题后使用 Seiving 求解。

一、求解环 R 中主理想 $a(x) = R_q$ 的概率

1. 计算方法

给定环 $R_q = \mathbb{Z}_q[X]/(X^n + 1)$，其中 $n = 256$，$q = 3329$（q 为质数）。需要计算在 R_q 中均匀随机选取元素 $a(X)$ 时，主理想 $(a(X))$ 等于整个环 R_q 的概率 p。

主理想 $(a(X)) = R_q$ 当且仅当 $a(X)$ 是 R_q 中的单位，即 $a(X)$ 在环中可逆。

$R_q = \mathbb{Z}_q[X]/(X^n + 1)$，其中 $\mathbb{Z}_q$ 是有限域（因为 q 是质数）。

元素 $a(X)$ 在 R_q 中可逆当且仅当在多项式环 $\mathbb{Z}_q[X]$ 中，$\gcd(a(X), X^n + 1) = 1$。这是因为在商环 $\mathbb{Z}_q[X]/(f(X))$ 中，元素可逆的条件是与模多项式互质。

设 $f(X) = X^n + 1 = X^{256} + 1$。

$X^{512} - 1 = (X^{256} - 1)(X^{256} + 1)$，且 $X^{512} - 1 = \prod_{d|512} \Phi_d(X)$，其中 $\Phi_d(X)$ 是分圆多项式。

$X^{256} + 1 = \Phi_{512}(X)$，因为 $512 = 2^9$ 是 $n \times 2 = 256 \times 2 = 512$。

$\Phi_{512}(X)$ 的次数为 $\phi(512) = 512 \times (1 - 1/2) = 256$，其中 ϕ 是欧拉函数。

在有限域 $\mathbb{Z}_q$ 上，分圆多项式 $\Phi_m(X)$ 的不可约因子次数等于 q 模 m 的乘法阶（当 $\gcd(q,m)=1$ 时）。

这里 $m=512$，$q=3329$，且 $\gcd(q,512)=1$（因为 q 是奇质数）。

计算 $q \mod 512$: $q=3329\equiv 257 \pmod{512}$（因为 $3329-6\times 512=3329-3072=257$）。

计算 q 模 512 的乘法阶：最小 d 使得 $q^d\equiv 1 \pmod{512}$。

$q\equiv 257\equiv 1+2^8 \pmod{512}$。

$q^2=257^2=66049\equiv 1 \pmod{512}$（因为 $512\times 129=66048$，$66049-66048=1$）。

$q^1=257\not\equiv 1 \pmod{512}$，故阶为 2。

因此，$\Phi_{512}(X)$ 在 $\mathbb{Z}_q$ 上分解为 $\phi(512)/\mathrm{ord}_q(512)=256/2=128$ 个互异的不可约因子，每个因子次数为 2。

即 $f(X)=X^{256}+1=p_1(X)p_2(X)\cdots p_{128}(X)$，其中每个 $p_i(X)$ 是 $\mathbb{Z}_q$ 上的首一不可约二次多项式。

因此，概率为：

$$p=\left(1-\frac{1}{q^2}\right)^{128} \tag{1.1}$$

其中 $q=3329$。

2. 结果

$$p=\left(1-\frac{1}{3329^2}\right)^{128} \tag{1.2}$$

。

二、题目二

1. 题目 (1)

1.1 解题思路

已知 $b(x)=a(x)s(x)+e(x)$，则多项式 $t(x)=s_0+s_1\cdot x+s_2\cdot x+\ldots+s_63\cdot x^{63}$ 可以表示为向量:

$$(s_0, s_1, s_2, ...s_{63}) \tag{2.1}$$

同理，$b(x)$ 和 $e(x)$ 也可以表示为:

$$(b_0, b_1, b_2, ...b_{63}) \tag{2.2}$$

$$(e_0, e_1, e_2, ...e_{63}) \tag{2.3}$$

将 $b(x) = a(x)s(x) + e(x)$ 转化为矩阵乘法形式:

$$(a_0, a_1, a_2, ...a_{n-1}) \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{n-1} \\ -b_{n-1} & b_0 & b_1 & \cdots & b_{n-2} \\ -b_{n-2} & -b_{n-1} & b_0 & \cdots & b_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_1 & -b_2 & -b_3 & \cdots & b_0 \end{pmatrix} = (c_0, c_1, c_2, ...c_{n-1}) \tag{2.4}$$

再把多项式乘法改为 $E = AS - B$ 形式将 (2.4) 中的矩阵构造格:

$$\lambda = \begin{pmatrix} p & & & & & & \\ & p & & & & & \\ & & p & & & & \\ & & & \ddots & & & \\ & & & & p & & \\ a_0 & a_1 & a_2 & \cdots & a_{n-1} & 1 & \\ -a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} & & 1 \\ -a_{n-2} & -a_{n-1} & a_0 & \cdots & a_{n-3} & & \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \\ -a_1 & -a_2 & -a_3 & \cdots & a_0 & & \\ b_0 & b_1 & b_2 & \cdots & b_{n-1} & & 1 \end{pmatrix} \tag{2.5}$$

格 λ 具有线性关系:

$$(k_0, k_1, ...k_{63}, s_0, s_1, ...s_{63}) \begin{pmatrix} p & & & & & & & & \\ & p & & & & & & & \\ & & p & & & & & & \\ & & & \cdots & & & & & \\ & & & & p & & & & \\ a_0 & a_1 & a_2 & \cdots & a_{n-1} & 1 & & & \\ -a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} & & 1 & & \\ -a_{n-2} & -a_{n-1} & a_0 & \cdots & a_{n-3} & & & 1 & \\ \vdots & \vdots & \vdots & \ddots & \vdots & & & \cdots & \\ -a_1 & -a_2 & -a_3 & \cdots & a_0 & & & & 1 \end{pmatrix} = (e_0, e_1, ...e_{63}, s_0, s_1, ...s_{63}) \tag{2.6}$$

这样问题就转换为格 λ 中的 CVP 问题. 再通过 Kannan 's embedding[1]，将问题转化为 SVP:

$$
(k_0,k_1,...k_{63},s_0,s_1,...s_{63},1)\begin{pmatrix}
p & & & & & & & \\
 & p & & & & & & \\
 & & \cdots & & & & & \\
 & & & p & & & & \\
a_0 & a_1 & \cdots & a_{n-1} & 1 & & & \\
-a_{n-1} & a_0 & \cdots & a_{n-2} & & & & \\
-a_{n-2} & -a_{n-1} & \cdots & a_{n-3} & & & & \\
\vdots & \vdots & \ddots & \vdots & & \cdots & & \\
-a_1 & -a_2 & \cdots & a_0 & & & 1 & \\
b_0 & b_1 & \cdots & b_{n-1} & & & & 1
\end{pmatrix} = (e_0,e_1,...e_{63},s_0,s_1,...s_{63},1) \tag{2.7}
$$

对格进行格基约化，则约化后的第一行的 [n,2n] 项即为私密多项式，时间复杂度为 $n^6(logB)^3$[2]

又或者使用 Sieving 求解 SVP 问题，在使用 *3-sieve (triple_sieve)* 时，时间复杂度为 $2^{0.396n+o(n)}$，其中 $n=2N+1$，N 为 RLWE 问题的维度，对于 $n=129$ 的问题，*total CPU time* 约为 *33.2h*[3]。

2. 题目 (2)

2.1 解题思路

3. 题目 (3)

4. 题目 (4)

5. 题目 (5)

6. 题目 (6)

7. 题目 (7)

8. 题目 (8)

三、解题结果

1. 题目 (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

四、结论

总结论文的主要贡献和结论。

参考文献

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

[2] L. M. Adleman and A. M. Odlyzko, “Irreducibility testing and factorization of polynomials,” in *Proceedings of the 22nd Annual IEEE Symposium on Foundations of Computer Science*, pp. 409–418, IEEE, 1981. Extended abstract of work to appear.

[3] 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.