- **环 LWE 上公钥加密方案 E4**

Lyubaskevsky 等人在 2010 年的欧密会上提出环 LWE 的公钥加密方案[48]，该方案可以认为是 Regev 的 LWE 公钥加密方案在环上的推广，方案如下。

参数模 $q \geq 2$，$n \geq 1$ 是 2 的幂次方，$f(x)=x^n+1$。令 $R=\mathbb{Z}[x]/(f(x))$，$R_q=\mathbb{Z}_q[x]/(f(x))$，$\chi$ 是 R 上的一个错误概率分布。

E4.SecretKeygen(1^λ)：随机均匀选取 $s' \leftarrow \chi$，输出密钥 $sk = \boldsymbol{s} \leftarrow (1, -s') \in R_q \times R_q$。

E4.PublicKeygen(sk): 随机均匀选取 $a \in R_q$，选取 $e_1 \leftarrow \chi$，计算 $b=as'+e_1$。输出公钥 $pk=\boldsymbol{A}=(b, a) \in R_q \times R_q$。注：$pk$ 可以看成是 2 维向量，也可以看成是一个 1×2 的矩阵 $\boldsymbol{A}$。

E4.Enc(pk, $\boldsymbol{m}$)：加密 n 位消息 $\boldsymbol{m} \in \{0, 1\}^n$，将其视为多项式 $m \in R_2$ 的系数。随机选择 $e_2, e_3, e_4 \leftarrow \chi$，输出密文 $\boldsymbol{c} \leftarrow (\lfloor q/2 \rfloor \cdot m, 0) + e_2\boldsymbol{A} + \boldsymbol{e} = (\lfloor q/2 \rfloor \cdot m + be_2 + e_3, ae_2 + e_4) \in R_q \times R_q$。其中 $\boldsymbol{e} = (e_3, e_4)$。

E4.Dec(sk, $\boldsymbol{c}$)：计算 $m \leftarrow \lfloor \frac{2}{q}[<\boldsymbol{c}, \boldsymbol{s}>]_q \rceil \bmod 2$，输出 m。