第5章 使用提升维数法设计环LWE上的无须密钥交换的全同态加密

本章使用提升维数法设计两个全同态加密方案：一个是环 LWE 上的无须密钥交换的全同态加密方案；另一个是 LWE 上的无须密钥交换的全同态加密方案。首先对两个方案的噪声进行详细分析，最后计算、分析并给出两个方案的具体安全参数，并且与同类的 GSW13 方案的具体参数进行对比分析。数据显示本章提出的两个方案在参数尺寸上具有明显的优势。

5.1 问题的提出

在第 4 章我们通过提升维数法设计了一个 NTRU 型无须密钥交换的全同态加密方案，因此有人会问：能否通过提升维数法设计环 LWE 上的无须密钥交换的全同态加密方案？

首先从密文的角度分析在目前环 LWE 加密方案上设计无须密钥交换的全同态加密方案的可行性。最典型的环 LWE 加密方案就是 Regev 在 2005 年设计的 LWE 上的公钥加密算法，后来 Lyubaskevsky 等在 2010 年的欧密会上将其推广到环 LWE 上。无论 LWE 上还是环 LWE 上的公钥加密，其密文都是向量。按照现在设计全同态加密的方法，密文乘积的定义必然导致其维数膨胀，如何才能避免密文乘积的维数膨胀呢？如果密文不是向量，而是矩阵，有可能避免密文乘积的维数膨胀，因为矩阵的乘积还是矩阵。密文如何才能从向量变成矩阵呢？这需要使用提升维数法。

第 4 章提出的提升维数法，能够将密文从多项式提升到向量。同样提升维数法也可以将密文从向量提升到矩阵。下面阐述如何使用提升维数法设计环 LWE 上无须密钥交换的全同态加密。这也说明了提升维数法的通用性与重要性。

5.2　解决问题的主要思想

本节分析如何使用提升维数法将密文从向量提升到矩阵，从而设计环 LWE 上无须密钥交换的全同态加密。

第 4 章使用提升维数法设计 NTRU 型全同态加密方案是非常自然的，因为环 LWE 上的 NTRU 加密方案的解密过程中含有形如 $mf+2v$ 的不变结构，该解密过程的不变结构中出现了密钥 f，使得密文乘积的解密过程中也保持了这种不变结构 $m_1m_2f+2m_2v_1+2c_1v_2$，如果噪声小，很自然地就获得了乘法同态性。但是，由于噪声很大，所以需要通过 BitDecomp 技术约减噪声，再通过提升维数法获得乘法同态性。

现在环 LWE 上公钥加密方案的密文是向量，其解密过程中的不变结构是 $\lfloor q/2 \rfloor \cdot m+e$，在该不变结构中不含有密钥 $\boldsymbol{s}$。如果想在环 LWE 上公钥加密方案上设计无密钥交换的全同态加密方案，密文应该是一个矩阵。这个矩阵是由一些密文向量组合构成的密文矩阵。例如，在环 LWE 公钥加密方案下，其加密可以看成 $\boldsymbol{c}\leftarrow(m,0)+\boldsymbol{e}$，其中 m 是一个明文多项式，$\boldsymbol{e}$ 是噪声。假设密钥是 $\boldsymbol{s}=(1,\boldsymbol{s}_1)$，解密过程中的不变结构为 $<\boldsymbol{c},\boldsymbol{s}>=m+e'$，其中 $e'=<\boldsymbol{e},\boldsymbol{s}>$。令 $\boldsymbol{c}_1$、$\boldsymbol{c}_2$ 是对 m 加密的两个密文，令 $\boldsymbol{C}\leftarrow\begin{bmatrix}\boldsymbol{c}_1^{\mathrm{T}}\\ \boldsymbol{c}_2^{\mathrm{T}}\end{bmatrix}=[\boldsymbol{c}_1^{\mathrm{T}}\ \boldsymbol{c}_2^{\mathrm{T}}]^{\mathrm{T}}$，则 $\boldsymbol{C}$ 是由 $\boldsymbol{c}_1$ 和 $\boldsymbol{c}_2$ 构成的一个矩阵，其中 $\boldsymbol{c}_1$、$\boldsymbol{c}_2$ 是列向量，所以 $\boldsymbol{c}_1^{\mathrm{T}}$ 和 $\boldsymbol{c}_2^{\mathrm{T}}$ 表示行向量，$\boldsymbol{C}$ 可以看成由两个密文行向量堆叠而成的矩阵。可以验证这样的矩阵是否具有乘法同态性。令 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 是加密 m_1 和 m_2 的两个矩阵，对应密钥是 $\boldsymbol{s}$，于是有

$$\boldsymbol{C}_1\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}=\boldsymbol{C}_1\cdot(\boldsymbol{C}_2\cdot\boldsymbol{s})=\boldsymbol{C}_1\cdot\left(\begin{bmatrix}m_2\\ m_2\end{bmatrix}+\begin{bmatrix}e_1'\\ e_2'\end{bmatrix}\right)$$

$$=\boldsymbol{C}_1\begin{bmatrix}m_2\\ m_2\end{bmatrix}+C_1\begin{bmatrix}e_1'\\ e_2'\end{bmatrix}=\boldsymbol{C}_1\begin{bmatrix}m_2\\ m_2\end{bmatrix}+\boldsymbol{C}_1\boldsymbol{E}_2$$

可见，在解密不变结构中不含有密钥 $\boldsymbol{s}$，使得 $\boldsymbol{C}_1$ 无法解密出来，导致无法获得乘法同态性。因此，必须在解密不变结构中含有密钥 $\boldsymbol{s}$。为了做到这一点，需要使用提升维数法。

为了表述清楚，可将提升维数法拆分成两步。先进行第一次提升。假设密钥的维数是 k 维，使用提升维数法对 $(m,0,\cdots,0)$、$(0,m,0,\cdots,0)$、……、$(0,\cdots,0,m)$ 分别加密，形成的密文按照上述方法组合成一个密文矩阵。例如，在环 LWE 公钥加密方案下，密钥的维数是 2，所以对 $(m,0)$、$(0,m)$ 分别加密形成两个 2×2 的密文矩阵 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$，对应密钥是 $\boldsymbol{s}=(1,\boldsymbol{s}_1)$，于是有

$$\boldsymbol{C}_1\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}=\boldsymbol{C}_1\cdot(\boldsymbol{C}_2\cdot\boldsymbol{s})=\boldsymbol{C}_1\cdot\left(\begin{bmatrix}m_2\\ m_2\ \boldsymbol{s}_1\end{bmatrix}+\begin{bmatrix}e_1'\\ e_2'\end{bmatrix}\right)$$

$$=\boldsymbol{C}_1\cdot\left(m_2\begin{bmatrix}1\\ \boldsymbol{s}_1\end{bmatrix}+\begin{bmatrix}e_1'\\ e_2'\end{bmatrix}\right)=m_2\boldsymbol{C}_1\boldsymbol{s}+C_1E_2$$

$$=m_1m_2\boldsymbol{s}+m_2\boldsymbol{E}_1+\boldsymbol{C}_1\boldsymbol{E}_2$$

上述解密结构中出现了密钥 $\boldsymbol{s}$，和第 4 章 NTRU 型加密方案的不变结构形式上是一样的。如果噪声 $m_2\boldsymbol{E}_1+\boldsymbol{C}_1\boldsymbol{E}_2$ 是小的，则可能具有乘法同态性。但是噪声 $m_2\boldsymbol{E}_1+\boldsymbol{C}_1\boldsymbol{E}_2$ 是依赖于密文 $\boldsymbol{C}_1$ 的，这和第 4 章 NTRU 型加密方案是一样的。所以，约减噪声可以采用 BitDecomp 技术，令 $l=\lceil\log q\rceil$，将密文乘积定义为 $\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2$，但是，由于 $\mathrm{BitDecomp}(\boldsymbol{C}_1)$ 是 $2\times 2l$ 的矩阵，而 $\boldsymbol{C}_2$ 是 2×2 的矩阵，所以两者还不能相乘，即使能够相乘，由于 $\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}=m_2\,\mathrm{BitDecomp}(\boldsymbol{C}_1)\boldsymbol{s}+C_1\boldsymbol{E}_2$，解密结构中没有 $\mathrm{Powerof2}(\boldsymbol{s})$，所以无法将 $\boldsymbol{C}_1$ 解密，因此不具有乘法同态性。为了在解密结构中出现 $\mathrm{Powerof2}(\boldsymbol{s})$，需要再次使用提升维数法。

第二次使用提升维数法是对每一维加密如下明文：m、$m\cdot 2$、$m\cdot 2^2$、…、$m\cdot 2^{l-1}$。例如，在上例中，密钥 $\boldsymbol{s}$ 的维数是 2，所以需要加密的明文向量是 $(m,0)$，$(m\cdot 2,0)$，…，$(m\cdot 2^{l-1},0)$，$(0,m)$，$(0,m\cdot 2)$，…，$(0,m\cdot 2^{l-1})$，一共有 $2l$ 个明文向量，经过加密后形成 $2l$ 个密文，这 $2l$ 个密文按照行向量的形式可以组合成一个 $2l\times 2$ 的矩阵，即该矩阵中的每一行就是一个密文向量，这个矩阵就是所需要的密文矩阵。下面验证其乘法同态性。

令 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 是按照上述方法加密 $(m_i,0)$，$(m_i\cdot 2,0)$，…，$(m_i\cdot 2^{l-1},0)$，$(0,m_i)$，$(0,m_i\cdot 2)$，…，$(0,m_i\cdot 2^{l-1})$ 的两个矩阵，其中 $i=1,2$。密文对应的密钥是 $\boldsymbol{s}$，$\mathrm{BitDecomp}(\boldsymbol{C}_1)$ 是一个 $2l\times 2$ 的矩阵，$\boldsymbol{C}_2$ 是一个 $2l\times 2$ 的矩阵，定义密文乘积是

$$\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2$$

有

$$\begin{aligned}\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}&=\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot(\boldsymbol{C}_2\cdot\boldsymbol{s})\\&=\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\left(\begin{bmatrix}m_2\\2m_2\\\vdots\\2^{l-1}m_2\end{bmatrix}\boldsymbol{s}_1+E_2\right)\\&=m_2\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\mathrm{Powerof}(\boldsymbol{s})+\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{E}_2\\&=(m_1m_2)\cdot\mathrm{Powerof}(\boldsymbol{s})+m_2\boldsymbol{E}_1+\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{E}_2\end{aligned}$$

上述密文乘积解密过程中保持了不变结构，而且噪声 $m_2\boldsymbol{E}_1+\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{E}_2$ 依赖于 $\mathrm{BitDecomp}(\boldsymbol{C}_1)$，由于 $\mathrm{BitDecomp}(\boldsymbol{C}_1)$ 是小的，所以噪声是小的，因此获得了乘法同态性。

由上述分析可知，对于环 LWE 上的公钥加密方案，使用提升维数法可以将密文从向量提升到矩阵，从而获得无须密钥交换的全同态加密方案。对于 LWE 上的公钥加密，用同样的方法也可获得无须密钥交换的全同态加密。

5.3 提升维数法

提升维数法的描述见第 4.3 节。注意，如果 $E1$ 方案是环 LWE 上的加密方案，则 $k=2$，$E2$ 的密文就是一个 $2l\times 2$ 的矩阵。如果 $E1$ 方案是 LWE 上的加密方案，则 $k=n+1$，$E2$ 的密文就是一个 $(n+1)l\times(n+1)$ 的矩阵。

5.4　密文是矩阵的环 LWE 上的加密方案

将提升维数法拆分成两步，本节使用第一步提升形成一个密文是矩阵的环 LWE 加密方案。该方案的解密过程中含有不变结构 $m\boldsymbol{s}+\boldsymbol{E}$，其中 m 是明文，$\boldsymbol{s}$ 是密钥，$\boldsymbol{C}$ 是密文矩阵，$\boldsymbol{E}$ 是噪声。可见，是可能获得乘法同态性的，只是由于密文噪声依赖于密文，导致噪声过大，无法正确解密，从而丧失乘法同态性。

R1.Setup(λ，L)：输入安全参数 λ 和电路深度 L，输出模 $q\geqslant 2$，多项式次数 $n\geqslant 1$，环 $R=\mathbb{Z}[x]/(f(x))$，$R_q=\mathbb{Z}_q[x]/(f(x))$，噪声分布 χ。其中 n 是 2 的幂次方，$f(x)=x^n+1$，以及 χ 是 R 上的一个错误概率分布。

R1.SecretKeygen(1^λ)：随机均匀选取 $s'\leftarrow\chi$，输出密钥 $\mathrm{sk}=\boldsymbol{s}\leftarrow(1,-s')\in R_q\times R_q$。

R1.PublicKeygen(sk)：随机均匀选取 $a\in R_q$，并选取 $e_1\leftarrow\chi$，计算 $b=as'+2e_1$。输出公钥 $\mathrm{pk}=\boldsymbol{A}=(b,a)\in R_q\times R_q$。其中 $\boldsymbol{As}=2e_1$。注意：pk 可看成一个 1×2 的矩阵 $\boldsymbol{A}$。

R1.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。随机选择矩阵 $\boldsymbol{E}_1\leftarrow\chi^{2\times 1}$，$\boldsymbol{E}_2\leftarrow\chi^{2\times 2}$，$\boldsymbol{E}_1$ 是 2×1 的矩阵，$\boldsymbol{E}_2$ 是 2×2 的矩阵，矩阵中的每个元素都是随机从 χ 中选取的。输出密文

$$\boldsymbol{C}\leftarrow\begin{bmatrix}m & 0\\ 0 & m\end{bmatrix}+\boldsymbol{E}_1\boldsymbol{A}+2\boldsymbol{E}_2\in R_q^{2\times 2}$$

R1.Dec(sk，$\boldsymbol{C}$)：令 $\boldsymbol{c}_1$ 是密文 $\boldsymbol{C}$ 的第一行，计算输出 $\langle\boldsymbol{c}_1,\boldsymbol{s}\rangle \bmod q \bmod 2$。

下面分析上述方案的解密结构，从而分析其同态特性。

解密结构　$\boldsymbol{C}\cdot\boldsymbol{s}=\begin{bmatrix}m & 0\\ 0 & m\end{bmatrix}\cdot\boldsymbol{s}+\boldsymbol{E}_1\boldsymbol{A}\,\boldsymbol{s}+2\boldsymbol{E}_2\,\boldsymbol{s}=m\,\boldsymbol{s}+2\boldsymbol{E}_1e_1+2\boldsymbol{E}_2\,\boldsymbol{s}=m\,\boldsymbol{s}+2\boldsymbol{e}'$。其中 $\boldsymbol{e}'$ 是噪声。令 $\boldsymbol{e}'=(e_1',e_2')$，$\langle\boldsymbol{c}_1,\boldsymbol{s}\rangle \bmod q=m+2e_1' \bmod q$，只要 $\|e_1'\|_\infty<q/4$，$\langle\boldsymbol{c}_1,\boldsymbol{s}\rangle \bmod q \bmod 2$ 就可以解密出 m。该解密结构和第 4 章 NTRU 型加密方案的解密结构形式是一样的。加法同态性是满足的，下面分析其乘法同态性。

乘法同态性　令 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 是上述加密方案生成的密文，密钥是 $\boldsymbol{s}$，根据解密结构有

$$\boldsymbol{C}_1\cdot\boldsymbol{s}=m_1\,\boldsymbol{s}+2\,\boldsymbol{e}_1'$$

$$\boldsymbol{C}_2\cdot\boldsymbol{s}=m_2\,\boldsymbol{s}+2\,\boldsymbol{e}_2'$$

密文乘积的解密结构是 $\boldsymbol{C}_1\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}=m_2\,\boldsymbol{C}_1\boldsymbol{s}+2\boldsymbol{C}_1\boldsymbol{e}_2'=m_1m_2\,\boldsymbol{s}+2(m_2\boldsymbol{e}_1'+\boldsymbol{C}_1\boldsymbol{e}_2')$，所以密文乘积的噪声依赖于密文，因此噪声过大会导致密文解密失败，从而丧失乘法同态性。为了降低噪声，将乘积定义为 $\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2$，但是 $\mathrm{BitDecomp}(\boldsymbol{C}_1)$ 是 $2\times 2l$ 的矩阵，而 $\boldsymbol{C}_2$ 是 2×2 的矩阵，两者还不能相乘，所以再次使用提升维数法将密文从 2×2 的矩阵扩展为 $2l\times 2$ 的矩阵，从而可以将乘积定义为 $\mathrm{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2$，达到约减噪声的目的，以获得乘法同态性。

5.5 环 LWE 上的扩展加密方案

第 5.4 节加密方案的密文是 2×2 的矩阵，下面使用提升维数法为矩阵中的每一行添加 $l-1$ 个辅助项，从而扩展为 $2l\times 2$ 的矩阵。

R2.Setup(λ)：输入安全参数 λ，输出模 $q\geqslant 2$，多项式次数 $n\geqslant 1$，环 $R=\mathbb{Z}[x]/(f(x))$，$R_q=\mathbb{Z}_q[x]/(f(x))$，噪声分布 χ。其中 n 是 2 的幂次方，$f(x)=x^n+1$，以及 χ 是 R 上的一个错误概率分布，$l=\lceil \log q \rceil$。

R2.SecretKeygen(1^λ)：随机均匀选取 $s'\leftarrow\chi$，输出密钥 $\mathrm{sk}=\boldsymbol{s}\leftarrow(1,\ -s')\in R_q\times R_q$。

R2.PublicKeygen(sk)：随机均匀选取 $a\in R_q$，并选取 $e_1\leftarrow\chi$，计算 $b=as'+e_1$。输出公钥 $\mathrm{pk}=\boldsymbol{A}=(b,\ a)\in R_q\times R_q$。注意：pk 可看成一个 1×2 的矩阵 $\boldsymbol{A}$。

R2.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。随机选择矩阵 $\boldsymbol{E}_1\leftarrow\chi^{2l\times 1}$，$\boldsymbol{E}_2\leftarrow\chi^{2l\times 2}$，$\boldsymbol{E}_1$ 是 $2l\times 1$ 的矩阵，$\boldsymbol{E}_2$ 是 $2l\times 2$ 的矩阵，矩阵中的每个元素都是随机从 χ 中选取的。输出密文

$$\boldsymbol{C}\leftarrow\begin{bmatrix} m & 0\\ 2m & 0\\ \vdots & \vdots\\ 2^{l-1}m & 0\\ 0 & m\\ 0 & 2m\\ \vdots & \vdots\\ 0 & 2^{l-1}m \end{bmatrix}+\boldsymbol{E}_1\boldsymbol{A}+\boldsymbol{E}_2\in R_q^{2l\times 2}$$

R2.Dec(sk, $\boldsymbol{C}$)：令 $\boldsymbol{c}_{l-1}$ 是密文 $\boldsymbol{C}$ 的第 $l-1$ 行，即该行对应的明文是 $2^{l-2}m$，输出 $\lfloor <\boldsymbol{c}_{l-1},\ \boldsymbol{s}> \bmod q/2^{l-2}\rceil$。

引理 5-1 （加密噪声）令 q、n、R、$|\chi|\leqslant B$ 是如上扩展加密方案的参数，任意 $s'\leftarrow\chi$，有 $\boldsymbol{s}\leftarrow(1,\ -s')\in R_q\times R_q$。任意 $m\in R_2$，令 $\boldsymbol{A}\leftarrow$**R2.PublicKeygen**($\boldsymbol{s}$)和 $\boldsymbol{C}\leftarrow$**R2.Enc**($\boldsymbol{A}$, m)，存在 $\boldsymbol{E}'\in R_q^{2l}$ 且 $\|\boldsymbol{E}'\|_\infty<2nB^2+B$，使得如下等式成立：

$$<\boldsymbol{C},\ \boldsymbol{s}>=m\cdot\mathrm{Powerof2}(\boldsymbol{s})+\boldsymbol{E}'\ (\bmod q)$$

证明：根据加密方案，有

$$<\boldsymbol{C},\ \boldsymbol{s}>=\begin{bmatrix} m & 0\\ 2m & 0\\ \vdots & \vdots\\ 2^{l-1}m & 0\\ 0 & m\\ 0 & 2m\\ \vdots & \vdots\\ 0 & 2^{l-1}m \end{bmatrix}\cdot\boldsymbol{s}+\boldsymbol{E}_1\boldsymbol{A}\ \boldsymbol{s}+\boldsymbol{E}_2\boldsymbol{s}\ (\bmod q)$$

$$=m\cdot \text{Powerof2}(\boldsymbol{s})+\boldsymbol{E}_1\boldsymbol{e}_1+\boldsymbol{E}_2\boldsymbol{s}(\bmod q)$$
$$=m\cdot \text{Powerof2}(\boldsymbol{s})+\boldsymbol{E}'(\bmod q)$$

其中 $\|\boldsymbol{E}'\|_\infty<\|\boldsymbol{E}_1\boldsymbol{e}_1+\boldsymbol{E}_2\boldsymbol{s}\|_\infty<\|\boldsymbol{E}_1\boldsymbol{e}_1\|_\infty+\|\boldsymbol{E}_2\boldsymbol{s}\|_\infty<nB^2+B+nB^2=2nB^2+B$。

引理 5-2　（解密噪声）χ 是 R 上的一个错误概率分布，随机选取 $s'\leftarrow\chi$，令 $\boldsymbol{s}\leftarrow(1,-s')$。若存在 $\boldsymbol{C}\in R_q^{2l\times 2}$，使得下式成立：

$$<\boldsymbol{C},\boldsymbol{s}>=m\cdot \text{Powerof2}(\boldsymbol{s})+\boldsymbol{E}'(\bmod q)$$

其中 $m\in R_2$，$\|\boldsymbol{E}'\|_\infty<q/8$，则有

$$m\leftarrow\textbf{R2.Dec}(\boldsymbol{s},\boldsymbol{C})$$

证明：因为 **R2.Dec**($\boldsymbol{s}$, $\boldsymbol{C}$)是取出密文 $\boldsymbol{C}$ 的第 $l-1$ 行 $\boldsymbol{c}_{l-1}$，计算$<\boldsymbol{c}_{l-1},\boldsymbol{s}>\bmod q$。根据已知条件$<\boldsymbol{c}_{l-1},\boldsymbol{s}>\bmod q=m\cdot 2^{l-2}+e'(\bmod q)$，且$|e'|<q/8$。由于$q/4<2^{l-2}<q/2$，所以 $\|e'/2^{l-2}\|_\infty<1/2$。因此，$m\leftarrow\lfloor<\boldsymbol{c}_{l-1},\boldsymbol{s}>\bmod q/2^{l-2}\rceil$。

引理 5-3　（安全性）令 q、n、R、$|\chi|\leqslant B$ 是满足判定性环 LWE 问题困难的参数。任意 $m\in R_2$，若 $\boldsymbol{s}\leftarrow\textbf{R2.SecretKeygen}(1^\lambda)$，$\boldsymbol{A}\leftarrow\textbf{R2.PublicKeygen}(\boldsymbol{s})$，$\boldsymbol{C}\leftarrow\textbf{R2.Enc}(\boldsymbol{A},\boldsymbol{m})$，则($\boldsymbol{A}$, $\boldsymbol{C}$)与 $R_q^2\times R_q^{2l\times 2}$ 上的均匀分布是不可区分的。

证明：$\boldsymbol{A}$ 就是环 LWE 上 Regev 公钥加密方案的公钥，所以根据参考文献[48]可知 $\boldsymbol{A}$ 与 R_q^2 上的均匀分布不可区分。而 $\boldsymbol{C}$ 是由 $2l$ 个环 LWE 上 Regev 公钥加密方案的密文构成的，所以根据参考文献[48]可知 $\boldsymbol{C}$ 与 $R_q^{2l\times 2}$ 上的均匀分布是不可区分的。因此，($\boldsymbol{A}$, $\boldsymbol{C}$)与 $R_q^2\times R_q^{2l\times 2}$ 上的均匀分布是不可区分的。

5.6　环 LWE 上扩展加密方案的同态性

本节分析上述环 LWE 扩展加密方案的同态性。令 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 是上述环 LWE 扩展加密方案分别加密 m_1 和 m_2 的两个密文，密钥是 $\boldsymbol{s}$，根据引理 5-2 有

$$\boldsymbol{C}_1\cdot\boldsymbol{s}=m_1\cdot \text{Powerof2}(\boldsymbol{s})+\boldsymbol{E}_1'\bmod q$$
$$\boldsymbol{C}_2\cdot\boldsymbol{s}=m_2\cdot \text{Powerof2}(\boldsymbol{s})+\boldsymbol{E}_2'\bmod q$$

其中 $\boldsymbol{E}_1'$ 和 $\boldsymbol{E}_2'$ 是小的，即 $\|\boldsymbol{E}_1'\|_\infty<q/8$，$\|\boldsymbol{E}_2'\|_\infty<q/8$。

5.6.1　加法同态性

令 $\boldsymbol{C}^+=\boldsymbol{C}_1+\boldsymbol{C}_2$，则 $\boldsymbol{C}^+\cdot\boldsymbol{s}=\boldsymbol{C}_1\cdot\boldsymbol{s}+\boldsymbol{C}_2\cdot\boldsymbol{s}=(m_1+m_2)\cdot \text{Powerof2}(\boldsymbol{s})+(\boldsymbol{E}_1'+\boldsymbol{E}_2')$。根据引理 5-2，只要 $\boldsymbol{E}_1'+\boldsymbol{E}_2'$ 是小的，就能正确解密得到 m_1+m_2。由于 $\boldsymbol{E}_1'$ 和 $\boldsymbol{E}_2'$ 是小的，所以加法同态性满足。

5.6.2　乘法同态性

令 $\boldsymbol{C}^\times=\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2$，则有

$$\boldsymbol{C}^\times\cdot\boldsymbol{s}=\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}$$
$$=\text{BitDecomp}(\boldsymbol{C}_1)\cdot(m_2\cdot \text{Powerof2}(\boldsymbol{s})+\boldsymbol{E}_2')$$

$$=m_1m_2\cdot \text{Powerof2}(\boldsymbol{s})+m_2\boldsymbol{E}_1'+\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{E}_2'$$

因为 $\boldsymbol{E}_1'$、$\boldsymbol{E}_2'$和 $\text{BitDecomp}(\boldsymbol{C}_1)$是小的，所以 $\boldsymbol{C}^{\times}$能够正确解密得到 m_1m_2。因此，按照上述乘法定义，乘法同态性是满足的。

5.7 密文同态计算的噪声分析

本节对扩展加密方案的加法和乘法的噪声进行分析，说明同态计算的电路深度，从而证明扩展加密方案可以进行多项式深度的同态密文电路计算。令 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 是上述环 LWE 扩展加密方案分别加密 m_1 和 m_2 的两个密文，密钥是 $\boldsymbol{s}$，且有 $\boldsymbol{C}_i\cdot\boldsymbol{s}=m_i\cdot\text{Powerof2}(\boldsymbol{s})+\boldsymbol{E}_i'$，其中 $i=1,2$。根据引理 5-1 有 $\|\boldsymbol{E}_i'\|_{\infty}<2nB^2+B$，所以密文 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$的噪声上界是 $2nB^2+B$。注意：这里的 $\boldsymbol{C}_1$和 $\boldsymbol{C}_2$是初始密文。下面分析密文加法与乘法的噪声。

5.7.1 加法噪声分析

由第 5.6.1 节可知 $\boldsymbol{C}^{+}\cdot\boldsymbol{s}=\boldsymbol{C}_1\cdot\boldsymbol{s}+\boldsymbol{C}_2\cdot\boldsymbol{s}=(m_1+m_2)\cdot\text{Powerof2}(\boldsymbol{s})+(\boldsymbol{E}_1'+\boldsymbol{E}_2')$。由于 $\|\boldsymbol{E}_i'\|_{\infty}<2nB^2+B$，所以 $\|\boldsymbol{E}_1'+\boldsymbol{E}_2'\|_{\infty}<4nB^2+2B$。因此，密文之和的噪声等于密文的噪声之和。和其他方案一样，加法噪声增长是缓慢的，所以这里主要考虑乘法的噪声增长。

5.7.2 乘法噪声分析

由第 5.6.2 节可知 $\boldsymbol{C}^{\times}\cdot\boldsymbol{s}=\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}=m_1m_2\cdot\text{Powerof2}(\boldsymbol{s})+m_2\boldsymbol{E}_1'+\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{E}_2'$。令 $\boldsymbol{E}''=m_2\boldsymbol{E}_1'+\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{E}_2'$，由于 $\|\boldsymbol{E}_i'\|_{\infty}<2nB^2+B=E$，所以 $\|\boldsymbol{E}''\|_{\infty}<2nlE+E$。令 $N=2l$，则 $\|\boldsymbol{E}''\|_{\infty}<(nN+1)E$。

经过深度为 L 的电路计算，结果密文的噪声至多为 $(nN+1)^LE$。根据引理 5-2 可知，经过深度为 L 的电路计算，结果密文解密的正确性条件是：

$$(nN+1)^LE=(2nl+1)^LE<q/8$$

另外，已知最好的求解 LWE 问题的时间是 $2^{n/\log(q/B)}$，环 LWE 问题也类似，所以对于 $\varepsilon<1$，选取 $q=2^{n^{\varepsilon}}$ 以及选取 B 为关于 n 的多项式，根据 $(nN+1)^LE<q/8$，有 $L\approx\log q\approx n^{\varepsilon}$。这意味着基于上述加法与乘法的定义，扩展加密方案能够执行一个多项式深度的密文同态电路计算，所以可获得一个多项式深度的层次型全同态加密方案。

5.8 环 LWE 上扩展加密方案上的层次型全同态加密方案

根据第 5.5 节的环 LWE 上的扩展加密方案，以及上述同态性和噪声分析，可以获得一个层次型全同态加密，方案如下。

R3.Setup(λ, L)：输入安全参数 λ 和电路深度 L，输出模 $q\geqslant 2$，多项式次数 $n\geqslant 1$，环 $R=\mathbb{Z}[x]/(f(x))$，$R_q=\mathbb{Z}_q[x]/(f(x))$，噪声分布 χ。其中 n 是 2 的幂次方，$f(x)=x^n+1$，以及 χ 是 R 上的一个错误概率分布，$l=\lceil \log q \rceil$。

R3.SecretKeygen(1^λ)：调用 sk←**R2.SecretKeygen**(1^λ)。

R3.PublicKeygen(sk)：调用 pk←**R2.PublicKeygen**(sk)。

R3.Enc(pk, $\boldsymbol{m}$)：加密 n 位消息 $\boldsymbol{m}\in\{0,1\}^n$，调用 $\boldsymbol{C}$←**R2.Enc**(pk, $\boldsymbol{m}$)。

R3.Dec(sk, $\boldsymbol{C}$)：$\boldsymbol{C}$←调用 **R2.Dec**(sk, $\boldsymbol{C}$)。

R3.Add(pk, $\boldsymbol{C}_1$, $\boldsymbol{C}_2$)：输出 $\boldsymbol{C}_1+\boldsymbol{C}_2$。

R3.Mult(pk, $\boldsymbol{C}_1$, $\boldsymbol{C}_2$)：输出 BitDecomp($\boldsymbol{C}_1$)$\cdot\boldsymbol{C}_2$。

上述层次型全同态加密方案的加密算法与解密算法和第 5.5 节环 LWE 上的扩展加密方案完全相同，只是在全同态加密方案中定义了密文计算，该计算就是矩阵的加法与乘法，因此其安全性与第 5.5 节环 LWE 上的扩展加密方案完全一样。

根据第 5.7 节的噪声分析，选择合适的参数，上述层次型全同态加密方案可以进行多项式深度的同态密文电路计算，所以上述层次型全同态加密方案是一个多项式深度的层次型全同态加密方案，由此得到定理 5-1。

定理 5-1　在环 LWE 问题的困难性假设下，且 $q/B\leqslant 2^{n^\varepsilon}$，对于每个多项式大小的 $L>0$，存在 $\varepsilon<1$，使得上述方案是一个层次型全同态加密方案。

以上是使用提升维数法设计环 LWE 上的无须密钥交换的层次型全同态加密方案，下面使用相同的方法设计 LWE 上的无须密钥交换的层次型全同态加密方案。同样，首先设计一个密文是矩阵的 LWE 加密方案，在此基础上再通过提升维数法设计一个 LWE 扩展加密方案，经过对乘法的合适定义就可获得一个多项式深度的层次型全同态加密方案。

以上是使用提升维数法设计的环 LWE 上的方案。下面使用提升维数法设计 LWE 上的方案。

5.9　密文是矩阵的 LWE 上加密方案

设计该方案是为了在解密过程中含有不变结构 $m\boldsymbol{s}+\boldsymbol{E}$，其中 m 是明文，$\boldsymbol{s}$ 是密钥，$\boldsymbol{C}$ 是密文矩阵，$\boldsymbol{E}$ 是噪声，从而可能获得乘法同态性。

L1.Setup(λ)：输入安全参数 λ，输出模 q、噪声分布 χ 和维数 n。其中分布 χ 是 $\mathbb{Z}$ 上的噪声高斯分布。

L1.SecretKeygen(1^n)：随机均匀选取向量 $\boldsymbol{s}'\leftarrow\mathbb{Z}_q^n$，输出 sk=$\boldsymbol{s}$←$(1,\boldsymbol{s}')\in\mathbb{Z}_q^{n+1}$。

L1.PublicKeygen($\boldsymbol{s}$)：令 $m\geqslant 2(n\log q)$。随机均匀选取矩阵 $\boldsymbol{A}'\leftarrow\mathbb{Z}_q^{m\times n}$ 和向量 $\boldsymbol{e}\leftarrow\chi^m$，计算 $\boldsymbol{b}\leftarrow\boldsymbol{A}'\boldsymbol{s}'+2\boldsymbol{e}$。令 $\boldsymbol{A}$ 是 $n+1$ 列矩阵，它由向量 $\boldsymbol{b}$ 和矩阵 $-\boldsymbol{A}'$ 构成，即 $\boldsymbol{A}=[\boldsymbol{b}\mid-\boldsymbol{A}']\in\mathbb{Z}_q^{m\times(n+1)}$，其中 $\boldsymbol{A}\cdot\boldsymbol{s}=2\boldsymbol{e}$。输出 pk=$\boldsymbol{A}$。

L1.Enc(pk,m)：加密消息 $m\in\{0,1\}$，选取 $\boldsymbol{R}\in\{0,1\}^{(n+1)\times m}$，输出密文

$$\boldsymbol{C}\leftarrow\begin{bmatrix} m & 0 & \cdots & 0 \\ 0 & m & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & m \end{bmatrix}_{(n+1)\times(n+1)} +\boldsymbol{RA}\in\mathbb{Z}_q^{(n+1)\times(n+1)}$$

L1.Dec(sk, $\boldsymbol{C}$)：令 $\boldsymbol{c}_1$是密文$\boldsymbol{C}$ 的第一行，计算输出$<\boldsymbol{c}_1, \boldsymbol{s}>\bmod q \bmod 2$。

下面分析上述方案的解密结构，从而分析其同态特性。

解密结构 $\boldsymbol{C}\cdot\boldsymbol{s}=\begin{bmatrix} m & 0 & \cdots & 0 \\ 0 & m & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & m \end{bmatrix}\boldsymbol{s}+\boldsymbol{RAs}=m\boldsymbol{s}+2\boldsymbol{Re}=m\boldsymbol{s}+2\boldsymbol{e}'$，其中 $\boldsymbol{e}'$是噪声。令 $\boldsymbol{e}'=(e_1', e_2', \cdots, e_{n+1}')$，则$<\boldsymbol{c}_1, \boldsymbol{s}>\bmod q = m+2e_1' \bmod q$，只要$|e_1'|<q/4$，则$<\boldsymbol{c}_1, \boldsymbol{s}>\bmod q \bmod 2$ 可以解密出 m。该解密结构和第 4 章 NTRU 型加密方案的解密结构形式是一样的。加法同态性是满足的，下面分析其乘法同态性。

乘法同态性 令 $\boldsymbol{C}_1$和 $\boldsymbol{C}_2$是上述加密方案生成的密文，密钥是 $\boldsymbol{s}$，根据解密结构有

$$\boldsymbol{C}_1\cdot\boldsymbol{s}=m_1\boldsymbol{s}+2\boldsymbol{e}_1'$$

$$\boldsymbol{C}_2\cdot\boldsymbol{s}=m_2\boldsymbol{s}+2\boldsymbol{e}_2'$$

密文乘积的解密结构是 $\boldsymbol{C}_1\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}=m_2\boldsymbol{C}_1\boldsymbol{s}+2\boldsymbol{C}_1\boldsymbol{e}_2'=m_1m_2\boldsymbol{s}+2(m_2\boldsymbol{e}_1'+\boldsymbol{C}_1\boldsymbol{e}_2')$，所以密文乘积的噪声依赖于密文，因此噪声过大会导致密文解密失败，从而丧失乘法同态性。为了降低噪声，将乘积定义为 BitDecomp($\boldsymbol{C}_1$)$\cdot\boldsymbol{C}_2$，但是 BitDecomp($\boldsymbol{C}_1$)是$(n+1)\times(n+1)l$ 的矩阵，而 $\boldsymbol{C}_2$是$(n+1)\times(n+1)$的矩阵，两者还不能相乘，所以再次使用提升维数法将密文从$(n+1)\times(n+1)$的矩阵扩展为$(n+1)l\times(n+1)$的矩阵，从而可以将乘积定义为 BitDecomp($\boldsymbol{C}_1$)$\cdot\boldsymbol{C}_2$，达到约减噪声的目的，以获得乘法同态性。

5.10 LWE 上的扩展加密方案

第 5.9 节加密方案的密文是$(n+1)\times(n+1)$的矩阵，下面使用提升维数法为矩阵中的每一行添加 $l-1$ 个辅助项，从而扩展为 $(n+1)l\times(n+1)$的矩阵。

L2.Setup(λ)：输入安全参数 λ，输出模 q、噪声分布 χ 和维数 n。其中分布 χ 是 $\mathbb{Z}$ 上的噪声高斯分布。$l=\lceil\log q\rceil$。

L2.SecretKeygen(1^n)：随机均匀选取向量 $\boldsymbol{s}'\leftarrow\mathbb{Z}_q^n$，输出 $\mathrm{sk}=\boldsymbol{s}\leftarrow(1, \boldsymbol{s}')\in\mathbb{Z}_q^{n+1}$。

L2.PublicKeygen (sk)：令 $k\geqslant 2(n\log q)$。随机均匀选取矩阵 $\boldsymbol{A}'\leftarrow\mathbb{Z}_q^{k\times n}$ 和向量 $\boldsymbol{e}\leftarrow\chi^k$，计算 $\boldsymbol{b}\leftarrow\boldsymbol{A}'\boldsymbol{s}'+\boldsymbol{e}$。令 $\boldsymbol{A}$ 是 $n+1$ 列矩阵，它由向量 $\boldsymbol{b}$ 和矩阵 $-\boldsymbol{A}'$构成，即 $\boldsymbol{A}=[\boldsymbol{b}|-\boldsymbol{A}']\in\mathbb{Z}_q^{k\times(n+1)}$，其中 $\boldsymbol{A}\cdot\boldsymbol{s}=\boldsymbol{e}$。输出 $\mathrm{pk}=\boldsymbol{A}$。

L2.Enc(pk, m)：加密消息 $m\in\{0,1\}$，选取 $\boldsymbol{R}\in\{0,1\}^{(n+1)l\times k}$，输出密文

$$\boldsymbol{C}\leftarrow\begin{bmatrix} m & & & & \\ 2m & & & & \\ \vdots & & & & \\ 2^{l-1}m & & & & \\ & m & & & \\ & 2m & & & \\ & \vdots & & & \\ & 2^{l-1}m & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & m \\ & & & & 2m \\ & & & & \vdots \\ & & & & 2^{l-1}m \end{bmatrix}_{(n+1)l\times(n+1)} + \boldsymbol{RA} \in \mathbb{Z}_q^{(n+1)l\times(n+1)}$$

L2.Dec(sk, $\boldsymbol{C}$)：令 $\boldsymbol{c}_1$ 是密文 $\boldsymbol{C}$ 的第 $l-1$ 行，即该行对应的明文是 $2^{l-2}m$，输出 $\lfloor <\boldsymbol{c}_{l-1}, \boldsymbol{s}> \bmod q/2^{l-2} \rceil$。

引理 5-4　（加密噪声）令 q、n、$|\chi|\leqslant B$ 是如上扩展加密方案的参数，任意 $\boldsymbol{s}'\leftarrow\mathbb{Z}_q^n$，有 $\boldsymbol{s}\leftarrow(1, \boldsymbol{s}')\in\mathbb{Z}_q^{n+1}$。任意 $m\in\{0,1\}$，令 $\boldsymbol{A}\leftarrow$**L2.PublicKeygen**($\boldsymbol{s}$)和 $\boldsymbol{C}\leftarrow$**L2.Enc**($\boldsymbol{A}$, m)，存在 $\boldsymbol{e}'\in\mathbb{Z}_q^{(n+1)l}$ 且 $\|e'\|_\infty<kB=2nB\log q$，使得如下等式成立：

$$<\boldsymbol{C}, \boldsymbol{s}>=m\cdot\text{Powerof2}(\boldsymbol{s})+\boldsymbol{e}' \pmod q$$

证明：根据加密方案，有

$$<\boldsymbol{C}, \boldsymbol{s}>=\begin{bmatrix} m & & & & \\ 2m & & & & \\ \vdots & & & & \\ 2^{l-1}m & & & & \\ & m & & & \\ & 2m & & & \\ & \vdots & & & \\ & 2^{l-1}m & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & m \\ & & & & 2m \\ & & & & \vdots \\ & & & & 2^{l-1}m \end{bmatrix}\boldsymbol{s}+\boldsymbol{RAs} \bmod q$$

$$=m\cdot\text{Powerof2}(\boldsymbol{s})+\boldsymbol{Re} \bmod q$$

$$=m\cdot\text{Powerof2}(\boldsymbol{s})+\boldsymbol{e}' \bmod q$$