NTRU 基本加密方案

下面是一个 NTRU 基本加密方案，该方案由文章[11]提出。消息空间是$\{0,1\}$，环 $R=\mathbb{Z}[x]/\phi(x)$，其中$\phi(x)$是一个 n 次分圆多项式，即$\phi(x)=x^n+1$，n 是 2 的幂次方。所有的密文计算都是在环 R_q 上进行。错误分布χ是一个离散高斯分布$D_{\mathbb{Z}^n,r}$，其中 r 是标准偏离。从环 R 上的错误分布χ中取样，例如$e\leftarrow\chi$，则$e\in R$且是一个界为$r\sqrt{n}$的多项式。λ是安全参数，模 q 是素数。设置上述参数使得在环 LWE 上能够获得2^{λ}安全。

E.SecretKeygen(1^{λ})：选取 $f'\leftarrow\chi$，计算 $f\leftarrow 2f'+1$ 使得 $f\equiv 1 \pmod 2$。若 f 在 R_q 上是不可逆的，则重新选取 f'。令私钥 **sk**=$f\in R$。

E.PublicKeygen(sk)：选取 $g\leftarrow\chi$，计算 $h=2gf^{-1}\in R_q$，令公钥 **pk**=h。

E.Enc(pk, m**)**：消息 $m\in\{0,1\}$，选取 s，$e\leftarrow\chi$，输出密文 $c\leftarrow m+hs+2e\in R_q$。

E.Dec(sk, c**)**：输出 $m\leftarrow cf \bmod 2$。

由于上述方案在加密过程中引入了噪音，所以解密要去掉噪音，但是只有当噪音小的时候，才能正确解密。下面从加密噪音和解密噪音的角度说明方案的正确性，也便于后面对同态操作的噪音进行分析。

引理 3.1 （加密噪音）q, n, R_q, χ 是上述加密方案的参数，令χ的上界是 B。任意 $f'\leftarrow\chi$，计算 $f\leftarrow 2f'+1$ 使得 $f\equiv 1 \pmod 2$。若 f 在 R_q 上是不可逆的，则重新选取 f'。任意 $m\in\{0,1\}$。令 $h\leftarrow$**E.PublicKeygen**(f)，$c\leftarrow$**E.Enc**(h, m)，则存在 v 且$\|v\|_\infty\le 3nB^2+nB$， 使得如下等式成立：

$$cf=mf+2v \quad \in R_q\text{。}$$

其中 v 称之为密文的噪音。

证明：根据基本加密方案有：

$$cf = mf + hsf + 2ef = mf + 2gs + 2ef = mf + 2v \in R_q。$$

由于 χ 的上界是 B，所以 g, s, e 的系数上界是 B，f 的系数上界是 $2B+1$。又根据推论 可知，gs 的系数上界是 nB^2，ef 的系数上界是 $nB\cdot(2B+1)$，所以 v 的系数上界是 $3nB^2+nB$，即 $\|v\|_\infty \le 3nB^2+nB$。

上述定理给出了初始密文（新鲜密文）的噪音上界。由于密文计算过程中噪音会增长，而解密的正确性与密文中噪音大小是相关的，下面引理 3.1 给出了密文能够正确解密的噪音界，只要密文中的噪音小于该界，就可以正确解密。

引理 3.2 （解密噪音）任意 $f, c \in R_q$，且有 $f \equiv 1 (\mathrm{mod}\ 2)$。若满足：

$$cf = mf + 2v \in R_q,$$

其中 $m \in \{0,1\}$，$\|v\|_\infty < q/4$。则有：

$$\mathbf{E.Dec}(f, c) = m。$$

证明：如果 $\|v\|_\infty < q/4$，则有：

$$\mathbf{E.Dec}(f, c) = cf\ (\mathrm{mod}\ 2) = mf + 2v\ (\mathrm{mod}2) = mf\ (\mathrm{mod}2) = m。$$

上述引理也说明了在解密过程中，只要保持形如“$mf + 2v$”的结构，且 $\|v\|_\infty < q/4$，就能够正确解密。这种不变结构的思想在后面设计同态加密属性的过程中非常有用。