# NTRU Lattice

Polynomial $v(x)$ is written as follows

$$\begin{array}{c}v(x)=v\_{0}+v\_{1}x+…+v\_{n-1}x^{n-1} \end{array}\left(1\right)$$

Then, its coefficient vector is $v=[v\_{0}, v\_{1},..,v\_{n-1}]$.

We consider polynomial ring

$$R\left(x\right)=Z(x)/(X^{N}-1)$$

Let $N=3, d=1,q=41, f(x)=x^{2}-x+1\in R\left(x\right), g(x)=x^{2}-1\in R\left(x\right), f\in T\left(d+1,d\right), g\in T(d,d) $. In Maple:





























From (1)

$$\begin{array}{c}f\_{0}=1, f\_{1}=-1, f\_{2}=1, \end{array}\left(2\right)$$

$$\begin{array}{c}g\_{0}=0, g\_{1}=-1, g\_{2}=1. \end{array}\left(3\right)$$

Then inverse of $f(x)$ modulo $q$, $F\_{q}(x)= 21x+21$ is calculated using Maple:













NTRU Public key, $h(x)$, in (4) is calculated using Maple:

$$\begin{array}{c}h\left(x\right)=F\_{q}\left(x\right)∙g\left(x\right) mod x^{3}-1 mod q=20x+21,\end{array}\left(4\right)$$





From (1) and (4), we have

$$\begin{array}{c}h\_{0}=21, h\_{1}=20, h\_{2}=0 \end{array}\left(5\right)$$

From (4), $\begin{array}{c}fh mod q=g. \end{array}\left(6\right)$

$$Then,$$

$$\begin{array}{c} f(x)∙h(x)+u(x)∙q=g\left(x\right) \end{array}\left(7\right)$$

 From [1, p.426] we can express (7) as follows

$$\begin{array}{c}g\_{k}= \sum\_{i=0}^{N-1}\sum\_{j=0}^{N-1}\left(f\_{i}⋅h\_{j}\right)+u\_{k}q, where i+j=k mod N \end{array}\left(8\right)$$

From (2), (5), and (8):

$$f\_{0}⋅h\_{0}+f\_{1}⋅h\_{2}+f\_{2}⋅h\_{1}+u\_{0}⋅q=1⋅21+\left(-1\right)⋅0+1⋅20+(-1)⋅41=g\_{0}= 0$$

$$f\_{0}⋅h\_{1}+f\_{1}⋅h\_{0}+f\_{2}⋅h\_{2}+u\_{1}⋅q=1⋅20+\left(-1\right)⋅21+1⋅0+0⋅41=g\_{1}=-1$$

$$f\_{0}⋅h\_{2}+f\_{1}⋅h\_{1}+f\_{2}⋅h\_{0} +u\_{2}⋅q= 1⋅0+\left(-1\right)⋅20+1⋅21+0⋅41=g\_{2} =1 $$

We can conclude that $f\left(x\right)⋅h\left(x\right)+u(x)⋅q=g(x) $ can be expressed as

$$\begin{array}{c}\left(f,u\right)\left(\begin{matrix}H\\qE\end{matrix}\right)=\left[\begin{matrix}f\_{0}&f\_{1}&f\_{2}\end{matrix} u\_{0} u\_{1} u\_{2}\right] \left[\begin{matrix}h\_{0}&h\_{1}&h\_{2}\\h\_{2}&h\_{0}&h\_{1}\\h\_{1}&h\_{2}&h\_{0}\\q&0&0\\0&q&0\\0&0&q\end{matrix}\right]=\left[\begin{matrix}g\_{0}&g\_{1}&g\_{2}\end{matrix}\right] , \end{array}\left(9\right)$$

where E is a unity matrix, and $H= \left[\begin{matrix}h\_{0}&h\_{1}&h\_{2}\\h\_{2}&h\_{0}&h\_{1}\\h\_{1}&h\_{2}&h\_{0}\end{matrix}\right]$. In the same way, we can express
 $f(x)⋅1+u(x)⋅0=f(x)$ as

$$\begin{array}{c}\left(f,u\right)\left(\begin{matrix}E\\0\end{matrix}\right)=\left[\begin{matrix}f\_{0}&f\_{1}&f\_{2}\end{matrix} u\_{0} u\_{1} u\_{2}\right] \left[\begin{matrix}1&0&0\\0&1&0\\0&0&1\\0&0&0\\0&0&0\\0&0&0\end{matrix}\right]=\left[\begin{matrix}f\_{0}&f\_{1}&f\_{2}\end{matrix}\right] \end{array}\left(10\right)$$

From (9) and (10), we can define

$$\begin{array}{c}L\_{NTRU}=\left(\begin{matrix}E&H\\0&qE\end{matrix}\right) \end{array}$$

Hence,

$$\left(f,u\right)\*L\_{NTRU}=\left[\begin{matrix}f\_{0}&f\_{1}&f\_{2}&u\_{0}&u\_{1}&u\_{2}\end{matrix} \right]\*\left[\begin{matrix}1&0&0&h\_{0}&h\_{1}&h\_{2}\\0&1&0&h\_{2}&h\_{0}&h\_{1}\\0&0&1&h\_{1}&h\_{2}&h\_{0}\\0&0&0&q&0&0\\0&0&0&0&q&0\\0&0&0&0&0&q\end{matrix}\right]=(f, g )$$

References

[1] J. Hoffstein, J. Pipher, and J. H. Silverman, An Introduction to Mathematical Cryptography, 2nd ed. Springer Publishing Company, Incorporated, 2014.