# NTRU Lattice

Polynomial is written as follows

Then, its coefficient vector is .

We consider polynomial ring

Let . In Maple:





























From (1)

Then inverse of modulo , is calculated using Maple:













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





From (1) and (4), we have

From (4),

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

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

We can conclude that can be expressed as

where E is a unity matrix, and . In the same way, we can express  
 as

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

Hence,

References

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