**Tutorial 10: A small sample on NTRU**

SYED AHMAD HARITH IZZAT BIN SYED HUSIN AZMI

B032110070

Instruction:

Given a random private (preferable irreducible) polynomial *f*(*x*) and a random camouflage polynomial g(*x*)

1. *f*(*x*) = −*x*10 + *x*9 + *x*6 − *x*4 + *x*2 + *x* −1 = [−1,1,0,0,1,0,−1,0,1,1,−1] (mod *p*) and
2. *g*(*x*) = −*x*10 − *x*8 + *x*5 + *x*3 + *x*2 −1 = [−1,0,−1,0,0,1,0,1,1,0,−1] in little endian.
3. an inverse *fp*−1 of *f* modulo *p*
4. and an inverse *fq*−1 of *f* modulo *q* against modulo truncated polynomial N(*x*) = *xn* −1.

*fp*−1(*x*) = 2*x*9 + *x*8 + 2*x*7 + *x*5 + 2*x*4 +2*x*3 + 2*x* +1 (mod *p*) in little endian.

= [ 2, 1, 2, 0, 1, 2, 2, 0, 2, 1] mod N(*x*)

= [-1, 1,-1, 0, 1,-1,-1, 0,-1, 1] in centered lifting format

*fq*−1(*x*) = 30*x*10 + 18*x*9 + 20*x*8 + 22*x*7 + 16*x*6 +15*x*5 + 4*x*4 +16*x*3 + 6*x*2 +9*x* +5 (mod *q*)

= [30, 18, 20, 22,16,15,4,16,6,9,5] mod N(*x*)

= [-2,-14,-12,-10,16,15,4,16,6,9,5]

Given a system parameter (*n*, p, q) = (11, 3, 32).

1. Compute a public key *h* from a given private key *f* and a blinding random g.
2. Take a plintext M = 1000 + (ID mod 1000).

M = B03211007016 = 120 (mod 1000)

= 1000 + 120 = 1120

M = 10001100000

1. Convert M into binary.
2. Convert M into a polynomial in Fp.
3. Encryp the plaintext M using the same public key h(*x*).
4. Decrypt M back into original plaintext.

Q1. Compute a public key *h*.

*h*(*x*) = *p* ⋅ *fq*−1(*x*)\*g(*x*) mod *q*.

= 16*x*10 + 19*x*9 + 12*x*8 + 19*x*7 + 15*x*6 +24*x*5 + 12*x*4 +20*x*3 + 22*x*2 +25*x* +8

= [16,19,12,19,15,24,12,20,22,25,8] (mod 32)

= [16,−13,12,−13,15,−8,12,−12,−10,−7,8].

**Note:** In the future, mulplitication shall be done via convolution.

*fq*−1(*x*)\*g(*x*)

[-2,-14,-12,-10,16,15,4,16,6,9,5] \*[−1,0,−1,0,0,1,0,1,1,0,−1]

= [−1, 0,−1, 0, 0, 1, 0, 1, 1, 0,−1]\*[-2,-14,-12,-10,16,15,4,16,6,9,5]

= -1[-2,-14,-12,-10, 16, 15, 4, 16, 6, 9, 5]

-1[-2,-14,-12,-10,16, 15, 4, 16, 6, 9, 5]

+1[-2,-14,-12,-10, 16, 15, 4, 16, 6, 9, 5]

+1[-2,-14,-12,-10, 16, 15, 4,16, 6, 9, 5]

+1[-2,-14,-12,-10, 16, 15, 4,16, 6, 9, 5]

-1[-2,-14,-12,-10,16,15, 4,16, 6, 9, 5]

+2, 14, 14, 24, -4, -7,-34,-45,-36,-35,-16, 15, 54, 35,13,12,11,-2,-1,-9,-5

= +2,14,14,24,-4,-7,-34,-45,-36,-35

-16,15,54,35,13,12,11, -2, -1, -9, -5

= -16,17,68,49,37, 8, 4,-36,-46,-45,-40 mod N(x)

= 16,17, 4,17, 5, 8, 4, 28, 18, 19, 24 mod q.

*H*(*x*) *= p* ⋅ *f*q−1(*x*)\*g(*x*)

= 48 51 12 51 15 24 12 84 54 57 72

= 16 19 12 19 15 24 12 20 22 25 8 mod q;

Take M=1120, and then my plaintext in binary is

m =[1 0 0 0 1 1 0 0 0 0 0]

Take r as a random encrypt key,

r =[1,-1, 0,-1, 0,-1, 1,-1, 0, 1, 1];

Encryption Process

*e*(*x*) = r(*x*) \**h*(*x*)

e= 16 3 25 23 9 13 30 16 16 31 2 30 6 12 16 31 15 2 15 1 8

= 16 3 25 23 9 13 30 16 16 31

2 30 6 12 16 31 15 2 15 1 8

= 2 46 9 37 39 40 28 32 31 17 39

m =[1 0 0 0 1 1 0 0 0 0 0]

*e*(*x*) = r(*x*) \**h*(*x*) + *m*(*x*)

e = 3 46 9 37 40 41 28 32 31 17 39

= 3 14 9 5 8 9 28 0 31 17 7 mod 32

Decryption Process of ciphertext *e*(*x*) (mod q)

*a*(*x*)= *f*(*x*)\**e*(*x*) (modulo q).

*f*(*x*) = [−1,1,0,0,1,0,−1,0,1,1,−1]

a= -3 -11 5 4 0 13 19 -13 3 35 -14 -2 7 -3 5 2 -4 -16 -7 22 -7

a= -3 -11 5 4 0 13 19 -13 3 35

-14 -2 7 -3 5 2 -4 -16 -7 22 -7

a= -14 -5 -4 2 9 2 9 3 -20 25 28

= 18 27 28 2 9 2 9 3 12 25 28 mod 32

Center Lifting mode

a= -14 -5 -4 2 9 2 9 3 12 -7 -4

b= 1 1 2 2 0 2 0 0 0 2 2 mod 3

c(*x*) = *fp*−1(*x*)\**b*(*x*) (modulo p).

c= 0 2 0 1 2 1 2 2 0 1 1 0 1 0 0 2 2 1 1 0 2

c= 0 2 0 1 2 1 2 2 0 1

1 0 1 0 0 2 2 1 1 0 2

= 1 0 3 0 1 4 3 3 3 0 3

= 1 0 3 0 1 4 3 3 3 0 3

C= 1 0 0 0 1 1 0 0 0 0 0 (mod 3)

We indeed get our plaintext back.