Home

Questions

Tags

Users

Unanswered

NTRU and one failed example

Ask Question

2

In **NTRU** crypto system I have used these polynomials and parameters:
$N = 17, p = 7, q = 64$ and f as private key is:

$$f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}$$

So the inverse of f in ring $\mathbb{Z}[X]/(X^N - 1)$ is:

$$f_p = 3x^{16} + 3x^{15} + x^{14} + 6x^{13} + 5x^{12} + 6x^{11} + x^{10} + 2x^9 + 2x^8 + 3x^7 + 4x^4 + 3x^3 + 3x^2 + 4x + 4$$

and

$$f_q = 63x^{16} + 54x^{15} + 7x^{14} + 44x^{13} + 51x^{12} + 16x^{11} + 35x^{10} + 12x^9 + 50x^8 + 29x^7 + 11x^6 + 4x^5 + 43x^4 + 19x^3 + 44x^2 + 50x + 45$$

and choose g to construct public key such that:

$$g = -1 + x^2 + x^3 + x^5 - x^8 - x^{10}$$

then compute h as public key as follow:

$$h = pf_q \cdot g \pmod{q}$$

then:

$$h = 49x^{16} + 45x^{15} + 62x^{14} + 46x^{13} + 14x^{12} + 44x^{11} + 33x^{10} + 26x^9 + 27x^8 + 8x^7 + 21x^6 + 2x^5 + 58x^4 + 52x^3 + 45x^2 + 54x + 54$$

Choose message
$m = -x^{13} + x^{12} + x^{11} - x^{10} + x^9 + x^7 + x^6 + x^5 - x^3 - 1$
, and random polynomial
$r = x^{10} + x^8 - x^7 + x^5 - x^3 - x^2 + x - 1$
to encode the message.
As we know, $e = r \cdot h + m$, so

$$e = 18x^{16} + 37x^{15} + 23x^{14} + 14x^{13} + 17x^{12} + 6x^{11} + 6x^{10} + 25x^9 + 55x^8 + 56x^7 + 32x^6 + 45x^5 + 36x^4 + 58x^3 + 24x^2 + 32x + 30$$

But when I want to decrypt the e in **NTRU**