The NTRU Cryptosystem and Lattice-based Cryptography

Sarah Hocutt

University of Connecticut

May 13, 2023

SVP and CVP

Closest Vector Problem (CVP)

For some vector $w \in \mathbb{R}^m$ such that $w \notin L$, find a vector that is closest to w; i.e., find $v \in L$ such that the Euclidean norm $||w - v||$ is minimized.

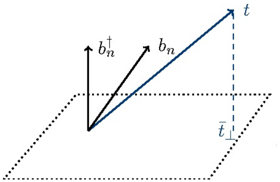

Figure: An example of the closest vector problem within a vector space

Shortest Vector Problem (SVP)

For some lattice L, find the shortest nonzero vector in L; i.e., find nonzero $v \in L$ such that the Euclidean norm $||v||$ is minimized.

General Definitions

The NTRU public key cryptosystem is primarily described as an algebraic structure over lattices [3], so we will first review some polynomial operations and ring theory:

Convolution

The **convolution product** of two vectors is defined as

$$(a_1, a_2, \ldots, a_{N-1}) * (b_1, b_2, \ldots, b_{N-1}) = (c_1, c_2, \ldots, c_{N-1}),$$

with each c_i defined by the polynomial product

$$a(x) * b(x) = c(x), \text{where}$$

$$c_i = \sum_{m+n \equiv l \mod N} a_m b_{l-m}.$$

General Definitions

Center lift

The **center lift** of a polynomial $a(x) \in R_q$ to R is the unique polynomial $a'(x) \in R$ such that

$$a'(x) \mod q = a(x),$$

where every coefficient lies in the interval

$$\frac{-q}{2} < a'_i < \frac{q}{2}.$$

i.e., the center lift lifts the coefficients of any given polynomial from a ring R modulo p to the full ring R.

Note: the sum or product of the lifts need *not* be equal to the lift of the sum or product.

Rings

Convolution Polynomial Rings

For some fixed integer $N > 0$, the ring of rank N convolution polynomials is defined by the quotient ring

$$R = \frac{\mathbb{Z}[x]}{(x^n - 1)}.$$

Taking any prime p, we can create the ring modulo p by

$$R_p = \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x^n - 1)}.$$

It is easier to do computations in the rings R and R_q than it is in more general polynomial quotient rings, because the polynomial $x^N - 1$ has such a simple form. In particular, when we mod out by $x^N - 1$, we are simply requiring x^N to equal 1.

NTRU

The general protocol of NTRU is in three steps:

Part 1: Key Creation

Alice chooses some

$$(N, d, p, q)$$

such that N is prime, $\gcd(N, q) = \gcd(p, q) = 1$, and $q > (6d + 1)p$.

Remark: The requirement of $q > (6d + 1)p$ is to guarantee decryption - otherwise, there is a slim chance that the coefficients of randomly chosen polynomials could cancel each other out.

Alice chooses two polynomials

$$f(x) \in T(d + 1, d),$$

and

$$g(x) \in T(d, d).$$

(Note that $f(x) \in T(d + 1, d)$ because elements in $T(d, d)$ do not have inverses.)

NTRU

Alice computes inverses of f:

$$F_p = f^{-1}(x) \mod p,$$

$$F_q = f^{-1}(x) \mod q.$$

Finally, she computes the convolution of F_q and $g(x)$:

$$h(x) = F_q(x) * g(x).$$

This is Alice's public key.

$$\textbf{Private key}: \ (\mathbf{f(x), F_p(x)}).$$

$$\textbf{Public key}: \ \mathbf{h(x)}.$$

NTRU

Part 2: Message Encryption Bob chooses his message, a polynomial $m(x) \in R_p$. Note that the coefficients of $m(x)$ fall within the bounds

$$\frac{-1}{2}p \leq m_i \leq \frac{1}{2}p.$$

This is to ensure that $m(x)$ is the center-lift of a polynomial in R_p. Next, Bob chooses a random $r(x) \in T(d, d)$ and creates the ciphertext:

$$c(x) \equiv ph(x) * r(x) + m(x) \mod q.$$

Lastly, Bob sends $c(x)$ to Alice.

NTRU

Part 3: Message Decryption Alice begins by convolving $c(x)$ with $f(x)$:

$$\begin{aligned} a(x) \equiv f(x) * c(x) &\equiv f(x) * [pr(x) * h(x) + m(x)] \mod q \\ &\equiv f(x) * pr(x) * (F_q * g(x)) + f(x) * m(x) \mod q \\ &\equiv pr(x) * g(x) + f(x) * m(x) \mod q. \end{aligned}$$

Alice center-lifts $a(x)$ to some element $b(x)$ within R_p; as the first term is a multiple of p, we're left with

$$b(x) = f(x) * m(x) \mod p.$$

Lastly, convolve $b(x)$ with F_p :

$$\begin{aligned} F_p * b(x) &= F_p * f(x) * m(x) \mod p \\ &= m(x) \bmod p. \end{aligned}$$

By center-lifting $m(x)$ to R, the original message $m(x)$ is easily obtainable.

NTRU Example

Part 1: Key Creation

Take $(N, p, q, d) = (7, 3, 41, 2)$. satisfying $41 = q > (6d + 1)p = 39$.
Let

$$f(x) = x^6 - x^4 + x^3 + x^2 - 1, \;\; g(x) = x^6 + x^4 - x^2 - x.$$

Find inverses of f mod p, mod q respectively:

$$F_q(x) = 8x^6 + 26x^5 + 31x^4 + 21x^3 + 40x^2 + 2x + 37 \in R_q,$$

and

$$F_p(x) = x^6 + 2x^5 + x^3 + x^2 + x + 1 \in R_p.$$

Finally, compute

$$h(x) = F_q(x) * g(x) = 20x^6 + 40x^5 + 2x^4 + 38x^3 + 8x^2 + 26x + 30 \in R_q.$$

$$\textbf{Private key}: \; (\mathbf{x^6 - x^4 + x^3 + x^2 - 1, \; x^6 + 2x^5 + x^3 + x^2 + x + 1}).$$

$$\textbf{Public key}: \; \mathbf{20x^6 + 40x^5 + 2x^4 + 38x^3 + 8x^2 + 26x + 30 \in R_q}.$$

NTRU Example

Part 2: Message Encryption
Set a message

$$m(x) = -x^5 + x^3 + x^2 - x + 1,$$

and choose a random polynomial

$$r(x) = x^6 - x^5 + x - 1.$$

Convolving $pr(x)$ with the public key, the full ciphertext will be

$$c(x) \equiv pr(x) * h(x) + m(x) = 31x^6 + 19x^5 + 4x^4 + 2x^3 + 40x^2 + 3x + 25 \pmod{q}.$$

NTRU Example

Part 3: Message Decryption

First, we convolve

$$f(x) * c(x) \equiv x^6 + 10x^5 + 33x^4 + 40x^3 + 40x^2 + x + 40 \pmod{q}.$$

By center-lifting modulo q, we bring the polynomial up to R and term it $a(x)$:

$$a(x) = x^6 + 10x^5 - 8x^4 - x^3 - x^2 + x - 1 \in R.$$

Lastly, we reduce $a(x)$ modulo p and convolve with F_p to get

$$F_p(x) * a(x) \equiv 2x^5 + x^3 + x^2 + 2x + 1 \pmod{p}.$$

This gives us $m(x) \bmod p$, which by center-lifting $m(x)$ modulo p can easily return the original $m(x)$.

NTRU Key Recovery Problem

The **NTRU Key Recovery Problem** is the core of breaking NTRU. Note that for polynomials $f(x), g(x)$ chosen by Alice, there exists the relationship

$$f(x) * h(x) = g(x),$$

where $h(x)$ is the public key. Therefore the official definition of this problem is as follows:

NTRU Key Recovery Problem

Given public key $h(x)$, find the *nonunique* ternary polynomials $f(x), g(x)$ such that

$$f(x) * h(x) = g(x).$$

Note that as decryption with $f(x)$ such that its coefficients are rotated k times, i.e. $f(x) * x^k$, yields a rotated message $x^k * m(x)$. This is why these solutions are not unique *up to rotation.*

NTRU Lattice

For some public key

$$h(x) = \sum_{i}^{N-1} h_i x^i,$$

we define the **NTRU lattice** of $h(x)$ as the lattice spanned by the matrix

$$M_{\mathbf{h}}^{\mathrm{NTRU}} = \left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right)$$

Figure: [1]

It is divided into 4 quadrants.

General Propositions on the NTRU Lattice

Now we will look at a way to estimate the shortest vector within an NTRU lattice:
With the previous identity $f(x) * h(x) \equiv g(x) \mod q$, consider $u(x)$ such that

$$f(x) * h(x) = g(x) + qu(x).$$

Then we have that for the NTRU matrix M_h^{NTRU},

$$(\mathbf{f}, -\mathbf{u})\mathbf{M_h^{NTRU}} = (\mathbf{f}, \mathbf{g}).$$

i.e. the vector (f, g) is contained within the NTRU lattice L_h^{NTRU}.

SVP in NTRU Lattice

To simplify this example, we let $(N, p, q, d) = (N, 3, 2pN, \frac{N}{3})$.

Consider the NTRU lattice L_h^{NTRU} with private key vector (f, g). Then the following properties hold:

- $det(L_h^{NTRU}) = q^N$
- $||(f, g)|| \approx \sqrt{4d} \approx \sqrt{4N/3}$
- The shortest nonzero vector in the NTRU lattice is predicted to have length

$$\sigma(L_h^{NTRU}) \approx \sqrt{Nq/\pi e} \approx 0.838N$$

Therefore when N is large, it is extremely probable that the shortest nonzero vectors within $\mathbf{L_h^{NTRU}}$ will be the rotations of $(\mathbf{f}, \mathbf{g})$.

Applications: Quantum Secure

- National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Project leading competitor Falcon is a lattice-based system designed from NTRU's lattice system [2].
- **There exists as of now no quantum algorithm that can crack either SVP or CVP that serve as the basis for lattice-based systems [3].**

Sources

Silverman, Joseph H. et al. "An Introduction to Mathematical Cryptography." Springer, 2014.

"Fast Fourier Lattice-based Compact Signatures over NTRU." Falcon. https://falcon-sign.info/

Peikert, Chris. "A Decade of Lattice Cryptography". Cryptology ePrint Archive, 2016. https://eprint.iacr.org/2015/939


"That's all Folks!"