Cutting dimensions in the LLL attack for the ETRU post-quantum cryptosystem

Augusto M. C. Silva[1]
Thiago do R. Sousa[2]
Tertuliano S. Neto[2]

[1]UFJF
[2]CEPESC

17 de setembro de 2024

Sumário

Summary

Quantum computer

- Quantum computers are now a reality
- Large-scale could break most public key cryptosystems
- Mathematical problems intractable by both quantum and conventional computers
- NIST PQ competition
- Lattice based systems

Figure: Credit: Getty Images/iStockphoto

Security of Lattice-based systems

- SVP (Shortest Vector Problem): find → given basis vectors

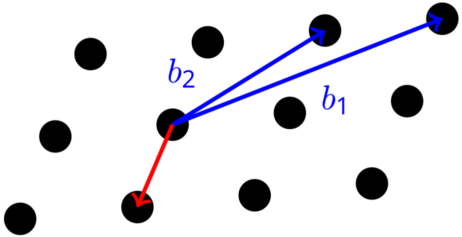

Figure: Credit: wikipedia Lattice problem

SVP problem

- Can we find an integer linear combination of lines that gives a small vector?

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 103 & 205 & 153 & 51 \\ 0 & 1 & 0 & 0 & 51 & 103 & 205 & 153 \\ 0 & 0 & 1 & 0 & 153 & 51 & 103 & 205 \\ 0 & 0 & 0 & 1 & 205 & 153 & 51 & 103 \\ 0 & 0 & 0 & 0 & 256 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 256 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 \end{bmatrix}$$

Summary

NTRU - Ingredients - Hoffstein [2016]

- Polynomials with INTEGER coefficients

$$f(x) = a_0 + a_1 x + \cdots + a_{N-1} x^{N-1}, \quad a_i \in \mathbb{Z}$$

- Modular reduction

$$a \mod b \equiv c$$

- Ring algebra for polynomial multiplication, polynomial reduction and inversion

$$R = \frac{\mathbb{Z}[x]}{(x^N - 1)}, \qquad R_p = \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x^N - 1)}, \qquad R_q = \frac{(\mathbb{Z}/q\mathbb{Z})[x]}{(x^N - 1)}$$

NTRU - Basic Example N = 4, p = 3, q = 256

- Private key

$$f(x) = -x^2 + x + 1, \quad g(x) = -x^3 - x^2 + x + 1$$

- Compute $f_q(x)$, the inverse f $\mod q$

$$f_q(x) = 103x^3 + 51x^2 - 102x - 51$$

- Public key

$$h(x) = pf_q(x) * g(x) = -103x^3 - 53x^2 + 103x + 53$$

- Encrypt message $m(x) = -x^3 + x^2 - x - 1$ using random $r(x)$:

$$c(x) = r(x) * h(x) + m(x) = 101x^3 + 56x^2 - 99x - 57$$

NTRU - Security and Attack

- Use public key $h(x) = h_0 x + h_1 x + \cdots + h_{N-1} x_{N-1}$ to create

$$H = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{N-1} \\ h_{N-1} & h_0 & h_1 & \cdots & h_{N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & h_3 & \cdots & h_0 \end{bmatrix}$$

- Use the public parameters p, q to construct a block matrix

$$L = \begin{bmatrix} I_N & p^{-1}H \\ 0 & qI_N \end{bmatrix}$$

- L generates a Lattice
- Private key pair (f, g) is a short vector

NTRU - Security and Attack

Seeing private key as short vector in Lattice

- SOLUTION: Sum lines in BLUE and subtract lines in RED

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 103 & 205 & 153 & 51 \\ 0 & 1 & 0 & 0 & 51 & 103 & 205 & 153 \\ 0 & 0 & 1 & 0 & 153 & 51 & 103 & 205 \\ 0 & 0 & 0 & 1 & 205 & 153 & 51 & 103 \\ 0 & 0 & 0 & 0 & 256 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 256 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 \\ \hline \\ 1 & 1 & -1 & 0 & 1 & 1 & -1 & -1 \end{bmatrix}$$

- Private key (f, g) is short in L.
- Approaches: Use LLL and BKZ (Basis reduction algorithms)
- Complexity: Proportional to lattice dimension $2n$

NTRU - Security and Attack

Seeing private key as short vector in Lattice

- SOLUTION: Sum lines in BLUE and subtract lines in RED

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 103 & 205 & 153 & 51 \\ 0 & 1 & 0 & 0 & 51 & 103 & 205 & 153 \\ 0 & 0 & 1 & 0 & 153 & 51 & 103 & 205 \\ 0 & 0 & 0 & 1 & 205 & 153 & 51 & 103 \\ 0 & 0 & 0 & 0 & 256 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 256 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 \\ \hdashline \\ 1 & 1 & -1 & 0 & 1 & 1 & -1 & -1 \end{bmatrix}$$

- Private key (f, g) is short in L.
- Approaches: Use LLL and BKZ (Basis reduction algorithms)
- Complexity: Proportional to lattice dimension $2n$

Find private key

- PROBLEM: Solve SVP in L:

$$L = \begin{bmatrix} I_N & p^{-1}H \\ 0 & qI_N \end{bmatrix}$$

- Find Private key (f, g) given Public key h
- Combined approach of dimension reduction May [2001] reduces complexity to

$$2n - k, \quad k \in \{1, n-1\}$$

1. APPLY THIS TO ETRU (NTRU over the Eisenstein Integers)?
2. IMPROVE ETRU PRACTICAL LATTICE ATTACK from Jarvis and Nevins [2013] ($n = 57$)?

Summary

- Recall NTRU

$$R = \frac{\mathbb{Z}[x]}{(x^N - 1)}, \qquad R_p = \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x^N - 1)}, \qquad R_q = \frac{(\mathbb{Z}/q\mathbb{Z})[x]}{(x^N - 1)}$$

- ETRU: Replace $\mathbb{Z}$ by $\mathbb{Z}[\omega]$ where $\omega^3 = 1$

$$\omega = \frac{1}{2}\left(-1 + i\sqrt{3}\right)$$

- Why: ETRU is faster and has smaller keys than NTRU (same security level)

SBSeg24 SÃO JOSÉ DOS CAMPOS

CEPESC

ETRU

Basic descryption

- ETRU is more complicated than NTRU
- Polynomials have coefficients of the form $z = a + b\omega \in \mathbb{Z}[\omega]$
- One has to work with modular algebra on the rings

$$R = \frac{\mathbb{Z}[\omega][x]}{(x^N - 1)}; \qquad R_p = \frac{\mathbb{Z}_p[\omega][x]}{(x^N - 1)}; \qquad R_q = \frac{\mathbb{Z}_q[\omega][x]}{(x^N - 1)}$$

- MAIN INGREDIENTS: Polynomial convolution, inversion module another polynomial modulo a prime in $\mathbb{Z}[\omega]$
- Given private key f, g, public key is $h(x) = pf_q(x) * g(x)$
- Encrypt a message $m(x)$ using random $r(x)$ and computing $c(x) = r(x) * h(x) + m(x)$
- We have implemented all functions in `sagemath`, available at github.

ETRU

Basic descryption

- ETRU is more complicated than NTRU
- Polynomials have coefficients of the form $z = a + b\omega \in \mathbb{Z}[\omega]$
- One has to work with modular algebra on the rings

$$R = \frac{\mathbb{Z}[\omega][x]}{(x^N - 1)}; \qquad R_p = \frac{\mathbb{Z}_p[\omega][x]}{(x^N - 1)}; \qquad R_q = \frac{\mathbb{Z}_q[\omega][x]}{(x^N - 1)}$$

- MAIN INGREDIENTS: Polynomial convolution, inversion module another polynomial modulo a prime in $\mathbb{Z}[\omega]$
- Given private key f, g, public key is $h(x) = pf_q(x) * g(x)$
- Encrypt a message $m(x)$ using random $r(x)$ and computing $c(x) = r(x) * h(x) + m(x)$
- We have implemented all functions in `sagemath`, available at github.

- ETRU Lattice

$$L_{\text{ETRU}} = \begin{bmatrix} I_{2n} & \langle H \rangle \\ 0 & \langle qI_{2n} \rangle \end{bmatrix}, \quad (1)$$

- L_{ETRU} has dimension $4n \times 4n$
- Private key (f, g) is a short vector in L_{ETRU}
- Finding f already suffices for the attack
- Attack complexity using BKZ proportional to $4n$
- Attack of Jarvis and Nevins [2013] using BKZ breaks ETRU for $n \leq 57$

SBSeg24 SÃO JOSÉ DOS CAMPOS

CEPESC

Summary

Attack idea

- IDEA: Look for $(f, g[1:k])$, which is still a short vector in

$$L_{\text{ETRU}} = \begin{bmatrix} I_{2n} & \langle H \rangle \\ 0 & \langle qI_{2n} \rangle \end{bmatrix} \quad (2)$$

- Cut some dimensions of of the right side of L_{ETRU} and solve SVP
- New lattice L'_{ETRU} can be expressed as:

$$L'_{\text{ETRU}} = \begin{bmatrix} I_{2n} & \langle H \rangle_k \\ 0 & \langle qI_{2n-k} \rangle \end{bmatrix} \quad (3)$$

- How to find a value for k ?

SBSeg24 SÃO JOSÉ DOS CAMPOS

CEPESC

Practical issues of the attack

- Problem with removing columns of L_{ETRU}
  - Loose information about private key
  - How to measure if we going to the right direction ?
  - Use norm of vectors found as a proxy ? Are we getting closer to TARGET $(f, g[1:k])$?
- So it is theoretically possible, but does it give better results ?

Results

Table: Private key attack for varying n and fixed $q = 383$. Success rate of the attack over 100 experiments.

n	41	47	57	61
Orig. Lattice Dim	164	188	228	244
BKZ block	10	10	20	20
cut k (success)	54 (6%) 50 (69%) 43 (94%) 21 (100%)	54 (3%) 50 (53%) 43 (88%) 27 (96%)	59 (1%) 50 (51%) 45 (94%)	49 (1%) 45 (7%)
JN [2013]	100%	93%	20%	0%

- Results from JN [2013] have slightly loose conditions.

SBSeg24 SÃO JOSÉ DOS CAMPOS

CEPESC

Conclusion

Security implications of the findings:

- Security of ETRU can also be lowered by using dimension reduction suggested for the original NTRU
- For cuts around the value of n the attack already has some success
- Can be used to lower attack complexity
- It should be considered when evaluating real security of ETRU

Muito obrigado!

augusto.miguel@engenharia.ufjf.br
thiagodoregosousa@gmail.com
tsouzaneto@gmail.com