

New NTRU Records with Improved Lattice Bases

PQCrypto'23

Elena Kirshanova^{1,3} Alexander May² **Julian Nowakowski**²

¹ Technology Innovation Institute, Abu Dhabi, UAE

² Ruhr-University Bochum, Bochum, Germany

³ I.Kant Baltic Federal University, Kaliningrad, Russia

<https://ia.cr/2023/582>

NTRU:

- First practical lattice-based cryptosystem.
- Most NIST PQC standards are heavily influenced by NTRU.


NTRU:


- First practical lattice-based cryptosystem.
- Most NIST PQC standards are heavily influenced by NTRU.

Progress in theoretical NTRU cryptanalysis:

- [ABD16,KF17,DvW21]: Discovery of the **overstretched** NTRU regime.

 [ABD16]: Albrecht, Bai, Ducas. A subfield lattice attack on overstretched NTRU assumptions. CRYPTO'16.

 [KF17]: Kirchner, Fouque. Revisiting Lattice Attacks on Overstretched NTRU Parameters. EUROCRYPT'17.

 [DvW21]: Ducas, van Woerden. NTRU Fatigue: How Stretched is Overstretched? ASIACRYPT'21.

NTRU:


- First practical lattice-based cryptosystem.
- Most NIST PQC standards are heavily influenced by NTRU.


Progress in theoretical NTRU cryptanalysis:


- [ABD16,KF17,DvW21]: Discovery of the **overstretched** NTRU regime.


Progress in implementation of lattice algorithms:

- [ADH+19]: G6K library, first practical implementation of **sieving** algorithms.

 [ABD16]: Albrecht, Bai, Ducas. A subfield lattice attack on overstretched NTRU assumptions. CRYPTO'16.

 [KF17]: Kirchner, Fouque. Revisiting Lattice Attacks on Overstretched NTRU Parameters. EUROCRYPT'17.

 [DvW21]: Ducas, van Woerden. NTRU Fatigue: How Stretched is Overstretched? ASIACRYPT'21.

 [ADH+19]: Albrecht, Ducas, Herold, Kirshanova, Postlethwaite, Stevens. The General Sieve Kernel and New Records in Lattice Reduction. EUROCRYPT'19.

NTRU:

- First practical lattice-based cryptosystem.
- Most NIST PQC standards are heavily influenced by NTRU.


Progress in theoretical NTRU cryptanalysis:


- [ABD16,KF17,DvW21]: Discovery of the **overstretched** NTRU regime.


Progress in implementation of lattice algorithms:

- [ADH+19]: G6K library, first practical implementation of **sieving** algorithms.


 [ABD16]: Albrecht, Bai, Ducas. A subfield lattice attack on overstretched NTRU assumptions. CRYPTO'16.

 [KF17]: Kirchner, Fouque. Revisiting Lattice Attacks on Overstretched NTRU Parameters. EUROCRYPT'17.

 [DvW21]: Ducas, van Woerden. NTRU Fatigue: How Stretched is Overstretched? ASIACRYPT'21.

 [ADH+19]: Albrecht, Ducas, Herold, Kirshanova, Postlethwaite, Stevens. The General Sieve Kernel and New Records in Lattice Reduction. EUROCRYPT'19.

Our work:

- Open source G6K-based Python implementation for attacking NTRU.
- New record computations. (For both overstretched and non-overstretched NTRU.)
- New lattice bases, that significantly improve the performance of attacks.  Topic of this talk.

The NTRU Problem

Parameters:

- $n, q \in \mathbb{N}$,
- $\Phi \in \mathbb{Z}[X]$, $\deg \Phi = n$,
- ring $R := \mathbb{Z}[X]/(\Phi)$,
- length bound $\sigma > 0$.

The NTRU Problem

Parameters:

- $n, q \in \mathbb{N}$,
- $\Phi \in \mathbb{Z}[X]$, $\deg \Phi = n$,
- ring $R := \mathbb{Z}[X]/(\Phi)$,
- length bound $\sigma > 0$.

NTRU Problem

Given:

- $h \in R$.

Find:

- $f, g \in R \setminus \{0\}$, such that
 1. $g \equiv fh \pmod{q}$,
 2. $\|f\|, \|g\| \leq \sigma\sqrt{n}$.

$$\| \sum_i a_i X^i \| := \sqrt{\sum_i a_i^2}.$$

The NTRU Problem

Parameters:

- $n, q \in \mathbb{N}$,
- $\Phi \in \mathbb{Z}[X]$, $\deg \Phi = n$,
- ring $R := \mathbb{Z}[X]/(\Phi)$,
- length bound $\sigma > 0$.

NTRU Problem

Given:

- $h \in R$.

Find:

- $f, g \in R \setminus \{0\}$, such that
 1. $g \equiv fh \pmod{q}$,
 2. $\|f\|, \|g\| \leq \sigma\sqrt{n}$.

$$\| \sum_i a_i X^i \| := \sqrt{\sum_i a_i^2}$$

NTRU as a Lattice Problem [CS'97]:

- Identify ring elements $a \in R$ with their coefficient vectors

$$a_0 + \dots + a_{n-1}X^{n-1} \simeq (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n.$$

- Gives rise to a lattice:

$$\mathcal{L} = \left\{ (g, f) \in R^2 \mid g \equiv fh \pmod{q} \right\} \subseteq \mathbb{Z}^{2n}.$$

The NTRU Problem

Parameters:

- $n, q \in \mathbb{N}$,
- $\Phi \in \mathbb{Z}[X]$, $\deg \Phi = n$,
- ring $R := \mathbb{Z}[X]/(\Phi)$,
- length bound $\sigma > 0$.

NTRU Problem

Given:

- $h \in R$.

Find:

- $f, g \in R \setminus \{0\}$, such that
 1. $g \equiv fh \pmod{q}$,
 2. $\|f\|, \|g\| \leq \sigma\sqrt{n}$.

$$\| \sum_i a_i X^i \| := \sqrt{\sum_i a_i^2}$$

NTRU as a Lattice Problem [CS'97]:

- Identify ring elements $a \in R$ with their coefficient vectors

$$a_0 + \dots + a_{n-1}X^{n-1} \simeq (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n.$$

- Gives rise to a lattice:

$$\mathcal{L} = \{ (g, f) \in R^2 \mid g \equiv fh \pmod{q} \} \subseteq \mathbb{Z}^{2n}.$$

Attack strategy:

- Run BKZ lattice reduction algorithm on \mathcal{L} to obtain $\mathbf{v} \in \mathcal{L}$ with $\|\mathbf{v}\| \leq \sigma\sqrt{2n}$.

The NTRU Problem

Parameters:

- $n, q \in \mathbb{N}$,
- $\Phi \in \mathbb{Z}[X]$, $\deg \Phi = n$,
- ring $R := \mathbb{Z}[X]/(\Phi)$,
- length bound $\sigma > 0$.

NTRU Problem

Given:

- $h \in R$.

Find:

- $f, g \in R \setminus \{0\}$, such that
 1. $g \equiv fh \pmod{q}$,
 2. $\|f\|, \|g\| \leq \sigma\sqrt{n}$.

$$\| \sum_i a_i X^i \| := \sqrt{\sum_i a_i^2}$$

NTRU as a Lattice Problem [CS'97]:

- Identify ring elements $a \in R$ with their coefficient vectors

$$a_0 + \dots + a_{n-1}X^{n-1} \simeq (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n.$$

- Gives rise to a lattice:

$$\mathcal{L} = \{ (g, f) \in R^2 \mid g \equiv fh \pmod{q} \} \subseteq \mathbb{Z}^{2n}.$$

Attack strategy:

- Run BKZ lattice reduction algorithm on \mathcal{L} to obtain $\mathbf{v} \in \mathcal{L}$ with $\|\mathbf{v}\| \leq \sigma\sqrt{2n}$.
- Complexity **mainly** depends on:
 1. the lattice dimension $d = 2n$,
 2. the lattice gap

$$\frac{\|\mathbf{v}\|}{\sqrt{d}(\det \mathcal{L})^{1/d}} \leq \frac{\sigma}{\sqrt{q}}.$$

How to Decrease the Lattice Dimension

- Typical NTRU ring: $R = \mathbb{Z}[X]/(X^n - 1)$.
- $X^n - 1 = \underbrace{(X - 1)}_{=:\Phi_1} \underbrace{(X^{n-1} + X^{n-2} + \dots + 1)}_{=:\Phi_n}$.

How to Decrease the Lattice Dimension

- Typical NTRU ring: $R = \mathbb{Z}[X]/(X^n - 1)$.
- $X^n - 1 = \underbrace{(X - 1)}_{=:\Phi_1} \underbrace{(X^{n-1} + X^{n-2} + \dots + 1)}_{=:\Phi_n}$.

Chinese Remainder Theorem

If

$$g \equiv fh \pmod{(q, X^n - 1)},$$

then

$$g \equiv fh \pmod{(q, \Phi_1)},$$

$$g \equiv fh \pmod{(q, \Phi_n)}.$$

How to Decrease the Lattice Dimension

- Typical NTRU ring: $R = \mathbb{Z}[X]/(X^n - 1)$.
- $X^n - 1 = \underbrace{(X - 1)}_{=:\Phi_1} \underbrace{(X^{n-1} + X^{n-2} + \dots + 1)}_{=:\Phi_n}$.

Chinese Remainder Theorem

If

$$g \equiv fh \pmod{(q, X^n - 1)},$$

then

$$g \equiv fh \pmod{(q, \Phi_1)},$$

$$g \equiv fh \pmod{(q, \Phi_n)}.$$

Idea:

- Solve the induced NTRU problem over $\mathbb{Z}[X]/(\Phi_1)$ or $\mathbb{Z}[X]/(\Phi_n)$.
- Lift to solution over $\mathbb{Z}[X]/(X^n - 1)$.

How to Decrease the Lattice Dimension

- Typical NTRU ring: $R = \mathbb{Z}[X]/(X^n - 1)$.
- $X^n - 1 = \underbrace{(X - 1)}_{=: \Phi_1} \underbrace{(X^{n-1} + X^{n-2} + \dots + 1)}_{=: \Phi_n}$.

Chinese Remainder Theorem

If

$$g \equiv fh \pmod{(q, X^n - 1)},$$

then

$$g \equiv fh \pmod{(q, \Phi_1)},$$

$$g \equiv fh \pmod{(q, \Phi_n)}.$$

Idea:

- Solve the induced NTRU problem over $\mathbb{Z}[X]/(\Phi_1)$ or $\mathbb{Z}[X]/(\Phi_n)$.
- Lift to solution over $\mathbb{Z}[X]/(X^n - 1)$.

| | Mod Φ_1 | Mod Φ_n |
|---------|--------------|--------------|
| Solving | Easy | ??? |
| Lifting | Difficult | Easy |

How to Decrease the Lattice Dimension

- Typical NTRU ring: $R = \mathbb{Z}[X]/(X^n - 1)$.
- $X^n - 1 = \underbrace{(X - 1)}_{=: \Phi_1} \underbrace{(X^{n-1} + X^{n-2} + \dots + 1)}_{=: \Phi_n}$.

Chinese Remainder Theorem

If

$$g \equiv fh \pmod{(q, X^n - 1)},$$

then

$$g \equiv fh \pmod{(q, \Phi_1)},$$

$$g \equiv fh \pmod{(q, \Phi_n)}.$$

Idea:

- Solve the induced NTRU problem over $\mathbb{Z}[X]/(\Phi_1)$ or $\mathbb{Z}[X]/(\Phi_n)$.
- Lift to solution over $\mathbb{Z}[X]/(X^n - 1)$.

| | Mod Φ_1 | Mod Φ_n |
|---------|--------------|--------------|
| Solving | Easy | ??? |
| Lifting | Difficult | Easy |

Is solving mod Φ_n easier than mod $X^n - 1$?

- Intuitively, yes:
 1. Lattice dimension decreases by 2.
 2. Lattice gap does not change.
- [DDGR20] estimator disagrees.

How to Not Improve the Attack

NTRU with $X^n - 1$:

- For every $i \in \mathbb{N}$, we have

$$\|X^i \cdot g\| = \|g\| \text{ and } \|X^i \cdot f\| = \|f\|.$$

$$\Leftrightarrow X^n \equiv 1 \pmod{(X^n - 1)}.$$

How to Not Improve the Attack

NTRU with $X^n - 1$:

- For every $i \in \mathbb{N}$, we have

$$\|X^i \cdot g\| = \|g\| \text{ and } \|X^i \cdot f\| = \|f\|.$$

$$\mathbb{F}[X] \quad X^n \equiv 1 \pmod{X^n - 1}.$$

- The NTRU problem has n solutions

$$X^i \cdot g \equiv (X^i \cdot f) \cdot h \pmod{(q, X^n - 1)},$$

where $i = 0, \dots, n - 1$.

How to Not Improve the Attack

NTRU with $X^n - 1$:

- For every $i \in \mathbb{N}$, we have

$$\|X^i \cdot g\| = \|g\| \text{ and } \|X^i \cdot f\| = \|f\|.$$

$$\mathbb{F}_q[X^n] \equiv 1 \pmod{(X^n - 1)}.$$

- The NTRU problem has n solutions

$$X^i \cdot g \equiv (X^i \cdot f) \cdot h \pmod{(q, X^n - 1)},$$

where $i = 0, \dots, n - 1$.

[DDGR20]

Presence of many solutions increases success probability of BKZ.

How to Not Improve the Attack

NTRU with $X^n - 1$:

- For every $i \in \mathbb{N}$, we have

$$\|X^i \cdot g\| = \|g\| \text{ and } \|X^i \cdot f\| = \|f\|.$$

$$\mathbb{F}_q[X^n] \equiv 1 \pmod{(X^n - 1)}.$$


- The NTRU problem has n solutions

$$X^i \cdot g \equiv (X^i \cdot f) \cdot h \pmod{(q, X^n - 1)},$$

where $i = 0, \dots, n - 1$.

[DDGR20]

Presence of many solutions increases success probability of BKZ.

 [DDGR'20]: Dachman-Soled, Ducas, Gong, Rossi. LWE with Side Information: Attacks and Concrete Security Estimation. CRYPTO'20.

NTRU with $\Phi_n = X^{n-1} + X^{n-2} + \dots + X + 1$:

How to Not Improve the Attack

NTRU with $X^n - 1$:

- For every $i \in \mathbb{N}$, we have

$$\|X^i \cdot g\| = \|g\| \text{ and } \|X^i \cdot f\| = \|f\|.$$

$$\mathbb{F}_q[X^n] \equiv 1 \pmod{X^n - 1}.$$


- The NTRU problem has n solutions

$$X^i \cdot g \equiv (X^i \cdot f) \cdot h \pmod{(q, X^n - 1)},$$

where $i = 0, \dots, n - 1$.

[DDGR20]

Presence of many solutions increases success probability of BKZ.

 [DDGR'20]: Dachman-Soled, Ducas, Gong, Rossi. LWE with Side Information: Attacks and Concrete Security Estimation. CRYPTO'20.

NTRU with $\Phi_n = X^{n-1} + X^{n-2} + \dots + X + 1$:

- For $n = 5$ and $f = 1 + X + X^2 - X^3$, we have

$$X \cdot f \pmod{\Phi_n} = 2X^3 + 2X^2 + 2X + 1.$$

- $\|f\| = \sqrt{4} = 2$, but $\|X \cdot f\| = \sqrt{13} \approx 3.6$.

How to Not Improve the Attack

NTRU with $X^n - 1$:

- For every $i \in \mathbb{N}$, we have

$$\|X^i \cdot g\| = \|g\| \text{ and } \|X^i \cdot f\| = \|f\|.$$

$$\mathbb{F}_q[X^n] \equiv 1 \pmod{X^n - 1}.$$


- The NTRU problem has n solutions

$$X^i \cdot g \equiv (X^i \cdot f) \cdot h \pmod{(q, X^n - 1)},$$

where $i = 0, \dots, n - 1$.

[DDGR20]

Presence of many solutions increases success probability of BKZ.

 [DDGR'20]: Dachman-Soled, Ducas, Gong, Rossi. LWE with Side Information: Attacks and Concrete Security Estimation. CRYPTO'20.

NTRU with $\Phi_n = X^{n-1} + X^{n-2} + \dots + X + 1$:

- For $n = 5$ and $f = 1 + X + X^2 - X^3$, we have

$$X \cdot f \pmod{\Phi_n} = 2X^3 + 2X^2 + 2X + 1.$$

- $\|f\| = \sqrt{4} = 2$, but $\|X \cdot f\| = \sqrt{13} \approx 3.6$.
- **By changing the ring, we lose solutions.**

How to Not Improve the Attack

NTRU with $X^n - 1$:

- For every $i \in \mathbb{N}$, we have

$$\|X^i \cdot g\| = \|g\| \text{ and } \|X^i \cdot f\| = \|f\|.$$

$$\mathbb{F}_q[X^n] \equiv 1 \pmod{(X^n - 1)}.$$


- The NTRU problem has n solutions

$$X^i \cdot g \equiv (X^i \cdot f) \cdot h \pmod{(q, X^n - 1)},$$

where $i = 0, \dots, n - 1$.

[DDGR20]

Presence of many solutions increases success probability of BKZ.

 [DDGR'20]: Dachman-Soled, Ducas, Gong, Rossi. LWE with Side Information: Attacks and Concrete Security Estimation. CRYPTO'20.

NTRU with $\Phi_n = X^{n-1} + X^{n-2} + \dots + X + 1$:

- For $n = 5$ and $f = 1 + X + X^2 - X^3$, we have

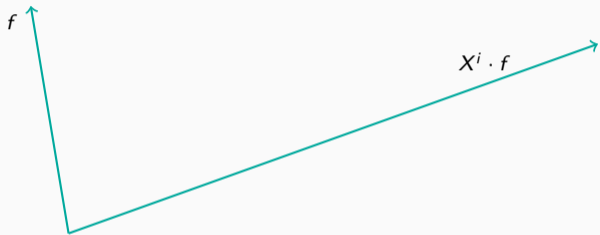
$$X \cdot f \pmod{\Phi_n} = 2X^3 + 2X^2 + 2X + 1.$$

- $\|f\| = \sqrt{4} = 2$, but $\|X \cdot f\| = \sqrt{13} \approx 3.6$.
- **By changing the ring, we lose solutions.**

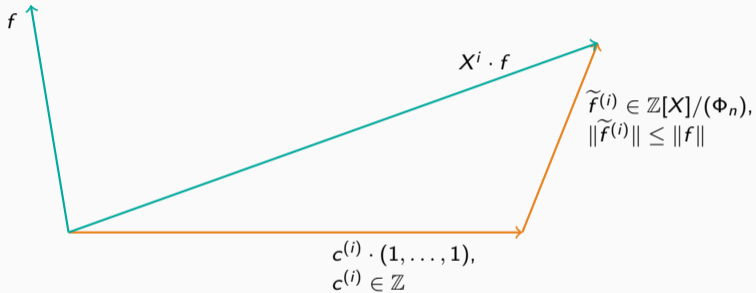
[DDGR20]

Benefits of decreasing lattice dimension are outweighed by decrease in success probability.

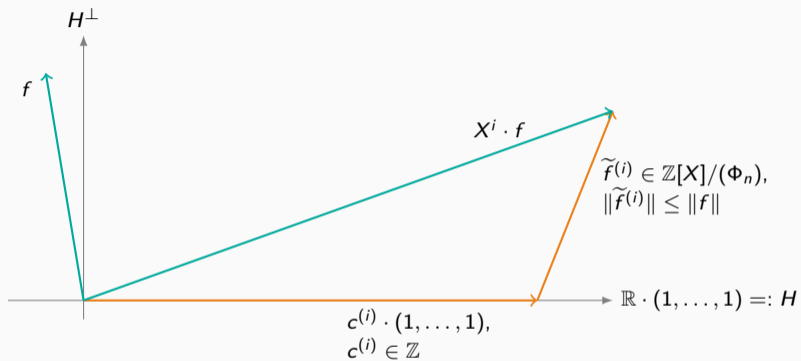
The Geometry of $\mathbb{Z}[X]/(\Phi_n)$



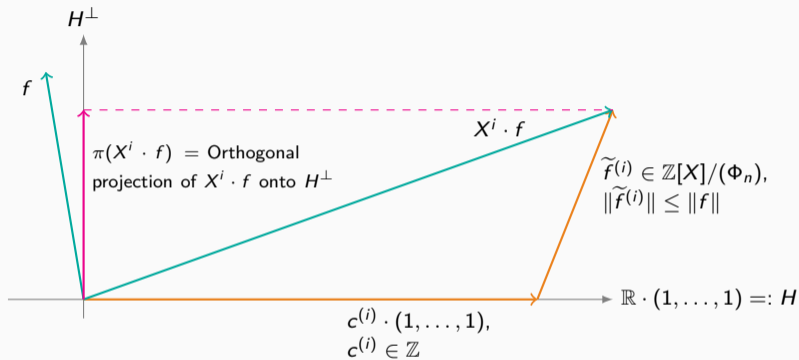
The Geometry of $\mathbb{Z}[X]/(\Phi_n)$



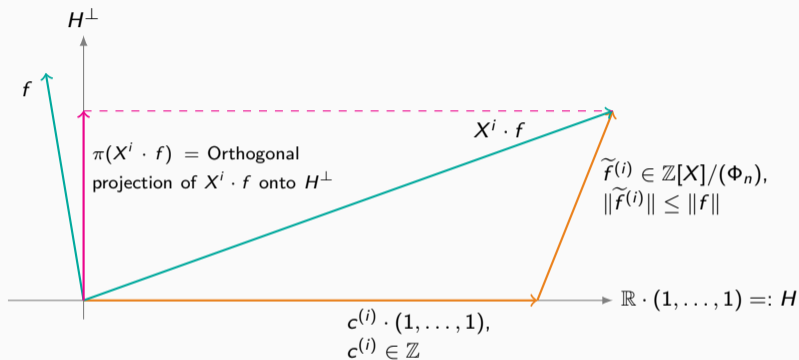
The Geometry of $\mathbb{Z}[X]/(\Phi_n)$



The Geometry of $\mathbb{Z}[X]/(\Phi_n)$



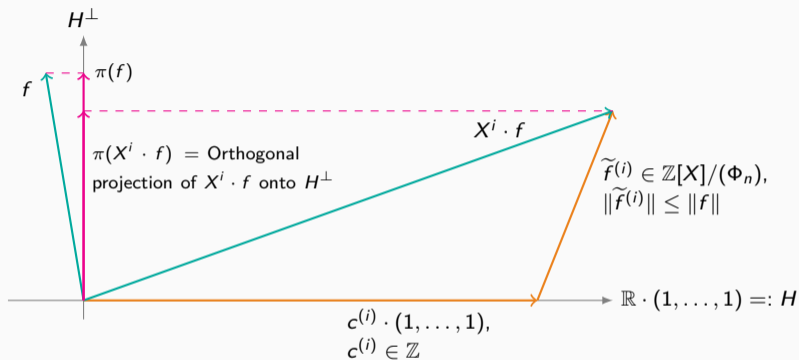
The Geometry of $\mathbb{Z}[X]/(\Phi_n)$



Projecting keeps solutions small

$\|\pi(X^i \cdot f)\| \leq \|\tilde{f}^{(i)}\| \leq \|f\|$ for every $i \in \mathbb{N}$.

The Geometry of $\mathbb{Z}[X]/(\Phi_n)$



Projecting keeps solutions small

$\|\pi(X^i \cdot f)\| \leq \|\tilde{f}^{(i)}\| \leq \|f\|$ for every $i \in \mathbb{N}$.

Four Dimensions for Free

$$\{(g, f) \mid g \equiv fh \pmod{(q, X^n - 1)}\}$$

Change ring.

Decrease dimension by 2.
Increase length of $(X^i \cdot f, X^i \cdot g)$.

$$\{(g, f) \mid g \equiv fh \pmod{(q, \Phi_n)}\}$$

Project f -part.

Decrease length of $X^i \cdot f$.
Decrease dimension by 1.

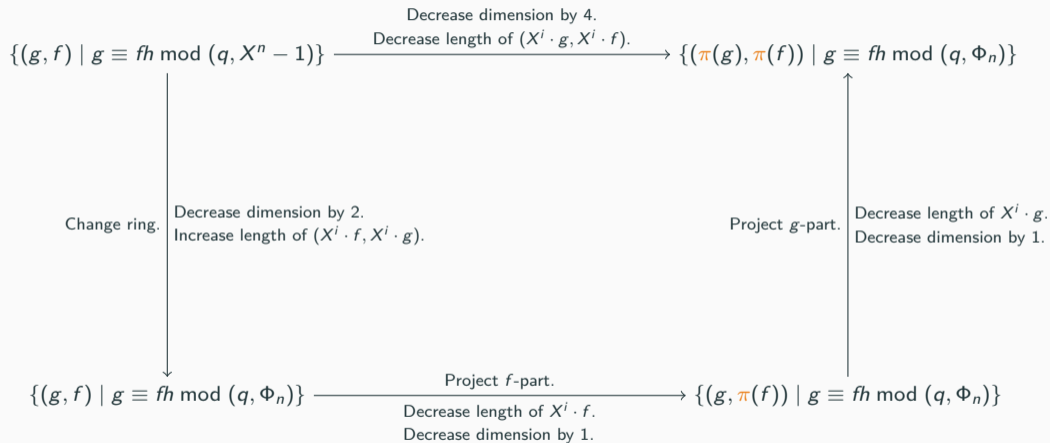
$$\{(\pi(g), \pi(f)) \mid g \equiv fh \pmod{(q, \Phi_n)}\}$$

Project g -part.

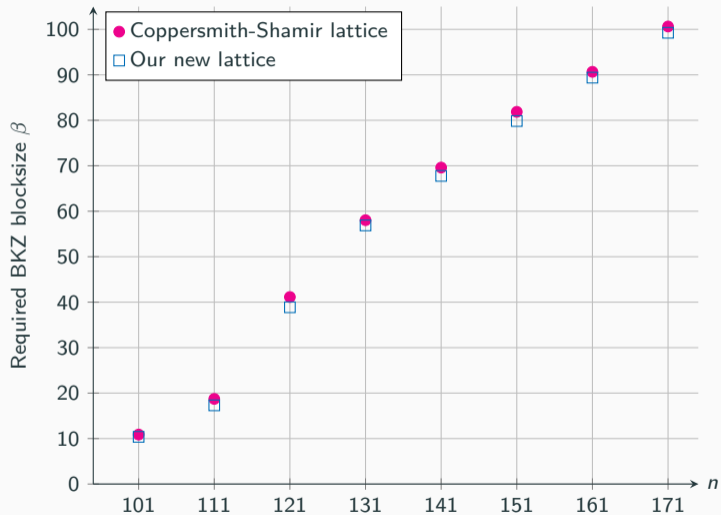
Decrease length of $X^i \cdot g$.
Decrease dimension by 1.

$$\{(g, \pi(f)) \mid g \equiv fh \pmod{(q, \Phi_n)}\}$$

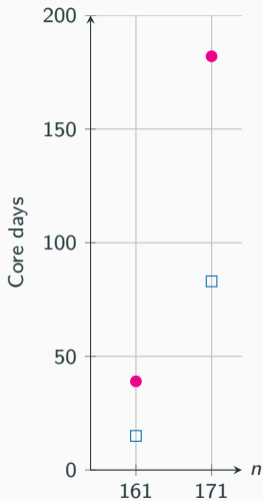
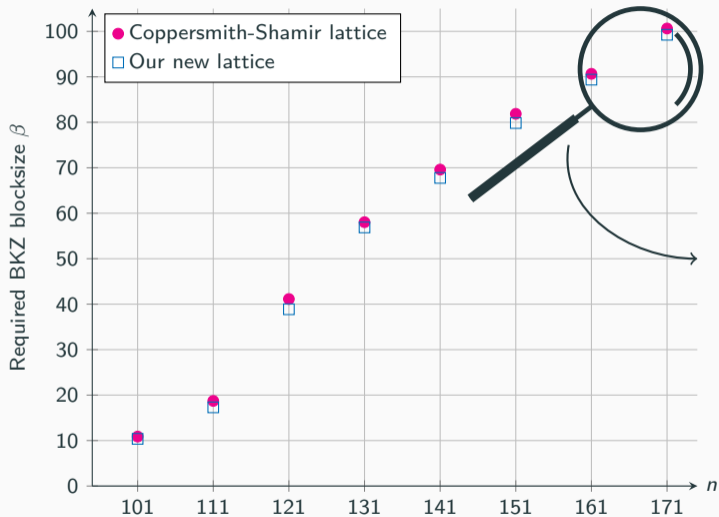
Four Dimensions for Free



Experimental Results for NTRU-HPS with $q = 512$



Experimental Results for NTRU-HPS with $q = 512$



Takeaways:

- Choosing $R = \mathbb{Z}[X]/(X^n - 1)$ in NTRU allows to decrease the lattice dimension by 4.
- No asymptotic improvements.
- But huge gain in practical runtime.

Takeaways:

- Choosing $R = \mathbb{Z}[X]/(X^n - 1)$ in NTRU allows to decrease the lattice dimension by 4.
- No asymptotic improvements.
- But huge gain in practical runtime.

- Attack not applicable to FALCON, which uses irreducible $X^n + 1$ with $n = 2^k$.

Takeaways:

- Choosing $R = \mathbb{Z}[X]/(X^n - 1)$ in NTRU allows to decrease the lattice dimension by 4.
- No asymptotic improvements.
- But huge gain in practical runtime.

- Attack not applicable to `FALCON`, which uses irreducible $X^n + 1$ with $n = 2^k$.

More in the paper:

- Open source implementation for attacking NTRU with sieving.
- New record computations.
- Attacks on overstretched NTRU-HRSS, up to $n = 211$ with BKZ blocksize $\beta = 93$.
- Record computation for Security Innovations, Inc. NTRU challenges with $n = 181$ and $\beta = 109$. (≈ 20 core years.)

- Paper: <https://ia.cr/2023/582>
- Code: https://github.com/ElenaKirshanova/ntru_with_sieving

Takeaways:

- Choosing $R = \mathbb{Z}[X]/(X^n - 1)$ in NTRU allows to decrease the lattice dimension by 4.
- No asymptotic improvements.
- But huge gain in practical runtime.

- Attack not applicable to FALCON, which uses irreducible $X^n + 1$ with $n = 2^k$.

More in the paper:

- Open source implementation for attacking NTRU with sieving.
- New record computations.
- Attacks on overstretched NTRU-HRSS, up to $n = 211$ with BKZ blocksize $\beta = 93$.
- Record computation for Security Innovations, Inc. NTRU challenges with $n = 181$ and $\beta = 109$. (≈ 20 core years.)

- Paper: <https://ia.cr/2023/582>
- Code: https://github.com/ElenaKirshanova/ntru_with_sieving

Want to do your own record computations?

- <https://bochum-challeng.es>