NTRU Fatigue: How Stretched is Overstretched?

Léo Ducas, **Wessel van Woerden** (CWI).

CWI

Centrum Wiskunde & Informatica

Overview

- NTRU is a lattice based Public Key Cryptosystem.
- Many variants exist, NIST PQC finalist 'NTRU'.
- Lattice reduction attacks were thought to behave similar as on (ring-)LWE.
- For large (overstretched) moduli q lattice reduction behaves even better [KF17].
- **When do we go from 'understretched' to 'overstretched?'**

Contributions

Explanation

We explain how lattice reduction breaks overstretched NTRU.

Concrete Predictions

We predict precisely when lattice reduction breaks overstretched NTRU.

NTRU Problem

- Secret key: small elements $f, g \in R$.
- Public key: $h := g \cdot f^{-1} \bmod q$ for some modulus q.
- For example $R = \mathbb{Z}[x]/(x^n - 1)$, $f_i, g_i \in \{-1, 0, 1\}$.

Definition (NTRU problem)

Given the public key h, recover (a rotation of) the secret key $(x^i \cdot f, x^i \cdot g)$.

Alternative

Given the public key h, find any 'short' pair $(a, b) \in R^2$ such that $h \cdot a = b \bmod q$.

NTRU Lattice

Definition (NTRU Lattice)

$$\mathcal{L}^{h,q} := \{(a, b) \in R^2 : h \cdot a = b \bmod q\}$$

- Dimension $d = 2n$, $\det(\mathcal{L}^{h,q}) = q^n$.

1. Short vector(s)

The rotations $(x^i \cdot f, x^i \cdot g)$ are unusually short vectors in $\mathcal{L}^{h,q}$.

2. Dense sublattice

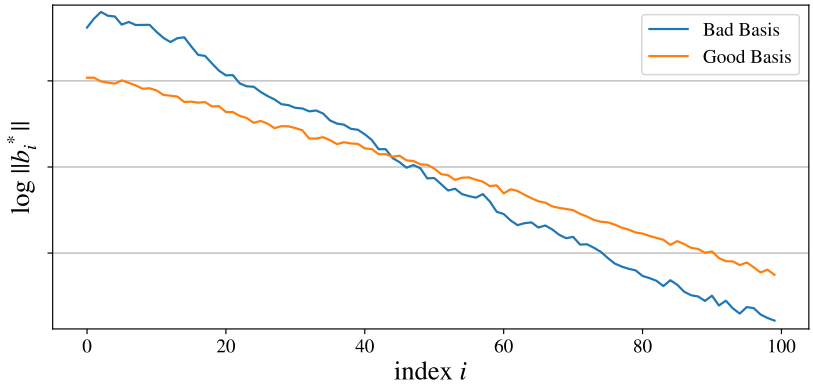
The rotations $(x^i \cdot f, x^i \cdot g)$ generate an unusually dense sublattice $\mathcal{L}^{f,g} \subset \mathcal{L}^{h,q}$.

1. Best attack for small moduli q [ADPS16, AGVW17, DDGR20, PV21].
2. Best attack for large (overstretched) moduli q [ABD16, CJL16, KF17].

What is the crossover (fatigue) point?

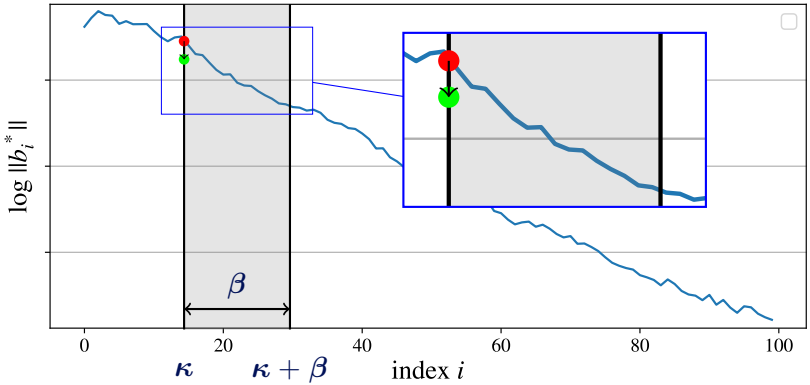
Lattice Reduction

- Let $\boldsymbol{B} = (\boldsymbol{b_0}, \ldots, \boldsymbol{b_{d-1}})$ be a lattice basis, and let $\boldsymbol{\pi_i}$ be the orthogonal projection away from $\boldsymbol{b_0}, \ldots, \boldsymbol{b_{i-1}}$.
- Gram-Schmidt basis: $\boldsymbol{b_i^*} := \boldsymbol{\pi_i}(\boldsymbol{b_i})$.
- Invariant: $\prod_i \|\boldsymbol{b_i^*}\| = \det(\boldsymbol{\mathcal{L}})$.



BKZ algorithm

- We define the projected sublattice basis $\boldsymbol{B}_{l:r} := (\pi_l(\boldsymbol{b}_l), \ldots, \pi_l(\boldsymbol{b}_{r-1}))$.
- For $\kappa = 0, \ldots, d-1$ find a shortest vector in $\mathcal{L}(\boldsymbol{B}_{\kappa:\min\{d,\kappa+\beta\}})$ and replace $\boldsymbol{b}_\kappa$.



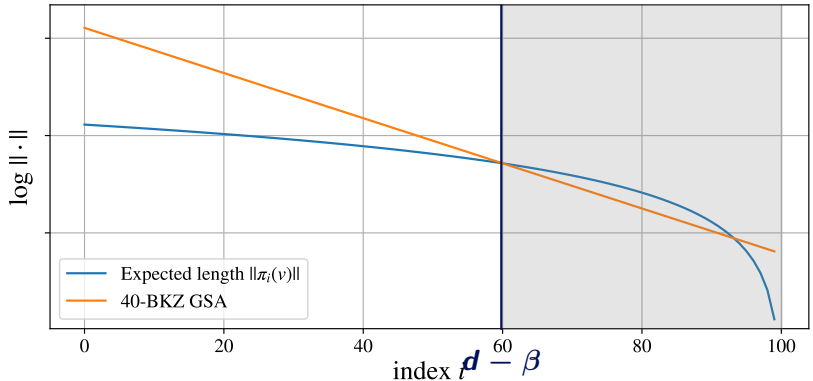
- Reduction better for larger blocksize β, but cost $\exp(\boldsymbol{O}(\beta))$.
- Behaviour well understood for 'random' lattices. [GSA]

Attack 1. Unusually short vector

Short vector

For which blocksize β does BKZ find an unusually short vector $\boldsymbol{v}$?

- BKZ is expected to find $\boldsymbol{\pi_{d-\beta}(v)}$ when $\|\boldsymbol{\pi_{d-\beta}(v)}\| < \|\boldsymbol{b^*_{d-\beta}}\|$.
- The projection $\boldsymbol{\pi_{d-\beta}(v)}$ has expected length $\sqrt{\frac{\beta}{d}} \cdot \|\boldsymbol{v}\|$.

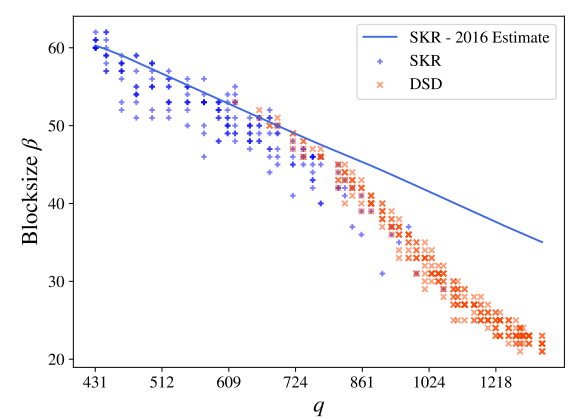


Attack 1. Estimates

GSA Intersect Method [ADPS16] - Prediction

BKZ finds the unusually shortest vector when $\beta \geq \tilde{\Theta}(n/\log q)$.

- Concrete improvements [AGVW17, DDGR20, PV21]



Attack 2. Dense sublattice

Short vector

For which blocksize β must BKZ have found a dense n-dimensional sublattice $\mathcal{D} \subset \mathcal{L}$?

Lemma (Pataki-Tural)

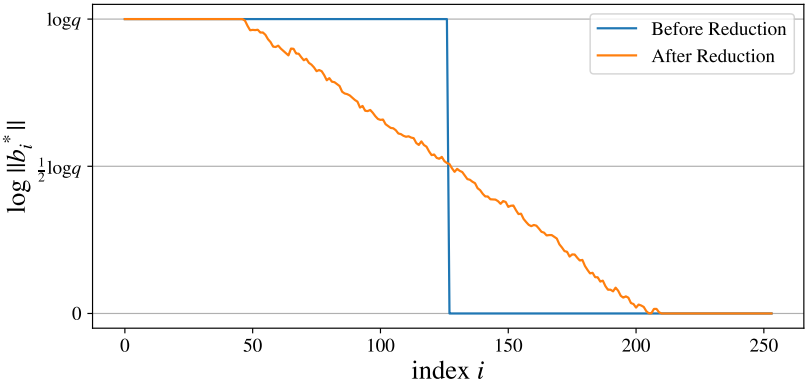
For any n-dimensional sublattice $\mathcal{D} \subset \mathcal{L}$ we have

$$\det(\mathcal{D}) \geq \min_{J} \prod_{j \in J} \|b_j^*\|,$$

where J ranges over the n-size subsets of $\{0, \ldots, d-1\}$.

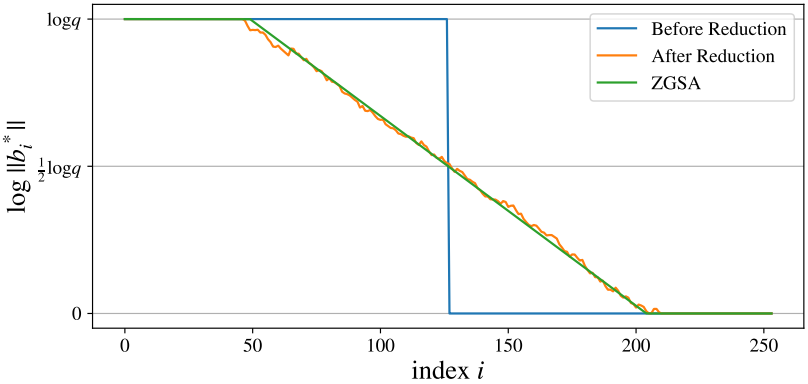
Attack 2. Z-shape

- For $\mathcal{L}^{h,q} = \{(a, b) \in R^2 : h \cdot a = b \bmod q\}$ we know the public basis: $(0, q), (0, qx), \ldots, (0, qx^{n-1}), (1, h), (x, hx), \ldots, (x^{n-1}, hx^{n-1})$.



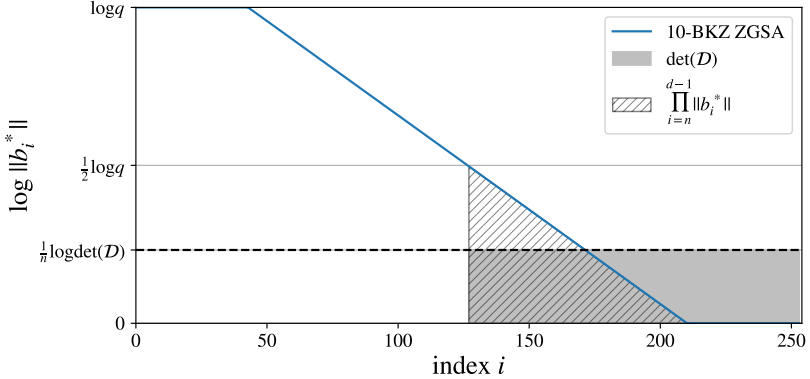
Attack 2. Z-shape

- For $\mathcal{L}^{h,q} = \{(a, b) \in R^2 : h \cdot a = b \bmod q\}$ we know the public basis: $(0, q), (0, qx), \ldots, (0, qx^{n-1}), (1, h), (x, hx), \ldots, (x^{n-1}, hx^{n-1})$.



Lemma (Pataki-Tural Simplified)

$$\det(\mathcal{D}) \geq \prod_{j=d-n}^{d-1} \|b_j^*\|,$$



Attack 2. Analysis

DSD-PT Estimate [KF17] - Prediction

BKZ finds a dense sublattice vector when $\beta \geq \Theta(n/\log^2 q)$.

- Breaks several FHE schemes with very large q.
- For $f, g \in \{-1, 0, 1\}^n$ the fatigue point lies at $q \leq n^{2.783+o(1)}$.

No explanation

How does BKZ actually find the dense sublattice?

Upper bound

Only gives an upper bound on the fatigue point.

No concrete predictions

The PT Lemma is a worst-case statement, far from practical average-case behaviour.

What happens in Practice?

Definition (Secret Key Recovery (SKR_κ))

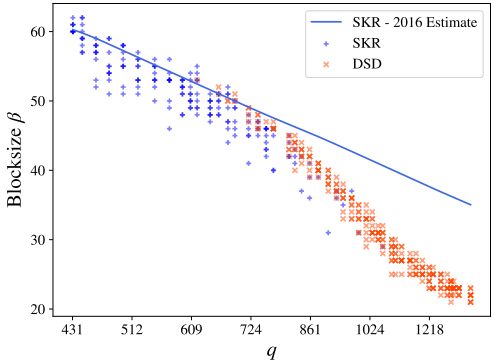
A vector as short as a secret key vector is inserted in the basis at any position κ.

Definition (Dense Sublattice Discovery (DSD_κ))

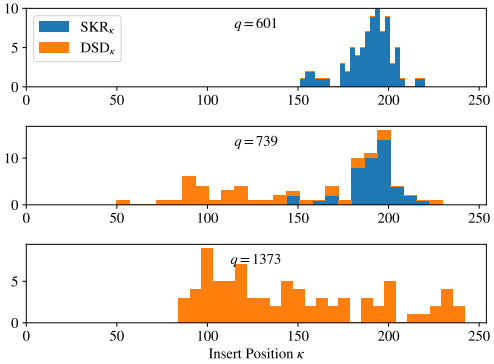
A dense sublattice vector from $\mathcal{L}^{f,g}$ longer than $\|(f|g)\|$ is inserted in the basis...

What happens in Practice?

SKR vs DSD



Blocksize (β) vs modulus ($\boldsymbol{q}$)



Insert Position ($\boldsymbol{\kappa}$)

DSD Estimate

- If β-BKZ finds a dense sublattice vector $\boldsymbol{v} \in \mathcal{L}^{f,g}$ at position κ, then $\boldsymbol{v} \in \mathcal{L}^{h,q}_{0:\kappa+\beta}$.
- Assume that $\boldsymbol{v}$ is a shortest vector in $\mathcal{L}^{h,q}_{0:\kappa+\beta} \cap \mathcal{L}^{f,g}$.

DSD-PT estimate [Our Work]

β-BKZ triggers the DSD_κ event if

$$\pi_\kappa(\boldsymbol{v}) < \left\|\boldsymbol{b}^*_\kappa\right\|,$$

where $\boldsymbol{v}$ is a shortest vector of $\mathcal{L}^{h,q}_{0:\kappa+\beta} \cap \mathcal{L}^{f,g}$ of length $\lambda_1(\mathcal{L}^{h,q}_{0:\kappa+\beta} \cap \mathcal{L}^{f,g})$.

Lemma (Minkowski's bound)

For any $\boldsymbol{d}$-dimensional lattice we have: $\lambda_1(\mathcal{L}) \leq 2\frac{\det(\mathcal{L})^{1/d}}{vol(\mathcal{B}^d)^{1/d}} \leq \sqrt{d}\det(\mathcal{L})^{1/d}$.

Intersection Volume

Goal

Estimate $\det(\mathcal{L}^{h,q}_{\mathbf{0}:\kappa+\beta} \cap \mathcal{L}^{f,g})$.

Lemma (Generalisation of Pataki-Tural)

Let $\mathcal{L}$ be a d-dimensional lattice with basis $\mathbf{b}_0, \ldots, \mathbf{b}_{d-1}$. Then for any n-dimensional sublattice $\mathcal{L}' \subset \mathcal{L}$ we have

$$\det(\mathcal{L}_{\mathbf{0}:s} \cap \mathcal{L}') \leq \det(\mathcal{L}') \cdot \left(\min_J \prod_{j \in J} \left\| \mathbf{b}_j^* \right\| \right)^{-1},$$

where $k := dim(\mathcal{L}_{\mathbf{0}:s} \cap \mathcal{L}')$ and J ranges over the $(n-k)$-size subsets of $\{s, \ldots, d-1\}$.

Asymptotics

DSD-PT Estimate - Prediction [Our Work]

BKZ finds a dense sublattice vector at position $\approx n - \beta/2$ when $\beta \geq \Theta(n/\log^2 q)$.

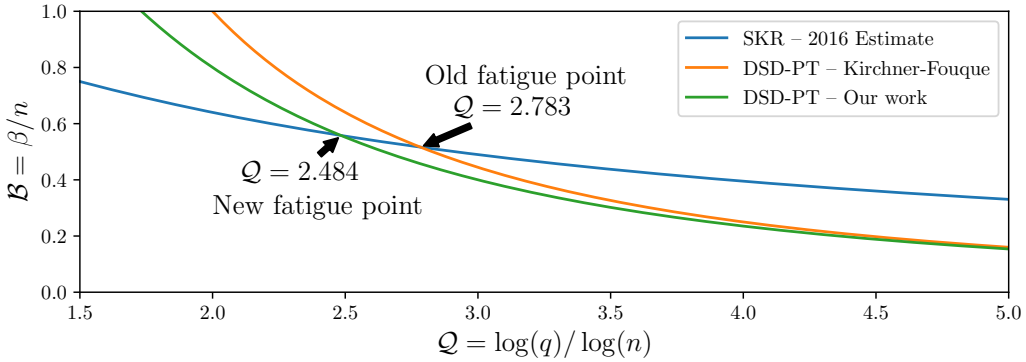
- For parameters $q = \Theta(n^{\mathcal{Q}})$, $\|(f|g)\| = O(n^{\mathcal{S}})$, and $\beta = \mathcal{B}n$ we have:

Estimate	Prediction
SKR	$\mathcal{B} \geq \frac{2\mathcal{Q}}{(\mathcal{Q}+1-\mathcal{S})^2}$ if $\mathcal{S} < 1$ $\mathcal{B} \geq \frac{2}{\mathcal{Q}+2-2\mathcal{S}}$ if $\mathcal{S} \geq 1$.
DSD-PT KF	$\mathcal{B} \geq \frac{8\mathcal{S}}{\mathcal{Q}^2}$.
DSD-PT [This work]	$\mathcal{B} \geq \frac{8\mathcal{S}}{\mathcal{Q}^2+1}$.

Asymptotics

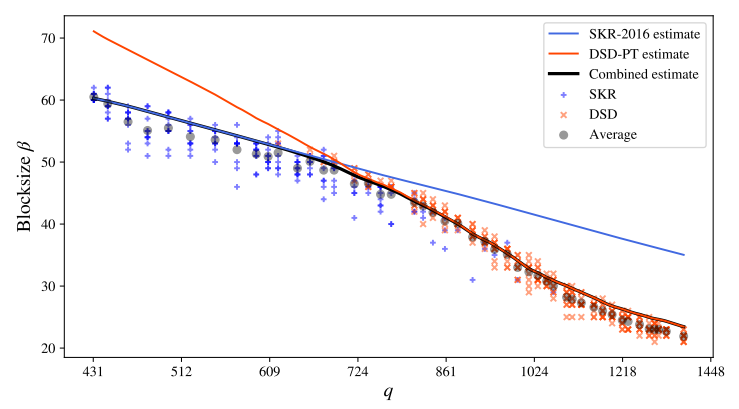
DSD-PT Estimate - Prediction [Our Work]

BKZ finds a dense sublattice vector at position $\approx n - \beta/2$ when $\beta \geq \Theta(n/\log^2 q)$.



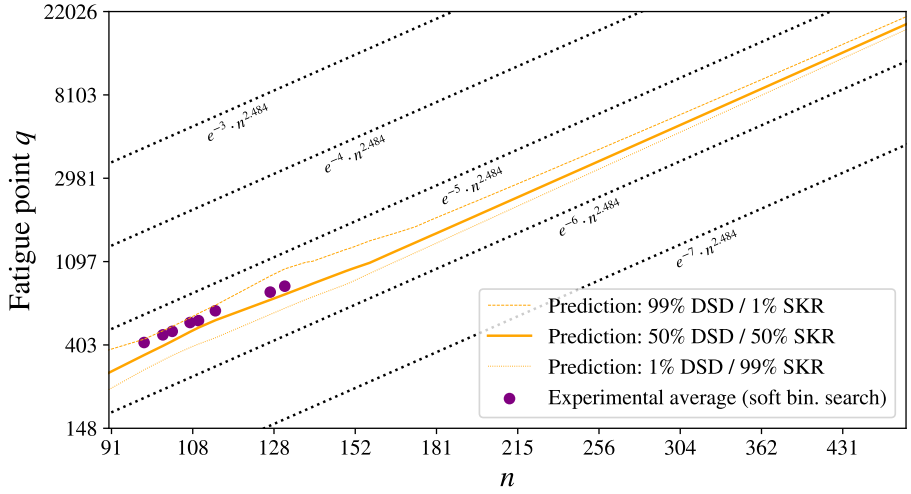
Concrete Predictions

- By a heuristic average-case analysis we can make concrete predictions.

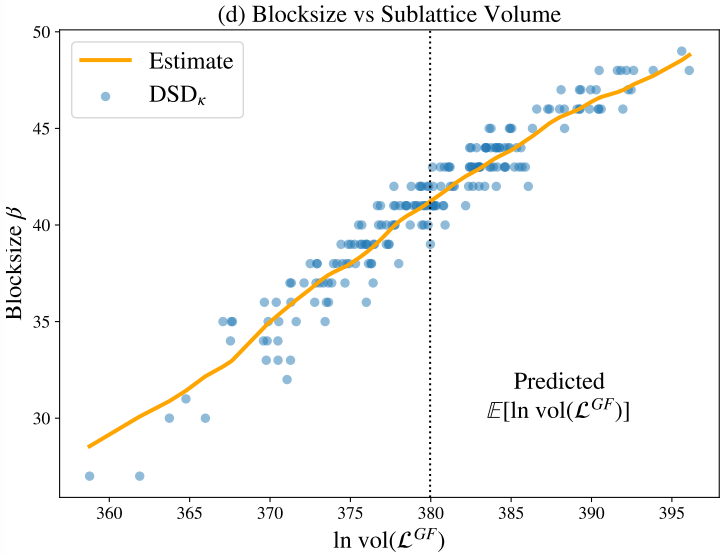


Concrete Fatigue Point

- For ternary $f, g \in \{-1, 0, 1\}^n$ the concrete fatigue point lies at $\approx 0.004 \cdot n^{2.484}$.



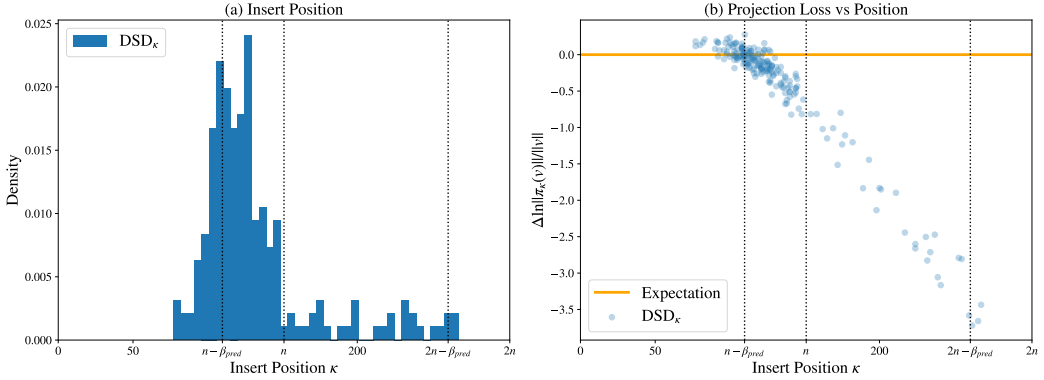
Volume Dense Sublattice



Open Question

Lucky Lifts?

Some DSD events at higher insert positions can't be explained by our estimate.



Takeaways

Concrete Predictions

We now have concrete predictions for all values of the modulus q.

Fatigue Point

The fatigue point lies much lower than expected, but still well above NIST parameters.

Large Variance

The determinant of the dense sublattice can vary a lot, which has a large influence on the blocksize β required.

Code available at:

`https://github.com/WvanWoerden/NTRUFatigue`

Thank you!

Bibliography

ADPS16 E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. "Post-quantum key exchange—a new hope." 25Th USENIX security symposium (USENIX security 16). 2016.

AGVW17 M.R. Albrecht, F. Göpfert, F. Virdia, and T. Wunderer. "Revisiting the expected cost of solving uSVP and applications to LWE." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2017.

DDGR20 D. Dachman-Soled, L. Ducas, H. Gong and M. Rossi. "LWE with side information: attacks and concrete security estimation." Annual International Cryptology Conference. Springer, Cham, 2020.

PV21 E.W. Postlethwaite and F. Virdia. "On the Success Probability of Solving Unique SVP via BKZ." IACR International Conference on Public-Key Cryptography. Springer, Cham, 2021.

KF17 P. Kirchner and P-A Fouque. "Revisiting lattice attacks on overstretched NTRU parameters." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2017.

DvW21 **L. Ducas, and W. van Woerden. "NTRU Fatigue: How Stretched is Overstretched?." Asiacrypt 2021.**