Improved Provable Reduction of NTRU and Hypercubic Lattices

Rennes Cryptography seminar

Henry Bambury [1,2], Phong Nguyen [1]

[1]DIENS, Inria Team CASCADE [2]DGA

Friday, October 18th, 2024

What is a lattice?

Choose your definition:

- A discrete (additive) subgroup of $\mathbb{R}^n$.
- A free $\mathbb{Z}$-submodule of $\mathbb{R}^n$.
- All $\mathbb{Z}$-linear combinations of basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \mathbb{R}^n$:

$$\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_m) := \left\{ \sum_{i=1}^{m} x_i \mathbf{b}_i : \mathbf{x} \in \mathbb{Z}^m \right\} = \mathbb{Z}^m \mathbf{B}.$$

A lattice Λ is **full-rank** in $\mathbb{R}^n$ if $\mathrm{span}(\Lambda) = \mathbb{R}^n$, e.g. if $\mathbf{B}$ is nonsingular.

Quick fact

Two bases $\mathbf{B}_1$ and $\mathbf{B}_2$ generate the same lattice iff $\mathbf{B}_1 = \mathbf{U}\mathbf{B}_2$ for some $\mathbf{U} \in \mathrm{SL}_n(\mathbb{Z})$.

Random real lattices: your *typical* lattice

Definition: Volume of a lattice

If $\Lambda = \mathcal{L}(\mathbf{B})$ is a full-rank lattice of $\mathbb{R}^n$, then its **volume**[a] is

$$\text{covol}(\Lambda) := \text{vol}(\mathbb{R}^n/\Lambda) = |\det(\mathbf{B})|.$$

[a] Cryptographers use the notation $\text{vol}(\Lambda)$, mathematicians $\text{covol}(\Lambda)$.

- The space of all lattices of (co)volume 1 is $X_n := \text{SL}_n(\mathbb{R})/\text{SL}_n(\mathbb{Z})$.

The Siegel (Haar) measure

There exists a unique $\text{SL}_n(\mathbb{Z})$-invariant probability measure on X_n.

- This is a satisfying way to define a random lattice.

Some lattices from crypto are not *typical*

Gaussian Heuristic

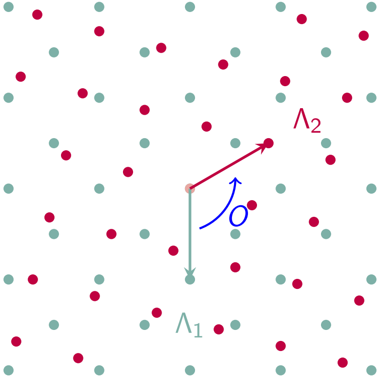
It follows from works of Siegel and Rogers that a random lattice Λ satifies

$$\frac{\lambda_1(\Lambda)}{\mathrm{vol}(\Lambda)^{1/n}} = (1 + o(1)) \frac{1}{\mathrm{vol}(\mathcal{B}_n(1))^{1/n}} \approx \sqrt{\frac{n}{2\pi e}}$$

with probability $(1 - o(1))$ as n grows.

This fails quite strongly for **hypercubic** lattices (i.e. with an orthonormal basis).

Hard algorithmic problems in lattice crypto (1)



$\Lambda_2 = O \cdot \Lambda_1$

Lattice Isomorphism Problem (LIP)

Given two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ such that there exists $O \in \mathcal{O}_n(\mathbb{R})$ for which $\Lambda_1 = O \cdot \Lambda_2$, recover such an O.

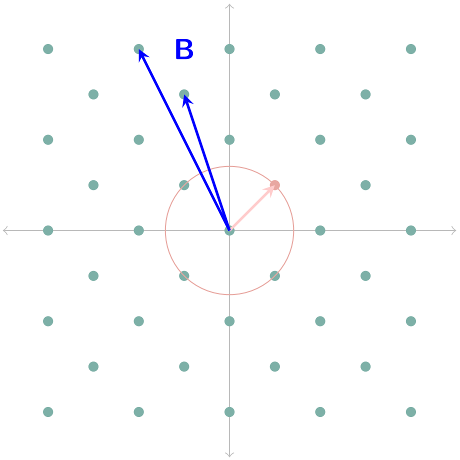
- If Λ_1 and Λ_2 are hypercubic, we call this problem $\mathbb{Z}$LIP.

Hard algorithmic problems in lattice crypto (2)

The Shortest Vector Problem (SVP)

Given $\mathbf{B}$ a basis of a lattice $\Lambda \subset \mathbb{R}^n$, find a $\mathbf{v} \in \Lambda$ such that $\|\mathbf{v}\|_2 = \lambda_1(\Lambda)$.

- $\mathbb{Z}$LIP reduces to SVP.
- So does almost all of lattice crypto.



Main results

Motivating question: can we provably show that some lattices can be reduced using SVP oracles in dimensions substantially smaller than their rank n?

Previous work:

- Heuristic estimates.
- Dimension $n/2$ SVP oracles are enough to reduce $\mathbb{Z}^n$ [Duc23].

Our results:

- Oracles in [Duc23] can be relaxed to approximate-SVP oracles.
- For many NTRU instances: $n/2$ is also sufficient.

We **do not** claim any security loss on $\mathbb{Z}$LIP or NTRU based schemes.

Roadmap

Gram-Schmidt Orthogonalisation

GSO

For a lattice $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, its Gram-Schmidt vectors $\mathbf{b}_1^\star, \ldots, \mathbf{b}_n^\star$ are defined by the following iterative procedure:

- $\mathbf{b}_1^\star := \mathbf{b}_1$;
- $\mathbf{b}_i^\star := \pi_{(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp}(\mathbf{b}_i)$.

- GSO preserves volumes:

$$\mathrm{vol}(\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_i)) = \mathrm{vol}(\mathcal{L}(\mathbf{b}_1^\star, \ldots, \mathbf{b}_i^\star)) = \prod_{j=1}^{i} \|\mathbf{b}_j^\star\|.$$

Lattice algorithms

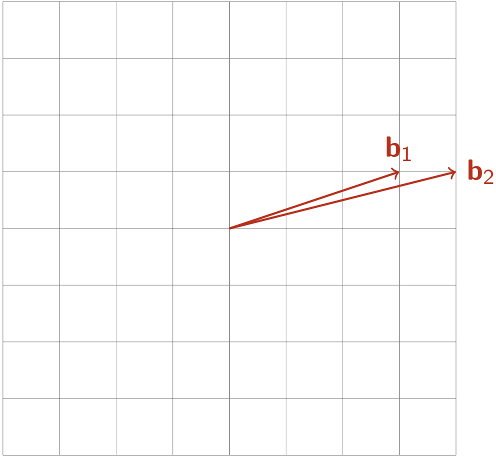
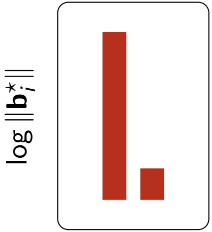
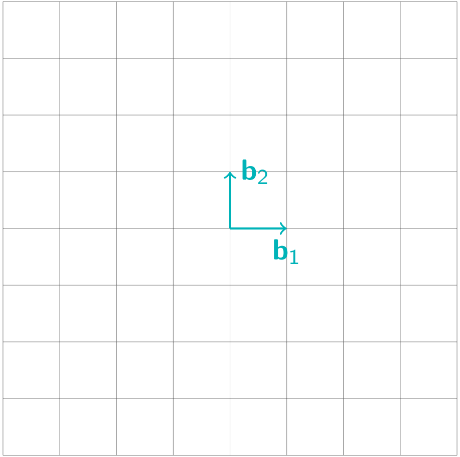


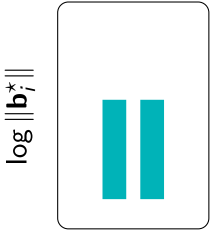
Figure: Gram-Schmidt profile



Convert a bad basis **B** into...

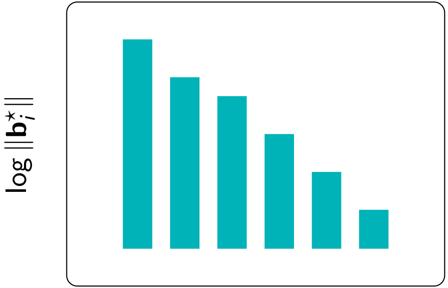
Lattice algorithms

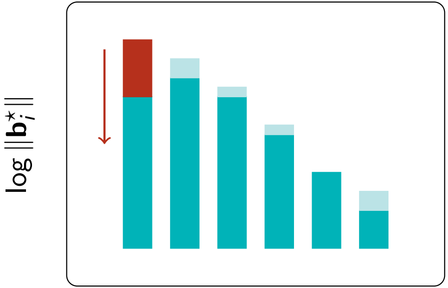




… a better basis $\mathbf{B}$.

Building block: SVP Reduction





γ-SVP oracle

Outputs a basis $\mathbf{B}$ whose first Gram-Schmidt norm is $\|\mathbf{b}_1^\star\| \leq \gamma\lambda_1(\mathcal{L}(\mathbf{B}))$.

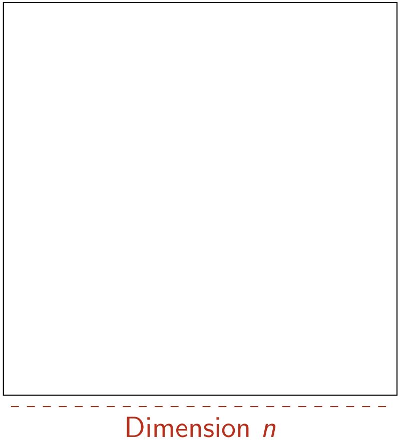
Blockwise Reduction

BKZ algorithm:

- State of the art lattice reduction.
- Calls SVP oracles on projected sub-lattices of dimension β.

Security estimates for lattices:

- Predict the smallest β that reduces the lattice.
- This is heuristic.



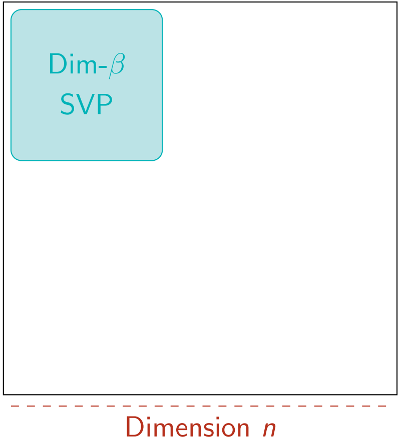
Blockwise Reduction

BKZ algorithm:

- State of the art lattice reduction.
- Calls SVP oracles on projected sub-lattices of dimension β.

Security estimates for lattices:

- Predict the smallest β that reduces the lattice.
- This is heuristic.



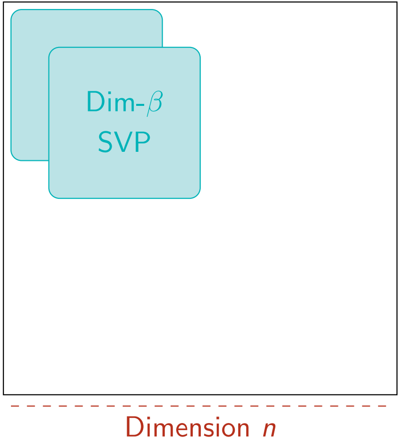
Blockwise Reduction

BKZ algorithm:

- State of the art lattice reduction.
- Calls SVP oracles on projected sub-lattices of dimension β.

Security estimates for lattices:

- Predict the smallest β that reduces the lattice.
- This is heuristic.



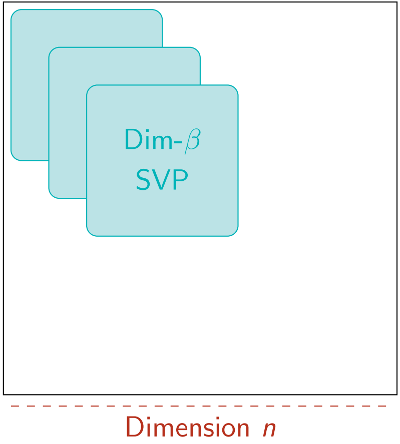
Blockwise Reduction

BKZ algorithm:

- State of the art lattice reduction.
- Calls SVP oracles on projected sub-lattices of dimension β.

Security estimates for lattices:

- Predict the smallest β that reduces the lattice.
- This is heuristic.



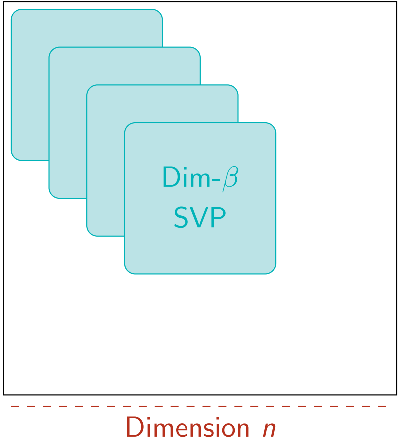
Blockwise Reduction

BKZ algorithm:

- State of the art lattice reduction.
- Calls SVP oracles on projected sub-lattices of dimension β.

Security estimates for lattices:

- Predict the smallest β that reduces the lattice.
- This is heuristic.



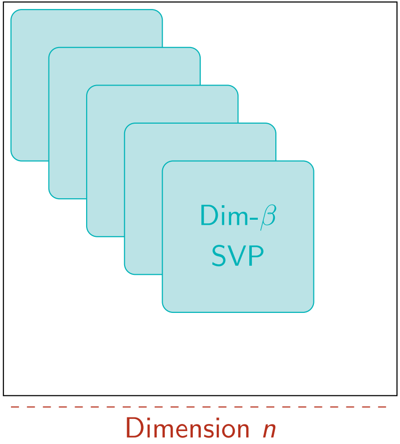
Blockwise Reduction

BKZ algorithm:

- State of the art lattice reduction.
- Calls SVP oracles on projected sub-lattices of dimension β.

Security estimates for lattices:

- Predict the smallest β that reduces the lattice.
- This is heuristic.



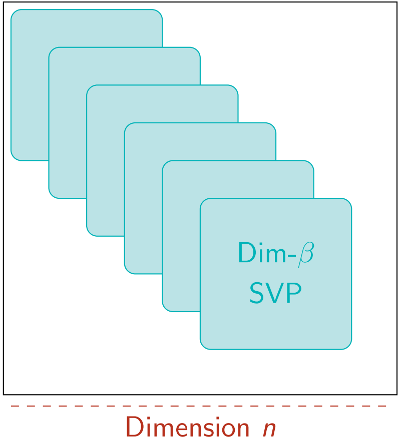
Blockwise Reduction

BKZ algorithm:

- State of the art lattice reduction.
- Calls SVP oracles on projected sub-lattices of dimension β.

Security estimates for lattices:

- Predict the smallest β that reduces the lattice.
- This is heuristic.



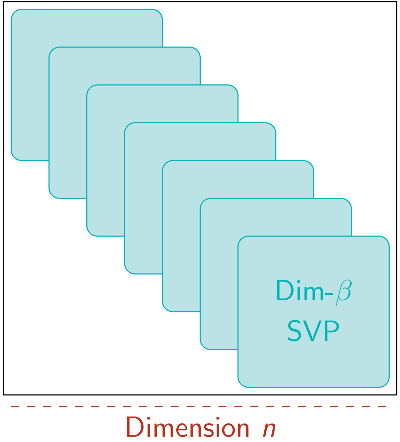
Blockwise Reduction

BKZ algorithm:

- State of the art lattice reduction.
- Calls SVP oracles on projected sub-lattices of dimension β.

Security estimates for lattices:

- Predict the smallest β that reduces the lattice.
- This is heuristic.



Two very special lattices

Hypercubic Lattices:

- Orthonormal basis
- Used in *Lattice Isomorphism Problem* ($\mathbb{Z}$LIP) and HAWK [DvW22, DPPvW22]

NTRU Lattices:

- Module structure
- Used in many schemes and standards: NTRU, Falcon, ... [HPS98, CDH^{+}20, FHK^{+}19]

- In general, lattice reduction estimates are heuristic and rely on low-dim experiments and predictions on the behaviour of lattice algorithms (BKZ).

Provable reduction with smaller blocks: what do we know?

Question

Is it possible to provably solve SVP in special families of lattices of rank n using only SVP-oracles in dimension $\beta = \alpha n$ for a constant $\alpha < 1$?

Provable reduction with smaller blocks: what do we know?

Question

Is it possible to provably solve SVP in special families of lattices of rank n using only SVP-oracles in dimension $\beta = \alpha n$ for a constant $\alpha < 1$?

For Hypercubic Lattices:

- In 2023, Ducas proved that $\alpha = \frac{1}{2}$ suffices [Duc23].

For NTRU Lattices:

- Until now, no α better than 1.
- In 2006, Gama, Howgrave-Graham and Nguyen conjectured $\alpha < 1$ [GHN06].

Duality (1)

Dual lattice

Every lattice Λ can be paired up with its **dual lattice**[a]

$$\Lambda^{\times} := \{\mathbf{w} \in \mathrm{span}(\Lambda) : \langle \mathbf{w}, \mathbf{v} \rangle \in \mathbb{Z} \text{ for all } \mathbf{v} \in \Lambda\}.$$

[a] Notations vary a lot in the literature: Λ^*, $\Lambda^\vee$, $\widehat{\Lambda}$,...

- $\dim(\mathrm{span}(\Lambda)) = \dim(\mathrm{span}(\Lambda^\times))$;
- $\mathrm{vol}(\Lambda) = \mathrm{vol}(\Lambda^\times)^{-1}$.

Hypercubic lattices are isodual ($\Lambda = \Lambda^\times$).

Duality (2)

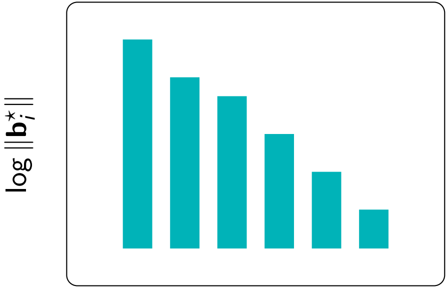
Dual basis

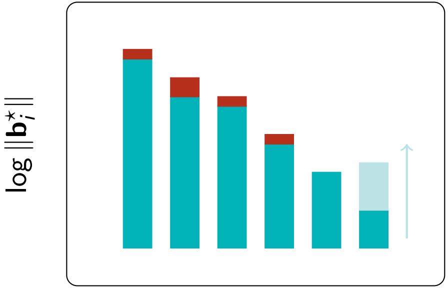
If Λ has basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, then there is a unique **dual basis** $(\mathbf{d}_1, \ldots, \mathbf{d}_n)$ of $\Lambda^\times$ such that $\langle \mathbf{b}_i, \mathbf{d}_j \rangle = \delta_{i,j}$ (Kronecker symbol) for all i, j.

- For all i,

$$\frac{\mathbf{b}_i^\star}{\|\mathbf{b}_i^\star\|^2} \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_i)^\times.$$

- In particular, $\mathbf{d}_n = \mathbf{b}_n^\star / \|\mathbf{b}_n^\star\|^2$ and $\|\mathbf{d}_n\| = \|\mathbf{b}_n^\star\|^{-1}$.





γ-Dual-SVP oracle

Outputs a basis $\mathbf{B}$ whose last dual Gram-Schmidt norm is

$$\|\mathbf{d}_n^\star\| = \|\mathbf{b}_n^\star\|^{-1} \leq \gamma\lambda_1(\mathcal{L}(\mathbf{B})^\times).$$

Primitivity, quotients and projections

Primitive sublattice

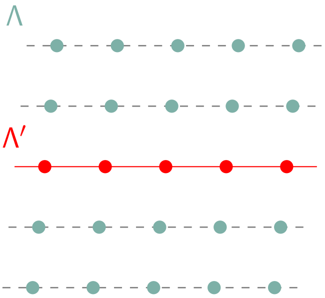
A sublattice Λ' of Λ is **primitive** if $\text{span}(\Lambda') \cap \Lambda = \Lambda'$. In this case, $\pi_{\Lambda'^{\perp}}(\Lambda)$ is a lattice.

Quotient

If Λ' is a primitive sublattice of Λ, then we can identify the **quotient** Λ/Λ' with the lattice $\pi_{\Lambda'^{\perp}}(\Lambda)$.

For a primitive Λ':

$$\Lambda/\Lambda' = \pi_{\Lambda'^{\perp}}(\Lambda) = (\Lambda^{\times} \cap \Lambda'^{\perp})^{\times}.$$



Primitive sublattice

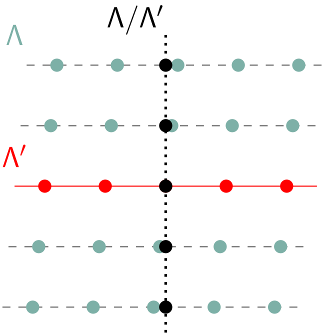
A sublattice Λ' of Λ is **primitive** if $\text{span}(\Lambda') \cap \Lambda = \Lambda'$. In this case, $\pi_{\Lambda'^{\perp}}(\Lambda)$ is a lattice.

Quotient

If Λ' is a primitive sublattice of Λ, then we can identify the **quotient** Λ/Λ' with the lattice $\pi_{\Lambda'^{\perp}}(\Lambda)$.

For a primitive Λ':

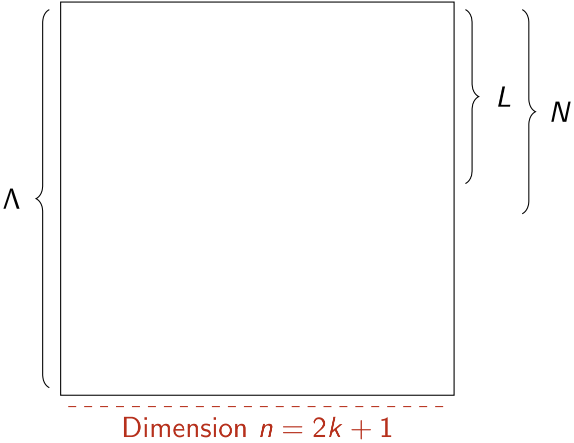
$$\Lambda/\Lambda' = \pi_{\Lambda'^{\perp}}(\Lambda) = (\Lambda^{\times} \cap \Lambda'^{\perp})^{\times}.$$

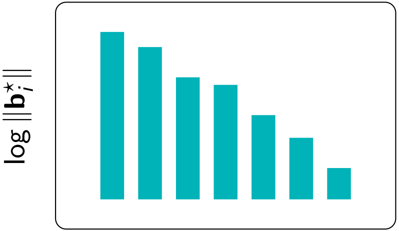


Roadmap

Primal/Dual Reduction: A nice tool for provable reduction

$$\Lambda = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \qquad L = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k) \qquad N = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{k+1})$$



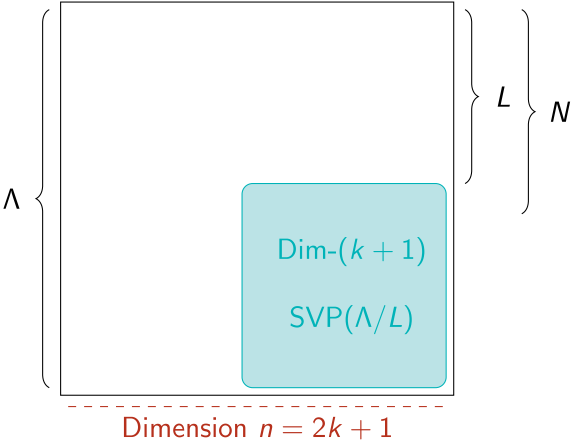


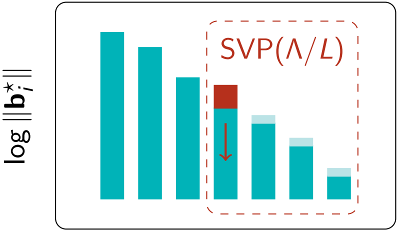
We know that

$$\mathrm{vol}(N) = \mathrm{vol}(L)\|\mathbf{b}^\star_{k+1}\|.$$

Slide-inspired Reduction: Primal step

$$\Lambda = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \qquad L = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k) \qquad N = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{k+1})$$



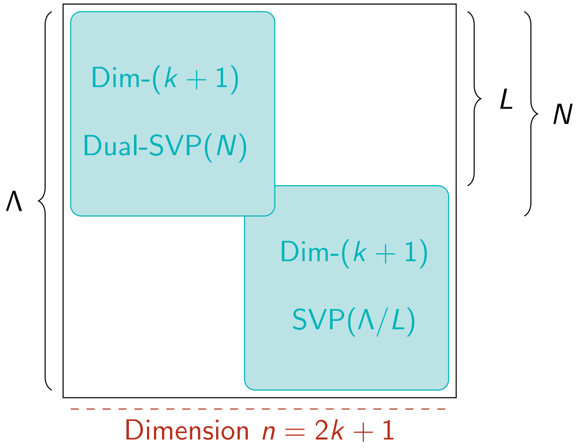


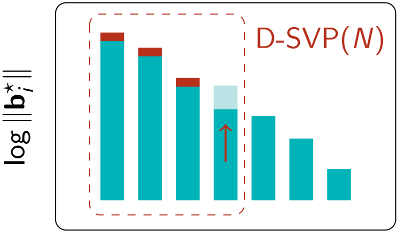
After SVP-reduction:

$$\|\mathbf{b}_{k+1}^{\star}\| = \lambda_1(\Lambda/L).$$

Slide-inspired Reduction: Dual step

$$\Lambda = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \qquad L = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k) \qquad N = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{k+1})$$





After D-SVP-reduction:

$$\|\mathbf{b}^\star_{k+1}\|^{-1} = \lambda_1(N^\times).$$

Slide-inspired Reduction: Analysis

How does each Primal/Dual step change $\mathrm{vol}(L)$?

After the Primal step

$$\mathrm{vol}(N) = \mathrm{vol}(L)\lambda_1(\Lambda/L)$$

Slide-inspired Reduction: Analysis

How does each Primal/Dual step change $\mathrm{vol}(L)$?

After the Primal step

$$\mathrm{vol}(N) = \mathrm{vol}(L)\lambda_1(\Lambda/L)$$

After the Dual step

$$\mathrm{vol}(N) = \mathrm{vol}(L')\lambda_1(N^{\times})^{-1}$$

Slide-inspired Reduction: Analysis

How does each Primal/Dual step change $\mathrm{vol}(L)$?

After the Primal step

$$\mathrm{vol}(N) = \mathrm{vol}(L)\lambda_1(\Lambda/L)$$

Finally

$$\frac{\mathrm{vol}(L')}{\mathrm{vol}(L)} = \lambda_1(\Lambda/L)\lambda_1(N^\times)$$

After the Dual step

$$\mathrm{vol}(N) = \mathrm{vol}(L')\lambda_1(N^\times)^{-1}$$

Slide-inspired Reduction: Analysis

How does each Primal/Dual step change vol(L)?

After the Primal step

$$\mathrm{vol}(N) = \mathrm{vol}(L)\lambda_1(\Lambda/L)$$

Finally

$$\frac{\mathrm{vol}(L')}{\mathrm{vol}(L)} = \lambda_1(\Lambda/L)\lambda_1(N^\times)$$

After the Dual step

$$\mathrm{vol}(N) = \mathrm{vol}(L')\lambda_1(N^\times)^{-1}$$

- If $\lambda_1(\Lambda/L)\lambda_1(N^\times) < 1 - \frac{1}{\mathrm{poly}(n)}$, we win!
- For general lattices, we can only use Minkowski's theorem to bound $\lambda_1(\Lambda/L)$ and $\lambda_1(N^\times)$.

Roadmap

I. Intro: Building Blocks

II. A Primal/Dual Reduction Framework

III. Application: Hypercubic Lattices

IV. Application: NTRU Lattices

V. Comparison with Heuristic Reduction

Ducas' idea: bounding λ_1 for projections of $\mathbb{Z}^n$

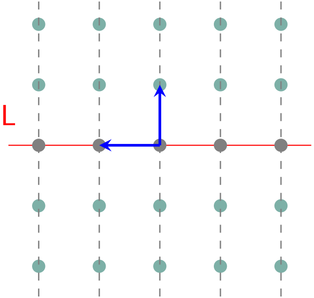
Lemma (From [Duc23])

Let L be a primitive sublattice of $\mathbb{Z}^n$ of rank k and volume $\mathrm{vol}(L) > 1$, then

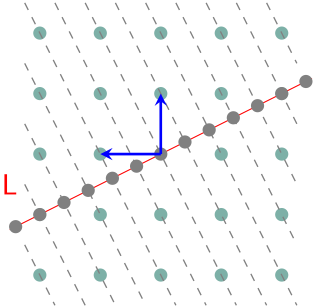
$$\lambda_1(\mathbb{Z}^n/L) \leq \sqrt{1 - \frac{1}{n}}.$$

- Gives much stronger bound on $\lambda_1(\Lambda/L)\lambda_1(N^\times)$ than Minkowski's theorem.
- $\mathrm{vol}(L)$ decreases by at least $(1 - \frac{1}{n})$ at each Primal/Dual step.

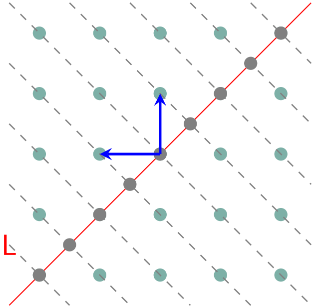
Projecting $\mathbb{Z}^2$ onto a line: Intuition from pictures



- $\lambda_1(L \cap \mathbb{Z}^2) = 1$;
- $\lambda_1(\pi_L(\mathbb{Z}^2)) = 1$.



- $\lambda_1(L \cap \mathbb{Z}^2) > 1$;
- $\lambda_1(\pi_L(\mathbb{Z}^2)) < \frac{1}{\sqrt{2}}$.



- $\lambda_1(L \cap \mathbb{Z}^2) > 1$;
- $\lambda_1(\pi_L(\mathbb{Z}^2)) = \frac{1}{\sqrt{2}}$.

A more general result: forcing small vectors into projections of $\mathbb{Z}^n$

Key Lemma

Let L be a primitive sublattice of $\mathbb{Z}^n$ of rank k such that $\lambda_1(L) > 1$, then

$$\lambda_1(\mathbb{Z}^n/L) \leq \sqrt{1 - \frac{k}{n}}.$$

A more general result: forcing small vectors into projections of $\mathbb{Z}^n$

Key Lemma

Let L be a primitive sublattice of $\mathbb{Z}^n$ of rank k such that $\lambda_1(L) > 1$, then

$$\lambda_1(\mathbb{Z}^n/L) \leq \sqrt{1 - \frac{k}{n}}.$$

Proof

First prove that $\sum_{i=1}^n \|\pi_{L^\perp}(\mathbf{e}_i)\|^2 = n - k$. The condition $\lambda_1(L) > 1$ means $\forall i, \pi_{L^\perp}(\mathbf{e}_i) > 0$. Hence $0 < \|\pi_{L^\perp}(\mathbf{e}_i)\|^2 \leq 1 - \frac{k}{n}$ for some i. □

- In particular if $k = \frac{n}{2}$, then $\lambda_1(\mathbb{Z}^n/L) \leq \frac{1}{\sqrt{2}}$.

Modified algorithm: relaxing the approximation factor

Input: A bad basis of a hypercubic Λ

Main loop:

I. Check for unit vectors in L
II. γ-SVP reduce Λ/L
III. Check for unit vectors in $(\Lambda/N)^\times$
IV. γ-Dual-SVP reduce N

Each line only uses a $\gamma < \sqrt{2}$ approximation oracle in halved dimension. vol(L) decreases by at least:

$$\gamma^2 \lambda_1(\Lambda/L)\lambda_1(N^\times) = \gamma^2 \lambda_1(\Lambda/L)\lambda_1(\Lambda^\times/(\Lambda/N)^\times) \leq \gamma^2/2 = 1-\varepsilon.$$

Does it matter? Perspectives

- The best (provable) algorithms for $\mathbb{Z}$LIP run in $2^{n/2+o(n)}$.
- For large enough (constant) γ, dim $n/2$ γ-SVP runs in $2^{0.401n+o(n)}$, provably.

Open problems:

- What is the *real* cost of solving $\sqrt{2}$-SVP?
- Can we break the $n/2$ barrier for $\mathbb{Z}$LIP?
- Is the "easiest lattice" really that hard?

Roadmap

- I. Intro: Building Blocks
- II. A Primal/Dual Reduction Framework
- III. Application: Hypercubic Lattices
- IV. Application: NTRU Lattices
- V. Comparison with Heuristic Reduction

Observation: a similar algorithm works more generally

Using exact-SVP-oracles: at each step $\mathrm{vol}(L)$ is multiplied by $\lambda_1(\Lambda/L)\lambda_1(N^\times)$.

Quick Lemma

If $\lambda_1(L) > \lambda_1(\Lambda)$, then $\lambda_1(\Lambda/L) \leq \lambda_1(\Lambda)$.

Consequence: Testing $\lambda_1(L) > \lambda_1(\Lambda)$ with an SVP-oracle

$\implies$ at each step $\mathrm{vol}(L)$ is multiplied by at most $\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$.

Surely no reasonable lattice family satisfies $\lambda_1(\Lambda)\lambda_1(\Lambda^\times) < 1 - \varepsilon$??

The NTRU lattice and its dual

The NTRU lattice has a public basis and its dual of the form

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I}_{n/2} & 0 \\ \mathbf{H} & \mathbf{I}_{n/2} \end{pmatrix} \text{ and } \mathbf{B}^{\times} = \begin{pmatrix} \frac{1}{q}\mathbf{I}_{n/2} & -\frac{1}{q}\mathbf{H}^{T} \\ 0 & \mathbf{I}_{n/2} \end{pmatrix},$$

where $\mathbf{H}$ is a circulant matrix.

The symplectic nature of NTRU

Lemma (rescaled NTRU is isodual)

If Λ is a NTRU lattice with modulus q over a ring $\mathbb{Z}[X]/(X^n \pm 1)$, then Λ and $q\Lambda^\times$ are isometric.

For such lattices, $\lambda_1(\Lambda)\lambda_1(\Lambda^\times) = \frac{\lambda_1(\Lambda)^2}{q}$.

So when is $\lambda_1(\Lambda)\lambda_1(\Lambda^\times) < 1 - \varepsilon$??

Upper bound on $\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$ for various NTRU parameters			
Lattice	$\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$	$\frac{1}{2}\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$	Approx factor
NIST-1 [CDH+20]	.2897	.1449	2.628
NIST-3 [CDH+20]	.3444	.1722	2.410
NIST-5 [CDH+20]	.2581	.1291	1.969

Conclusion: Many NTRU instances are provably solvable with $n/2$ SVP oracles only.

Average behaviour of $\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$

- The quantity $\gamma'(\Lambda) := \sqrt{\lambda_1(\Lambda)\lambda_1(\Lambda^\times)}$ was introduced by Martinet and called the dual Hermite invariant of Λ;
- $\gamma'(\Lambda)$ is independent of $\mathrm{vol}(\Lambda)$;
- For a random lattice of X_n, we expect each term to be of size $\sqrt{\frac{n}{2\pi e}}$;
- Södergren and Strömbergsson studied the independence of limit distributions of shortest vector statistics for Λ and $\Lambda^\times$. We can likely deduce that

$$\mathbb{E}(\lambda_1(\Lambda)\lambda_1(\Lambda^\times)) = (1 + o(1))\frac{n}{2\pi e}.$$

Roadmap

I. Intro: Building Blocks

II. A Primal/Dual Reduction Framework

III. Application: Hypercubic Lattices

IV. Application: NTRU Lattices

V. Comparison with Heuristic Reduction

The Primal Attack Model

Question: For which blocksize β does BKZ-β recover the secret vector $\mathbf{s}$?

Since [ADPS16], the heuristic value for β is taken as the smallest such that

$$\mathbb{E}_{\text{random dim } \beta \text{ subspace } F}\left(\pi_F(\|\mathbf{s}\|)\right) < \mathbb{E}_{\text{BKZ-}\beta \text{ reduction}}\left(\|\mathbf{b}^{\star}_{n-\beta+1}\|\right).$$

- If this holds, the projection of the secret onto the last BKZ block is short enough that the SVP oracle is likely to recover it.
- Very heuristic, yet used by all lattice schemes to estimate concrete security.

Comparing with Primal Attack Asymptotics

Asymptotically, how close are the best provable and heuristic estimates?

Lattice (dim n)	Provable blocksize	Heuristic blocksize (GSA + 2016 est.)
Hypercubic	$n/2 + o(n)$	$n/2 - o(n)$
NTRU[1]	$n/2 + o(n)$	$4n/9 - o(n)$

- The difference comes from the public NTRU q-vectors, that are better reduced than what one would expect from BKZ-$n/2$.

[1] Assuming $q = \Theta(n)$ and $\lambda_1(\Lambda) = \Theta(\sqrt{n})$.

The Primal Attack Model - Multi Target Mode

Lattice estimators like [DSDGR20] have an option for *multiple targets*, when

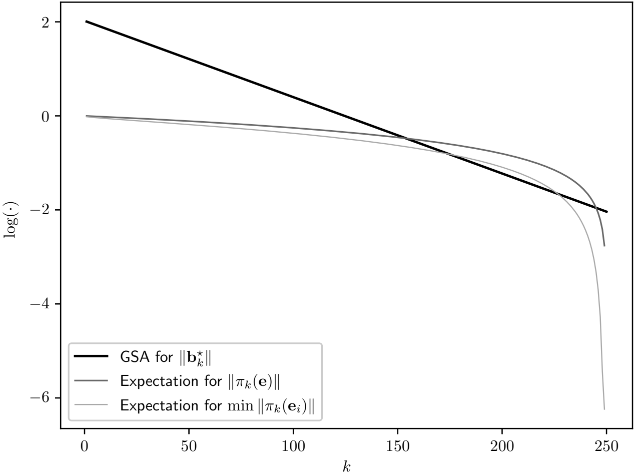
$$\lambda_1(\Lambda) = \ldots = \lambda_k(\Lambda).$$

Indeed $\mathbb{E}\left(\min_{1 \leq i \leq k} \|\pi(\mathbf{s}_i)\|^2\right) < \mathbb{E}\left(\|\pi(\mathbf{s}_1)\|^2\right)$, so the primal attack blocksize should be smaller.

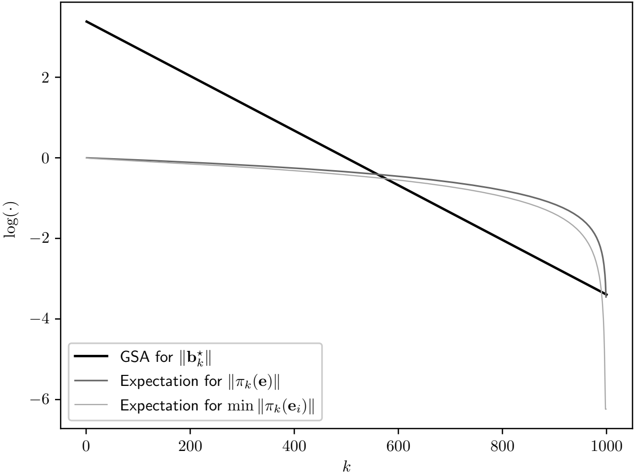
Claim

Asymptotically, a linear number of (independent) short secrets does not change the first order terms in the asymptotic blocksize.

The Primal Attack Model - Multi Target Mode



The Primal Attack Model - Multi Target Mode



Recap/Takeaway

Conclusions:

- Like $\mathbb{Z}^n$, NTRU's geometry makes it easier to provably reduce.
- We give an algorithm that uses dim $n/2$ SVP-oracles.
- Those oracles can be relaxed by a constant γ.
- We help reduce the gap between provable and heuristic results.
- We provide new insights into the asymptotics of the primal attack.

The End

Bonus questions:

- Which of NTRU and $\mathbb{Z}$LIP is easier?
- Can we exploit isoduality better?
- Can Primal/Dual reduction be made practical?

Check out the paper at:

`iacr.org/2024/601.`
(PQCrypto'2024)

Thank you
For listening! :-)

References I

Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe.
Post-quantum key exchange - A new hope.
In *Proc. 25th USENIX*, pages 327–343. USENIX, 2016.

Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hulsing, Joost Rijneveld, John M. Schanck, Tsunekazu Saito, Peter Schwabe, William Whyte, Keita Xagawa, Takashi Yamakawa, and Zhenfei Zhang.
Ntru algorithm specifications and supporting documentation, 9 2020.

Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden.
Hawk: Module LIP makes lattice signatures fast, compact and simple.
In *Advances in Cryptology - Proc. ASIACRYPT 2022*, volume 13794 of *Lecture Notes in Computer Science*, pages 65–94. Springer, 2022.

References II

Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi.
Lwe with side information: Attacks and concrete security estimation.
In *Advances in Cryptology – Proc. CRYPTO 2020*, page 329–358, Berlin, Heidelberg, 2020. Springer-Verlag.

Léo Ducas.
Provable lattice reduction of $\mathbb{Z}^n$ with blocksize $n/2$.
Designs, Codes and Cryptography, Nov 2023.

Léo Ducas and Wessel van Woerden.
On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography.
In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - Proc. EUROCRYPT 2022*, volume 13277 of *Lecture Notes in Computer Science*, pages 643–673. Springer, 2022.

References III

Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang.
Falcon: Fast-fourier lattice-based compact signatures over ntru, 3 2019.

Nicolas Gama, Nick Howgrave-Graham, and Phong Q. Nguyen.
Symplectic lattice reduction and NTRU.
In Serge Vaudenay, editor, *Advances in Cryptology - Proc. EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 233–253. Springer, 2006.

J. Hoffstein, J. Pipher, and J.H. Silverman.
NTRU: a ring based public key cryptosystem.
In *Proc. of ANTS III*, volume 1423 of *LNCS*, pages 267–288. Springer-Verlag, 1998.