Algorithms for Lattice Problems: In Practice

Martin R. Albrecht

Information Security Group, Royal Holloway, University of London

23 January 2020, Lattice Boot Camp @ Simons

Based on joint work with Alex Davidson, Amit Deo, Benjamin R. Curtis, Damien Stehlé, Eamonn W. Postlethwaite, Elena Kirshanova, Fernando Virdia, Florian Göpfert, Gottfried Herold, John M. Schanck, Léo Ducas, Marc Stevens, Paul Kirchner, Pierre-Alain Fouque, Rachel Player, Sam Scott, Shi Bai, Thomas Wunderer, Vlad Gheorghiu and Weiqiang Wen as well as the works of many other authors.

Introduction

NIST PQ Round 1: Selected Cost Estimates

Cost Model \ Scheme	Kyber	NewHope	NTRU HRSS	SNTRU’
$0.292\,\beta$ [1]	180	259	136	155
$1/(2e)\,\beta\log(\beta) - \beta + 16.1$ [2]	456	738	313	370
$1/8\,\beta\log(\beta) - 0.75\beta + 2.3$ [3]	248	416	165	200
$0.265\,\beta$ [1]	163	235	123	140
$1/(4e)\,\beta\log(\beta) - 0.5\beta + 8$	228	369	157	187

Source: Martin R. Albrecht, Benjamin R. Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W. Postlethwaite, Fernando Virdia, and Thomas Wunderer. Estimate All the LWE, NTRU Schemes! In: *SCN 18*. Ed. by Dario Catalano and Roberto De Prisco. Vol. 11035. LNCS. Springer, Heidelberg, Sept. 2018, pp. 351–367. DOI: 10.1007/978-3-319-98113-0_19, https://estimate-all-the-lwe-ntru-schemes.github.io/docs/

---

[1] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343

[2] Martin R. Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of Learning with Errors. In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203

[3] Le Trieu Phong, Takuya Hayashi, Yoshinori Aono, and Shiho Moriai. LOTUS. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions. National Institute of Standards and Technology, 2017

Learning with Errors

Given $(\mathbf{A}, \mathbf{c})$, find $\mathbf{s}$ when

$$\begin{pmatrix} \\ \\ \mathbf{c} \\ \\ \\ \end{pmatrix} \equiv \begin{pmatrix} \leftarrow & n & \rightarrow \\ & & \\ & \mathbf{A} & \\ & & \\ & & \end{pmatrix} \cdot \begin{pmatrix} \\ \mathbf{s} \\ \\ \end{pmatrix} + \begin{pmatrix} \\ \\ \mathbf{e} \\ \\ \\ \end{pmatrix}$$

for $\mathbf{c} \in \mathbb{Z}_q^m$, $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, and $\mathbf{s} \in \mathbb{Z}^n$ and $\mathbf{e} \in \mathbb{Z}^m$ having small coefficients.

(Matrix-)NTRU

Let $\mathbf{F}, \mathbf{G}$ be two $n \times n$ matrices over $\mathbb{Z}_q$ with short entries. Given

$$\mathbf{H} \equiv \mathbf{F}^{-1} \cdot \mathbf{G}$$

find (a small multiple of) $\mathbf{F}$ or $\mathbf{G}$.

(Matrix-)NTRU

Let $\mathbf{F}, \mathbf{G}$ be two $n \times n$ matrices over $\mathbb{Z}_q$ with short entries. Given

$$\mathbf{H} \equiv \mathbf{F}^{-1} \cdot \mathbf{G}$$

find (a small multiple of) $\mathbf{F}$ or $\mathbf{G}$.

Note

I will focus on LWE in this talk, but the techniques translate (with some modifications) to NTRU.

Primal Approach

Unique SVP Approach

We can reformulate $\mathbf{c} - \mathbf{A} \cdot \mathbf{s} \equiv \mathbf{e} \bmod q$ over the Integers as:

$$\begin{pmatrix} q\mathbf{I} & -\mathbf{A} \\ 0 & \mathbf{I} \end{pmatrix} \cdot \begin{pmatrix} * \\ \mathbf{s} \end{pmatrix} + \begin{pmatrix} \mathbf{c} \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{e} \\ \mathbf{s} \end{pmatrix}$$

Alternatively:

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I} & -\mathbf{A} & \mathbf{c} \\ 0 & \mathbf{I} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \mathbf{B} \cdot \begin{pmatrix} * \\ \mathbf{s} \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{e} \\ \mathbf{s} \\ 1 \end{pmatrix}$$

In other words, there exists an integer-linear combination of the columns of $\mathbf{B}$ that produces a vector with “unusually” small coefficients $\rightarrow$ a unique shortest vector.

Computational Problem

Unique Shortest Vector Problem

Find a unique shortest vector amongst the integer combinations of the columns of:

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I} & -\mathbf{A} & \mathbf{c} \\ 0 & \mathbf{I} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $\mathbf{B} \in \mathbb{Z}^{d \times d}$.

Decision Variant

Decide if $\mathbf{B}$ has an unusually short vector.

Computational Problem

Unique Shortest Vector Problem

Find a unique shortest vector amongst the integer combinations of the columns of:

$$\mathbf{B} = \begin{pmatrix} q\mathbf{I} & -\mathbf{A} & \mathbf{c} \\ 0 & \mathbf{I} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $\mathbf{B} \in \mathbb{Z}^{d \times d}$.

Decision Variant

Decide if $\mathbf{B}$ has an unusually short vector.

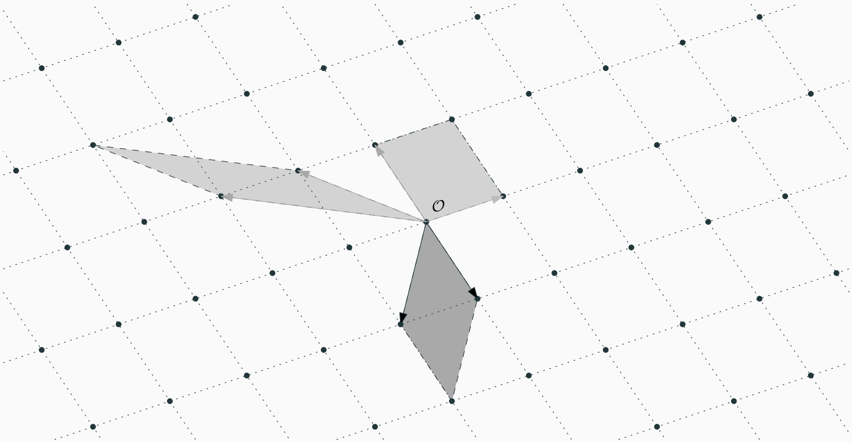
NTRU

For LWE we have (up to $\pm$) one such short vector. For NTRU we have n.

Lattice Reduction

Lattice Volume

The volume of a lattice is the volume of its fundamental parallelepiped.



Picture Credit: Joop van de Pol

Gaussian Heuristic

The shortest vector in the lattice has expected norm

$$\lambda_1(\Lambda) \approx \mathrm{gh}(d) \cdot \mathrm{Vol}(\Lambda)^{1/d} \approx \sqrt{\frac{d}{2\pi e}} \cdot \mathrm{Vol}(\Lambda)^{1/d}.$$

Unusually Shortest Vector

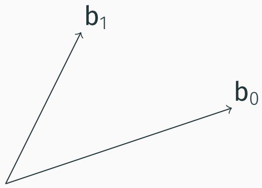
When $\lambda_1(\Lambda) \ll \sqrt{\frac{d}{2\pi e}} \cdot \mathrm{Vol}(\Lambda)^{1/d}$.

Length of Gram-Schmidt Vectors

It will be useful to consider the lengths of the Gram-Schmidt vectors.

The vector $\mathbf{b}_i^*$ is the orthogonal projection of $\mathbf{b}_i$ to the space spanned by the vectors $\mathbf{b}_0, \ldots, \mathbf{b}_{i-1}$.

Informally, this means taking out the contributions in the directions of previous vectors $\mathbf{b}_0, \ldots, \mathbf{b}_{i-1}$.

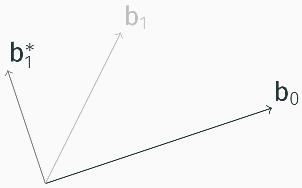


Length of Gram-Schmidt Vectors

It will be useful to consider the lengths of the Gram-Schmidt vectors.

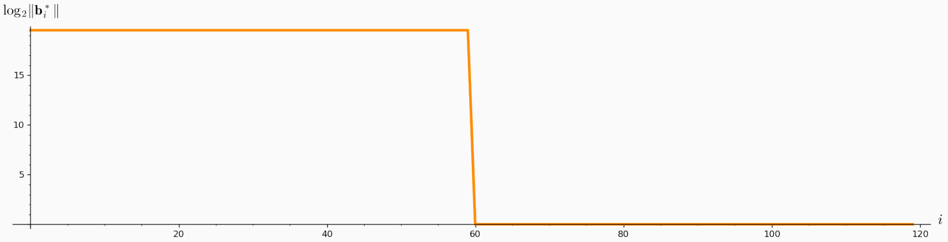
The vector $\mathbf{b}_i^*$ is the orthogonal projection of $\mathbf{b}_i$ to the space spanned by the vectors $\mathbf{b}_0, \ldots, \mathbf{b}_{i-1}$.

Informally, this means taking out the contributions in the directions of previous vectors $\mathbf{b}_0, \ldots, \mathbf{b}_{i-1}$.



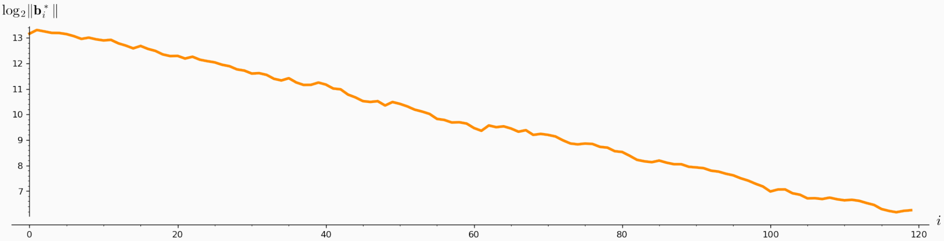
Example

```
sage: A = IntegerMatrix.random(120, "qary", k=60, bits=20)[::-1]
sage: M = GSO.Mat(A); M.update_gso()
sage: line([(i,log(r_, 2)/2) for i, r_ in enumerate(M.r())], **plot_kwds)
```

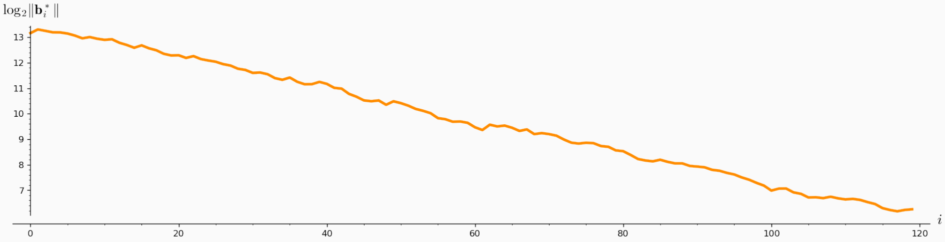


Example - LLL

```
sage: A = LLL.reduction(A)
sage: M = GSO.Mat(A); M.update_gso()
sage: line([(i,log(r_, 2)/2) for i, r_ in enumerate(M.r())], **plot_kwds)
```



GSA



Geometric Series Assumption: The shape after lattice reduction is a line with a flatter slope as lattice reduction gets stronger.[4]

[4] Claus-Peter Schnorr. Lattice Reduction by Random Sampling and Birthday Methods. In: *STACS 2003, 20th Annual Symposium on Theoretical Aspects of Computer Science, Berlin, Germany, February 27 - March 1, 2003, Proceedings*. Ed. by Helmut Alt and Michel Habib. Vol. 2607. Lecture Notes in Computer Science. Springer, 2003, pp. 145–156. DOI: `10.1007/3-540-36494-3_14`. URL: `http://dx.doi.org/10.1007/3-540-36494-3_14`.

Strong Lattice Reduction: BKZ Algorithm

$$\left(\begin{array}{ccccccccc} \multicolumn{5}{c}{\overbrace{\hspace{10em}}^{\beta = 5}} & & & & \\ b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & \dots \end{array}\right)$$

Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm

$$\left(\underbrace{\overbrace{b_0 \quad b_1 \quad b_2 \quad b_3 \quad b_4}^{\beta = 5}} \quad b_5 \quad b_6 \quad b_7 \quad \ldots\right)$$

Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm

$$\left(\overbrace{b_0 \quad b_1 \quad b_2 \quad b_3 \quad b_4}^{\beta = 5} \quad b_5 \quad b_6 \quad b_7 \quad \ldots \right)$$

Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm

$$\left(\begin{array}{c|ccccc|ccc} b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & \dots \end{array}\right)$$

$$\overbrace{b_1 \; b_2 \; b_3 \; b_4 \; b_5}^{\beta = 5}$$

Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm

$$\left(b_0 \quad \overbrace{b_1 \quad b_2 \quad b_3 \quad b_4 \quad b_5}^{\beta = 5} \quad b_6 \quad b_7 \quad \dots \right)$$

Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm

$$\begin{pmatrix} b_0 & \overbrace{b_1 & b_2 & b_3 & b_4 & b_5}^{\beta = 5} & b_6 & b_7 & \dots \end{pmatrix}$$

Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm

$$\left(\; {\color{red}b_0} \quad {\color{red}b_1} \quad \overbrace{\Big| \; b_2 \quad b_3 \quad b_4 \quad b_5 \quad b_6 \; \Big|}^{\beta = 5} \quad b_7 \quad \ldots \; \right)$$

Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm

$$\begin{pmatrix} b_0 & b_1 & \overbrace{b_2 \quad b_3 \quad b_4 \quad b_5 \quad b_6}^{\beta = 5} & b_7 & \ldots \end{pmatrix}$$

Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm

$$\left(b_0 \quad b_1 \quad \overbrace{b_2 \quad b_3 \quad b_4 \quad b_5 \quad b_6}^{\beta = 5} \quad b_7 \quad \dots \right)$$

Picture credit: Eamonn Postlethwaite

BKZ Algorithm

Data: LLL-reduced lattice basis **B**

Data: block size β

repeat *until no more change*

    for $\kappa \leftarrow 0$ **to** $d - 1$ **do**

        LLL on local projected block $[\kappa, \ldots, \kappa + \beta - 1]$;

        v $\leftarrow$ find shortest vector in local projected block $[\kappa, \ldots, \kappa + \beta - 1]$;

        insert **v** into **B**;

    end

Quality: Guarantees

BKZ

- $\|\mathbf{b}_0\| \leq \sqrt{\gamma_\beta}^{\frac{d-1}{\beta-1}+1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$ and
- $\|\mathbf{b}_0\| \leq \gamma_\beta^{\frac{d-1}{\beta-1}} \cdot \lambda_1(\Lambda)$

Slide

- $\|\mathbf{b}_0\| \leq \sqrt{(1+\epsilon)\cdot\gamma_\beta}^{\frac{d-1}{\beta-1}} \cdot \mathrm{Vol}(\Lambda)^{1/d}$ and
- $\|\mathbf{b}_0\| \leq ((1+\epsilon)\cdot\gamma_\beta)^{\frac{d-\beta}{\beta-1}} \cdot \lambda_1(\Lambda)$

β	2	3	4	5	6	7	8	24
$\gamma_\beta{}^{1/(2(\beta\text{-}1))}$	1.074	1.059	1.059	1.053	1.052	1.050	1.050	1.031

Table 1: Hermite's constant γ_β in dimension β.

Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. In: *Math. Program.* 66 (1994), pp. 181–199. DOI: `10.1007/BF01581144`. URL: `https://doi.org/10.1007/BF01581144`

Nicolas Gama and Phong Q. Nguyen. Finding short lattice vectors within Mordell's inequality. In: *40th ACM STOC*. ed. by Richard E. Ladner and Cynthia Dwork. ACM Press, May 2008, pp. 207–216. DOI: `10.1145/1374376.1374408`

Quality: Average I

BKZ

- $\|\mathbf{b}_0\| \approx {\delta_\beta}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$ or
- $\|\mathbf{b}_0\| \approx {\delta_\beta}^{2\cdot(d-1)} \cdot \lambda_1(\Lambda)$

Slide

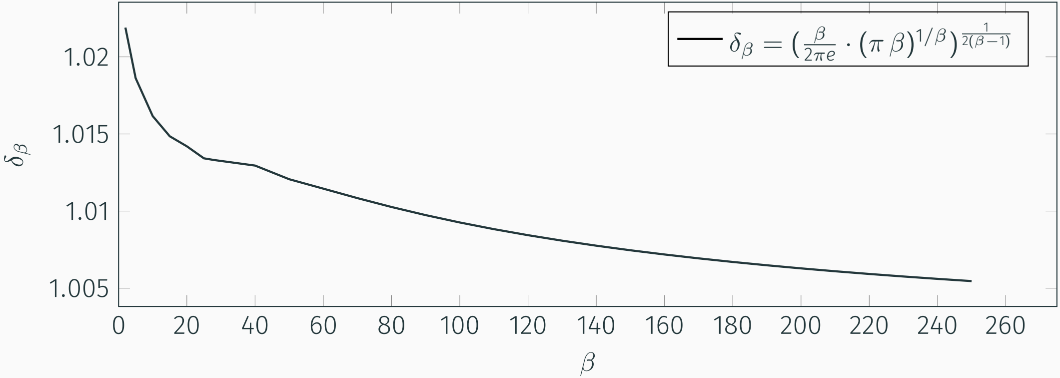
- $\|\mathbf{b}_0\| \approx {\delta_\beta}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$ or
- $\|\mathbf{b}_0\| \approx {\delta_\beta}^{2\cdot(d-\beta)} \cdot \lambda_1(\Lambda)$

β	2	5	24	50	100	200	500
δ_β	1.0219	1.0186	1.0142	1.0121	1.0096	1.0063	1.0034

- We have $\delta_\beta = \mathrm{gh}(\beta)^{1/(\beta-1)}$ for $\beta > 50$.
- The slope under the **Geometric Series Assumption** is

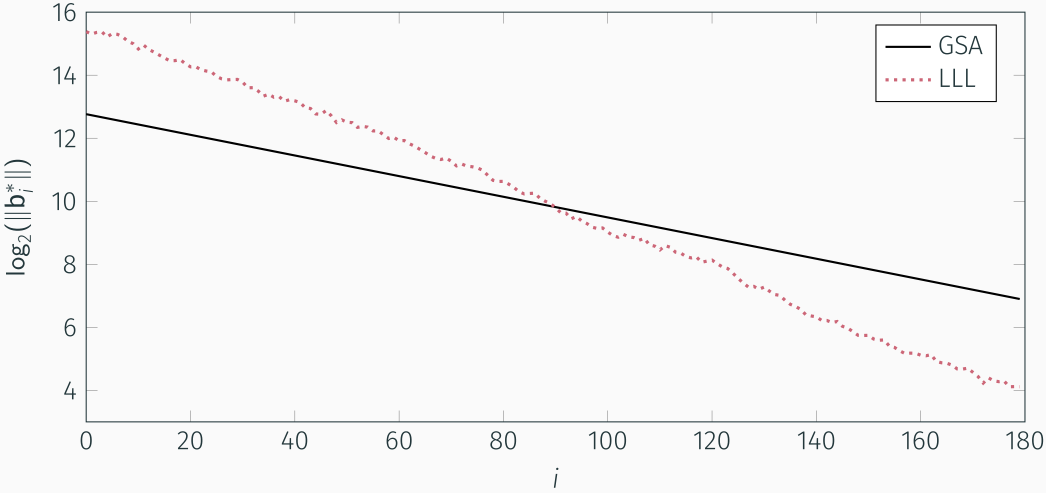
$$\alpha_\beta = \delta_\beta^{-2}.$$

Quality: Average II

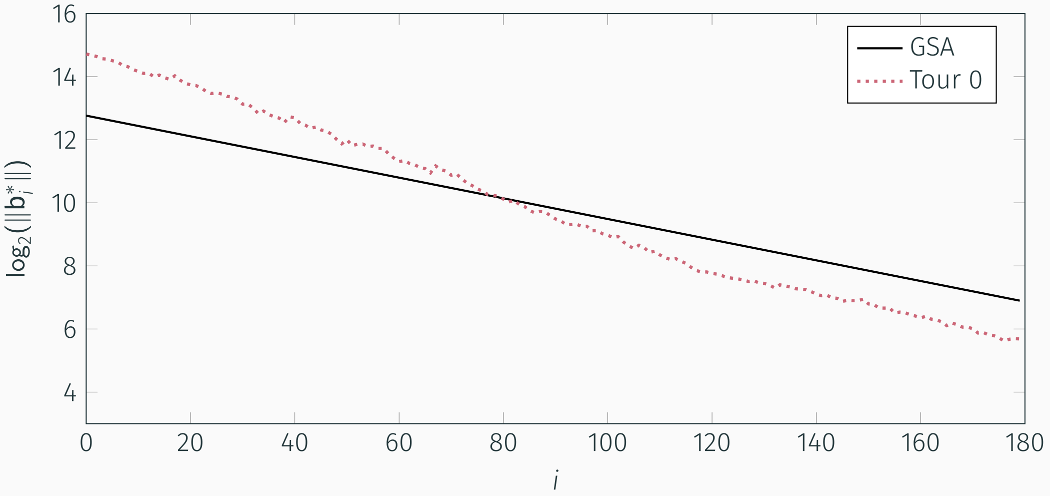


Yuanmi Chen. Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe. PhD thesis. Paris 7, 2013

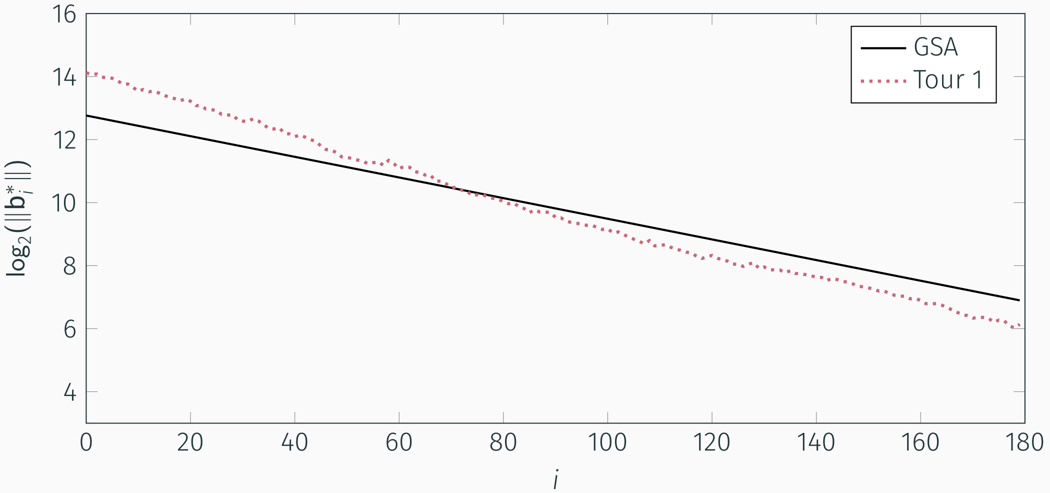
Behaviour in Practice: BKZ-60 in Dimension 180 I



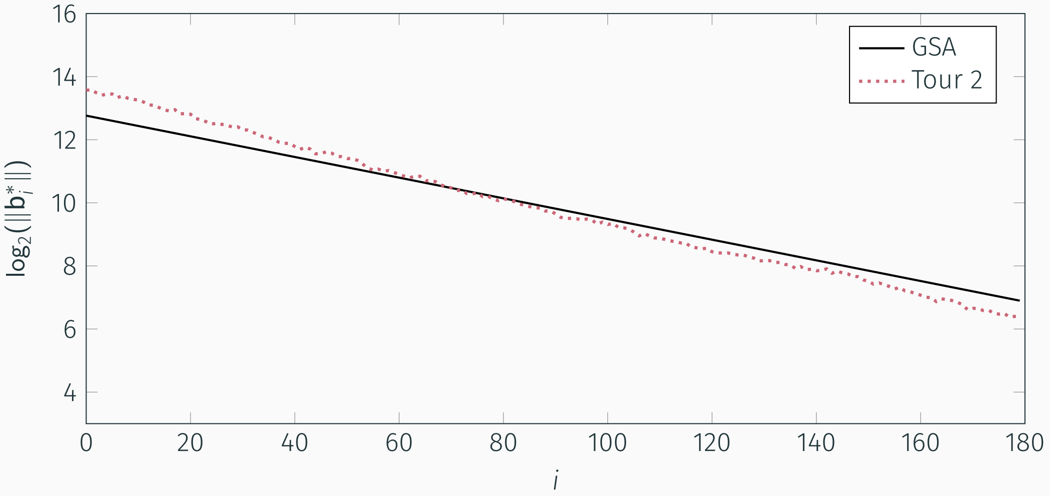
Behaviour in Practice: BKZ-60 in Dimension 180 II



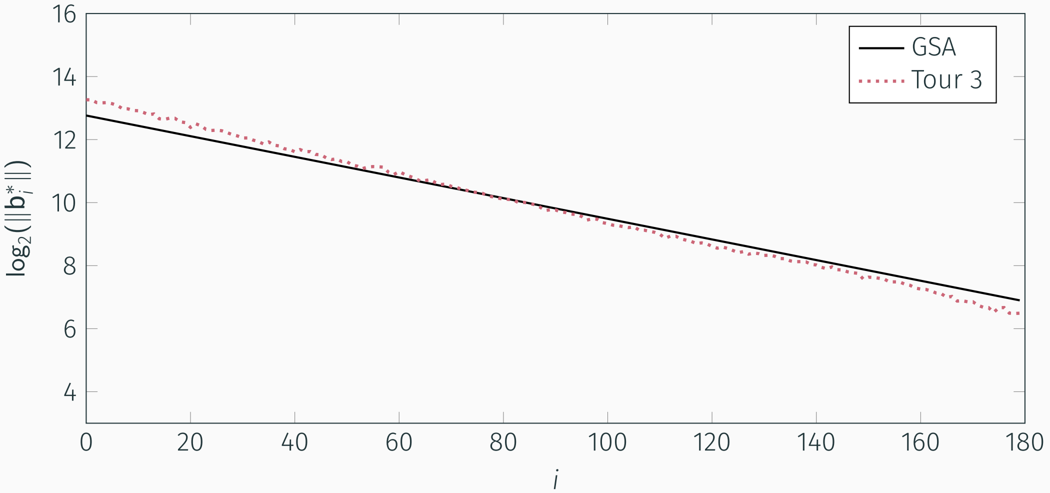
Behaviour in Practice: BKZ-60 in Dimension 180 III



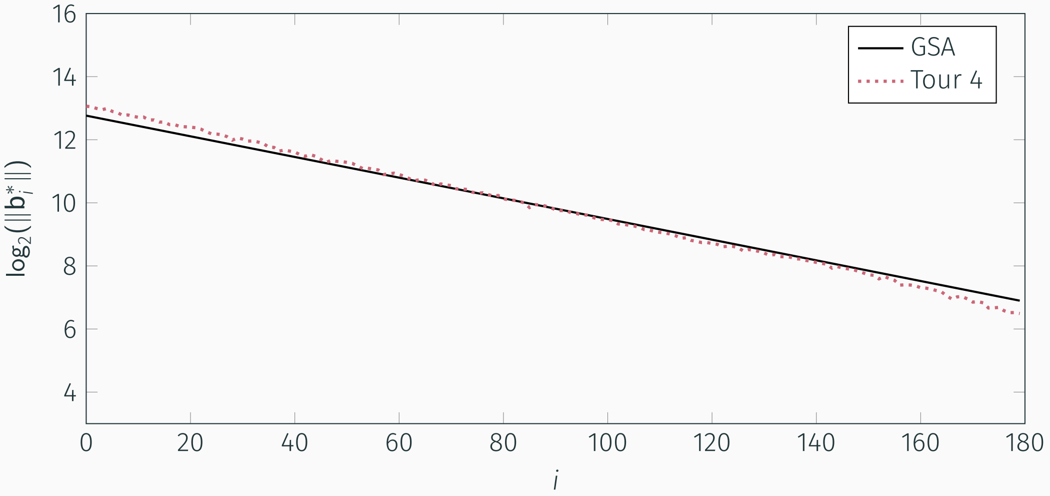
Behaviour in Practice: BKZ-60 in Dimension 180 iv



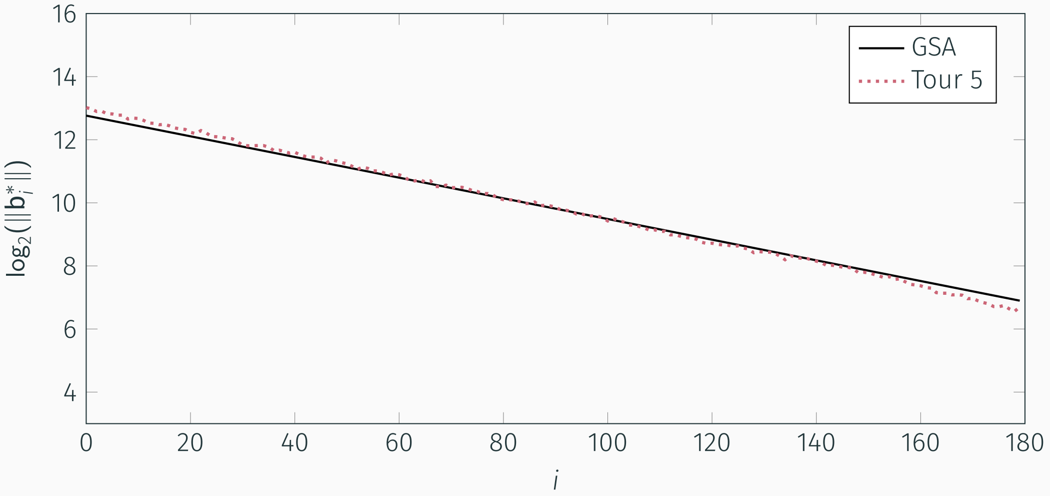
Behaviour in Practice: BKZ-60 in Dimension 180 v

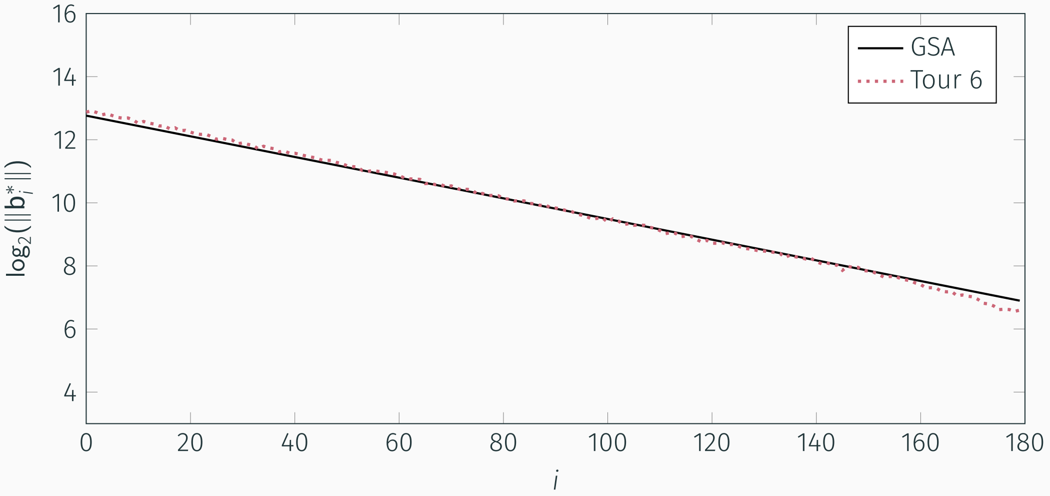


Behaviour in Practice: BKZ-60 in Dimension 180 vi

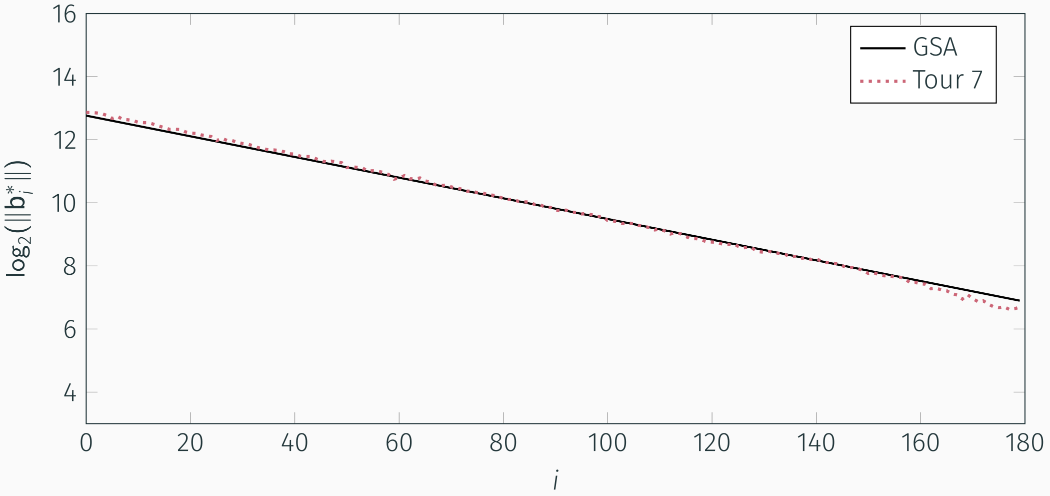


Behaviour in Practice: BKZ-60 in Dimension 180 vii

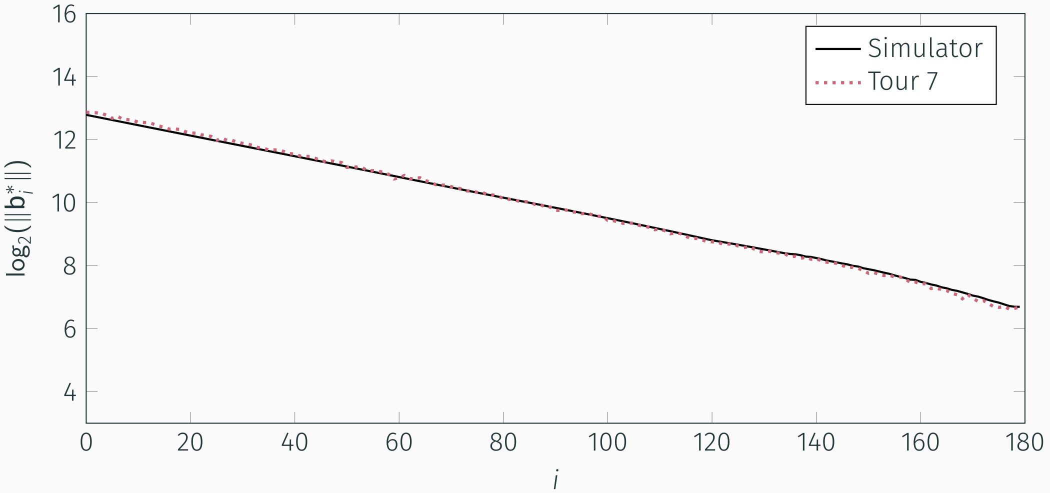



16
14
12
10
8
6
4
0
20
40
60
80
100
120
140
160
180
$\log_2(\|\mathbf{b}_i^*\|)$
i
GSA
Tour 6

Behaviour in Practice: BKZ-60 in Dimension 180 ix



Behaviour in Practice: BKZ-60 in Dimension 180 x



Try it at Home

```
from fpylll import *
from fpylll.algorithms.bkz2 import BKZReduction as BKZ2
A = IntegerMatrix.random(180, "qary", k=90, bits=20)
bkz = BKZ2(A)
bkz(BKZ.EasyParam(block_size=60))
```

`https://github.com/fplll/fplll` C++ library

`https://github.com/fplll/fpylll` Python interface

`https://sagemath.org` FPyLLL is in Sage

`https://sagecell.sagemath.org/` Sage in your browser

`https://cocalc.com/` Sage worksheets in your browser

Success Condition for uSVP (Expectation)

Can decide that $\Lambda = \Lambda(\mathrm{B})$ has unusually short vector when

BKZ

- $\delta_\beta{}^{2\,(d-1)} \cdot \lambda_1(\Lambda) < \delta_\beta{}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < \delta_\beta{}^{-d+1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

Slide

- $\delta_\beta{}^{2\cdot(d-\beta)} \cdot \lambda_1(\Lambda) < \delta_\beta{}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < \delta_\beta{}^{2\beta-d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

Success Condition for uSVP (Expectation)

Can decide that $\Lambda = \Lambda(\mathbf{B})$ has unusually short vector when

BKZ

- ${\delta_\beta}^{2\,(d-1)} \cdot \lambda_1(\Lambda) < {\delta_\beta}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < {\delta_\beta}^{-d+1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

Slide

- ${\delta_\beta}^{2\cdot(d-\beta)} \cdot \lambda_1(\Lambda) < {\delta_\beta}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < {\delta_\beta}^{2\beta-d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

"2016 Estimate"

$$\sqrt{\beta/d} \cdot \|(\mathbf{e} \mid \mathbf{s} \mid 1)\| \approx \sqrt{\beta} \cdot \sigma < \delta_\beta^{2\beta-d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$$

Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343

Success Condition for uSVP (Expectation)

Can decide that $\Lambda = \Lambda(\mathbf{B})$ has unusually short vector when

BKZ

- $\delta_\beta{}^{2\,(d-1)} \cdot \lambda_1(\Lambda) < \delta_\beta{}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < \delta_\beta{}^{-d+1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

Slide

- $\delta_\beta{}^{2\cdot(d-\beta)} \cdot \lambda_1(\Lambda) < \delta_\beta{}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < \delta_\beta{}^{2\beta-d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

"2016 Estimate"

$$\sqrt{\beta/d} \cdot \|(\mathbf{e} \mid \mathbf{s} \mid 1)\| \approx \sqrt{\beta} \cdot \sigma < \delta_\beta^{2\beta-d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$$

Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343

Success Condition for uSVP (Expectation)

Can decide that $\Lambda = \Lambda(\mathbf{B})$ has unusually short vector when

BKZ

- ${\delta_\beta}^{2\,(d-1)} \cdot \lambda_1(\Lambda) < {\delta_\beta}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < {\delta_\beta}^{-d+1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

Slide

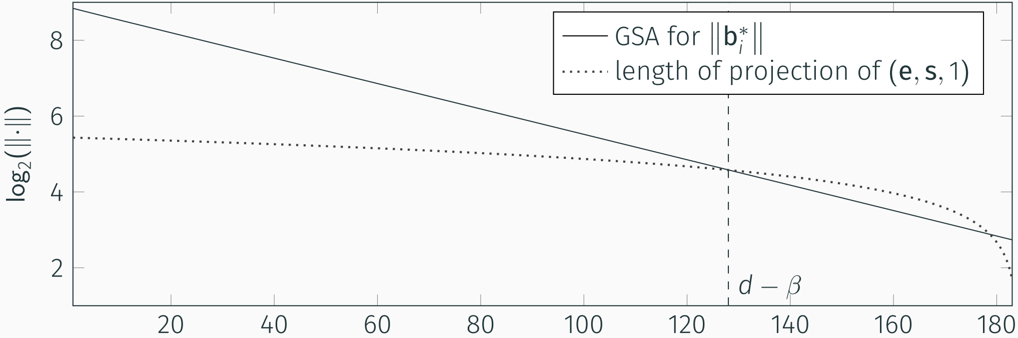
- ${\delta_\beta}^{2\cdot(d-\beta)} \cdot \lambda_1(\Lambda) < {\delta_\beta}^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < {\delta_\beta}^{2\beta-d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

“2016 Estimate”

$$\sqrt{\beta/d} \cdot \|(\mathbf{e} \mid \mathbf{s} \mid 1)\| \approx \sqrt{\beta} \cdot \sigma < \delta_\beta^{2\beta-d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$$

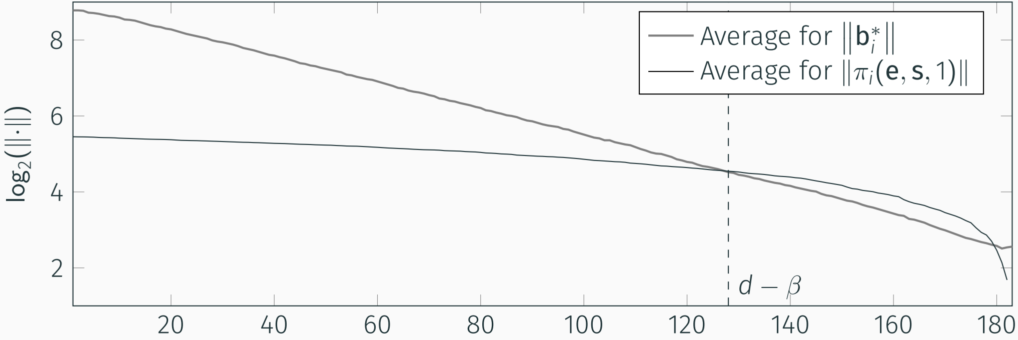
Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343

Success Condition for uSVP (Expectation)



Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343

Success Condition for uSVP (Observed)



Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the Expected Cost of Solving uSVP and Applications to LWE. In: *ASIACRYPT 2017, Part I*. ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10624. LNCS. Springer, Heidelberg, Dec. 2017, pp. 297–322. DOI: `10.1007/978-3-319-70694-8_11`

Solving SVP

Solving SVP

Cost Model \ Scheme	Kyber	NewHope	NTRU HRSS	SNTRU'
$0.292\,\beta$ [1]	180	259	136	155
$1/(2e)\,\beta\log(\beta) - \beta + 16.1$ [2]	456	738	313	370
$1/8\,\beta\log(\beta) - 0.75\beta + 2.3$ [3]	248	416	165	200
$0.265\,\beta$ [1]	163	235	123	140
$1/(4e)\,\beta\log(\beta) - 0.5\beta + 8$	228	369	157	187

Sieving

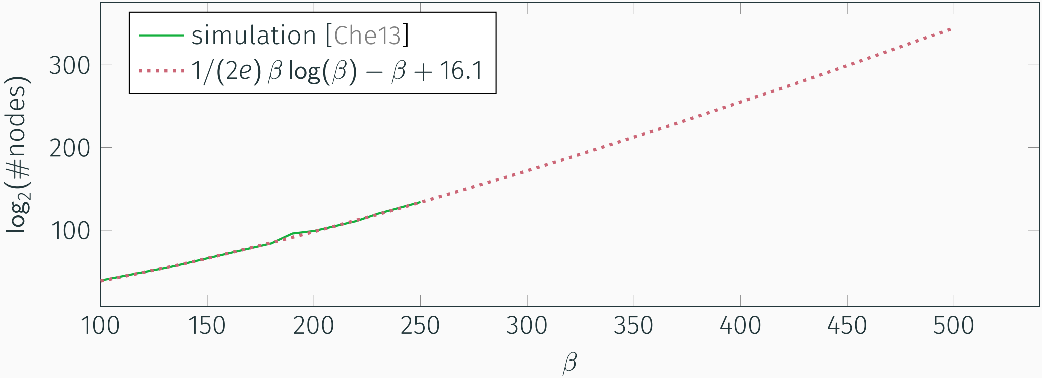
- Produce new, shorter vectors by considering sums and differences of existing vectors
- **Time:** $2^{\Theta(\beta)}$
- **Memory:** $2^{\Theta(\beta)}$

Enumeration

- Search through vectors smaller than a given bound: project down to 1-dim problem, lift to 2-dim problem …
- **Time:** $2^{\Theta(\beta\log\beta)}$
- **Memory:** $\mathrm{poly}(\beta)$

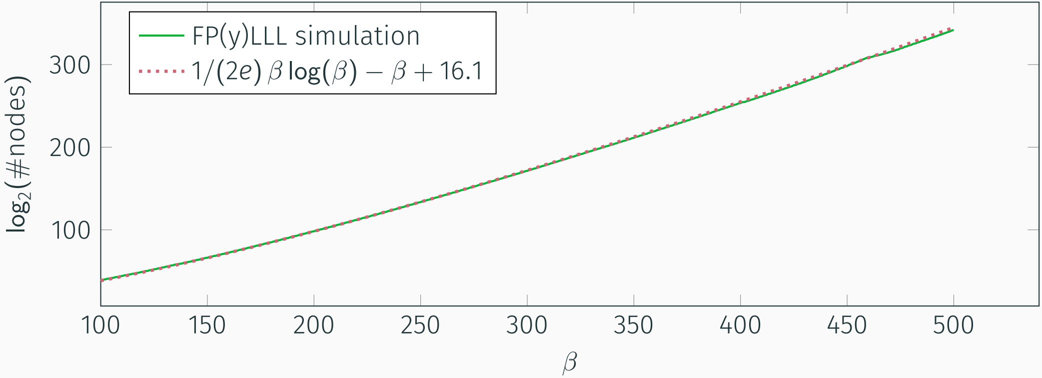
Enumeration Estimates

The $1/(2e)$ estimate extrapolates a dataset from [Che13]



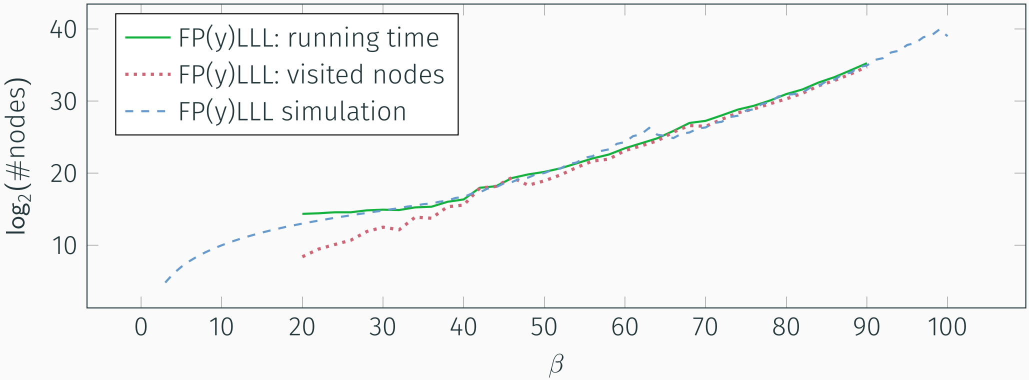
Extended Enumeration Simulation

That estimate compared to our simulation



Enumeration Simulation vs Experiments

Assuming 1 node $\approx$ 100 cpu cycles:



Enumeration Worst-Case Complexity

Cost Model \ Scheme	Kyber	NewHope	NTRU HRSS	SNTRU’
$1/(2e)\,\beta\log(\beta) - \beta + 16.1$	456	738	313	370
$1/8\,\beta\log(\beta) - 0.75\beta + 2.3$	248	416	165	200

“We obtain a new worst-case complexity upper bound, as well as the first worst-case complexity lower bound, both of the order d of $2^{O(d)} \cdot d^{\frac{d}{2e}}$ (up to polynomial factors) bit operations, where d is the rank of the lattice.”[5]

[5] Full version of Guillaume Hanrot and Damien Stehlé. Improved Analysis of Kannan’s Shortest Lattice Vector Algorithm. In: *CRYPTO 2007*. Ed. by Alfred Menezes. Vol. 4622. LNCS. Springer, Heidelberg, Aug. 2007, pp. 170–186. DOI: `10.1007/978-3-540-74143-5_10`, available at `http://perso.ens-lyon.fr/damien.stehle/KANNAN_EXTENDED.html`

Enumeration Heuristic Best-Case Complexity

Cost Model \ Scheme	Kyber	NewHope	NTRU HRSS	SNTRU'
$1/(2e)\,\beta\log(\beta) - \beta + 16.1$	456	738	313	370
$1/8\,\beta\log(\beta) - 0.75\beta + 2.3$	248	416	165	200

"Some authors favor the hypothesis that the average behaviour of an HKZ-reduced basis is rather a geometric decrease of the $\|\mathbf{b}_i^*\|$'s, i.e., roughly $\|\mathbf{b}_i^*\| \approx d^{\frac{i}{d}} \cdot \|\mathbf{b}_1\|$. With such a basis, solving SVP by Kannan's algorithm would have a $2^{O(d)} \cdot d^{\frac{d}{8}}$ complexity."[5]

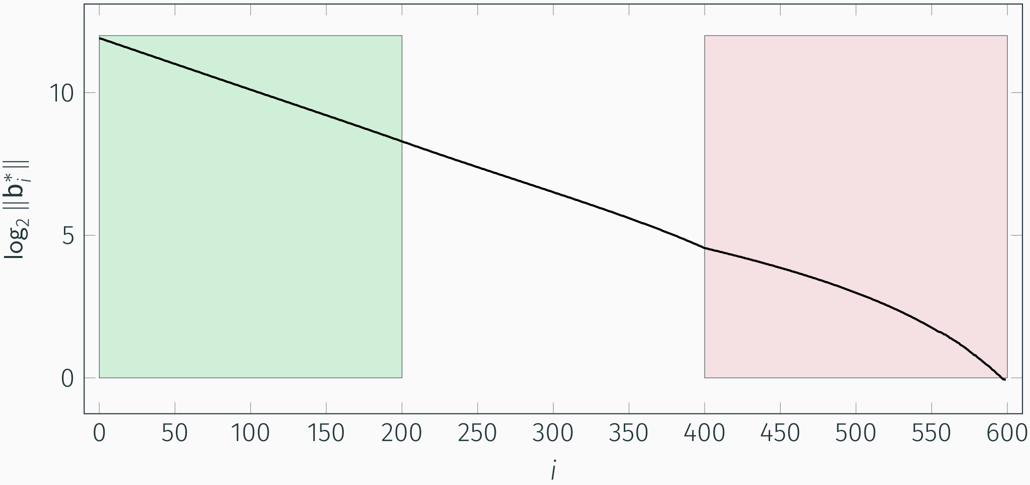
Enumeration Heuristic Best-Case Complexity

Cost Model \ Scheme	Kyber	NewHope	NTRU HRSS	SNTRU'
$1/(2e)\,\beta\log(\beta) - \beta + 16.1$	456	738	313	370
$1/8\,\beta\log(\beta) - 0.75\beta + 2.3$	248	416	165	200

"This suggests that, independently of the quality of the reduced basis, the complexity of enumeration will be at least $d^{\frac{d}{8}}$ polynomial-time operations for many lattices."[6]

[6] Phong Q. Nguyen. Hermite's Constant and Lattice Algorithms. In: ed. by Phong Q. Nguyen and Brigitte Vallée. ISC. Springer, Heidelberg, 2010, pp. 19–69. ISBN: 978-3-642-02294-4. DOI: 10.1007/978-3-642-02295-1.

$1/8 = 0.125$ v $1/(2e) \approx 0.184$

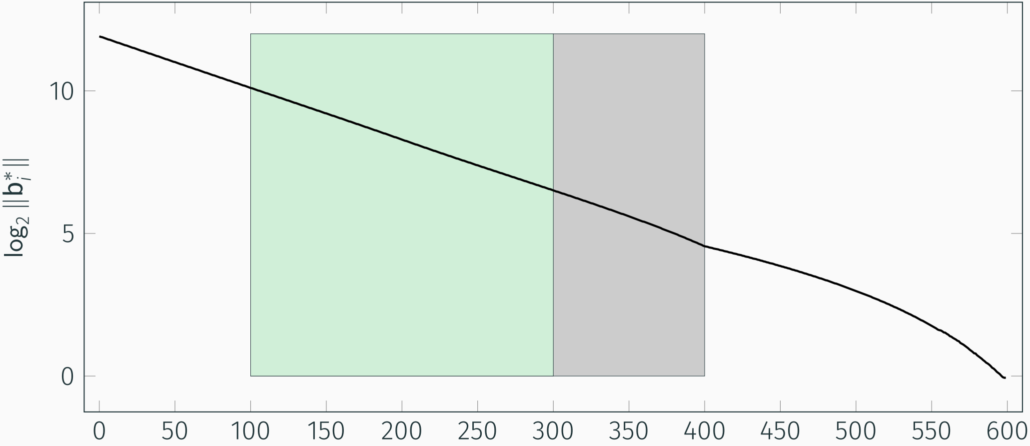


Why we can't have Nice Things

1. We run enumeration many times each succeeding with low probability of success and re-randomise in between: this destroys the nice GSA-line shape
   - Thus, before enumerating a local block, we run some local preprocessing with some block size $\beta' < \beta$
2. In the sandpile model,[7] as the algorithm proceeds through the indices i, a "bump" accumulates from index $i + 1$ onward.

[7] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing Blockwise Lattice Algorithms Using Dynamical Systems. In: *CRYPTO 2011*. Ed. by Phillip Rogaway. Vol. 6841. LNCS. Springer, Heidelberg, Aug. 2011, pp. 447–464. DOI: 10.1007/978-3-642-22792-9_25.

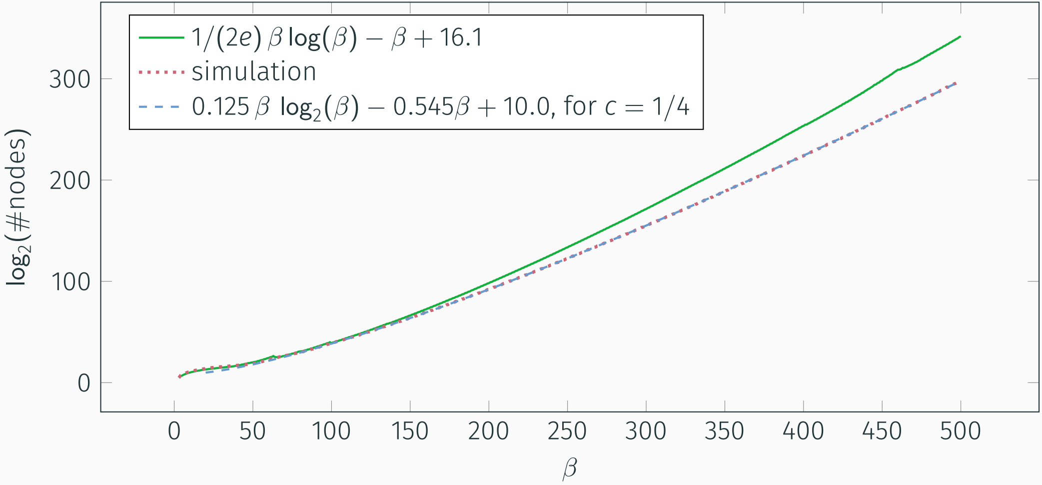
Idea: Overshoot Preprocessing (WIP)



Preprocessing in dimension $(1+c)\cdot\beta$ for enumeration in dimension β.[8]

[8] Joint work with Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé and Weiqiang Wen

Performance (WIP)



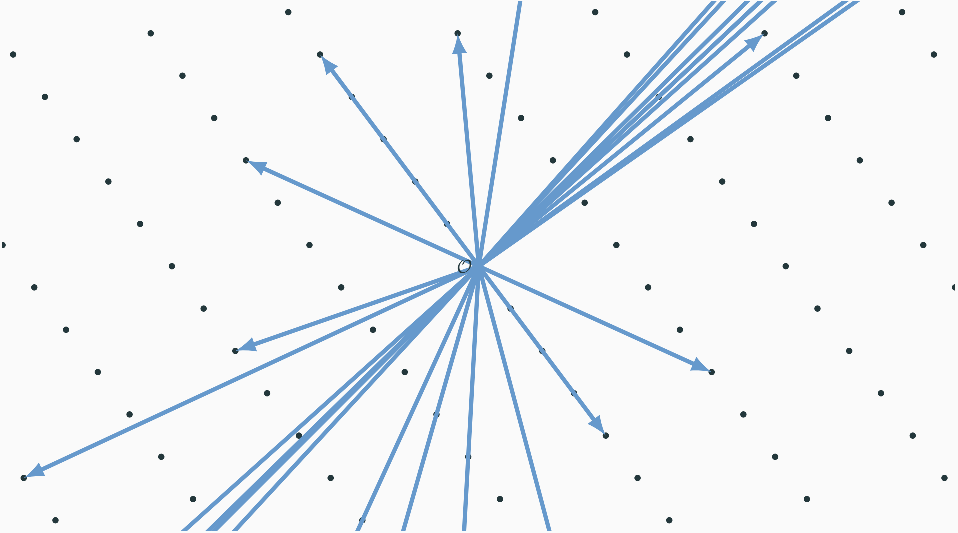
Sieving vs Enumeration

Cost Model \ Scheme	Kyber	NewHope	NTRU HRSS	SNTRU'
$0.292\,\beta$	180	259	136	155
$1/(2e)\,\beta\log(\beta) - \beta + 16.1$	456	738	313	370
$1/8\,\beta\log(\beta) - 0.75\beta + 2.3$	248	416	165	200

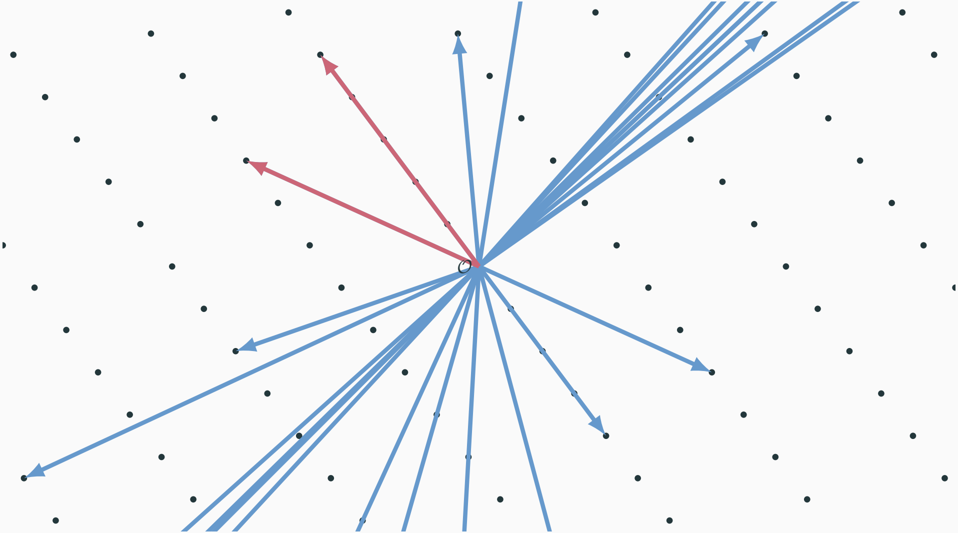
Crossover

Sieving is asymptotically faster than enumeration, but does it beat enumeration in practical or cryptographic dimensions?

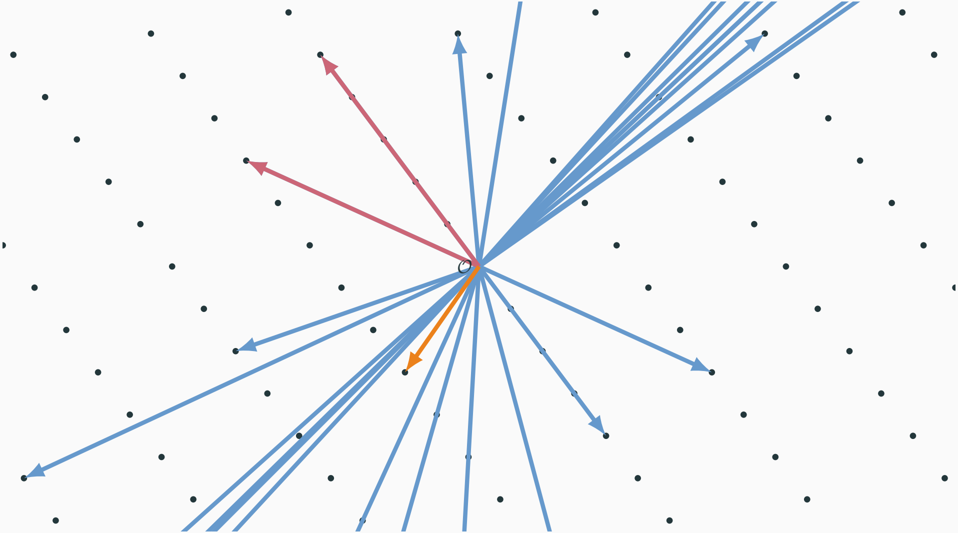
Sieving: Key Ideas I



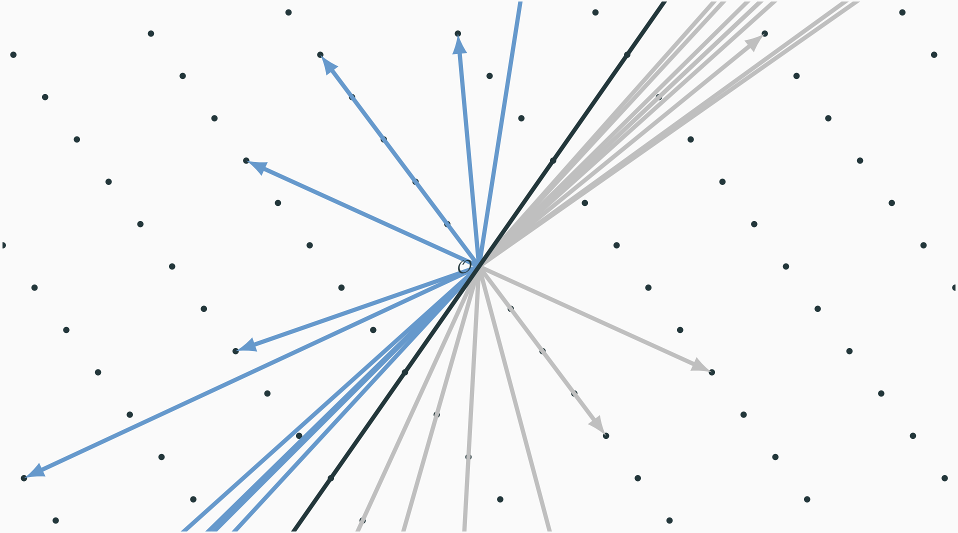
Sieving: Key Ideas II



Sieving: Key Ideas III



Sieving: Popcount I



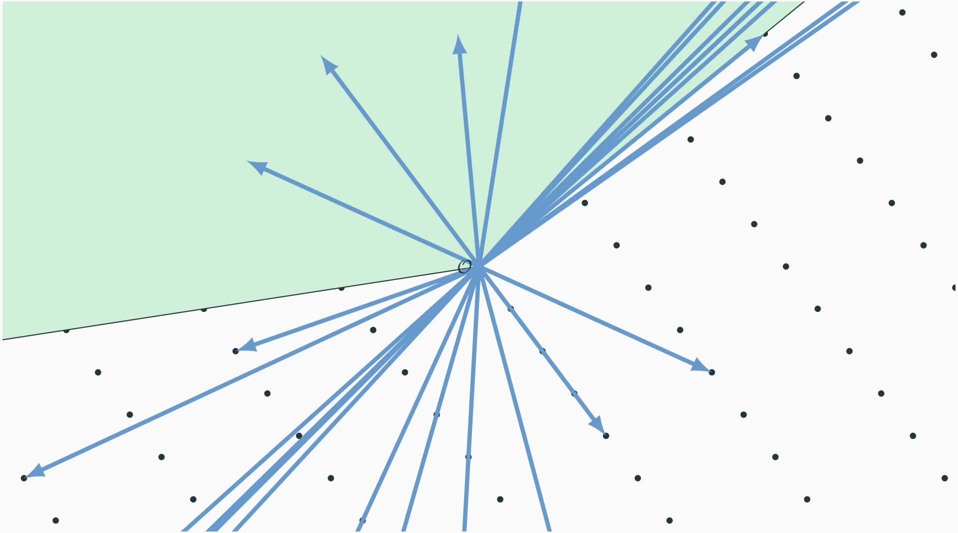
Sieving: Popcount II

- For a given plane, denote a vector being on the “left” as 0, being on the “right” as 1.
- This defines a 1-bit locality sensitive hash (LSH) function.
- Consider many such hash functions and concatenate their output.
- Two vectors are close if they agree on many bits of their hashes

Comparison Operation

XOR hash values and compute Hamming weight (“popcount”).

Sieving: Buckets



Sieving: Some Algorithms

Gauss Sample $(4/3)^{\beta/2+o(\beta)}$ vectors, compare them pairwise if they reduce to something shorter. **Cost**: $(4/3)^{\beta+o(\beta)} \approx 2^{0.41\,\beta+o(\beta)}$.[9]

BGJ Split search space into “buckets”. **Cost**: $2^{0.311\,\beta+o(\beta)}$.[10]

BDGL Use codes to decide which bucket to consider. **Cost**: $2^{0.292\,\beta+o(\beta)}$.[11]

---

[9] Daniele Micciancio and Panagiotis Voulgaris. Faster Exponential Time Algorithms for the Shortest Vector Problem. In: *21st SODA*. ed. by Moses Charika. ACM-SIAM, Jan. 2010, pp. 1468–1480. DOI: `10.1137/1.9781611973075.119`.

[10] Anja Becker, Nicolas Gama, and Antoine Joux. Speeding-up lattice sieving without increasing the memory, using sub-quadratic nearest neighbor search. Cryptology ePrint Archive, Report 2015/522. `https://eprint.iacr.org/2015/522`. 2015.

[11] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In: *27th SODA*. ed. by Robert Krauthgamer. ACM-SIAM, Jan. 2016, pp. 10–24. DOI: `10.1137/1.9781611974331.ch2`.

Sieving: G6K

G6K[12] is a Python/C++ framework for experimenting with sieving algorithms (inside and outside BKZ)

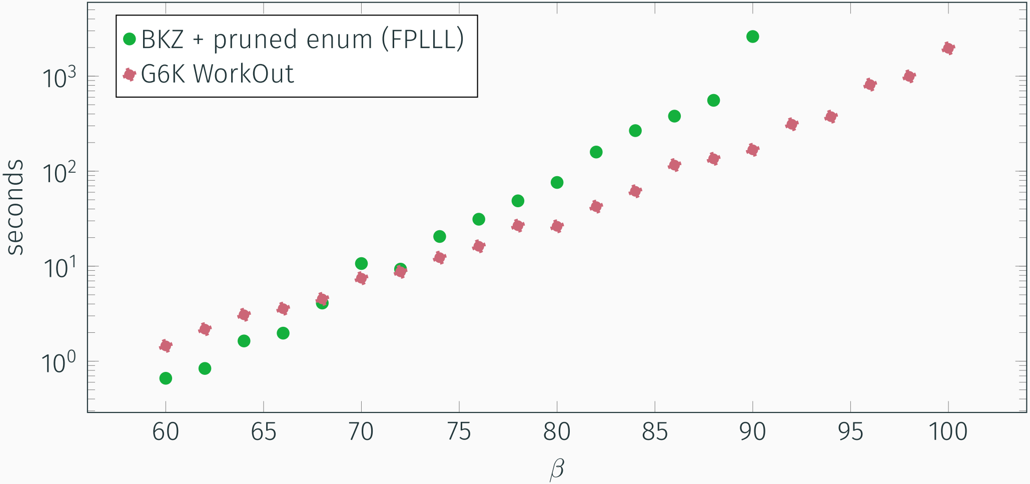
- Does not take the "oracle" view but considers sieves as stateful machines.
- Implements several sieve algorithms[13] (but not BDGL)
- Applies recent tricks and adds new tricks for improving performance of sieving

---

[12] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. The General Sieve Kernel and New Records in Lattice Reduction. In: *EUROCRYPT 2019, Part II*. ed. by Yuval Ishai and Vincent Rijmen. Vol. 11477. LNCS. Springer, Heidelberg, May 2019, pp. 717–746. DOI: 10.1007/978-3-030-17656-3_25.

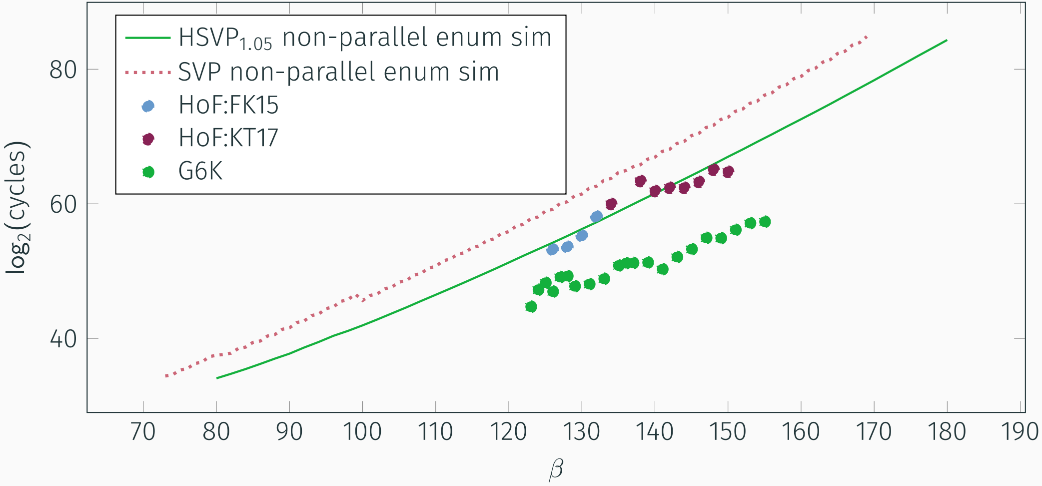
[13] Gauss, NV, BGJ1 (BGJ with one level of filtration)

Sieving: SVP



Average time in seconds for solving exact SVP

Darmstadt HSVP$_{1.05}$ Challenges



Estimated and reported costs for solving Darmstadt SVP Challenges.

Try it at Home

```python
from fpylll import IntegerMatrix, GSO, LLL
from fpylll.tools.bkz_stats import dummy_tracer
from g6k import Siever
from g6k.algorithms.bkz import pump_n_jump_bkz_tour

A = LLL.reduction(IntegerMatrix.random(180, "qary", k=90, bits=20))
g6k = Siever(A)

for b in range(20, 60+1, 10):
    pump_n_jump_bkz_tour(g6k, dummy_tracer, b, pump_params={"down_sieve": True})
```

`https://github.com/fplll/g6k` C++ kernel + Python frontend

Practical Sieving: Open Questions

- Parallelism in non-uniform memory access (NUMA) architectures
- Practical performance of asymptotically faster sieves
- Dedicated hardware . . .

Quantum Estimates

Type	Cost Model \ Scheme	Kyber	NewHope	NTRU HRSS	SNTRU’
classical	$0.292\,\beta$	180	259	136	155
quantum	$0.265\,\beta$	163	235	123	140
classical	$1/(2e)\,\beta\log(\beta) - \beta + 16.1$	456	738	313	370
quantum	$1/(4e)\,\beta\log(\beta) - 0.5\beta + 8$	228	369	157	187

Sieving Given some vector $\mathbf{w}$ and a list of vectors L, apply Grover’s algorithm to find $\{\mathbf{v} \in L \text{ s.t. } \|\mathbf{v} \pm \mathbf{w}\| \leq \|\mathbf{w}\|\}$.[14]

Enumeration Apply Montanaro’s quantum backtracking algorithm for quadratic speed-up.[15]

[14] Thijs Laarhoven. Search problems in cryptography: From fingerprinting to lattice sieving. PhD thesis. Eindhoven University of Technology, 2015.

[15] Yoshinori Aono, Phong Q. Nguyen, and Yixin Shen. Quantum Lattice Enumeration and Tweaking Discrete Pruning. Cryptology ePrint Archive, Report 2018/546. `https://eprint.iacr.org/2018/546`. 2018.

Quantum Sieving

- A quantum sieve needs list of $2^{0.2075\beta}$ vectors before pairwise search with Grover
- Fast sieves use that the search is structured, Grover does unstructured search
  - Quantum Gauss Sieve

$$2^{(0.2075+\frac{1}{2}0.2075)\,\beta+o(\beta)} = 2^{0.311\,\beta+o(\beta)} \text{ time}, \qquad 2^{0.2075\,\beta+o(\beta)} \text{ memory}$$

  - Classical BGJ Sieve[16]

$$2^{0.311\,\beta+o(\beta)} \text{ time}, \qquad 2^{0.2075\,\beta+o(\beta)} \text{ memory}$$

- Asymptotically fastest sieves have small lists and thus less Grover speed-up potential

[16] Anja Becker, Nicolas Gama, and Antoine Joux. Speeding-up lattice sieving without increasing the memory, using sub-quadratic nearest neighbor search. Cryptology ePrint Archive, Report 2015/522. `https://eprint.iacr.org/2015/522`. 2015.

Implementing Quantum Algorithms for SVP

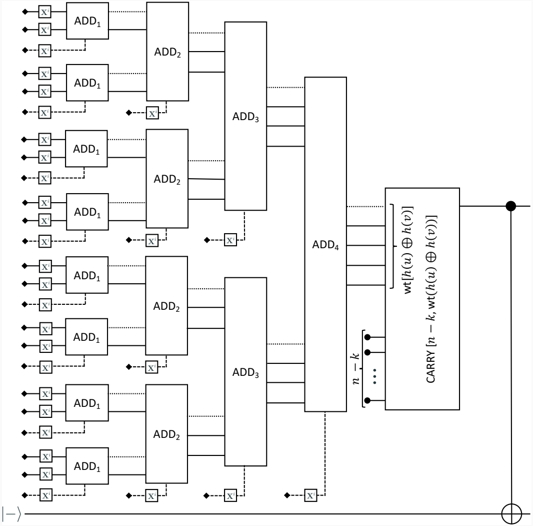
Sieving

- Major operation is to check whether two vectors reduce to some smaller vector
- Can be implemented using the XOR and popcount trick $\Rightarrow$ the quantum circuit is relatively small.
- Sieving requires exponentially large quantum accessible RAM (qRAM). Not clear that this can be built efficiently (due to error correction being required).

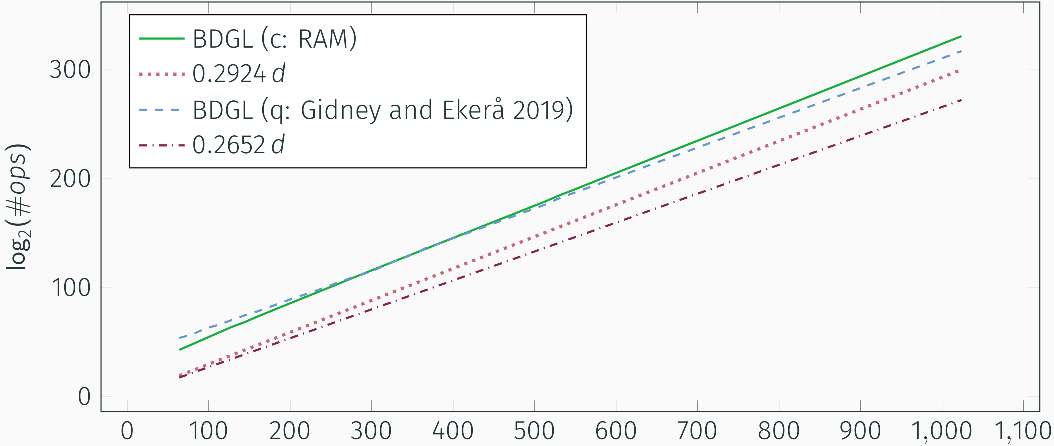
Enumeration

- Enumeration requires higher precision floating point arithmetic.
- Quantum circuit for enumeration is likely to be larger than for sieving.
- But no exponential qRAM.

Implementing Quantum Algorithms for SVP: Sieving



Implementing Quantum Algorithms for SVP: Sieving (Underestimates)



Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, and John M. Schanck. Quantum speedups for lattice sieves are tenuous at best. Cryptology ePrint Archive, Report 2019/1161. `https://eprint.iacr.org/2019/1161`. 2019

Quantum Algorithms Open Problems

- A quantum circuit for enumeration.
- Better algorithms than best classical + Grover.

A Word on Lower Bounds

Cost Model \ Scheme	Kyber	NewHope	NTRU HRSS	SNTRU'
$0.292\,\beta$	180	259	136	155
$1/(2e)\,\beta\log(\beta) - \beta + 16.1$	456	738	313	370
$1/8\,\beta\log(\beta) - 0.75\beta + 2.3$	248	416	165	200
$0.265\,\beta$	163	235	123	140
$1/(4e)\,\beta\log(\beta) - 0.5\beta + 8$	228	369	157	187

These estimates ignore:

- (large) polynomial factors hidden in $o(\beta)$
- MAXDEPTH of quantum computers
- cost of a Grover iteration
- cost of memory (access)

Thus:

- cannot claim parameters need to be adjusted when these estimates are lowered
- careful about conclusions drawn: some attacks don't work here but work in practice

Alternative Approaches

BKW combinatorial technique, relatively efficient for small secrets

Arora-Ge use Gröbner bases, asymptotically efficient , but large constants in the exponent

Hybrid Attack combine combinatorial techniques with lattice reduction

Rule of Thumb

Don’t need to worry about these unless secret is unusually small (e.g. ternary) and/or sparse.

THANK YOU

[Alb+17] Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the Expected Cost of Solving uSVP and Applications to LWE. In: *ASIACRYPT 2017, Part I*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10624. LNCS. Springer, Heidelberg, Dec. 2017, pp. 297–322. DOI: 10.1007/978-3-319-70694-8_11.

[Alb+18] Martin R. Albrecht, Benjamin R. Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W. Postlethwaite, Fernando Virdia, and Thomas Wunderer. Estimate All the LWE, NTRU Schemes! In: *SCN 18*. Ed. by Dario Catalano and Roberto De Prisco. Vol. 11035. LNCS. Springer, Heidelberg, Sept. 2018, pp. 351–367. DOI: 10.1007/978-3-319-98113-0_19.

[Alb+19a] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. The General Sieve Kernel and New Records in Lattice Reduction. In: *EUROCRYPT 2019, Part II*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11477. LNCS. Springer, Heidelberg, May 2019, pp. 717–746. DOI: 10.1007/978-3-030-17656-3_25.

[Alb+19b] Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, and John M. Schanck. Quantum speedups for lattice sieves are tenuous at best. Cryptology ePrint Archive, Report 2019/1161. https://eprint.iacr.org/2019/1161. 2019.

[Alk+16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343.

[ANS18] Yoshinori Aono, Phong Q. Nguyen, and Yixin Shen. Quantum Lattice Enumeration and Tweaking Discrete Pruning. Cryptology ePrint Archive, Report 2018/546. https://eprint.iacr.org/2018/546. 2018.

References II

[APS15] Martin R. Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of Learning with Errors. In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203.

[Bec+16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In: *27th SODA*. Ed. by Robert Krauthgamer. ACM-SIAM, Jan. 2016, pp. 10–24. DOI: 10.1137/1.9781611974331.ch2.

[BGJ15] Anja Becker, Nicolas Gama, and Antoine Joux. Speeding-up lattice sieving without increasing the memory, using sub-quadratic nearest neighbor search. Cryptology ePrint Archive, Report 2015/522. https://eprint.iacr.org/2015/522. 2015.

[Che13] Yuanmi Chen. Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe. PhD thesis. Paris 7, 2013.

[GN08] Nicolas Gama and Phong Q. Nguyen. Finding short lattice vectors within Mordell's inequality. In: *40th ACM STOC*. Ed. by Richard E. Ladner and Cynthia Dwork. ACM Press, May 2008, pp. 207–216. DOI: 10.1145/1374376.1374408.

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing Blockwise Lattice Algorithms Using Dynamical Systems. In: *CRYPTO 2011*. Ed. by Phillip Rogaway. Vol. 6841. LNCS. Springer, Heidelberg, Aug. 2011, pp. 447–464. DOI: 10.1007/978-3-642-22792-9_25.

[HS07] Guillaume Hanrot and Damien Stehlé. Improved Analysis of Kannan's Shortest Lattice Vector Algorithm. In: *CRYPTO 2007*. Ed. by Alfred Menezes. Vol. 4622. LNCS. Springer, Heidelberg, Aug. 2007, pp. 170–186. DOI: 10.1007/978-3-540-74143-5_10.

[Laa15] Thijs Laarhoven. Search problems in cryptography: From fingerprinting to lattice sieving. PhD thesis. Eindhoven University of Technology, 2015.

[MV10] Daniele Micciancio and Panagiotis Voulgaris. Faster Exponential Time Algorithms for the Shortest Vector Problem. In: *21st SODA*. Ed. by Moses Charika. ACM-SIAM, Jan. 2010, pp. 1468–1480. DOI: 10.1137/1.9781611973075.119.

[Ngu10] Phong Q. Nguyen. Hermite's Constant and Lattice Algorithms. In: ed. by Phong Q. Nguyen and Brigitte Vallée. ISC. Springer, Heidelberg, 2010, pp. 19–69. ISBN: 978-3-642-02294-4. DOI: 10.1007/978-3-642-02295-1.

[Pho+17] Le Trieu Phong, Takuya Hayashi, Yoshinori Aono, and Shiho Moriai. LOTUS. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions. National Institute of Standards and Technology, 2017.

[Sch03] Claus-Peter Schnorr. Lattice Reduction by Random Sampling and Birthday Methods. In: *STACS 2003, 20th Annual Symposium on Theoretical Aspects of Computer Science, Berlin, Germany, February 27 - March 1, 2003, Proceedings*. Ed. by Helmut Alt and Michel Habib. Vol. 2607. Lecture Notes in Computer Science. Springer, 2003, pp. 145–156. DOI: 10.1007/3-540-36494-3_14. URL: http://dx.doi.org/10.1007/3-540-36494-3_14.

[SE94] Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. In: *Math. Program.* 66 (1994), pp. 181–199. DOI: 10.1007/BF01581144. URL: https://doi.org/10.1007/BF01581144.