Introduction to Lattice Cryptanalysis (of LWE)

Martin R. Albrecht

Workshop on Foundations and Applications of Lattice-based Cryptography 2022 @ ICMS

Introduction

Learning with Errors

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

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

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 for q-ary Lattices

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 for q-ary Lattices

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

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

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

Decision Variant

Decide if B has an unusually short vector.

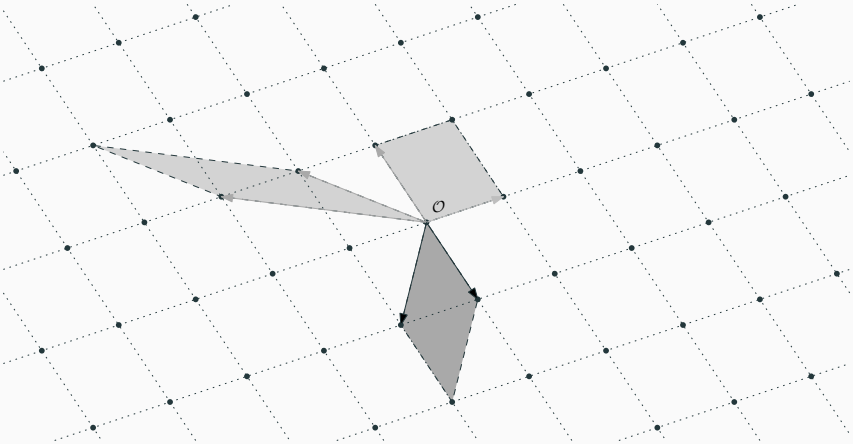
NTRU

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 der Pol

Gaussian Heuristic

- The Gaussian heuristic predicts that the number $|\Lambda \cap \mathcal{B}|$ of lattice points inside a measurable body $\mathcal{B} \subset \mathbb{R}^d$ is approximately equal to $\mathrm{Vol}(\mathcal{B})/\mathrm{Vol}(\Lambda)$.
- Applied to Euclidean d-balls, this means that a shortest vector in a 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 $\lambda_1(\Lambda) \ll \sqrt{\frac{d}{2\pi e}} \cdot \mathrm{Vol}(\Lambda)^{1/d}$.

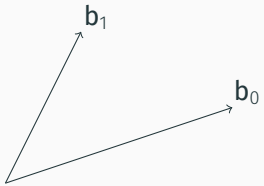
Length of Gram–Schmidt Vectors

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 $\mathbf{b}_0, \ldots, \mathbf{b}_{i-1}$.

We have $\mathrm{Vol}(\Lambda) = \prod_{i=0}^{d-1} \|\mathbf{b}_i^*\|$.



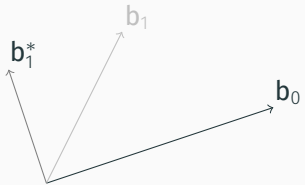
Length of Gram–Schmidt Vectors

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 $\mathbf{b}_0, \ldots, \mathbf{b}_{i-1}$.

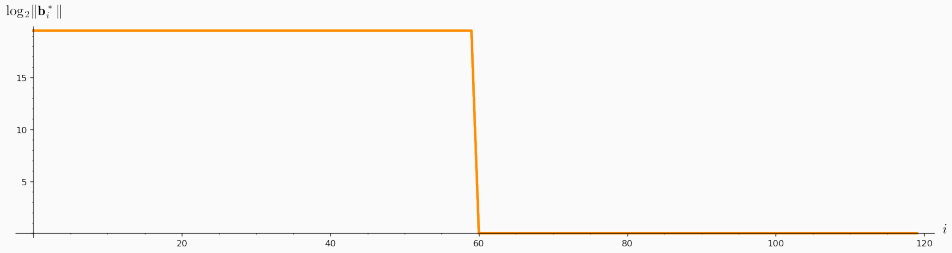
Informally, this means taking out the contributions in the directions of previous vectors $\mathbf{b}_0, \ldots, \mathbf{b}_{i-1}$.

We have $\mathrm{Vol}(\Lambda) = \prod_{i=0}^{d-1} \|\mathbf{b}_i^*\|$.



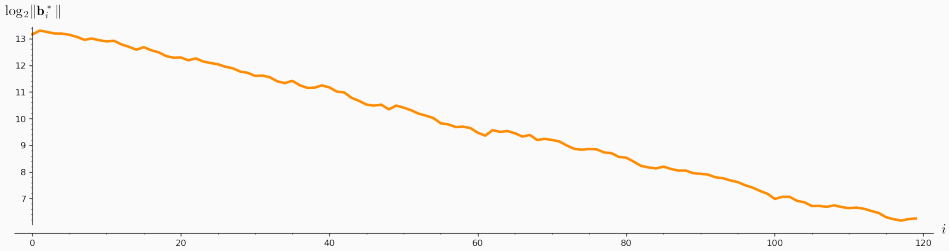
Example

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



Example - LLL

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



LLL: Definitions / Intuition

- Let $\{\mathbf{b}_0, \ldots, \mathbf{b}_{d-1}\}$ be a basis $\mathbf{B}$ for a lattice Λ.
- Denote by $\{\mathbf{b}_0^*, \ldots, \mathbf{b}_{d-1}^*\}$ be the corresponding Gram–Schmidt orthogonal basis and for $0 \leq j < i < d$ let $\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle$.
- An (ordered) basis is **LLL reduced** if:
  - It is **size reduced**, i.e.

$$|\mu_{i,j}| \leq 1/2 \text{ for } 0 \leq j < i < d.$$

  - The **Lovász condition** holds: for $1 \leq i < d$ and $\delta \in (1/4, 1)$

$$\|\mathbf{b}_i^*\|^2 \geq \left(\delta - \mu_{i,i-1}^2\right) \cdot \|\mathbf{b}_{i-1}^*\|^2$$

Intuition for Lovász Condition

- We know that $\det(\Lambda) = \prod_i \mathbf{b}_i^*$ is invariant.
- If $\mathbf{b}_i^*$ is not much smaller than $\mathbf{b}_{i-1}^*$ then we "moved" some of the contributions of $\mathbf{b}_j^*$ for $j < i$ to $\mathbf{b}_i^*$.
- Since $\mathbf{b}_0 = \mathbf{b}_0^*$ this means that we are also producing a shorter vector $\mathbf{b}_0$.

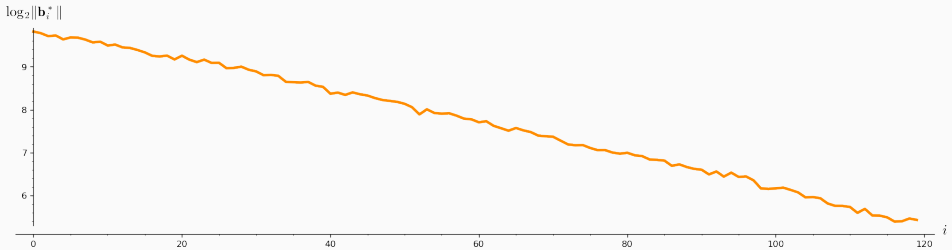
LLL: Algorithm / Guarantees

Data: Lattice basis $\mathbf{B}$
Data: Parameter $\delta \in (1/4, 1)$
$k \leftarrow 1$;
repeat *until* $k \geq d$
  for $j \leftarrow k-1$ **to** 0 **do**
    $\mathbf{b}_k \leftarrow \mathbf{b}_k - \lfloor \mu_{k,j} \rceil \cdot \mathbf{b}_j$;
  end
  if $\|\mathbf{b}_k^*\|^2 \geq (\delta - \mu_{k,j-1}^2) \cdot \|\mathbf{b}_{k-1}^*\|^2$ **then**
    $k \leftarrow k+1$;
  else
    swap $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$;
    $k \leftarrow k-1$;
  end

An LLL-reduced basis satisfies:

- $\|\mathbf{b}_0\| \leq 2^{(d-1)/4} \cdot \mathrm{Vol}(\Lambda)^{1/d}$ and
- $\|\mathbf{b}_0\| \leq 2^{(d-1)/2} \cdot \|\lambda_1(\Lambda)\|$.

GSA



Geometric Series Assumption: The shape after lattice reduction is a line with a flatter slope as lattice reduction gets stronger.[1]

[1] 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.

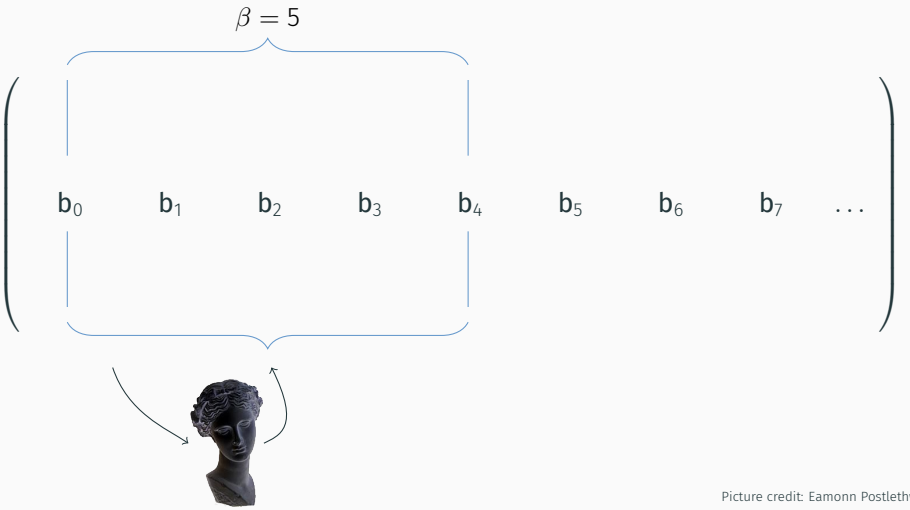
Strong Lattice Reduction: BKZ Algorithm (Block 0)

$$\beta = 5$$

$$\begin{pmatrix} \mathbf{b}_0 & \mathbf{b}_1 & \mathbf{b}_2 & \mathbf{b}_3 & \mathbf{b}_4 & \mathbf{b}_5 & \mathbf{b}_6 & \mathbf{b}_7 & \dots \end{pmatrix}$$

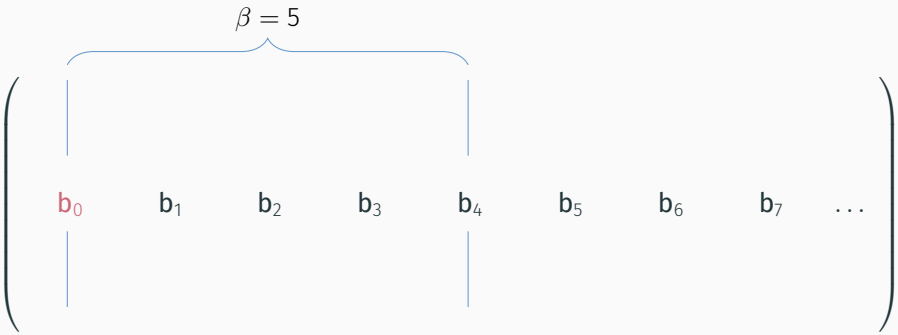
Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm (Block 0)



Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm (Block 0)



Picture credit: Eamonn Postlethwaite

Strong Lattice Reduction: BKZ Algorithm (Block 1)

$$\beta = 5$$

$$\begin{pmatrix} \mathbf{b}_0 & \pi_0(\mathbf{b}_1) & \pi_0(\mathbf{b}_2) & \pi_0(\mathbf{b}_3) & \pi_0(\mathbf{b}_4) & \pi_0(\mathbf{b}_5) & \mathbf{b}_6 & \mathbf{b}_7 & \dots \end{pmatrix}$$

$\pi_i(\mathbf{v})$: project $\mathbf{v}$ orthogonally to $\mathbf{b}_0, \dots, \mathbf{b}_i$

Strong Lattice Reduction: BKZ Algorithm (Block 1)

$\beta = 5$

$$\begin{pmatrix} \mathbf{b}_0 & \pi_0(\mathbf{b}_1) & \pi_0(\mathbf{b}_2) & \pi_0(\mathbf{b}_3) & \pi_0(\mathbf{b}_4) & \pi_0(\mathbf{b}_5) & \mathbf{b}_6 & \mathbf{b}_7 & \dots \end{pmatrix}$$

$\pi_i(\mathbf{v})$: project $\mathbf{v}$ orthogonally to $\mathbf{b}_0, \dots, \mathbf{b}_i$

Strong Lattice Reduction: BKZ Algorithm (Block 1)

$$\beta = 5$$

$$\begin{pmatrix} \mathbf{b}_0 & \pi_0(\mathbf{b}_1) & \pi_0(\mathbf{b}_2) & \pi_0(\mathbf{b}_3) & \pi_0(\mathbf{b}_4) & \pi_0(\mathbf{b}_5) & \mathbf{b}_6 & \mathbf{b}_7 & \dots \end{pmatrix}$$

$\pi_i(\mathbf{v})$: project $\mathbf{v}$ orthogonally to $\mathbf{b}_0, \dots, \mathbf{b}_i$

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	n
$\gamma_\beta^{\frac{1}{2(\beta-1)}}$	1.074	1.059	1.059	1.053	1.052	1.050	1.050	1.031	$\leq \sqrt{2}\,\mathrm{GH}(n)$

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

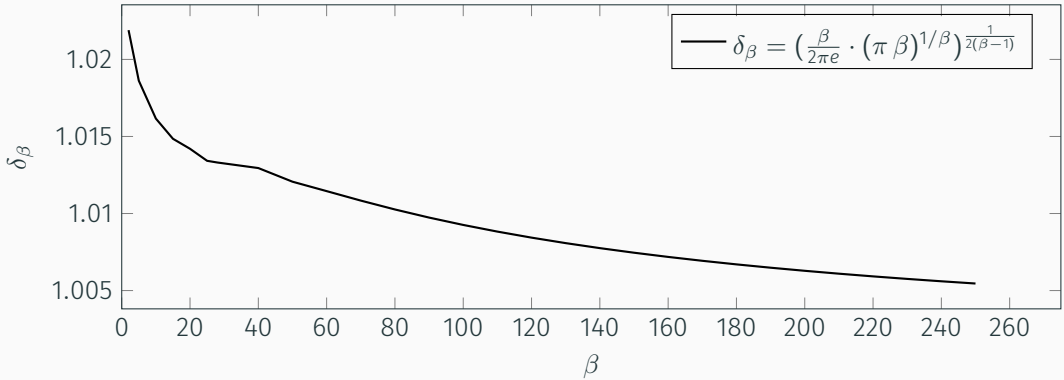
- $\|\mathbf{b}_0\| \approx \delta_\beta^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$ or
- $\|\mathbf{b}_0\| \approx \delta_\beta^{2\cdot(d-\beta)} \cdot \lambda_1(\Lambda)$

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

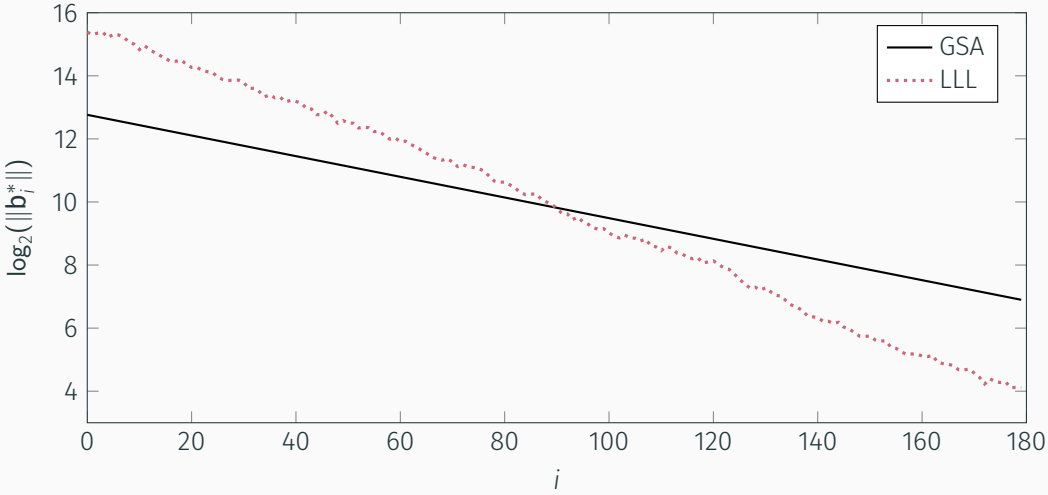
$$\alpha_\beta = \delta_\beta^{-2}.$$

Quality: Average II

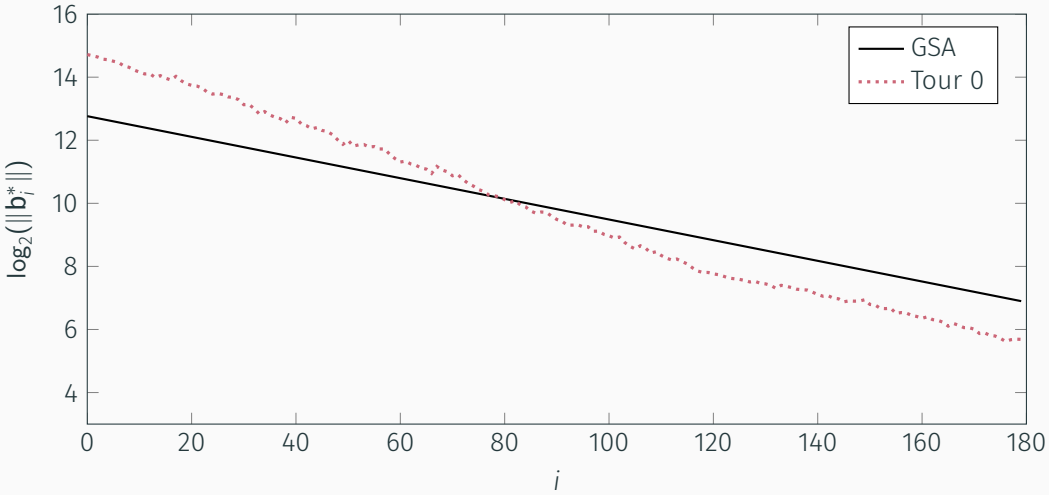


Yuanmi Chen. Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe. PhD thesis. Paris 7, 2013

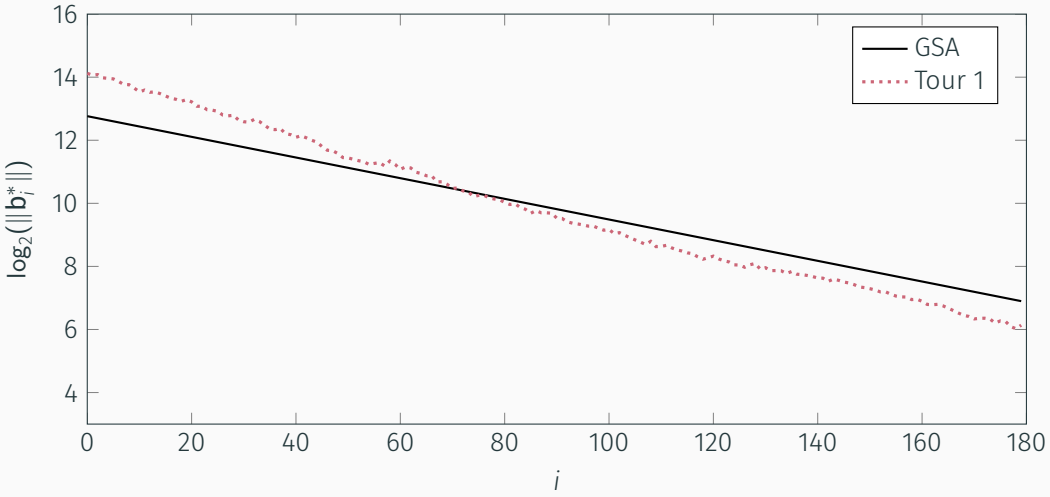
Behaviour in Practice: BKZ-60 in Dimension 180 I



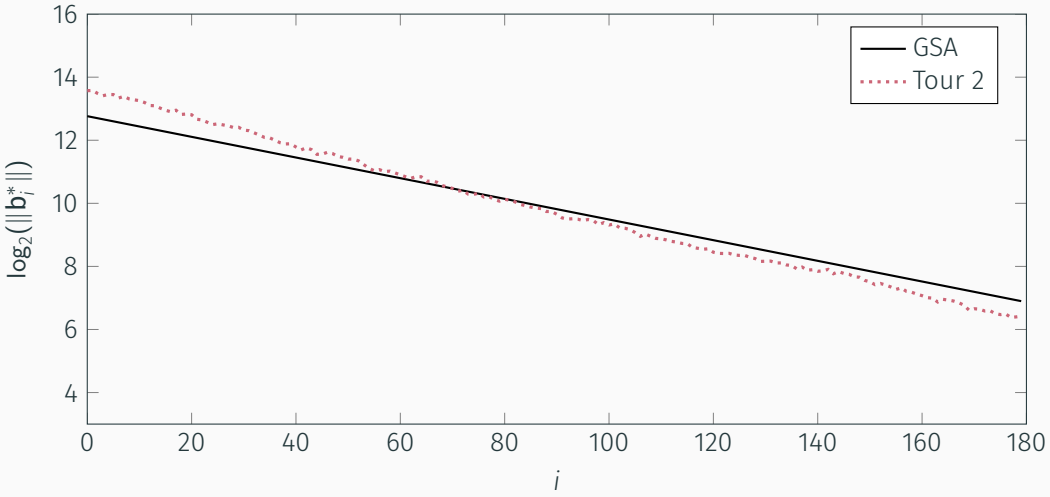
Behaviour in Practice: BKZ-60 in Dimension 180 II



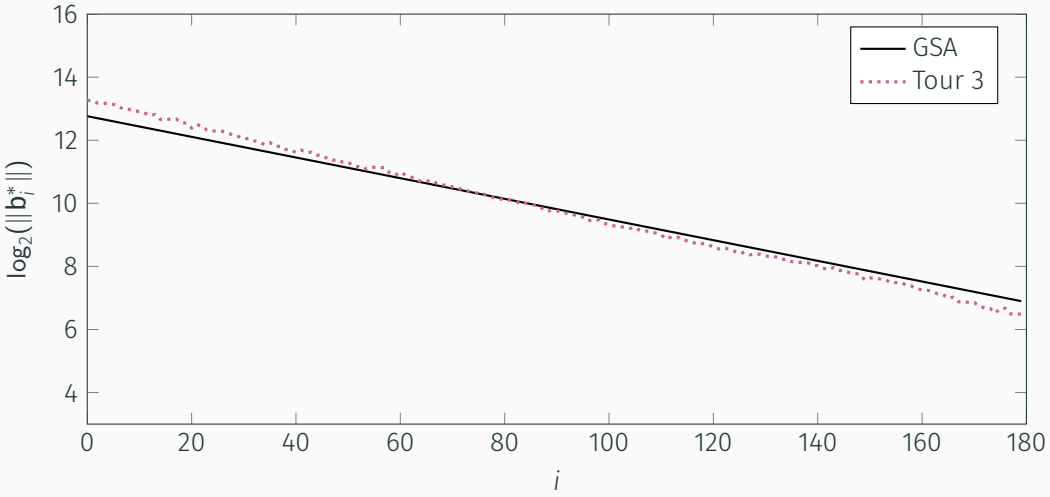
Behaviour in Practice: BKZ-60 in Dimension 180 III



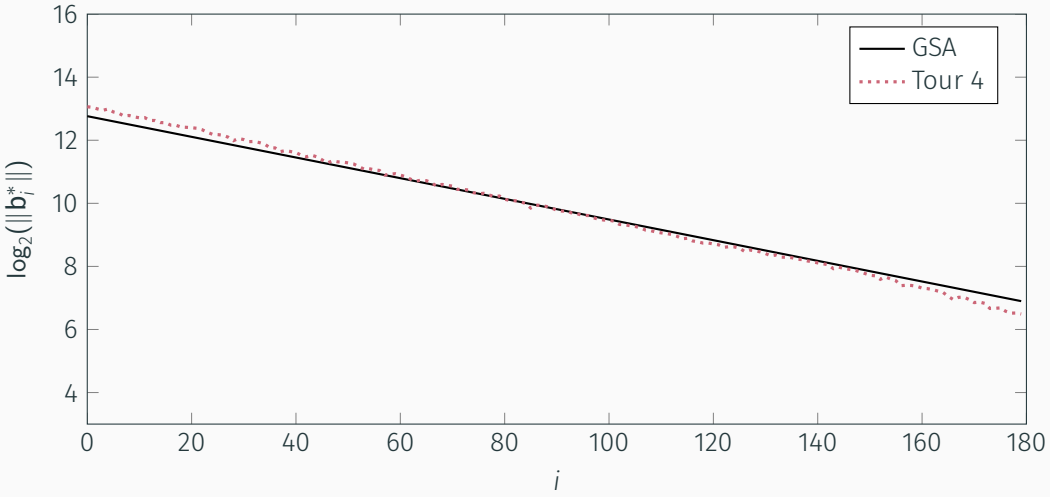
Behaviour in Practice: BKZ-60 in Dimension 180 iv

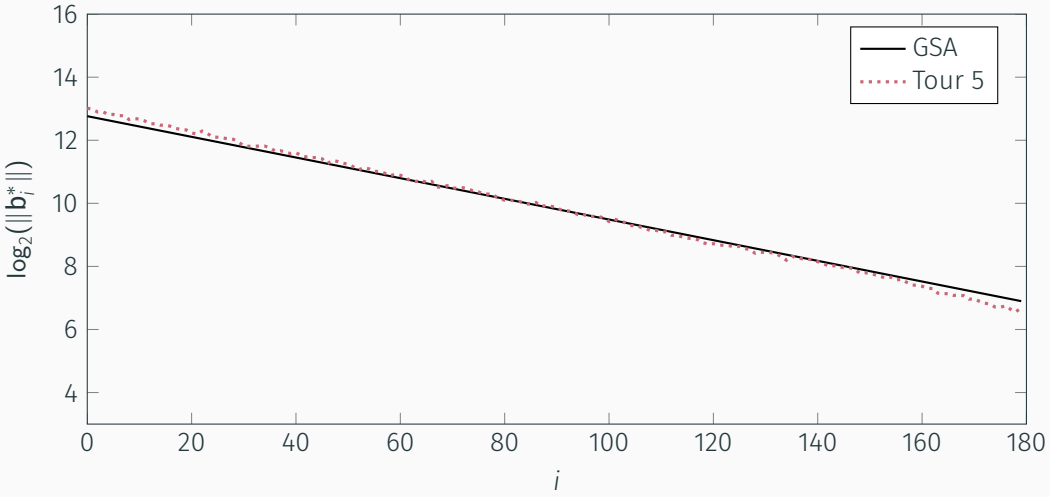


Behaviour in Practice: BKZ-60 in Dimension 180 v

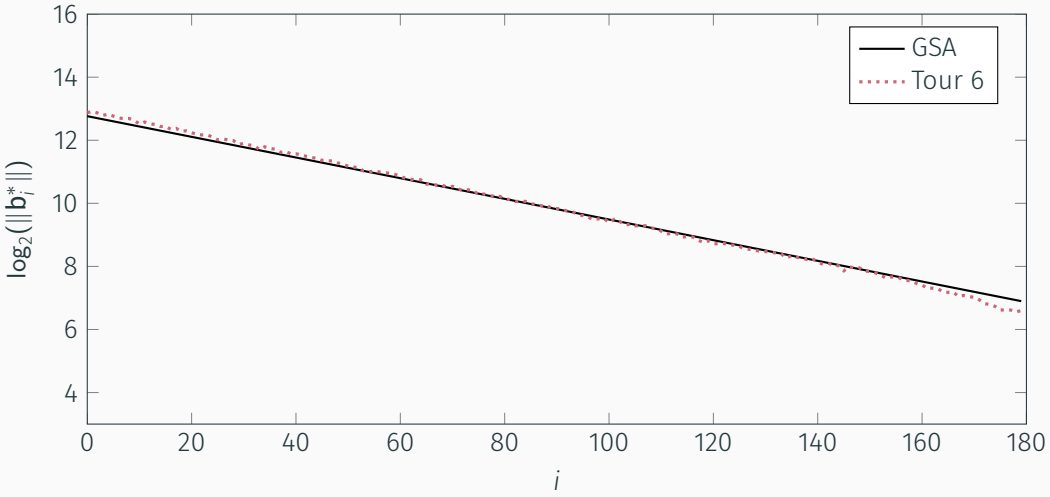


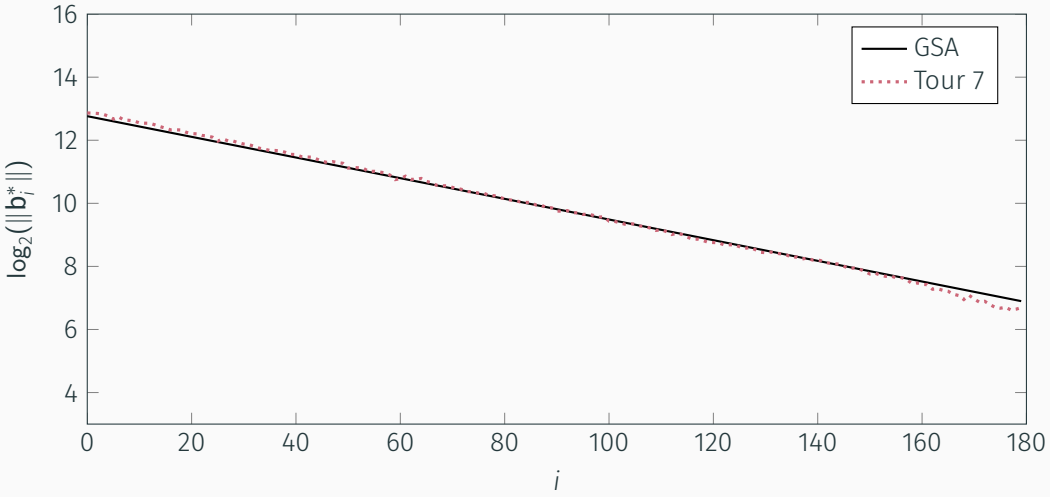
Behaviour in Practice: BKZ-60 in Dimension 180 vi



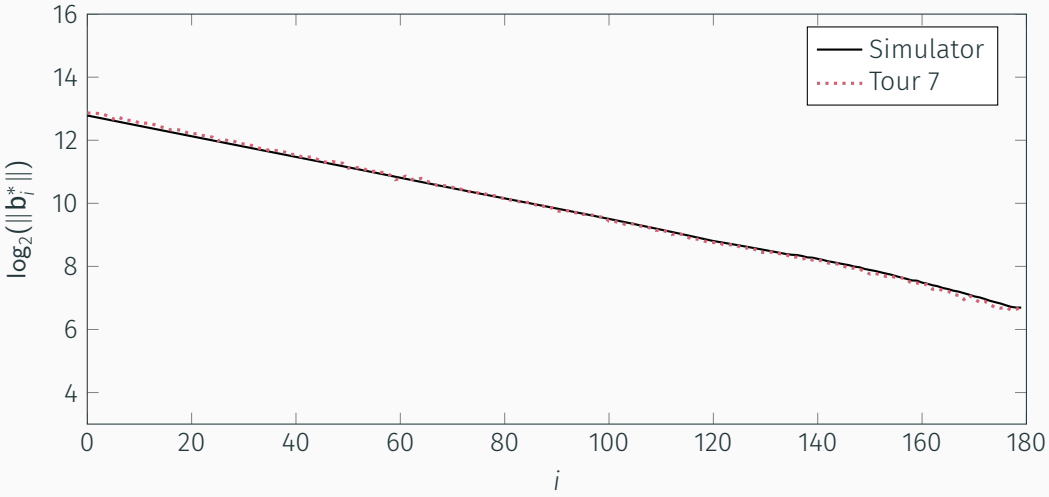

GSA
Tour 5
$\log_2(\|\mathbf{b}_i^*\|)$
i
16
14
12
10
8
6
4
0
20
40
60
80
100
120
140
160
180

Behaviour in Practice: BKZ-60 in Dimension 180 viii




GSA
Tour 7
$\log_2(\|\mathbf{b}_i^*\|)$
i
16
14
12
10
8
6
4
0
20
40
60
80
100
120
140
160
180

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 $\Lambda = \Lambda(B)$ 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

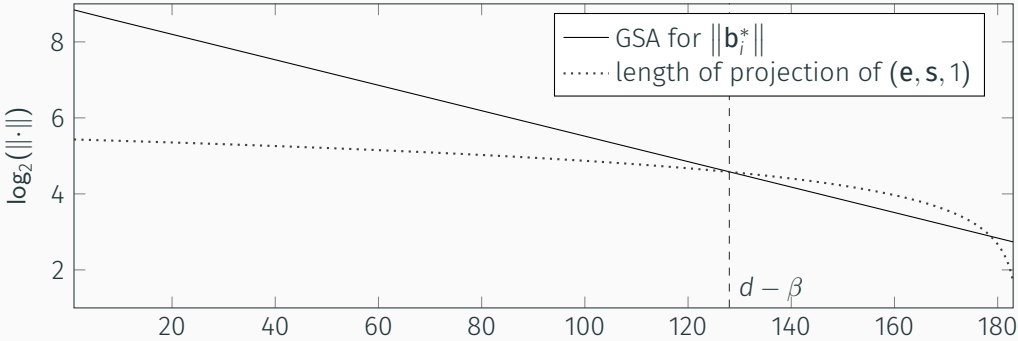
- $\delta_\beta^{2\cdot(d-\beta)} \cdot \lambda_1(\Lambda) < \delta_\beta^{d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$
- $\lambda_1(\Lambda) < \delta_\beta^{2\beta-d-1} \cdot \mathrm{Vol}(\Lambda)^{1/d}$

"2016 Estimate"

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

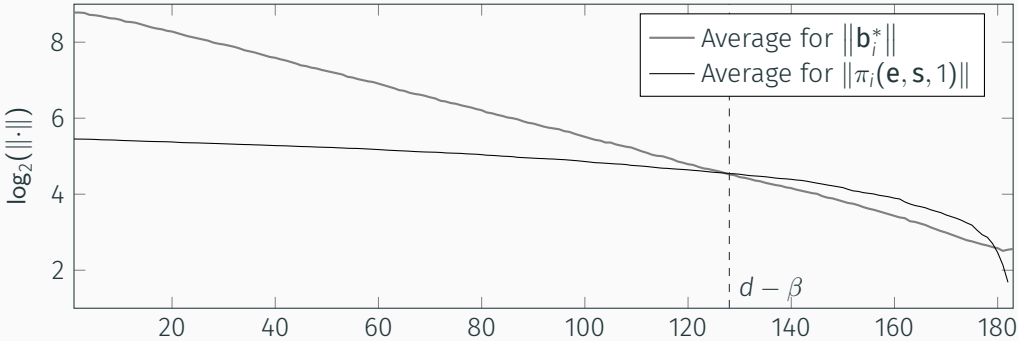
Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In: *USENIX Security 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, Aug. 2016, pp. 327–343

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

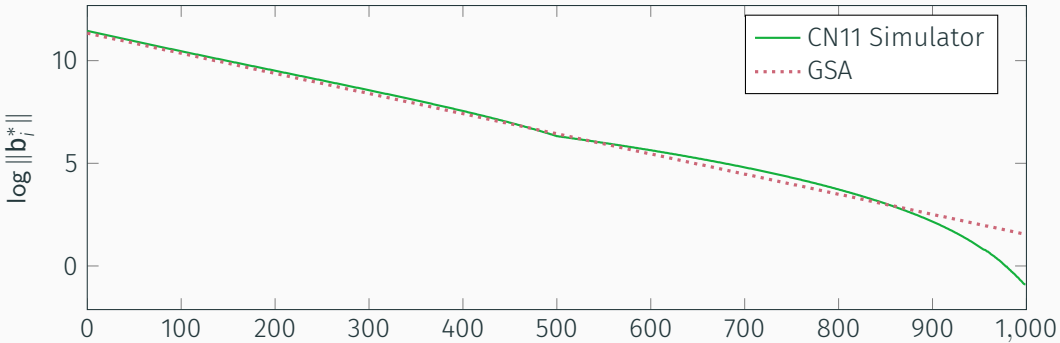
Success Condition for uSVP (Observed)



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

Eamonn W. Postlethwaite and Fernando Virdia. On the Success Probability of Solving Unique SVP via BKZ. In: *PKC 2021, Part I*. ed. by Juan Garay. Vol. 12710. LNCS. Springer, Heidelberg, May 2021, pp. 68–98. DOI: 10.1007/978-3-030-75245-3_4

The GSA is a Lie: Tail Shape



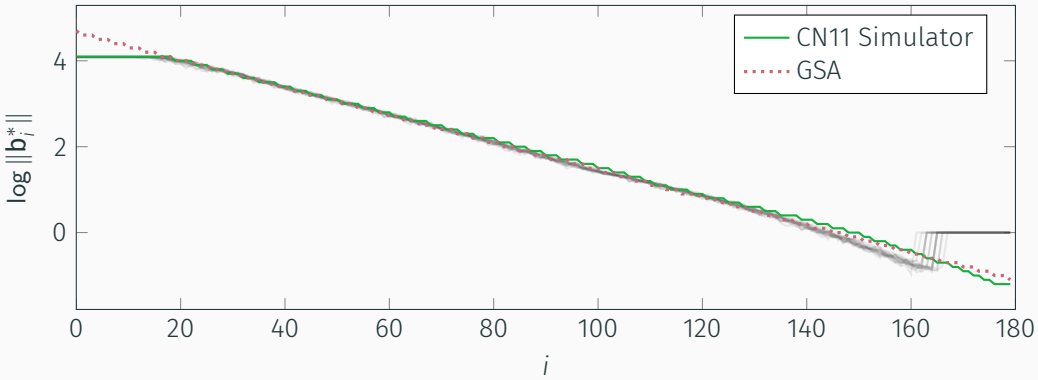
Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, Heidelberg, Dec. 2011, pp. 1–20. DOI: 10.1007/978-3-642-25385-0_1

The GSA is a Lie: Tail Shape

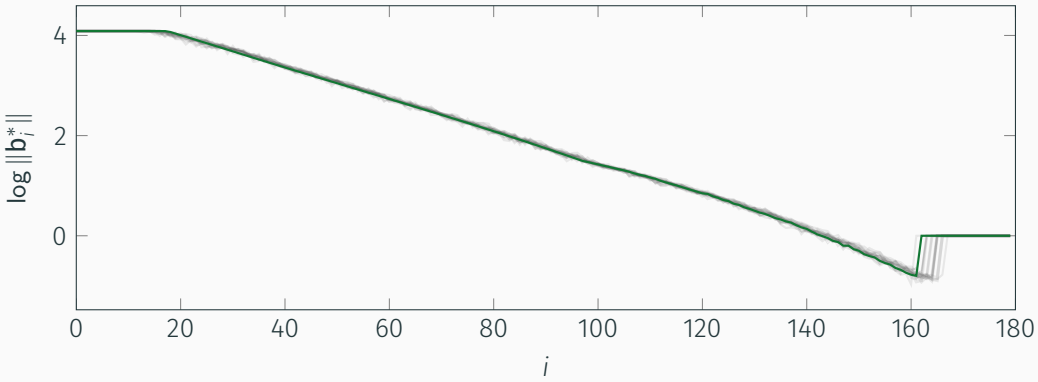
```
from estimator import *
print(repr(LWE.primal_usvp(Kyber768, red_shape_model="GSA")))
print(repr(LWE.primal_usvp(Kyber768, red_shape_model="CN11")))
```

```
rop: ≈2^204.9, red: ≈2^204.9, δ: 1.002902, β: 624, d: 1427, tag: usvp
rop: ≈2^209.9, red: ≈2^209.9, δ: 1.002842, β: 642, d: 1421, tag: usvp
```

The GSA is a Lie: Z-Shape



The GSA is a Lie: Z-Shape



. . . but the Z-shape can be observed to vanish when breaking standard parameter sets.

Martin R. Albrecht and Jianwei Li. Predicting BKZ Z-Shapes on q-ary Lattices. Cryptology ePrint Archive, Paper 2022/843. https://eprint.iacr.org/2022/843. 2022. URL: https://eprint.iacr.org/2022/843

Solving SVP

Solving SVP

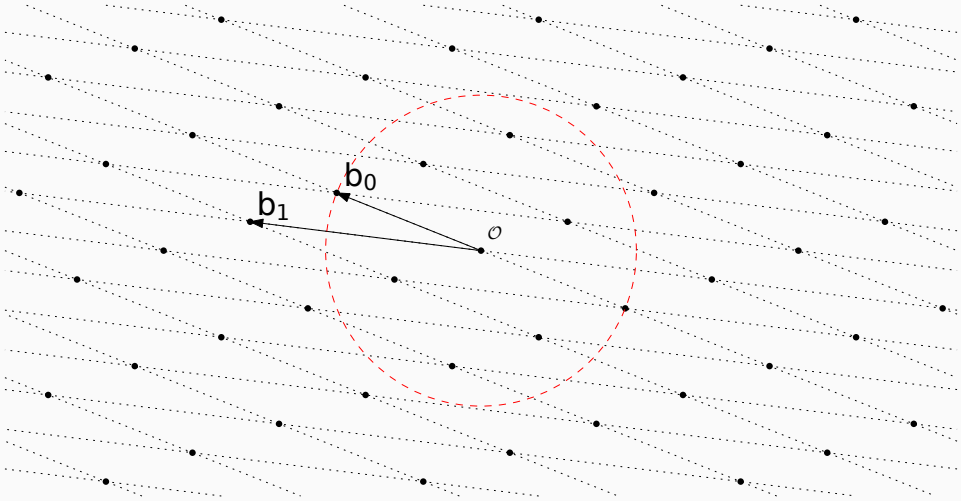
Enumeration

- Search through vectors smaller than a given bound: project down to 1-dim problem, lift to 2-dim problem ...
- Sensitive to the quality of the input basis
- **Time:** $2^{\Theta(\beta \log \beta)}$
- **Memory:** $\text{poly}(\beta)$

Sieving

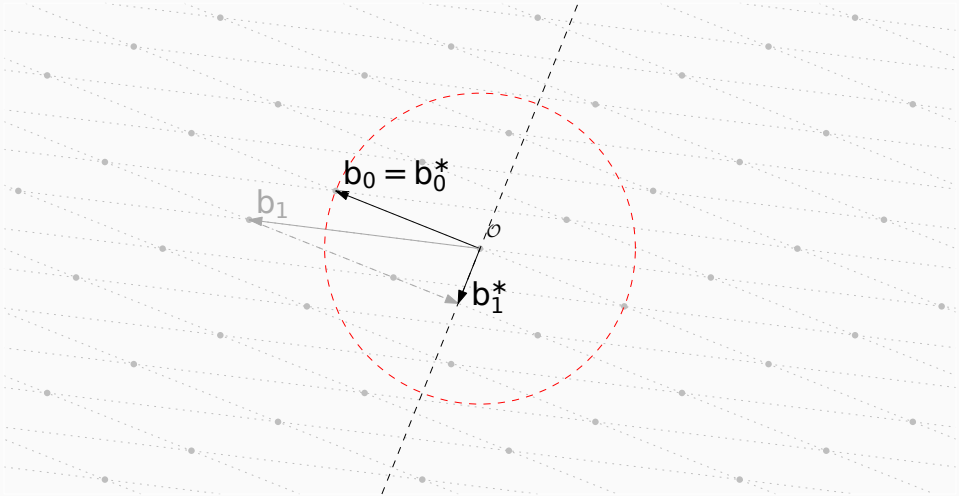
- Produce new, shorter vectors by considering sums and differences of existing vectors
- Fairly oblivious to the quality of the input basis
- **Time:** $2^{\Theta(\beta)}$
- **Memory:** $2^{\Theta(\beta)}$

Enumeration I – Pick a radius



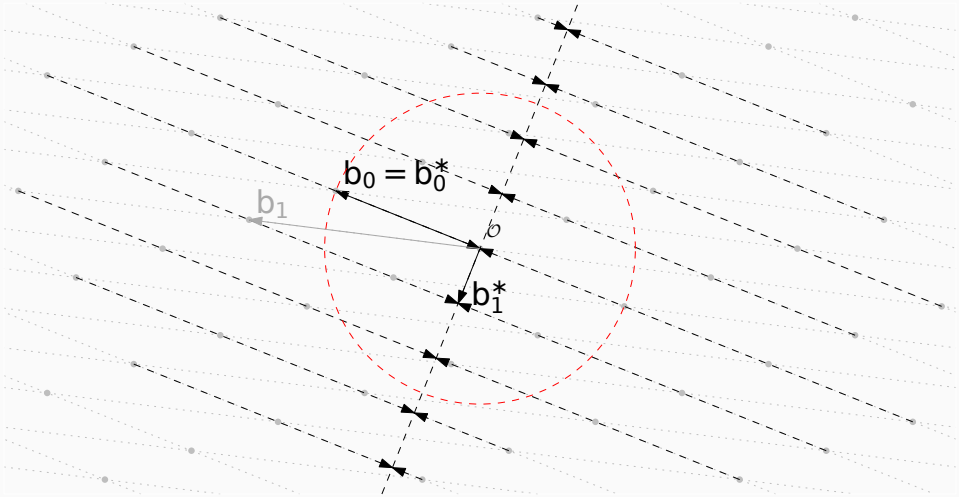
Picture credit: Joop van de Pol

Enumeration II – Project basis



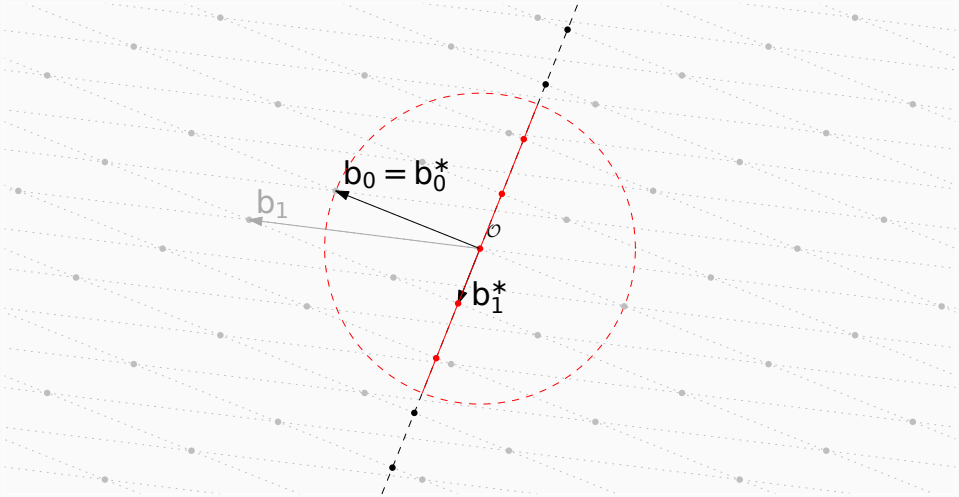
Picture credit: Joop van de Pol

Enumeration III – Project lattice



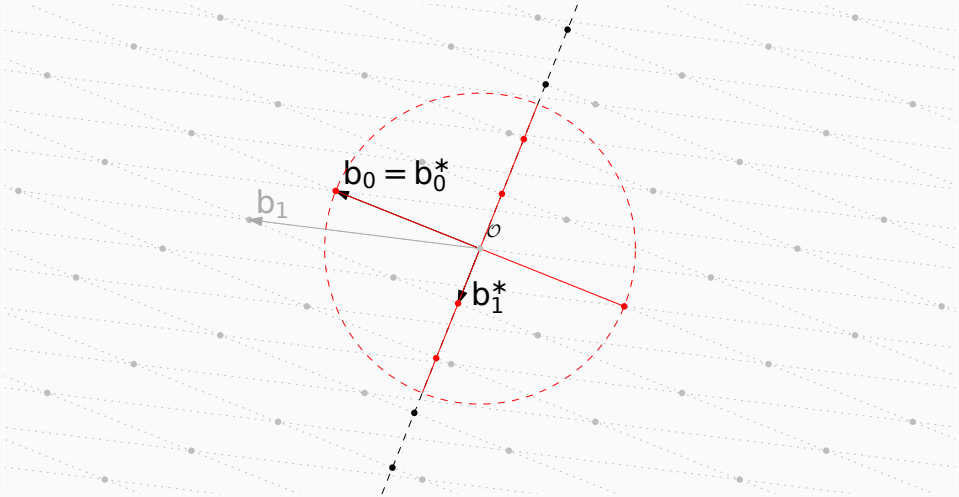
Picture credit: Joop van de Pol

Enumeration IV – Enumerate projections



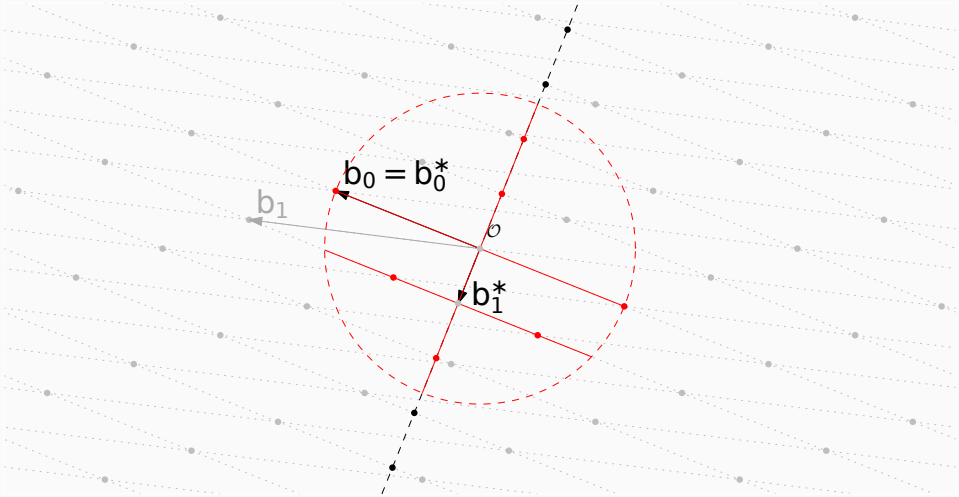
Picture credit: Joop van de Pol

Enumeration V – For each lift and enumerate



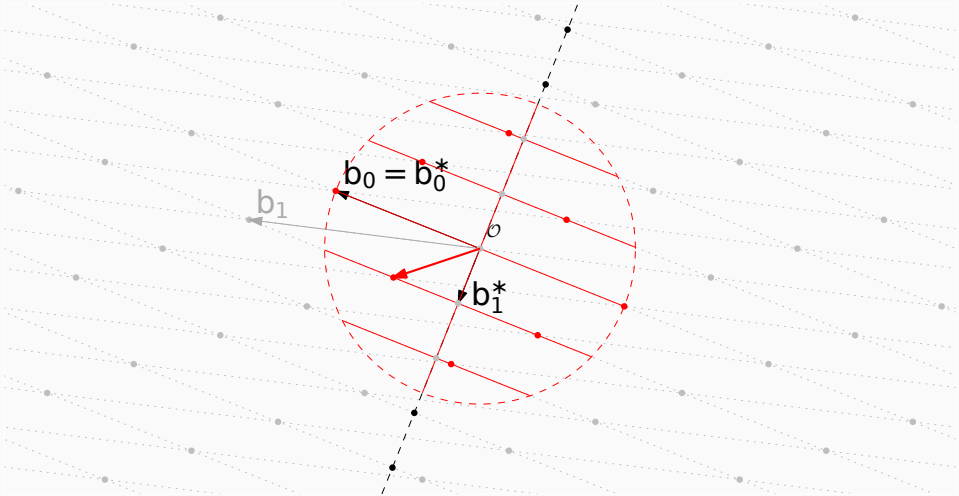
Picture credit: Joop van de Pol

Enumeration V – For each lift and enumerate



Picture credit: Joop van de Pol

Enumeration VI – Keep shortest

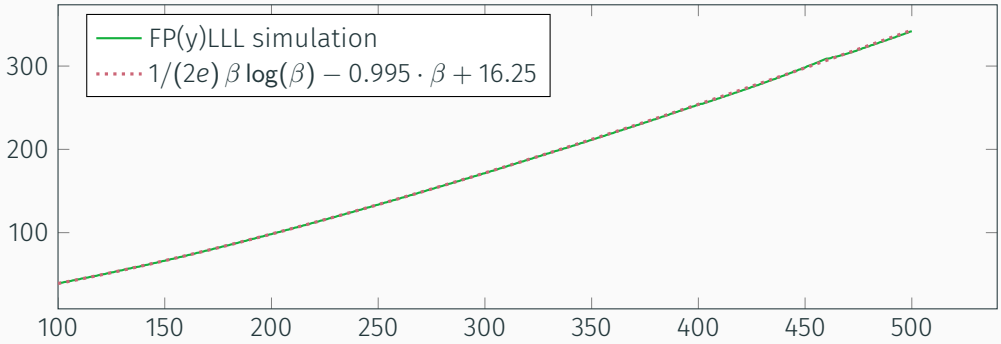


Picture credit: Joop van de Pol

Fast Enumeration

- Do not exhaust the search space, but focus on a fraction with exponentially small probability of success, repeat exponentially often: speed-up $2^{\Theta(\beta)}$
- Preprocess the basis with BKZ-β' for some $\beta' \leq \beta$ before enumerating.

Enumeration Cost: $\beta^{\beta/(2e)+o(\beta)}$



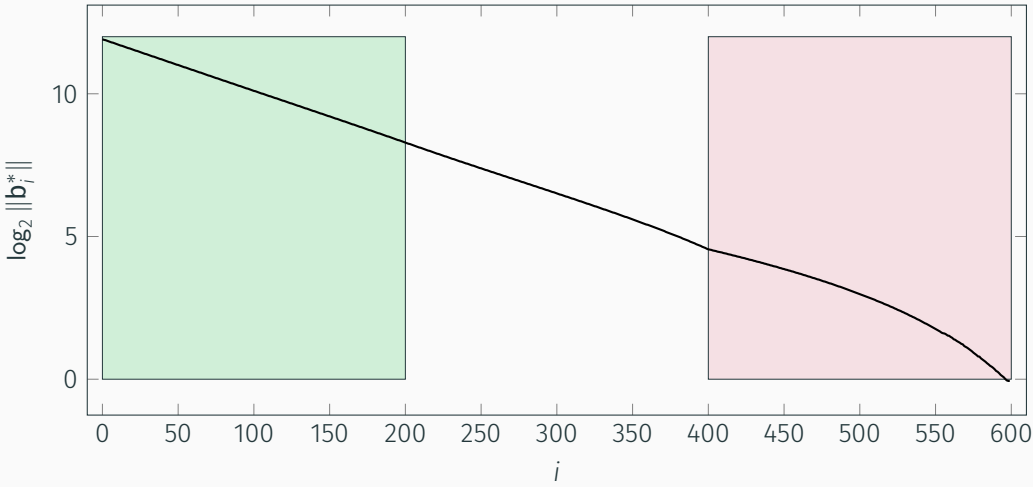
Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, and Weiqiang Wen. Faster Enumeration-Based Lattice Reduction: Root Hermite Factor $k^{1/(2k)}$ Time $k^{k/8+o(k)}$. In: *CRYPTO 2020, Part II*. ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Heidelberg, Aug. 2020, pp. 186–212. DOI: 10.1007/978-3-030-56880-1_7

Enumeration Cost: $\beta^{\beta/8+o(\beta)}$

"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."[2]

[2] 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

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

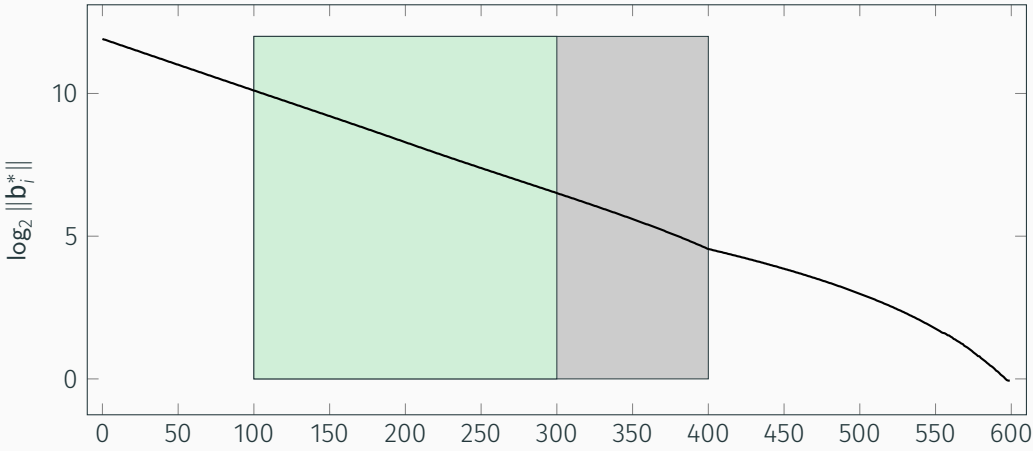


Why we can't have Nice Things™

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,[3] as the algorithm proceeds through the indices i, a "bump" accumulates from index $i + 1$ onward.

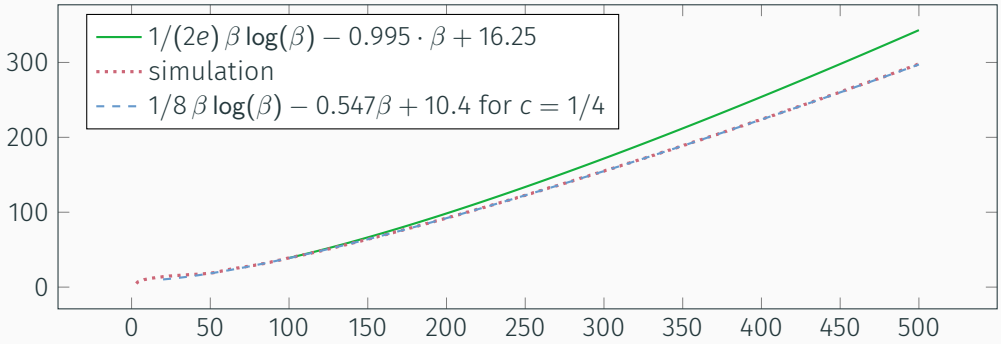
[3] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing Blockwise Lattice Algorithms Using Dynamical Systems. In: *CRYPTO 2011*. Ed. by Phillip Rogaway. Vol. 6841. LNCS. Springer, Heidelberg, Aug. 2011, pp. 447–464. DOI: 10.1007/978-3-642-22792-9_25.

Idea: Overshoot Preprocessing



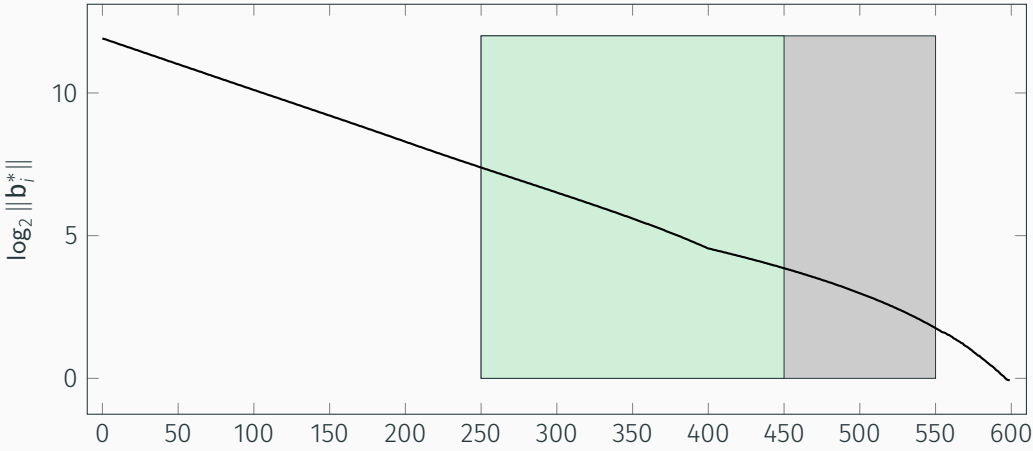
Preprocessing in dimension $(1 + c) \cdot \beta$ for enumeration in dimension β.

Practical Performance (Simulation)

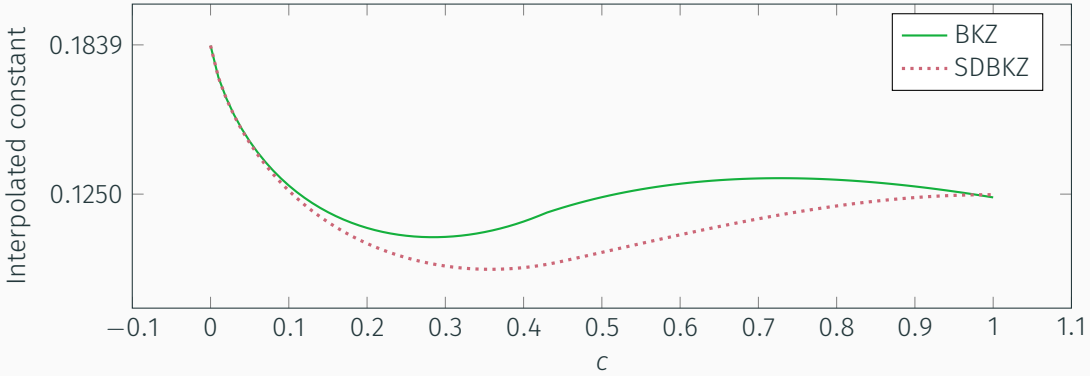


Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, and Weiqiang Wen. Faster Enumeration-Based Lattice Reduction: Root Hermite Factor $k^{1/(2k)}$ Time $k^{k/8+o(k)}$. In: *CRYPTO 2020, Part II*. ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Heidelberg, Aug. 2020, pp. 186–212. DOI: 10.1007/978-3-030-56880-1_7

Open Question: Can we do better?

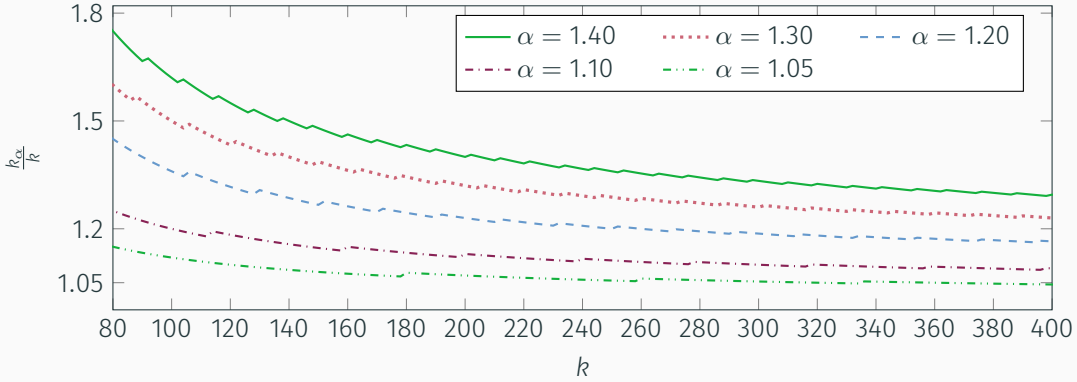


Open Question: Can we do better?



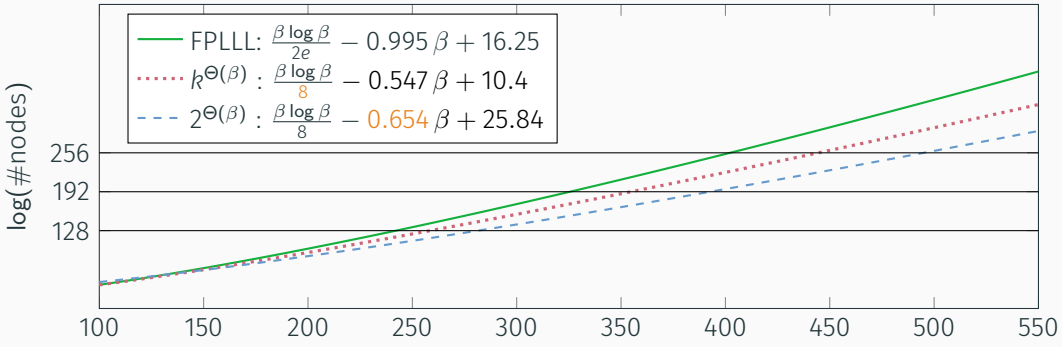
Leading constant assuming **free preprocessing**.

Tuning Lower Order Terms: $(\alpha \cdot \mathrm{GH}(k_\alpha))^{\frac{1}{k_\alpha - 1}} \leq \mathrm{GH}(k)^{\frac{1}{k-1}}$



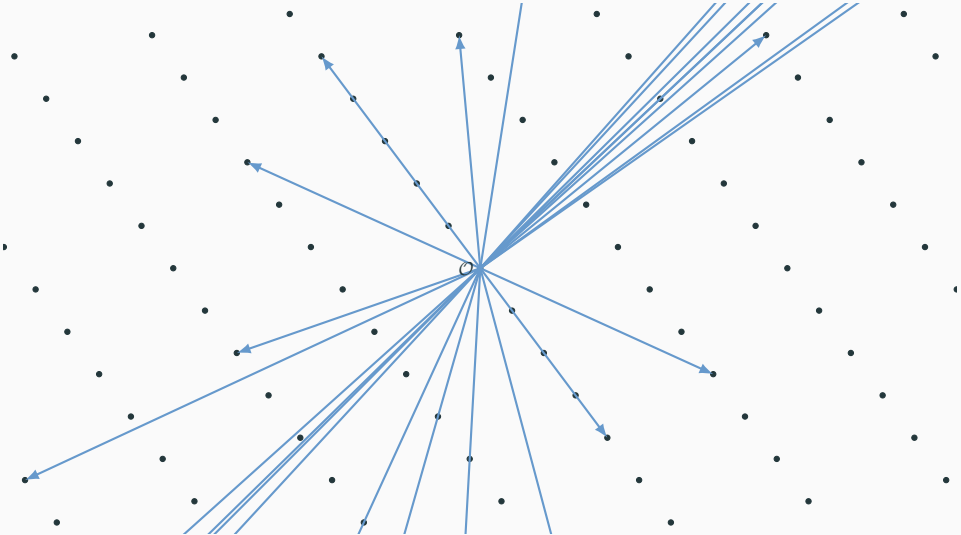
k_α is the smallest integer greater than k such that $\mathrm{GH}(k)^{\frac{1}{k-1}} \geq (\alpha \cdot \mathrm{GH}(k_\alpha))^{\frac{1}{k_\alpha - 1}}$ for $\alpha \geq 1$ and $k \geq 36$.

Practical Performance (Simulation)

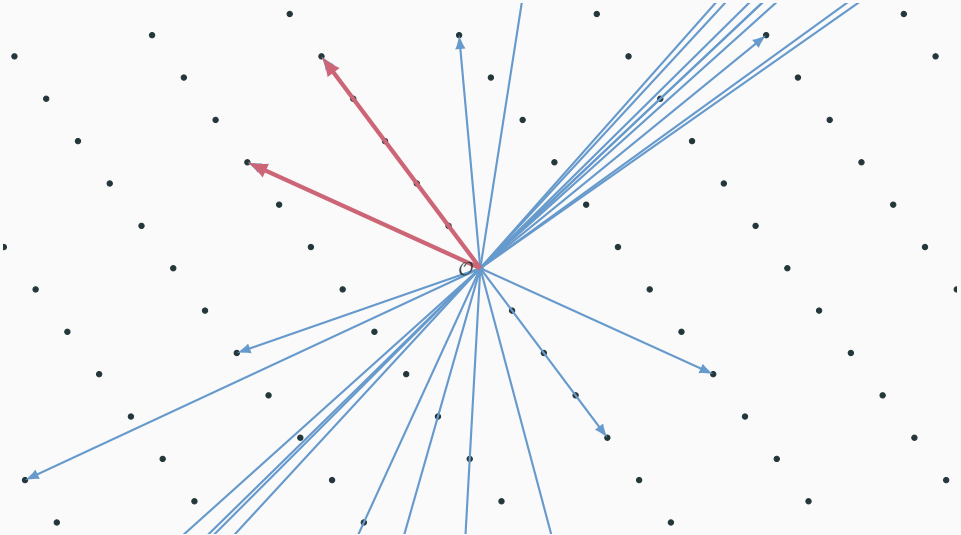


Martin R. Albrecht, Shi Bai, Jianwei Li, and Joe Rowell. Lattice Reduction with Approximate Enumeration Oracles - Practical Algorithms and Concrete Performance. In: *CRYPTO 2021, Part II*. ed. by Tal Malkin and Chris Peikert. Vol. 12826. LNCS. Virtual Event: Springer, Heidelberg, Aug. 2021, pp. 732–759. DOI: 10.1007/978-3-030-84245-1_25

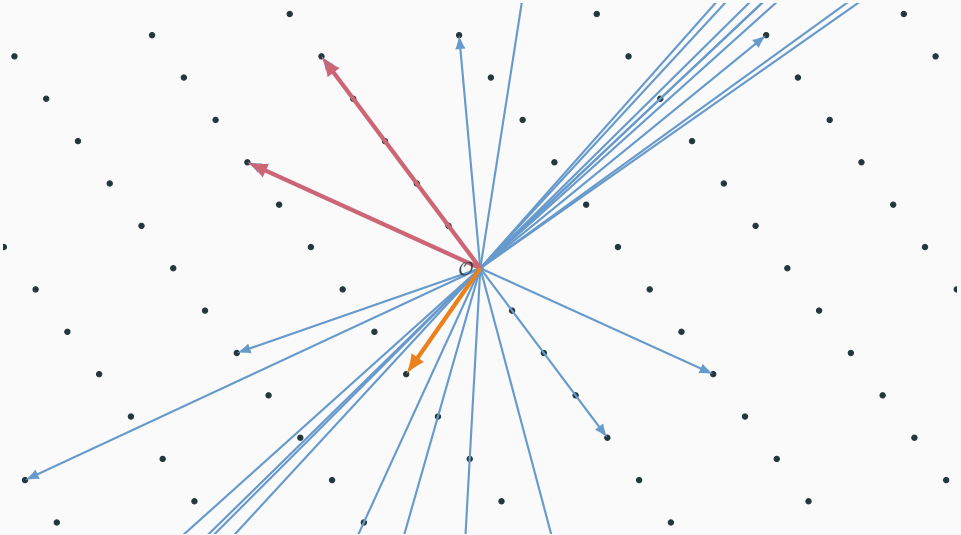
Sieving: Key Idea I



Sieving: Key Idea II



Sieving: Key Idea III



Sieving: Basic (Gauss) Sieve Complexity

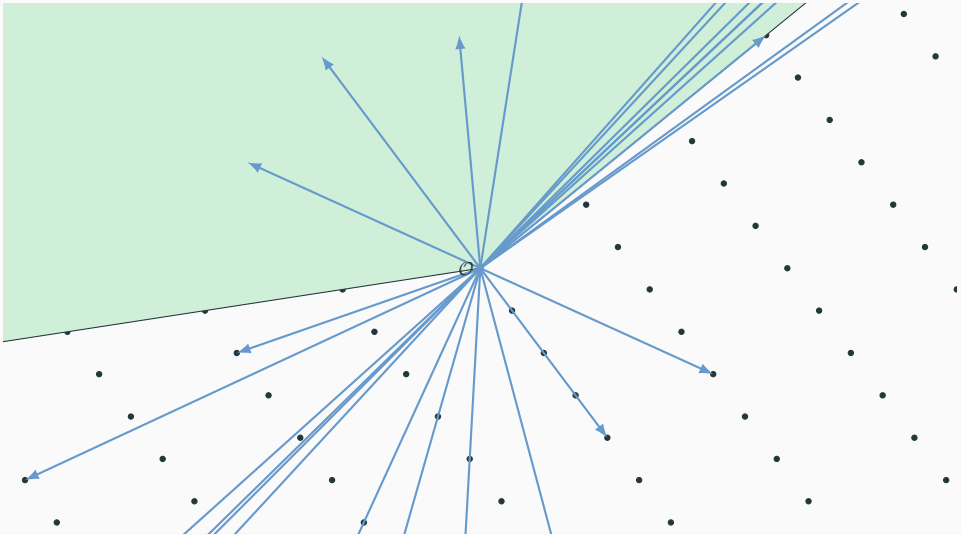
- Assume all vectors have (roughly) the same length
- Normalise to unit sphere $\mathcal{S}^{d-1} \coloneqq \{\mathbf{x} \in \mathbb{R}^d | \|\mathbf{x}\| = 1\}$
- We have $\|\mathbf{v} - \mathbf{w}\| \leq 1$ iff $\langle \mathbf{v}, \mathbf{w} \rangle \geq 1/2 = \cos(\pi/3)$
- The probability that two random $\mathbf{v}, \mathbf{w} \in \mathcal{S}^{d-1}$ satisfy $\langle \mathbf{v}, \mathbf{w} \rangle \geq 1/2$ is

$$\frac{1}{\sqrt{\pi}} \cdot \frac{\Gamma(d/2)}{\Gamma((d-1)/2)} \cdot \int_0^{\pi/3} \sin^{d-2}(x)\,\mathrm{d}x = \mathrm{poly}(d) \cdot \left(\frac{4}{3}\right)^{d/2} \approx 2^{0.2075\,d + o(d)}$$

- Need $\mathrm{poly}(d) \cdot \left(\frac{4}{3}\right)^{d/2}$ vectors, comparing all pairs costs $\mathrm{poly}(d) \cdot \left(\frac{4}{3}\right)^{d} \approx 2^{0.4150\,d + o(d)}$.

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

Sieving: Buckets I



Sieving: Buckets II

If $\mathbf{v}$, $\mathbf{c}$ are somewhat close and $\mathbf{w}$, $\mathbf{c}$ are somewhat close then perhaps $\mathbf{w}$, $\mathbf{v}$ are close?

Strategy

- Sort vectors into somewhat loose buckets,
- Do quadratic pairwise comparison only within each bucket.

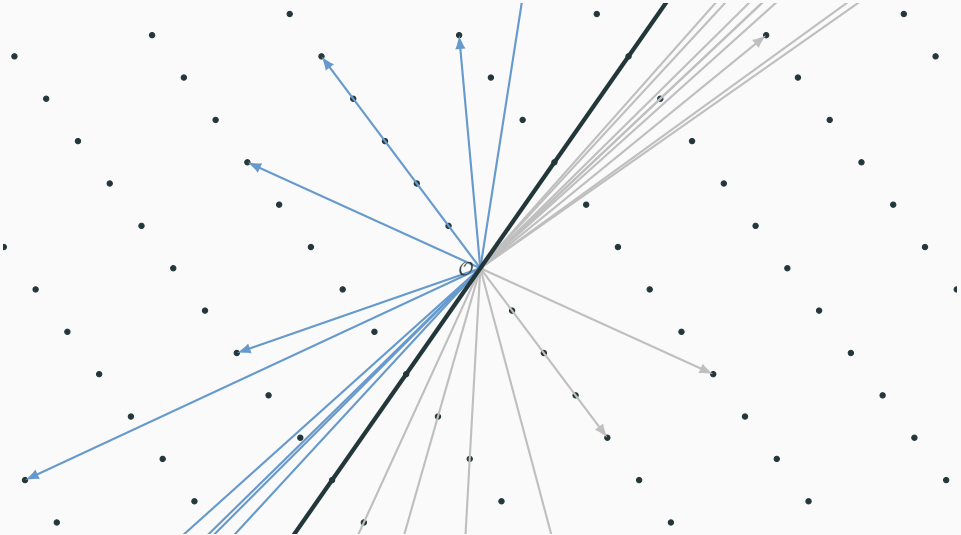
BGJ Split search space into buckets. **Cost**: $2^{0.311\,\beta+o(\beta)}$.[4]

BDGL Use codes to decide which bucket to consider. **Cost**: $2^{0.292\,\beta+o(\beta)}$.[5]

[4] 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.

[5] 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: Popcount I



Sieving: Popcount II

Most comparisons result in a ”no” answer, rejecting those pairs quickly improves performance, even if we lose a few good pairs.

- 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”).

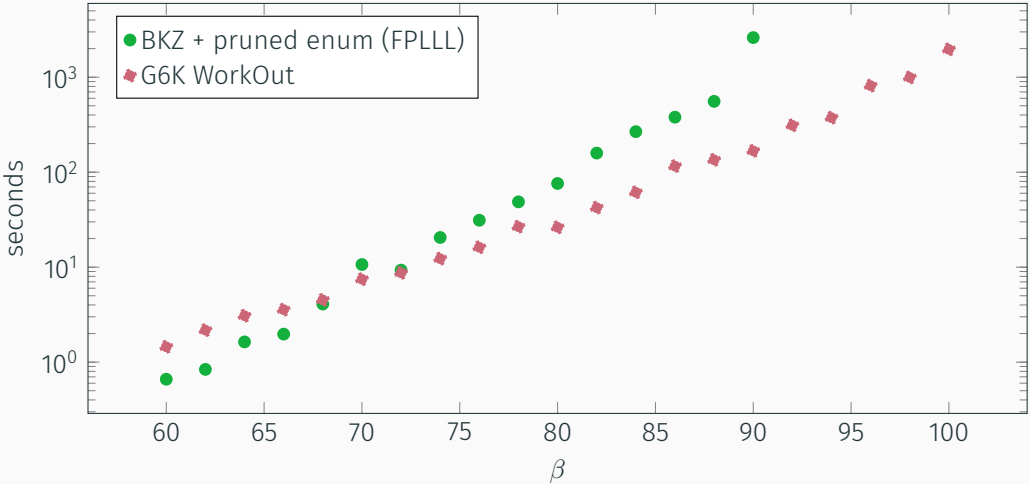
Sieving: G6K

G6K[6] 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
  - Gauss and NV
  - Triple Sieve
  - BGJ1 (BGJ with one level of filtration)
  - BDGL (with one and two block respectively)
- Applies recent tricks and adds new tricks for improving performance of sieving

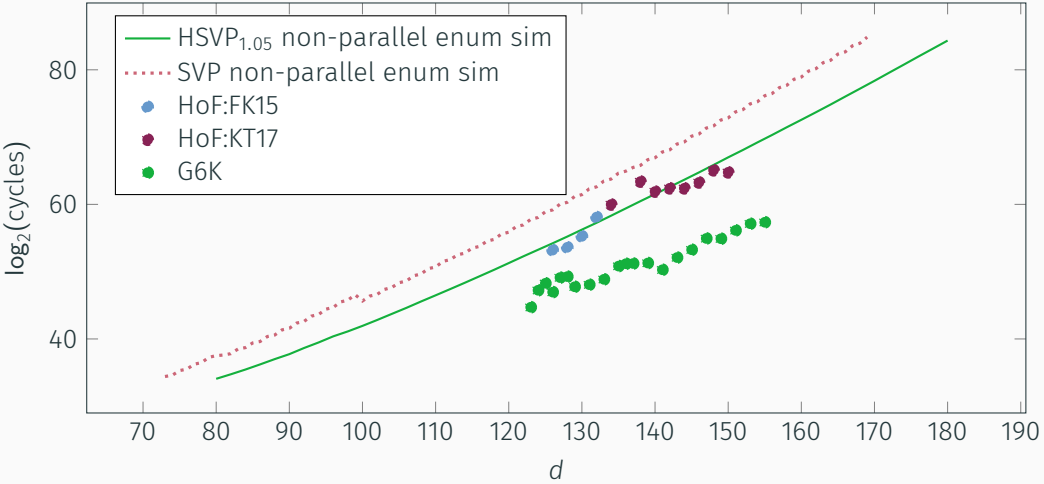
[6] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. The General Sieve Kernel and New Records in Lattice Reduction. In: *EUROCRYPT 2019, Part II*. ed. by Yuval Ishai and Vincent Rijmen. Vol. 11477. LNCS. Springer, Heidelberg, May 2019, pp.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

Sieving: SVP



Average time in seconds for solving exact SVP

Darmstadt $HSVP_{1.05}$ Challenges



GPU Sieving

- Stream database of vectors to GPU
- Run low precision inner products there in the spirit of popcount

dim	TD4F	D4F	MSD	Norm	Norm/GH	FLOP	Walltime	Mem GiB
158	31	29	129	3303	1.04329	262.1	9h 16m	89
162	31	31	131	3341	1.04220	263.2	18h 32m	156
176	34	33	143	3487	1.04412	267.5	12d 11h	806
178	34	32	146	3447	1.02725	268.6	22d 18h	1060
180	34	30	150	3509	1.04003	269.9	51d 14h	1443

Léo Ducas, Marc Stevens, and Wessel P. J. van Woerden. Advanced Lattice Sieving on GPUs, with Tensor Cores. In: *EUROCRYPT 2021, Part II*. ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. LNCS. Springer, Heidelberg, Oct. 2021, pp. 249–279. DOI: 10.1007/978-3-030-77886-6_9

Try it at Home

```
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

https://github.com/WvanWoerden/G6K-GPU-Tensor G6K fork adding GPU support

Details Matter

"The main difference is the cost of the random product code decoding algorithm. Our algorithm requires one addition, one xor, and three comparisons per legal codeword, which translate to 433 gates for a lattice of rank 400, as opposed to [AGPS20] which requires a super-constant number of inner products per legal codeword, which translate to 3,540,524 gates for a lattice of rank 400."

MATZOV. Report on the Security of LWE: Improved Dual Lattice Attack. Apr. 2022. DOI: 10.5281/zenodo.6412487. URL: https://doi.org/10.5281/zenodo.6412487

"Concretely, we conclude on an overhead factor of about on the number of gates in the RAM model compared to the idealized model for dimensions around after an appropriate re-parametrization. Part of this overhead can be traded for extra memory, at a costly rate."

Léo Ducas. Estimating the Hidden Overheads in the BDGL Lattice Sieving Algorithm. Cryptology ePrint Archive, Paper 2022/922. https://eprint.iacr.org/2022/922. 2022. URL: https://eprint.iacr.org/2022/922

Quantum Stuff

Quantum Estimates

Sieving Given some vector $\mathbf{w}$ and a list of vectors L, apply Grover's algorithm to find $\{\mathbf{v} \in L \text{ s.t. } \|\mathbf{v} \pm \mathbf{w}\| \leq \|\mathbf{w}\|\}$.[7]

Enumeration Apply Montanaro's quantum backtracking algorithm for quadratic speed-up.[8]

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

[8] 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[9]

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

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

[9] 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

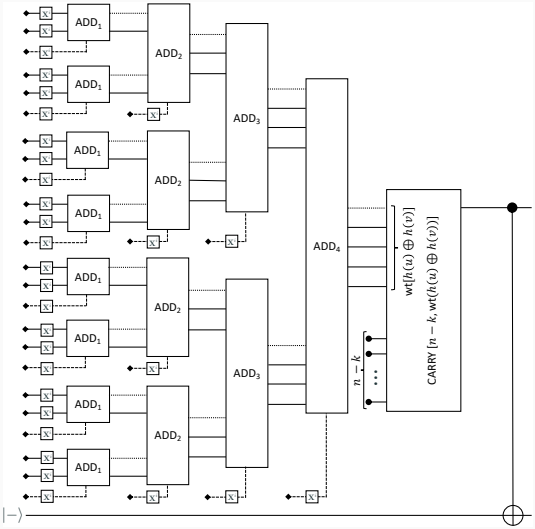
Sieving

- 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).

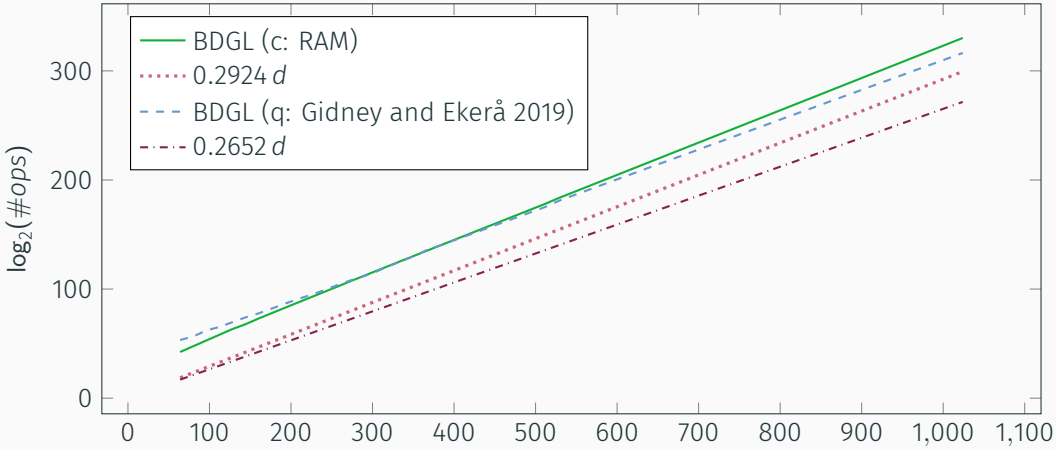
Enumeration

- 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?
- Near-term noisy quantum computers?
- Quantum improvements on a higher level?

Other 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

References I

[ABFKSW20] Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, and Weiqiang Wen. Faster Enumeration-Based Lattice Reduction: Root Hermite Factor $k^{1/(2k)}$ Time $k^{k/8+o(k)}$. In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Heidelberg, Aug. 2020, pp. 186–212. DOI: 10.1007/978-3-030-56880-1_7.

[ABLR21] Martin R. Albrecht, Shi Bai, Jianwei Li, and Joe Rowell. Lattice Reduction with Approximate Enumeration Oracles - Practical Algorithms and Concrete Performance. In: *CRYPTO 2021, Part II*. Ed. by Tal Malkin and Chris Peikert. Vol. 12826. LNCS. Virtual Event: Springer, Heidelberg, Aug. 2021, pp. 732–759. DOI: 10.1007/978-3-030-84245-1_25.

[ADHKPS19] 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.

[ADPS16] 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.

[AGPS19] 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.

References II

[AGVW17] 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.

[AL22] Martin R. Albrecht and Jianwei Li. Predicting BKZ Z-Shapes on q-ary Lattices. Cryptology ePrint Archive, Paper 2022/843. https://eprint.iacr.org/2022/843. 2022. URL: https://eprint.iacr.org/2022/843.

[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.

[BDGL16] 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.

[CN11] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, Heidelberg, Dec. 2011, pp. 1–20. DOI: 10.1007/978-3-642-25385-0_1.

References III

[DSW21] Léo Ducas, Marc Stevens, and Wessel P. J. van Woerden. Advanced Lattice Sieving on GPUs, with Tensor Cores. In: *EUROCRYPT 2021, Part II*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. LNCS. Springer, Heidelberg, Oct. 2021, pp. 249–279. DOI: 10.1007/978-3-030-77886-6_9.

[Duc22] Léo Ducas. Estimating the Hidden Overheads in the BDGL Lattice Sieving Algorithm. Cryptology ePrint Archive, Paper 2022/922. https://eprint.iacr.org/2022/922. 2022. URL: https://eprint.iacr.org/2022/922.

[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.

References iv

[MAT22] MATZOV. Report on the Security of LWE: Improved Dual Lattice Attack. Apr. 2022. DOI: 10.5281/zenodo.6412487. URL: https://doi.org/10.5281/zenodo.6412487.

[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.

[PV21] Eamonn W. Postlethwaite and Fernando Virdia. On the Success Probability of Solving Unique SVP via BKZ. In: *PKC 2021, Part I*. Ed. by Juan Garay. Vol. 12710. LNCS. Springer, Heidelberg, May 2021, pp. 68–98. DOI: 10.1007/978-3-030-75245-3_4.

[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.