RUHR-UNIVERSITÄT BOCHUM

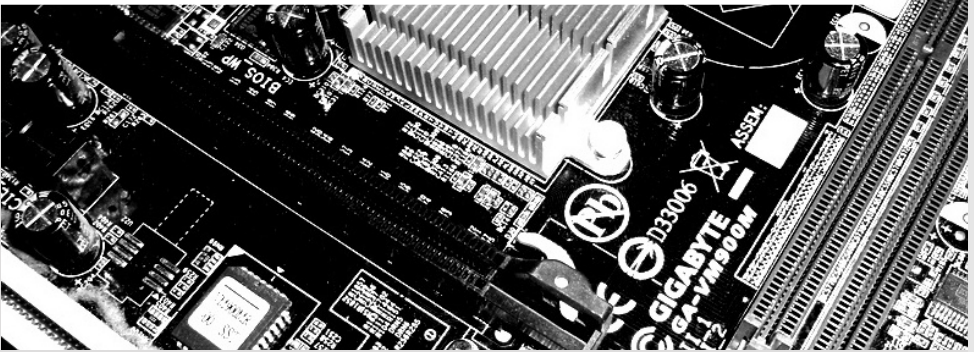
Attacks on Lattice Crypto

December 7th, 2016

FluxFingers

Workgroup Symmetric Cryptography
Ruhr University Bochum

Friedrich Wiemer



Why is Lattice Based Crypto important?

Or interesting? Or. . . ? Buzzword Bingo.

RUB

Some facts

- It is a Post-Quantum secure Cryptosystem (PQC)

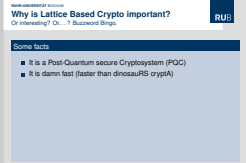
Why is Lattice Based Crypto important?

Or interesting? Or. . . ? Buzzword Bingo.

RUB

Some facts

- It is a Post-Quantum secure Cryptosystem (PQC)
- It is damn fast (faster than dinosauRS cryptA)



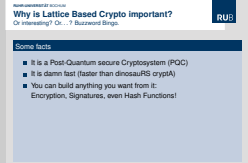
Why is Lattice Based Crypto important?

Or interesting? Or. . . ? Buzzword Bingo.

RUB

Some facts

- It is a Post-Quantum secure Cryptosystem (PQC)
- It is damn fast (faster than dinosauRS cryptA)
- You can build anything you want from it:
  Encryption, Signatures, even Hash Functions!



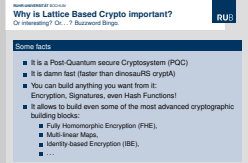
Why is Lattice Based Crypto important?

Or interesting? Or. . . ? Buzzword Bingo.

RUB

Some facts

- It is a Post-Quantum secure Cryptosystem (PQC)
- It is damn fast (faster than dinosauRS cryptA)
- You can build anything you want from it:
  Encryption, Signatures, even Hash Functions!
- It allows to build even some of the most advanced cryptographic building blocks:
  - Fully Homomorphic Encryption (FHE),
  - Multi-linear Maps,
  - Identity-based Encryption (IBE),
  - . . .



Why is Lattice Based Crypto important?

Is everything done?

Fully Homomorphic Encryption

GF(¯_(ツ)_/¯)
@hdevalence

Follow

Kirchner/Fouque: our attack lets us do FHE faster by just breaking the crypto & decrypting eprint.iacr.org/2016/717.pdf

The parameters proposed for schemes using similar overstretched NTRU assumption, such as in homomorphic encryption [8, 31, 17, 18, 16, 12, 32, 20] or in private information retrieval [19], are also broken in practical time using LLL. For example, we recovered a decryption key of the FHE described in [17] in only 10 hours. For comparison, they evaluated AES in 29 h: that means that we can more efficiently than the FHE evalution, recover the secret, perform the AES evaluation, and then re-encrypt the result! A decryption key was recovered for [20] in 4 h. Other instanciations such as [11, 29] are harder, but within range of practical cryptanalysis, using BKZ with moderate block-size [13].

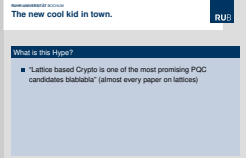
RETWEETS 33 LIKES 34

5:37 AM - 23 Jul 2016

The new cool kid in town.

What is this Hype?

- “Lattice based Crypto is one of the most promising PQC candidates blablabla” (almost every paper on lattices)



The new cool kid in town.

What is this Hype?

- “Lattice based Crypto is one of the most promising PQC candidates blablabla” (almost every paper on lattices)
- NSA supported this by announcing the need for PQC [KM15] in 2015

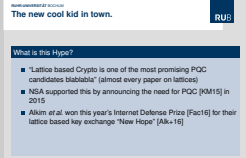
RUHR-UNIVERSITÄT BOCHUM
The new cool kid in town.
What is this Hype?
- “Lattice based Crypto is one of the most promising PQC candidates blablabla” (almost every paper on lattices)
- NSA supported this by announcing the need for PQC [KM15] in 2015

The new cool kid in town.

RUB

What is this Hype?

- “Lattice based Crypto is one of the most promising PQC candidates blablabla” (almost every paper on lattices)
- NSA supported this by announcing the need for PQC [KM15] in 2015
- Alkim *et al.* won this year’s Internet Defense Prize [Fac16] for their lattice based key exchange “New Hope” [Alk+16]



The new cool kid in town.

RUB

What is this Hype?

- “Lattice based Crypto is one of the most promising PQC candidates blablabla” (almost every paper on lattices)
- NSA supported this by announcing the need for PQC [KM15] in 2015
- Alkim *et al.* won this year’s Internet Defense Prize [Fac16] for their lattice based key exchange “New Hope” [Alk+16]
- Google even implemented this in Chrome [Goob]

RUHR-UNIVERSITÄT BOCHUM
The new cool kid in town.
RUB
What is this Hype?
- “Lattice based Crypto is one of the most promising PQC candidates blablabla” (almost every paper on lattices)
- NSA supported this by announcing the need for PQC [KM15] in 2015
- Alkim *et al.* won this year’s Internet Defense Prize [Fac16] for their lattice based key exchange “New Hope” [Alk+16]
- Google even implemented this in Chrome [Goob]

The new cool kid in town.

RUB

What is this Hype?

- “Lattice based Crypto is one of the most promising PQC candidates blablabla” (almost every paper on lattices)
- NSA supported this by announcing the need for PQC [KM15] in 2015
- Alkim *et al.* won this year’s Internet Defense Prize [Fac16] for their lattice based key exchange “New Hope” [Alk+16]
- Google even implemented this in Chrome [Goob]
- So, research is really vibrant here

RUHR-UNIVERSITÄT BOCHUM
The new cool kid in town.
RUB
What is this Hype?
- “Lattice based Crypto is one of the most promising PQC candidates blablabla” (almost every paper on lattices)
- NSA supported this by announcing the need for PQC [KM15] in 2015
- Alkim *et al.* won this year’s Internet Defense Prize [Fac16] for their lattice based key exchange “New Hope” [Alk+16]
- Google even implemented this in Chrome [Goob]
- So, research is really vibrant here

Everything was fine.
And then Shor entered the stage. . .

RUB

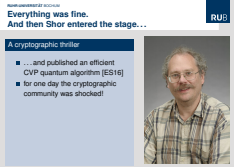
A cryptographic thriller

Everything was fine. And then Shor entered the stage. . .

RUB

A cryptographic thriller

- . . . and published an efficient CVP quantum algorithm [ES16]
- for one day the cryptographic community was shocked!

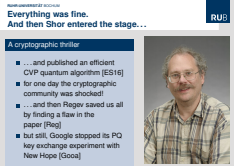


Everything was fine.
And then Shor entered the stage. . .

RUB

A cryptographic thriller

- . . . and published an efficient CVP quantum algorithm [ES16]
- for one day the cryptographic community was shocked!
- . . . and then Regev saved us all by finding a flaw in the paper [Reg]
- but still, Google stopped its PQ key exchange experiment with New Hope [Gooa]



Enough motivation!

How does Lattice Crypto work?

Enough motivation!
How does Lattice Crypto work?

How does Lattice Based Crypto work?

Wait! Lattice, wtf?

RUB

Definition:

A lattice L is an discrete, additive, abelian subgroup of $\mathbb{R}^n$.

How does Lattice Based Crypto work?

Wait! Lattice, wtf?

RUB

Definition:

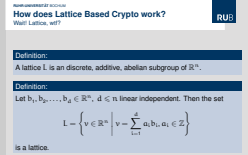
A lattice L is an discrete, additive, abelian subgroup of $\mathbb{R}^n$.

Definition:

Let $b_1, b_2, \ldots, b_d \in \mathbb{R}^n,\ d \leqslant n$ linear independent. Then the set

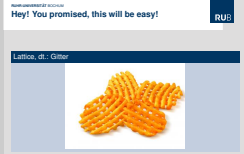
$$L = \left\{ v \in \mathbb{R}^n \;\middle|\; v = \sum_{i=1}^{d} a_i b_i, a_i \in \mathbb{Z} \right\}$$

is a lattice.



Hey! You promised, this will be easy!

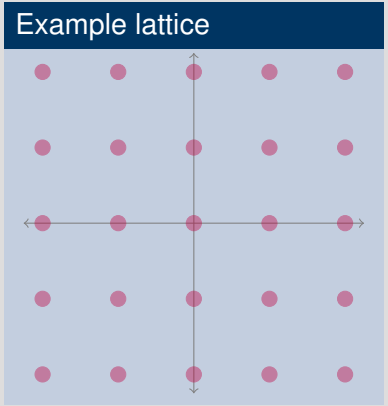
Lattice, dt.: Gitter

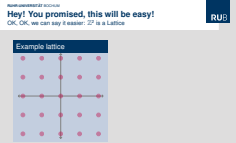


Hey! You promised, this will be easy!

OK, OK, we can say it easier: $\mathbb{Z}^2$ is a Lattice

Example lattice



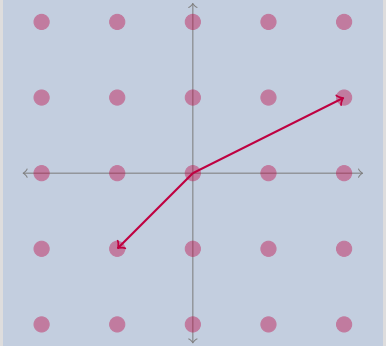


Hey! You promised, this will be easy!

OK, OK, we can say it easier: $\mathbb{Z}^2$ is a Lattice

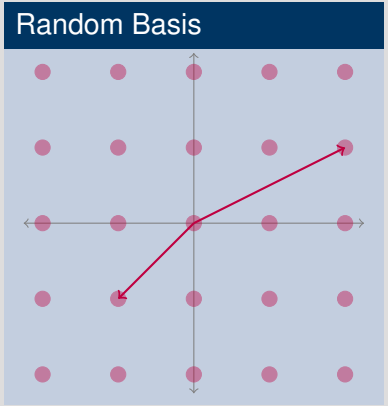
RUB

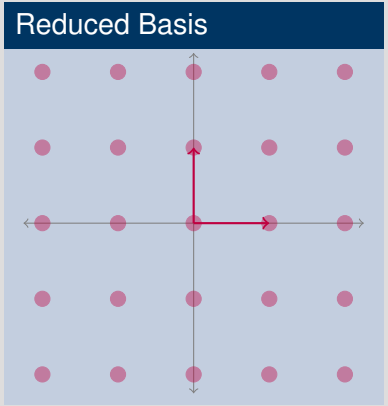
Random Basis



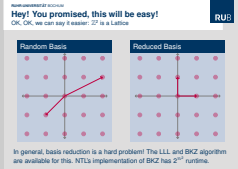
Hey! You promised, this will be easy!

OK, OK, we can say it easier: $\mathbb{Z}^2$ is a Lattice





In general, basis reduction is a hard problem! The LLL and BKZ algorithm are available for this. NTL's implementation of BKZ has 2^{n^2} runtime.



Hard Problems in Lattices...

...are what we need for crypto.

RUB

Shortest Vector Problem (SVP)

Given a lattice L, what is a shortest vector $v \in \mathrm{L} \setminus \{0\}$?

RUHR-UNIVERSITÄT BOCHUM
Hard Problems in Lattices...
...are what we need for crypto.
RUB
Shortest Vector Problem (SVP)
Given a lattice L, what is a shortest vector $v \in \mathrm{L} \setminus \{0\}$?

Hard Problems in Lattices...

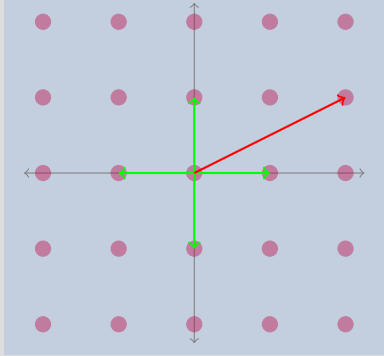
...are what we need for crypto.

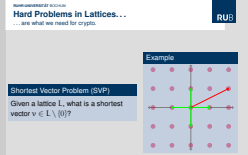
RUB

Shortest Vector Problem (SVP)

Given a lattice L, what is a shortest vector $v \in \mathrm{L} \setminus \{0\}$?

Example





Hard Problems in Lattices...

...are what we need for crypto.

RUB

Closest Vector Problem (CVP)

Given a lattice L and a target $\mathrm{t} \notin \mathrm{L}$,
what is the closest vector $\nu \in \mathrm{L}$ to t?

RUHR-UNIVERSITÄT BOCHUM
Hard Problems in Lattices...
...are what we need for crypto.
RUB
Closest Vector Problem (CVP)
Given a lattice L and a target $\mathrm{t} \notin \mathrm{L}$, what is the closest vector $\nu \in \mathrm{L}$ to t?

Hard Problems in Lattices...

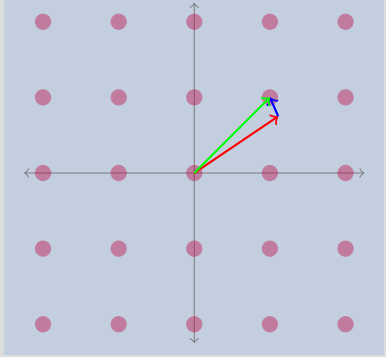
... are what we need for crypto.

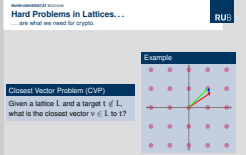
RUB

Closest Vector Problem (CVP)

Given a lattice L and a target $\mathrm{t} \notin \mathrm{L}$, what is the closest vector $\mathrm{v} \in \mathrm{L}$ to t?

Example

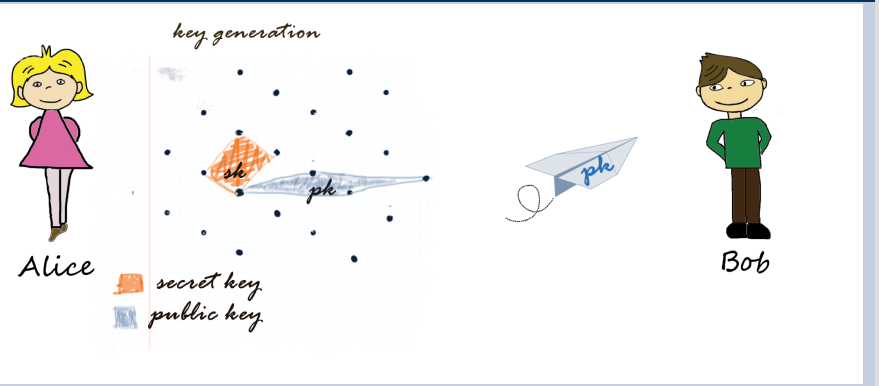




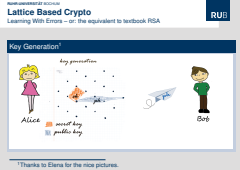
Lattice Based Crypto

Learning With Errors – or: the equivalent to textbook RSA

Key Generation[1]



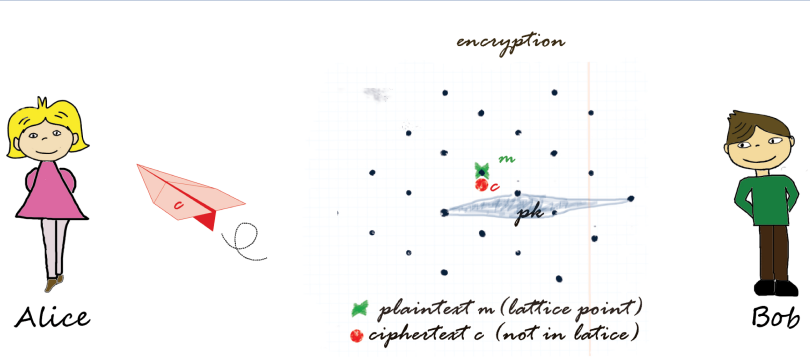
[1] Thanks to Elena for the nice pictures.

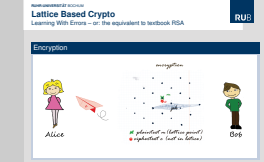


Lattice Based Crypto

Learning With Errors – or: the equivalent to textbook RSA

Encryption



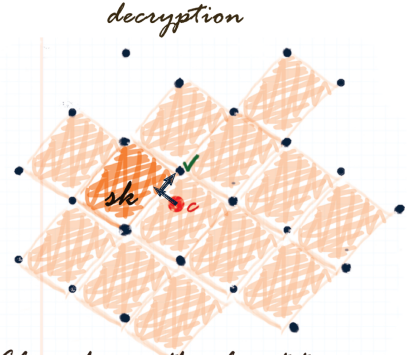


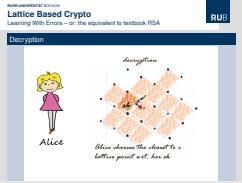
Lattice Based Crypto

Learning With Errors – or: the equivalent to textbook RSA

Decryption

Alice





Attack Algorithm

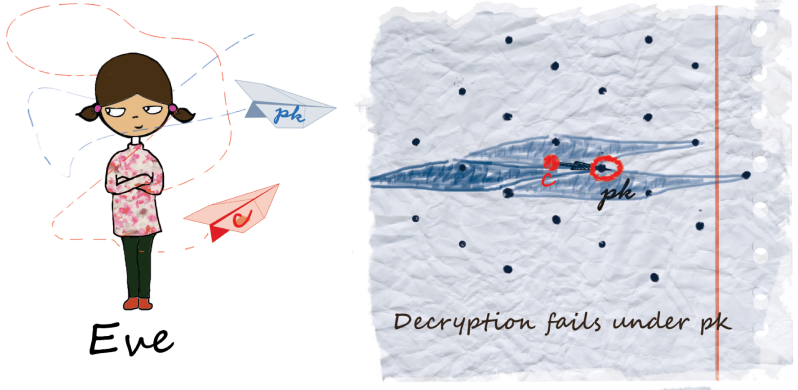
In practice most efficient strategy is Babai's Nearest Plane [Bab86], improved by Lindner and Peikert [LP11] and Gama *et al*. [GNR10].

In practice most efficient strategy is Babai's Nearest Plane [Bab86], improved by Lindner and Peikert [LP11] and Gama *et al*. [GNR10].

Nearest Plane
or BDD Enumeration

RUB

Attack



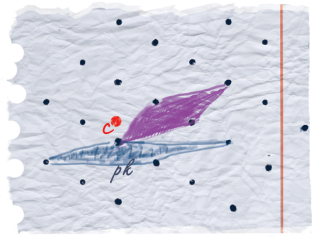
Nearest Plane
or BDD Enumeration

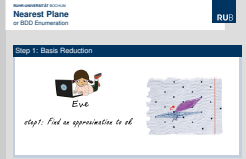
RUB

Step 1: Basis Reduction

Eve

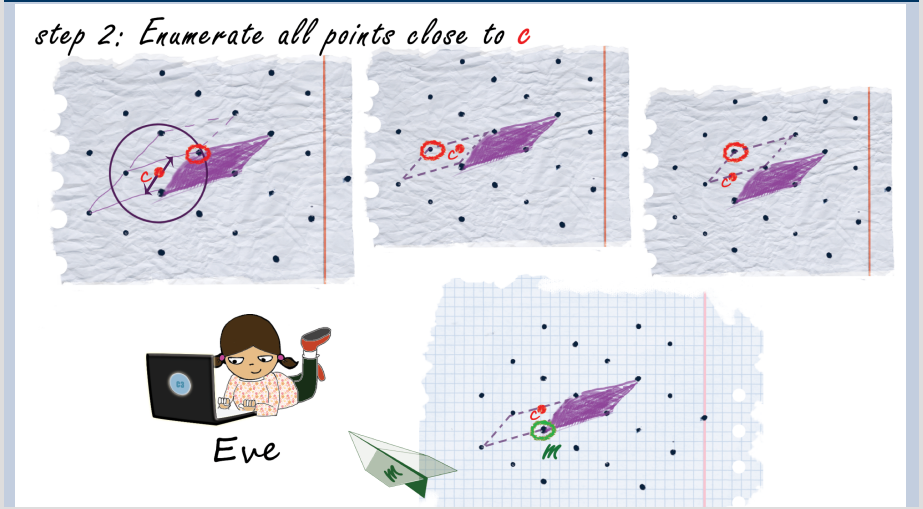
step1: Find an approximation to sk

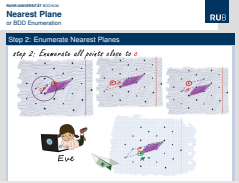




Nearest Plane
or BDD Enumeration

Step 2: Enumerate Nearest Planes





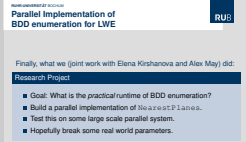
Parallel Implementation of BDD enumeration for LWE

RUB

Finally, what we (joint work with Elena Kirshanova and Alex May) did:

Research Project

- Goal: What is the *practical* runtime of BDD enumeration?
- Build a parallel implementation of `NearestPlanes`.
- Test this on some large scale parallel system.
- Hopefully break some real world parameters.

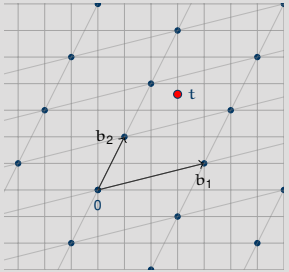


Parallelisation of Enumeration

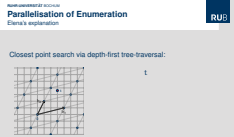
Elena's explanation

RUB

Closest point search via depth-first tree-traversal:



t

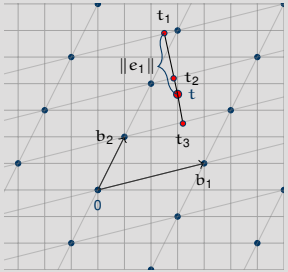


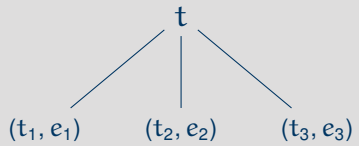
Parallelisation of Enumeration

Elena's explanation

RUB

Closest point search via depth-first tree-traversal:



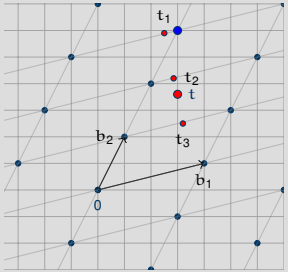


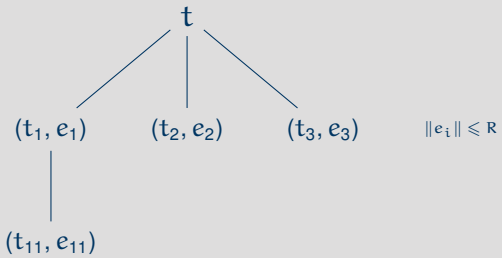
RUHR-UNIVERSITÄT BOCHUM
Parallelisation of Enumeration
Elena's explanation
RUB
Closest point search via depth-first tree-traversal:

Parallelisation of Enumeration

Elena's explanation

Closest point search via depth-first tree-traversal:





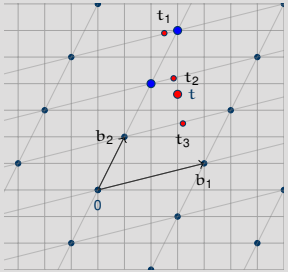
$\|e_i\| \leqslant R$

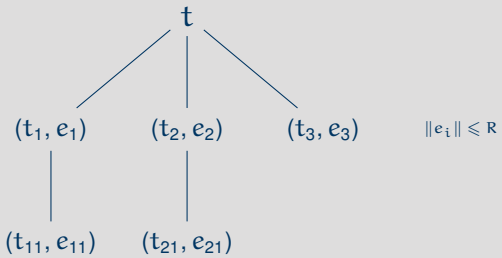
Parallelisation of Enumeration

Elena's explanation

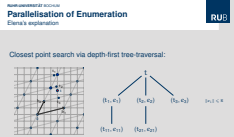
RUB

Closest point search via depth-first tree-traversal:





$\|e_i\| \leqslant R$

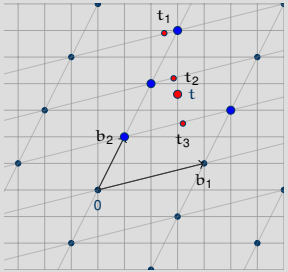


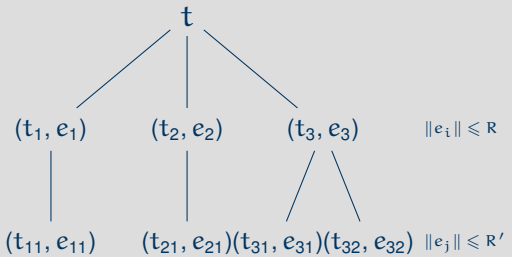
Parallelisation of Enumeration

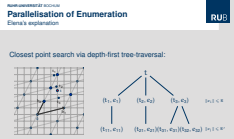
Elena's explanation

RUB

Closest point search via depth-first tree-traversal:





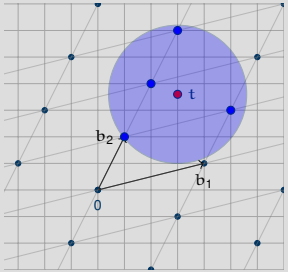


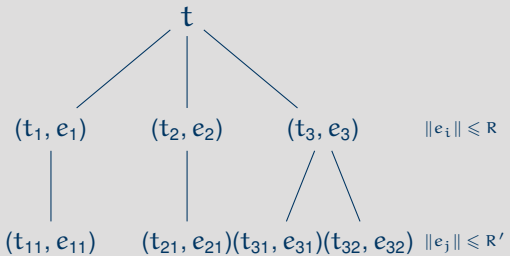
Parallelisation of Enumeration

Elena's explanation

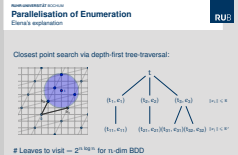
RUB

Closest point search via depth-first tree-traversal:





Leaves to visit $= 2^{n \log n}$ for n-dim BDD



Results

After more than one year of work, two submissions and something like over 9000 weeks of benchmarking

We ended up with:

Results

After more than one year of work, two submissions and something like over 9000 weeks of benchmarking

We ended up with:

- an open source implementation:
  `https://github.com/pfasante/cvp-enum`
- an ACNS paper [KMW16] and a Best Student Paper Award 😄
- huge table of runtimes

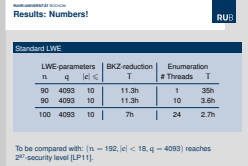
RUHR-UNIVERSITÄT BOCHUM
Results
RUB
After more than one year of work, two submissions and something like over 9000 weeks of benchmarking
We ended up with:
- an open source implementation: https://github.com/pfasante/cvp-enum
- an ACNS paper [KMW16] and a Best Student Paper Award
- huge table of runtimes

Results: Numbers!

Standard LWE

LWE-parameters			BKZ-reduction	Enumeration	
n	q	$\lvert e\rvert \leqslant$	T	# Threads	T
90	4093	10	11.3h	1	35h
90	4093	10	11.3h	10	3.6h
100	4093	10	7h	24	2.7h

To be compared with: $(n = 192, |e| < 18, q = 4093)$ reaches 2^{87}-security level [LP11].



Results: Numbers!

LWE variant: Small secret

LWE-parameters			BKZ-reduction	Enumeration	
n	q	m	T	# Threads	T
140	16411	170	12h	1	16h
140	16411	170	12h	10	1.7h

To be compared with: $(n = 128, q = 16411, m = 2^{28}, T = 13h)$ for combinatorial attack on LWE [KF15].

RUHR-UNIVERSITÄT BOCHUM
Results: Numbers!
LWE variant: Small secret
To be compared with: $(n = 128, q = 16411, m = 2^{28}, T = 13h)$ for combinatorial attack on LWE [KF15].

Results: Numbers!

LWE variant: Binary matrix

LWE-parameters			BKZ-reduction	Enumeration
n	q	m	T	T
256	500009	440	4.5h	2min

To be compared with: Estimation by Galbraith [Gal] roughly one day.

RUHR-UNIVERSITÄT BOCHUM
Results: Numbers!
LWE variant: Binary matrix
LWE-parameters | BKZ-reduction | Enumeration
n q m | T | T
256 500009 440 | 4.5h | 2min
To be compared with: Estimation by Galbraith [Gal] roughly one day.

Questions?

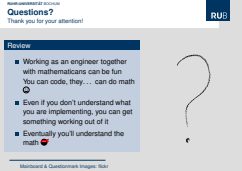
Thank you for your attention!

RUB

Review

- Working as an engineer together with mathematicans can be fun
  You can code, they… can do math ☺
- Even if you don't understand what you are implementing, you can get something working out of it
- Eventually you'll understand the math

Mainboard & Questionmark Images: flickr



References I

[Alk+16] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. “Post-quantum Key Exchange - A New Hope”. In: *USENIX Security Symposium*. USENIX Association, 2016, pp. 327–343.

[Bab86] L. Babai. “On Lovász’ lattice reduction and the nearest lattice point problem”. In: *Combinatorica* 6.1 (1986), pp. 1–13.

[ES16] L. Eldar and P. W. Shor. “An Efficient Quantum Algorithm for a Variant of the Closest Lattice-Vector Problem”. In: *arXiv Preprint Archive* (2016). URL: https://arxiv.org/abs/1611.06999.

[Fac16] Facebook. *Internet Defense Prize*. 2016. URL: https://internetdefenseprize.org/.

[Gal] S. D. Galbraith. “Space-efficient variants of cryptosystems based on learning with errors”. URL: https://www.math.auckland.ac.nz/~sgal018/compact-LWE.pdf.

[GNR10] N. Gama, P. Q. Nguyen, and O. Regev. “Lattice Enumeration Using Extreme Pruning”. In: *EUROCRYPT*. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 257–278.

[Gooa] Google. *CECPQ1 results*. URL: https://www.imperialviolet.org/2016/11/28/cecpq1.html.

References II

[Goob] Google. *Experimenting with Post-Quntum Cryptography.* URL: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.

[KF15] P. Kirchner and P. Fouque. “An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices”. In: *CRYPTO (1)*. Vol. 9215. Lecture Notes in Computer Science. Springer, 2015, pp. 43–62.

[KM15] N. Koblitz and A. Menezes. “A Riddle Wrapped in an Enigma”. In: *IACR Cryptology ePrint Archive* 2015 (2015), p. 1018.

[KMW16] E. Kirshanova, A. May, and F. Wiemer. “Parallel Implementation of BDD Enumeration for LWE”. In: *ACNS*. Vol. 9696. Lecture Notes in Computer Science. Springer, 2016, pp. 580–591.

[LP11] R. Lindner and C. Peikert. “Better Key Sizes (and Attacks) for LWE-Based Encryption”. In: *CT-RSA*. Vol. 6558. Lecture Notes in Computer Science. Springer, 2011, pp. 319–339.

[Reg] O. Regev. *Regarding the arXiv preprint by Eldar and Shor.* URL: https://groups.google.com/forum/#!topic/cryptanalytic-algorithms/WNMuTfJuSRc.