

# Attacks on Lattice Crypto

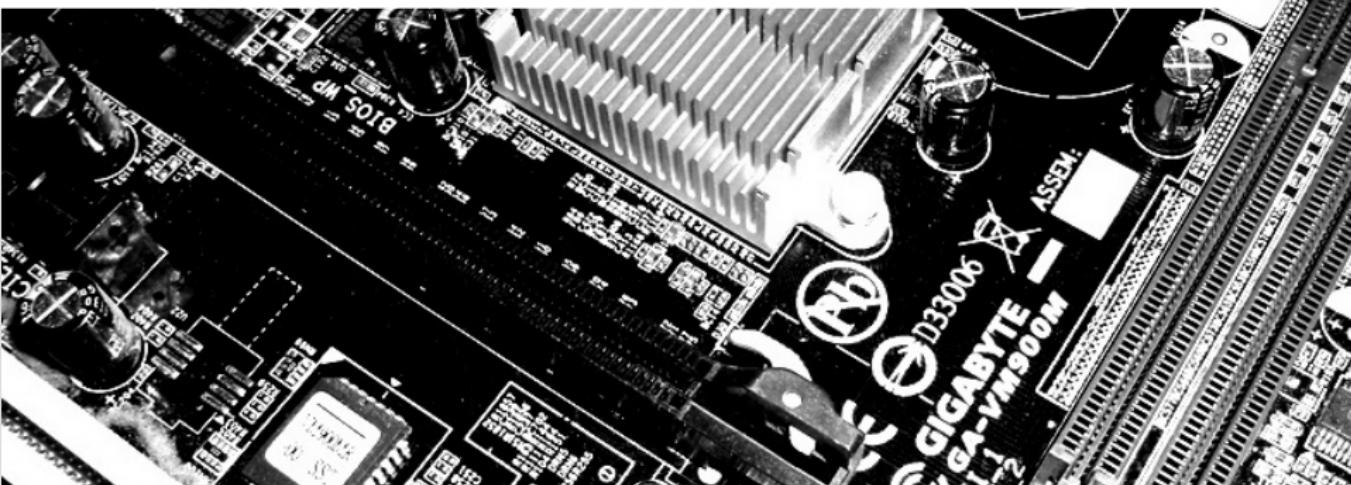
December 7th, 2016

FluxFingers

Workgroup Symmetric Cryptography

Ruhr University Bochum

Friedrich Wiemer



## Attacks on Lattice Crypto

2016-12-07



# Why is Lattice Based Crypto important?

Or interesting? Or...? Buzzword Bingo.



## Some facts

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

2016-12-07

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

└ Why is Lattice Based Crypto important?

# Why is Lattice Based Crypto important?

Or interesting? Or...? Buzzword Bingo.



## Some facts

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

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

└ Why is Lattice Based Crypto important?

2016-12-07

### 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.



## 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!

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

└ Why is Lattice Based Crypto important?

2016-12-07

### 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.



## 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), (The Holy Grail!)
  - Multi-linear Maps,
  - Identity-based Encryption (IBE),
  - ...

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

└ Why is Lattice Based Crypto important?

2016-12-07

### 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), (The Holy Grail!)
  - Multi-linear Maps,
  - Identity-based Encryption (IBE),
  - ...

# Why is Lattice Based Crypto important?

Is everything done?



## Fully Homomorphic Encryption



**GF(＼\_(＼)＼\_)**  
@hdevalence

Follow

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

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

└ Why is Lattice Based Crypto important?

2016-12-07

RUHR-UNIVERSITÄT BOCHUM  
Why is Lattice Based Crypto important?  
Is everything done?

Fully Homomorphic Encryption

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

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

└ The new cool kid in town.

2016-12-07

# 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

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting, . . .

└ The new cool kid in town.

2016-12-07

# 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
- Alkim *et al.* won this year’s Internet Defense Prize [Fac16] for their lattice based key exchange “New Hope” [Alk+16]

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting, . . .

└ The new cool kid in town.

2016-12-07

### 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.

## 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]

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting, . . .

└ The new cool kid in town.

2016-12-07

### 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.

## 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

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting, . . .

└ The new cool kid in town.

2016-12-07

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



## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

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

2016-12-07

A cryptographic thriller



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



## A cryptographic thriller

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



2016-12-07

## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

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



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

## 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]



## Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting,...

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

2016-12-07

### 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?

2016-12-07

Attacks on Lattice Crypto

└ Why is Lattice Crypto important, interesting, . . .

Enough motivation!

How does Lattice Crypto work?

# How does Lattice Based Crypto work?

Wait! Lattice, wtf?



## Definition:

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

## Attacks on Lattice Crypto

└ How does Lattice Crypto work?

└ How does Lattice Based Crypto work?

2016-12-07

Definition:  
A lattice  $L$  is an discrete, additive, abelian subgroup of  $\mathbb{R}^n$ .  
Wait! Lattice, wtf?

RUHR-UNIVERSITÄT BOCHUM  
How does Lattice Based Crypto work?  
Wait! Lattice, wtf?

RUB

# How does Lattice Based Crypto work?

Wait! Lattice, wtf?



## Definition:

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

## Definition:

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

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

is a lattice.

2016-12-07

## Attacks on Lattice Crypto

└ How does Lattice Crypto work?

└ How does Lattice Based Crypto work?

**Definition:**  
A lattice  $L$  is an discrete, additive, abelian subgroup of  $\mathbb{R}^n$ .  
**Definition:**  
Let  $b_1, b_2, \dots, b_d \in \mathbb{R}^n$ ,  $d \leq n$  linear independent. Then the set  

$$L = \left\{ v \in \mathbb{R}^n \mid v = \sum_{i=1}^d a_i b_i, a_i \in \mathbb{Z} \right\}$$
is a lattice.

Hey! You promised, this will be easy!

Lattice, dt.: Gitter



2016-12-07

## Attacks on Lattice Crypto

- └ How does Lattice Crypto work?

- └ Hey! You promised, this will be easy!

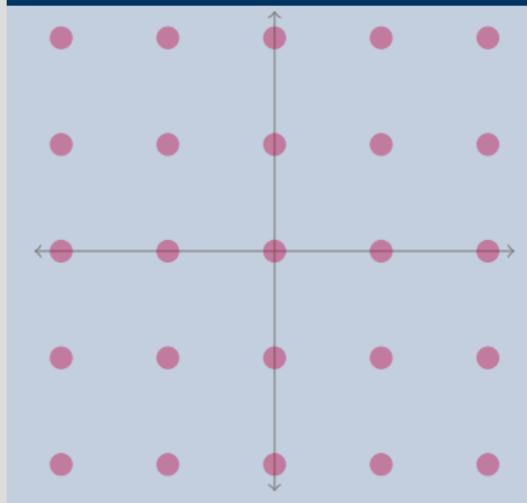


# Hey! You promised, this will be easy!

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



Example lattice



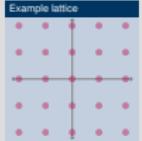
In general, basis reduction is a hard problem! The LLL and BKZ algorithm are available for this. NTL's implementation of BKZ has  $2^{n^2}$  runtime.

2016-12-07

## Attacks on Lattice Crypto

└ How does Lattice Crypto work?

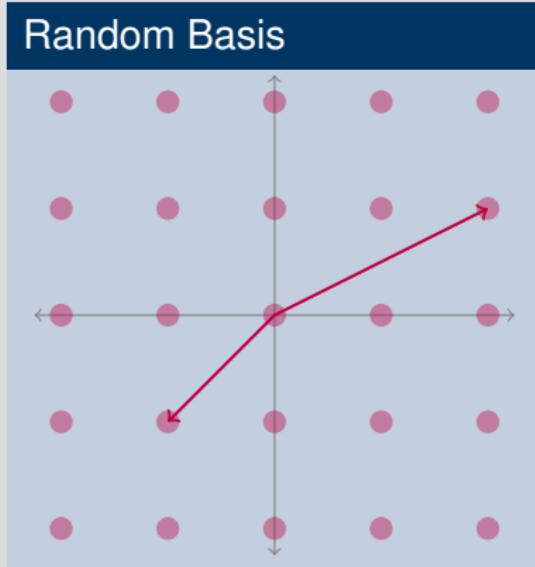
└ Hey! You promised, this will be easy!



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.

# Hey! You promised, this will be easy!

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



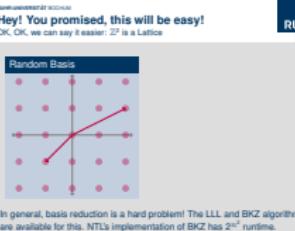
In general, basis reduction is a hard problem! The LLL and BKZ algorithm are available for this. NTL's implementation of BKZ has  $2^{n^2}$  runtime.

2016-12-07

## Attacks on Lattice Crypto

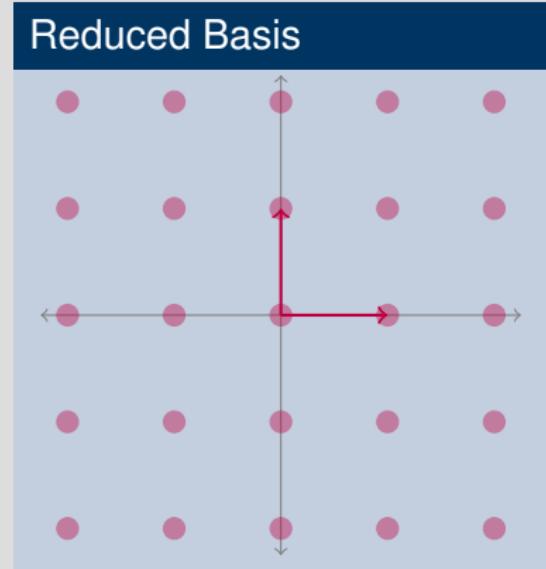
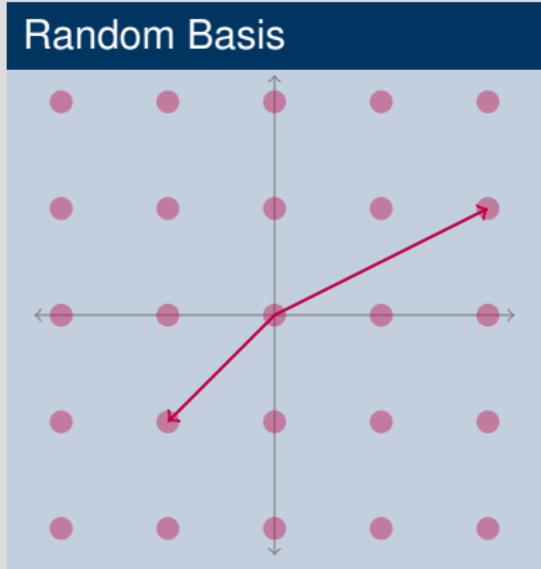
└ How does Lattice Crypto work?

└ Hey! You promised, this will be easy!



# Hey! You promised, this will be easy!

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



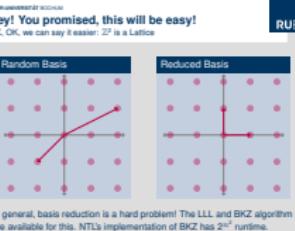
In general, basis reduction is a hard problem! The LLL and BKZ algorithm are available for this. NTL's implementation of BKZ has  $2^{n^2}$  runtime.

2016-12-07

## Attacks on Lattice Crypto

└ How does Lattice Crypto work?

└ Hey! You promised, this will be easy!



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.

## Shortest Vector Problem (SVP)

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

2016-12-07      Attacks on Lattice Crypto  
└ How does Lattice Crypto work?  
    └ Hard Problems in Lattices...

Shortest Vector Problem (SVP)  
Given a lattice  $L$ , what is the shortest vector  $v \in L \setminus \{0\}$ ?

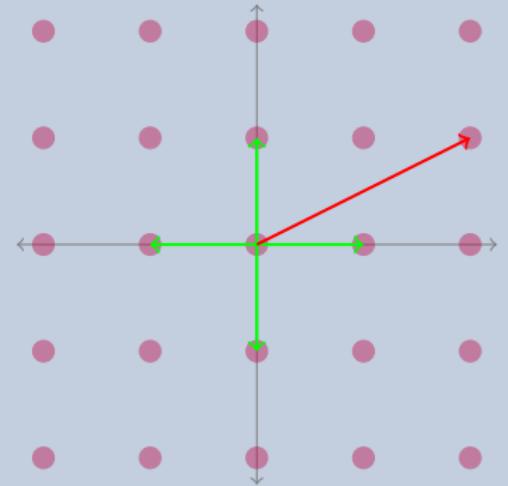
# Hard Problems in Lattices...

...are what we need for crypto.

## Shortest Vector Problem (SVP)

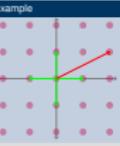
Given a lattice  $L$ , what is the shortest vector  $v \in L \setminus \{0\}$ ?

### Example



2016-12-07

- Attacks on Lattice Crypto
  - └ How does Lattice Crypto work?
    - └ Hard Problems in Lattices...



# Hard Problems in Lattices...

...are what we need for crypto.



2016-12-07 Attacks on Lattice Crypto  
└ How does Lattice Crypto work?  
  └ Hard Problems in Lattices...

Closest Vector Problem (CVP)  
Given a lattice  $L$  and a target  $t \notin L$ ,  
what is the closest vector  $v \in L$  to  $t$ ?

## Closest Vector Problem (CVP)

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

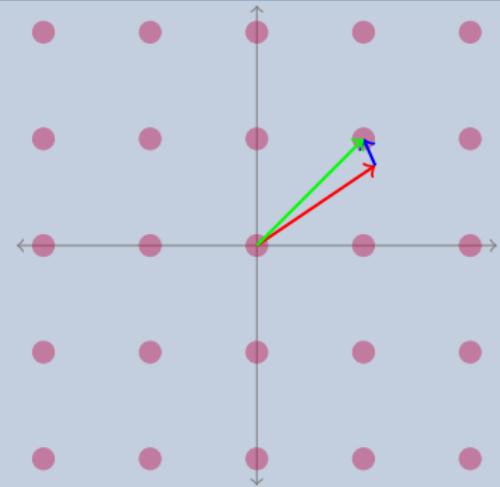
# Hard Problems in Lattices...

...are what we need for crypto.

## Closest Vector Problem (CVP)

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

### Example



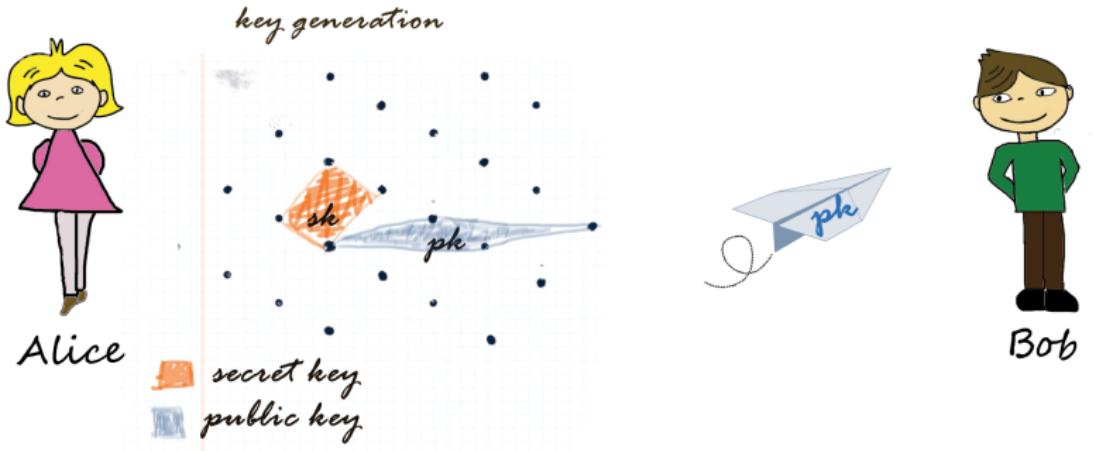
2016-12-07

- Attacks on Lattice Crypto
  - └ How does Lattice Crypto work?
    - └ Hard Problems in Lattices...

# Lattice Based Crypto

Learning With Errors – or: the equivalent to textbook RSA

## Key Generation<sup>1</sup>



<sup>1</sup>Thanks to Elena for the nice pictures.

## Attacks on Lattice Crypto

- └ How does Lattice Crypto work?
- └ Lattice Based Crypto

2016-12-07

RUHR-UNIVERSITÄT BOCHUM  
Lattice Based Crypto  
Learning With Errors – or: the equivalent to textbook RSA  
RUB

Key Generation<sup>1</sup>

Alice (secret key) → Bob (public key)

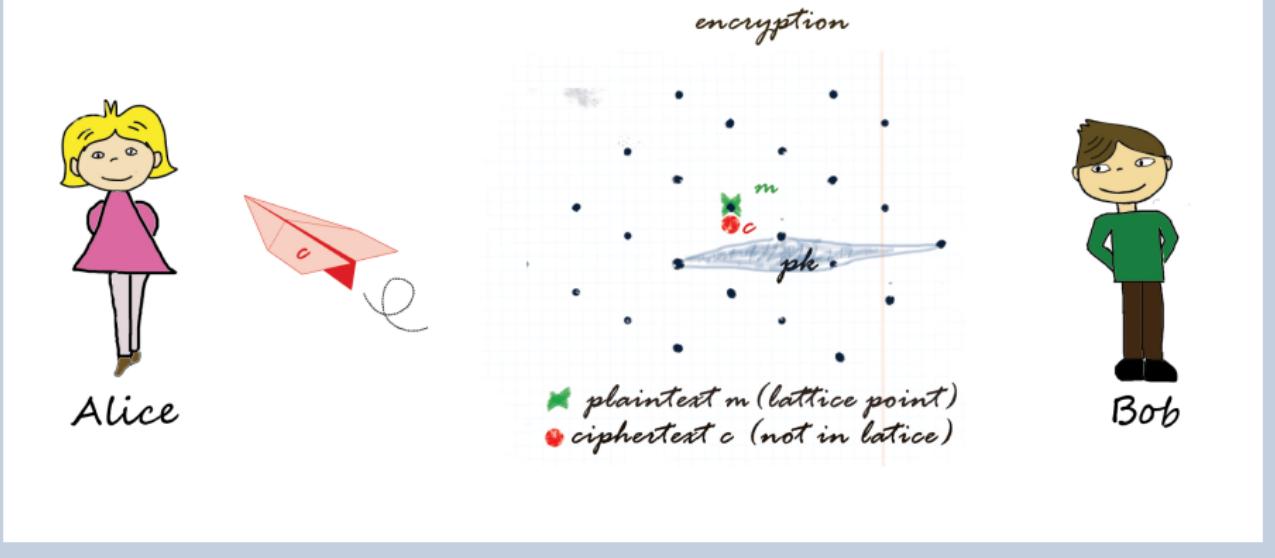
Bob

<sup>1</sup>Thanks to Elena for the nice pictures.

# Lattice Based Crypto

Learning With Errors – or: the equivalent to textbook RSA

## Encryption



2016-12-07

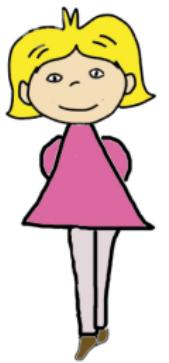
- Attacks on Lattice Crypto
  - └ How does Lattice Crypto work?
  - └ Lattice Based Crypto

A screenshot of a presentation slide titled "Encryption". The slide features two cartoon characters, Alice and Bob, and a 2D grid representing a lattice. A green dot labeled "plaintext  $m$  (lattice point)" and a red dot labeled "ciphertext  $c$  (not in lattice)" are shown. A blue shaded region labeled "pk" represents the public key. The slide is part of a larger presentation titled "Attacks on Lattice Crypto" and includes the subtitle "Learning With Errors – or: the equivalent to textbook RSA". The RUB logo is visible in the top right corner.

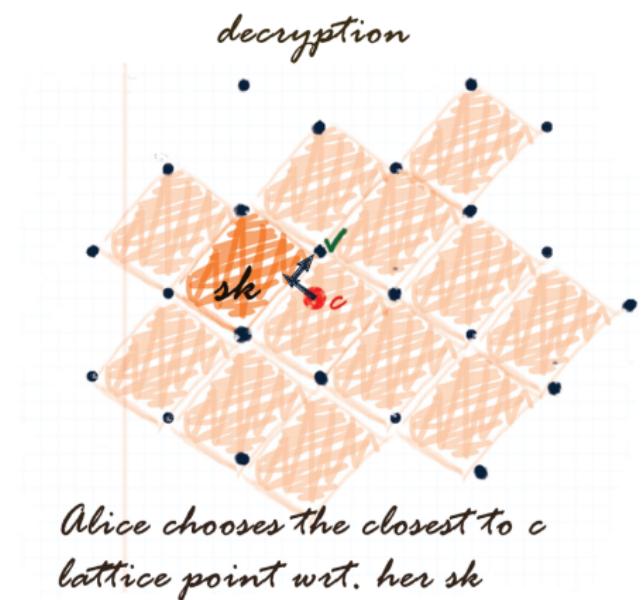
# Lattice Based Crypto

Learning With Errors – or: the equivalent to textbook RSA

## Decryption



Alice



2016-12-07

- Attacks on Lattice Crypto
  - └ How does Lattice Crypto work?
    - └ Lattice Based Crypto

RUHR-UNIVERSITÄT BOCHUM  
Lattice Based Crypto  
Learning With Errors – or: the equivalent to textbook RSA

Decryption

A small diagram on the right side of the slide. It shows a 2D grid lattice with several black dots representing lattice points. A red shaded area surrounds one specific black dot, which is labeled 'c'. A green arrow points from a point labeled 'sh' to this red-shaded dot. The text 'Alice chooses the closest to c lattice point w.r.t. her sh' is written below the diagram. In the top right corner of the slide, there is a small logo for Ruhr University Bochum.

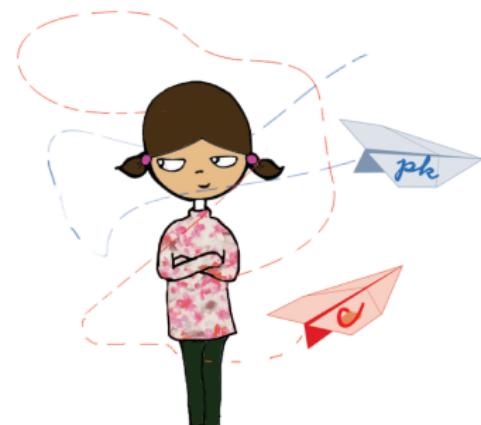
In practice most efficient strategy is Babai's Nearest Plane [Bab86], improved by Lindner and Peikert [LP11] and Gama *et al.* [GNR10].

2016-12-07

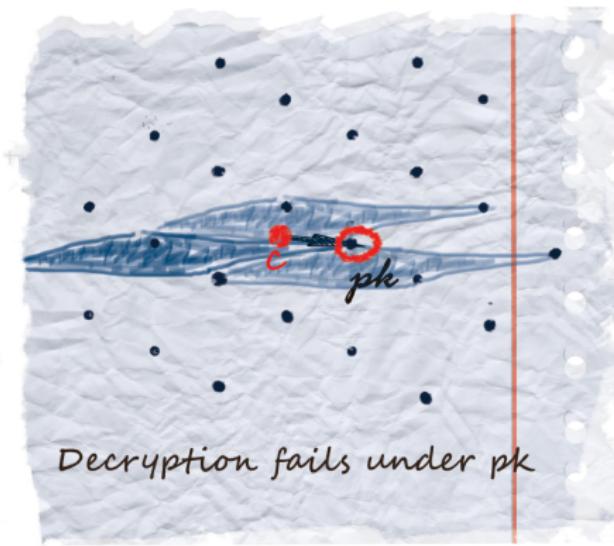
Attacks on Lattice Crypto  
└ Attacks on Lattice Based Crypto  
    └ Attack Algorithm

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

## Attack



Eve



Decryption fails under pk

2016-12-07

- Attacks on Lattice Crypto
  - Attacks on Lattice Based Crypto
    - Nearest Plane

RUHR-UNIVERSITÄT BOCHUM  
Nearest Plane  
or BDD Enumeration

RUB

Attack

A small version of the Eve illustration from the main slide, showing her standing next to a crumpled paper diagram of a lattice. The text 'Decryption fails under pk' is visible at the bottom right of the diagram.

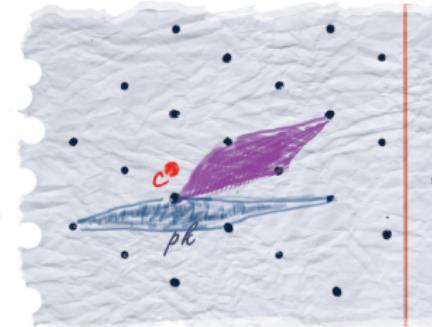
Eve

Decryption fails under pk

## Step 1: Basis Reduction



*step1: Find an approximation to  $s_k$*



2016-12-07

- Attacks on Lattice Crypto
  - Attacks on Lattice Based Crypto
    - Nearest Plane

Step 1: Basis Reduction

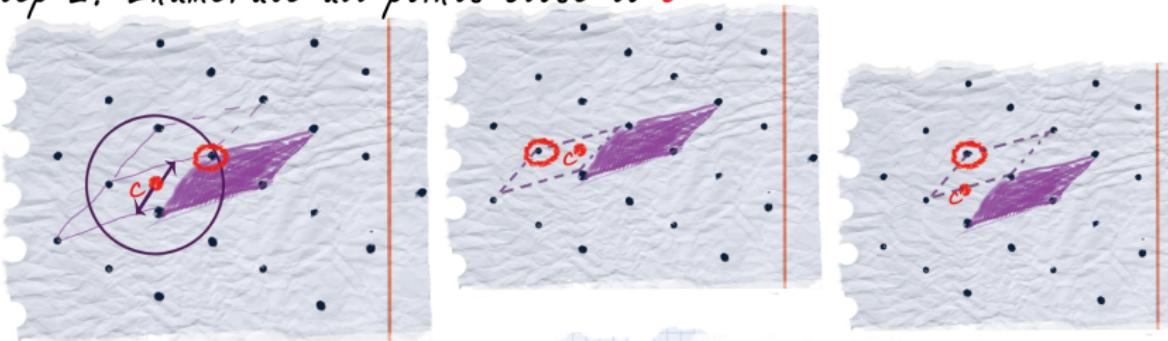
Eve

*step1: Find an approximation to  $s_k$*

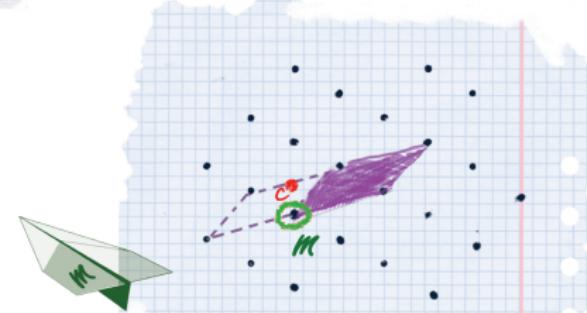
# Nearest Plane or BDD Enumeration

## Step 2: Enumerate Nearest Planes

step 2: Enumerate all points close to  $c$



Eve



2016-12-07

- Attacks on Lattice Crypto
  - Attacks on Lattice Based Crypto
    - Nearest Plane

RUHR-UNIVERSITÄT BOCHUM  
Nearest Plane  
or BDD Enumeration

Step 2: Enumerate Nearest Planes

Step 2: Enumerate all points close to  $c$

# Parallel Implementation of BDD enumeration for LWE

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.

2016-12-07

## Attacks on Lattice Crypto

└ OK. And what did I do?

└ Parallel Implementation of BDD enumeration for LWE

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

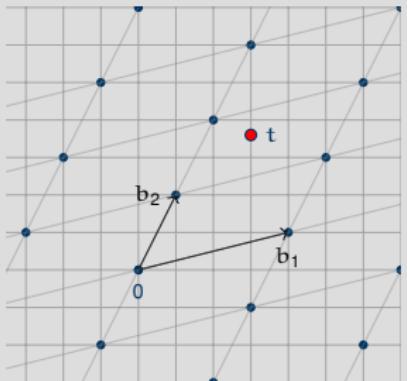
- Goal: What is the practical runtime of BDD enumeration?
- Build a parallel implementation of NearestPlanes.
- Test this on some large scale parallel system.
- Hopefully break some real world parameters.

# Parallelisation of Enumeration

Elena's explanation



Closest point search via depth-first tree-traversal:



$t$

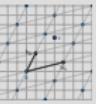
2016-12-07

## Attacks on Lattice Crypto

└ OK. And what did I do?

└ Parallelisation of Enumeration

Closest point search via depth-first tree-traversal:



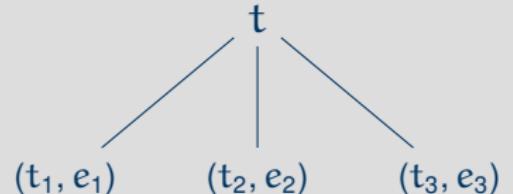
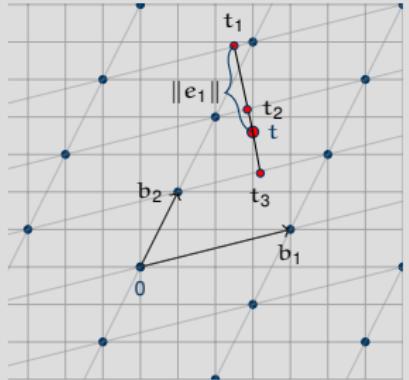
t

# Parallelisation of Enumeration

Elena's explanation



Closest point search via depth-first tree-traversal:

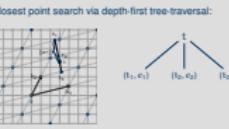


2016-12-07

## Attacks on Lattice Crypto

└ OK. And what did I do?

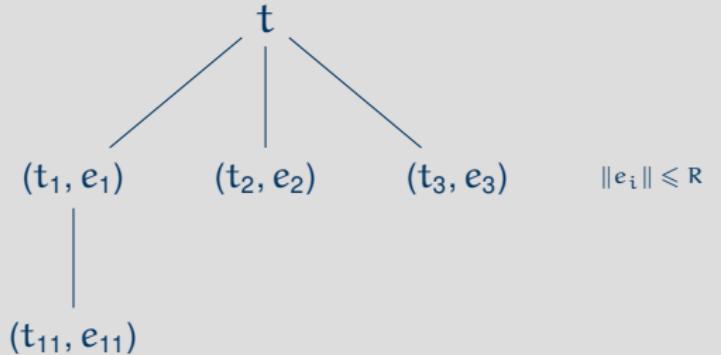
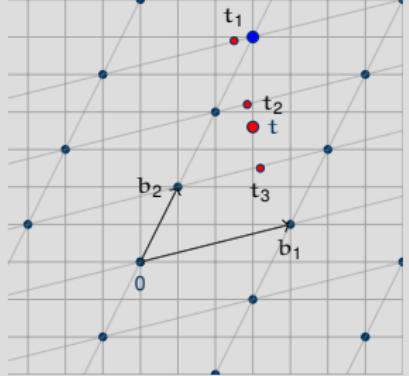
└ Parallelisation of Enumeration



# Parallelisation of Enumeration

Elena's explanation

Closest point search via depth-first tree-traversal:



2016-12-07

## Attacks on Lattice Crypto

- └ OK. And what did I do?

- └ Parallelisation of Enumeration

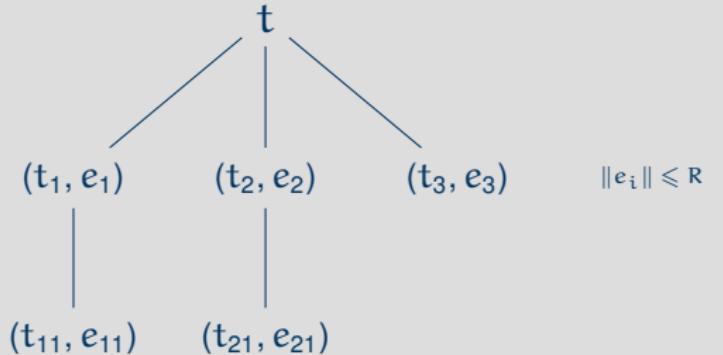
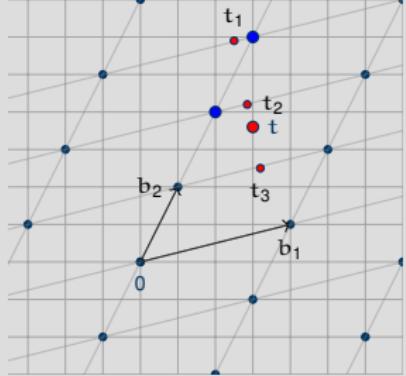
Closest point search via depth-first tree-traversal:



# Parallelisation of Enumeration

Elena's explanation

Closest point search via depth-first tree-traversal:



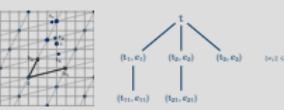
2016-12-07

## Attacks on Lattice Crypto

- └ OK. And what did I do?

- └ Parallelisation of Enumeration

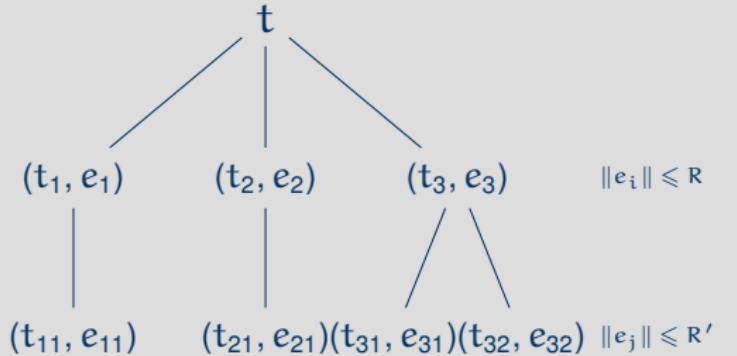
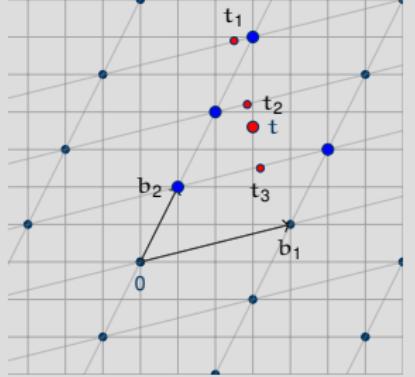
Closest point search via depth-first tree-traversal:



# Parallelisation of Enumeration

Elena's explanation

Closest point search via depth-first tree-traversal:



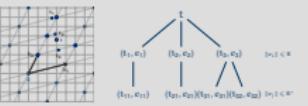
2016-12-07

## Attacks on Lattice Crypto

- └ OK. And what did I do?

- └ Parallelisation of Enumeration

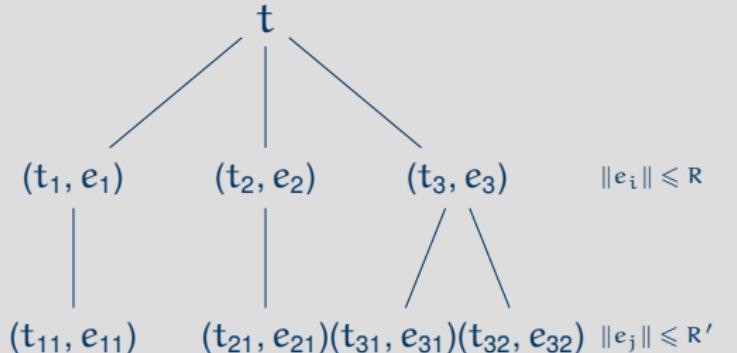
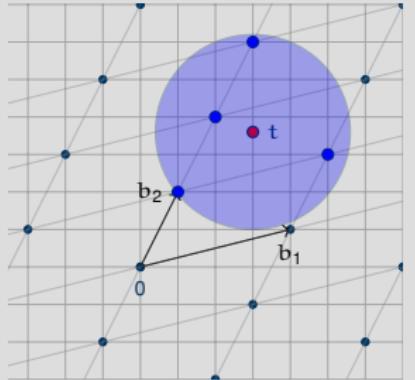
Closest point search via depth-first tree-traversal:



# Parallelisation of Enumeration

Elena's explanation

Closest point search via depth-first tree-traversal:



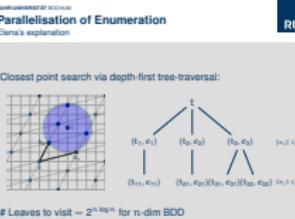
$\# \text{Leaves to visit} = 2^{n \log n}$  for  $n$ -dim BDD

2016-12-07

## Attacks on Lattice Crypto

- └ OK. And what did I do?

- └ Parallelisation of Enumeration



# Results



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

We ended up with:

2016-12-07

Attacks on Lattice Crypto  
└ OK. And what did I do?  
  └ 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

2016-12-07

## Attacks on Lattice Crypto

### └ OK. And what did I do?

#### └ 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

# Results: Numbers!



## Standard LWE

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

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

2016-12-07

## Attacks on Lattice Crypto

└ OK. And what did I do?

└ Results: Numbers!

Standard LWE			Results: Numbers!	
LWE-parameters			BKZ-reduction	Enumeration
n	q	$ e  \leqslant$	T	T
90	4093	10	11.3h	1
90	4093	10	11.3h	10
100	4093	10	7h	24

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].

2016-12-07

## Attacks on Lattice Crypto

└ OK. And what did I do?

└ 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].

# 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.

2016-12-07

## Attacks on Lattice Crypto

└ OK. And what did I do?

└ Results: Numbers!

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!

## Review

- Working as an engineer together with mathematicians 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

# Attacks on Lattice Crypto

└ OK. And what did I do?

└ Questions?

2016-12-07

RUHR-UNIVERSITÄT BOCHUM  
**Questions?**  
Thank you for your attention!

Review

- Working as an engineer together with mathematicians 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>.

2016-12-07

# Attacks on Lattice Crypto

## └ OK. And what did I do?

### └ References

RUHR-UNIVERSITÄT BOCHUM	
References I	
[Alk+16]	E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. "Post-quantum Key Exchange - A New Hope". In: <i>USENIX Security Symposium</i> . USENIX Association, 2016, pp. 327–343.
[Bab86]	L. Babai. "On Lovász' lattice reduction and the nearest lattice point problem". In: <i>Combinatorica</i> 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: <i>arXiv Preprint Archive</i> (2016). URL: <a href="https://arxiv.org/abs/1611.06999">https://arxiv.org/abs/1611.06999</a> .
[Fac16]	Facebook. <i>Internet Defense Prize</i> . 2016. URL: <a href="https://internetdefenseprize.org/">https://internetdefenseprize.org/</a> .
[Gal]	S. D. Galbraith. "Space-efficient variants of cryptosystems based on learning with errors". URL: <a href="https://www.math.auckland.ac.nz/~sgal018/compact-LWE.pdf">https://www.math.auckland.ac.nz/~sgal018/compact-LWE.pdf</a> .
[GNR10]	N. Gama, P. Q. Nguyen, and O. Regev. "Lattice Enumeration Using Extreme Pruning". In: <i>EUROCRYPT</i> . Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 257–278.
[Gooa]	Google. <i>CECPQ1 results</i> . URL: <a href="https://www.imperialviolet.org/2016/11/28/cecpq1.html">https://www.imperialviolet.org/2016/11/28/cecpq1.html</a> .

- [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>.

2016-12-07

# Attacks on Lattice Crypto

## └ OK. And what did I do?

### └ References

	RUHR-UNIVERSITÄT BOCHUM	References II	RUB
[Goob]	Google. <i>Experimenting with Post-Quntum Cryptography</i> . URL: <a href="https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html">https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html</a> .		
[KF15]	P. Kirchner and P. Fouque. “An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices”. In: <i>CRYPTO (1)</i> . 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: <i>IACR Cryptology ePrint Archive</i> 2015 (2015), p. 1018.		
[KMW16]	E. Kirshanova, A. May, and F. Wiemer. “Parallel Implementation of BDD Enumeration for LWE”. In: <i>ACNS</i> . 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: <i>CT-RSA</i> . Vol. 6558. Lecture Notes in Computer Science. Springer, 2011, pp. 319–339.		
[Reg]	O. Regev. <i>Regarding the arXiv preprint by Eldar and Shor</i> . URL: <a href="https://groups.google.com/forum/#!topic/cryptanalytic-algorithms/WNMuTfJuSRc">https://groups.google.com/forum/#!topic/cryptanalytic-algorithms/WNMuTfJuSRc</a> .		