Post-Quantum Cryptography from Lattices

Cryptographie post-quantique à base de réseaux euclidiens

Katharina Boudgoust

CNRS, Univ Montpellier, LIRMM, France

https://katinkabou.github.io/

Overview

Questions we try to answer today:

- *What is post-quantum cryptography?*
- *What are lattice problems?*
- *What is lattice-based cryptography?*
- *What are some (of my) current challenges?*

References:

- Crash Course Spring 2025
  https://katinkabou.github.io/LatticeClub2025.html
- The Lattice Club
  https://thelatticeclub.com/

Part 1:

Post-Quantum Cryptography

Cryptography

👉 The word **cryptography** is composed of the two ancient Greek words *kryptos* (hidden) and *graphein* (to write). Its goal is to provide **secure communication**.

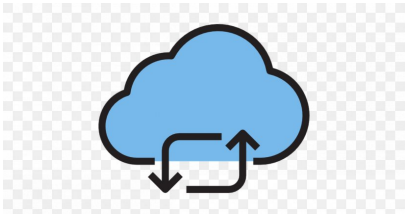
- Encryption
- Digital Signatures

Cryptography

👉 The word **cryptography** is composed of the two ancient Greek words *kryptos* (hidden) and *graphein* (to write). Its goal is to provide **secure communication**.

- Encryption
- Digital Signatures
- Zero-Knowledge Proofs
- Fully-Homomorphic Encryption

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9



Cryptography is everywhere!

Security Reductions

Security of cryptographic scheme ⟵ Mathematical problem

e.g. an adversary cannot find the secret key

e.g. it is difficult to factor a number N which is the product of two large primes $N = p \cdot q$

👉 The security in cryptography is based on presumably hard mathematical problems.

Current Security Paradigm

👉 The security in cryptography is based on presumably hard mathematical problems.

Currently used problems:

- Discrete logarithm
- Factoring

  Given N, find p, q such that $N = p \cdot q$

*Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal of Computations 1997

Current Security Paradigm

👉 The security in cryptography is based on presumably hard mathematical problems.

Currently used problems:

- ~~Discrete logarithm~~
- ~~Factoring~~

  Given N, find p, q such that $N = p \cdot q$

⚠ $\exists$ poly-time quantum algorithm [Sho97]*

Quantum-resistant candidates:

- Codes
- Lattices $\Rightarrow$ today's focus
- Isogenies
- Multivariate systems
- **?**

*Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal of Computations 1997

Post-Quantum Cryptography

👉 Post-quantum cryptography denotes schemes which plausibly resist attacks by quantum computers.

US National Institute of Standards and Technology (NIST) Project

- 2016: start of NIST's post-quantum cryptography project*
- 2022+25: selection of 5 schemes, 3 of them relying on lattice problems

Public Key Encryption:

- Kyber
- HQC

Digital Signature:

- Dilithium
- Falcon
- SPHINCS+

Lattice-based cryptography plays a leading role in designing post-quantum cryptography.

*https://csrc.nist.gov/projects/post-quantum-cryptography

Lattices are more than just post-quantum!

Example: Fully-Homomorphic Encryption

- Securely outsource data and do analysis on the encrypted data
- Very powerful
- Only known from lattices so far

Lattices are more than just post-quantum!

Example: Fully-Homomorphic Encryption

- Securely outsource data and do analysis on the encrypted data
- Very powerful
- Only known from lattices so far

BUT: Lattices also bring new challenges! More later . . .

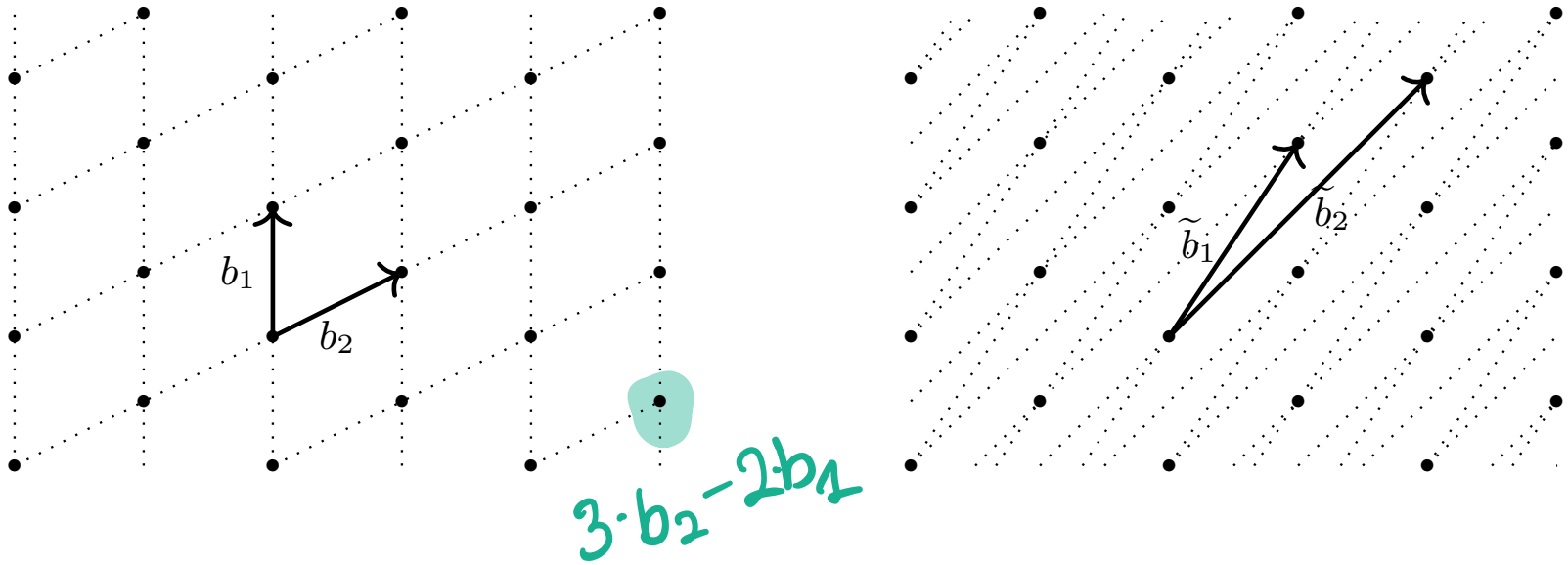
Part 2:

Euclidean Lattice Problems

Euclidean Lattices

Let $\mathbf{B} = (\mathbf{b}_i)_{i=1,\dots,n}$ be a set of linearly independent vectors over $\mathbb{R}$, defining the lattice

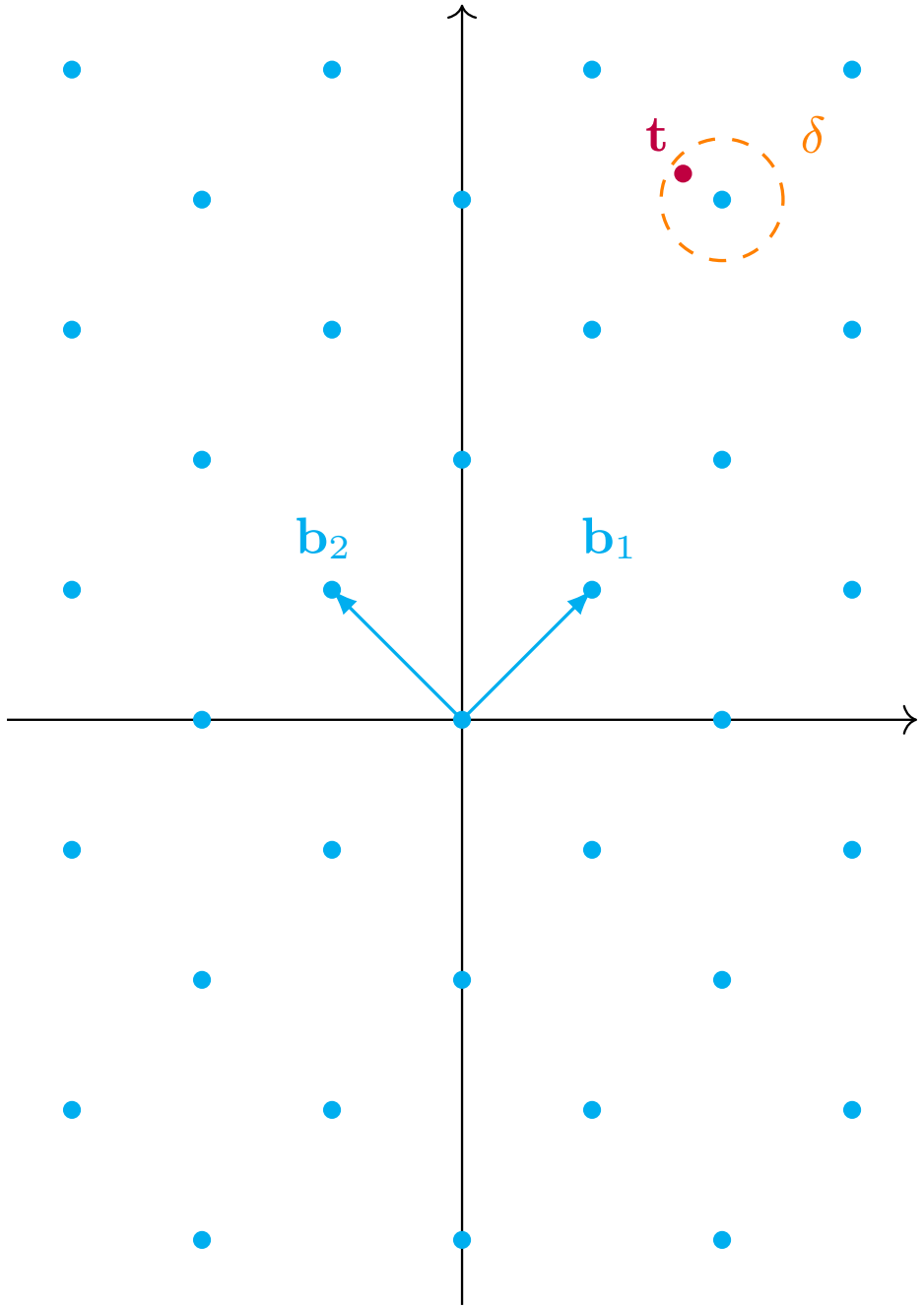
$$\Lambda(\mathbf{B}) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$



Bounded Distance Decoding

Given a lattice Λ and a target $\mathbf{t}$ such that

$$\text{dist}(\Lambda, \mathbf{t}) \leq \delta.$$



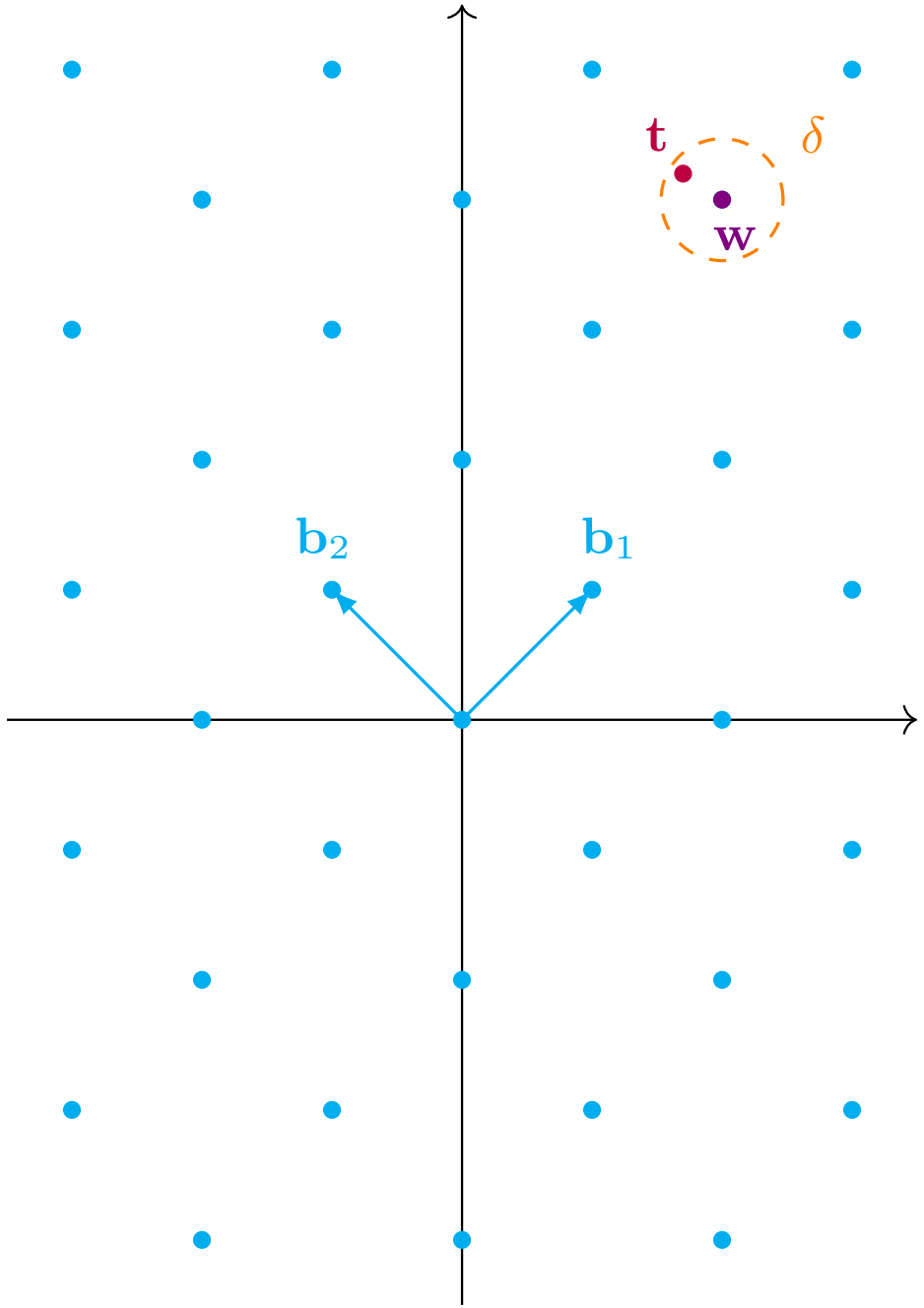
Bounded Distance Decoding

Given a lattice Λ and a target $\mathbf{t}$ such that

$$\text{dist}(\Lambda, \mathbf{t}) \leq \delta.$$

The **bounded distance decoding** (BDD) problem asks to find the unique vector $\mathbf{w} \in \Lambda$ such that

$$\|\mathbf{w} - \mathbf{t}\|_2 \leq \delta.$$



Bounded Distance Decoding

Given a lattice Λ and a target $\mathbf{t}$ such that

$$\text{dist}(\Lambda, \mathbf{t}) \leq \delta.$$

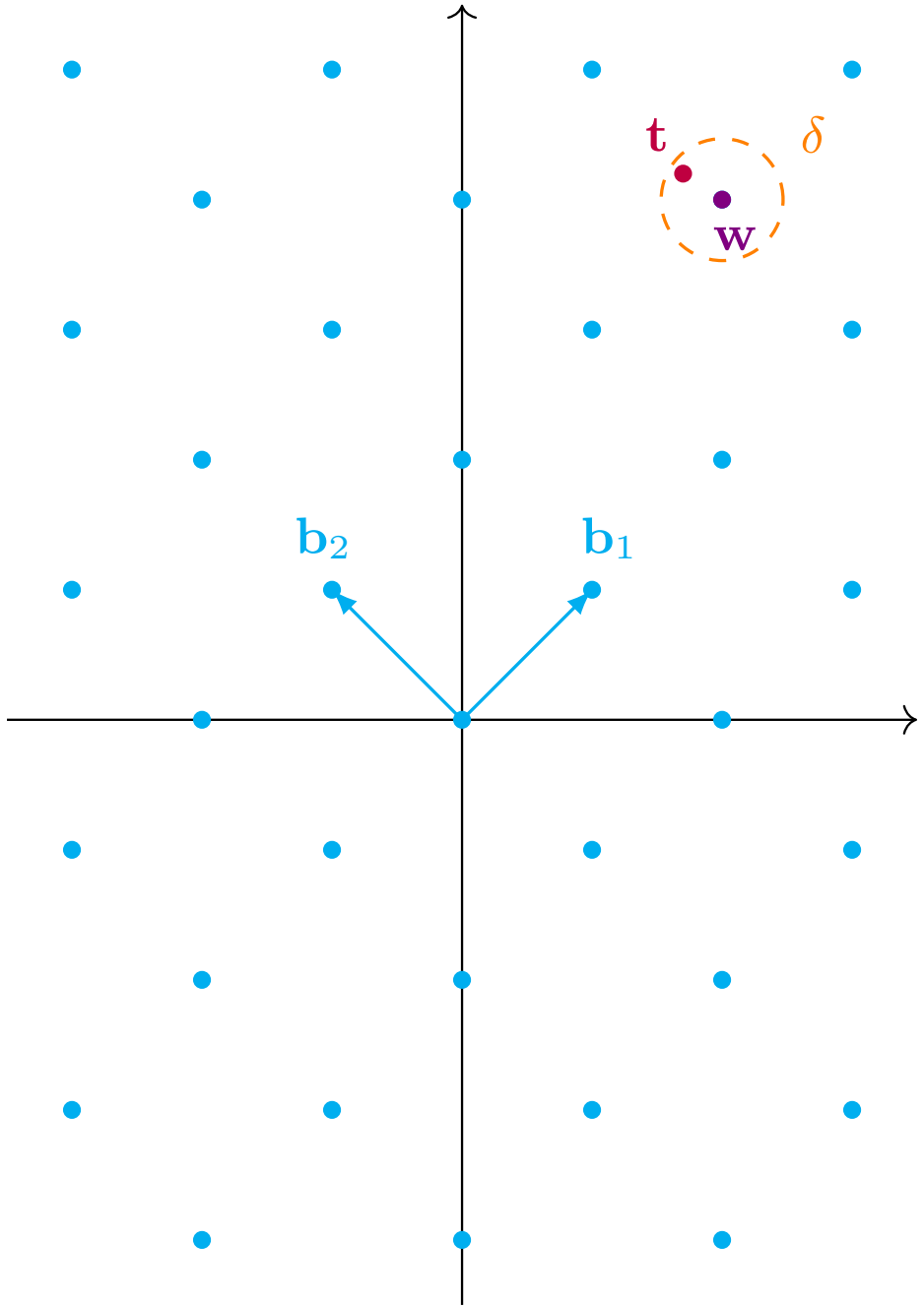
The **bounded distance decoding** (BDD) problem asks to find the unique vector $\mathbf{w} \in \Lambda$ such that

$$\|\mathbf{w} - \mathbf{t}\|_2 \leq \delta.$$

The complexity of BDD increases with the lattice dimension and promised radius δ.

Conjecture:

There is no polynomial-time classical or quantum algorithm that solves BDD **for all** lattices to within polynomial factors.



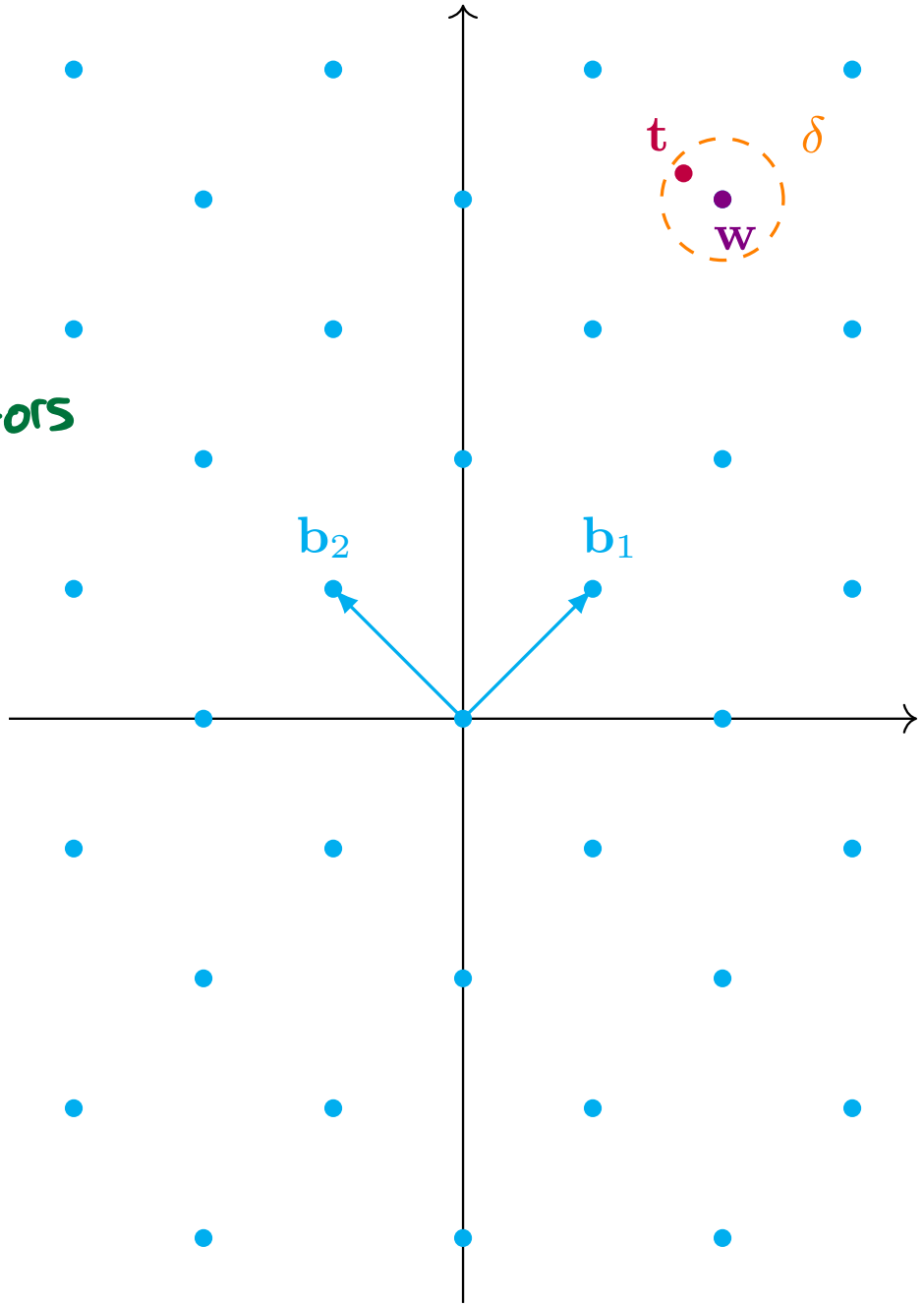
Bounded Distance Decoding

But: BDD might be easy to solve for some lattices!

Example: $\Lambda = \mathbb{Z}^n$ generated by unit vectors

↝ simply round

How do we sample "hard" instances?



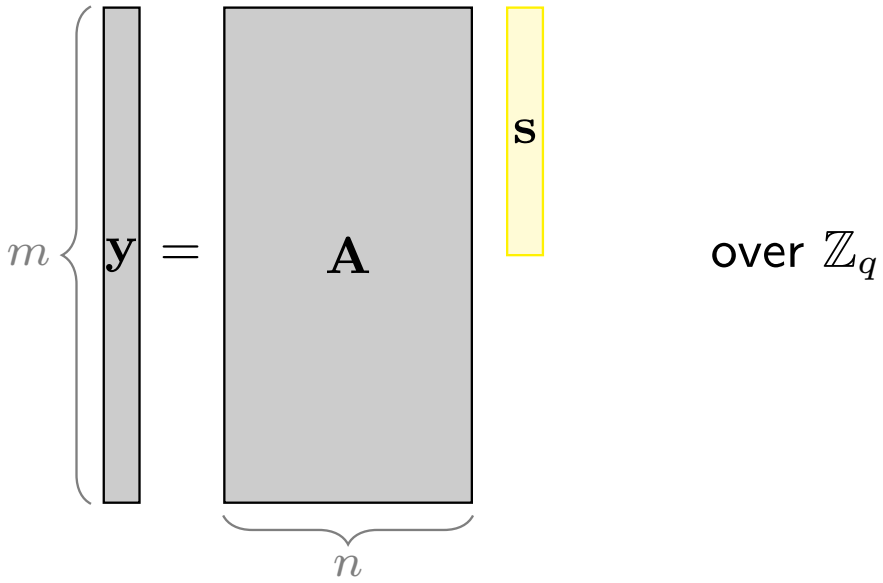
Conjecture:

There is no polynomial-time classical or quantum algorithm that solves BDD **for all** lattices to within polynomial factors.

A family of random lattices

$\mathbb{Z}_q$ = Integers modulo q
$= \{0, \ldots, q-1\}$

- Let $\mathbb{Z}_q$ be a finite field
- Sample $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ uniformly at random
- Define the lattice $\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}\mathbf{s} \bmod q \text{ for some } \mathbf{s} \in \mathbb{Z}^n\}$



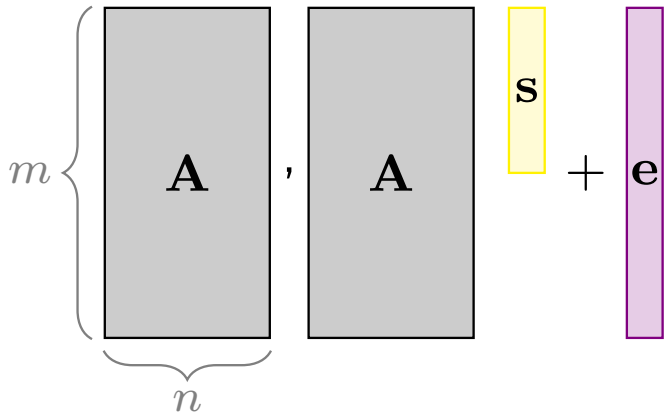
over $\mathbb{Z}_q$

Learning With Errors

Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random.

Given a vector $\mathbf{b} \in \mathbb{Z}_q^m$, where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ for

- secret $\mathbf{s} \in \mathbb{Z}^n$ sampled from distribution D_s and
- noise/error $\mathbf{e} \in \mathbb{Z}^m$ sampled from distribution D_e such that $\|\mathbf{e}\|_2 \leq \delta \ll q$.



Learning With Errors

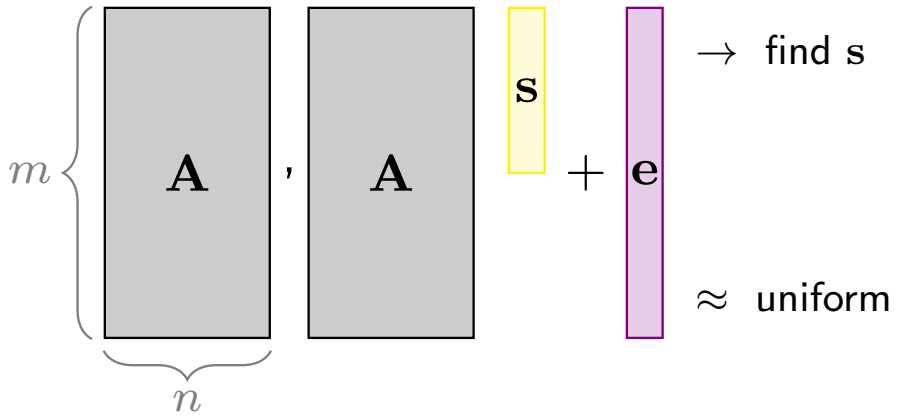
Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random.

Given a vector $\mathbf{b} \in \mathbb{Z}_q^m$, where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ for

- secret $\mathbf{s} \in \mathbb{Z}^n$ sampled from distribution D_s and
- noise/error $\mathbf{e} \in \mathbb{Z}^m$ sampled from distribution D_e such that $\|\mathbf{e}\|_2 \leq \delta \ll q$.

Search learning with errors (S-LWE) asks to find $\mathbf{s}$.

Decision learning with errors (D-LWE) asks to distinguish $(\mathbf{A}, \mathbf{b})$ from the uniform distribution over $\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$.



Learning With Errors

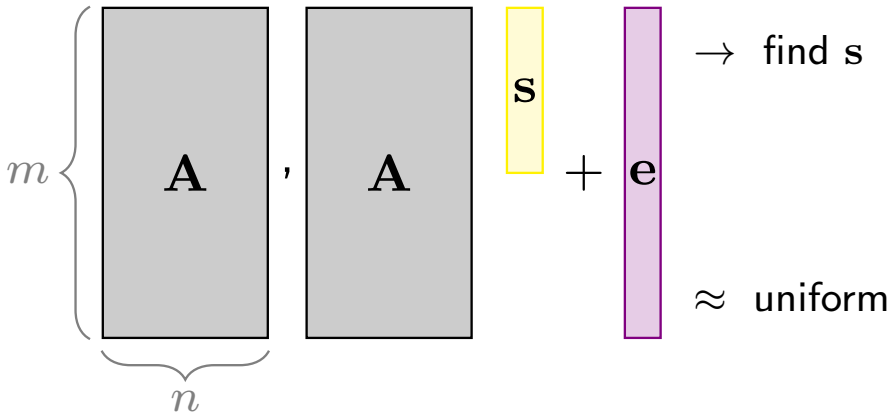
Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random.

Given a vector $\mathbf{b} \in \mathbb{Z}_q^m$, where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ for

- secret $\mathbf{s} \in \mathbb{Z}^n$ sampled from distribution D_s and
- noise/error $\mathbf{e} \in \mathbb{Z}^m$ sampled from distribution D_e such that $\|\mathbf{e}\|_2 \leq \delta \ll q$.

Search learning with errors (S-LWE) asks to find $\mathbf{s}$.

Decision learning with errors (D-LWE) asks to distinguish $(\mathbf{A}, \mathbf{b})$ from the uniform distribution over $\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$.



⚠ The present noise makes S-LWE a hard problem.

⚠ The norm restriction on $\mathbf{e}$ makes D-LWE a hard problem!

Learning With Errors

- Introduced by [Reg05]*
- Most important hardness assumption in lattice-based cryptography
- $=$ Bounded distance decoding in random lattices $\Lambda_q(\mathbf{A})$
- $\approx$ Solving random noisy linear equations over finite fields

*Regev, *On lattices, learning with errors, random linear codes, and cryptography*, STOC'05

Example Parameters for Learning With Errors

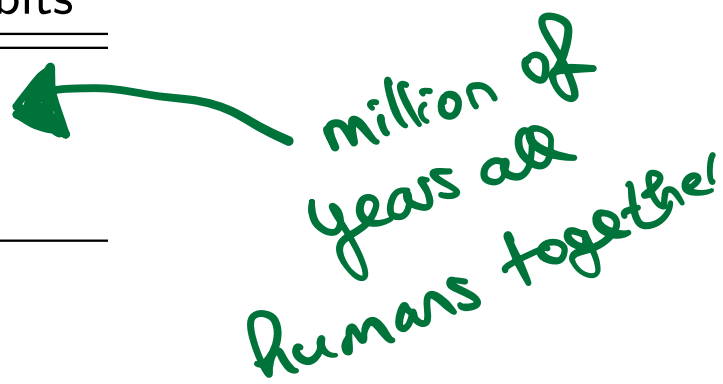
- LWE is flexible $\rightarrow$ good for constructions
- LWE is parametrized by multiple parameters $\rightarrow$ various choices possible
  - Integers m, n and q
  - Distribution of error D_e
  - Distribution of secret D_s

Example Parameters for Learning With Errors

- LWE is flexible $\rightarrow$ good for constructions
- LWE is parametrized by multiple parameters $\rightarrow$ various choices possible
  - Integers m, n and q
  - Distribution of error D_e
  - Distribution of secret D_s

For simplicity, D_e and D_s bounded uniform distribution with infinity norm bound δ.

n, m	q	δ	security bits
512	3329	3	118
768	3329	2	183
1024	3329	3	256



Part 3:

How to build encryption schemes from lattices

Reminder: Encryption

An encryption scheme $\Pi = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ consists of three algorithms:

- $\mathsf{KGen} \to \mathsf{sk}$
- $\mathsf{Enc}(\mathsf{sk}, m) \to \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = m'$

Correctness: $\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{sk}, m)) = m$ during an honest execution

Security: $\mathsf{Enc}(\mathsf{sk}, m_0)$ is indistinguishable from $\mathsf{Enc}(\mathsf{sk}, m_1)$

Encryption from LWE

Let D_s and D_e be secret and error distributions and $\mathbb{Z}_q$ be a finite field.

KGen:

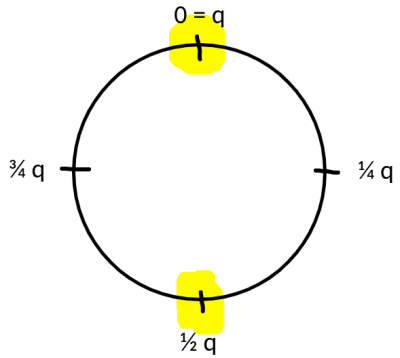
- Output $\mathbf{s} \leftarrow D_s$

Enc$(\mathbf{s}, m \in \{0,1\}^n)$:

- $\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{n \times n})$
- $\mathbf{e} \leftarrow D_e$
- $\mathbf{u} = \mathbf{A}\mathbf{s} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m \bmod q$
- Output $(\mathbf{A}, \mathbf{u})$

Dec$(\mathbf{s}, \mathbf{A}, \mathbf{u})$:

- For every coefficient of $\mathbf{u} - \mathbf{A}\mathbf{s}$:
- If closer to 0 than to $q/2$, output 0
- Else output 1



Encryption from LWE

Let D_s and D_e be secret and error distributions and $\mathbb{Z}_q$ be a finite field.

KGen:

- Output $\mathbf{s} \leftarrow D_s$

Enc$(\mathbf{s}, m \in \{0,1\}^n)$:

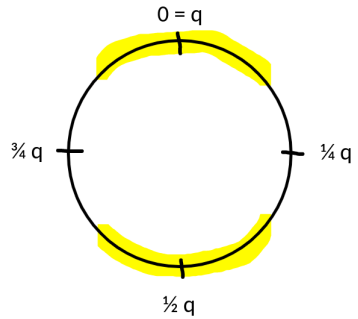
- $\mathbf{A} \leftarrow$ Unif$(\mathbb{Z}_q^{n \times n})$
- $\mathbf{e} \leftarrow D_e$
- $\mathbf{u} = \mathbf{As} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m \bmod q$
- Output $(\mathbf{A}, \mathbf{u})$

Dec$(\mathbf{s}, \mathbf{A}, \mathbf{u})$:

- For every coefficient of $\mathbf{u} - \mathbf{As}$:
- If closer to 0 than to $q/2$, output 0
- Else output 1

Correctness:

$$\begin{aligned} \mathbf{u} - \mathbf{As} &= \mathbf{As} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m - \mathbf{As} \\ &= \mathbf{e} + \lfloor q/2 \rfloor m \end{aligned}$$



Decryption succeeds if $\|\mathbf{e}\|_\infty < q/8$

Encryption from LWE 2/2

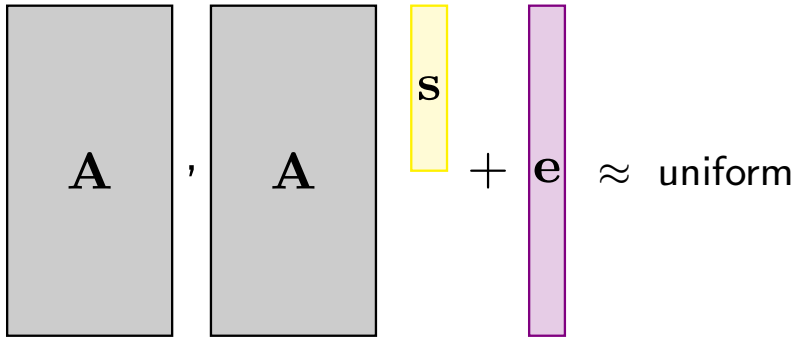
Let D_s and D_e be secret and error distributions and $\mathbb{Z}_q$ be a finite field.

KGen:

- Output $\mathbf{s} \leftarrow D_s$

Enc$(\mathbf{s}, m \in \{0,1\}^n)$:

- $\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{n \times n})$
- $\mathbf{e} \leftarrow D_e$
- $\mathbf{u} = \mathbf{A}\mathbf{s} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m \bmod q$
- Output $(\mathbf{A}, \mathbf{u})$



Security:

- Assume hardness of decision Learning with Errors (D-LWE)
- $\mathbf{A}\mathbf{s} + \mathbf{e} + \lfloor q/2 \rfloor m_0 \approx \text{uniform} + \lfloor q/2 \rfloor m_0 \approx \text{uniform} + \lfloor q/2 \rfloor m_1 \approx \mathbf{A}\mathbf{s} + \mathbf{e} + \lfloor q/2 \rfloor m_1$
- Encryption of m_0 indistinguishable from encryption of m_1

Kyber - Standardized by NIST

Kyber = the previous construction + several improvements

Main improvements:

0. Public-key variant
1. Structured LWE variant (most important)
2. LWE secret and noise from centered binomial distribution
3. Pseudorandomness for distributions
4. Ciphertext compression

≈120 bits of security

Kyber 512:

* $|ct| \approx |pk| \approx 800$ Bytes
* $\approx 4\,\mu s$

Sources:

- Website of Kyber: https://pq-crystals.org/kyber/
- Specifications [link]

DH-based:

* $|ct| \approx |pk| \approx 32$ Bytes
* $\approx 0.1\,\mu s$

Part 4:

Some (of my) current challenges

Challenges from Encryption

KGen:

- Output $\mathbf{s} \leftarrow D_s$

Enc$(\mathbf{s}, m \in \{0,1\}^n)$:

- $\mathbf{A} \leftarrow$ Unif$(\mathbb{Z}_q^{n \times n})$
- $\mathbf{e} \leftarrow D_e$
- $\mathbf{u} = \mathbf{As} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m \bmod q$
- Output $(\mathbf{A}, \mathbf{u})$

Dec$(\mathbf{s}, \mathbf{A}, \mathbf{u})$:

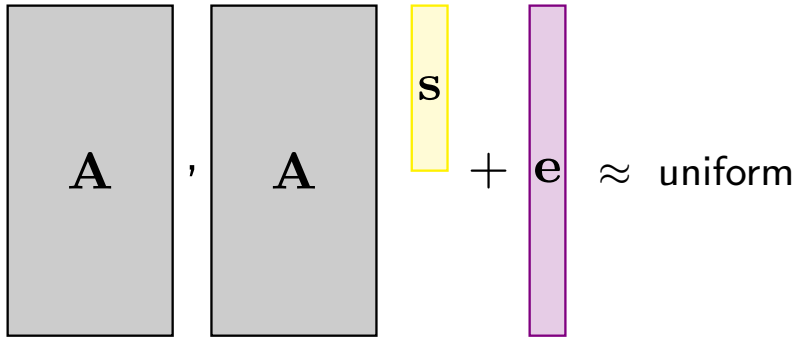
- For every coefficient of $\mathbf{u} - \mathbf{As} \bmod q$:
- If closer to 0 than to $q/2$, output 0
- Else output 1

- Difficult to distribute calculation among multiple people [BS23]*
- Linearly split $\mathbf{s} = \mathbf{s}_1 + \mathbf{s}_2 \Rightarrow \mathbf{As}_1 + \mathbf{As}_2 = \mathbf{As}$
- How to "split" the non-linear rounding step ?

*Boudgoust and Scholl, *Simple Threshold (Fully Homomorphic) Encryption From LWE With Polynomial Modulus*, Asiacrpyt'23

Challenges from LWE

- Many options for secret distribution D_s and error distribution D_e
- For different choices same hardness?
- Goal: show that only the min-entropy (and norm bound) matter
- Theoretical answer: [BJTW25]*
- What if we change structure of $\mathbf{A}$?



*

*Boudgoust, Jeudy, Tairi, Wen, *Hardness of M-LWE with General Distributions and Applications to Leaky Variants* IACR ePrint 2025/1472

Wrap-Up

Hopefully you have now a rough idea:

- *What post-quantum cryptography is:*
  Cryptography assumed to be secure against quantum computers
- *What lattice problems are:*
  Learning with Errors (LWE): Noisly random linear equations in finite fields
- *How to build cryptography from lattices:*
  Encryption from LWE
- *What new challenges come with lattices:*
  Distributing computations & LWE choices

Any questions or interested in my research?

- Write me an e-mail

Wrap-Up

Jerejef !

Hopefully you have now a rough idea:

- *What post-quantum cryptography is:*
  Cryptography assumed to be secure against quantum computers
- *What lattice problems are:*
  Learning with Errors (LWE): Noisly random linear equations in finite fields
- *How to build cryptography from lattices:*
  Encryption from LWE
- *What new challenges come with lattices:*
  Distributing computations & LWE choices

Any questions or interested in my research?

- ✉ Write me an e-mail


Katharina Boudgoust, Corentin Jeudy, Erkan Tairi, and Weiqiang Wen.
Hardness of M-LWE with general distributions and applications to leaky variants.
IACR Cryptol. ePrint Arch., page 1472, 2025.


Katharina Boudgoust and Peter Scholl.
Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus.
In *ASIACRYPT (1)*, volume 14438 of *Lecture Notes in Computer Science*, pages 371–404. Springer, 2023.


Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In *STOC*, pages 84–93. ACM, 2005.


Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM J. Comput., 26(5):1484–1509, 1997.

References Figures

- ECO group photo, personal, 21.1.26
- Signal on the phone https://www.kaspersky.fr/blog/signal-hacked-but-still-secure/19311/ 18.1.26
- Carte CBAO https://cbaobank.com/fr/nos-cartes 18.1.26
- Senegal passport https://ambasen-es.sn/passeports-senegal-en-espagne/ 18.1.26
- Quantum copmuter https://quantumai.google/discover/whatisqc 19.1.26