Lattice-Based Cryptography

A Gentle Introduction

Katharina Boudgoust

CNRS, Univ Montpellier, LIRMM, France

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

Context

The security in public-key cryptography relies 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

Context

The security in public-key cryptography relies 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
- Isogenies
- Multivariate systems
- **?**

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

Context

The security in public-key cryptography relies 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
- Isogenies
- Multivariate systems
- **?**

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

US National Institute of Standards and Technology (NIST) Project

- 2016: start of NIST's post-quantum cryptography project*
- 2022: selection of 4 schemes, 3 of them relying on lattice problems

Public Key Encryption:

- Kyber

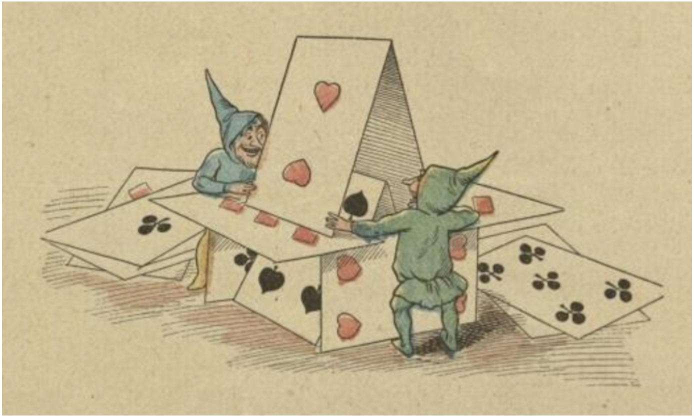
Digital Signature:

- Dilithium
- Falcon
- SPHINCS+

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

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

Really Post-Quantum?



Really Post-Quantum?

Quantum Algorithms for Lattice Problems

Yilei Chen*

April 18, 2024

ia.cr/2024/555

Really Post-Quantum?

Quantum Algorithms for Lattice Problems

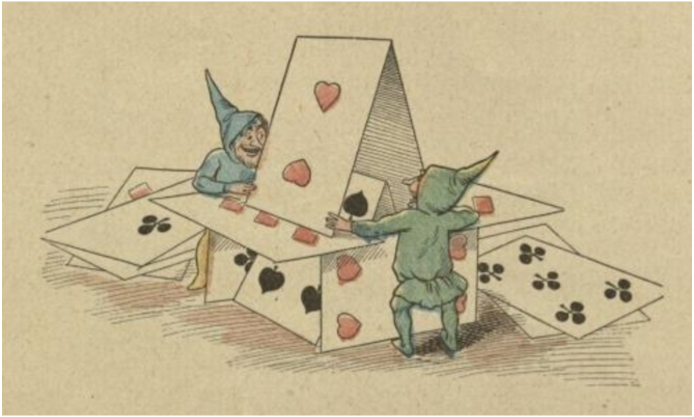
ERROR IN PROOF!

Yilei Chen

April 18, 2024

ia.cr/2024/555

Really Post-Quantum?



Overview of Today's Presentation

Questions we are trying to answer today:

- Part 1: *What are lattices?*
- Part 2: *What are lattice problems?*
- Part 3: *What is lattice-based cryptography?*
- Part 4: *What are some (of my) current challenges?*

References:

- The Lattice Club [website]
- Crash Course Spring 2022 [lecture notes]

Part 1:

What is a lattice?

Euclidean Lattices

An Euclidean lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.

Euclidean Lattices

An Euclidean lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.

- additive subgroup: $\mathbf{0} \in \Lambda$, and for all $\mathbf{x}, \mathbf{y} \in \Lambda$ it holds $\mathbf{x} + \mathbf{y}, -\mathbf{x} \in \Lambda$;
- discrete: every $\mathbf{x} \in \Lambda$ has a neighborhood in which $\mathbf{x}$ is the only lattice point.
  $\exists \varepsilon > 0$ such that $\mathcal{B}(\mathbf{x}, \varepsilon) \cap \Lambda = \{ \mathbf{x} \}$

Euclidean Lattices

An Euclidean lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$.

- additive subgroup: $\mathbf{0} \in \Lambda$, and for all $\mathbf{x}, \mathbf{y} \in \Lambda$ it holds $\mathbf{x} + \mathbf{y}, -\mathbf{x} \in \Lambda$;
- discrete: every $\mathbf{x} \in \Lambda$ has a neighborhood in which $\mathbf{x}$ is the only lattice point.
  $\exists \varepsilon > 0$ such that $\mathcal{B}(\mathbf{x}, \varepsilon) \cap \Lambda = \{ \mathbf{x} \}$

There exists a finite basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \subset \mathbb{R}^n$ such that

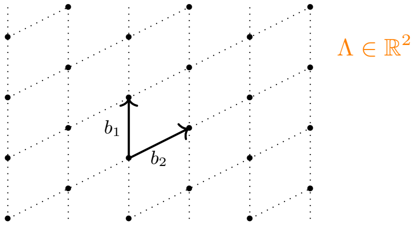
$$\Lambda(\mathbf{B}) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$

- n is the dimension of Λ

Euclidean Lattices

Let $\mathbf{B} \in \mathbb{R}^{n \times n}$ be a basis for Λ, i.e.,

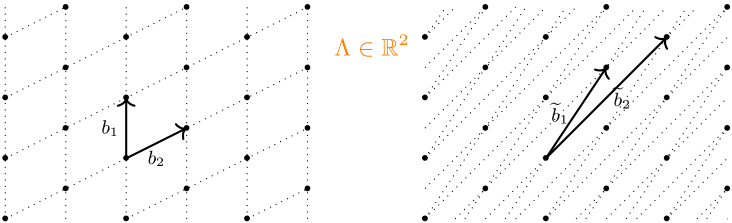
$$\Lambda(\mathbf{B}) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i \colon z_i \in \mathbb{Z} \right\} = \{\mathbf{B}\mathbf{z} \colon \mathbf{z} \in \mathbb{Z}^n\}.$$



Euclidean Lattices

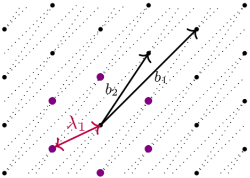
Let $\mathbf{B} \in \mathbb{R}^{n \times n}$ be a basis for Λ, i.e.,

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



- $\mathbf{U} \in \mathbb{Z}^{n \times n}$ unimodular, then $\widetilde{\mathbf{B}} = \mathbf{B} \cdot \mathbf{U}$ also a basis of Λ $\quad \det(\mathbf{U}) = \pm 1$
- $\det(\Lambda) := |\det(\mathbf{B})|$

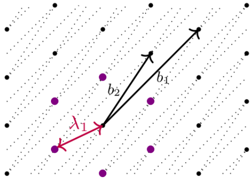
Lattice Minimum & Special Lattices



The **minimum** of a lattice $\Lambda \subset \mathbb{R}^n$ is defined as

$$\lambda_1(\Lambda) = \min_{\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{x}\|_2.$$

Lattice Minimum & Special Lattices



The **minimum** of a lattice $\Lambda \subset \mathbb{R}^n$ is defined as

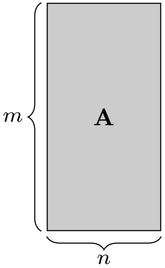
$$\lambda_1(\Lambda) = \min_{\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{x}\|_2.$$

Let $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ for some $n, m, q \in \mathbb{N}$ with $n \leq m$

$\mathbb{Z}_q$ integers modulo q

$$\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}\mathbf{s} \bmod q \text{ for some } \mathbf{s} \in \mathbb{Z}^n\}$$

q-ary lattice

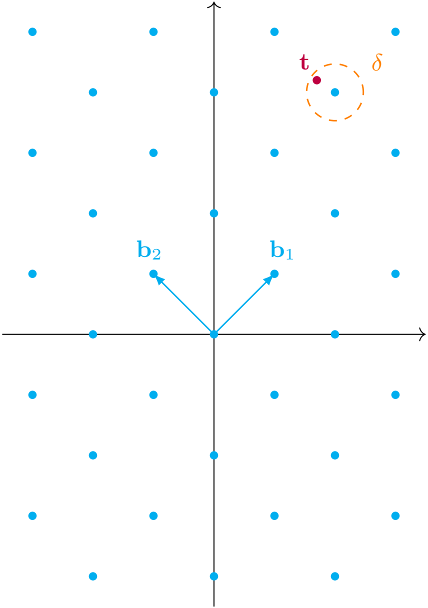


Part 2:

What are lattice problems?

Bounded Distance Decoding

Given a lattice $\Lambda \in \mathbb{R}^n$ of dimension n and a target $\mathbf{t} \in \mathbb{R}^n$ such $\mathrm{dist}(\Lambda, \mathbf{t}) \leq \delta < \lambda_1(\Lambda)/2$.

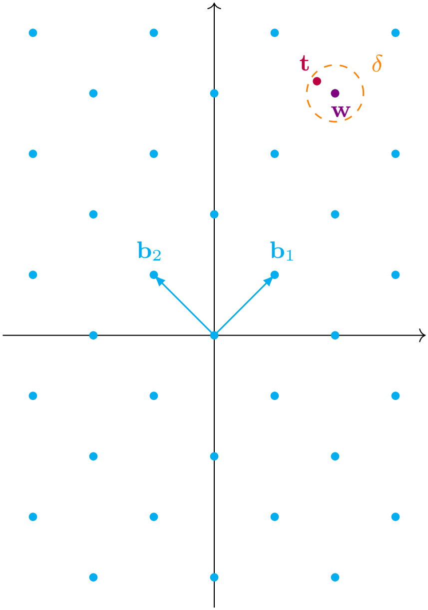


Bounded Distance Decoding

Given a lattice $\Lambda \in \mathbb{R}^n$ of dimension n and a target $\mathbf{t} \in \mathbb{R}^n$ such $\text{dist}(\Lambda, \mathbf{t}) \leq \delta < \lambda_1(\Lambda)/2$.

The **bounded distance decoding** (BDD_δ) 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 $\Lambda \in \mathbb{R}^n$ of dimension n and a target $\mathbf{t} \in \mathbb{R}^n$ such $\text{dist}(\Lambda, \mathbf{t}) \le \delta < \lambda_1(\Lambda)/2$.

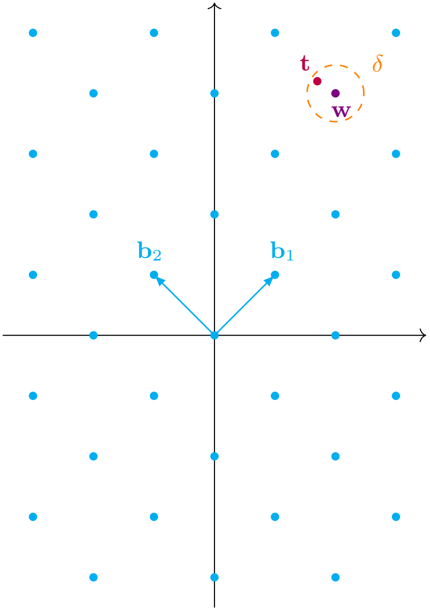
The **bounded distance decoding** (BDD_δ) problem asks to find the unique vector $\mathbf{w} \in \Lambda$ such that

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

The complexity of BDD_δ increases with n and with δ.

Conjecture:

There is no polynomial-time classical or quantum algorithm that solves BDD_δ on any lattice to within inverse polynomial factors.

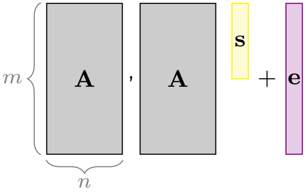


Learning With Errors [Reg05]*

Given a matrix $\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{m \times n})$.

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

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



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

Learning With Errors [Reg05]*

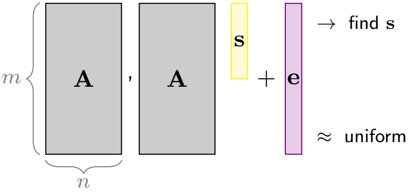
Given a matrix $\mathbf{A} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^{m \times n})$.

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

- secret $\mathbf{s} \in \mathbb{Z}_q^n$ 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$_\delta$) asks to find $\mathbf{s}$.

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



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

Learning With Errors [Reg05]*

Given a matrix $\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{m \times n})$.

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

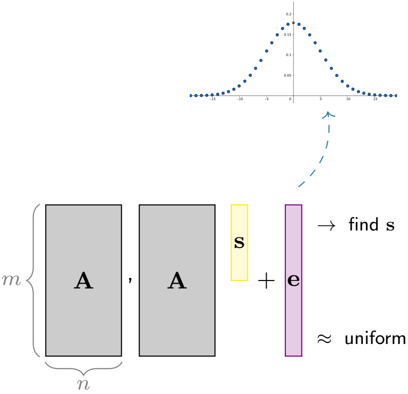
- secret $\mathbf{s} \in \mathbb{Z}_q^n$ sampled from distribution D_s and
- noise/error $\mathbf{e} \in \mathbb{Z}^m$ sampled from distribution D_e such that $\|\mathbf{e}\|_2 \leq \delta \ll q$.

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

Decision learning with errors (D-LWE$_\delta$) 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!



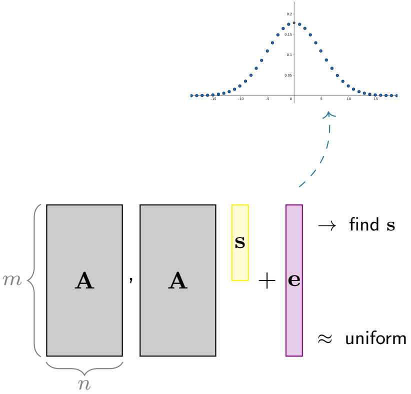
* Regev, *On lattices, learning with errors, random linear codes, and cryptography*, STOC'05

Learning With Errors [Reg05]*

Given a matrix $\mathbf{A} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^{m\times n})$.

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

- secret $\mathbf{s} \in \mathbb{Z}_q^n$ 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$_\delta$) asks to find $\mathbf{s}$.

Decision learning with errors (D-LWE$_\delta$) 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!

S-LWE$_\delta$ equals BDD$_\delta$ in the lattice $\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}\mathbf{s} \bmod q,\ \mathbf{s} \in \mathbb{Z}^n\}$.

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

Part 3:

What is lattice-based cryptography?

Public-Key Encryption (PKE)

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

- $\mathsf{KGen}(1^\lambda) \to (\mathsf{sk}, \mathsf{pk})$ λ security parameter
- $\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = m'$

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

Semantic Security: $\mathsf{Enc}(\mathsf{pk}, m_0)$ is indistinguishable from $\mathsf{Enc}(\mathsf{pk}, m_1)$
(IND-CPA)

Public-Key Encryption from LWE [Reg05]

Let χ be distribution on $\mathbb{Z}$.

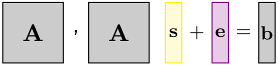
- $\mathsf{KGen}(1^\lambda)$:
  - $\mathbf{A} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^{n \times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output $\mathsf{sk} = \mathbf{s}$ and $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$

$$\boxed{\mathbf{A}}\ ,\ \boxed{\mathbf{A}}\ \boxed{\mathbf{s}} + \boxed{\mathbf{e}} = \boxed{\mathbf{b}}$$

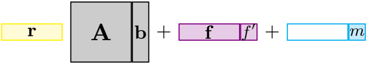
Public-Key Encryption from LWE [Reg05]

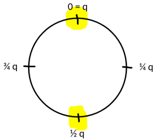
Let χ be distribution on $\mathbb{Z}$.

- KGen(1^λ):
  - $\mathbf{A} \leftarrow$ Unif$(\mathbb{Z}_q^{n \times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output sk $= \mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$



- Enc(pk, $m \in \{0,1\}$):
  - $\mathbf{r}, \mathbf{f} \leftarrow \chi^n$ and $f' \leftarrow \chi$
  - $\mathbf{u} = \mathbf{r}\mathbf{A} + \mathbf{f}$
  - $v = \mathbf{r}\mathbf{b} + f' + \lfloor q/2 \rfloor \cdot m$
  - Output ct $= (\mathbf{u}, v)$

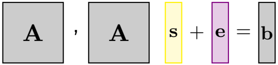




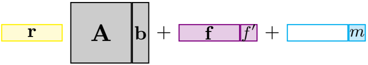
Public-Key Encryption from LWE [Reg05]

Let χ be distribution on $\mathbb{Z}$.

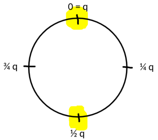
- KGen(1^λ):
  - $\mathbf{A} \leftarrow$ Unif$(\mathbb{Z}_q^{n\times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output sk $= \mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$



- Enc(pk, $m \in \{0,1\}$):
  - $\mathbf{r}, \mathbf{f} \leftarrow \chi^n$ and $f' \leftarrow \chi$
  - $\mathbf{u} = \mathbf{r}\mathbf{A} + \mathbf{f}$
  - $v = \mathbf{r}\mathbf{b} + f' + \lfloor q/2 \rfloor \cdot m$
  - Output ct $= (\mathbf{u}, v)$

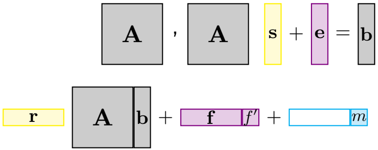


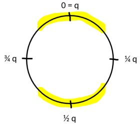
- Dec(sk, ct):
  - If $v - \mathbf{u}\mathbf{s}$ is closer to 0 than to $q/2$, output $m' = 0$
  - Else output $m' = 1$



Public-Key Encryption from LWE [Reg05]

- KGen(1^λ):
  - $\mathbf{A} \leftarrow$ Unif$(\mathbb{Z}_q^{n\times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output sk $= \mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$
- Enc(pk, $m \in \{0,1\}$):
  - $\mathbf{r}, \mathbf{f} \leftarrow \chi^n$ and $f' \leftarrow \chi$
  - $\mathbf{u} = \mathbf{r}\mathbf{A} + \mathbf{f}$
  - $v = \mathbf{r}\mathbf{b} + f' + \lfloor q/2 \rfloor \cdot m$
  - Output ct $= (\mathbf{u}, v)$
- Dec(sk, ct):
  - If $v - \mathbf{u}\mathbf{s}$ is closer to 0 than to $q/2$, output $m' = 0$
  - Else output $m' = 1$





Correctness:

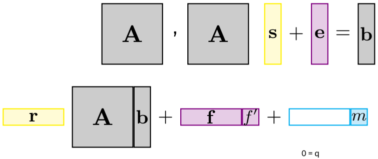
$$v - \mathbf{u}\mathbf{s} = \mathbf{r}(\mathbf{A}\mathbf{s} + \mathbf{e}) + f' + \lfloor q/2 \rfloor \cdot m - (\mathbf{r}\mathbf{A} + \mathbf{f})\mathbf{s}$$

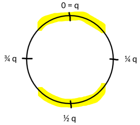
$$= \underbrace{\mathbf{r}\mathbf{e} + f' - \mathbf{f}\mathbf{s}}_{*\ \text{ciphertext noise}} + \lfloor q/2 \rfloor m$$

Decryption succeeds if $|*| < q/8$

Public-Key Encryption from LWE [Reg05]

- KGen(1^λ):
  - $\mathbf{A} \leftarrow$ Unif$(\mathbb{Z}_q^{n\times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output sk $= \mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$
- Enc(pk, $m \in \{0,1\}$):
  - $\mathbf{r}, \mathbf{f} \leftarrow \chi^n$ and $f' \leftarrow \chi$
  - $\mathbf{u} = \mathbf{r}\mathbf{A} + \mathbf{f}$
  - $v = \mathbf{r}\mathbf{b} + f' + \lfloor q/2 \rfloor \cdot m$
  - Output ct $= (\mathbf{u}, v)$
- Dec(sk, ct):
  - If $v - \mathbf{u}\mathbf{s}$ is closer to 0 than to $q/2$, output $m' = 0$
  - Else output $m' = 1$





Correctness: Let χ be B-bounded with $2nB^2 + B < q/8$

$$v - \mathbf{u}\mathbf{s} = \mathbf{r}(\mathbf{A}\mathbf{s} + \mathbf{e}) + f' + \lfloor q/2 \rfloor \cdot m - (\mathbf{r}\mathbf{A} + \mathbf{f})\mathbf{s}$$

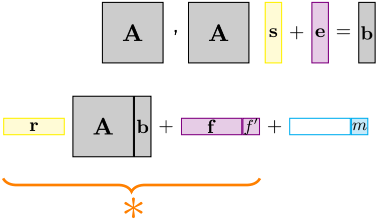
$$= \underbrace{\mathbf{r}\mathbf{e} + f' - \mathbf{f}\mathbf{s}}_{*\ \text{ciphertext noise}} + \lfloor q/2 \rfloor m$$

Decryption succeeds if $|*| < q/8$

$$|*| = |\mathbf{r}\mathbf{e} + f' - \mathbf{f}\mathbf{s}| \le \|\mathbf{r}\|_2 \cdot \|\mathbf{e}\|_2 + \|\mathbf{f}\|_2 \cdot \|\mathbf{s}\|_2 + |f'| \le 2(\sqrt{n}B \cdot \sqrt{n}B) + B < q/8$$

Public-Key Encryption from LWE [Reg05]

- $\mathsf{KGen}(1^\lambda)$:
  - $\mathbf{A} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^{n\times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output $\mathsf{sk} = \mathbf{s}$ and $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$
- $\mathsf{Enc}(\mathsf{pk}, m \in \{0,1\})$:
  - $\mathbf{r}, \mathbf{f} \leftarrow \chi^n$ and $f' \leftarrow \chi$
  - $\mathbf{u} = \mathbf{r}\mathbf{A} + \mathbf{f}$
  - $v = \mathbf{r}\mathbf{b} + f' + \lfloor q/2 \rceil \cdot m$
  - Output $\mathsf{ct} = (\mathbf{u}, v)$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$:
  - If $v - \mathbf{u}\mathbf{s}$ is closer to 0 than to $q/2$, output $m' = 0$
  - Else output $m' = 1$



Semantic Security: Assume hardness of decision LWE

1. replace $\mathbf{b}$ by uniform random vector
2. replace non-message part ($*$) by uniform random vector
3. then the message is completely hidden

Kyber - Selected for Standardization by NIST

Kyber = the previous construction + several improvements

Main improvements:

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

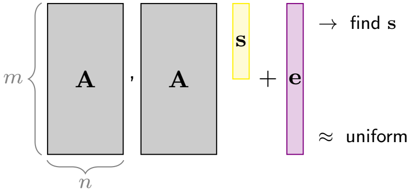
Sources:

- Website of Kyber: https://pq-crystals.org/kyber/
- Latest specifications [link]
- Tutorial by V. Lyubashevsky [link]

Example Parameters for Learning With Errors

Kyber Parameters:

- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow D_s$, $\mathbf{e} \leftarrow D_e$
- $m = ?$
- $n = ?$
- $q = ?$
- $D_e = ?$
- $D_s = ?$

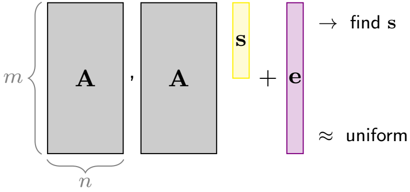


[*] https://github.com/malb/lattice-estimator

Example Parameters for Learning With Errors

Kyber Parameters:

- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow D_s$, $\mathbf{e} \leftarrow D_e$
- $m = n$
- $n = ?$
- $q = ?$
- $D_e = ?$
- $D_s = D_e$ for simplicity



n	q	$\|\mathbf{e}\|_\infty$	security bits
512	3329	3	118
768	3329	2	183
1024	3329	2	256

* https://github.com/malb/lattice-estimator

Part 4:

What are (my) current challenges?

Reminder: Public-Key Encryption (PKE)

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

- $\mathsf{KGen}(1^\lambda) \to (\mathsf{sk}, \mathsf{pk})$ — λ security parameter
- $\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = m'$

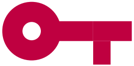
Reminder: Public-Key Encryption (PKE)

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

- $\mathsf{KGen}(1^\lambda) \to (\mathsf{sk}, \mathsf{pk})$ — λ security parameter
- $\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = m'$

The secret key sk can be seen as a **single point of failure**.

- Someone else learns it: security issue
- I loose it: operability issue



Home › Cryptocurrency › Youtuber Loses $60,000 In Crypto and NFTs After Exposing His Private Key...

Cryptocurrency News

Youtuber Loses $60,000 In Crypto and NFTs After Exposing His Private Key While Live Streaming

By **Newton Gitonga** - September 2, 2023

DARRYN POLLOCK NOV 30, 2017

Infamous Discarded Hard Drive Holding 7,500 Bitcoins Would be Worth $80 Million Today

Cryptonews • Altcoin News • LHV Bank Founder Has Lost Private Key to ETH Stash Worth $470 Million

LHV Bank Founder Has Lost Private Key to ETH Stash Worth $470 Million

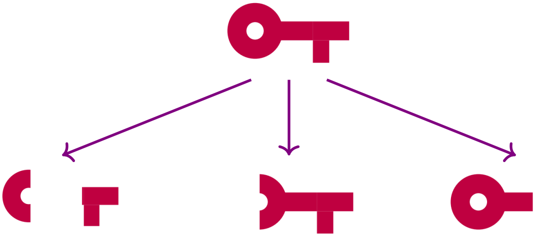
Ruholamin Haqshanas

Last updated: **November 7, 2023 02:36 EST** | 2 min read

Motivation Threshold Cryptography [DF89]*

The secret key can be seen as a **single point of failure**.

Idea: divide the secret key into multiple shares



- Better security: multiple secret key shares needed
- Better operability: not necessarily all secret key shares needed

* Desmedt and Frankel, *Threshold Cryptosystems*, CRYPTO'89

Threshold Public-Key Encryption

PKE scheme:

- $\mathsf{KGen} \to (\mathsf{pk}, \mathsf{sk})$
- $\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$ $\quad m \in \{0,1\}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to m$

Threshold Public-Key Encryption

***t*-out-of-*n* Threshold** PKE scheme:

- KGen $\rightarrow (\mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_n)$
- $\mathsf{Enc}(\mathsf{pk}, m) \rightarrow \mathsf{ct}$ $\qquad m \in \{0, 1\}$
- $\mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct}) \rightarrow d_i$
- $\mathsf{Combine}(\{ d_i \}_{i \in S}) \rightarrow m$ $\qquad S \subseteq \{ 1, \ldots, n \}$

Threshold Public-Key Encryption

t**-out-of-**n **Threshold** PKE scheme:

- $\mathsf{KGen} \to (\mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_n)$
- $\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$ $\qquad m \in \{0, 1\}$
- $\mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct}) \to d_i$
- $\mathsf{Combine}(\{\, d_i \,\}_{i \in S}) \to m$ $\qquad S \subseteq \{\, 1, \ldots, n \,\}$

Properties:

- Correctness $\qquad$ t parties can recover the message
- Security $\qquad$ less than t parties learn nothing about message

Applications:

- Encrypting highly sensitive data
- Electronic voting protocols

Research Question

Can we construct

Threshold Public-Key Encryption

based on **Euclidean Lattices**?

---

*Bendlin and Damgaard, *Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems*, TCC'10

*Boudgoust and Scholl, *Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus*, Asiacrypt'23

*Micciancio and Suhl, *Simulation-Secure Threshold PKE from LWE with Polynomial Modulus*, e-print'23

Can we construct

Threshold Public-Key Encryption

based on **Euclidean Lattices**?

Yes, but . . .

Either:	**Or:**	**Or:**
Inefficient	Efficient	Efficient
Strong Security	Weaker Security	Strong Security
Any distributions	Any distributions	Only Gaussians
[BD10]*	[BS23]*	[MS23]*

* Bendlin and Damgaard, *Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems*, TCC'10

* Boudgoust and Scholl, *Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus*, Asiacrypt'23

* Micciancio and Suhl, *Simulation-Secure Threshold PKE from LWE with Polynomial Modulus*, e-print'23

Research Question

Can we construct

Threshold Public-Key Encryption

based on **Euclidean Lattices**?

Yes, but ...

Either:	**Or:**	**Or:**	**OPEN:**
Inefficient	Efficient	Efficient	Efficient
Strong Security	Weaker Security	Strong Security	Strong Security
Any distributions	Any distributions	Only Gaussians	Any distributions
[BD10]*	[BS23]*	[MS23]*	

---

*Bendlin and Damgaard, *Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems*, TCC'10

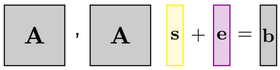
*Boudgoust and Scholl, *Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus*, Asiacrypt'23

*Micciancio and Suhl, *Simulation-Secure Threshold PKE from LWE with Polynomial Modulus*, e-print'23

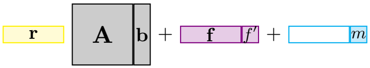
Reminder: Public-Key Encryption from LWE [Reg05]

Let χ be distribution on $\mathbb{Z}$.

- $\mathsf{KGen}(1^\lambda)$:
  - $\mathbf{A} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^{n\times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output $\mathsf{sk} = \mathbf{s}$ and $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$



- $\mathsf{Enc}(\mathsf{pk}, m \in \{0,1\})$:
  - $\mathbf{r}, \mathbf{f} \leftarrow \chi^n$ and $f' \leftarrow \chi$
  - $\mathbf{u} = \mathbf{r}\mathbf{A} + \mathbf{f}$
  - $v = \mathbf{r}\mathbf{b} + f' + \lfloor q/2 \rfloor \cdot m$
  - Output $\mathsf{ct} = (\mathbf{u}, v)$



- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$:
  - If $v - \mathbf{u}\mathbf{s}$ is closer to 0 than to $q/2$, output $m' = 0$
  - Else output $m' = 1$

Correctness:

$$v - \mathbf{u}\mathbf{s} = \mathbf{r}(\mathbf{A}\mathbf{s} + \mathbf{e}) + f' + \lfloor q/2 \rfloor \cdot m - (\mathbf{r}\mathbf{A} + \mathbf{f})\mathbf{s}$$

$$= \underbrace{\mathbf{r}\mathbf{e} + f' - \mathbf{f}\mathbf{s}}_{*\text{ ciphertext noise}} + \lfloor q/2 \rfloor m$$

Decryption succeeds if $|*| < q/8$

US National Institute of Standards and Technology (NIST) Project ⌛

- 2023: initial public draft for Multi-Party Threshold Cryptography*
- 2025: expected submission?

👉 Threshold cryptography attracts a lot of research interest at the moment.

* https://csrc.nist.gov/Projects/threshold-cryptography

Bonus:

A little Quiz :-)

When poll is active respond at PollEv.com/katharinaboudgoust042

Little Quiz after the gentle introduction to lattice-based cryptography (ICO)

Win up to 1,000 points per answer

Wrap-Up

Hopefully you have now a rough idea:

- Part 1: *What lattices are!*
- Part 2: *What lattice problems are!*
- Part 3: *What lattice-based cryptography is!*
- Part 4: *What (my) particular challenges are!*

Any questions or interested in my research?

- Reach out to me today
- Write me an e-mail

Wrap-Up

Hopefully you have now a rough idea:

- Part 1: *What lattices are!*
- Part 2: *What lattice problems are!*
- Part 3: *What lattice-based cryptography is!*
- Part 4: *What (my) particular challenges are!*

Merci !

Any questions or interested in my research?

- Reach out to me today
- Write me an e-mail

Rikke Bendlin and Ivan Damgård.
Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems.
In *TCC*, volume 5978 of *Lecture Notes in Computer Science*, pages 201–218. Springer, 2010.

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.

Yvo Desmedt and Yair Frankel.
Threshold cryptosystems.
In *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 307–315. Springer, 1989.

Daniele Micciancio and Adam Suhl.
Simulation-secure threshold PKE from LWE with polynomial modulus.
IACR Cryptol. ePrint Arch., page 1728, 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.