Lattice-Based Cryptography

A Gentle Introduction - Part 2

Katharina Boudgoust

CNRS, Univ Montpellier, LIRMM, France

Overview

Questions we tried to answer last time:

- *What are lattices?*
  'Infinite, regular grids in high dimensions'
- *What are lattice problems?*
  SIS problem: searching for short vectors in specific & random lattices
- *What is lattice-based cryptography?*
  Collision-resistant hashing & signatures from SIS
- *What are some (of my) current challenges?*
  Aggregating lattice signatures

Today:

- Part 1: Reminder
- Part 2: More lattice problems
- Part 3: How to build encryption schemes
- Part 4: What else you need to know

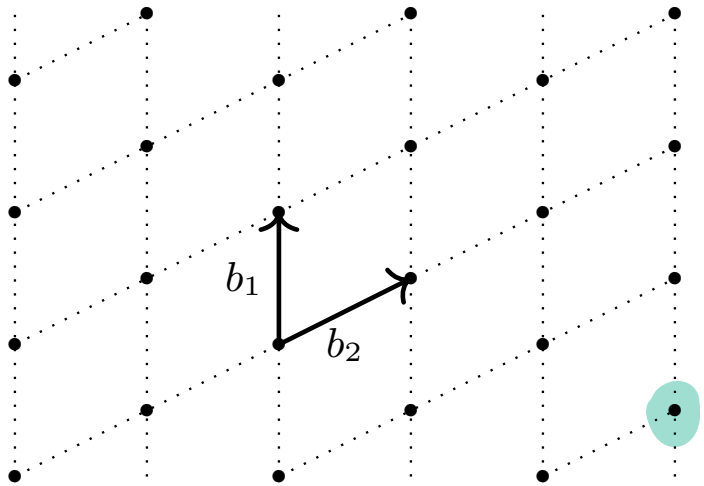
Part 1:

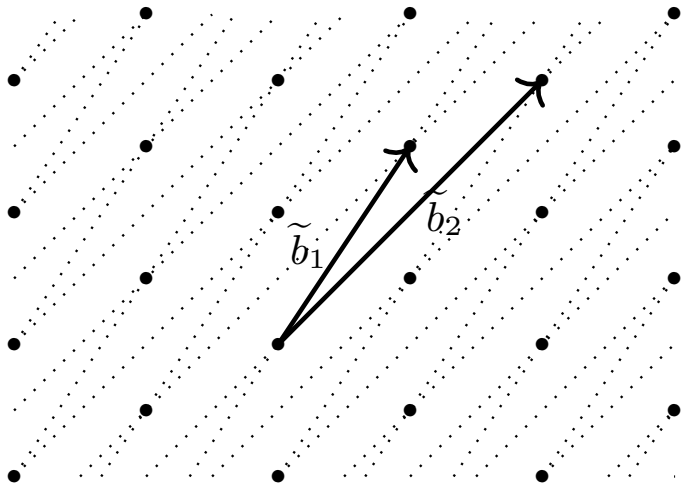
Reminder

Euclidean Lattices

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

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





$3 \cdot b_2 - 2 \cdot b_1$

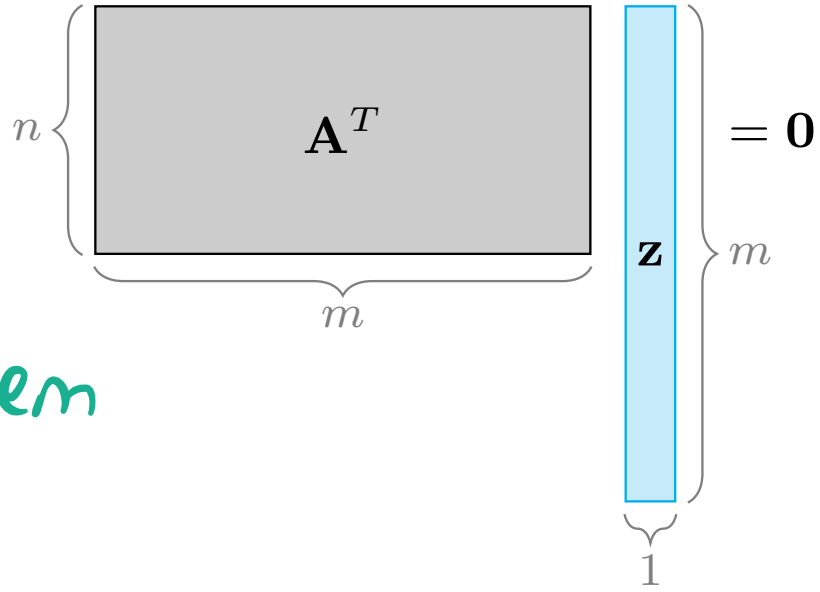
Short Integer Solution [Ajt96]*

Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random and bound $\beta > 0$.

The **short integer solution** (SIS) problem asks to find a vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $0 < \|\mathbf{z}\|_2 \leq \beta$ such that

$$\mathbf{A}^T \mathbf{z} = \mathbf{0} \bmod q.$$

makes it a hard problem



Recall:

$$\Lambda_q^{\perp}(\mathbf{A}) = \left\{ \mathbf{y} \in \mathbb{Z}^m : \mathbf{A}^T \mathbf{y} = \mathbf{0} \bmod q \right\}$$

👉 Solving SIS equals finding a short vector in the specific & random lattice $\Lambda_q^{\perp}(\mathbf{A})$

*Ajtai, *Generating hard instances of lattice problems*, STOC'96

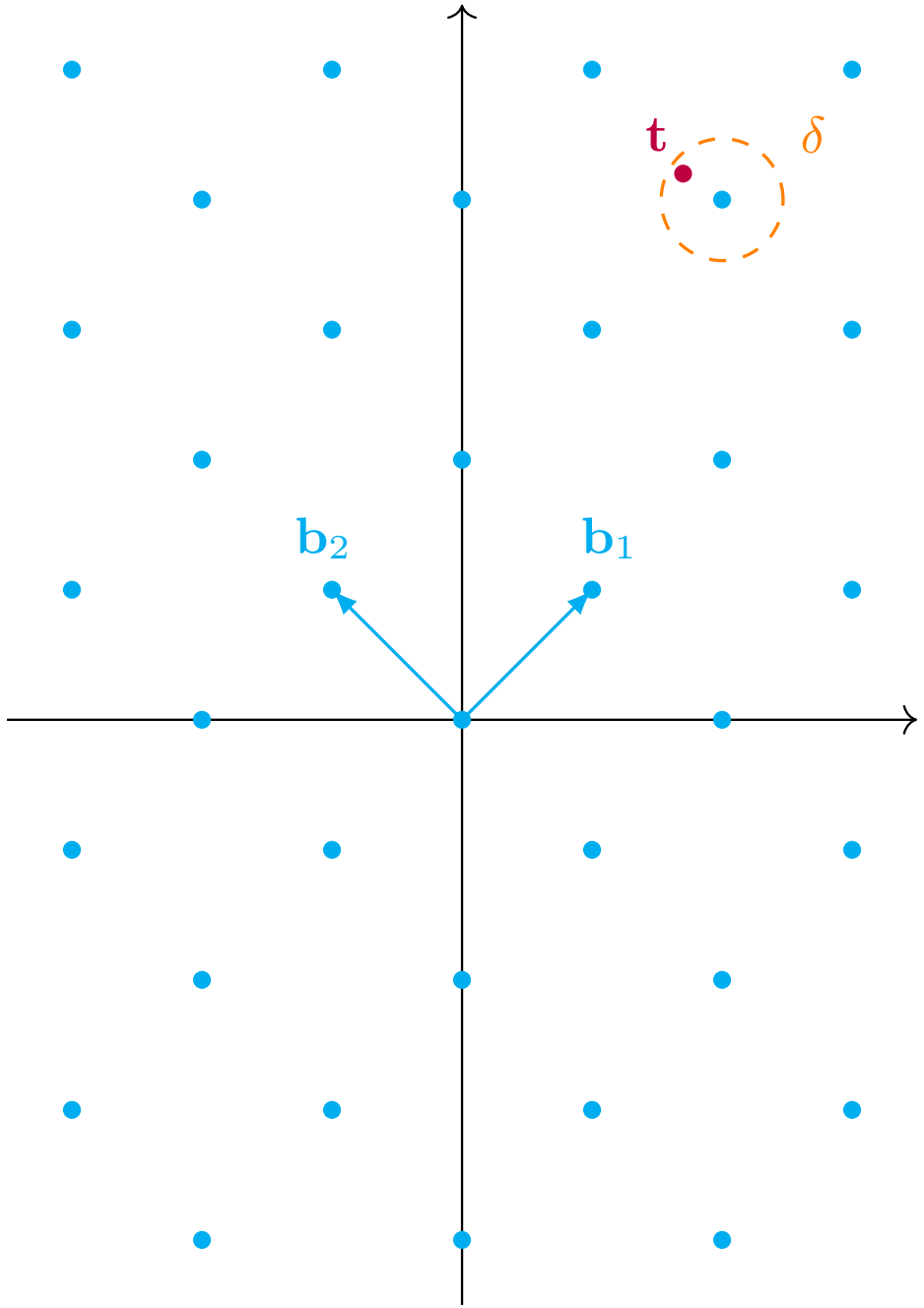
Part 2:

More lattice problems

Bounded Distance Decoding

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

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



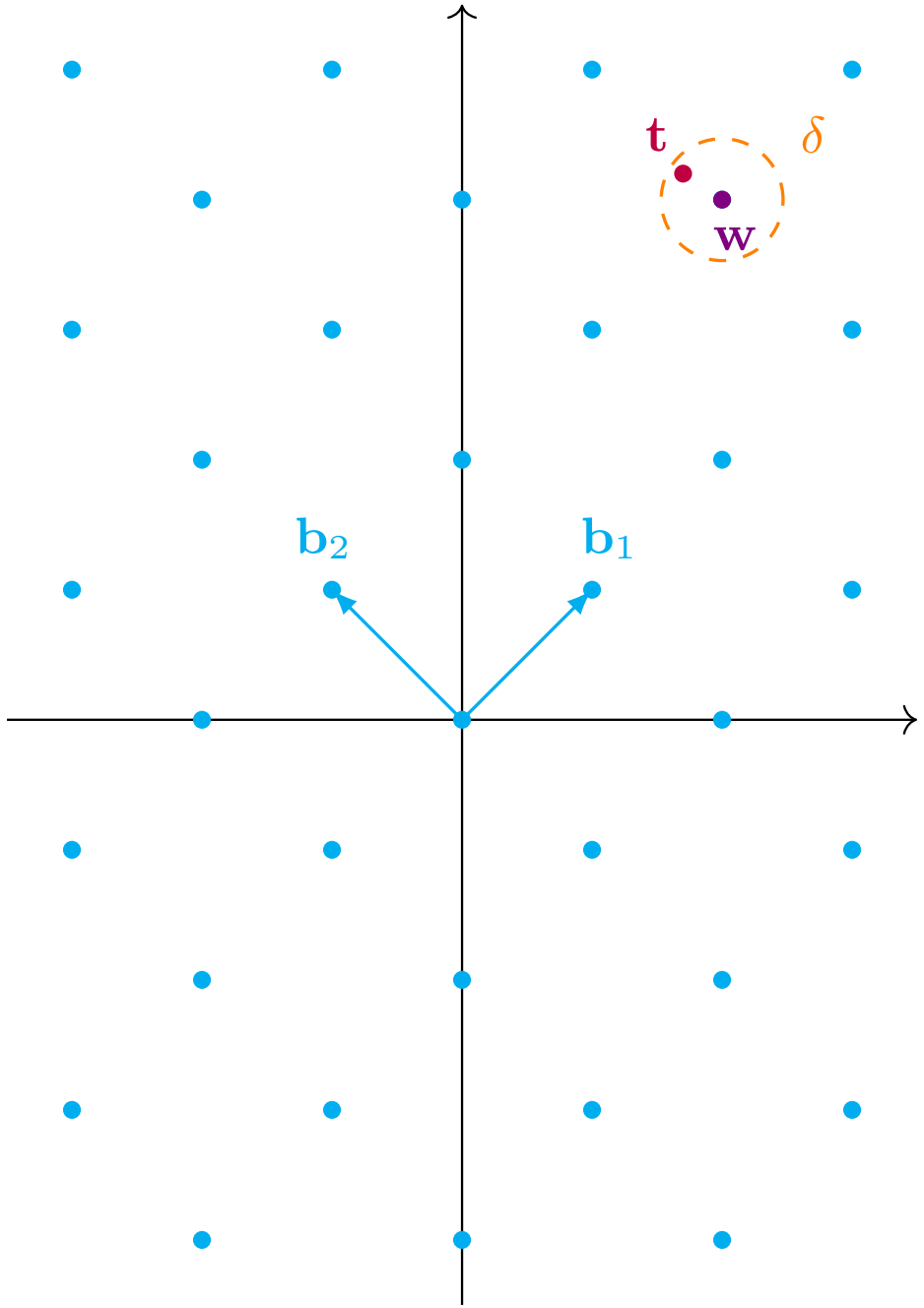
Bounded Distance Decoding

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

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

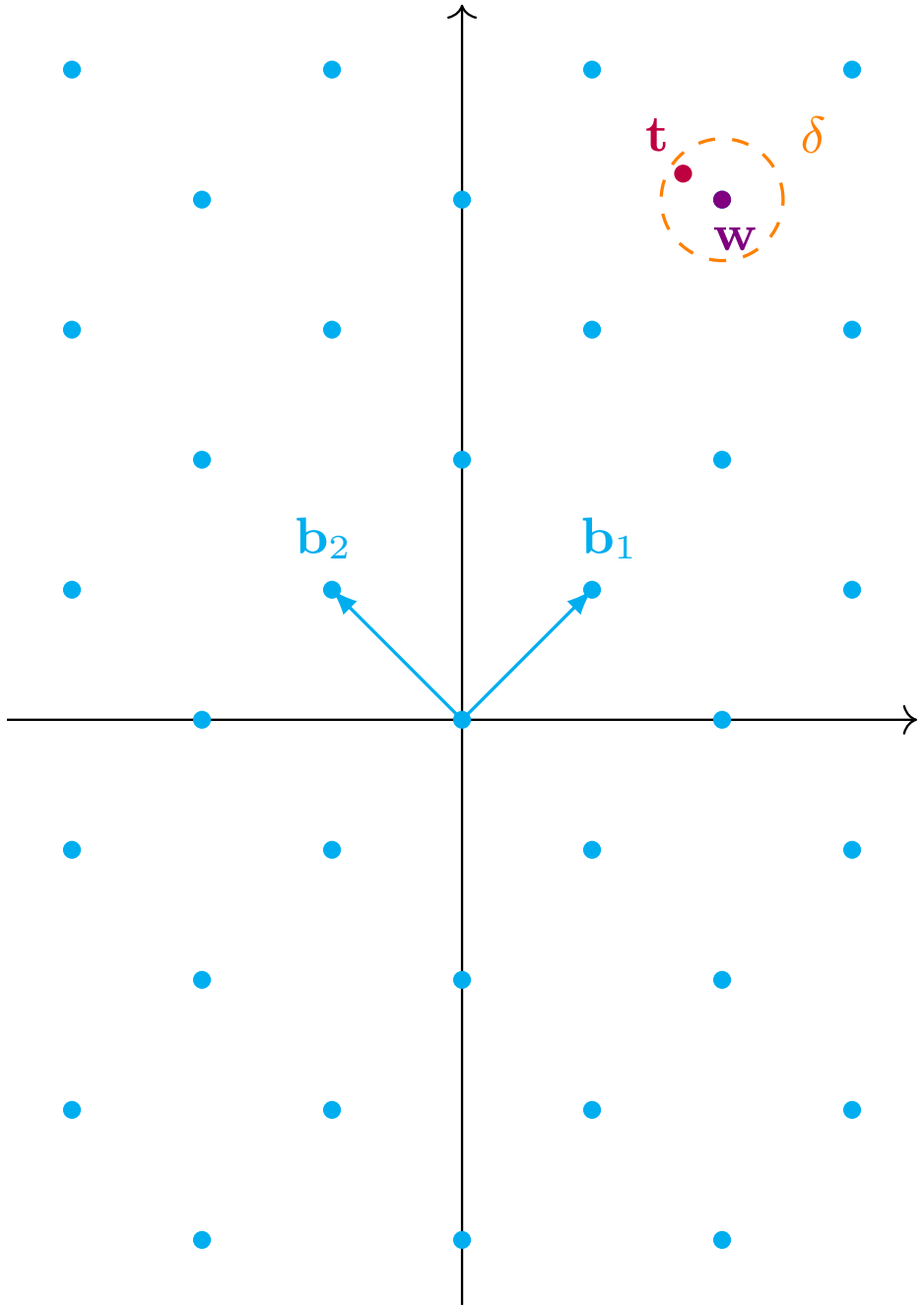
The **bounded distance decoding** (BDD) problem asks to find the unique vector $\mathbf{w} \in \Lambda$ such that

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

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.

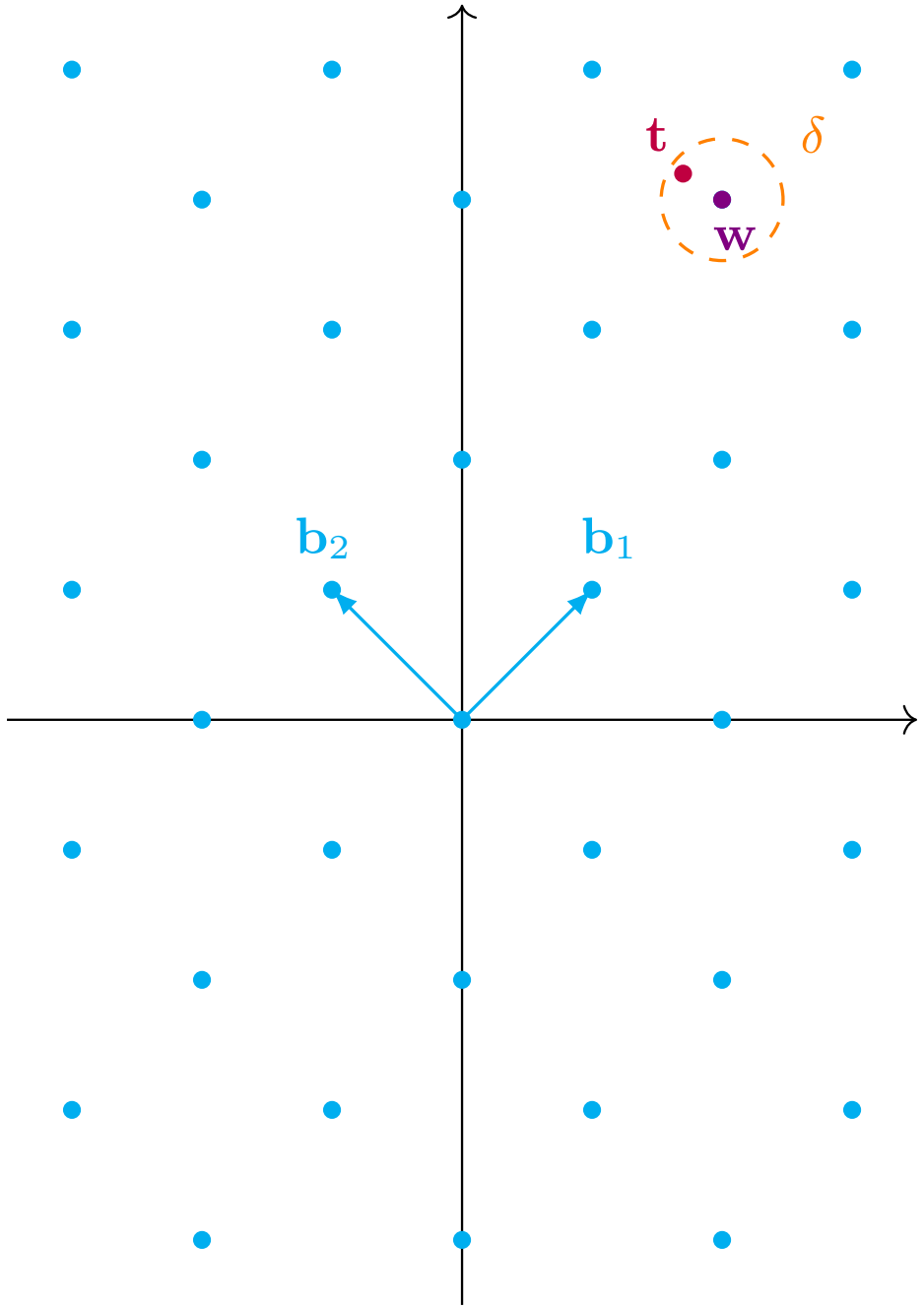


Bounded Distance Decoding

But BDD might be easy for some lattices!

For instance $\mathbb{Z}^n$ → rounding to nearest integer

Again: restrict to specif + random lattices

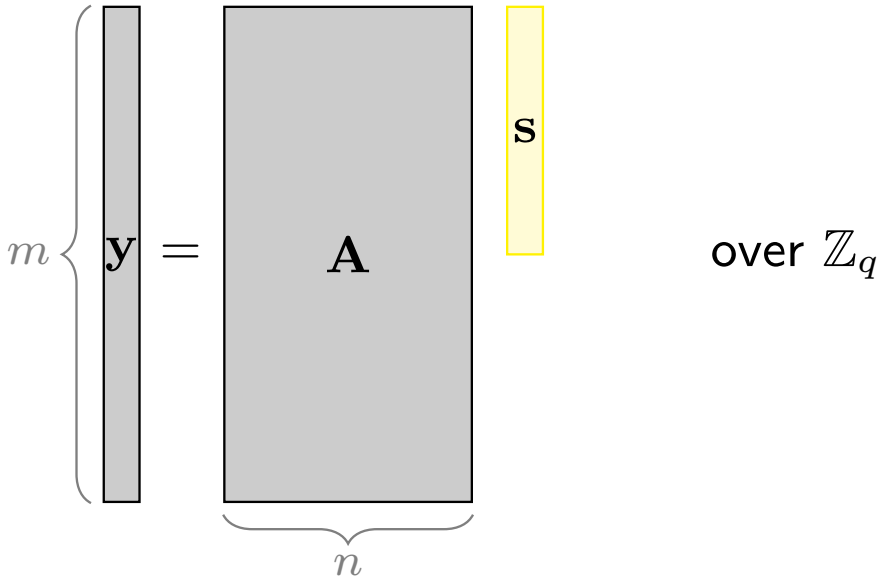


Conjecture:

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

More specific classes of lattices

- Last time: $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{A}^T\mathbf{y} = \mathbf{0} \bmod q\}$
- This time: $\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}\mathbf{s} \bmod q \text{ for some } \mathbf{s} \in \mathbb{Z}^n\}$



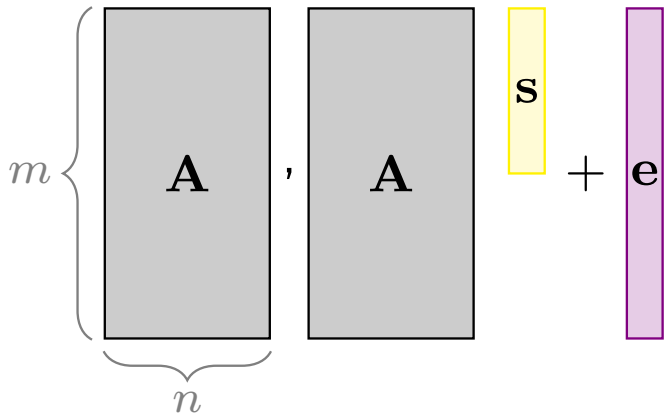
over $\mathbb{Z}_q$

Learning With Errors [Reg05]*

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 $\mathbf{s} \in \mathbb{Z}_q^n$ 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]*

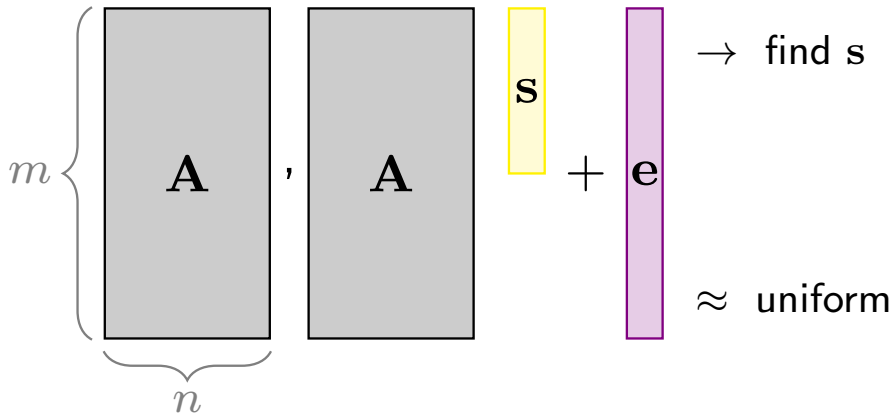
Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ sampled uniformly at random.

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

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

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



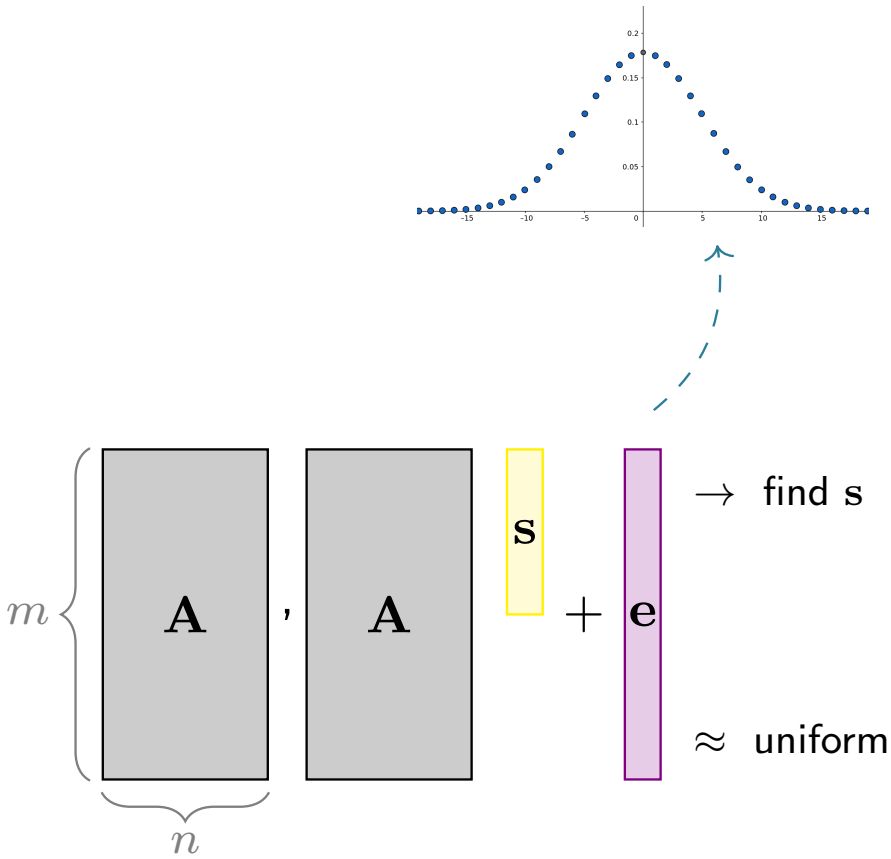
*Regev, *On lattices, learning with errors, random linear codes, and cryptography*, STOC'05

Learning With Errors [Reg05]*

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 $\mathbf{s} \in \mathbb{Z}_q^n$ 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) 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!

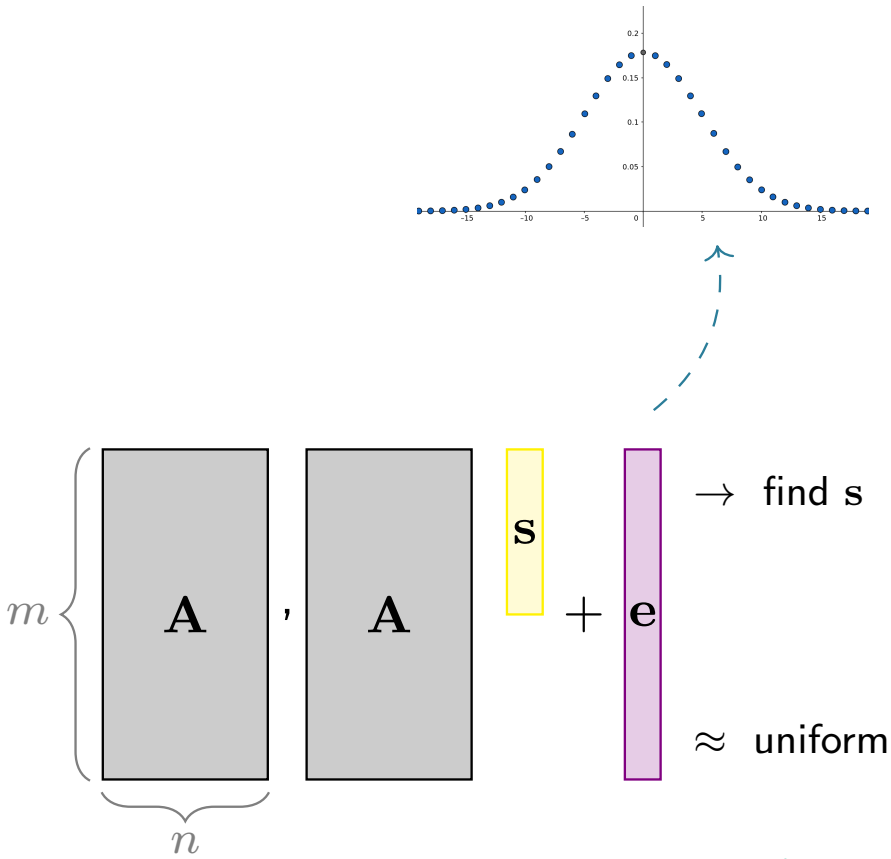
*Regev, *On lattices, learning with errors, random linear codes, and cryptography*, STOC'05

Learning With Errors [Reg05]*

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 $\mathbf{s} \in \mathbb{Z}_q^n$ 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) 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!

"hard instances"

👉 S-LWE equals BDD in the specific & random lattice $\Lambda_q(\mathbf{A})$.

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

Connection between LWE and SIS

👉 If there is an efficient solver for SIS, then there is an efficient solver for D-LWE.

Connection between LWE and SIS

If there is an efficient solver for SIS, then there is an efficient solver for D-LWE.

Proof.

Given $(\mathbf{A}, \mathbf{b})$, our goal is to decide whether
1) $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ for short error $\mathbf{e}$ or 2) $\mathbf{b} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^m)$.

Connection between LWE and SIS

If there is an efficient solver for SIS, then there is an efficient solver for D-LWE.

Proof.

Given $(\mathbf{A}, \mathbf{b})$, our goal is to decide whether
1) $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ for short error $\mathbf{e}$ or 2) $\mathbf{b} \leftarrow \text{Unif}(\mathbb{Z}_q^m)$.

Forward $\mathbf{A}$ to SIS-solver and receive back $\mathbf{z}$ such that $\mathbf{A}^T\mathbf{z} = \mathbf{0} \bmod q$ and $\mathbf{z}$ short.

Connection between LWE and SIS

👉 If there is an efficient solver for SIS, then there is an efficient solver for D-LWE.

Proof.

Given $(\mathbf{A}, \mathbf{b})$, our goal is to decide whether
1) $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ for short error $\mathbf{e}$ or 2) $\mathbf{b} \leftarrow \text{Unif}(\mathbb{Z}_q^m)$.

Forward $\mathbf{A}$ to SIS-solver and receive back $\mathbf{z}$ such that $\mathbf{A}^T\mathbf{z} = \mathbf{0} \bmod q$ and $\mathbf{z}$ short.

Compute $\left\|\mathbf{b}^T\mathbf{z}\right\|$. If the norm is $\ll q$, claim that we are in case 1). Else, claim that we are in case 2).

□

Connection between LWE and SIS

👉 If there is an efficient solver for SIS, then there is an efficient solver for D-LWE.

Proof.

Given $(\mathbf{A}, \mathbf{b})$, our goal is to decide whether
1) $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ for short error $\mathbf{e}$ or 2) $\mathbf{b} \leftarrow \text{Unif}(\mathbb{Z}_q^m)$.

Forward $\mathbf{A}$ to SIS-solver and receive back $\mathbf{z}$ such that $\mathbf{A}^T\mathbf{z} = \mathbf{0} \bmod q$ and $\mathbf{z}$ short.

Compute $\left\|\mathbf{b}^T\mathbf{z}\right\|$. If the norm is $\ll q$, claim that we are in case 1). Else, claim that we are in case 2).

Case 1) $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, thus $\mathbf{b}^T\mathbf{z} = \mathbf{s}^T\mathbf{A}^T\mathbf{z} + \mathbf{e}^T\mathbf{z} = \mathbf{e}^T\mathbf{z} \bmod q$. Thus $\left\|\mathbf{b}^T\mathbf{z}\right\| \leq \|\mathbf{e}\| \cdot \|\mathbf{z}\| \ll q$.

Case 2) $\mathbf{b}$ uniform, so is $\mathbf{b}^T\mathbf{z}$ and hence $\left\|\mathbf{b}^T\mathbf{z}\right\|$ is not particularly small with high chances. □

Example Parameters for Learning With Errors

- LWE is more flexible $\rightarrow$ good for constructions
- LWE is parametrized by more parameters $\rightarrow$ harder to choose concrete parameters
  - m, n and q as for SIS
  - Distribution of error D_e
  - Distribution of secret D_s

I'm very much interested in understanding under what choices LWE "remains" a hard problem?

Example Parameters for Learning With Errors

- LWE is more flexible $\rightarrow$ good for constructions
- LWE is parametrized by more parameters $\rightarrow$ harder to choose concrete parameters
  - m, n and q as for SIS
  - Distribution of error D_e
  - Distribution of secret D_s

For simplicity, 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

Reminder: Public-Key Encryption

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

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

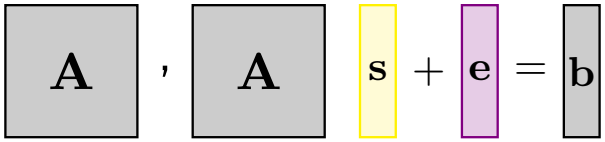
Correctness: $\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m)) = m$ during an honest execution

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

Public-Key Encryption from LWE [Reg05]*

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

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

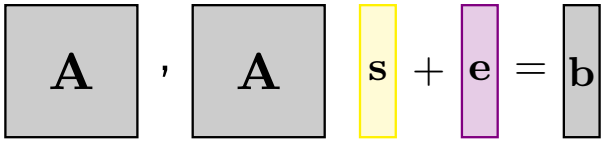


*Regev, *On lattices, learning with errors, random linear codes, and cryptography*, STOC'05

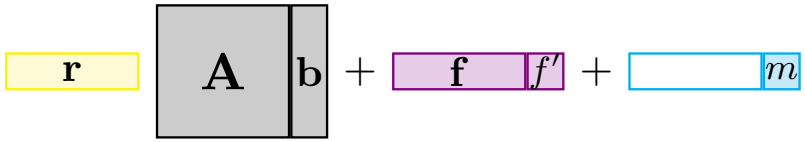
Public-Key Encryption from LWE [Reg05]*

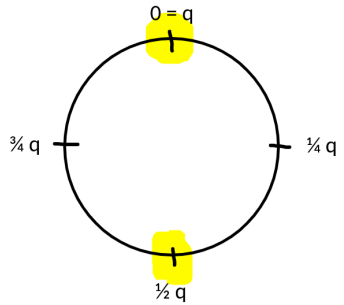
Let χ be distribution on $\mathbb{Z}$.

- KGen:
  - $\mathbf{A} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^{n \times n})$ 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 $\mathsf{ct} = (\mathbf{u}, v)$



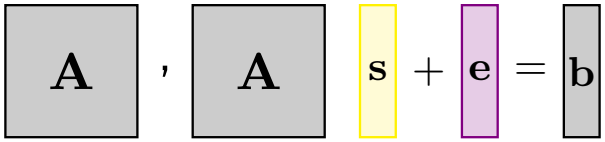


*Regev, *On lattices, learning with errors, random linear codes, and cryptography*, STOC'05

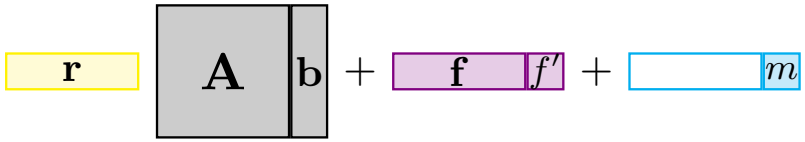
Public-Key Encryption from LWE [Reg05]*

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

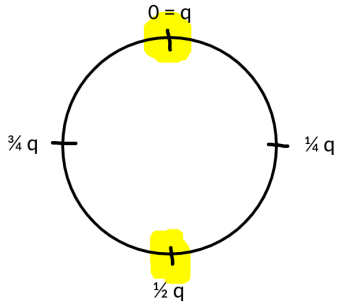
- KGen:
  - $\mathbf{A} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^{n \times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output $\mathsf{sk} = \mathbf{s}$ and $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$



- $\mathsf{Enc}(\mathsf{pk}, m \in \{0,1\})$:
  - $\mathbf{r}, \mathbf{f} \leftarrow \chi^n$ 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 $\mathsf{ct} = (\mathbf{u}, v)$



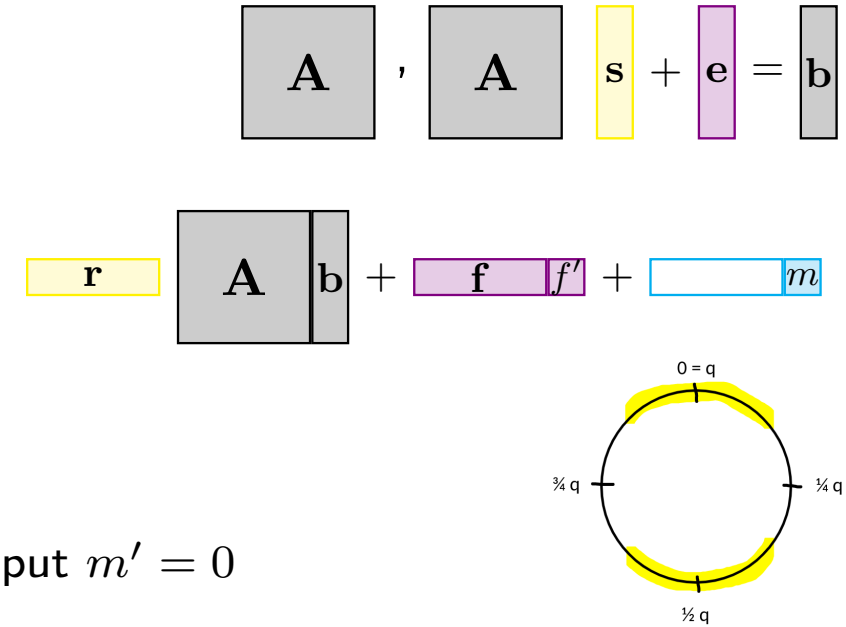
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$:
  - If $v - \mathbf{u}\mathbf{s}$ is closer to 0 than to $q/2$, output $m' = 0$
  - Else output $m' = 1$



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

Public-Key Encryption from LWE [Reg05]*

- KGen:
  - $\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{n \times n})$ and $\mathbf{s}, \mathbf{e} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  - Output $\text{sk} = \mathbf{s}$ and $\text{pk} = (\mathbf{A}, \mathbf{b})$
- Enc$(\text{pk}, m \in \{0,1\})$:
  - $\mathbf{r}, \mathbf{f} \leftarrow \chi^n$ 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 $\text{ct} = (\mathbf{u}, v)$
- 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:

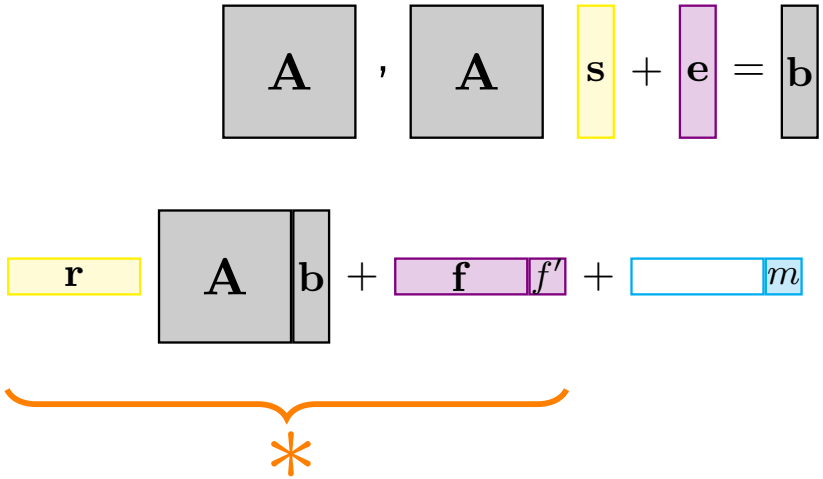
$$\begin{aligned} v - \mathbf{u}\mathbf{s} &= \mathbf{r}(\mathbf{A}\mathbf{s} + \mathbf{e}) + f' + \lfloor q/2 \rfloor \cdot m - (\mathbf{r}\mathbf{A} + \mathbf{f})\mathbf{s} \\ &= \underbrace{\mathbf{r}\mathbf{e} + f' - \mathbf{f}\mathbf{s}}_{*\text{ ciphertext noise}} + \lfloor q/2 \rfloor m \end{aligned}$$

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

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

Public-Key Encryption from LWE [Reg05]*

- KGen:
  - $\mathbf{A} \leftarrow \mathsf{Unif}(\mathbb{Z}_q^{n \times n})$ 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 $m' = 1$



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

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

Kyber - Standardized by NIST

Kyber = the previous construction + several improvements

Main improvements:

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

Kyber512:
- 118 security bits
- $|ct| \approx |pk| \approx 800$ Bytes
- < 0.1 ms

$\cdot 2$

Kyber1024:
- 256 security bits
- $|ct| \approx |pk| \approx 1600$ Bytes
- < 0.2 ms

Sources:

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

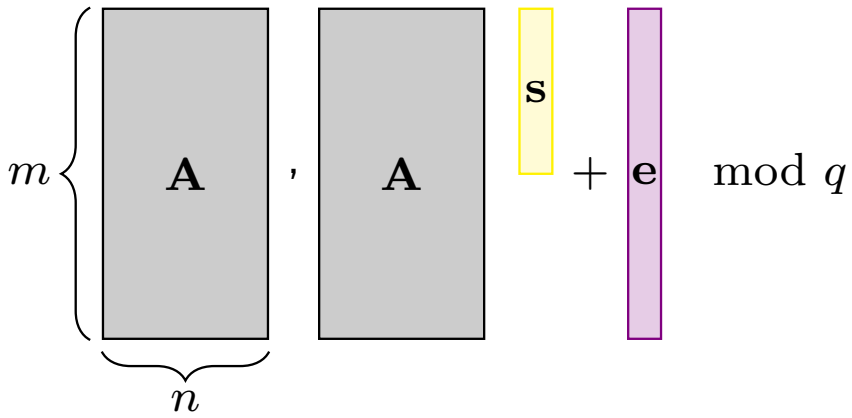
Part 4:

What else you need to know

Recall: The Learning With Errors (LWE) Problem

$\mathbb{Z}_q$ = integers modulo q

$\mathbf{A} \sim \text{Unif}(\mathbb{Z}_q^{m \times n})$, $\mathbf{s} \sim$ DistrS and $\mathbf{e} \sim$ DistrE

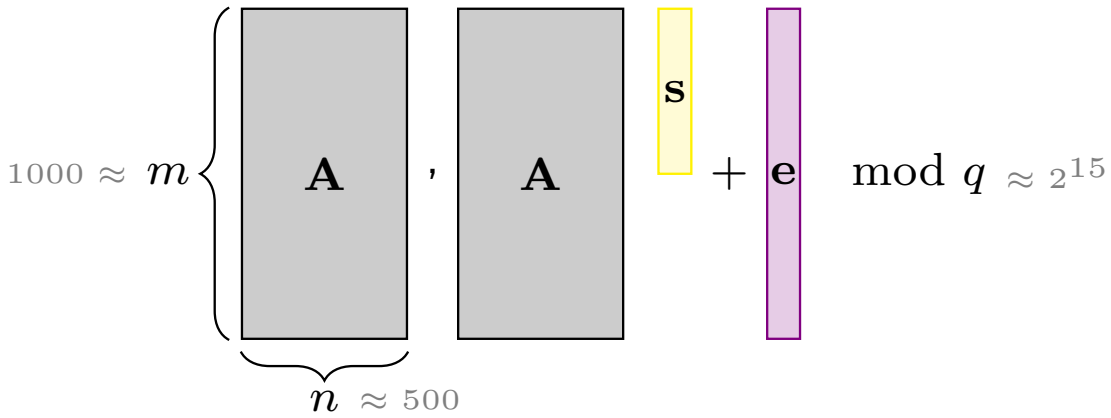


Given $(\mathbf{A}, \mathbf{As} + \mathbf{e} \bmod q)$, find $\mathbf{s}$

Recall: The Learning With Errors (LWE) Problem

$\mathbb{Z}_q$ = integers modulo q

$\mathbf{A} \sim \mathsf{Unif}(\mathbb{Z}_q^{m \times n})$, $\mathbf{s} \sim$ DistrS and $\mathbf{e} \sim$ DistrE

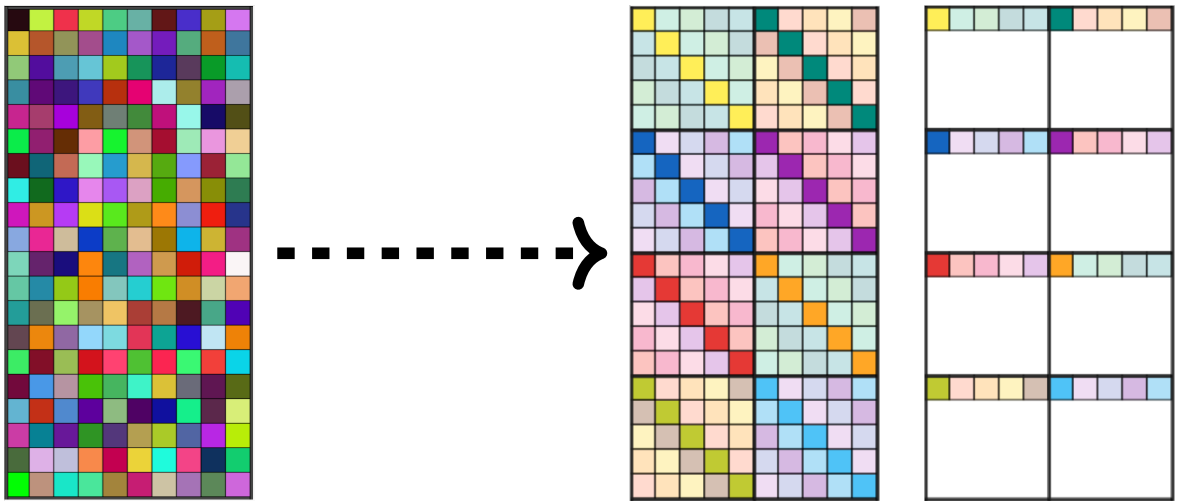


Given $(\mathbf{A}, \mathbf{As} + \mathbf{e} \bmod q)$, find $\mathbf{s}$

- ⚠ Storage: $m(n+1)\log_2 q$ bits
- ⚠ Computation: $O(mn)$ operations over $\mathbb{Z}_q$

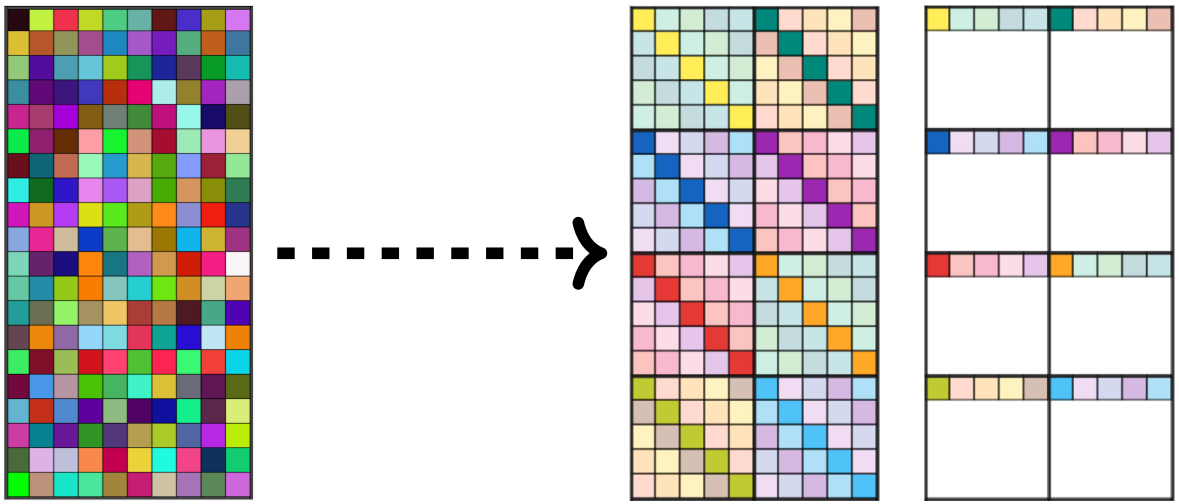
Idea

Improve efficiency by adding **structure**!



Idea

Improve efficiency by adding **structure**!



How? Replace $\mathbb{Z}$ by $R = \mathbb{Z}[x]/(x^d + 1)$ for some d

Concrete Example

Consider $d = 4$, yielding $R = \mathbb{Z}[x]/(x^4 + 1)$

⚠ Very low degree, **not** suited for real crypto schemes

Concrete Example

Consider $d = 4$, yielding $R = \mathbb{Z}[x]/(x^4 + 1)$

⚠ Very low degree, **not** suited for real crypto schemes

Let $f = 3x^3 + 7x^2 - 4x + 5$ and $g = -x^3 - x^2 + 2x + 3$ be elements in R

$$
\begin{aligned}
\textbf{+} \quad f + g &= 2x^3 + 6x^2 - 2x + 8 \\
\textbf{×} \quad f \cdot g &= -3x^6 - 10x^5 + 3x^4 + 22x^3 + 8x^2 - 2x + 15 \qquad \text{(use } x^4 + 1 = 0\text{)} \\
&= 22x^3 + (3 + 8)x^2 + (10 - 2)x + (-3 + 15) \\
&= 22x^3 + 11x^2 + 8x + 12
\end{aligned}
$$

Concrete Example

Consider $d = 4$, yielding $R = \mathbb{Z}[x]/(x^4 + 1)$

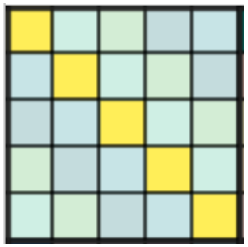
⚠ Very low degree, **not** suited for real crypto schemes

Let $f = 3x^3 + 7x^2 - 4x + 5$ and $g = -x^3 - x^2 + 2x + 3$ be elements in R

$$
\begin{aligned}
\textbf{+} \quad f + g &= 2x^3 + 6x^2 - 2x + 8 \\
\textbf{×} \quad f \cdot g &= -3x^6 - 10x^5 + 3x^4 + 22x^3 + 8x^2 - 2x + 15 \qquad (\text{use } x^4 + 1 = 0) \\
&= 22x^3 + (3 + 8)x^2 + (10 - 2)x + (-3 + 15) \\
&= 22x^3 + 11x^2 + 8x + 12
\end{aligned}
$$

Other way:

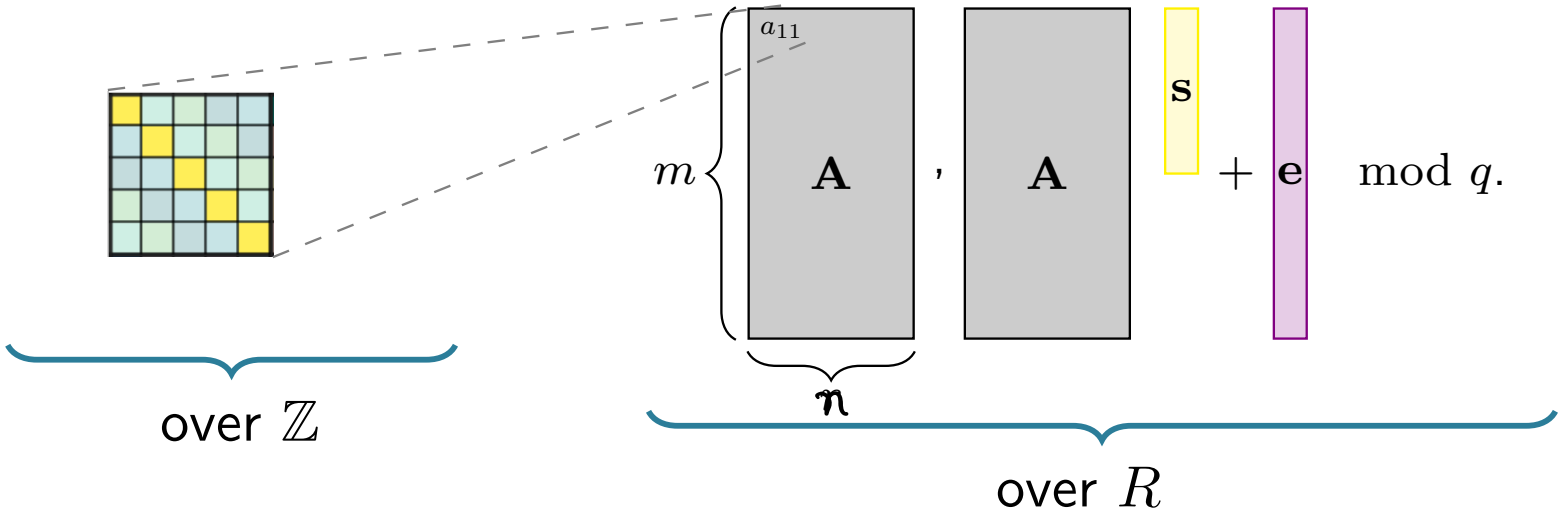
$$
f \cdot g = \begin{bmatrix} 5 & -3 & -7 & 4 \\ -4 & 5 & -3 & -7 \\ 7 & -4 & 5 & -3 \\ 3 & 7 & -4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 2 \\ -1 \\ -1 \end{bmatrix} = \begin{bmatrix} 12 \\ 8 \\ 11 \\ 22 \end{bmatrix}
$$



Module Learning With Errors (Module-LWE)

Idea: sample $\mathbf{A}$ random over $R \Rightarrow$ structured over $\mathbb{Z}$

$\mathbf{A} \sim \mathsf{Unif}(R_q^{m \times \mathfrak{n}})$, $\mathbf{s} \sim$ DistrS and $\mathbf{e} \sim$ DistrE



Given $(\mathbf{A}, \mathbf{As} + \mathbf{e} \bmod q)$, find $\mathbf{s}$

- Before: LWE
- Kyber: Module-LWE with $R_q = \mathbb{Z}_q[x]/(x^d + 1)$, where $d = 256$ and $q = 3329$

↳ very popular choice nowadays

Beyond Encrypting Messages

- Same blueprint for FHE (fully homomorphic encryption)
  - But much larger modulus q (around 40-60 bits)
- Prone to side-channel attacks (like timing or leakage)
  - Hard to apply standard protection techniques
  - Ongoing project on modifying Kyber in a way that it's better protected against side-channel attacks
- Delicate to thresholdize
  - Smallness conditions provide security issues
  - So far: either have to pay in terms of efficiency or security

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?

- ✉ 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!*

Any questions or interested in my research?

- ✉️ Write me an e-mail

Thanks!


Miklós Ajtai.
Generating hard instances of lattice problems (extended abstract).
In *STOC*, pages 99–108. ACM, 1996.


Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham.
Aggregate and verifiably encrypted signatures from bilinear maps.
In *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.


Whitfield Diffie and Martin E. Hellman.
New directions in cryptography.
IEEE Trans. Inf. Theory, 22(6):644–654, 1976.


Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
Trapdoors for hard lattices and new cryptographic constructions.
In *STOC*, pages 197–206. ACM, 2008.


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