Lattice Cryptosystems

Hari

Lattice Cryptosystems

- Why this?

Lattice Cryptosystems

- Why this?
- Lattices

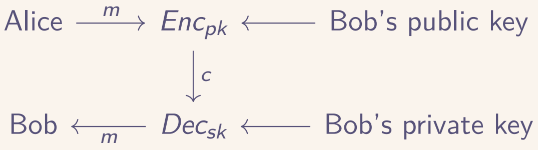
Lattice Cryptosystems

- Why this?
- Lattices
- Cryptosystems

Public Key Encryption

- $\mathsf{Gen} \to (pk, sk)$
- $\mathsf{Enc}_{pk}(m) \to c$
- $\mathsf{Dec}_{sk}(c) \to m$

Public Key Encryption



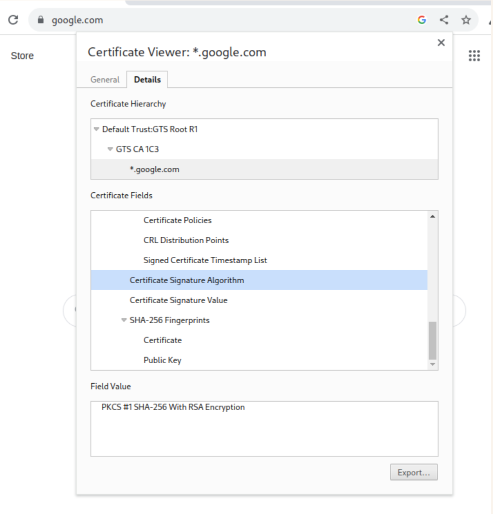
Public Key Encryption

- Most commonly used today is *RSA*
- Relies on the problem of factoring two large numbers

Public Key Encryption

- Most commonly used today is *RSA*
- Relies on the problem of factoring two large numbers
- Can be factored in polynomial time by quantum computers: Shor's algorithm

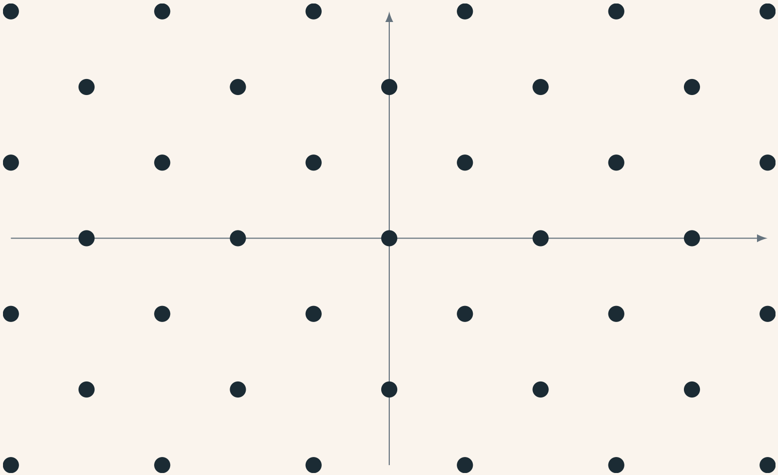
Public Key Encryption



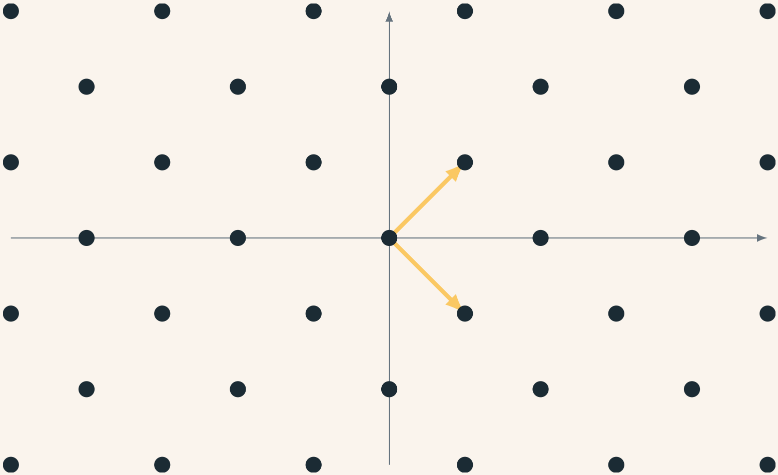
Lattices

What is a Lattice?

A **discrete additive subgroup** of $\mathbb{R}^n$



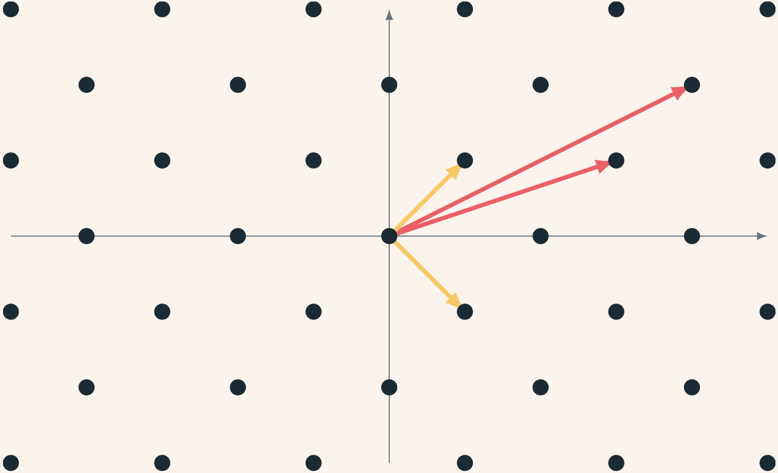
What is a Lattice?



What is a Lattice?

$$\mathcal{L} = \mathcal{L}(\boldsymbol{B}) = \left\{ \sum_{i=1}^{k} z_i \boldsymbol{b}_i : z_i \in \mathbb{Z} \right\}$$

What is a Lattice?



Shortest Vector

Definition (Minimum Distance)

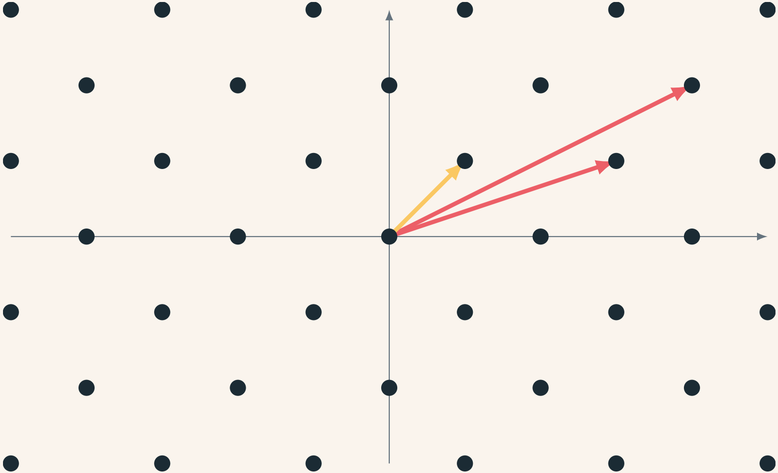
The minimum distance of a lattice $\mathcal{L}$ is the length of the shortest nonzero lattice vector:

$$\lambda_1(\mathcal{L}) = \min_{v \in \mathcal{L} \setminus \{0\}} \|\boldsymbol{v}\|$$

*(more generally: $\lambda_i(\mathcal{L})$ is the smallest r such that $\mathcal{L}$ has i linearly independent vectors of norm at most r)

Shortest Vector

$$\mathcal{L}(\boldsymbol{B}) \to \lambda_1(\mathcal{L})?$$



Shortest Vector

Definition (Shortest Vector Problem (SVP))

Given an arbitrary basis $\boldsymbol{B}$ of some lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, find a shortest nonzero lattice vector $\boldsymbol{v} \in \mathcal{L}$ for which $\|\boldsymbol{v}\| = \lambda_1(\mathcal{L})$.

Shortest Vector

Definition (Shortest Vector Problem (SVP))

Given an arbitrary basis $\boldsymbol{B}$ of some lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, find a shortest nonzero lattice vector $\boldsymbol{v} \in \mathcal{L}$ for which $\|\boldsymbol{v}\| = \lambda_1(\mathcal{L})$.

- Known to be NP hard

Shortest Vector

Definition (Shortest Vector Problem (SVP))

Given an arbitrary basis $\boldsymbol{B}$ of some lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, find a shortest nonzero lattice vector $\boldsymbol{v} \in \mathcal{L}$ for which $\|\boldsymbol{v}\| = \lambda_1(\mathcal{L})$.

- Known to be NP hard
- No known polynomial time quantum algorithm

Relaxations of SVP

Definition (Approximate SVP (SVP_γ))

Given a basis $\boldsymbol{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, find a nonzero vector $\boldsymbol{v} \in \mathcal{L}$ for which $\|\boldsymbol{v}\| \leq \gamma(n) \cdot \lambda_1(\mathcal{L})$.

Relaxations of SVP

Definition (Approximate SVP (SVP_γ))

Given a basis $\boldsymbol{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, find a nonzero vector $\boldsymbol{v} \in \mathcal{L}$ for which $\|\boldsymbol{v}\| \leq \gamma(n) \cdot \lambda_1(\mathcal{L})$.

- “kinda close”

Relaxations of SVP

Definition (Approximate SVP (SVP_γ))

Given a basis $\boldsymbol{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, find a nonzero vector $\boldsymbol{v} \in \mathcal{L}$ for which $\|\boldsymbol{v}\| \leq \gamma(n) \cdot \lambda_1(\mathcal{L})$.

- "kinda close"
- $\gamma = 1$ is standard SVP

Relaxations of SVP

Definition (Decisional Approximate SVP (GapSVP_γ))

Given a basis $\boldsymbol{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, where either $\lambda_1(\mathcal{L}) \leq 1$ or $\lambda_1(\mathcal{L}) > \gamma(n)$, determine which is the case.

Relaxations of SVP

Definition (Decisional Approximate SVP (GapSVP_γ))

Given a basis $\boldsymbol{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, where either $\lambda_1(\mathcal{L}) \leq 1$ or $\lambda_1(\mathcal{L}) > \gamma(n)$, determine which is the case.

- Is the shortest vector "small" or "big"

Relaxations of SVP

Definition (Approximate Shortest Independent Vectors (SIVP_γ))

Given a basis $\boldsymbol{B}$ of a full rank n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, output a set $S = \{\boldsymbol{s}_i\} \subset \mathcal{L}$ of n linearly independent lattice vectors where $\|\boldsymbol{s}_i\| \leq \gamma(n) \cdot \lambda_n(\mathcal{L})$ for all i.

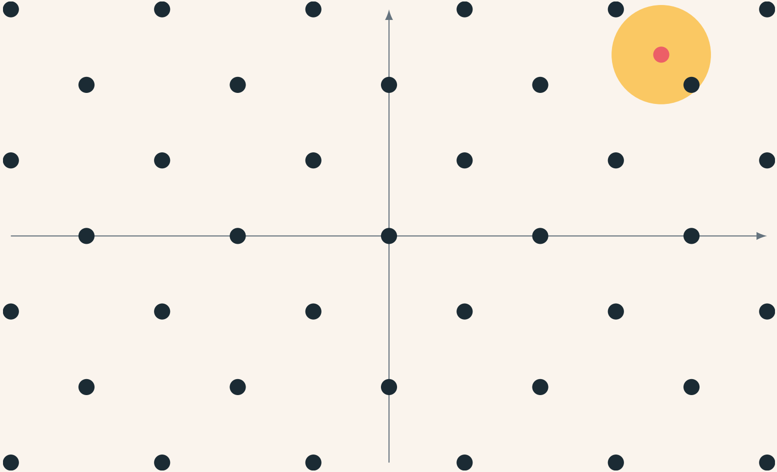
Relaxations of SVP

Definition (Approximate Shortest Independent Vectors (SIVP_γ))

Given a basis $\boldsymbol{B}$ of a full rank n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$, output a set $S = \{\boldsymbol{s}_i\} \subset \mathcal{L}$ of n linearly independent lattice vectors where $\|\boldsymbol{s}_i\| \leq \gamma(n) \cdot \lambda_n(\mathcal{L})$ for all i.

- Give me a basis of short vectors

Bounded Distance Decoding



Bounded Distance Decoding

Definition (Bounded Distance Decoding (BDD_γ))

Given a basis $\boldsymbol{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$ and a target point $\boldsymbol{t} \in \mathbb{R}^n$ with the guarantee that

$$\mathrm{dist}(\boldsymbol{t}, \mathcal{L}) < d = \lambda_1(\mathcal{L})/(2\gamma(n))$$

find the unique lattice vector $\boldsymbol{v} \in \mathcal{L}$ such that $\|\boldsymbol{t} - \boldsymbol{v}\| < d$.

Bounded Distance Decoding

Definition (Bounded Distance Decoding (BDD_γ))

Given a basis $\boldsymbol{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$ and a target point $\boldsymbol{t} \in \mathbb{R}^n$ with the guarantee that

$$\mathrm{dist}(\boldsymbol{t}, \mathcal{L}) < d = \lambda_1(\mathcal{L})/(2\gamma(n))$$

find the unique lattice vector $\boldsymbol{v} \in \mathcal{L}$ such that $\|\boldsymbol{t} - \boldsymbol{v}\| < d$.

- "Find the close point"

Bounded Distance Decoding

Definition (Bounded Distance Decoding (BDD_γ))

Given a basis $\boldsymbol{B}$ of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\boldsymbol{B})$ and a target point $\boldsymbol{t} \in \mathbb{R}^n$ with the guarantee that

$$\mathrm{dist}(\boldsymbol{t}, \mathcal{L}) < d = \lambda_1(\mathcal{L})/(2\gamma(n))$$

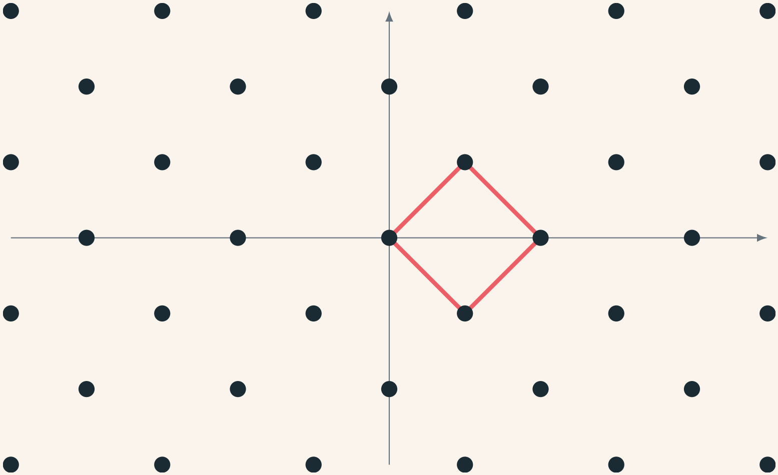
find the unique lattice vector $\boldsymbol{v} \in \mathcal{L}$ such that $\|\boldsymbol{t} - \boldsymbol{v}\| < d$.

- "Find the close point"
- Equivalent to another SVP relaxation with dimension $n + 1$

Bounded Distance Decoding

$$\begin{bmatrix} \boldsymbol{B} & \boldsymbol{t} \\ \mathbf{0} & M \end{bmatrix}$$

Some Fun Lattice Things



Some Fun Lattice Things

Definition (Fundamental Parallelepiped)

$$\mathcal{P}(\boldsymbol{B}) = \{\boldsymbol{B}x : x \in \mathbb{R}^n, \forall i, 0 \leq x_i \leq 1\}$$

Some Fun Lattice Things

Definition (Fundamental Parallelepiped)

$$\mathcal{P}(\boldsymbol{B}) = \{\boldsymbol{B}x : x \in \mathbb{R}^n, \forall i, 0 \leq x_i \leq 1\}$$

Definition (Volume of a Lattice $\mathcal{L}$)

$$\mathrm{vol}(\mathcal{L}) = \sqrt{\det\left(\boldsymbol{B}^T\boldsymbol{B}\right)}$$

Some Fun Lattice Things

Definition (Fundamental Parallelepiped)

$$\mathcal{P}(\boldsymbol{B}) = \{\boldsymbol{B}x : x \in \mathbb{R}^n, \forall i, 0 \leq x_i \leq 1\}$$

Definition (Volume of a Lattice $\mathcal{L}$)

$$\mathrm{vol}(\mathcal{L}) = \sqrt{\det\left(\boldsymbol{B}^T\boldsymbol{B}\right)}$$

When the Lattice is full rank, we have $\mathrm{vol}(\mathcal{L}) = |\det B|$

Some Fun Lattice Things

Theorem

Let $\mathcal{L}$ *be a lattice of rank n. Let* $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots \boldsymbol{b}_n \in \mathcal{L}$ *be n linearly independent lattice vectors. Then* $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots \boldsymbol{b}_n$ *form a basis of* $\mathcal{L}$ *if and only if* $\mathcal{P}(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots \boldsymbol{b}_n) \cap \mathcal{L} = \{\mathbf{0}\}$.

Some Fun Lattice Things

Theorem

Two basis $\boldsymbol{B_1}$, $\boldsymbol{B_2}$ span the same lattice if and only if there exists an integer unimodular matrix $\boldsymbol{U}$ ($|\det \boldsymbol{U}| = 1$) such that $\boldsymbol{B_2} = \boldsymbol{B_1}\boldsymbol{U}$.

Some Fun Lattice Things

Theorem (Blichfeld's Theorem)

Let $\mathcal{L}$ be a lattice, and let $S \subseteq \mathbb{R}^n$ be a set with $\mathrm{vol}(S) > \mathrm{vol}(\mathcal{L})$. Then there exists two nonequal points $z_1, z_2 \in S$ such that $z_1 - z_2 \in \mathcal{L}$.

Some Fun Lattice Things

Theorem (Minkowski's Bound)

Let $\mathcal{L}$ be a lattice. Then there is an $x \in \mathcal{L} \setminus \{0\}$ with

$$\|x\| \leq \sqrt{n}\,|\mathrm{vol}(\mathcal{L})\,|^{1/n}$$

Applications

- Sphere Packing
- Crystallography
- Coding Theory and Error Correction
- **Lattice based Cryptosystems**
- Lattice based Cryptanalysis: CSEC@UMD (Wednesday!)

Cryptosystems

Short Integer Solutions

Definition (Short Integer Solutions ($\mathrm{SIS}_{n,q,\beta,m}$))

Given a uniformly random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, find nonzero integer vector $\boldsymbol{z} \in \mathbb{Z}^m$ of norm $\|\boldsymbol{z}\| \leq \beta < q$ such that

$$\boldsymbol{Az} = \boldsymbol{0} \in \mathbb{Z}_q^n$$

Short Integer Solutions

Definition (Short Integer Solutions ($\mathrm{SIS}_{n,q,\beta,m}$))

Given a uniformly random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, find nonzero integer vector $\boldsymbol{z} \in \mathbb{Z}^m$ of norm $\|\boldsymbol{z}\| \leq \beta < q$ such that

$$\boldsymbol{Az} = \mathbf{0} \in \mathbb{Z}_q^n$$

- Find a “short” linear combination of column vectors to get $\mathbf{0}$.

Short Integer Solutions

Definition (Short Integer Solutions ($\mathrm{SIS}_{n,q,\beta,m}$))

Given a uniformly random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, find nonzero integer vector $\boldsymbol{z} \in \mathbb{Z}^m$ of norm $\|\boldsymbol{z}\| \leq \beta < q$ such that

$$\boldsymbol{Az} = \mathbf{0} \in \mathbb{Z}_q^n$$

- Find a "short" linear combination of column vectors to get $\mathbf{0}$.
- Note $\beta < q$ as the vector $(q, 0, 0, \ldots)$ satisfies the solution.

Short Integer Solutions

Definition (Short Integer Solutions ($\mathrm{SIS}_{n,q,\beta,m}$))

Given a uniformly random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, find nonzero integer vector $\boldsymbol{z} \in \mathbb{Z}^m$ of norm $\|\boldsymbol{z}\| \leq \beta < q$ such that

$$\boldsymbol{A}\boldsymbol{z} = \boldsymbol{0} \in \mathbb{Z}_q^n$$

- Find a "short" linear combination of column vectors to get **0**.
- Note $\beta < q$ as the vector $(q, 0, 0, \ldots)$ satisfies the solution.
- Non homogeneous SIS: $\boldsymbol{A}\boldsymbol{z} = \boldsymbol{k}$

Short Integer Solutions

Theorem

For any $m = \mathrm{poly}(n)$, $\beta > 0$, $q \geq \beta \cdot \mathrm{poly}(n)$, *solving* $\mathrm{SIS}_{n,\beta,q,m}$ *is at least as hard as solving* GapSVP_γ *and* SIVP_γ *for some* $\gamma = \beta \cdot \mathrm{poly}(n)$.

Short Integer Solutions

Theorem

For any $m = \mathrm{poly}(n)$, $\beta > 0$, $q \geq \beta \cdot \mathrm{poly}(n)$, *solving* $\mathrm{SIS}_{n,\beta,q,m}$ *is at least as hard as solving* GapSVP_γ *and* SIVP_γ *for some* $\gamma = \beta \cdot \mathrm{poly}(n)$.

- SIS is as hard as approximate SVP

Short Integer Solutions

Theorem

For any $m = \mathrm{poly}(n)$, $\beta > 0$, $q \geq \beta \cdot \mathrm{poly}(n)$, solving $\mathrm{SIS}_{n,\beta,q,m}$ is at least as hard as solving GapSVP_γ and SIVP_γ for some $\gamma = \beta \cdot \mathrm{poly}(n)$.

- SIS is as hard as approximate SVP
- Intuition behind proof: We have an **oracle** that solves SIS, can we then solve approximate SVP?

Short Integer Solutions

- High level idea: we take a set of lattice vectors $\boldsymbol{S} \subset \mathcal{L}$, and reduce it to a new set $\|\boldsymbol{S}'\| \leq \|\boldsymbol{S}\|/2$ (where $\|S\| = \max \|S_i\|$)

Short Integer Solutions

- High level idea: we take a set of lattice vectors $\boldsymbol{S} \subset \mathcal{L}$, and reduce it to a new set $\|\boldsymbol{S}'\| \leq \|\boldsymbol{S}\|/2$ (where $\|S\| = \max \|S_i\|$)
- Iterate until vectors satisfy the SIVP condition, so we have solved SIVP using SIS

Short Integer Solutions

- High level idea: we take a set of lattice vectors $\boldsymbol{S} \subset \mathcal{L}$, and reduce it to a new set $\|\boldsymbol{S}'\| \leq \|\boldsymbol{S}\|/2$ (where $\|S\| = \max \|S_i\|$)
- Iterate until vectors satisfy the SIVP condition, so we have solved SIVP using SIS

Short Integer Solutions

- The core reduction step is to take a set of random "somewhat short" feasible vectors $\boldsymbol{V}$, and provide $\boldsymbol{S}^{-1}\boldsymbol{V} \mod q$ to the oracle

Short Integer Solutions

- The core reduction step is to take a set of random "somewhat short" feasible vectors $\boldsymbol{V}$, and provide $\boldsymbol{S}^{-1}\boldsymbol{V} \mod q$ to the oracle
- If the oracle outputs vector $\boldsymbol{z}$, add $\boldsymbol{V}\boldsymbol{z}/q$ to the new set.

Short Integer Solutions

- The core reduction step is to take a set of random "somewhat short" feasible vectors $\boldsymbol{V}$, and provide $\boldsymbol{S}^{-1}\boldsymbol{V} \mod q$ to the oracle
- If the oracle outputs vector $\boldsymbol{z}$, add $\boldsymbol{V}\boldsymbol{z}/q$ to the new set.
- The devil is in the details:
  - Prove $v \in \mathcal{L}$ and $\|\boldsymbol{v}\| \leq \|\boldsymbol{S}\|/2$
  - $\boldsymbol{A}$ must be "close enough" to a uniform matrix

Quick Aside: Relaxing SIS

- Whole Zoo of *SIS*-like assumptions: useful for different cryptography constructions

Quick Aside: Relaxing SIS

- Whole Zoo of *SIS*-like assumptions: useful for different cryptography constructions
- Provide some "hint" information with the base $\boldsymbol{A}$ matrix

Quick Aside: Relaxing SIS

- Whole Zoo of *SIS*-like assumptions: useful for different cryptography constructions
- Provide some "hint" information with the base $\boldsymbol{A}$ matrix
- Some add structure: for example, module SIS replaces elements in the matrix with structured ring elements

Quick Aside: Relaxing SIS

- Whole Zoo of *SIS*-like assumptions: useful for different cryptography constructions
- Provide some "hint" information with the base $\boldsymbol{A}$ matrix
- Some add structure: for example, module SIS replaces elements in the matrix with structured ring elements
- Some don't have reductions: open problems

Learning with Error

Definition (Learning With Error ($LWE_{n,q,\chi,m}$))

Given uniform random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{nxm}$ and

$$\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \mod q$$

where $\boldsymbol{s}$ is sampled from a short distribution χ^n and $\boldsymbol{e}$ is sampled from a short distribution χ^m,
Find the vector $\boldsymbol{s}$.

Learning with Error

Definition (Learning With Error ($LWE_{n,q,\chi,m}$))

Given uniform random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{nxm}$ and

$$\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \mod q$$

where $\boldsymbol{s}$ is sampled from a short distribution χ^n and $\boldsymbol{e}$ is sampled from a short distribution χ^m,
Find the vector $\boldsymbol{s}$.

- Has a quantum reduction to GapSVP and SIVP (idk how it works some QFFT magic)

Learning with Error

Definition (Learning With Error ($LWE_{n,q,\chi,m}$))

Given uniform random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{nxm}$ and

$$\boldsymbol{b} = \boldsymbol{As} + \boldsymbol{e} \mod q$$

where $\boldsymbol{s}$ is sampled from a short distribution χ^n and $\boldsymbol{e}$ is sampled from a short distribution χ^m,
Find the vector $\boldsymbol{s}$.

- Has a quantum reduction to GapSVP and SIVP (idk how it works some QFFT magic)
- Also has more structured variants: Ring-LWE and friends

Public Key Encryption

- Generate $\boldsymbol{b}^T = \boldsymbol{s}^T \boldsymbol{A} + \boldsymbol{e}^T \mod q$

Public Key Encryption

- Generate $\boldsymbol{b}^T = \boldsymbol{s}^T\boldsymbol{A} + \boldsymbol{e}^T \mod q$
- Public: $(\boldsymbol{A}, \boldsymbol{b})$
- Private: $(\boldsymbol{s}^T, \boldsymbol{e}^T)$

Public Key Encryption

- Encryption of bit μ:

Public Key Encryption

- Encryption of bit μ:
- Choose random small $\boldsymbol{x} \leftarrow \chi^{m}$

Public Key Encryption

- Encryption of bit μ:
- Choose random small $\boldsymbol{x} \leftarrow \chi^m$
- $\boldsymbol{c}_0 = \boldsymbol{A}\boldsymbol{x}$
- $\boldsymbol{c}_1 = \boldsymbol{b}^T\boldsymbol{x} + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor$

Public Key Encryption

- Decryption with secret key $\boldsymbol{s}^T$:

Public Key Encryption

- Decryption with secret key $\boldsymbol{s}^T$:
- $\boldsymbol{c}_1 - \boldsymbol{s}^T \boldsymbol{c}_0$

Public Key Encryption

- Decryption with secret key $\boldsymbol{s}^T$:
- $\boldsymbol{c}_1 - \boldsymbol{s}^T \boldsymbol{c}_0$
- $\boldsymbol{b}^T \boldsymbol{x} + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor - \boldsymbol{s}^T \boldsymbol{A} \boldsymbol{x}$

Public Key Encryption

- Decryption with secret key $\boldsymbol{s}^T$:
- $\boldsymbol{c}_1 - \boldsymbol{s}^T\boldsymbol{c}_0$
- $\boldsymbol{b}^T\boldsymbol{x} + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor - \boldsymbol{s}^T\boldsymbol{A}\boldsymbol{x}$
- $\boldsymbol{e}^T\boldsymbol{x} + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor$

Public Key Encryption

- Decryption with secret key $\boldsymbol{s}^T$:
- $\boldsymbol{c}_1 - \boldsymbol{s}^T \boldsymbol{c}_0$
- $\boldsymbol{b}^T \boldsymbol{x} + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor - \boldsymbol{s}^T \boldsymbol{A} \boldsymbol{x}$
- $\boldsymbol{e}^T \boldsymbol{x} + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor$
- $\boldsymbol{e}$ and $\boldsymbol{x}$ are **small**

Fun Lattice Things Part 2

- Ring-LWE and Ring-SIS: Elements of the matrices chosen from cyclotomic rings

Fun Lattice Things Part 2

- Ring-LWE and Ring-SIS: Elements of the matrices chosen from cyclotomic rings
- Notion of "short" vector is different: based on the canonical embedding

Fun Lattice Things Part 2

- Ring-LWE and Ring-SIS: Elements of the matrices chosen from cyclotomic rings
- Notion of "short" vector is different: based on the canonical embedding
- More "structured": security proofs are more subtle

Fun Lattice Things Part 2

- Ring-LWE and Ring-SIS: Elements of the matrices chosen from cyclotomic rings
- Notion of “short” vector is different: based on the canonical embedding
- More “structured”: security proofs are more subtle
- Security reductions are based on short vector problems in ideal lattices (not arbitrary lattices)

Fin

- Discussed Lattices
- Lattice based hardness assumptions
- Built cryptography from lattices!