Lattice-Based Cryptography: LWE, SIS and Their Applications

Mriganka Dey

CREST Crypto Summer School

June 27, 2025

tcg crest
Inventing Harmonious Future

RAMAKRISHNA MISSION

Recall: Lattices

- A Lattice is an additive subgroup of $\mathbb{Z}^m$(full rank).

Recall: Lattices

- A Lattice is an additive subgroup of $\mathbb{Z}^m$(full rank).
- Given a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$, the lattice is:

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

Recall: Lattices

- A Lattice is an additive subgroup of $\mathbb{Z}^m$(full rank).
- Given a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$, the lattice is:

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

- Lattices can have many different bases.

Examples of Lattice

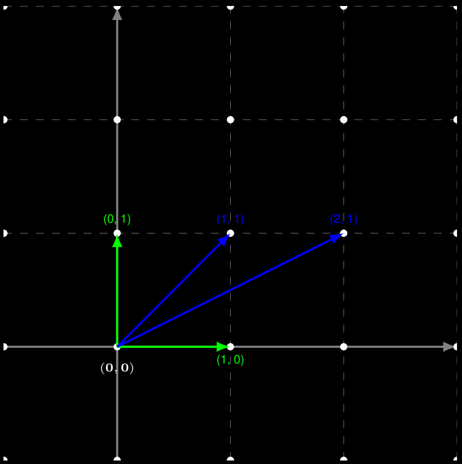


Figure: Depicting $B_1 = \{(0,1),(1,0)\}$ (green) and $B_2 = \{(1,1),(2,1)\}$ (blue) generates $\mathbb{Z}^2$.

Examples of Lattice

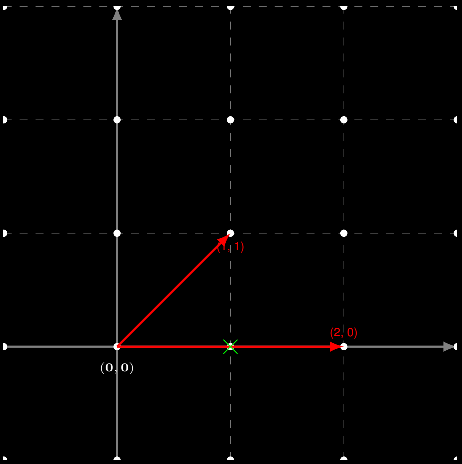


Figure: Depicting $B_3 = \{(1,1),(2,0)\}$ (red) does not generate $\mathbb{Z}^2$.

Some Hard Problems

- SVP (Shortest Vector Problem)
- CVP (Closest Vector Problem)
- SIVP (Shortest Independent Vectors Problem)

Some Hard Problems

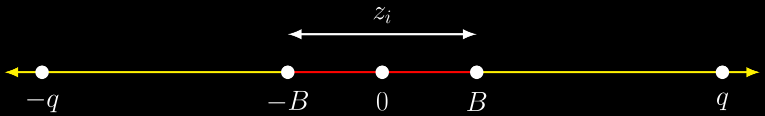
- SVP (Shortest Vector Problem)
- CVP (Closest Vector Problem)
- SIVP (Shortest Independent Vectors Problem)
- SIS (Shortest Integer Solution)
- LWE (Learning With Error)

SIS

- Introduced by Ajtai in 1996
- Problem.(Homogeneous) Given $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, find $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{Az} \equiv \mathbf{0} \mod q$, where $\mathbf{z} \neq \mathbf{0}$ and $\mathbf{z} \in [-B, B]^m$ (and $B << \frac{q}{2}$).(SIS$_2$ problem is defined similarly except $\|\mathbf{z}\|_2 \leq \beta$, $\beta << \frac{q}{2}$)

SIS

$$\underset{n \times m}{\mathbf{A}} \; \underset{m \times 1}{\mathbf{z}} \equiv \underset{n \times 1}{\mathbf{0}} \mod q$$



SIS Lattice

SIS Lattice. $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} \equiv \mathbf{0} \mod q\}, \quad \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$

SIS Lattice

Claim. Suppose the first n columns of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ are linearly independent over $\mathbb{Z}_q$. Then $\mathbf{A}$ can be row-reduced to:

$$\tilde{\mathbf{A}} = \left[\mathbf{I}_n \;\middle|\; \bar{\mathbf{A}}\right], \quad \text{where } \bar{\mathbf{A}} \in \mathbb{Z}_q^{n\times(m-n)}.$$

Then the following matrix forms a basis for the SIS lattice:

$$\mathbf{C} = \begin{bmatrix} q \cdot \mathbf{I}_n & -\bar{\mathbf{A}} \\ \mathbf{0} & \mathbf{I}_{m-n} \end{bmatrix} \in \mathbb{Z}^{m\times m}$$

SIS Lattice

The matrix $\mathbf{C}$ above is a basis matrix for the SIS lattice:

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} \equiv \mathbf{0} \mod q\}$$

Try to prove it!!

SIS Lattice

- Result: SIS_2 is equivalent to solve SVP in an SIS lattice.

- Hardness: Finding a short $\mathbf{z} \in \Lambda_q^\perp(\mathbf{A})$ (i.e., $\|\mathbf{z}\|_2 \le \beta$) for uniformly random $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ implies a solution to $\mathsf{SIVP}_{\beta\sqrt{n}}$ on any n-dimensional lattices.

SIS Example

- Let $n = 3$, $m = 5$, $q = 13$, and $B = 3$.
- SIS instance:

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 7 & 12 & 4 \\ 2 & 11 & 3 & 6 & 12 \\ 9 & 8 & 10 & 5 & 1 \end{bmatrix}$$

- We need to find nonzero $\mathbf{z} = (z_1, z_2, z_3, z_4, z_5) \in [-3, 3]^5$ such that $\mathbf{Az} = \mathbf{0} \mod 13$.

SIS Example

- Let $n = 3$, $m = 5$, $q = 13$, and $B = 3$.
- SIS instance:

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 7 & 12 & 4 \\ 2 & 11 & 3 & 6 & 12 \\ 9 & 8 & 10 & 5 & 1 \end{bmatrix}$$

- We need to find nonzero $\mathbf{z} = (z_1, z_2, z_3, z_4, z_5) \in [-3, 3]^5$ such that $\mathbf{Az} = \mathbf{0} \mod 13$.
- Performing Gaussian elimination on $\mathbf{A}$ yields the reduced matrix:

$$\tilde{\mathbf{A}} = \begin{bmatrix} 1 & 0 & 0 & 5 & 10 \\ 0 & 1 & 0 & 10 & 12 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- Among the $13^2 = 169$ total solutions $\mathbf{z} \in \mathbb{Z}_{13}^5$, six are SIS solutions (i.e., in $[-3, 3]^5$):

$$\mathbf{z} = \pm(3, 1, -1, 0, 1), \quad \pm(1, 0, -2, -1, 3), \quad \pm(2, 1, 1, 1, -2)$$

Inhomogeneous SIS

Problem.(Inhomogeneous) Given $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, find $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{z} \equiv \mathbf{b} \mod q$, where $\mathbf{b} \neq \mathbf{0},\ \mathbf{z} \neq \mathbf{0}$ and $\mathbf{z} \in [-B, B]^m$ (and $B << \frac{q}{2}$).(SIS$_2$ problem is defined similarly except $\|\mathbf{z}\|_2 \leq \beta$, $\beta << \frac{q}{2}$)

Hash Function based on SIS

- **Construction.** Select $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, where $m > n\log q$. Construct

$$\mathsf{H}_{\mathbf{A}} : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n, \quad \mathsf{H}_{\mathbf{A}}(\mathbf{z}) = \mathbf{A}\mathbf{z} \mod q$$

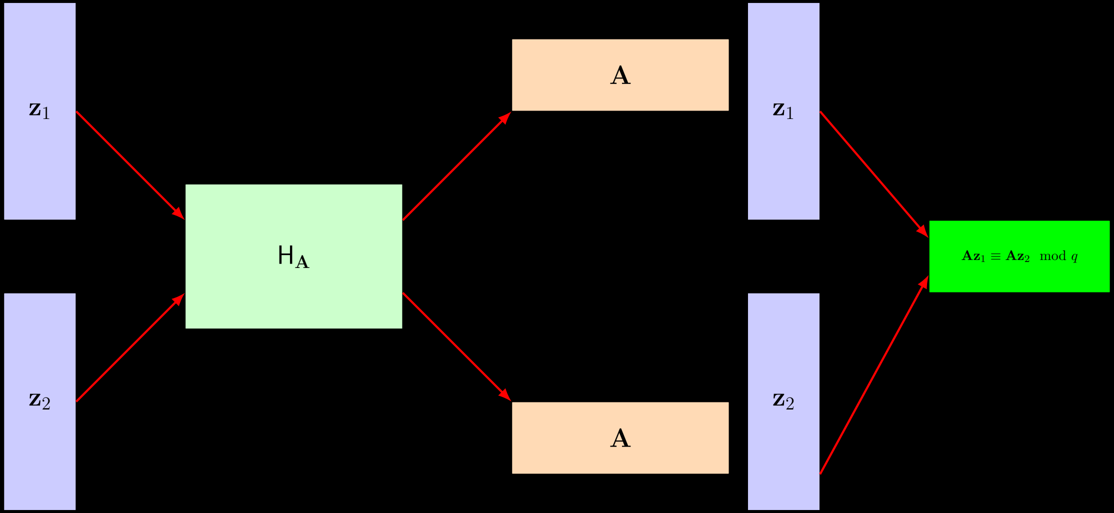
Hash Function based on SIS

- Construction. Select $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, where $m > n \log q$. Construct

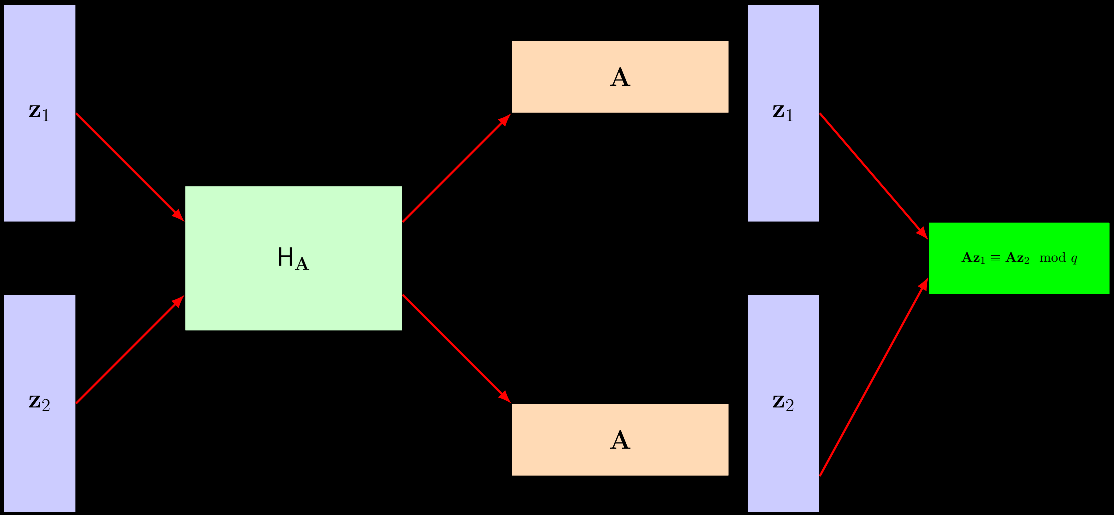
$$\mathsf{H}_{\mathbf{A}} : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n, \quad \mathsf{H}_{\mathbf{A}}(\mathbf{z}) = \mathbf{A}\mathbf{z} \mod q$$

- Collision Resistance. If $\exists$ a probabilistic polynomial time (PPT) algorithm that can compute $\mathbf{z}_1 \neq \mathbf{z}_2$ such that $\mathbf{A}\mathbf{z}_1 = \mathbf{A}\mathbf{z}_2 \mod q$, then it can be used to solve SIS problem.

Hash Function based on SIS



Hash Function based on SIS



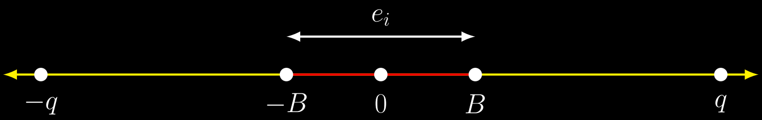
- $\mathbf{z}_1 - \mathbf{z}_2 \in [-1,1]^m$ is a solution of the equation $\mathbf{A}\mathbf{z} = 0 \mod q,$ for $B = 1$.

LWE

- Introduced by Regev in 2005
- Problem. Let $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$ and $\mathbf{e} \xleftarrow{\$} [-B, B]^m$(for more security measures $\mathbf{e} \xleftarrow{\$} \chi$, error distribution) where $B << \frac{q}{2}$. Given $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \mod q \in \mathbb{Z}_q^m$, find $\mathbf{s}$.

LWE

$$\overset{m \times n}{\mathbf{A}}\;\overset{n \times 1}{\mathbf{s}} + \overset{m \times 1}{\mathbf{e}} \equiv \overset{m \times 1}{\mathbf{b}} \mod q$$



Decisional LWE(DLWE)

Problem. Let $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n, \mathbf{e} \xleftarrow{\$} [-B, B]^m$ (for more security measures $\mathbf{e} \xleftarrow{\$} \chi$, error distribution), where $B << \frac{q}{2}$, and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$. Let $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^m$. Let $\mathbf{c} = \mathbf{b}$ with probability $\frac{1}{2}$ and $\mathbf{c} = \mathbf{r}$ with probability $\frac{1}{2}$. Given $(\mathbf{A}, \mathbf{c})$, the problem is to decide (with success probability significantly greater than $\frac{1}{2}$) whether $\mathbf{c} = \mathbf{b}$ or $\mathbf{c} = \mathbf{r}$.

Decisional LWE(DLWE)

Problem. Let $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n, \mathbf{e} \xleftarrow{\$} [-B, B]^m$ (for more security measures $\mathbf{e} \xleftarrow{\$} \chi$, error distribution), where $B << \frac{q}{2}$, and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$. Let $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^m$. Let $\mathbf{c} = \mathbf{b}$ with probability $\frac{1}{2}$ and $\mathbf{c} = \mathbf{r}$ with probability $\frac{1}{2}$. Given $(\mathbf{A}, \mathbf{c})$, the problem is to decide (with success probability significantly greater than $\frac{1}{2}$) whether $\mathbf{c} = \mathbf{b}$ or $\mathbf{c} = \mathbf{r}$.

Result. LWE is as hard as DLWE.

LWE Lattice

LWE Lattice. $\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{y} \mod q$ for some $\mathbf{z} \in \mathbb{Z}^n\}$

LWE Lattice

Claim. Let $\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{bmatrix}, \quad \mathbf{A}_1 \in \mathbb{Z}_q^{n \times n}, \quad \mathbf{A}_2 \in \mathbb{Z}_q^{(m-n) \times n}$ and suppose that $\mathbf{A}_1$ is invertible modulo q.

Define

$$\mathbf{D}_2 = \mathbf{A}_2 \mathbf{A}_1^{-1} \mod q, \quad \mathbf{D} = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{D}_2 & q \cdot \mathbf{I}_{m-n} \end{bmatrix} \in \mathbb{Z}^{m \times m}$$

Then $\mathbf{D}$ is a basis matrix for the LWE lattice:

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

LWE Lattice

Claim. Let $\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{bmatrix}, \quad \mathbf{A}_1 \in \mathbb{Z}_q^{n \times n}, \quad \mathbf{A}_2 \in \mathbb{Z}_q^{(m-n) \times n}$ and suppose that $\mathbf{A}_1$ is invertible modulo q.

Define

$$\mathbf{D}_2 = \mathbf{A}_2 \mathbf{A}_1^{-1} \mod q, \quad \mathbf{D} = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{D}_2 & q \cdot \mathbf{I}_{m-n} \end{bmatrix} \in \mathbb{Z}^{m \times m}$$

Then $\mathbf{D}$ is a basis matrix for the LWE lattice:

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

Try to prove it!!

LWE Example

- Let $m = 5$, $n = 3$, $q = 31$, $B = 2$.

- LWE instance:

$$\mathbf{A} = \begin{bmatrix} 11 & 3 & 27 \\ 12 & 21 & 7 \\ 6 & 23 & 30 \\ 5 & 6 & 2 \\ 21 & 0 & 14 \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} 25 \\ 25 \\ 12 \\ 29 \\ 17 \end{bmatrix}$$

- We need to find $\mathbf{s} \in \mathbb{Z}_q^3$ and $\mathbf{e} \in [-2, 2]^5$ such that $\mathbf{A}\mathbf{s} + \mathbf{e} = \mathbf{b} \mod 31$.

LWE Example

- Let $m = 5$, $n = 3$, $q = 31$, $B = 2$.
- LWE instance:

$$\mathbf{A} = \begin{bmatrix} 11 & 3 & 27 \\ 12 & 21 & 7 \\ 6 & 23 & 30 \\ 5 & 6 & 2 \\ 21 & 0 & 14 \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} 25 \\ 25 \\ 12 \\ 29 \\ 17 \end{bmatrix}$$

- We need to find $\mathbf{s} \in \mathbb{Z}_q^3$ and $\mathbf{e} \in [-2, 2]^5$ such that $\mathbf{As} + \mathbf{e} = \mathbf{b} \mod 31$.
- There are three LWE solutions:

$$\begin{aligned} \mathbf{s} &= (2, 11, 7)^T, & \mathbf{e} &= (-2, 0, 2, 1, 1)^T \\ \mathbf{s} &= (27, 13, 16)^T, & \mathbf{e} &= (1, -2, 1, 1, 1)^T \\ \mathbf{s} &= (30, 9, 5)^T, & \mathbf{e} &= (-2, -1, 2, 1, -1)^T \end{aligned}$$

Regev's Encryption Scheme based on LWE

- **Key Genereation:**
  - **Private Key:** Choose $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$.
    sk: $\mathbf{s}$
  - **Public key:**
    for $i = 1, 2, \ldots, m$
    Choose $\mathbf{a}_i \xleftarrow{\$} \mathbb{Z}_q^n$
    Choose $\mathbf{e}_i \xleftarrow{\$} \chi$ where $\chi : \mathbb{Z}_q \to \mathbb{R}^+$.
    pk: $(\mathbf{a}_i, b_i)_{i=1}^m$ where $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + \mathbf{e}_i$.

Regev's Encryption Scheme based on LWE

- **Encryption:** To encrypt a "bit" do the following.
  - Choose a random subset $S \subseteq [m] \triangleq \{1, 2, \ldots, m\}$.
  - For the encryption of 0 sets

$$(\mathbf{a}, b) \equiv \left(\sum_{i \in S} \mathbf{a}_i, \sum_{i \in S} b_i \right)$$

  - For the encryption of 1 sets

$$(\mathbf{a}, b) \equiv \left(\sum_{i \in S} \mathbf{a}_i, \left\lfloor \frac{q}{2} \right\rfloor + \sum_{i \in S} b_i \right)$$

Regev's Encryption Scheme based on LWE

- **Decryption:** The decryption of of a pair $(\mathbf{a}, b)$ is
  - 0 if $b - \langle \mathbf{a}, \mathbf{s} \rangle$ is "closer" to 0 than $\left\lfloor \frac{q}{2} \right\rfloor$
  - 1 otherwise

Regev's Encryption Scheme based on LWE

- **Decryption:** The decryption of of a pair $(\mathbf{a}, b)$ is
  - 0 if $b - \langle \mathbf{a}, \mathbf{s} \rangle$ is "closer" to 0 than $\lfloor \frac{q}{2} \rfloor$
  - 1 otherwise

Result. The encryption scheme is CPA secure under DLWE assumption.

Materials Consulted

- Miklos Ajtai: **Generating Hard Instances of Lattice Problems (Extended Abstract (STOC' 96)**
- Oded Regev: **On lattices, learning with errors, random linear codes, and cryptography (STOC' 05)**

Thank You

Questions!!