Crafting a Lattice from the Kernels (SIS problem and more)

Debadatta Kar, PhD Scholar,
Electrical Engineering and Computer Science,
Indian Institute of Science Education and Research, Bhopal

November, 2025

XII

---

1 Introduction

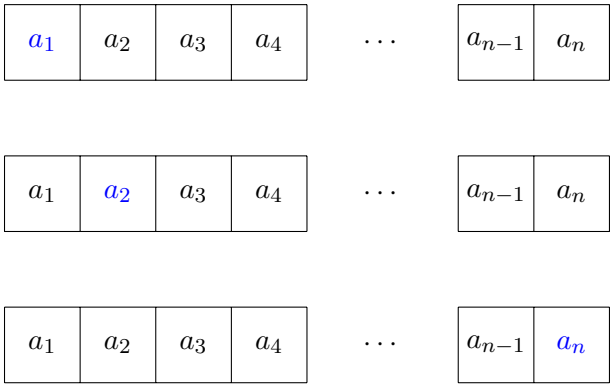
The Short Integer Solution (SIS) problem was first introduced by Ajtai in 1996 in his paper "Generating Hard Instances of the Short Basis Problem". This result became remarkable and established in lattice based cryptography. It showed connection between worst case and average case hardness of problems. SIS then became a foundational problem of designing collision resistant hash function, digital signatures, commitment schemes and id protocols. Over time post-quantum cryptography offering security agianst attacks by quantum computers uses SIS to design cryptographic protocols.

2 Complexity

In Computational complexity theory, we borrow two terms, the average case complexity and the worst-case complexity. The average case complexity of an algorithm is amount of resources used by an algorithm, averaged over all the inputs. The worst-case complexity of an algorithm is the maximum resources consumed by an algorithm over all the inputs. We use the worst case of DDH, CDH, Factoring problems in classical cryptography. In lattice cryptography the underlying problems like SIS or LWE have worst case to average case reduction, i,.e we can build security with an worst case lattice problem.

Example 2.1. *Given a list with n entries and all integers, we wish to search a specific integer a in this list. An algorithm here we use is linear search in which we search over the entries one by one starting from one end to the other. The worst case would be searching in all the n entries and a is found at the $n-th$ position. The least would be if we find a in the first entry itself. The average case would be $\frac{n+1}{2}$.*
For average case we consider the all possibility in the algorithm and take its average which calculates as

$$\frac{1+2+3+4+\cdots+(n-1)+n}{n} = \frac{n\cdot(n+1)}{2\cdot n} = \frac{n+1}{2}$$



3 Shortest Integer Solution (SIS)

Consider a system of linear equations (coefficients and constants are from $\mathbb{R}$) with variables z_1, z_2 as,

$$a_{11}z_1 + a_{12}z_2 = b_1$$
$$a_{21}z_2 + a_{22}z_2 = b_2$$

and we tend to write it as a matrix equation

$$A \cdot \mathbf{z} = \mathbf{b}$$

where,

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}; \qquad \mathbf{z} = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}; \qquad \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

This setup looks very clean and we can construct some variations of system of equations. Consider, A and $\mathbf{b}$ are knowns and $\mathbf{z}$ is unknown. If our matrix A is of size $n \times m$ then it forces the vector $\mathbf{z}$ to be of size $m \times 1$ and $\mathbf{b}$ of size $n \times 1$. In such case we would say $A\mathbf{z} = \mathbf{b}$ is a system of equations with n knowns and m unknowns. Target is to find a vector $\mathbf{z}$ that satisfies the equation.

Input: $A_{n\times m}, \mathbf{b_{n\times 1}}$

Output: $\mathbf{z_{m\times 1}}$

For such a system that we have described it can be categorized into two types, one is non-homogeneous system of equation, where the vector $\mathbf{b}$ is always non-zero, the other one is where $\mathbf{b} = \mathbf{0}$ which we call the homogeneous system of equation. Our focus here is on homogeneous system of equations. An immediate claim is that $\mathbf{z} = \mathbf{0}$ will always serve as a solution to the homogeneous system. However, there can be other solutions too. In this problems a non-trivial solution is desired. If existence of solution is guaranteed then Gaussian elimination serves the purpose of finding one.

The set of all solutions forms a linear space and we call it the kernel or solution space. We represent it as $\Lambda^{\perp}$.

$$\Lambda^{\perp} := \{\mathbf{z} \in \mathbb{Z}^m | \mathbf{Az} = \mathbf{0}\} = \ker(\mathbf{A} : \mathbb{Z}_q^m \to \mathbb{Z}_q^n)$$

As m becomes larger than n it makes the solution space larger as well. This is evident because our solution space searches for $\mathbf{z}$ in $\mathbb{Z}^m$ which gets larger on increasing m.

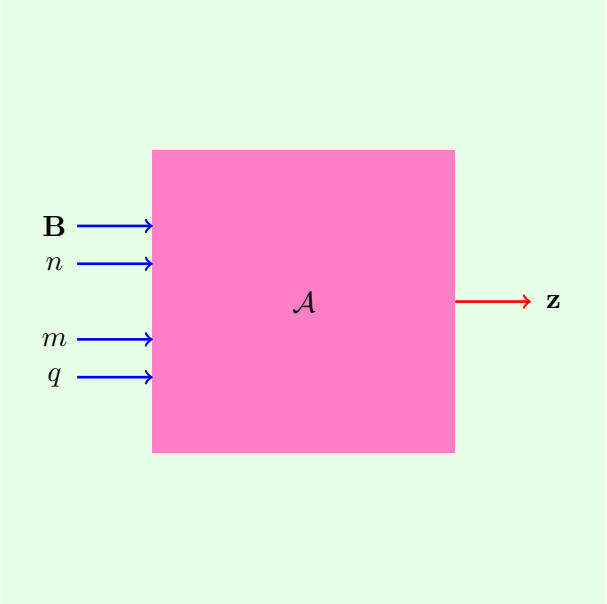
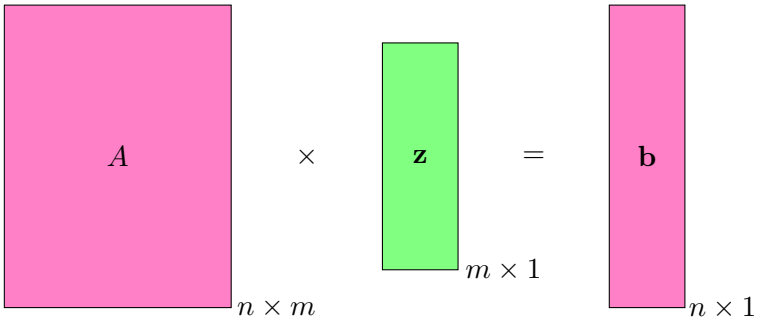


Figure 1: The $\text{SIS}_{n,m,q,\beta}$ oracle



We now introduce this problem as a conjectured hard problem by modifying some parameters and giving a norm bound β which we would call the $\text{SIS}_{n,m,q,\beta}$ problem.

Definition 3.1. **[Short Integer Solution(SIS)]** *For a positive integer modulus q, dimension n, m and a norm bound $\beta > 0$ the $\text{SIS}_{n,m,q,\beta}$ problem is defined as, given uniformly random $\mathbf{A}$ find a non-zero $\mathbf{z} \in [-\beta, \beta]^m$ such that $\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \pmod q$.*

SIS is easy to solve by Gaussian elimination if norm bound $\beta < q$ is not set at first. Moreover, the fact is that $\mathbf{z} = (q, 0, \cdots, 0)$ serves as an immediate solution.

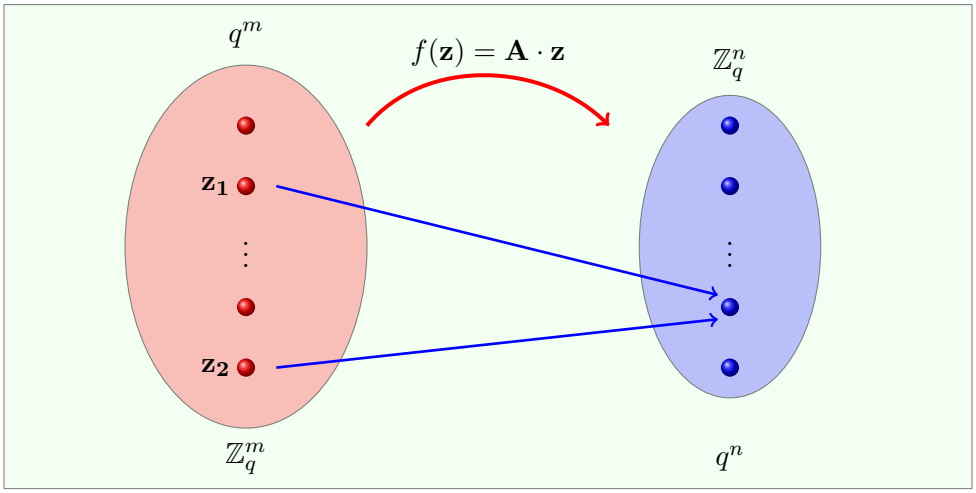
Input: $n, m, q, \beta \in \mathbb{N}$
Prepossessing: $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$
Output: $0 \neq \mathbf{z} \in [-\beta, \beta]^m$ such that $A\mathbf{z} = 0 \pmod q$ with $\|\mathbf{z}\| \leq \beta$

Conjuncture:
For sufficiently large security parameter n and $m, q, \beta \in \mathbb{N}$ (satisfying $q > \beta \cdot poly(n)$ and $\beta << q$) $\text{SIS}_{n,m,q,\beta}$ is hard.

Theorem 3.2. *If $m > n$ then $\text{SIS}_{n,m,q,\beta}$ guarantees a solution $\mathbf{z}$ with $\|\mathbf{z}\| \leq q \cdot \sqrt{m}$.*

Proof. Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ be fixed. Now for $\mathbf{A}$ define the map $f : \mathbb{Z}_q^m \to \mathbb{Z}_q^n$, such that $f(\mathbf{z}) = \mathbf{A}\mathbf{z}$. Here we have q^m choices for $\mathbf{z}$ and q^n choices for $f(\mathbf{z})$. So, by pigeonhole principle, if we have,

$$q^m > q^n \iff m > n$$



then we can get at least one pair $\mathbf{z_1}, \mathbf{z_2} \in \mathbb{Z}_q^m$ such that

$$\mathbf{A} \cdot \mathbf{z_1} = \mathbf{A} \cdot \mathbf{z_2} \pmod{q} \implies \mathbf{A} \cdot (\mathbf{z_1} - \mathbf{z_2}) = \mathbf{0} \pmod{q} \implies \mathbf{A} \cdot \mathbf{z} = \mathbf{0} \pmod{q}$$

Moreover, making $m >> n$ guarantees existence of more such solutions.
Now for bounding $\mathbf{z} = (\mathbf{z_1} - \mathbf{z_2})$ we have,

$$\|\mathbf{z_1} - \mathbf{z_2}\| = \left(\sum_{i=1}^{m} (\mathbf{z_1} - \mathbf{z_2})^2\right)^{1/2} \leq \left(\sum_{i=1}^{m} (q)^2\right)^{1/2} \leq q \cdot \sqrt{m}$$

□

Often to prove the boundedness of the solution, authors tend to use the domain as $\{0, 1\}^m$ for which the analysis come up as

$$2^m > q^n \iff m > n \log q$$

$$\|\mathbf{z_1} - \mathbf{z_2}\| = \left(\sum_{i=1}^{m} (\mathbf{z_1} - \mathbf{z_2})^2\right)^{1/2} \leq \left(\sum_{i=1}^{m} (\pm 1)^2\right)^{1/2} \leq \sqrt{m}$$

3.1 SIS Lattice

The SIS lattice is defined as $\Lambda^\perp := \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{A} \cdot \mathbf{z} = \mathbf{0}\}$, and in its modular form , for a positive integer q it is defined as $\Lambda^\perp := \{\mathbf{z} \in \mathbb{Z}_q^m \mid \mathbf{A} \cdot \mathbf{z} = \mathbf{0} \pmod{q}\}$. $\mathbf{A}$ is often called the parity check matrix.

Claim 3.3. $\Lambda^\perp := \{\mathbf{z} \in \mathbb{Z}^m | \mathbf{A}\mathbf{z} = \mathbf{0}\}$ *is a lattice* **(we call it the SIS lattice).**

Proof. We have to show that $\Lambda^\perp$ is discrete and it is an additive group.

(i) $\Lambda^\perp$ is discrete:

$$\Lambda^\perp := \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{z} = \mathbf{0}\} \subseteq \mathbb{Z}^m$$

which is a subset of a discrete set $\mathbb{Z}^m$ so it is discrete.

(ii) $\Lambda^\perp$ is an additive group: Let $\mathbf{z_1}, \mathbf{z_2} \in \Lambda^\perp$ then we have

$$\mathbf{A}\mathbf{z_1} = \mathbf{0} \qquad \text{and} \qquad \mathbf{A}\mathbf{z_2} = \mathbf{0}$$

Then we have,

$$\mathbf{A}\mathbf{z_1} - \mathbf{A}\mathbf{z_2} = \mathbf{A} \cdot (\mathbf{z_1} - \mathbf{z_2}) = \mathbf{0}$$

Thus, $\mathbf{z_1} - \mathbf{z_2} \in \Lambda^\perp$.
This completes the proof.

□

Since, the SIS lattice $\Lambda^{\perp}(\mathbf{A})$ contains all the solutions of $\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \pmod{q}$, we say that a solution to SVP in $\Lambda^{\perp}(\mathbf{A})$ lattice is a solution to $\text{SIS}_{n,m,q,\beta}$ problem.

3.2 Basis of the SIS Lattice

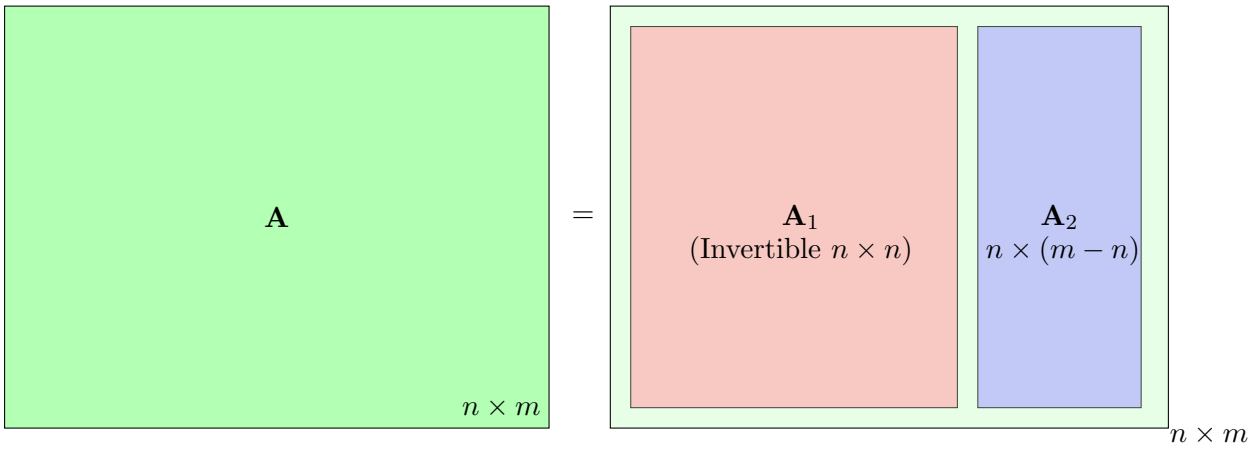
Next natural question to ask here is, how are we going to characterize the SIS lattice? In particular, what is the basis of the lattice? we try to answer this question here[1].
Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ be of rank n where $m \geq n$, then the SIS lattice is defined as,

$$\Lambda^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{A} \cdot \mathbf{x} = \mathbf{0}\}$$

$\mathbf{A}$ is now a matrix of dimension $n \times m$, which we can block decompose as

$$\mathbf{A} = [\mathbf{A}_1 \mid \mathbf{A}_2]_{n \times m}$$

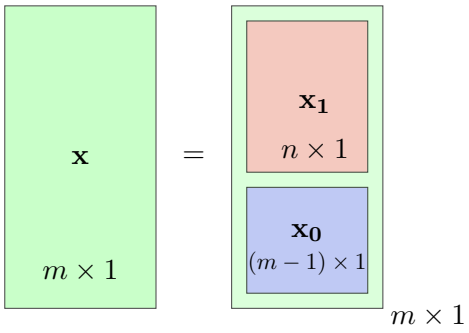
where $\mathbf{A}_1$ is of size $n \times n$ and is invertible, and $\mathbf{A}_2$ is of size $n \times (m - n)$



Similarly, we can also decompose $\mathbf{x}$ of size $m \times 1$ as,

$$\mathbf{x}_{m \times 1} = \begin{bmatrix} \mathbf{x_1} \\ \mathbf{x_2} \end{bmatrix}_{m \times 1}$$

where $\mathbf{x}_1$ is of size $n \times 1$ and $\mathbf{x}_2$ is of size $(m - n) \times 1$



[1]Thanks to **Arup Mazumder** for his insights to this sub-topic, browse his notes here

We begin with

$$\mathbf{A}_{n\times m}\cdot\mathbf{x}_{m\times 1} = [(\mathbf{A}_1)_{n\times n} \mid (\mathbf{A}_2)_{n\times(m-n)}]_{n\times m}\begin{bmatrix}(\mathbf{x_1})_{n\times 1}\\(\mathbf{x_2})_{(m-n)\times 1}\end{bmatrix}_{m\times 1} = \mathbf{A}_1\cdot\mathbf{x}_1+\mathbf{A}_2\cdot\mathbf{x}_2 = \mathbf{0}_{n\times 1} \pmod q$$

Now multiplying both sides by $\mathbf{A}_1^{-1}$ we obtain ($\mathbf{A}_1^{-1}$ is of size $n \times n$)

$$\mathbf{A}_1^{-1}\cdot(\mathbf{A}_1\cdot\mathbf{x}_1+\mathbf{A}_2\cdot\mathbf{x}_2) = \mathbf{A}_1^{-1}\cdot\mathbf{0}_{n\times 1} \pmod q$$

or,

$$\mathbf{I}_{n\times n}\cdot\mathbf{x}_1+\mathbf{A}_1^{-1}\cdot\mathbf{A}_2\cdot\mathbf{x}_2 = \mathbf{0}_{n\times 1} \pmod q$$

or,

$$\mathbf{x}_1 = -\underbrace{(\mathbf{A}_1^{-1})_{n\times n}\cdot(\mathbf{A}_2)_{n\times(m-n)}}_{n\times(m-n)}\cdot(\mathbf{x_2})_{(m-n)\times 1} \pmod q = -\underbrace{\mathbf{A}_1^{-1}\cdot\mathbf{A}_2\cdot\mathbf{x}_2}_{n\times 1}+(q\mathbf{u})_{n\times 1}$$

Thus, any lattice point $\mathbf{x}\in\Lambda^{\perp}$ can now be expressed as,

$$\mathbf{x} = \begin{bmatrix}\mathbf{x}_1\\\mathbf{x}_2\end{bmatrix} = \begin{bmatrix}-\mathbf{A}_1^{-1}\cdot\mathbf{A}_2\cdot\mathbf{x}_2+q\mathbf{u}\\\mathbf{x}_2\end{bmatrix}$$

where, $\mathbf{u}\in\mathbb{Z}^n, \mathbf{x}_2\in\mathbb{Z}^{m-n}$
Now the next step is constructing a basis from this, and to do this we would separate the contributions of the two free integer vectors $\mathbf{u}$ and $\mathbf{x}_2$ as,

$$\begin{aligned}\mathbf{x} = \begin{bmatrix}(\mathbf{x_1})_{n\times 1}\\(\mathbf{x_2})_{(m-n)\times 1}\end{bmatrix} &= \begin{bmatrix}-\mathbf{A}_1^{-1}\cdot\mathbf{A}_2\cdot\mathbf{x}_2+q\mathbf{u}\\(\mathbf{x}_2)_{(m-n)\times 1}\end{bmatrix}\\ &= \begin{bmatrix}q\mathbf{u}-\mathbf{A}_1^{-1}\cdot\mathbf{A}_2\cdot\mathbf{x}_2\\\mathbf{0}+\mathbf{x}_2\end{bmatrix}\\ &= \begin{bmatrix}q\mathbf{I}_{n\times n} & -(\mathbf{A}_1^{-1}\cdot\mathbf{A}_2)_{n\times(m-n)}\\\mathbf{0}_{(m-n)\times n} & \mathbf{I}_{(m-n)\times(m-n)}\end{bmatrix}\begin{bmatrix}\mathbf{u}\\\mathbf{x}_2\end{bmatrix}\end{aligned}$$

Combining both parts, a full basis matrix for the lattice $\Lambda^{\perp}(A)$ is

$$\boxed{B = \begin{bmatrix}q\mathbf{I}_{n\times n} & -\mathbf{A}_1^{-1}\mathbf{A}_2\\\mathbf{0}_{(m-n)\times n} & \mathbf{I}_{m-n}\end{bmatrix}}$$

This is an $m\times m$ integer matrix whose columns form a basis of the SIS lattice.

- The first n basis vectors $q\cdot\mathbf{e_i}$ correspond to trivial solutions, since adding multiples of q does not change the value of $\mathbf{A}\cdot\mathbf{x} \pmod q$.
- The remaining $m-n$ vectors describe the true integer kernel of $\mathbf{A}$.

Thus, the SIS lattice is fully characterized by the basis B.

Result 3.4. *The basis matrix for the SIS lattice $\Lambda^{\perp}(\mathbf{A})$ is*

$$B = \begin{bmatrix}q\mathbf{I}_{n\times n} & -\mathbf{A}_1^{-1}\mathbf{A}_2\\\mathbf{0} & \mathbf{I}_{m-n}\end{bmatrix}$$

So, we can write $\Lambda^{\perp}(\mathbf{A}) = \mathcal{L}(B)$

Lemma 3.5. $\det(\Lambda^{\perp}) = q^n$

Proof.

$$\det(\Lambda^{\perp}(\mathbf{A})) = \begin{vmatrix} q\mathbf{I}_{n\times n} & -\mathbf{A}_1^{-1}\mathbf{A}_2 \\ \mathbf{0} & \mathbf{I}_{m-n} \end{vmatrix} = q^n$$

□

Lemma 3.6. $\lambda_1(\Lambda^{\perp}) \leq \sqrt{m} \cdot q^{n/m}$

Proof. By applying the minkowski's bound we get,

$$\lambda_1(\Lambda^{\perp}) \leq \sqrt{m} \cdot (\det(\Lambda^{\perp}))^{1/m} \leq \sqrt{m} \cdot q^{n/m}$$

□

Lemma 3.7. *For an invertible matrix* $H_{n\times n}$

$$\Lambda^{\perp}(\mathbf{HA}) = \Lambda^{\perp}(\mathbf{A})$$

Proof. □

Proof. Let $\mathbf{z} \in \Lambda^{\perp}(\mathbf{HA})$

$$\begin{aligned}
&\iff \mathbf{H}_{n\times n} \cdot \mathbf{A}_{n\times m} \cdot \mathbf{z}_{m\times 1} = \mathbf{0}_{n\times 1} \\
&\iff \mathbf{H}^{-1}_{n\times n} \cdot \mathbf{H}_{n\times n} \cdot \mathbf{A}_{n\times m} \cdot \mathbf{z}_{m\times 1} = \mathbf{H}^{-1}_{n\times n} \cdot \mathbf{0}_{n\times 1} \\
&\iff I_{n\times n} \cdot \mathbf{A}_{n\times m} \cdot \mathbf{z}_{m\times 1} = \mathbf{0}_{n\times 1} \\
&\iff \mathbf{A}_{n\times m} \cdot \mathbf{z}_{m\times 1} = \mathbf{0}_{n\times 1} \\
&\iff \mathbf{z}_{m\times 1} \in \Lambda^{\perp}(\mathbf{A})
\end{aligned}$$

□

Definition 3.8. **($q-$ary Lattice)**
A lattice Λ *is called* $q-$*ary lattice of dimension* n *if it satisfies*

$$q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$$

Claim 3.9. $\Lambda^{\perp}(\mathbf{A})$ *is a* $q-$*ary lattice of dimension* m*.*

Proof. Since, all elements $\mathbf{x} \in q\mathbb{Z}^m$ would serve as solution to $\mathbf{A}\cdot\mathbf{x} = 0 \pmod q$ the containment $q\mathbb{Z}^m \subseteq \Lambda^{\perp}$ is justified. Moreover, as we ask for integer solutions only, yhe later containment $\Lambda^{\perp} \subseteq \mathbb{Z}^m$ is also justified.
Finally,

$$q\mathbb{Z}^m \subseteq \Lambda^{\perp} \subseteq \mathbb{Z}^m$$

□

Definition 3.10. **(Coset)**
Let $\mathbf{x} \in \mathbb{Z}_q^m$ *such that* $\mathbf{A} \cdot \mathbf{x} = \mathbf{y}$*, then define,*

$$\mathcal{L}^{\perp}_{\mathbf{y}}(\mathbf{A}) = \{\mathbf{x}' \in \mathbb{Z}^m \mid \mathbf{A} \cdot \mathbf{x}' = \mathbf{y}\} = \mathbf{x} + \Lambda^{\perp}(\mathbf{A})$$

Definition 3.11. **(Row-Generated Lattice)**
Let $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ *then define,*

$$\Lambda_q(\mathbf{A}) = \{\mathbf{y}' \in \mathbb{Z}^m \mid \mathbf{y} = \mathbf{A} \cdot \mathbf{y} \pmod q, \text{ for some } s \in \mathbb{Z}^n\} = \mathbf{A}\mathbb{Z}^n + q\mathbb{Z}^m$$

4 Applications of SIS

Definition 4.1. **(Hash Function & Family)**
A function $f : \mathcal{D} \to \mathcal{R}$ is a called a hash function, where $|\mathcal{R}| < |\mathcal{D}|$. A collection of such functions is called a hash function family

$$\mathcal{F} = \{H_a : \mathcal{D} \to \mathcal{R} \mid a \in \mathbb{N}\}$$

By definition, we have $|\mathcal{D}| > |\mathcal{R}|$ so we must be able to find at least one distinct pair $x_1, x_2 \in \mathcal{D}$ such that $f(x_1) = f(x_2)$. Such a pair is called a collision pair. A family of hash function is said to be collision resistant if for any $f_a \in \mathcal{H}$, it is infeasible for an adversary $\mathcal{A}$ to find a collision pair.

$$\Pr[\mathcal{A} \text{ finds a collision in } f] \leq negl(a)$$

4.1 Collision Resistant Hashing from SIS

For a fixed value of n, let $q = n^2$ and $m > n\log(q)$

- Define key space $\mathcal{K} = \mathbb{Z}_q^{n \times m}$
- $\mathcal{D} = \{0,1\}^m$
- $\mathcal{R} = \mathbb{Z}_q^n$

Construct a keyed hash function $f : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ as

$$f(\mathbf{A}, \mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \pmod{p}$$

Compression

$$|\mathcal{D}| = 2^m$$
$$|\mathcal{R}| = q^n$$

if $|\mathcal{R}| < |\mathcal{D}|$ then $q^n < 2^m$ or $n \cdot \log(q) < m$
Collision Resistant
Let there be $\mathbf{x_1}$ and corresponding to this we find another point $\mathbf{x_2}$ such that $f(\mathbf{A}, \mathbf{x_1}) = f(\mathbf{A}, \mathbf{x_2})$.

$$\begin{aligned} & f(\mathbf{A}, \mathbf{x_1}) = f(\mathbf{A}, \mathbf{x_2}) \\ \implies & f(\mathbf{A}, \mathbf{x_1}) - f(\mathbf{A}, \mathbf{x_2}) = 0 \\ \implies & \mathbf{A} \cdot \mathbf{x_1} - \mathbf{A} \cdot \mathbf{x_2} = 0 \\ \implies & \mathbf{A} \cdot (\mathbf{x_1} - \mathbf{x_2}) = 0 \end{aligned}$$

We see that the SIS problem is solved, where the short vector is $\mathbf{x} = \mathbf{x_1} - \mathbf{x_2} \in \{-1, 0, 1\}^m$ with $\|\mathbf{x_1} - \mathbf{x_2}\| \leq \sqrt{m}$. So finding a collision over here is as hard as solving the SIS problem, which is conjectured to be a hard problem.

Result 4.2. *If* SIS *is hard for security parameter $n = \lambda$, $q \geq 2, m > n\log_2 q$ and $\beta = \sqrt{m}$, then we have a family of collision resistant hash function*

$$\mathcal{F} = \{f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n | \mathbf{A} \in \mathbb{Z}_q^{n \times m}\}$$

where, $H_{\mathbf{A}}(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \pmod{q}$

We would call this SIS hash family.

4.2 One-Way Function Family

Definition 4.3. **($\varepsilon-$regular Family)**
A function family $\mathcal{F} = \{f_a : \mathcal{D} \to \mathcal{R}\}$ is ε regular if

$$(f, f(x)) \approx_\varepsilon (f, y)$$

where $f \leftarrow \mathcal{F}, x \leftarrow \mathcal{D}, y \leftarrow \mathcal{R}$ and $\approx_\varepsilon$ denotes that the statistical distance between the two distributions is atmost ε.

Definition 4.4. **(One Way Function)**
A family of hash function $\mathcal{F}_\lambda = \{f_a : \mathcal{D}_\lambda \to \mathcal{R}_\lambda\}$ is one way if for all PPT adversary $\mathcal{A}$ we have,

$$\Pr_{x \leftarrow \mathcal{D}_\lambda, y \leftarrow \mathcal{R}_\lambda}[\mathcal{A}(f_a, y) = x \text{ such that } f_a(x) = y] = negl(\lambda)$$

Definition 4.5. **(Universal Hash Function)**
A hash function family $\mathcal{F} = \{f_a : \mathcal{D} \to \mathcal{R}\}$ is universal if for any two distinct elements $x_1, x_2 \in \mathcal{D}$, we have

$$\Pr[f_a(x_1) = f_a(x_2)] = \frac{1}{|\mathcal{R}|}$$

Lemma 4.6. *The* SIS *hash family with domain $\mathcal{D} = \{0,1\}^n$ is universal, $\varepsilon-$regular, one way.*

Definition 4.7. **(Guessing Probability)**
Let $\mathcal{D}$ be a finite set and $\mathcal{D}_\mathcal{D}$ be some distribution on $\mathcal{D}$, then the guessing probability of $\mathcal{D}_\mathcal{D}$ is defined as,

$$\gamma = \max_{\mathbf{x}^* \in \mathcal{D}} \Pr_{\mathbf{x} \leftarrow \mathcal{D}_\mathcal{D}}[\mathbf{x}^* = \mathbf{x}]$$

Lemma 4.8. **(Leftover Hash Lemma)**
A univaersal hash family $\mathcal{F} = \{f_a : \mathcal{D} \to \mathcal{R}\}$ is $\varepsilon-$regular with $\varepsilon = \sqrt{|\mathcal{R}|/|\mathcal{D}|}$

5 Inhomogeneous SIS

Definition 5.1. **[Inhomogeneous SIS(ISIS)]** *For a positive integer modulus q, dimension n, m and a norm bound $\beta > 0$ the* $\text{InhomSIS}_{n,m,q,\beta}$ *problem is defined as, given uniformly random $\mathbf{A}$ and $\mathbf{b}$ find $\mathbf{z} \in [-\beta, \beta]^m$ such that $\mathbf{A} \cdot \mathbf{z} = \mathbf{b} \pmod q$.*

Theorem 5.2. $\text{InhomSIS}_{n,m,q,\beta}$ *and* $\text{SIS}_{n,m,q,\beta}$ *are computationally equivalent.*

Proof. Let $\mathbf{A}$ be an instance of $\text{SIS}_{n,m,q,\beta}$ and $(\mathbf{A}, \mathbf{b})$ be an instance of $\text{InhomSIS}_{n,m,q,\beta}$.

ISIS solver with SIS oracle ($\text{InhomSIS}_{n,m,q,\beta} \leq \text{SIS}_{n,m,q,\beta}$)

Input : $\mathbf{A} \in \mathbb{Z}^{n \times m}, \mathbf{b} \in \mathbb{Z}_q^n$, and norm bound β.
Result: $\mathbf{z}$ with $\mathbf{Az} = \mathbf{b} \pmod q$ and $\|\mathbf{z}\| \leq \beta$.

1 Pick $i \xleftarrow{\$} \{1, 2 \cdots, m+1\}$
2 Pick $c \xleftarrow{\$} [-\beta, \beta] - \{0\}$
3 Construct $\mathbf{A}'_{n \times (m+1)} = \begin{bmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \cdots & \mathbf{a}_{i-1} & -c^{-1}\mathbf{b} & \mathbf{a}_i & \cdots & \mathbf{a}_m \end{bmatrix}$
4 Query SIS for $\mathbf{A}'$ to get $\mathbf{z}' = \begin{bmatrix} z_1 & z_2 & \cdots & z_{i-1} & z^* & z_i & \cdots & z_m \end{bmatrix}^T$
5 Check if $z^* = c$ else restart
6 **return** $\mathbf{z} = \begin{bmatrix} z_1 & z_2 & \cdots & z_{i-1} & z_i & \cdots & z_m \end{bmatrix}^T$

SIS solver with ISIS oracle ($\text{SIS}_{n,m,q,\beta} \leq \text{InhomSIS}_{n,m,q,\beta}$)

Input : $\mathbf{A} \in \mathbb{Z}^{n \times m}$, and norm bound β.
Result: $\mathbf{z}$ with $\mathbf{Az} = 0 \pmod q$ and $\|\mathbf{z}\| \leq \beta$.

1 Choose short $\mathbf{z}_1$
2 Let $\mathbf{y} = \mathbf{Az}_1$
3 Query ISIS for $(\mathbf{A}, \mathbf{y})$ to get $\mathbf{z}_2$
4 **return** $(\mathbf{z}_1 - \mathbf{z}_2)$

□

Definition 5.3. [Module SIS(MSIS)] *For a positive integer modulus q with n, dimension k, ℓ and a norm bound $\beta > 0$ the* $\text{MSIS}_{n,m,k,l,q,\beta}$ *problem is defined as, given uniformly random* $\mathbf{A} \xleftarrow{\$} R_q^{k \times \ell}$ *find* $\mathbf{z} \in R_q^{\ell}$ *such that* $\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \pmod q$ *with* $\|\mathbf{z}\|_\infty \leq \beta$.

Definition 5.4. [Normal Form SIS(nfSIS)] *For a positive integer modulus q with n, dimension k, ℓ and a norm bound $\beta > 0$ the* $\text{MSIS}_{n,m,k,l,q,\beta}$ *problem is defined as, given uniformly random* $\mathbf{A} \xleftarrow{\$} R_q^{k \times \ell}$ *find* $\mathbf{z} \in R_q^{\ell}$ *such that* $\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \pmod q$ *with* $\|\mathbf{z}\|_\infty \leq \beta$.

Some bullet points

- RSA function
  Let $N = p \times q$ where p, q are large radnom primes and e be a randomly chosen number which is coprime to $\phi(N) = (p-1) \times (q-1)$. Now for the function $\text{RSA}_{p,q,e}(x) = xe \pmod N$ is a one way function.
- Rabin function
  Let N be a composite number and define $f_N(x) = x^2 \pmod N$. Inverting f_N in $1/poly(\log N)$ time provides factorization of N in $poly(\log N)$ time.
- In public key cryptography both the RSA and Rabin problem are useful. Using them one can design trap door i.e some extra information to invert the function efficiently, which can be kept secret.

Theorem 5.5. *If there exists an algorithm that solves γ-approximate* SVP *on m-dimensional lattices, then one can solve the* $\text{SIS}_{n,m,q,\beta}$ *problem for any* $\beta \geq \gamma \cdot \sqrt{m}\, q^{n/m}$.

$$\text{SIS}_{n,m,q,\beta} \leq_p \text{SVP}_\gamma$$

$$\text{SIS}_{n,m,q,\beta} \xrightarrow{\textit{reduces to}} \text{SVP}_\gamma$$

or,

$$\text{SVP}_\gamma \ \textit{is atleast as hard as} \ \text{SIS}_{n,m,q,\beta}$$

Being able to solve SVP_γ *implies we can also solve* $\text{SIS}_{n,m,q,\beta}$

Proof. Assume that we have an **oracle access to** SVP_γ. On input of lattice basis B it outputs a lattice vector $\mathbf{v} \neq \mathbf{0}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L}(B))$.
We have the SIS lattice

$$\Lambda^\perp(\mathbf{A}) := \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{A}_{n \times m}\mathbf{z}_{m \times 1} = \mathbf{0}_{n \times 1} \pmod q\}$$

This is a rank n lattice with dimension m and determinant

$$\det(\Lambda^\perp(\mathbf{A})) = q^n$$

By Minkowski's First Theorem,

$$\lambda_1(\Lambda^\perp(\mathbf{A})) \leq \sqrt{m}\det(\Lambda^\perp(\mathbf{A}))^{1/m} = \sqrt{m}q^{n/m} \tag{1}$$

Apply the SVP_γ **oracle** to the lattice to obtain non-zero $\mathbf{z} \in \Lambda^\perp(\mathbf{A})$ with

$$\|\mathbf{z}\| \leq \gamma \cdot \lambda_1(\Lambda^\perp(\mathbf{A})) \tag{2}$$

using (1) and (2) we conclude

$$\|\mathbf{z}\| \leq \gamma \cdot \lambda_1(\Lambda^\perp(\mathbf{A})) \leq \gamma \cdot \sqrt{m}q^{n/m}$$

Setting $\beta = \gamma \cdot \sqrt{m}q^{n/m}$, we obtain

$$\|\mathbf{z}\| \leq \gamma \cdot \lambda_1(\Lambda^\perp(\mathbf{A})) \leq \beta$$

Finally, we get

$$A\mathbf{z} = 0 \pmod{q} \quad \text{and} \quad \|\mathbf{z}\| \leq \beta$$

which is a valid solution to the $\mathrm{SIS}_{n,m,q,\beta}$ problem. □

References

[Maz25] Arup Mazumder. *Primal Attack on LWE*. Sept. 2025. URL: https://arupmazumder.github.io/Primal%20Attack%20on%20LWE.pdf.

[MR07] Daniele Micciancio and Oded Regev. "Worst-Case to Average-Case Reductions Based on Gaussian Measures". In: *SIAM Journal on Computing* 37.1 (Jan. 2007), pp. 267–302. ISSN: 1095-7111. DOI: 10.1137/s0097539705447360. URL: http://dx.doi.org/10.1137/S0097539705447360.

[Pei22] Chris Peikert. *Worst to Average Case Reduction*. Lattices in Cryptography. Lecture 11, Scribed by Abhishek Banarjee. Fall 2022.

[Rib23] João Ribeiro. *Codes and Lattices in Cryptography: Mini-Course FCT-UNL, Spring 2023*. 2023. URL: https://sites.google.com/site/joaorib94/codes-lattices-in-crypto?authuser=0.