

# Post Quantum Cryptography

## Lattice Based Cryptography

Shashank Singh

IISER Bhopal

November 17, 2025

SYSTEM OF  $m$  LINEAR EQUATIONS WITH  $n$  VARIABLES

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = t_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = t_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = t_m \end{cases} \pmod{q}$$

# SYSTEM OF $m$ LINEAR EQUATIONS WITH $n$ VARIABLES

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = t_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = t_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = t_m \end{cases} \quad (\text{mod } q)$$

We can write it in the matrix form as follows.

$$\underbrace{\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}}_{\mathbf{A}} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{\mathbf{x}} = \underbrace{\begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_m \end{pmatrix}}_{\mathbf{t}} \quad (\text{mod } q)$$

## (IN)-HOMOGENEOUS SYSTEM OF EQUATION

- We use  $\mathbb{Z}_q$  to denote  $\mathbb{Z}/q\mathbb{Z}$  and use the notation  $a \in_R A$  to mean that  $a$  is chosen randomly from  $A$ .
- Vectors are always treated as column vectors and they are denoted by small letter bold font.
- Capital bold letter will represent a matrix and  $\mathbf{A}^T$  will be used to present the transpose of matrix  $\mathbf{A}$ .

$$\mathbf{Ax} = \mathbf{t} \pmod{q}, \text{ where } \mathbf{A} \in \mathbb{Z}_q^{m \times n} \quad (1)$$

- If  $\mathbf{t} = \mathbf{0}$ , the system in Eq. (1) is called a homogeneous system of linear equations. For  $\mathbf{t} \neq \mathbf{0}$ , it is termed as inhomogeneous system of linear equations.

# SHORTEST INTEGER SOLUTION PROBLEM

## Definition 0.1

Given  $n, m, q, \beta \in \mathbb{Z}_{>0}$  and

$$\mathbf{A}^T := \begin{bmatrix} | & | & & | \\ \mathbf{a}_1 & \mathbf{a}_2 & \dots & \mathbf{a}_m \\ | & | & & | \end{bmatrix} \leftarrow \mathsf{U}(\mathbb{Z}_q^{n \times m}), \quad (2)$$

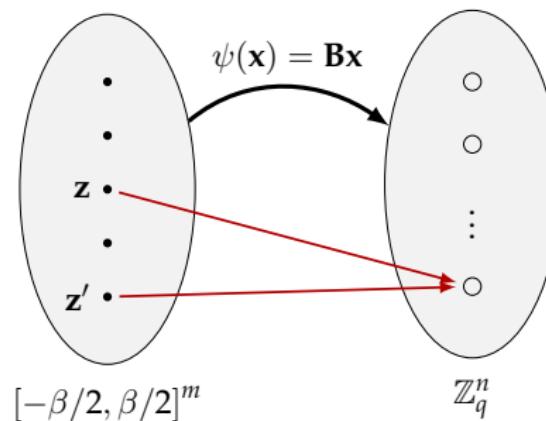
where  $m > n$ ,  $q = \text{poly}(n)$  and  $\beta \ll q/2$ . Find a nonzero vector  $\mathbf{z} \in \mathbb{Z}^m$  with  $\mathbf{z} \in [-\beta, \beta]^m$  such that

$$\mathbf{A}^T \mathbf{z} \equiv \mathbf{0} \pmod{q}. \quad (3)$$

## Remark

1. In the above Definition 0.1, the use of  $\mathbf{A}^T$  is just for the notation convenience, which we leverage later. For simplicity we can use by  $\mathbf{B} := \mathbf{A}^T$ .
2. As the number of equations ( $n$ ) is less than the number of variables ( $m$ ), the system in Eq. (2) is under-determined system.
3. Although the SIS system has many solutions, but what is the guarantee of having such a small solution.
4. How is the SIS problem connected to lattice ?

## SIS ..



- Size of domain:  $(\beta + 1)^m$ ; size of co-domain:  $q^n$ .
- If  $(\beta + 1)^m > q^n$ , by Pigeonhole Principle, there exists  $\mathbf{z}_1, \mathbf{z}_2 \in [-\beta/2, \beta/2]^m$  with  $\mathbf{z}_1 \neq \mathbf{z}_2$  such that  $\mathbf{Bz}_1 = \mathbf{Bz}_2 \pmod{q}$ . Thus  $\mathbf{z} = \mathbf{z}_1 - \mathbf{z}_2$  is a SIS solution.
- The SIS problem does not have unique solution. -z

# INHOMOGENEOUS SIS PROBLEM (ISIS)

Definition 0.2

Given  $n, m, q, \beta \in \mathbb{Z}_{>0}$  and

$$\mathbf{A}^T := \begin{bmatrix} | & & | \\ \mathbf{a}_1 & \dots & \mathbf{a}_m \\ | & & | \end{bmatrix} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \mathbf{b} := \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \xleftarrow{\$} \mathbb{Z}_q^n, \quad (4)$$

where  $m > n$  and  $(2\beta + 1)^m \gg q^n$ . Find a nonzero vector  $\mathbf{z} \in \mathbb{Z}^m$  with  $\mathbf{z} \in [-\beta, \beta]^m$  such that  $\mathbf{A}^T \mathbf{z} \equiv \mathbf{b} \pmod{q}$ .

Remark

The condition  $(2\beta + 1)^m \gg q^n$  is required for a solution to likely exist.

# EQUIVALENCE OF SIS AND ISIS

## Theorem

The following statements hold.

- $\text{SIS} \leq \text{ISIS}$ .
- $\text{ISIS} \leq \text{SIS}$ .

# NORMAL-FORM ISIS (NF-ISIS)

Definition 0.3 (nf-ISIS<sub>n,m,q,β</sub>)

Given  $m, n, q, \beta, \mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$  and  $\mathbf{b} \xleftarrow{\$} \mathbb{Z}_q^n$ , find  $\mathbf{z} \in \mathbb{Z}_q^{m+n}$  such that  $[\mathbf{B} | \mathbf{I}_n] \mathbf{z} \equiv \mathbf{b} \pmod{q}$ .

Claim 1

nf-ISIS<sub>n,m,q,β</sub> and ISIS<sub>n,m+n,q,β</sub> are equivalent.

# SIS PROBLEM AND LATTICE

## Definition 0.4

- (i) A ***q*-ary lattice**  $\Lambda$  of dimension  $m$  is a lattice satisfying

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

- (ii) Let  $\mathbf{B} \in \mathbb{Z}^{n \times m}$ , we define a *q*-ary lattice  $\Lambda_q^\perp(\mathbf{B})$ , called the **kernel lattice of  $\mathbf{B}$** , as

$$\Lambda_q^\perp(\mathbf{B}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{B} \cdot \mathbf{x} = 0 \pmod{q}\}.$$

- (iii) We define a lattice called, **row lattice of  $\mathbf{B}$** , as

$$\Lambda_q(\mathbf{B}) = \left\{ \mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{B}^T \mathbf{s} \pmod{q}, \text{ for some } \mathbf{s} \in \mathbb{Z}^n \right\}.$$

# HARDNESS OF SIS

**Theorem 1.1 (Corollary of Theorem 3.8).** Let  $n$  and  $m = \text{poly}(n)$  be integers, let  $\beta \geq \beta_\infty \geq 1$  be reals, let  $Z = \{\mathbf{z} \in \mathbb{Z}^m : \|\mathbf{z}\|_2 \leq \beta \text{ and } \|\mathbf{z}\|_\infty \leq \beta_\infty\}$ , and let  $q \geq \beta \cdot n^\delta$  for some constant  $\delta > 0$ . Then solving (on the average, with non-negligible probability) SIS with parameters  $n, m, q$  and solution set  $Z \setminus \{\mathbf{0}\}$  is at least as hard as approximating lattice problems in the worst case on  $n$ -dimensional lattices to within  $\gamma = \max\{1, \beta \cdot \beta_\infty/q\} \cdot \tilde{O}(\beta\sqrt{n})$  factors.

1

## Remark

For  $m > n \log q$ , the function  $f_{\mathbf{B}} : \{0, 1\}^m \mapsto \mathbb{Z}_q^n$  defined as  $f_{\mathbf{B}}(\mathbf{x}) := \mathbf{Bx} \pmod{q}$  is a **collision resistant** hash function.

---

<sup>1</sup><https://web.eecs.umich.edu/~cpeikert/pubs/LWe.pdf>

# LWE PROBLEM

Given a system, for example,

$$\left. \begin{array}{l} 14s_1 + 15s_2 + 5s_3 + 2s_4 \approx 8 \pmod{17} \\ 13s_1 + 14s_2 + 14s_3 + 6s_4 \approx 16 \pmod{17} \\ 6s_1 + 10s_2 + 13s_3 + 1s_4 \approx 3 \pmod{17} \\ 10s_1 + 4s_2 + 12s_3 + 16s_4 \approx 12 \pmod{17} \\ 9s_1 + 5s_2 + 9s_3 + 6s_4 \approx 9 \pmod{17} \\ 3s_1 + 6s_2 + 4s_3 + 5s_4 \approx 16 \pmod{17} \\ \vdots \\ 6s_1 + 7s_2 + 16s_3 + 2s_4 \approx 3 \pmod{17} \end{array} \right\}, \quad (5)$$

where the approximation error is random and small in size, we look for a solution, i.e.  $\mathbf{s} = (s_1, s_2, s_3, s_4)^T$  satisfying above.

## LWE PROBLEM..

- If the System 5 has no solution, it is of no use.
  - So we generate such a system starting from a solution, i.e. from a fixed value of  $\mathbf{s} = (s_1, s_2, s_3, s_4)^T$ , and pick the coefficients randomly and complete the LHS of Eq. (5) and add a small random error to the value of the RHS.
  - Irrespective of the number of equations in such a system, a solution is always guaranteed, because we construct the system using a solution.

## LWE PROBLEM..

We can convert the System (5) into the following exact system by introducing the error variables.

$$\left. \begin{array}{l} 14s_1 + 15s_2 + 5s_3 + 2s_4 + e_1 = 8 \pmod{17} \\ 13s_1 + 14s_2 + 14s_3 + 6s_4 + e_2 = 16 \pmod{17} \\ 6s_1 + 10s_2 + 13s_3 + 1s_4 + e_3 = 3 \pmod{17} \\ 10s_1 + 4s_2 + 12s_3 + 16s_4 + e_4 = 12 \pmod{17} \\ 9s_1 + 5s_2 + 9s_3 + 6s_4 + e_5 = 9 \pmod{17} \\ 3s_1 + 6s_2 + 4s_3 + 5s_4 + e_6 = 16 \pmod{17} \\ \vdots \\ 6s_1 + 7s_2 + 16s_3 + 2s_4 + e_7 = 3 \pmod{17} \end{array} \right\} \quad (6)$$

## LWE PROBLEM..

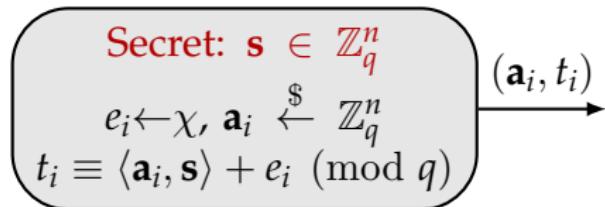
We can formally write the above system in the matrix form as follow:

$$\mathbf{A}\mathbf{s} + \mathbf{e} = \mathbf{b} \pmod{q}, \text{ where } \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}, \mathbf{e} \xleftarrow{\chi} \mathbb{Z}_q^n, \mathbf{s} \in \mathbb{Z}_q^n. \quad (7)$$

- Given  $(\mathbf{A}, \mathbf{b}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$ , satisfying Eq. (7), the LWE problem is to find the secret  $\mathbf{s}$ .

## LWE PROBLEM..

- The LWE instance is generated using a LWE-sampler, which on input  $\mathbf{s}$ , picks a random vector  $\mathbf{a}_i$  from  $\mathbb{Z}_q^n$  and samples an error  $e_i$  for the distribution  $\chi$  and outputs  $(\mathbf{a}_i, b_i := \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i)$ .



- We run the LWE-sampler and collect  $m$  LWE-samples and set

$$\mathbf{A} := \begin{bmatrix} \text{---} & \mathbf{a}_1 & \text{---} \\ \text{---} & \mathbf{a}_2 & \text{---} \\ \vdots & \vdots & \vdots \\ \text{---} & \mathbf{a}_m & \text{---} \end{bmatrix}, \mathbf{b} := \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}, \mathbf{e} := \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}. \quad (8)$$

# LWE PARAMETERS

$$\mathbf{A}\mathbf{s} + \mathbf{e} = \mathbf{b} \pmod{q}, \text{ where } \mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}, \mathbf{e} \leftarrow \chi, \mathbf{s} \in \mathbb{Z}_q^n.$$

- The notation  $(n, q, \chi)$ -LWE is used to mean a computational LWE with following parameters  $n, q$  and  $\chi$ , where
  - $n$  represent the length of secret vector. It is called LWE dimension.
  - $q \in \text{poly}(n)$  is called LWE modulus.
  - $\chi$  is a probability distribution. The errors (noise), i.e.  $\mathbf{e}$ , are sampled from  $\chi$ .
- We write  $(n, q, \alpha)$ -LWE to mean  $(n, q, D_{\alpha q})$ -LWE, where  $D_{\alpha q}$  is discrete gaussian distribution with standard deviation  $\alpha q$ . The error parameter  $\alpha$  is typically  $1/\text{poly}(n)$  and  $\alpha q > \sqrt{n}$ .
- The number of samples(LWE-equations), i.e.  $m$ , is usually not very important. It does not affect much the hardness of LWE.

# MATRIX LWE (MULTI-SECRET EXTENSION OF LWE)

- Similar to the matrix-SIS problem, the matrix-LWE problem replaces secret vector of LWE with a **secret matrix**. Each column of secret matrix correspond to the classical LWE secret.
- For a fixed secret matrix  $\mathbf{S} \in_{\phi} \mathbb{Z}_q^{n \times k}$ ,  $\mathbf{A} \in_U \mathbb{Z}_q^{m \times n}$  and error matrix  $\mathbf{E} \in_{\chi} \mathbb{Z}_q^{m \times k}$ , we compute

$$\mathbf{T} = \mathbf{AS} + \mathbf{E} \pmod{q}.$$

The matrix-LWE problem is to find  $(\mathbf{S}, \mathbf{E})$ , given  $(\mathbf{A}, \mathbf{T})$ .

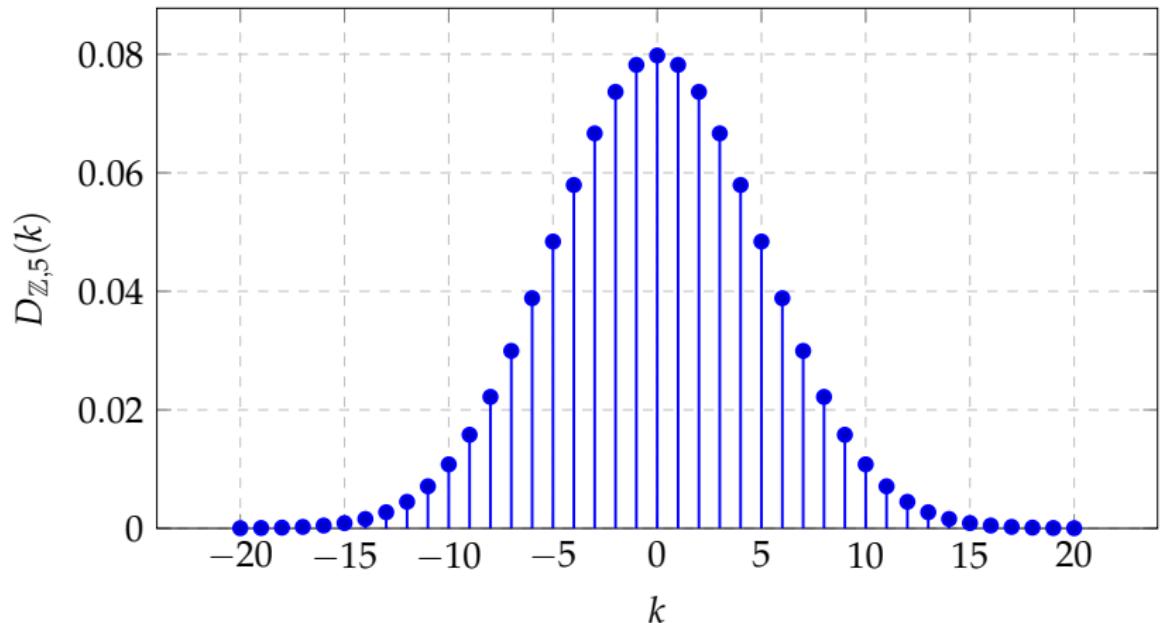
- The decision version of matrix-LWE problem is to distinguish  $(\mathbf{A}, \mathbf{AS} + \mathbf{E})$  from  $(\mathbf{A}, \mathbf{R})$ , where  $\mathbf{R} \in_U \mathbb{Z}_q^{m \times k}$ .

# MATRIX LWE (MULTI-SECRET EXTENSION OF LWE)..

Let

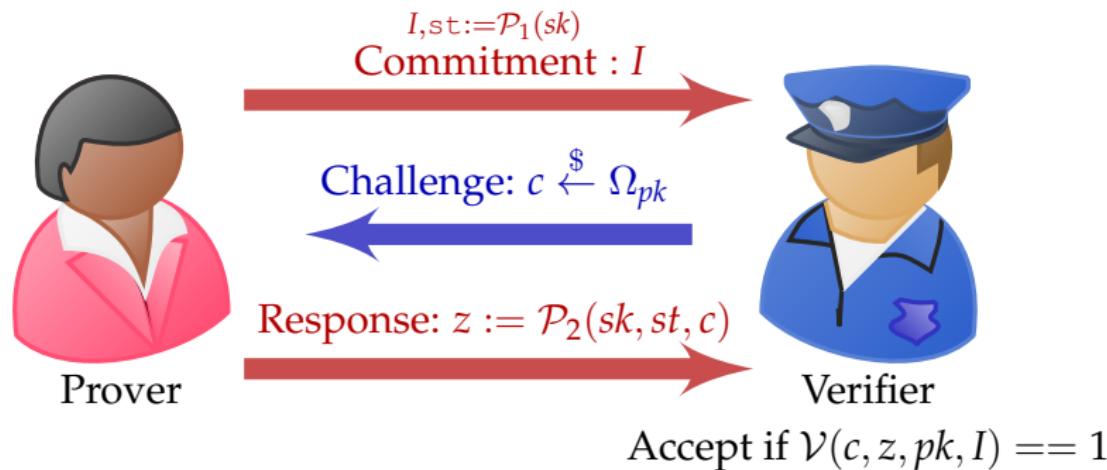
$$\mathbf{S} = \begin{bmatrix} | & | & & | \\ \mathbf{s}_1 & \mathbf{s}_2 & \dots & \mathbf{s}_k \\ | & | & & | \end{bmatrix} \text{ and } \mathbf{E} = \begin{bmatrix} | & | & & | \\ \mathbf{e}_1 & \mathbf{e}_2 & \dots & \mathbf{e}_k \\ | & | & & | \end{bmatrix}$$

- The matrix-LWE problem can be treated as  $k$  parallel LWE instances  $(\mathbf{A}, \mathbf{As}_i + \mathbf{e}_i)$ , with a shared coefficient matrix  $\mathbf{A}$ .
- $\text{LWE} \leq \text{Matrix-LWE}$  i.e., matrix-LWE problem is at least as hard as ordinary LWE problem.

Discrete Gaussian  $D_{\mathbb{Z},5}$  (normalized over  $k = -20 \dots 20$ )

# FORMAL DEFINITION OF ID PROTOCOL

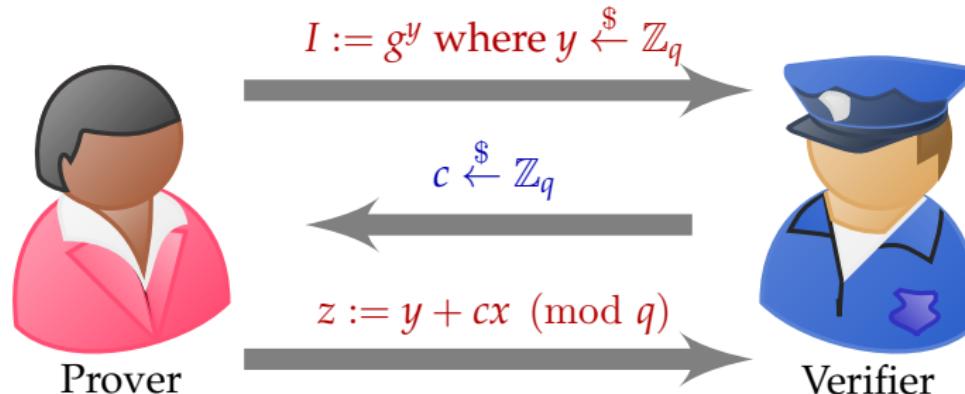
Formally an ID protocol  $\Pi$  is a collection of PPT algorithms  $(\mathbf{KeyGen}, \mathcal{P}, \mathcal{V})$ , where  $\mathcal{P} = (\mathcal{P}_1, \mathcal{P}_2)$ .



# THE SCHNORR IDENTIFICATION SCHEME

Let  $(G, \cdot) = \langle g \rangle$  be a cyclic group of order  $q$ . It is known that the discrete logarithm problem in  $G$  is computationally hard.

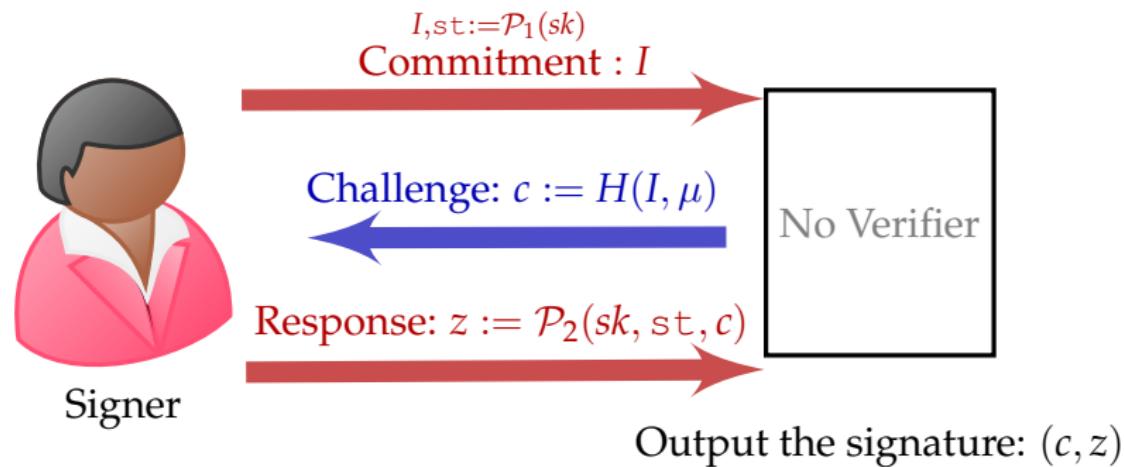
$$sk := x, \quad pk := g^x \text{ where } x \xleftarrow{\$} \mathbb{Z}_q$$



Accept if  $g^z \cdot pk^{-c} \stackrel{?}{=} I$

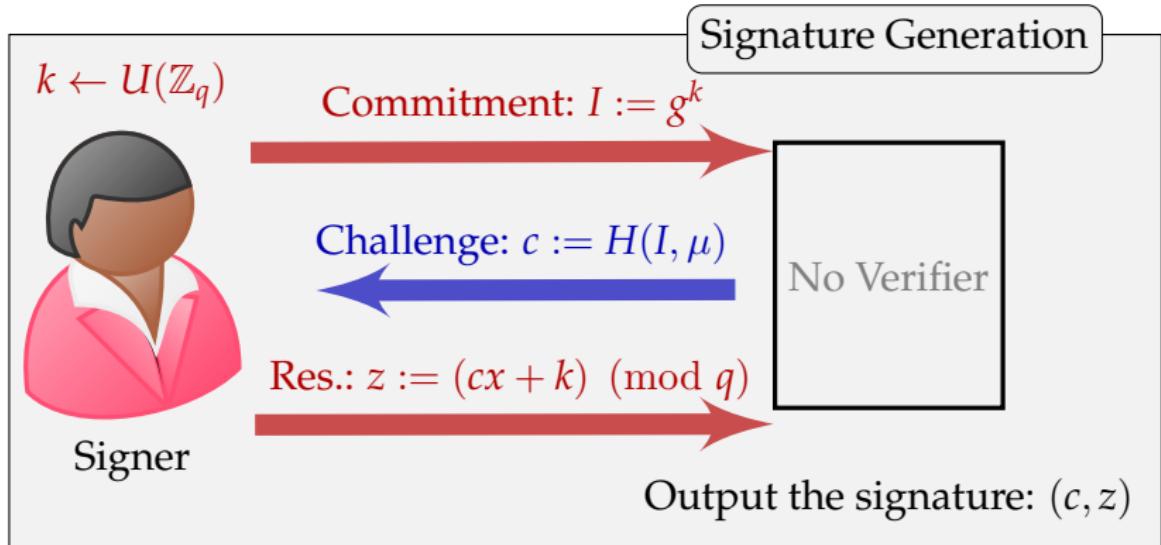
# FIAT-SHAMIR TRANSFORM

CONSTRUCTION OF SIGNATURE FROM ID SCHEME



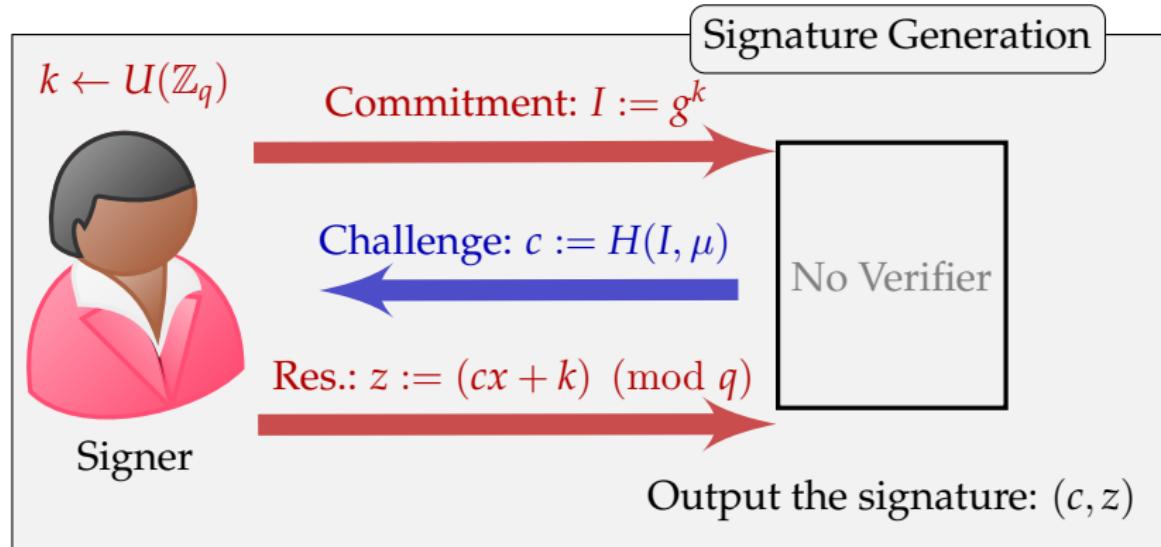
# SCHNORR SIGNATURE SCHEME

$(G, \cdot) = \langle g \rangle, |G| = q, sk := x \leftarrow U(\mathbb{Z}_q)$  and  $pk := g^x$



# SCHNORR SIGNATURE SCHEME

$(G, \cdot) = \langle g \rangle, |G| = q, sk := x \leftarrow U(\mathbb{Z}_q)$  and  $pk := g^x$



Verification

$$H(g^z \cdot (pk)^{-c}, \mu) \stackrel{?}{=} c$$

# A SIS BASED DIGITAL SIGNATURE ALGORITHM

## Algorithm 1 — **KeyGen**( $n, m, k, q$ )

**Input:**  $n, m, k, q$

**Output:**  $sk, pk$

1  $\mathbf{S} \xleftarrow{\$} \{-1, 0, 1\}^{m \times k}$

2  $\mathbf{A}^T \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \mathbf{T} = \mathbf{A}^T \cdot \mathbf{S} \pmod{q}$

3 **return**  $sk := \mathbf{S}$  and  $pk := (\mathbf{A}^T, \mathbf{T})$

- Given  $(\mathbf{A}^T, \mathbf{T})$ , it is computationally hard to recover  $\mathbf{S}$ . This is multi-secret (matrix) variant of the ISIS problem.
- Corresponding column vectors of  $\mathbf{T}$  and  $\mathbf{S}$  together with  $\mathbf{A}^T$  will represent the individual ISIS problems.
- In fact there are  $k$  ISIS instances with a shared coefficient matrix  $\mathbf{A}^T$ .

# A SIS BASED DIGITAL SIGNATURE ALGORITHM..

FIAT-SHAMIR WITH ABORTS FRAMEWORK

## Algorithm 2 — $\text{Sign}(\mu, sk, pk)$

**Input:** Signing key  $sk$  and message  $\mu$

**Output:** Signature

- 1  $\mathbf{y} \leftarrow D_{\sigma}^m$  ▷ Commitment:  $\mathbf{A}^T \mathbf{y}$
- 2  $\mathbf{c} = \mathsf{H}(\mathbf{A}^T \cdot \mathbf{y}, \mu) \in \{-1, 0, +1\}^k$  ▷ Challenge:  $\mathbf{c}$
- 3  $\mathbf{z} = \mathbf{Sc} + \mathbf{y}$  ▷ Response:  $\mathbf{z}$
- 4 **return**  $(\mathbf{z}, \mathbf{c})$  with probability  $\min\left(\frac{D_{\sigma}^m}{MD_{\mathbf{Sc}, \sigma}^m}, 1\right)$ ,

where  $M \in \mathbb{R}$  is such that

$$\Pr \left[ MD_{\mathbf{Sc}, \sigma}^m (\mathbf{z}) \geq D_{\sigma}^m (\mathbf{z}) : \mathbf{z} \leftarrow D_{\sigma}^m \right] \geq 1 - \varepsilon.$$

# A SIS BASED DIGITAL SIGNATURE ALGORITHM..

Algorithm 3 — **Verify** ( $pk := (\mathbf{A}, \mathbf{T}) , \mu, (\mathbf{z}, \mathbf{c})$ )

if  $\mathbf{c} = \mathsf{H}(\mathbf{A}^T \mathbf{z} - \mathbf{T}\mathbf{c}, \mu)$  and  $\|\mathbf{z}\| \leq \sigma\sqrt{m}$  then  
  └ return 1

## LWE BASED DIGITAL SIGNATURE ALGORITHM

Algorithm 4 — **KeyGen**( $n, m, k, q$ )

- 1  $\mathbf{S} \in_{\phi} \mathbb{Z}_q^{n \times k}$
- 2  $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}, \mathbf{E} \in_{\chi} \mathbb{Z}_q^{m \times k}$  and  $\mathbf{T} = \mathbf{A} \cdot \mathbf{S} + \mathbf{E} \pmod{q}$
- 3 **return**  $sk := \mathbf{S}$  and  $pk := (\mathbf{A}, \mathbf{T})$

# A FRAMEWORK FOR LWE BASED SIGNATURE

## Algorithm 5 — $\text{Sign}(\mu, sk, pk)$

```
1  $\mathbf{y}_1, \mathbf{y}_2 \leftarrow D_{\mathbf{y}}^n$ 
2  $\mathbf{w} = \mathbf{A} \cdot \mathbf{y}_1 + \mathbf{y}_2$                                 ▷ Commitment:  $\mathbf{w}$ 
3  $\mathbf{c} = \mathsf{H}(\mu || \mathbf{w}) \in \{-1, 0, +1\}^k$       ▷ Challenge: sparse  $\mathbf{c}$ 
4  $\mathbf{z}_1 = \mathbf{S}\mathbf{c} + \mathbf{y}_1, \mathbf{z}_2 = \mathbf{E}\mathbf{c} + \mathbf{y}_2$     ▷ Response:  $\mathbf{z}_1, \mathbf{z}_2$ 
5 if ( $\mathbf{z}_1, \mathbf{z}_2$ ) leaks dist of  $\mathbf{S}$  then ▷  $\|\mathbf{z}_i\| > bd_i$ 
6   restart
7 return ( $\mathbf{z}_1, \mathbf{z}_2, \mathbf{c}$ )
```

## Algorithm 6 — $\text{Verify}(pk := (\mathbf{A}, \mathbf{T}), \mu, (\mathbf{z}_1, \mathbf{z}_2, \mathbf{c}))$

```
1 if  $\|\mathbf{z}_i\| \leq bd_i \forall i$  then
2   return  $H(\mu || \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{T}\mathbf{c}) \stackrel{?}{=} \mathbf{c}$ 
```

# A FRAMEWORK FOR LWE BASED SIGNATURE..

- ❑ The main draw back of this framework (Algorithm 5) is the signature size. In comparison to the SIS based schemes, the signature has an additional vector  $\mathbf{z}_2$  of dimension  $n$ .
- ❑ This can be resolved using the Bai-Galbraith technique. We discuss this in the signature scheme given in the Algorithm 7 below.

## LWE BASED DIGITAL SIGNATURE ALGORITHM..

Algorithm 7 — **Sign**( $\mu, sk, pk$ )

```
1  $y \leftarrow D_\sigma^n; w = A \cdot y$                                 ▷ Commitment: w
2  $w_1 = \text{HighBits}(w)$ 
3  $c = H(\mu || w_1) \in \{-1, 0, +1\}^k$       ▷ Challenge: sparse c
4 if  $\text{LowBits}(w - Ec) > bd$  then
5   restart
6  $z = Sc + y$                                               ▷ Response: z
7 if  $z$  leaks dist of S then ▷  $\|z\| > bd_1$ 
8   restart
9 return (z, c)
```

# LWE BASED DIGITAL SIGNATURE ALGORITHM..

## Algorithm 8 — **verify** ( $pk := (\mathbf{A}, \mathbf{T}) , \mu, (\mathbf{z}, \mathbf{c})$ )

```
1 w'1 = HighBits(AZ – Tc)
2 if c = H( $\mu || \mathbf{w}'_1$ ) and  $\|\mathbf{z}\| \leq bd_1$  then
3   return 1
```