# Lattice-based cryptographic constructions

Elena Kirshanova

at Post-Quantum Cryptography Summer School
Hammamet, Tunisia

## Logistics

There will be two lectures on lattices:

1. Lattice-based cryptographic constructions (now)
2. Cryptanalysis of lattice-based constructions (tomorrow)

Lecture materials are available at
`https://elenakirshanova.github.io/teaching/summerschoolTunis2026.html`

# Agenda

1. Learning with Errors (LWE)
2. Algebraic versions of LWE and Kyber
3. Short Integer Solution problem (SIS)
4. Dilithium Signature

## Learning with Errors (LWE) [Regev'05]

Fix dimension $n > 0$, modulus $q > 1$, and noise distribution $\chi$

Search LWE: Find secret $\mathbf{s} \in \mathbb{Z}_q^n$ given noisy inner products:

$$\begin{aligned} \mathbf{a}_1 &\xleftarrow{\$} \mathbb{Z}_q^n,\ e_1 \leftarrow \chi, \quad (\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \bmod q), \\ &\vdots \\ \mathbf{a}_m &\xleftarrow{\$} \mathbb{Z}_q^n,\ e_m \leftarrow \chi, \quad (\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s} \rangle + e_m \bmod q) \end{aligned}$$

## Learning with Errors (LWE) [Regev'05]

Fix dimension $n > 0$, modulus $q > 1$, and noise distribution $\chi$

Search LWE: Find secret $\mathbf{s} \in \mathbb{Z}_q^n$ given noisy inner products:

$$\begin{aligned} \mathbf{a}_1 &\xleftarrow{\$} \mathbb{Z}_q^n,\ e_1 \leftarrow \chi, \quad (\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \bmod q), \\ &\vdots \\ \mathbf{a}_m &\xleftarrow{\$} \mathbb{Z}_q^n,\ e_m \leftarrow \chi, \quad (\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s} \rangle + e_m \bmod q) \end{aligned}$$

Decision LWE: Distinguish between the two distributions:

$$\begin{aligned} \mathbf{a}_1 &\xleftarrow{\$} \mathbb{Z}_q^n,\ b \xleftarrow{\$} \mathbb{Z}_q \\ &\vdots \\ \mathbf{a}_m &\xleftarrow{\$} \mathbb{Z}_q^n,\ b \xleftarrow{\$} \mathbb{Z}_q \end{aligned} \qquad \begin{aligned} \mathbf{a}_1 &\xleftarrow{\$} \mathbb{Z}_q^n,\ b = \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \bmod q \\ &\vdots \\ \mathbf{a}_m &\xleftarrow{\$} \mathbb{Z}_q^n,\ b = \langle \mathbf{a}_m, \mathbf{s} \rangle + e_m \bmod q \end{aligned}$$

## LWE: numerical example

$$n = 1,\ q = 13, \chi \text{ is central binomial distribution over } \{-1, 0, 1\}$$
$$\Pr[e = -1] = \Pr[e = 1] = \tfrac{1}{4}, \Pr[e = 0] = \tfrac{1}{2}.$$

Can you guess $\mathbf{s}$ from

$$\mathbf{a}_1 = (10),\ b_1 = 9$$
$$\mathbf{a}_2 = (5),\ b_2 = 5$$

## LWE: numerical example

$$n = 1,\ q = 13, \chi \text{ is central binomial distribution over } \{-1, 0, 1\}$$
$$\Pr[e = -1] = \Pr[e = 1] = \tfrac{1}{4}, \Pr[e = 0] = \tfrac{1}{2}.$$

Can you guess $\mathbf{s}$ from

$$\mathbf{a}_1 = (10),\ b_1 = 9$$
$$\mathbf{a}_2 = (5),\ b_2 = 5$$
$$\mathbf{a}_3 = (8),\ b_3 = 9$$
$$\mathbf{a}_4 = (11),\ b_4 = 11$$

## LWE: numerical example

$$n = 1,\ q = 13, \chi \text{ is central binomial distribution over } \{-1, 0, 1\}$$
$$\Pr[e = -1] = \Pr[e = 1] = \tfrac{1}{4}, \Pr[e = 0] = \tfrac{1}{2}.$$

Can you guess $\mathbf{s}$ from

$$\mathbf{a}_1 = (10),\ b_1 = 9$$
$$\mathbf{a}_2 = (5),\ b_2 = 5$$
$$\mathbf{a}_3 = (8),\ b_3 = 9$$
$$\mathbf{a}_4 = (11),\ b_4 = 11$$
$$\mathbf{a}_5 = (12),\ b_4 = 0$$

## LWE: numerical example

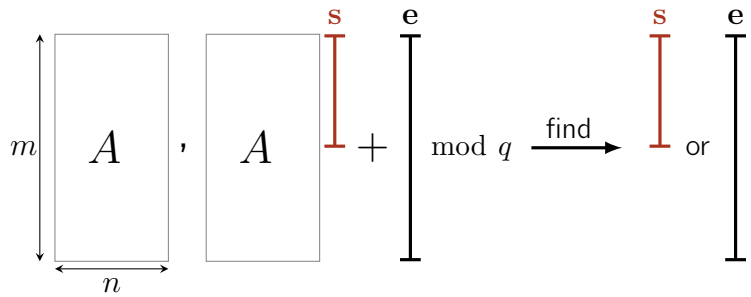
$$n = 1,\ q = 13, \chi \text{ is central binomial distribution over } \{-1, 0, 1\}$$
$$\Pr[e = -1] = \Pr[e = 1] = \tfrac{1}{4}, \Pr[e = 0] = \tfrac{1}{2}.$$

Can you guess $\mathbf{s}$ from

$$\mathbf{a}_1 = (10),\ b_1 = 9$$
$$\mathbf{a}_2 = (5),\ b_2 = 5$$
$$\mathbf{a}_3 = (8),\ b_3 = 9$$
$$\mathbf{a}_4 = (11),\ b_4 = 11$$
$$\mathbf{a}_5 = (12),\ b_4 = 0$$

$$\mathbf{s} = (1)$$

# LWE in matrix form

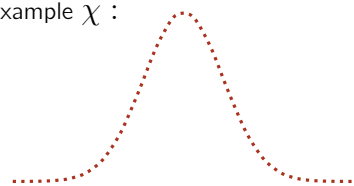



$$A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$$

$$\mathbf{s} \leftarrow \mathbb{Z}_q^n$$

$$\mathbf{e} \leftarrow \chi^m$$

Example $\chi$ :



## LWE hardness

- The solution is unique for enough number of LWE samples $(\mathbf{a}, b)$ ($\#$ samples $> n \log q$ is enough).
- The larger $n$, the harder LWE. In crypto we use $n \geq 512$
- Modulus $q$ is typically $\mathrm{poly}(n)$, i.e., $q = n^2$
- Exact distribution of the secret does not play a significant role, as long as $\mathbf{s}$ has enough entropy. Binary or ternary $\mathbf{s}$ are common choices.
- The distribution of $\mathbf{e}$ is important: $\mathbf{e} = 0$ makes LWE trivially easy (why?), if $\mathbf{e} \xleftarrow{\$} \mathbb{Z}_q^m$ makes LWE trivially hard. Common choices: discrete Gaussian, central binomial, ternary.
- Best known attack on LWE runs in time $\sim 2^{\mathcal{O}(n)}$.

...more about LWE hardness tomorrow.

## Search vs. Decision LWE

Decision-to-Search: Trivial

Search-to-Decision: Let $\mathbf{s}^\star$ be the secret. Goal: find $s_1^\star$ with access to decision LWE oracle and with $\{(\mathbf{a}_i, b_i)\}$.

## Search vs. Decision LWE

Decision-to-Search: Trivial

Search-to-Decision: Let $\mathbf{s}^\star$ be the secret. Goal: find $s_1^\star$ with access to decision LWE oracle and with $\{(\mathbf{a}_i, b_i)\}$.

1. Make a guess $s_1' \xleftarrow{\$} \mathbb{Z}_q$ for $s_1^\star$. Call Decision LWE oracle on modified samples

$$\mathbf{a}_i + (1, 0, \ldots, 0)^T, b_i + s_1'$$

## Search vs. Decision LWE

Decision-to-Search: Trivial

Search-to-Decision: Let $\mathbf{s}^\star$ be the secret. Goal: find $s_1^\star$ with access to decision LWE oracle and with $\{(\mathbf{a}_i, b_i)\}$.

1. Make a guess $s_1' \xleftarrow{\$} \mathbb{Z}_q$ for $s_1^\star$. Call Decision LWE oracle on modified samples

$$\mathbf{a}_i + (1, 0, \ldots, 0)^T, b_i + s_1'$$

- If $s_1' = s_1^\star$,

$$b_i + s_1' = \langle \mathbf{a}_i, \mathbf{s} \rangle + e + s_1' = \langle \mathbf{a}_i, \mathbf{s} \rangle + e + \langle (1, 0, \ldots, 0), \mathbf{s} \rangle = \langle \mathbf{a}_i + (1, 0, \ldots, 0), \mathbf{s} \rangle + e$$

## Search vs. Decision LWE

Decision-to-Search: Trivial

Search-to-Decision: Let $\mathbf{s}^\star$ be the secret. Goal: find $s_1^\star$ with access to decision LWE oracle and with $\{(\mathbf{a}_i, b_i)\}$.

1. Make a guess $s_1' \xleftarrow{\$} \mathbb{Z}_q$ for $s_1^\star$. Call Decision LWE oracle on modified samples

$$\mathbf{a}_i + (1, 0, \ldots, 0)^T, b_i + s_1'$$

- If $s_1' = s_1^\star$,

$$b_i + s_1' = \langle \mathbf{a}_i, \mathbf{s} \rangle + e + s_1' = \langle \mathbf{a}_i, \mathbf{s} \rangle + e + \langle (1, 0, \ldots, 0), \mathbf{s} \rangle = \overbrace{\langle \mathbf{a}_i + (1, 0, \ldots, 0), \mathbf{s} \rangle + e}^{\text{Correct LWE sample!}}$$

- If $s_1' \neq s_1^\star$,

$$b_i + s_1' \text{ is uniform in } \mathbb{Z}_q.$$

$\implies$ LWE Decision oracle distinguishes correct guess from the incorrect ones.

# PKE from LWE

Alice

Bob

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$

$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

$$\mu \in \{0, 1\}$$

# PKE from LWE

Alice

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$
$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

Bob

$$\mu \in \{0, 1\}$$

Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$$
$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

# PKE from LWE

Alice

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$
$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

Bob

$$\mu \in \{0, 1\}$$

Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$$
$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

$\xleftarrow{c=(\mathbf{c}_1, c_2)}$

$$c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

# PKE from LWE

Alice

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$
$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

Bob

$$\mu \in \{0, 1\}$$

Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$$
$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

$\xleftarrow{c=(\mathbf{c}_1, c_2)}$

$$c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

Decryption:

$$\text{if } |c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle| \text{ close to } 0 \implies \mu = 0$$

# PKE from LWE

Alice

Bob

Correctness:

$$c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle =$$
$$\langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 - \mathbf{t}_1^T A\mathbf{s} - \mathbf{t}_2^T \mathbf{s} + \mu \lfloor \tfrac{q}{2} \rfloor$$
$$=$$

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$
$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

$$\mu \in \{0, 1\}$$

Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$$
$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

$$\xleftarrow{c = (\mathbf{c}_1, c_2)} \quad c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

Decryption:

if $|c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle|$ close to 0 $\implies \mu = 0$

# PKE from LWE

Alice

Bob

Correctness:

$$c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle =$$
$$\langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 - \mathbf{t}_1^T A\mathbf{s} - \mathbf{t}_2^T \mathbf{s} + \mu \lfloor \tfrac{q}{2} \rfloor$$
$$=$$
$$\mathbf{t}_1^T A\mathbf{s} + \mathbf{t}_1^T \mathbf{e} + t_3 - \mathbf{t}_1^T A\mathbf{s} - \mathbf{t}_2^T \mathbf{s} + \mu \lfloor \tfrac{q}{2} \rfloor$$
$$=$$

$\mu \in \{0,1\}$

$\mathrm{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$

$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$

Encryption:

$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$

$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$

$\xleftarrow{c = (\mathbf{c}_1, c_2)}$

$c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$

Decryption:

if $|c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle|$ close to 0 $\implies \mu = 0$

# PKE from LWE



Correctness:

$$c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle =$$
$$\langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 - \mathbf{t}_1^T A\mathbf{s} - \mathbf{t}_2^T \mathbf{s} + \mu \lfloor \tfrac{q}{2} \rfloor$$
$$=$$
$$\mathbf{t}_1^T A\mathbf{s} + \mathbf{t}_1^T \mathbf{e} + t_3 - \mathbf{t}_1^T A\mathbf{s} - \mathbf{t}_2^T \mathbf{s} + \mu \lfloor \tfrac{q}{2} \rfloor$$
$$=$$
$$\underbrace{\mathbf{t}_1^T \mathbf{e} + t_3 - \mathbf{t}_2^T \mathbf{s}}_{\text{small}} + \mu \lfloor \tfrac{q}{2} \rfloor$$

$\mathrm{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$

$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$

$\mu \in \{0, 1\}$

Encryption:

$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$

$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$

$\xleftarrow{c = (\mathbf{c}_1, c_2)}$

$c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$

Decryption:

if $|c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle|$ close to 0 $\implies \mu = 0$

# PKE from LWE. Security

Alice

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$
$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

Bob

$$\mu \in \{0, 1\}$$

Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$$
$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

$\xleftarrow{c=(\mathbf{c}_1, c_2)}$

$$c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

Decryption:

if $|c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle|$ close to 0 $\implies \mu = 0$

# PKE from LWE. Security

Alice

Indistinguishable under Decision LWE

Bob

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$

$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

$$\mu \in \{0, 1\}$$

Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$$

$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

$$\xleftarrow{c = (\mathbf{c}_1, c_2)} \quad c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

Decryption:

$$\text{if } |c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle| \text{ close to } 0 \implies \mu = 0$$

# PKE from LWE. Security

Alice

Bob

Indistinguishable under Decision LWE

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$

$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

$$\mu \in \{0, 1\}$$

Encryption:

Indistinguishable under Decision LWE

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, t_3 \leftarrow \chi$$

$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

$$c = (\mathbf{c}_1, c_2)$$

$$c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + t_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

Decryption:

if $|c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle|$ close to 0 $\implies \mu = 0$

# Algebraic LWE: motivation

- Storing LWE samples requires $\Omega(n^2 \log q)$ bits
- Matrix vector multiplication require $O(n^2)$ operations in $\mathbb{Z}_q$

$\implies$ 'standard' LWE is inefficient[1]

Solution: Algebraic versions of LWE

Options: polynomial LWE, Ring-LWE, Module-LWE, ...

[1] Although concrete PKE proposals exist (e.g., Frodo) with $\mathrm{pk}$ and $\mathrm{ct} \approx 10\mathrm{kB}$

## Polynomial rings

- $\mathbb{Z}[x]$ – polynomial ring (i.e., polynomial with integer coefficients)
- $\mathbb{Z}_q[x]$ – quotient polynomial ring i.e., polynomials with coefficients taken $\bmod q$
- $f \in \mathbb{Z}[x]$ is unitary if its leading coefficient is 1 (example: $f = x^4 + 4x^3 + 7$)
- $f$ is irreducible in $\mathbb{Z}[x]$ if it does not have roots in $\mathbb{Z}[x]$ (example: $f = x^2 + 1$)
- $\mathbb{Z}[x]/f$ polynomial quotient ring, i.e., set of polynomials taken $\bmod f$
- To multiply $g, h \in \mathbb{Z}[x]/f$, fist compute $r = g \cdot h$ using ordinary polynomial multiplication, $\deg(r) \leq 2n - 2$ then divide $r$ by $f$ and take the remainder of the division.

## Polynomial multiplication as matrix-vector product

Any polynomial can be represented as a vector via coefficient embedding.

For $f \in \mathbb{Z}[x]$ a unitary irreducible of degree $n$:

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

## Polynomial multiplication as matrix-vector product

Any polynomial can be represented as a vector via coefficient embedding.

For $f \in \mathbb{Z}[x]$ a unitary irreducible of degree $n$:

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

For $a, b \in \mathbb{Z}[x]/f$ and $c = a \cdot b \in \mathbb{Z}[x]/f$, it holds

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-2} \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} | & | & \cdots & | \\ | & | & \cdots & | \\ \mathsf{coeff}(a) & \mathsf{coeff}(x \cdot a) & \ddots & \mathsf{coeff}(x^{n-1} \cdot a) \\ | & | & \cdots & | \\ | & | & \cdots & | \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-2} \\ b_{n-1} \end{bmatrix}$$

## Polynomial multiplication as matrix-vector product

Any polynomial can be represented as a vector via coefficient embedding.

For $f \in \mathbb{Z}[x]$ a unitary irreducible of degree $n$:

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Example: $f = x^n + 1$:

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-2} \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} a_0 & -a_{n-1} & \ldots & -a_1 \\ a_1 & a_0 & \ldots & -a_2 \\ \vdots & \vdots & \ddots & \\ a_{n-2} & a_{n-3} & \ldots & -a_{n-1} \\ \underbrace{a_{n-1}}_{a} & \underbrace{a_{n-2}}_{x \cdot a} & \ldots & \underbrace{a_0}_{x^{n-1} \cdot a} \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-2} \\ b_{n-1} \end{bmatrix}$$

## Polynomial multiplication as matrix-vector product

Any polynomial can be represented as a vector via coefficient embedding.

For $f \in \mathbb{Z}[x]$ a unitary irreducible of degree $n$:

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Example: $f = x^n + 1$:

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-2} \\ c_{n-1} \end{bmatrix} = \underbrace{\begin{bmatrix} a_0 & -a_{n-1} & \ldots & -a_1 \\ a_1 & a_0 & \ldots & -a_2 \\ \vdots & & \mathsf{Rot}_f(a) & \\ a_{n-2} & a_{n-3} & \ldots & -a_{n-1} \\ a_{n-1} & a_{n-2} & \ldots & a_0 \end{bmatrix}}_{a \qquad x \cdot a \qquad\qquad x^{n-1} \cdot a} \cdot \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-2} \\ b_{n-1} \end{bmatrix}$$

## Polynomial-LWE, SSTX'09

Let $f \in \mathbb{Z}[x]$ be unitary irreducible of degree $n$, $q \geq 2$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Search Poly-LWE$_f$:

- Sample $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $a_i$'s $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample coefficients of $\mathbf{e}_i$ from $\chi$

Given $(a_1, \ldots, a_m)$ and
$(a_1 \cdot \mathbf{s} + \mathbf{e}_1, \ldots a_m \cdot \mathbf{s} + \mathbf{e}_m)$, find $\mathbf{s}$.

## Polynomial-LWE, SSTX'09

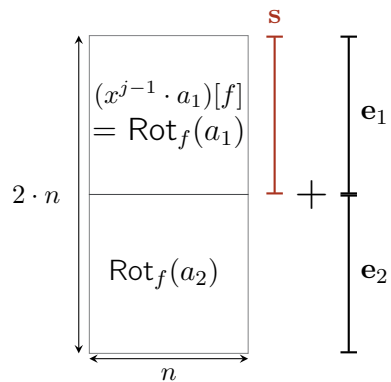
Let $f \in \mathbb{Z}[x]$ be unitary irreducible of degree $n$, $q \geq 2$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Search Poly-LWE$_f$:

- Sample $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $a_i$'s $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample coefficients of $\mathbf{e}_i$ from $\chi$

Given $(a_1, \ldots, a_m)$ and $(a_1 \cdot \mathbf{s} + \mathbf{e}_1, \ldots a_m \cdot \mathbf{s} + \mathbf{e}_m)$, find $\mathbf{s}$.



## Polynomial-LWE, SSTX'09

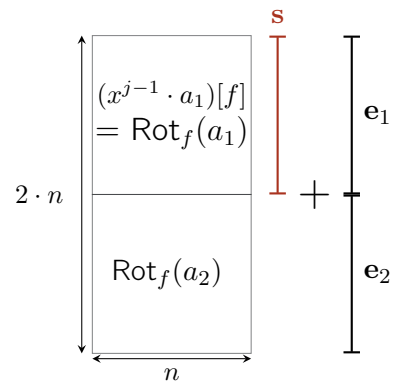
Let $f \in \mathbb{Z}[x]$ be unitary irreducible of degree $n$, $q \geq 2$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Search Poly-LWE$_f$:

- Sample $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $a_i$'s $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample coefficients of $\mathbf{e}_i$ from $\chi$

Given $(a_1, \ldots, a_m)$ and $(a_1 \cdot \mathbf{s} + \mathbf{e}_1, \ldots a_m \cdot \mathbf{s} + \mathbf{e}_m)$, find $\mathbf{s}$.




One Poly-LWE samples $(a_i, a_i s + e_i)$ gives $n$ 'standard' LWE samples

Can multiply two polynomials in time $\mathcal{O}(n \log q)$

## Canonical embedding

Any polynomial can be represented as a vector via canonical embedding.

Let $f = x^n + 1$ be a polynomial with $n = 2^k$ (such polynomials are called cyclotomic).

Let $\omega_1, \ldots, \omega_n \in \mathbb{C}$ be the roots of $f$: $\omega_i = e^{\frac{\pi i}{n}}$

Canonical embedding $\sigma$ of $a$ evaluates $a$ in all $\omega_i$:

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \ldots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Canonical and coefficient embeddings are related via the Vandermond matrix of $\omega_i$'s:

$$V = \begin{bmatrix} 1 & \omega_1 & \ldots & \omega_1^{n-1} \\ 1 & \omega_2 & \ldots & \omega_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n & \ldots & \omega_n^{n-1} \end{bmatrix}$$

$$(a(\omega_0), \ldots, a(\omega_{n-1}))^T = V \cdot (a_0, \ldots, a_{n-1})^T$$

## Ring-LWE for $f = x^{2^k} + 1$, LPR'10

For $f = x^n + 1$, $n = 2^k$, $q \geq 2$, and

$\omega_1, \ldots, \omega_n \in \mathbb{C}$ – the roots of $f$, $V_f$ - Vandermond matrix of $\omega_i$'s

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \ldots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Search Ring-LWE$_f$:

- Sample $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $a_i$'s $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $\sigma(e_i)$'s from $\chi$

## Ring-LWE for $f = x^{2^k} + 1$, LPR'10

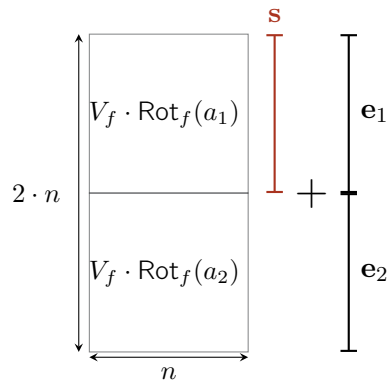
For $f = x^n + 1$, $n = 2^k$, $q \geq 2$, and

$\omega_1, \ldots, \omega_n \in \mathbb{C}$ – the roots of $f$, $V_f$ - Vandermond matrix of $\omega_i$'s

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \ldots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Search Ring-LWE$_f$:

- Sample $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $a_i$'s $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $\sigma(e_i)$'s from $\chi$



## Ring-LWE for $f = x^{2^k} + 1$, LPR'10

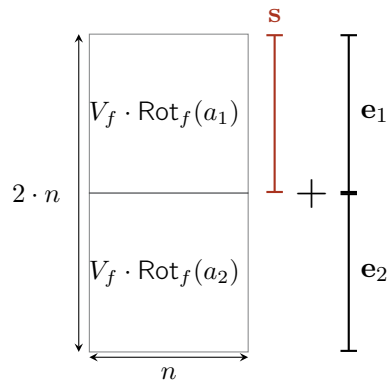
For $f = x^n + 1$, $n = 2^k$, $q \geq 2$, and

$\omega_1, \ldots, \omega_n \in \mathbb{C}$ – the roots of $f$, $V_f$ - Vandermond matrix of $\omega_i$'s

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \ldots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Search Ring-LWE$_f$:

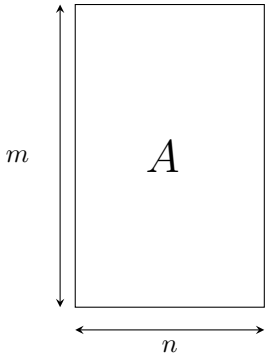
- Sample $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $a_i$'s $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $\sigma(e_i)$'s from $\chi$




- Can multiple in time $O(n \log q)$
- Poly-LWE and Ring-LWE are related for $f$'s with $V_f$ of small operator norm

# Module LWE

LWE

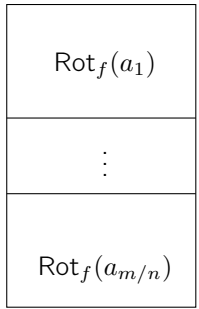



$\mathbf{a}_i \in \mathbb{Z}_q^n$

$(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i)$

$\mathbf{s} \in \mathbb{Z}_q^n, e_i \in \mathbb{Z}$

Ring-LWE



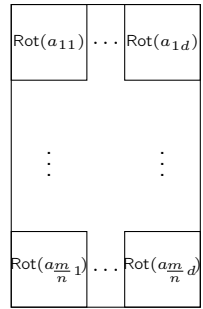

$f = x^n + 1$

$a_i \in \mathbb{Z}[x]/f$

$(a_i, a_i \cdot s + e_i)$

$s \in \mathbb{Z}[x]/f, e_i \in \mathbb{Z}[x]/f$

Module-LWE




$f = x^{n/d} + 1$

$\mathbf{a}_i \in (\mathbb{Z}[x]/f)^d$

$(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i$

$\mathbf{s} \in (\mathbb{Z}[x]/f)^d, e_i \in \mathbb{Z}[x]/f$

# Kyber (ML-KEM) design

Recall PKE from LWE

Alice

Bob

$$\text{pk} = (A \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m)$$
$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

$$\mu \in \{0,1\}$$

Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, \mathbf{t}_3 \leftarrow \chi^m$$
$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

$$\xleftarrow{c=(\mathbf{c}_1, c_2)} \quad c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + \mathbf{t}_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

Decryption:

if $|c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle|$ close to 0 $\implies \mu = 0$

# Kyber (ML-KEM) design

Alice

Recall PKE from LWE

Change $\mathbb{Z}_q$ to $\mathbb{Z}_q[x]/(x^{256}+1) := \mathcal{R}$

Bob

$$\text{pk} = (A \in \mathcal{R}^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathcal{R}^m)$$
$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

$$\mu \in \{0,1\}$$

Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, \mathbf{t}_3 \leftarrow \chi^m$$
$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$

$\xleftarrow{c=(\mathbf{c}_1, c_2)}$

$$c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + \mathbf{t}_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

Decryption:

if $|c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle|$ close to 0 $\implies \mu = 0$

# Kyber (ML-KEM) design

Alice

Recall PKE from LWE

Change $\mathbb{Z}_q$ to $\mathbb{Z}_q[x]/(x^{256}+1) := \mathcal{R}$

Now Bob encrypts a vector

$\chi$ is a distribution over $\mathcal{R}$

Bob

$$\text{pk} = (A \in \mathcal{R}^{m \times n}, \mathbf{b} = A\mathbf{s} + \mathbf{e} \in \mathcal{R}^m)$$
$$\mathbf{s} \leftarrow \chi^n, \mathbf{e} \leftarrow \chi^m$$

$$\mu \in \{0,1\}^n$$

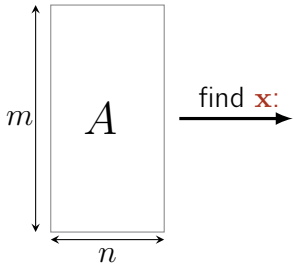
Encryption:

$$\mathbf{t}_1 \leftarrow \chi^m, \mathbf{t}_2 \leftarrow \chi^n, \mathbf{t}_3 \leftarrow \chi^m$$
$$\mathbf{c}_1 = \mathbf{t}_1^T \cdot A + \mathbf{t}_2^T \bmod q$$
$$\xleftarrow{c=(\mathbf{c}_1, c_2)} \quad c_2 = \langle \mathbf{t}_1, \mathbf{b} \rangle + \mathbf{t}_3 + \mu \lfloor \tfrac{q}{2} \rfloor \bmod q$$

Decryption (coefficient-wise):

if $|c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle|$ close to 0 $\implies \mu = 0$

# Short Integer Solution (SIS), Ajtai'96



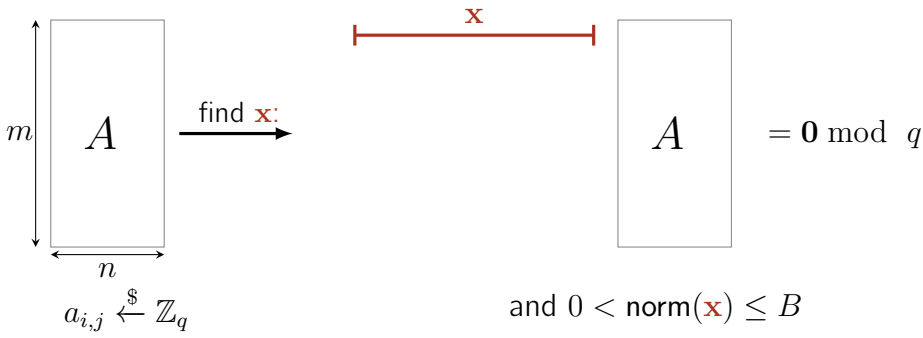

$a_{i,j} \xleftarrow{\$} \mathbb{Z}_q$



$= \mathbf{0} \bmod q$

and $0 < \mathsf{norm}(\mathbf{x}) \leq B$

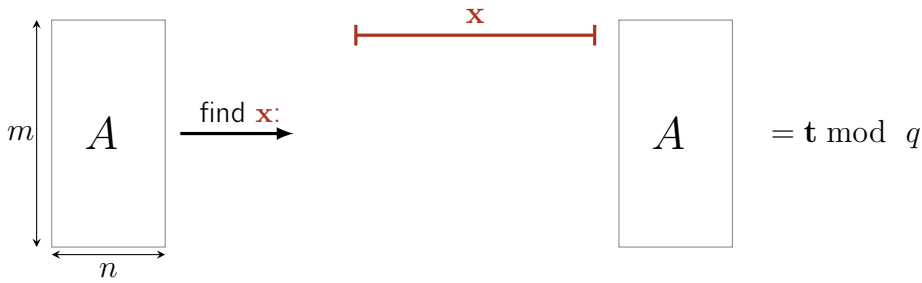
## Short Integer Solution (SIS), Ajtai'96




The problem is interesting in the Euclidean norm: $\|\mathbf{x}\| \leq B$

and in the infinity norm: $\|\mathbf{x}\|_\infty = \max_i\{|\mathbf{x}_i|\} \leq B$

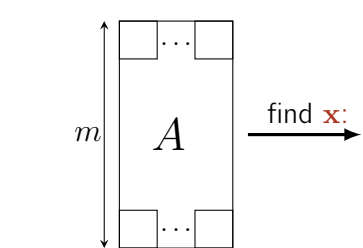
# Inhomogenous Short Integer Solution (ISIS), Ajtai'96



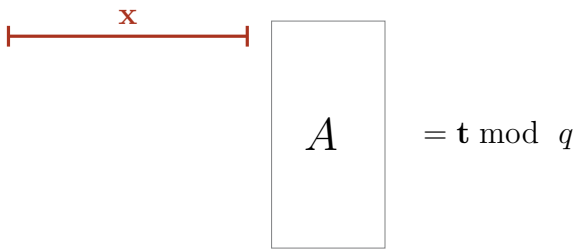

The problem is interesting in the Euclidean norm: $\|\mathbf{x}\| \leq B$

and in the infinity norm: $\|\mathbf{x}\|_\infty = \max_i\{|\mathbf{x}_i|\} \leq B$

# Module SIS over $\mathbb{Z}[x]/f$




find $\mathbf{x}$:




and $0 < \mathsf{norm}(\mathbf{x}) \leq B$

## (Module)-SIS hardness

- Inhomogenus version and homogenus versions are equivalent (think why)
- The larger $B$ – the upper bound on the solution, the easier the problem is ($B = q$ is trivial)
- For very small $B$ (and $m$) a solution may not exist
- Typically, $B$ is chosen such that there are exponentially many solutions ($B^m > q^n$)
- The larger $n$, the harder the problem is
- Interesting parameters to solve will be $n = 1024$, $B = q/8$

## Methods to construct a signature scheme

### I. Hash-and-Sign Paradigm

Examples: Falcon = NTRUSign + [GPV08]

Pros: short signatures (0.7kB for Falcon 512), fast verification

Cons: complex to implement, expensive KeyGen

### II. Fiat-Shamir Heuristic [FS]

Examples: Bai-Gabraith, Dilithium, HAWK (not based on SIS)

Pros: easy to implement, fast KeyGen, Sign

Cons: larger signatures (2.7kB for Dilithium3)

## Dilithium simplified

$\chi$ – a distribution over $R = \mathbb{Z}_q[x]/(x^{256+1})$ that outputs 'short' polynomials

$\mathcal{H}$ – a cryptographic hash function that outputs short digests

I. KeyGen :

1. $A \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow \chi^k$
3. $\mathbf{t} = \mathbf{s}A$
4. $\mathsf{vk} = (A, \mathbf{t})$, $\mathsf{sk} = (\mathbf{s}, A, \mathbf{t})$.

## Dilithium simplified

$\chi$ – a distribution over $R = \mathbb{Z}_q[x]/(x^{256+1})$ that outputs 'short' polynomials

$\mathcal{H}$ – a cryptographic hash function that outputs short digests

I. KeyGen :

1. $A \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow \chi^k$
3. $\mathbf{t} = \mathbf{s}A$
4. $\mathsf{vk} = (A, \mathbf{t})$, $\mathsf{sk} = (\mathbf{s}, A, \mathbf{t})$.

II. Sign$(\mathsf{sk}, m)$ :

1. $\mathbf{r} \leftarrow \chi^\ell$
2. $\mathbf{u} = \mathbf{r}A$
3. $c = \mathcal{H}(m||\mathbf{u})$
4. $\mathbf{z} = \mathbf{r} + c\mathbf{s}$
5. **return** $\sigma = (\mathbf{u}, \mathbf{z})$

## Dilithium simplified

$\chi$ – a distribution over $R = \mathbb{Z}_q[x]/(x^{256+1})$ that outputs 'short' polynomials

$\mathcal{H}$ – a cryptographic hash function that outputs short digests

I. KeyGen :

1. $A \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow \chi^k$
3. $\mathbf{t} = \mathbf{s}A$
4. $\mathsf{vk} = (A, \mathbf{t})$, $\mathsf{sk} = (\mathbf{s}, A, \mathbf{t})$.

II. Sign$(\mathsf{sk}, m)$ :

1. $\mathbf{r} \leftarrow \chi^\ell$
2. $\mathbf{u} = \mathbf{r}A$
3. $c = \mathcal{H}(m||\mathbf{u})$
4. $\mathbf{z} = \mathbf{r} + c\mathbf{s}$
5. **return** $\sigma = (\mathbf{u}, \mathbf{z})$

III. Verify$(\mathsf{vk}, m, \sigma = (\mathbf{u}, \mathbf{z}))$ :

1. $c = \mathcal{H}(m||\mathbf{u})$
2. If $\mathbf{z}$ is short and $\mathbf{z}A - c\mathbf{t} == \mathbf{u}$:
   **return** "Accept"
   Else **return** "Reject"

## Dilithium simplified

$\chi$ – a distribution over $R = \mathbb{Z}_q[x]/(x^{256+1})$ that outputs 'short' polynomials

$\mathcal{H}$ – a cryptographic hash function that outputs short digests

I. KeyGen :

1. $A \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow \chi^k$
3. $\mathbf{t} = \mathbf{s}A$ Module SIS
4. $\mathsf{vk} = (A, \mathbf{t})$, $\mathsf{sk} = (\mathbf{s}, A, \mathbf{t})$.

II. Sign$(\mathsf{sk}, m)$ :

1. $\mathbf{r} \leftarrow \chi^\ell$
2. $\mathbf{u} = \mathbf{r}A$ Module SIS
3. $c = \mathcal{H}(m||\mathbf{u})$
4. $\mathbf{z} = \mathbf{r} + c\mathbf{s}$
5. **return** $\sigma = (\mathbf{u}, \mathbf{z})$

III. Verify$(\mathsf{vk}, m, \sigma = (\mathbf{u}, \mathbf{z}))$ :

1. $c = \mathcal{H}(m||\mathbf{u})$
2. If $\mathbf{z}$ is short and $\mathbf{z}A - c\mathbf{t} == \mathbf{u}$:

   **return** "Accept"

   Else **return** "Reject"

Correctness:

- $\mathbf{z}A - c\mathbf{t} = \mathbf{r}A + c\mathbf{s} \cdot A - c\mathbf{s} \cdot A = \mathbf{r}A$
- $\mathbf{z}$ short since $\mathbf{r}, c, \mathbf{s}$ are short

## Dilithium simplified

$\chi$ – a distribution over $R = \mathbb{Z}_q[x]/(x^{256+1})$ that outputs 'short' polynomials

$\mathcal{H}$ – a cryptographic hash function that outputs short digests

I. KeyGen :

1. $A \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow \chi^k$
3. $\mathbf{t} = \mathbf{s}A$ Module SIS
4. $\mathsf{vk} = (A, \mathbf{t})$, $\mathsf{sk} = (\mathbf{s}, A, \mathbf{t})$.

II. Sign$(\mathsf{sk}, m)$ :

1. $\mathbf{r} \leftarrow \chi^\ell$
2. $\mathbf{u} = \mathbf{r}A$ Module SIS
3. $c = \mathcal{H}(m||\mathbf{u})$
4. $\mathbf{z} = \mathbf{r} + c\mathbf{s}$ Leaks $\mathbf{s}$!
5. **return** $\sigma = (\mathbf{u}, \mathbf{z})$

III. Verify$(\mathsf{vk}, m, \sigma = (\mathbf{u}, \mathbf{z}))$ :

1. $c = \mathcal{H}(m||\mathbf{u})$
2. If $\mathbf{z}$ is short and $\mathbf{z}A - c\mathbf{t} == \mathbf{u}$:

   **return** "Accept"

   Else **return** "Reject"

Correctness:

- $\mathbf{z}A - c\mathbf{t} = \mathbf{r}A + c\mathbf{s} \cdot A - c\mathbf{s} \cdot A = \mathbf{r}A$
- $\mathbf{z}$ short since $\mathbf{r}, c, \mathbf{s}$ are short

## Dilithium simplified

$\chi$ – a distribution over $R = \mathbb{Z}_q[x]/(x^{256+1})$ that outputs 'short' polynomials

$\mathcal{H}$ – a cryptographic hash function that outputs short digests

I. KeyGen :

1. $A \leftarrow R_q^{k \times \ell}$
2. $\mathbf{s} \leftarrow \chi^k$
3. $\mathbf{t} = \mathbf{s}A$ Module SIS
4. $\mathsf{vk} = (A, \mathbf{t})$, $\mathsf{sk} = (\mathbf{s}, A, \mathbf{t})$.

II. Sign$(\mathsf{sk}, m)$ :

1. $\mathbf{r} \leftarrow \chi^\ell$
2. $\mathbf{u} = \mathbf{r}A$ Module SIS
3. $c = \mathcal{H}(m||\mathbf{u})$
4. $\mathbf{z} = \mathbf{r} + c\mathbf{s}$ Leaks $\mathbf{s}$! Solution: hide the distribution of $\mathbf{z}$ by rejecting some $\mathbf{z}$
5. **return** $\sigma = (\mathbf{u}, \mathbf{z})$

III. Verify$(\mathsf{vk}, m, \sigma = (\mathbf{u}, \mathbf{z}))$ :

1. $c = \mathcal{H}(m||\mathbf{u})$
2. If $\mathbf{z}$ is short and $\mathbf{z}A - c\mathbf{t} == \mathbf{u}$:
   **return** "Accept"
   Else **return** "Reject"

Correctness:

- $\mathbf{z}A - c\mathbf{t} = \mathbf{r}A + c\mathbf{s} \cdot A - c\mathbf{s} \cdot A = \mathbf{r}A$
- $\mathbf{z}$ short since $\mathbf{r}, c, \mathbf{s}$ are short

## Beyond PKE and Signature

- Constrained PRFs
- Identity-based encryption
- Advanced signature: blind, threshold, ring signatures (often constructions require to modify the assumptions)
- Fully Homomorphic Encryption (very hot topic)
- ... and many more constructions!

## Useful resources

- The lattice club `https://thelatticeclub.com/`
- Cryptography 101 with Alfred Menezes
  `https://cryptography101.ca/lattice-based-cryptography/`
- Lectures of Damien Stehlé
  `https://perso.ens-lyon.fr/damien.stehle/LBCF_course.html`

# References


- [Ajtai'96] M. Ajtai. Generating hard instances of lattice problems
- [FS] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems.
- [GVP08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions.
- [LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings.
- [Regev05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography.
- [SSTX'09] D. Stehlé, R. Steinfeld, K. Tanaka and K. Xagawa. Efficient Public-Key Encryption Based on Ideal Lattices.