Lecture 14 – Short Integer Solutions, lattice signatures, ML-DSA

TEK4500

19.11.2025

Håkon Jacobsen

hakon.jacobsen@its.uio.no

Recap: notation

- **Bold** UPPERCASE: a matrix in $\mathbf{Z}_q^{m \times n}$

$$\mathbf{A} = \begin{pmatrix} 4 & 9 & 11 & 5 \\ 0 & 13 & 7 & 1 \\ 6 & 8 & 1 & 3 \end{pmatrix}$$

- **Bold** lowercase: a *column* vector in $\mathbf{Z}_q^n$

$$\mathbf{v} = \begin{pmatrix} 9 \\ 1 \\ 6 \\ 8 \end{pmatrix}$$

Transpose (row vectors)

$$\mathbf{v}^T = \begin{pmatrix} 9 \\ 1 \\ 6 \\ 8 \end{pmatrix}^T = (9 \quad 1 \quad 6 \quad 8)$$

- Normal lowercase: a value (scalar) in $\mathbf{Z}_q$:

$$c = 18$$

Recap: linear algebra basics

Matrix-vector multiplication

$$\underset{\mathbf{A}}{\begin{pmatrix} 4 & 9 & 11 & 5 \\ 0 & 13 & 7 & 1 \\ 6 & 8 & 1 & 3 \end{pmatrix}} \cdot \underset{\mathbf{v}}{\begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix}} = \underset{\mathbf{y}}{\begin{pmatrix} 4 \cdot v_1 + 9 \cdot v_2 + 11 \cdot v_3 + 5 \cdot v_4 \\ 0 \cdot v_1 + 13 \cdot v_2 + 7 \cdot v_3 + 1 \cdot v_4 \\ 6 \cdot v_1 + 8 \cdot v_2 + 1 \cdot v_3 + 3 \cdot v_4 \end{pmatrix}} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

$$\begin{pmatrix} | & | & | & | \\ \mathbf{a}_1 & \mathbf{a}_2 & \mathbf{a}_3 & \mathbf{a}_4 \\ | & | & | & | \end{pmatrix} \cdot \mathbf{v} = v_1 \cdot \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + v_2 \cdot \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} + v_3 \cdot \begin{pmatrix} | \\ \mathbf{a}_3 \\ | \end{pmatrix} + v_4 \cdot \begin{pmatrix} | \\ \mathbf{a}_4 \\ | \end{pmatrix}$$

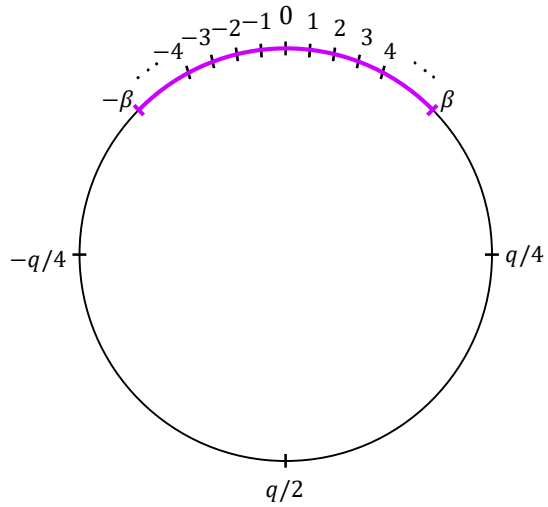
$$\underset{\mathbf{w}^T}{\begin{pmatrix} w_1 & w_2 & w_3 \end{pmatrix}} \underset{\mathbf{A}}{\begin{pmatrix} 4 & 9 & 11 & 5 \\ 0 & 13 & 7 & 1 \\ 6 & 8 & 1 & 3 \end{pmatrix}} = (4 \cdot w_1 + 0 \cdot w_2 + 6 \cdot w_3 \quad \square \quad 5 \cdot w_1 + 1 \cdot w_2 + 3 \cdot w_3) = \underset{\mathbf{z}^T}{(z_1 \quad z_2 \quad z_3 \quad z_4)}$$

$$\mathbf{w}^T \cdot \begin{pmatrix} - & \mathbf{a}_1 & - \\ - & \mathbf{a}_2 & - \\ - & \mathbf{a}_3 & - \end{pmatrix} = \begin{matrix} w_1 \cdot (- & \mathbf{a}_1 & -) \\ & + & \\ w_2 \cdot (- & \mathbf{a}_2 & -) \\ & + & \\ w_3 \cdot (- & \mathbf{a}_3 & -) \end{matrix}$$

Recap: Learning With Errors (LWE)

random in $\mathbf{Z}_q^{m \times n}$ random in $\mathbf{Z}_q^m$ random in $[\pm\beta]^n$ random in $[\pm\beta]^m$

Search LWE problem: Given a LWE sample $(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e})$ find $\mathbf{s}$



Decision LWE problem: Distinguish LWE sample $(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e})$ from random sample $(\mathbf{A}, \widetilde{\mathbf{b}})$

random in $\mathbf{Z}_q^m$

Recap: LWE-KEM

public $\mathbf{A} \in \mathbf{Z}_q^{n \times n}$





$\mathbf{t}^T = \mathbf{s}^T \cdot \mathbf{A} + \mathbf{e}_1^T$

$\mathbf{s} \xleftarrow{\$} [\pm\beta]^n$

$\mathbf{r} \xleftarrow{\$} [\pm\beta]^n$

$\mathbf{u} = \mathbf{A} \cdot \mathbf{r} + \mathbf{e}_2$

$\mathbf{e}_1 \xleftarrow{\$} [\pm\beta]^n$

$\mathbf{e}_2 \xleftarrow{\$} [\pm\beta]^n$

$v = \mathbf{t}^T \cdot \mathbf{r} + e_3 + k \cdot \lceil q/2 \rfloor$

$w \leftarrow v - \mathbf{s}^T \cdot \mathbf{u}$

$e_3 \xleftarrow{\$} [\pm\beta] \quad k \xleftarrow{\$} \{0,1\}$

$$k' \leftarrow \begin{cases} 0 & \text{if } w \approx 0 \\ 1 & \text{if } w \approx q/2 \end{cases}$$

Correct decryption if $2n\beta^2 + \beta < q/4$

Correctness:

$$w = v - \mathbf{s}^T \cdot \mathbf{u} = \cancel{\mathbf{s}^T \cdot \mathbf{A} \cdot \mathbf{r}} + \mathbf{e}_1^T \cdot \mathbf{r} + e_3 + k \cdot \lceil q/2 \rfloor - \cancel{\mathbf{s}^T \cdot \mathbf{A} \cdot \mathbf{r}} - \mathbf{s}^T \cdot \mathbf{e}_2$$

$$= \underbrace{\mathbf{e}_1^T \cdot \mathbf{r} - \mathbf{s}^T \cdot \mathbf{e}_2 + e_3}_{e} + k \cdot \lceil q/2 \rfloor$$

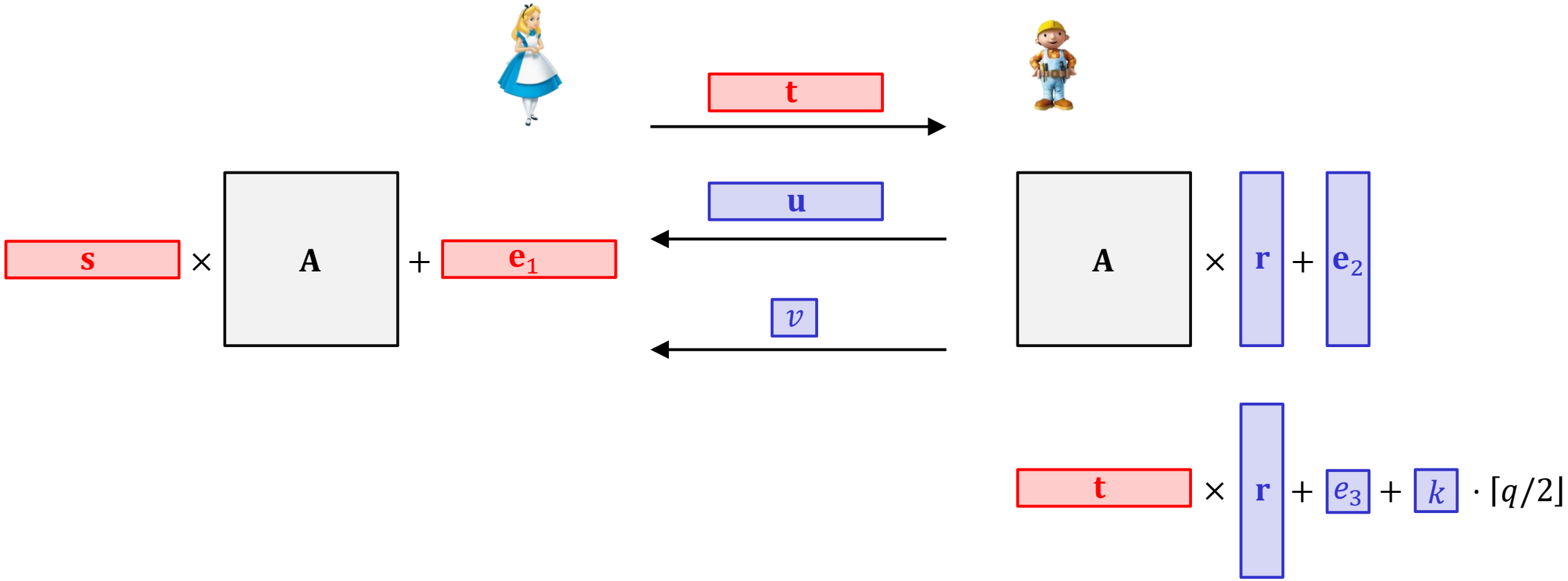
$|\mathbf{e}_1^T \cdot \mathbf{r}| \leq n\beta^2$

$|\mathbf{s}^T \cdot \mathbf{e}_2| \leq n\beta^2$

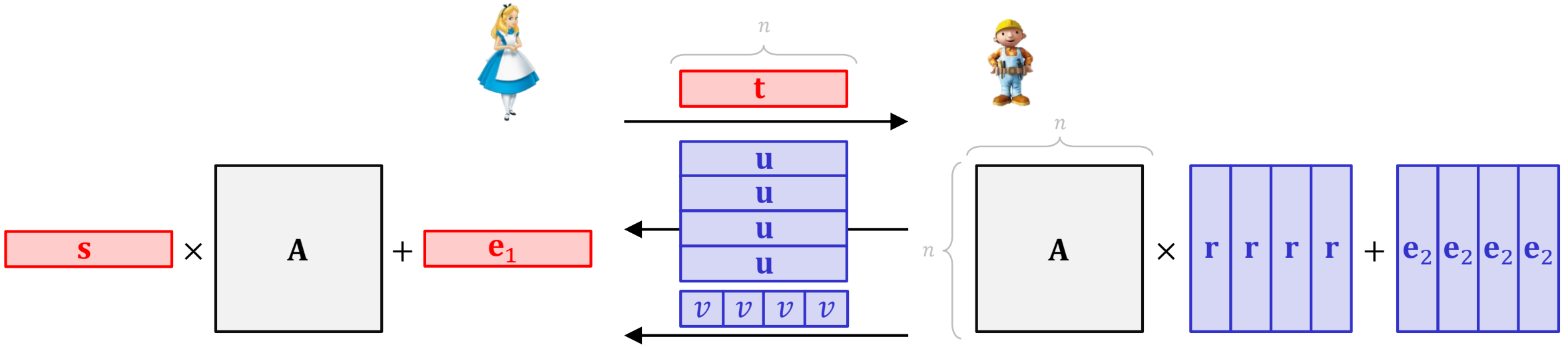
$|e_3| \leq \beta$

$|e| \leq 2n\beta^2 + \beta$

Recap: computational aspects



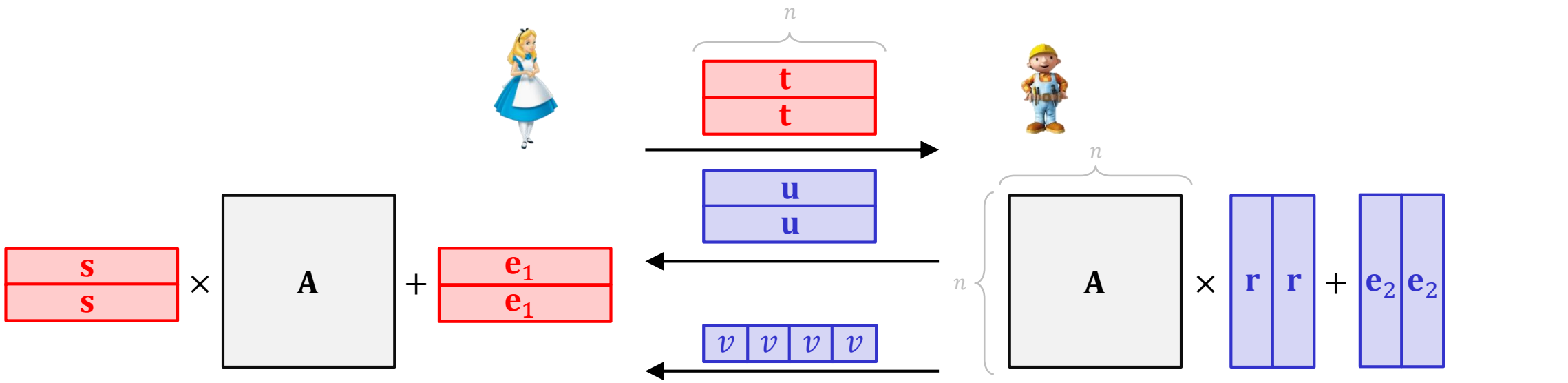
Recap: computational aspects



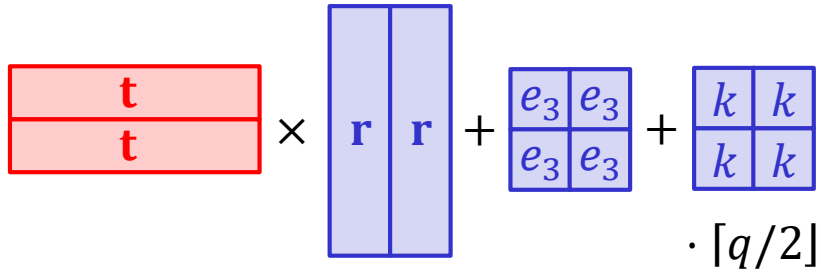
All matrix and vector elements belong to $\mathbf{Z}_q$
hence require $\log_2 q$ bits to represent

		$q \approx 2^{15}$, $n = 640$	$q \approx 2^{16}$, $n = 1344$
Secret key ($\mathbf{s}$):	n elements	≈ 1 kB	≈ 2.7 kB
Public key ($\mathbf{t}$):	n elements	≈ 1 kB	≈ 2.7 kB
Ciphertext ($\mathbf{u}, \mathbf{v}$):	$256 \cdot (n+1)$ elements	≈ 307 kB	≈ 689 kB

Recap: computational aspects

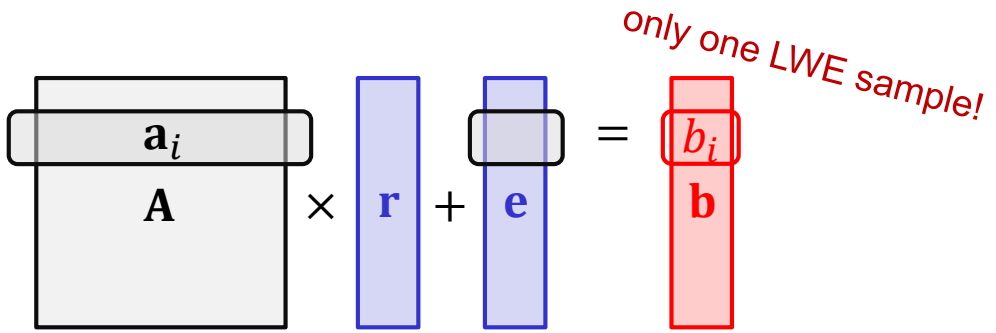


All matrix and vector elements belong to $\mathbf{Z}_q$
hence require $\log_2 q$ bits to represent

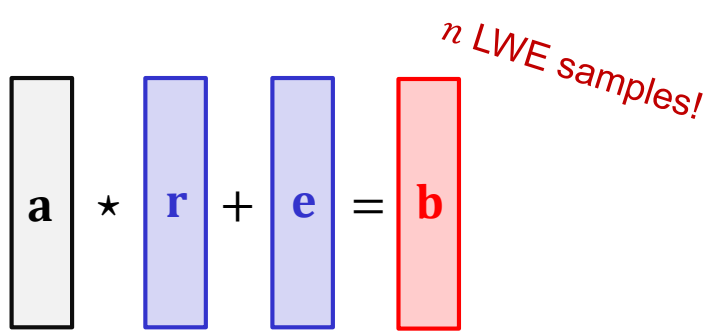


		$q \approx 2^{15}$, $n = 640$	$q \approx 2^{16}$, $n = 1344$
Secret key ($\mathbf{s}$):	$\sqrt{256} \cdot n$ elements	≈ 19.2 kB	≈ 43.0 kB
Public key ($\mathbf{t}$):	$\sqrt{256} \cdot n$ elements	≈ 19.2 kB	≈ 43.0 kB
Ciphertext ($\mathbf{u}, \mathbf{v}$):	$\sqrt{256} \cdot n + 256$ elements	≈ 19.7 kB	≈ 43.5 kB

Making LWE more efficient – Ring-LWE



The dream:



$$\begin{pmatrix} a_{i,0} \\ a_{i,1} \\ \vdots \\ a_{i,n-1} \end{pmatrix}^T \times \begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{n-1} \end{pmatrix}$$

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \star \begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} \in \mathbf{Z}_q^n$$

$$\underbrace{a_{i,0} \cdot r_0 + a_{i,1} \cdot r_1 + \quad \cdots \quad + a_{i,n-1} \cdot r_{n-1} \; + \; e_i}_{n \text{ multiplications } (n \text{ additions})} = b_i \in \mathbf{Z}_q$$

$\mathcal{O}(n^2)$ mults. in total to create whole $\mathbf{b}$

Solution: **polynomials** $a(X) \cdot r(X) + e(X) = b(X)$

$$(a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}) \cdot (r_0 + r_1 X + \cdots + r_{n-1} X^{n-1}) + (e_0 + e_1 X + \cdots e_{n-1} X^{n-1})$$

$$= b_0 + b_1 X + \cdots + b_{n-1} X^{n-1} \pmod{X^n + 1}$$

Naively: still $\mathcal{O}(n^2)$ mults. in total to create $b(X)$

Can be optimized to only $\mathcal{O}(n \cdot \log n)$ mults. with FFT

Plain-LWE vs. Module-LWE vs. Ring-LWE

representing multiplication with *one* polynomial $a(X)$ modulo $X^7 + 1$

Plain-LWE

$$\begin{pmatrix} 4 & 3 & 11 & 12 & 5 & 10 \\ 7 & 0 & 5 & 2 & 3 & 12 \\ 3 & 8 & 2 & 3 & 12 & 9 \\ 11 & 7 & 9 & 7 & 1 & 0 \\ 4 & 9 & 11 & 10 & 8 & 2 \\ 4 & 3 & 9 & 10 & 1 & 12 \end{pmatrix}$$

A

Completely random matrix; no structure

Ring-LWE

$$\begin{pmatrix} 4 & 3 & 11 & 12 & 5 & 10 \\ 10 & 4 & 3 & 11 & 12 & 5 \\ 5 & 10 & 4 & 3 & 11 & 12 \\ 12 & 5 & 10 & 4 & 3 & 11 \\ 11 & 12 & 5 & 10 & 4 & 3 \\ 3 & 11 & 12 & 5 & 10 & 4 \end{pmatrix}$$

A

Each row is the cyclic shift of the row above; lots of structure

Plain-LWE vs. Module-LWE vs. Ring-LWE

representing multiplication with *one* polynomial $a(X)$ modulo $X^7 + 1$

Plain-LWE

$$\begin{pmatrix} 4 & 3 & 11 & 12 & 5 & 10 \\ 7 & 0 & 5 & 2 & 3 & 12 \\ 3 & 8 & 2 & 3 & 12 & 9 \\ 11 & 7 & 9 & 7 & 1 & 0 \\ 4 & 9 & 11 & 10 & 8 & 2 \\ 4 & 3 & 9 & 10 & 1 & 12 \end{pmatrix}$$

$\mathbf{A}$

Completely random matrix; no structure

Module-LWE

$$\left(\begin{array}{ccc|ccc} 4 & 3 & 11 & 12 & 5 & 10 \\ -11 & 4 & 3 & -10 & 12 & 5 \\ -3 & -11 & 4 & -5 & -10 & 12 \\ \hline 11 & 7 & 9 & 6 & 1 & 0 \\ -9 & 11 & 7 & -0 & 6 & 1 \\ -7 & -9 & 11 & -1 & -0 & 6 \end{array}\right)$$

$\mathbf{A}$

"Hybrid" between plain LWE and Ring-LWE

More structure than plain-LWE, less structure than Ring-LWE

Can extra structure be exploited?
Module-LWE assumption: no

Ring-LWE

$$\begin{pmatrix} 4 & 3 & 11 & 12 & 5 & 10 \\ -10 & 4 & 3 & 11 & 12 & 5 \\ -5 & -10 & 4 & 3 & 11 & 12 \\ -12 & -5 & -10 & 4 & 3 & 11 \\ -11 & -12 & -5 & -10 & 4 & 3 \\ -3 & -11 & -12 & -5 & -10 & 4 \end{pmatrix}$$

$\mathbf{A}$

Each row is the cyclic shift of the row above; lots of structure

…with a special wrapping rule:
x wraps to $-x \pmod{13}$

Only need to store one row of $\mathbf{A}$

Can extra structure be exploited?
Ring-LWE assumption: no

ML-KEM (Kyber)

- Standardized LWE-based KEM
  - Selected as the winner of NIST-led competition that began in in 2017
  - Based on Module-LWE
- *Many* optimizations over the simple LWE-KEM scheme
  - Closer to Ring-LWE than Plain-LWE
  - LWE + LWR (Learning With Rounding)
  - Number Theoretic Transform (NTT) for faster (polynomial) multiplication
  - Secret and error sampled from centered binomial distribution over $[\pm\beta]^n$ instead of uniform distribution

	n	q	k	β_1/β_2	$\lvert ek \rvert$ (bytes)	$\lvert dk \rvert$ (bytes)	$\lvert C \rvert$ (bytes)	Failure prob.
ML-KEM-512	256	3329	2	3/2	800	1632	768	$2^{-138.8}$
ML-KEM-768	256	3329	3	2/2	1184	2400	1088	$2^{-164.8}$
ML-KEM-1024	256	3329	4	2/2	1568	3168	1568	$2^{-174.8}$



Check for updates

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

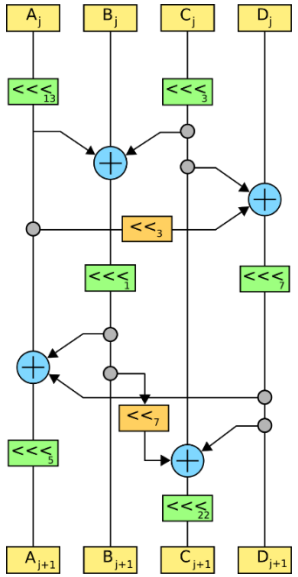
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

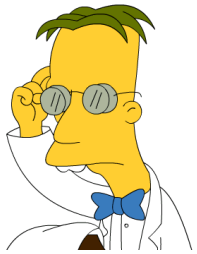
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology



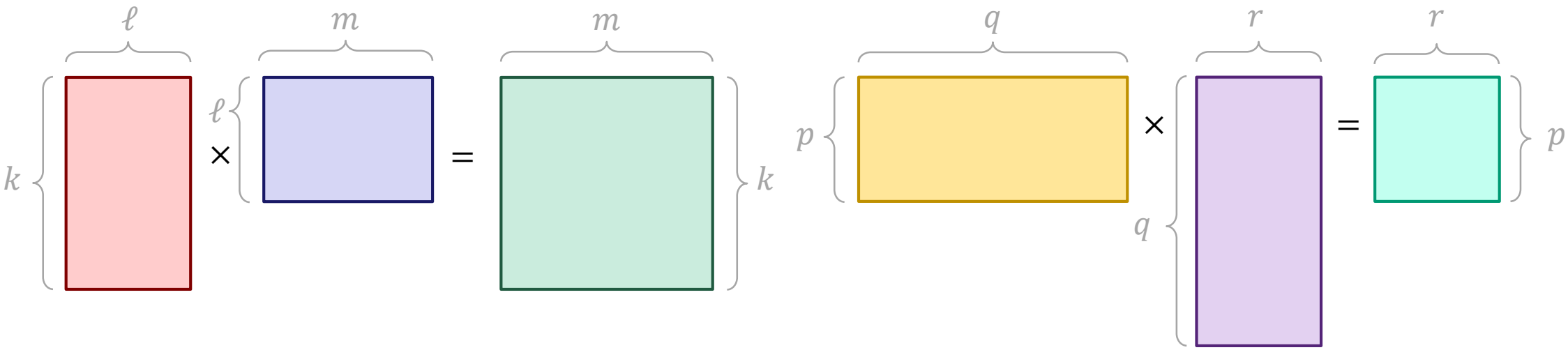


Signatures from lattices

Linear algebra basics

Matrix-matrix multiplication

$$\underset{\mathbf{A}}{\begin{pmatrix} 4 & 9 & 11 & 5 \\ 0 & 13 & 7 & 1 \\ 6 & 8 & 1 & 3 \end{pmatrix}} \cdot \underset{\mathbf{B}}{\begin{pmatrix} 1 & 8 \\ 3 & 7 \\ 12 & 0 \\ 5 & 7 \end{pmatrix}} = \underset{\mathbf{A} \cdot \mathbf{B}}{\begin{pmatrix} 188 & 130 \\ 128 & 98 \\ 57 & 125 \end{pmatrix}}$$



Short Integer Solutions (SIS) problem

SIS problem: Given a random matrix $\mathbf{A} \in \mathbf{Z}_q^{n \times m}$ find a *short vector* $\mathbf{z} \in [\pm\beta]^m$ such that

$$\mathbf{Az} = \mathbf{0} \pmod{q}$$

Inhomogeneous SIS problem (ISIS): Given a random matrix $\mathbf{A} \in \mathbf{Z}_q^{n \times m}$ and a random vector $\mathbf{b} \in \mathbf{Z}_q^n$, find a *short vector* $\mathbf{z} \in [\pm\beta]^m$ such that

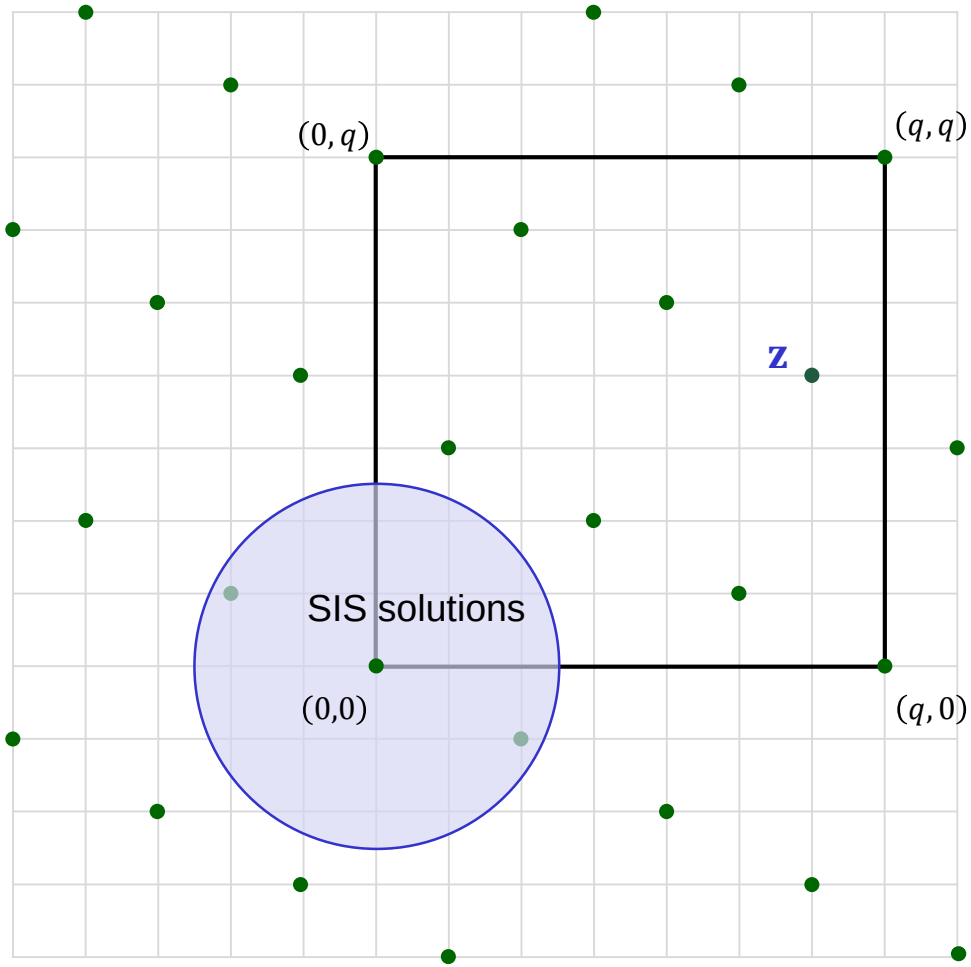
$$\mathbf{Az} = \mathbf{b} \pmod{q}$$

Theorem: The SIS and ISIS problems are computationally equivalent

SIS as a lattice problem

not a basis!

$$\mathcal{L}^{\perp}_{\mathrm{SIS}}(\mathbf{A}) = \left\{ \mathbf{z} \in \mathbf{Z}_q^m \mid \mathbf{Az} = \mathbf{0} \pmod{q} \right\}$$



- **SIS** ≡ average case SVPγ
  - Solution is *not* unique
- Solver SIS ⟹ solver LWE
  - Note: SIS and LWE lattices are different ($\mathcal{L}^{\perp}_{\mathrm{SIS}}(\mathbf{A})$ vs. $\mathcal{L}_{\mathrm{LWE}}(\mathbf{A})$)
- Solver LWE ⟹ solver SIS ?
  - Only a quantum reduction is known

Recap: DLOG proof of knowledge

$A = g^a$ $(\boldsymbol{G}, \star) = \langle g \rangle$





r

$r \xleftarrow{\$} \{1, \dots, |\boldsymbol{G}|\}$

$a + r \pmod{|\boldsymbol{G}|}$

z

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't trick Bob to accept ✓
3. No one (including Bob) learns anything about a from the interaction ✗

Recap: DLOG proof of knowledge

$A = g^a$ $\quad (\boldsymbol{G}, \star) = \langle g \rangle$



$R = g^r$



$r \xleftarrow{\$} \{1, \ldots, |\boldsymbol{G}|\}$

$a + r \pmod{|\boldsymbol{G}|}$

z

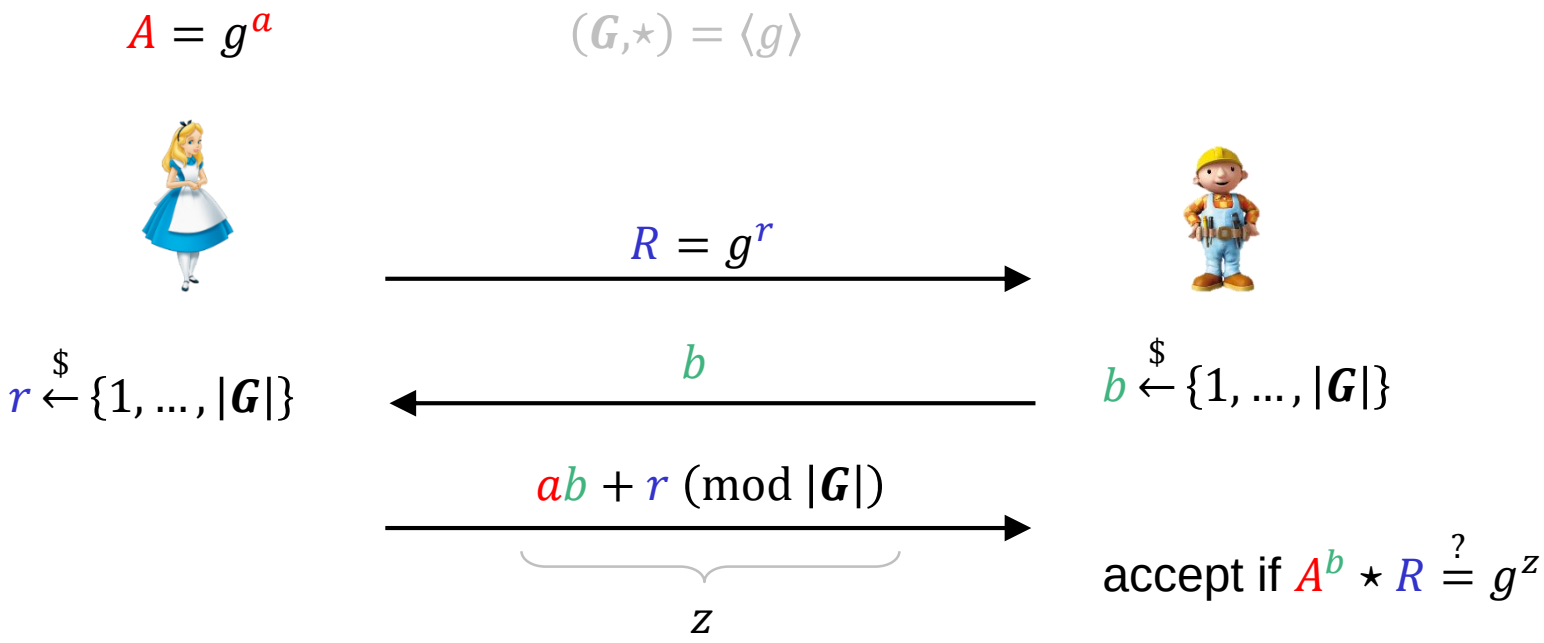
accept if $A \star R \stackrel{?}{=} g^z$

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't trick Bob to accept ✗
3. No one (including Bob) learns anything about a from the interaction ✓

pick z at random then define $R = A^{-b} \star g^z$

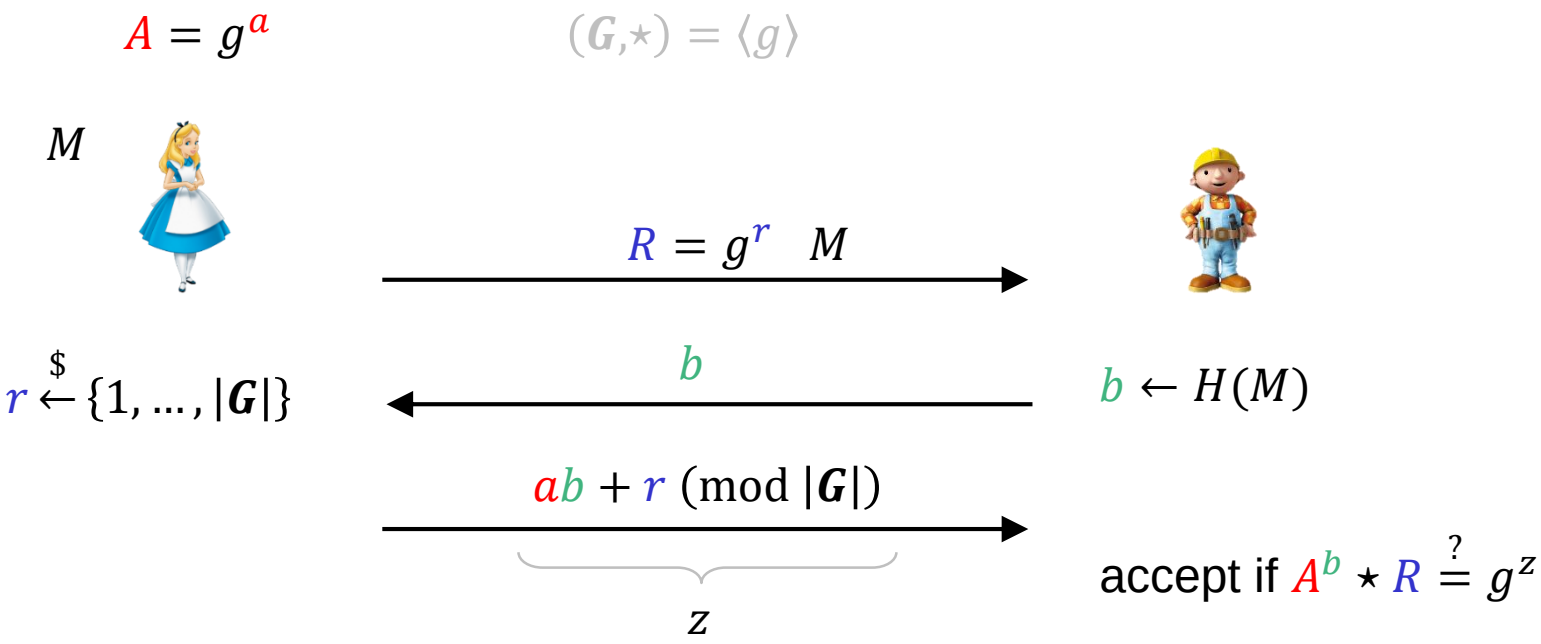
Recap: DLOG proof of knowledge



Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't trick Bob to accept ✓
3. No one (including Bob) learns anything about a from the interaction ✓

Recap: Interactive signature scheme



Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't trick Bob to accept ✓
3. No one (including Bob) learns anything about a from the interaction ✓

Recap: Non-interactive signature scheme

$A = g^a$ $(\boldsymbol{G}, \star) = \langle g \rangle$

M



$R = g^r$

$r \xleftarrow{\$} \{1, \dots, |\boldsymbol{G}|\}$ b

$b \leftarrow H(A, R, M)$ $ab + r \pmod{|\boldsymbol{G}|}$

z

$\sigma = (R, z)$

accept if $A^b \star R \stackrel{?}{=} g^z$ **and** $H(M) = b$

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't trick Bob to accept ✗
3. No one (including Bob) learns anything about a from the interaction ✓

pick z at random then define $R = A^{-b} \star g^z$

Recap: Non-interactive signature scheme (Schnorr)

$A = g^a$ $(\boldsymbol{G}, \star) = \langle g \rangle$

M



$R = g^r$

$r \xleftarrow{\$} \{1, \dots, |\boldsymbol{G}|\}$

$\sigma = (R, z)$

$b \leftarrow H(A, R, M)$

$ab + r \pmod{|\boldsymbol{G}|}$

z

accept if $A^{\overbrace{H(A,R,M)}^{b}} \star R \stackrel{?}{=} g^z$

Proof requirements

1. If Alice knows a she can get Bob to accept ✓
2. If Alice doesn't know a she can't trick Bob to accept ✓
3. No one (including Bob) learns anything about a from the interaction ✓

Lattice-based proof of knowledge

$\mathbf{T} = \mathbf{A}\mathbf{S}_1 + \mathbf{S}_2$ $\quad \mathbf{A} \in \mathbb{Z}_q^{K \times L}$

$\mathbb{Z}_q^{K \times n}$ $\quad [\pm\beta]^{L \times n}$ $\quad [\pm\beta]^{K \times n}$





$\mathbf{w} = \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$ →

$\mathbf{y}_1 \xleftarrow{\$} [\pm\beta]^L$ $\quad \mathbf{y}_2 \xleftarrow{\$} [\pm\beta]^K$

← $\mathbf{c}$

$\mathbf{c} \xleftarrow{\$} \mathbb{Z}_q^n$

$\mathbf{z}_1 = \mathbf{S}_1\mathbf{c} + \mathbf{y}_1$

$\mathbf{z}_2 = \mathbf{S}_2\mathbf{c} + \mathbf{y}_2$ →

no requirements on the lengths of $\mathbf{z}_1, \mathbf{z}_2$

accept if $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{T}\mathbf{c} \stackrel{?}{=} \mathbf{w}$

$\mathbf{A}\cancel{\mathbf{S}_1}\mathbf{c} + \mathbf{A}\mathbf{y}_1 + \cancel{\mathbf{S}_2}\mathbf{c} + \mathbf{y}_2$

$-\mathbf{A}\cancel{\mathbf{S}_1}\mathbf{c} - \cancel{\mathbf{S}_2}\mathbf{c}$

Proof requirements

1. If Alice knows $\mathbf{S}_1$ and $\mathbf{S}_2$ she can get Bob to accept ✓
2. If Alice doesn't know $\mathbf{S}_1$ and $\mathbf{S}_2$ she can't trick Bob to accept ✗
3. No one (including Bob) learns anything about $\mathbf{S}_1$ and $\mathbf{S}_2$ from the interaction

$\mathbf{A}\mathbf{z}_1' + \mathbf{z}_2' = \mathbf{w} + \mathbf{T}\mathbf{c}$

difficult to find by the LWE assumption…or is it?

Lattice-based proof of knowledge

$\mathbf{T} = \mathbf{A}\mathbf{S}_1 + \mathbf{S}_2$ $\quad \mathbf{A} \in \mathbb{Z}_q^{K \times L}$

$\mathbb{Z}_q^{K \times n}$ $\quad [\pm\beta]^{L \times n}$ $\quad [\pm\beta]^{K \times n}$





$\mathbf{w} = \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$ →

$\mathbf{y}_1 \xleftarrow{\$} [\pm\beta]^L$ $\quad \mathbf{y}_2 \xleftarrow{\$} [\pm\beta]^K$

← $\mathbf{c}$

$\mathbf{c} \xleftarrow{\$} \mathbb{Z}_q^n$

$\mathbf{z}_1 = \mathbf{S}_1\mathbf{c} + \mathbf{y}_1$

$\mathbf{z}_2 = \mathbf{S}_2\mathbf{c} + \mathbf{y}_2$ →

accept if $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{T}\mathbf{c} \stackrel{?}{=} \mathbf{w}$

and $\mathbf{z}_1 \in [\pm\beta]^L, \mathbf{z}_2 \in [\pm\beta]^K$

no guarantee that these are small

Proof requirements

1. If Alice knows $\mathbf{S}_1$ and $\mathbf{S}_2$ she can get Bob to accept ✔
2. If Alice doesn't know $\mathbf{S}_1$ and $\mathbf{S}_2$ she can't trick Bob to accept
3. No one (including Bob) learns anything about $\mathbf{S}_1$ and $\mathbf{S}_2$ from the interaction

Lattice-based proof of knowledge

$\mathbf{T} = \mathbf{A}\mathbf{S}_1 + \mathbf{S}_2$ $\quad \mathbf{A} \in \mathbb{Z}_q^{K \times L}$

$\mathbb{Z}_q^{K \times n}$ $\quad [\pm\beta]^{L \times n}$ $\quad [\pm\beta]^{K \times n}$





$\mathbf{w} = \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$ →

$\mathbf{y}_1 \xleftarrow{\$} [\pm\beta]^L$ $\quad \mathbf{y}_2 \xleftarrow{\$} [\pm\beta]^K$

← $\mathbf{c}$

$\mathbf{c} \xleftarrow{\$} \{\mathbf{x} \in [\pm 1]^n, \text{with } \tau \text{ nonzero entries}\}$

$\mathbf{z}_1 = \mathbf{S}_1\mathbf{c} + \mathbf{y}_1$

$\mathbf{z}_2 = \mathbf{S}_2\mathbf{c} + \mathbf{y}_2$ →

accept if $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{T}\mathbf{c} \stackrel{?}{=} \mathbf{w}$

and $\mathbf{z}_1 \in [\pm\beta]^L, \mathbf{z}_2 \in [\pm\beta]^K$

$\|\mathbf{S}_1[i] \cdot \mathbf{c}\| \leq \tau \cdot \beta$

$\|\mathbf{y}_1[i]\| \leq \beta$

$\|\mathbf{z}_1[i]\| \leq \tau \cdot \beta + \beta$

$\gamma \stackrel{\text{def}}{=} \tau \cdot \beta$

Proof requirements

1. If Alice knows $\mathbf{S}_1$ and $\mathbf{S}_2$ she can get Bob to accept
2. If Alice doesn't know $\mathbf{S}_1$ and $\mathbf{S}_2$ she can't trick Bob to accept
3. No one (including Bob) learns anything about $\mathbf{S}_1$ and $\mathbf{S}_2$ from the interaction

Lattice-based proof of knowledge

$\mathbf{T} = \mathbf{A}\mathbf{S}_1 + \mathbf{S}_2$ $\quad \mathbf{A} \in \mathbb{Z}_q^{K \times L}$

$\mathbb{Z}_q^{K \times n}$ $\quad [\pm\beta]^{L \times n}$ $\quad [\pm\beta]^{K \times n}$





$\mathbf{w} = \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$ →

$\mathbf{y}_1 \xleftarrow{\$} [\pm\beta]^L$ $\quad \mathbf{y}_2 \xleftarrow{\$} [\pm\beta]^K$

← $\mathbf{c}$

$\mathbf{c} \xleftarrow{\$} \{\mathbf{x} \in [\pm 1]^n, \text{with } \tau \text{ nonzero entries}\}$

$\mathbf{z}_1 = \mathbf{S}_1\mathbf{c} + \mathbf{y}_1$

$\mathbf{z}_2 = \mathbf{S}_2\mathbf{c} + \mathbf{y}_2$ →

accept if $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{T}\mathbf{c} \stackrel{?}{=} \mathbf{w}$

and $\mathbf{z}_1 \in [\pm 2\gamma]^L, \mathbf{z}_2 \in [\pm 2\gamma]^K$

$$\|\mathbf{S}_1[i] \cdot \mathbf{c}\| \le \tau \cdot \beta$$
$$\|\mathbf{y}_1[i]\| \le \beta$$
$$\|\mathbf{z}_1[i]\| \le \tau \cdot \beta + \beta$$

$\gamma \stackrel{\text{def}}{=} \tau \cdot \beta$

Proof requirements

1. If Alice knows $\mathbf{S}_1$ and $\mathbf{S}_2$ she can get Bob to accept ✓
2. If Alice doesn't know $\mathbf{S}_1$ and $\mathbf{S}_2$ she can't trick Bob to accept
3. No one (including Bob) learns anything about $\mathbf{S}_1$ and $\mathbf{S}_2$ from the interaction ✗

$\mathbf{y}_1$ and $\mathbf{y}_2$ don't completely hide $\mathbf{S}_1\mathbf{c}$ and $\mathbf{S}_2\mathbf{c}$

e.g. $\mathbf{S}_1[i] \cdot \mathbf{c}$ can be larger than $\mathbf{y}_1[i]$

Lattice-based proof of knowledge

$\mathbf{T} = \mathbf{A}\mathbf{S}_1 + \mathbf{S}_2$ $\quad \mathbf{A} \in \mathbb{Z}_q^{K \times L}$

$\mathbb{Z}_q^{K \times n}$ $\quad [\pm\beta]^{L \times n}$ $\quad [\pm\beta]^{K \times n}$



$\beta \ll \bar{\beta}$

$\mathbf{w} = \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$



$\mathbf{y}_1 \xleftarrow{\$} [\pm\bar{\beta}]^L$ $\quad \mathbf{y}_2 \xleftarrow{\$} [\pm\bar{\beta}]^K$

$\mathbf{c}$

$\mathbf{c} \xleftarrow{\$} \{\mathbf{x} \in [\pm 1]^n, \text{with } \tau \text{ nonzero entries}\}$

if $\mathbf{z}_1 \in [\pm\bar{\beta}]^L$ and $\mathbf{z}_2 \in [\pm\bar{\beta}]^K$

$\mathbf{z}_1 = \mathbf{S}_1\mathbf{c} + \mathbf{y}_1$

$\mathbf{z}_2 = \mathbf{S}_2\mathbf{c} + \mathbf{y}_2$

accept if $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{T}\mathbf{c} \stackrel{?}{=} \mathbf{w}$

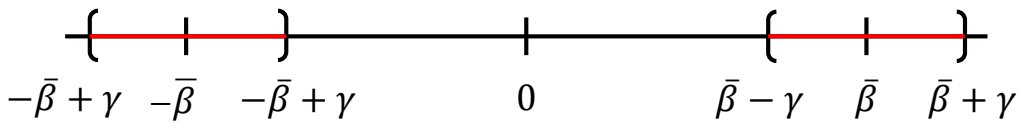
and $\mathbf{z}_1 \in [\pm\bar{\beta}]^L, \mathbf{z}_2 \in [\pm\bar{\beta}]^K$

else **abort**

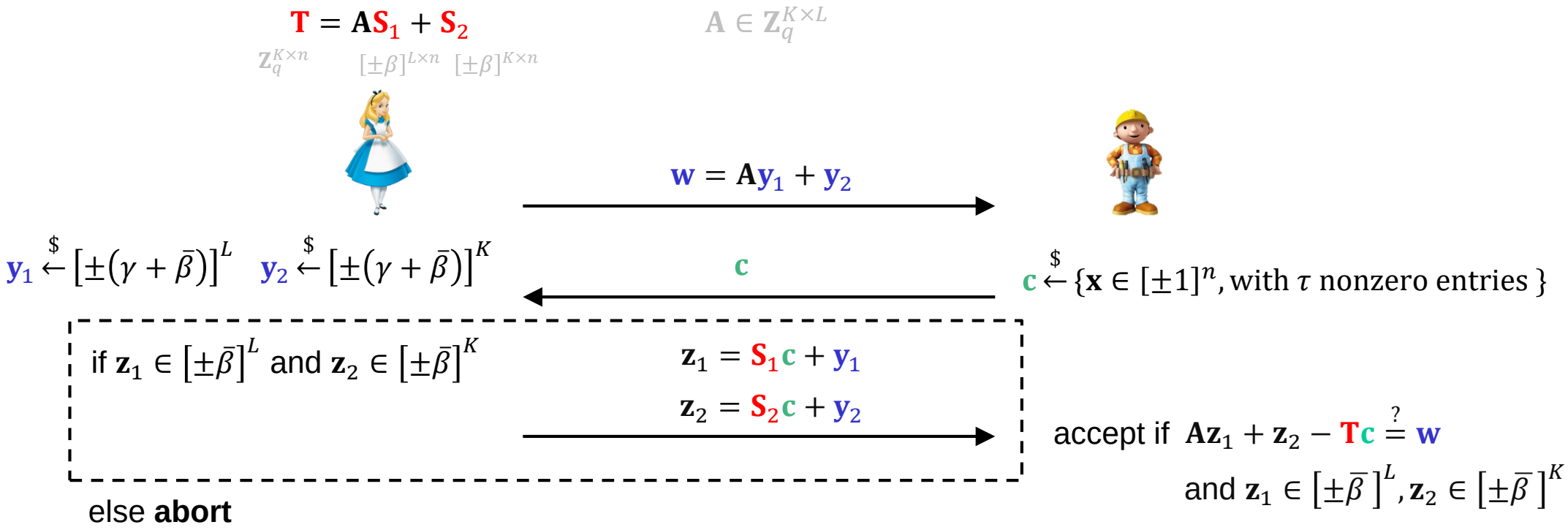
Proof requirements

1. If Alice knows $\mathbf{S}_1$ and $\mathbf{S}_2$ she can get Bob to accept
2. If Alice doesn't know $\mathbf{S}_1$ and $\mathbf{S}_2$ she can't trick Bob to accept
3. No one (including Bob) learns anything about $\mathbf{S}_1$ and $\mathbf{S}_2$ from the interaction





Lattice-based proof of knowledge



Proof requirements

1. If Alice knows $\mathbf{S}_1$ and $\mathbf{S}_2$ she can get Bob to accept ✘
2. If Alice doesn't know $\mathbf{S}_1$ and $\mathbf{S}_2$ she can't trick Bob to accept ✓ tricking Bob ⟹ can solve either LWE or SIS problem
3. No one (including Bob) learns anything about $\mathbf{S}_1$ and $\mathbf{S}_2$ from the interaction ✓ (assuming no abort)

Lattice-based signatures

$\mathbf{T} = \mathbf{A}\mathbf{S}_1 + \mathbf{S}_2$ $\quad \mathbf{A} \in \mathbb{Z}_q^{K \times L}$

$\mathbb{Z}_q^{K \times n}$ $\quad [\pm\beta]^{L \times n}$ $\quad [\pm\beta]^{K \times n}$

M



$\mathbf{y}_1 \xleftarrow{\$} [\pm(\gamma + \bar{\beta})]^L$

$\mathbf{y}_2 \xleftarrow{\$} [\pm(\gamma + \bar{\beta})]^K$

$\mathbf{w} = \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$

$\mathbf{c} \leftarrow H(\mathbf{T}, \mathbf{w}, M)$

$\mathbf{z}_1 \leftarrow \mathbf{S}_1\mathbf{c} + \mathbf{y}_1$

$\mathbf{z}_2 \leftarrow \mathbf{S}_2\mathbf{c} + \mathbf{y}_2$

if $\mathbf{z}_1 \notin [\pm\bar{\beta}]^L$ or $\mathbf{z}_2 \notin [\pm\bar{\beta}]^K$:
try again

$\mathbf{w}$ →

$\mathbf{c}$ →

$\mathbf{z}_1, \mathbf{z}_2$ →



accept if $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{T}\mathbf{c} \stackrel{?}{=} \mathbf{w}$

and $\mathbf{z}_1 \in [\pm\bar{\beta}]^L, \mathbf{z}_2 \in [\pm\bar{\beta}]^K$

Proof requirements

1. If Alice knows $\mathbf{S}_1$ and $\mathbf{S}_2$ she can get Bob to accept ✓
2. If Alice doesn't know $\mathbf{S}_1$ and $\mathbf{S}_2$ she can't trick Bob to accept ✓ tricking Bob ⟹ can solve either LWE or SIS problem
3. No one (including Bob) learns anything about $\mathbf{S}_1$ and $\mathbf{S}_2$ from the interaction ✓ (assuming no abort)

Lattice-based signatures

$\mathbf{T} = \mathbf{A}\mathbf{S}_1 + \mathbf{S}_2$ $\quad \mathbf{A} \in \mathbb{Z}_q^{K \times L}$

$\mathbb{Z}_q^{K \times n}$ $\quad [\pm\beta]^{L \times n}$ $\quad [\pm\beta]^{K \times n}$

M





$\mathbf{y}_1 \xleftarrow{\$} [\pm(\gamma + \bar{\beta})]^L$

$\mathbf{y}_2 \xleftarrow{\$} [\pm(\gamma + \bar{\beta})]^K$

$\mathbf{w} = \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$

$\mathbf{c} \leftarrow H(\mathbf{T}, \mathbf{w}, M)$

$\mathbf{z}_1 \leftarrow \mathbf{S}_1\mathbf{c} + \mathbf{y}_1$

$\mathbf{z}_2 \leftarrow \mathbf{S}_2\mathbf{c} + \mathbf{y}_2$

if $\mathbf{z}_1 \notin [\pm\bar{\beta}]^L$ or $\mathbf{z}_2 \notin [\pm\bar{\beta}]^K$:
try again

$\mathbf{c}$ →

$\mathbf{z}_1, \mathbf{z}_2$ →

accept if $H(\mathbf{T}, \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - \mathbf{T}\mathbf{c}, M) \stackrel{?}{=} \mathbf{c}$

and $\mathbf{z}_1 \in [\pm\bar{\beta}]^L, \mathbf{z}_2 \in [\pm\bar{\beta}]^K$

Proof requirements

1. If Alice knows $\mathbf{S}_1$ and $\mathbf{S}_2$ she can get Bob to accept ✓
2. If Alice doesn't know $\mathbf{S}_1$ and $\mathbf{S}_2$ she can't trick Bob to accept ✓ tricking Bob ⟹ can solve either LWE or SIS problem
3. No one (including Bob) learns anything about $\mathbf{S}_1$ and $\mathbf{S}_2$ from the interaction ✓ (assuming no abort)

ML-DSA (Dilithium)

- Standardized Lattice-based signature scheme
  - Selected as the winner of NIST-led competition that began in in 2017
  - Based on Module-LWE/SIS
- *Many* optimizations over the previous signature scheme
  - Closer to Ring-LWE than Plain-LWE
  - Number Theoretic Transform (NTT) for faster (polynomial) multiplication
  - Compresses signing key, verification key, and signature

	q	$k l \ell$	$\beta / \bar{\beta}$	$\gamma = \tau\beta$	τ	$\|sk\|$ (bytes)	$\|vk\|$ (bytes)	$\|sig\|$ (bytes)	Expected loop reps.
ML-DSA-44	8380417	4/4	$2 / 2^{17}$	78	80	2560	1312	2420	4.25
ML-DSA-65	8380417	6/5	$4 / 2^{19}$	196	55	4032	1952	3309	5.1
ML-DSA-87	8380417	8/7	$2 / 2^{19}$	120	75	4896	2592	4627	3.85



Check for updates

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

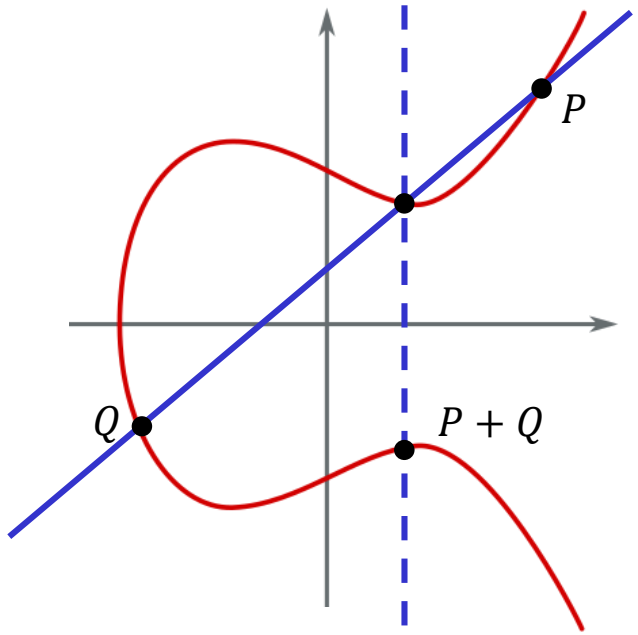
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.204

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology



$y^2 = x^3 + ax + b$

$a, b, x, y \in \mathbf{R}$

End of Part II

(Asymmetric crypto)

Summary of asymmetric cryptography

Primitive	Functionality + syntax	Hardness assumption / security goal	Acronym	Examples
Diffie-Hellman	Derive shared value (key) in a cyclic group $A^b = g^{ab} = B^a$	Discrete logarithm (DLOG) Diffie-Hellman (DH)	DH	$(\boldsymbol{Z}_p^*, \cdot)$ −DH $(E(\boldsymbol{F}_p), +)$ −DH
Public-key encryption (PKE)	Encrypt variable-length input $\mathrm{Enc} : \mathcal{PK} \times \mathcal{M} \to \mathcal{C}$	Confidentiality: attacker should learn nothing about plaintext (except length) from ciphertexts	IND-CPA IND-CCA	ElGamal Fujisaki-Okomoto-transform
Key Encapsulation mechanism (KEM)	Distribute symmetric key $K \in \mathcal{K}$ $\mathrm{Encaps} : \mathcal{EK} \to \mathcal{K} \times \mathcal{C}$ $\mathrm{Decaps} : \mathcal{DK} \times \mathcal{C} \to \mathcal{K} \cup \{\perp\}$	Confidentiality: attacker should learn nothing about symmetric key from ciphertexts	IND-CPA IND-CCA	ElGamal ML-KEM, Fujisaki-Okomoto-transform
Digital signatures	Create signature on variable length input $\mathrm{Sign} : \mathcal{SK} \times \mathcal{M} \to \mathcal{S}$ $\mathrm{Vrfy} : \mathcal{VK} \times \mathcal{M} \times \mathcal{S} \to \{1,0\}$	Integrity: attacker shouldn't be able to forge messages, i.e., create new messages with valid signatures	UF-CMA	Schnorr, ECDSA, ML-DSA

Summary of asymmetric cryptography

Computational problem / assumption	Description	Best-known attacks	Common sizes	Comment
Discrete logarithm (DLOG)	Given $g, A = g^a$ find a	General number field sieve (GNFS) for $(\mathbf{Z}_p^*, \cdot)$ Generic algorithms for $(E(\boldsymbol{F}_q), +)$, e.g., Baby-Step Giant-Step, Pollards-rho, etc.	$\lvert\mathbf{Z}_p^*\rvert \approx 2^{2000}$ to 2^{4000} $\lvert E(\boldsymbol{F}_q)\rvert \approx 2^{256}$ to 2^{512}	Solvable by Shor's algorithm
Diffie-Hellman (DH)	Given $g, A = g^a, B = g^b$ find g^{ab}	Same as DLOG		Solvable by Shor's algorithm
Learning With Errors (LWE)	Given $(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e})$, where $\mathbf{e}$ (and possibly $\mathbf{s}$) are short vectors, find $\mathbf{s}$	Algorithms for solving lattice problems (SVP_γ, CVP_γ, BDD_γ, etc.)	$n \approx 600$ to 1500 (secret dimension) $q \approx 2^{16}$ to 2^{30} (modulus) $\beta \approx 2$ to 2^{16} (error size)	Variants: Ring-LWE, Module-LWE
Decisional LWE	Distinguish real LWE samples $(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e})$ from random samples $(\mathbf{A}, \tilde{\mathbf{b}})$	Same as LWE		Equivalent to search LWE (for plain LWE)

Summary of asymmetric cryptography

Computational problem / assumption	Description	Best-known attacks	Common sizes	Comment
Short Integer Solutions	Given $\mathbf{A}$ find a *short* vector $\mathbf{z}$ such that $\mathbf{Az} = \mathbf{0} \pmod q$	Same as LWE		Variants: *Inhomogeneous* SIS (given $\mathbf{A}, \mathbf{b}$ find a *short* vector $\mathbf{z}$ such that $\mathbf{Az} = \mathbf{b} \pmod q$
(Approximate) Shortest Vector Problem (SVP_γ)	Given a lattice $\mathcal{L}(\mathbf{B})$ find a nonzero vector $\mathbf{v}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda(\mathcal{L})$	LLL and newer variants, such as BKZ	$n = 600$ to 1000 (lattice dimension)	$\mathbf{B}$ is a basis for the lattice $\lambda(\mathcal{L})$ is the length of the shortest nonzero vector in the lattice
(Approximate) Closest Vector Problem (CVP_γ)	Given a lattice $\mathcal{L}(\mathbf{B})$ and a point $\mathbf{t}$ *not* on the lattice, find a lattice point $\mathbf{v}$ such that $\|\mathbf{t} - \mathbf{v}\| \leq \gamma \cdot \mathrm{dist}(\mathbf{t}, \mathcal{L})$	Same as SVP_γ		$\mathrm{dist}(\mathbf{t}, \mathcal{L})$ is the distance from $\mathbf{t}$ to the closest vector in the lattice
(Approximate) Bounded Distance Decoding (BDD_γ)	Same as CVP_γ, but where $\mathbf{t}$ is guaranteed to be close to a lattice point, i.e., $\mathrm{dist}(\mathbf{t}, \mathcal{L}) \leq \lambda(\mathcal{L})/2\gamma$	Same as SVP_γ		$\mathrm{dist}(\mathbf{t}, \mathcal{L})$ is the distance from $\mathbf{t}$ to the closest vector point

Next week

- **Guest lecture** by Hagen Echzell
  - Topic: end-to-end encryption in group messaging protocols

- **Course recap**
  - Mini-lecture summarizing the main topics covered this year

- Going through old exams