Introduction to lattice cryptography

Damien Stehlé

ENS Lyon

Edinburgh, July 2022

Plan for this lecture

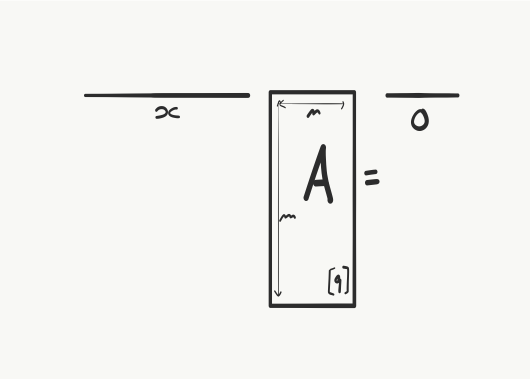
1. **Signing from SIS**
2. Improving efficiency
3. NTRU

$\mathrm{SIS}_{\beta,q,m}$

The Small Integer Solution Problem

Given a uniform $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, find $\mathbf{x} \in \mathbb{Z}^m$ such that:

$$0 < \|\mathbf{x}\| \leq \beta \quad \text{and} \quad \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0} \bmod q.$$



Design principle

Start from a one-way function $x \mapsto y = f(x)$.

- Signing key: x
- Verification key: y

The signer uses a zero-knowledge proof that it knows x s.t. $f(x) = y$.

The random oracle methodology allows to:

- Make the proof non-interactive
- Embed the message in the proof challenge

This is the (heuristic) **Fiat-Shamir transform**.

Which one-way function to start from?

The Short Integer Solution Problem

Given a uniform $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m$ such that:

$$0 < \|\mathbf{x}\| \leq \beta \quad \text{and} \quad \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0} \bmod q.$$

We want a function that is easy to evaluate and (SIS-)hard to invert.

$$f_{\mathbf{A}} : \begin{array}{ccc} \{-B, \ldots, B\}^m & \to & \mathbb{Z}_q^n \\ \mathbf{x} & \mapsto & \mathbf{x}^T \cdot \mathbf{A} \bmod q \end{array}$$

Why is it hard to invert?

- Let $\mathbf{A}$ be a SIS instance.
- Sample $\mathbf{x} \hookleftarrow U(\{-B, \ldots, B\})^m$, set $\mathbf{y} = \mathbf{x}^T \cdot \mathbf{A}$.
- Adversary gets $\mathbf{A}$ and $\mathbf{y}$, and gives back a pre-image $\mathbf{x}'$ of $\mathbf{y}$.
- Claim: $\mathbf{x} - \mathbf{x}'$ is a SIS_β solution for $\beta = 2B$ (with high probability).

Which one-way function to start from?

The Short Integer Solution Problem

Given a uniform $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m$ such that:

$$0 < \|\mathbf{x}\| \leq \beta \quad \text{and} \quad \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0} \bmod q.$$

We want a function that is easy to evaluate and (SIS-)hard to invert.

$$f_{\mathbf{A}} : \begin{array}{ccc} \{-B, \ldots, B\}^m & \to & \mathbb{Z}_q^n \\ \mathbf{x} & \mapsto & \mathbf{x}^T \cdot \mathbf{A} \bmod q \end{array}$$

Why is it hard to invert?

- Let $\mathbf{A}$ be a SIS instance.
- Sample $\mathbf{x} \hookleftarrow U(\{-B, \ldots, B\})^m$, set $\mathbf{y} = \mathbf{x}^T \cdot \mathbf{A}$.
- Adversary gets $\mathbf{A}$ and $\mathbf{y}$, and gives back a pre-image $\mathbf{x}'$ of $\mathbf{y}$.
- Claim: $\mathbf{x} - \mathbf{x}'$ is a SIS_β solution for $\beta = 2B$ (with high probability).

Which one-way function to start from?

The Short Integer Solution Problem

Given a uniform $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m$ such that:

$$0 < \|\mathbf{x}\| \leq \beta \quad \text{and} \quad \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0} \bmod q.$$

We want a function that is easy to evaluate and (SIS-)hard to invert.

$$f_{\mathbf{A}} : \begin{array}{ccc} \{-B, \ldots, B\}^m & \to & \mathbb{Z}_q^n \\ \mathbf{x} & \mapsto & \mathbf{x}^T \cdot \mathbf{A} \bmod q \end{array}$$

Why is it hard to invert?

- Let $\mathbf{A}$ be a SIS instance.
- Sample $\mathbf{x} \hookleftarrow U(\{-B, \ldots, B\})^m$, set $\mathbf{y} = \mathbf{x}^T \cdot \mathbf{A}$.
- Adversary gets $\mathbf{A}$ and $\mathbf{y}$, and gives back a pre-image $\mathbf{x}'$ of $\mathbf{y}$.
- Claim: $\mathbf{x} - \mathbf{x}'$ is a SIS_β solution for $\beta = 2B$ (with high probability).

Proof of knowledge for the SIS one-way function

Prover wants to convince **Verifier** that it knows $\mathbf{s}$ small s.t.:
$\mathbf{s}^T \cdot \mathbf{A} = \mathbf{t}^T$, where $\mathbf{A}$ and $\mathbf{t}$ are known.

Prover generates a blinding equation:

$$\mathbf{y}^T \cdot \mathbf{A} = \mathbf{w}^T,$$

with $\mathbf{y}$ small. It sends $\mathbf{w}$ to **Verifier**.

After receiving $\mathbf{w}$, **Verifier** sends a challenge $c \in \mathbb{Z}$ small to **Prover**.

Prover replies with $\mathbf{y} + c \cdot \mathbf{s}$.

Verifier checks whether

$$\mathbf{y} + c \cdot \mathbf{s} \quad \text{is small and} \quad (\mathbf{y} + c \cdot \mathbf{s})^T \mathbf{A} = \mathbf{w}^T + c\mathbf{t}^T.$$

Proof of knowledge for the SIS one-way function

Prover wants to convince **Verifier** that it knows $\mathbf{s}$ small s.t.:
$\mathbf{s}^T \cdot \mathbf{A} = \mathbf{t}^T$, where $\mathbf{A}$ and $\mathbf{t}$ are known.

Prover generates a blinding equation:

$$\mathbf{y}^T \cdot \mathbf{A} = \mathbf{w}^T,$$

with $\mathbf{y}$ small. It sends $\mathbf{w}$ to **Verifier**.

After receiving $\mathbf{w}$, **Verifier** sends a challenge $c \in \mathbb{Z}$ small to **Prover**.

Prover replies with $\mathbf{y} + c \cdot \mathbf{s}$.

Verifier checks whether

$$\mathbf{y} + c \cdot \mathbf{s} \ \text{ is small and } \ (\mathbf{y} + c \cdot \mathbf{s})^T \mathbf{A} = \mathbf{w}^T + c\mathbf{t}^T.$$

Challenge space is too small:
Prover can guess c and succeed without knowing $\mathbf{s}$.

Proof of knowledge for the SIS one-way function

Prover wants to convince **Verifier** that it knows $\mathbf{s}$ small s.t.:
$\mathbf{s}^T \cdot \mathbf{A} = \mathbf{t}^T$, where $\mathbf{A}$ and $\mathbf{t}$ are known.

Prover generates a blinding equation:

$$\mathbf{y}^T \cdot \mathbf{A} = \mathbf{w}^T,$$

with $\mathbf{y}$ small. It sends $\mathbf{w}$ to **Verifier**.

After receiving $\mathbf{w}$, **Verifier** sends a challenge $c \in \mathbb{Z}$ small to **Prover**.

Prover replies with $\mathbf{y} + c \cdot \mathbf{s}$.

Verifier checks whether

$$\mathbf{y} + c \cdot \mathbf{s} \ \text{ is small and } \ (\mathbf{y} + c \cdot \mathbf{s})^T \mathbf{A} = \mathbf{w}^T + c\mathbf{t}^T.$$

Challenge space is too small:
Prover can guess c and succeed without knowing $\mathbf{s}$.

Proof of knowledge for the SIS one-way function

Prover wants to convince **Verifier** that it knows $\mathbf{s}$ small s.t.:
$\mathbf{s}^T \cdot \mathbf{A} = \mathbf{t}^T$, where $\mathbf{A}$ and $\mathbf{t}$ are known.

Prover generates a blinding equation:

$$\mathbf{y}^T \cdot \mathbf{A} = \mathbf{w}^T,$$

with $\mathbf{y}$ small. It sends $\mathbf{w}$ to **Verifier**.

After receiving $\mathbf{w}$, **Verifier** sends a challenge $c \in \mathbb{Z}$ small to **Prover**.

Prover replies with $\mathbf{y} + c \cdot \mathbf{s}$.

Verifier checks whether

$$\mathbf{y} + c \cdot \mathbf{s} \ \text{ is small and } \ (\mathbf{y} + c \cdot \mathbf{s})^T \mathbf{A} = \mathbf{w}^T + c\mathbf{t}^T.$$

Challenge space is too small:
Prover can guess c and succeed without knowing $\mathbf{s}$.

Proof of knowledge for the SIS one-way function

Prover wants to convince **Verifier** that it knows $\mathbf{s}$ small s.t.:
$\mathbf{s}^T \cdot \mathbf{A} = \mathbf{t}^T$, where $\mathbf{A}$ and $\mathbf{t}$ are known.

Prover generates a blinding equation:

$$\mathbf{y}^T \cdot \mathbf{A} = \mathbf{w}^T,$$

with $\mathbf{y}$ small. It sends $\mathbf{w}$ to **Verifier**.

After receiving $\mathbf{w}$, **Verifier** sends a challenge $c \in \mathbb{Z}$ small to **Prover**.

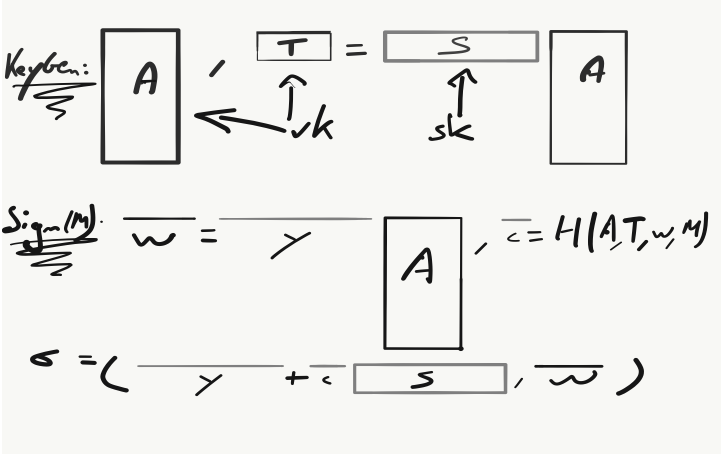
Prover replies with $\mathbf{y} + c \cdot \mathbf{s}$.

Verifier checks whether

$$\mathbf{y} + c \cdot \mathbf{s} \text{ is small and } (\mathbf{y} + c \cdot \mathbf{s})^T \mathbf{A} = \mathbf{w}^T + c\mathbf{t}^T.$$

Challenge space is too small:
Prover can guess c and succeed without knowing $\mathbf{s}$.

SIS-based signature, 1st attempt



Verify: accept iff $\|\sigma_1\|$ is small and $\sigma_1^T \mathbf{A} = \mathbf{w}^T + \mathbf{c}^T \mathbf{T}$.

This signature scheme is insecure but can be fixed

Assume for simplicity that the coefficients of $\mathbf{S}$, $\mathbf{c}$ and $\mathbf{y}$ are iid uniform in the interval $[-B, +B]$, where $B \ll q$.

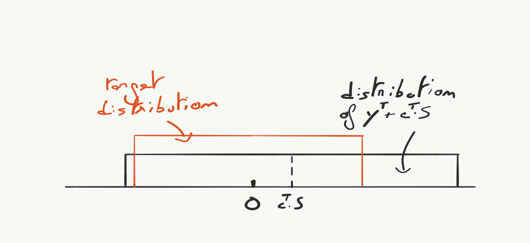
$\sigma_1^T = \mathbf{y}^T + \mathbf{c}^T \cdot \mathbf{S}$ conditioned on $\mathbf{c}$ and $\mathbf{S}$, has center $\mathbf{c}^T \cdot \mathbf{S}$.

This signature scheme is insecure but can be fixed

Assume for simplicity that the coefficients of $\mathbf{S}$, $\mathbf{c}$ and $\mathbf{y}$ are iid uniform in the interval $[-B, +B]$, where $B \ll q$.

$\sigma_1^T = \mathbf{y}^T + \mathbf{c}^T \cdot \mathbf{S}$ conditioned on $\mathbf{c}$ and $\mathbf{S}$, has center $\mathbf{c}^T \cdot \mathbf{S}$.

Fix: use **rejection sampling** [Lyu09,Lyu12]



- For uniform distributions in intervals, rejection is simple
- Need to restart signing process, if rejection occurs

Security proof intuition (in the random oracle model)

To answer signing queries, the challenger simulates by sampling σ_1 and $\mathbf{c}$ from their distributions, and **defines**

$$H(\mathbf{A}, \mathbf{T}, \mathbf{w} = \sigma_1 \mathbf{A} - \mathbf{c}\mathbf{T}, M) := \mathbf{c}$$

$\Rightarrow$ No need for a signing key anymore! Simply set $\mathbf{T}$ uniform.

By **rewinding** a forging algorithm $\mathcal{A}$ and **reprogramming** H, we obtain:

$$\begin{aligned} \sigma_1^T \mathbf{A} &= \mathbf{w}^T + \mathbf{c}^T \mathbf{T} \\ \sigma_1'^T \mathbf{A} &= \mathbf{w}^T + \mathbf{c}'^T \mathbf{T} \end{aligned}$$

Subtracting gives a SIS solution to instance $(\mathbf{A} \| \mathbf{T})$.

This is Schnorr's signature (and its proof) adapted to SIS!

Security proof intuition (in the random oracle model)

To answer signing queries, the challenger simulates by sampling σ_1 and $\mathbf{c}$ from their distributions, and **defines**

$$H(\mathbf{A}, \mathbf{T}, \mathbf{w} = \sigma_1 \mathbf{A} - \mathbf{c}\mathbf{T}, M) := \mathbf{c}$$

$\Rightarrow$ No need for a signing key anymore! Simply set $\mathbf{T}$ uniform.

By **rewinding** a forging algorithm $\mathcal{A}$ and **reprogramming** H, we obtain:

$$\begin{aligned} \sigma_1^T \mathbf{A} &= \mathbf{w}^T + \mathbf{c}^T \mathbf{T} \\ \sigma_1'^T \mathbf{A} &= \mathbf{w}^T + \mathbf{c}'^T \mathbf{T} \end{aligned}$$

Subtracting gives a SIS solution to instance $(\mathbf{A} \| \mathbf{T})$.

This is Schnorr's signature (and its proof) adapted to SIS!

Security proof intuition (in the random oracle model)

To answer signing queries, the challenger simulates by sampling σ_1 and $\mathbf{c}$ from their distributions, and **defines**

$$H(\mathbf{A}, \mathbf{T}, \mathbf{w} = \sigma_1 \mathbf{A} - \mathbf{c}\mathbf{T}, M) := \mathbf{c}$$

$\Rightarrow$ No need for a signing key anymore! Simply set $\mathbf{T}$ uniform.

By **rewinding** a forging algorithm $\mathcal{A}$ and **reprogramming** H, we obtain:

$$\begin{aligned} \sigma_1^T \mathbf{A} &= \mathbf{w}^T + \mathbf{c}^T \mathbf{T} \\ \sigma_1'^T \mathbf{A} &= \mathbf{w}^T + \mathbf{c}'^T \mathbf{T} \end{aligned}$$

Subtracting gives a SIS solution to instance $(\mathbf{A} \| \mathbf{T})$.

This is Schnorr's signature (and its proof) adapted to SIS!

Further remarks

- Setting parameters requires work. Compromises between:
  - Security
  - Probability of rejection (and hence signing time)
  - Size of signatures
- Further improvement: rely on LWE to use a shorter $\mathbf{S}$.
  - Shorter $\mathbf{S}$ $\Rightarrow$ shorter $\mathbf{y}$ $\Rightarrow$ smaller signatures
  - Security proof can be made tight

- Efficient variant of Lyubashevsky's signature without rejection.
- Precise comparison to GPV-type signatures.
- Efficient signature without the random oracle heuristic.

Further remarks

- Setting parameters requires work. Compromises between:
  - Security
  - Probability of rejection (and hence signing time)
  - Size of signatures
- Further improvement: rely on LWE to use a shorter $\mathbf{S}$.
  - Shorter $\mathbf{S}$ $\Rightarrow$ shorter $\mathbf{y}$ $\Rightarrow$ smaller signatures
  - Security proof can be made tight

- Efficient variant of Lyubashevsky's signature without rejection.
- Precise comparison to GPV-type signatures.
- Efficient signature without the random oracle heuristic.

Plan for this lecture

1. Signing from SIS
2. **Improving efficiency**
3. NTRU

It's all big and slow

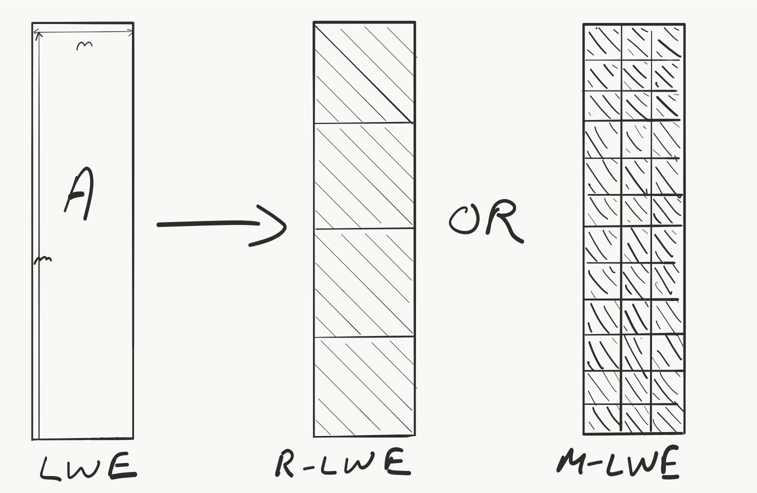
Public key contains a uniformly sampled matrix $\mathbf{A}$.

- Share $\mathbf{A}$ among users
  (but maybe an adversary can work on $\mathbf{A}$ to break all keys)
- Store only the seed of the randomness used to sample $\mathbf{A}$.

Encrypting, Signing and Verifying require matrix-vector multiplication.

Encryption is only for bits.

Replace matrices by structured matrices



Ring-LWE, Module-LWE

Structured matrices $\Leftrightarrow$ Polynomials

This allows us to exploit fast polynomial arithmetic.

The encryption scheme we saw still works. But:

- (Matrix $\times$ vector) is replaced by (polynomial $\times$ polynomial)
- Encryption of a bit is replaced by encryption of a binary polynomial

$\Rightarrow$ Quasi-optimal efficiency: handling n plaintext bits costs $\widetilde{O}(n)$.

What about security?

Ideal/Polynomial-SIS [LM06,PR06]

Let $q \geq 2$, $\beta > 0$, $m > 0$. Let $f = x^n + 1 \in \mathbb{Z}[x]$ with $n = 2^k$.

Ideal-SIS$^f_{m,q,\beta}$

Given $(a_1, \ldots, a_m)$ uniform in $\mathbb{Z}_q[x]/f$, find $x_1, \ldots, x_m \in \mathbb{Z}[x]/f$ s.t.:

- $\sum_i x_i a_i = 0 \bmod q$,
- $0 < \|\mathbf{x}\| \leq \beta$, where $\mathbf{x} \in \mathbb{Z}^{mn}$ consists in the coeffs of the x_i's.

This is SIS, with matrix $\mathbf{A}$ made of stacked blocks $\mathrm{Rot}_f(a_i)$.
The j-th row of $\mathrm{Rot}_f(a_i)$ is made of the coefficients of $x^{j-1} \cdot a_i \bmod f$.

Why this f?

f is irreducible $\Rightarrow$ $\mathbb{Q}[x]/f$ is a field.
For $q = 1 \bmod (2n)$ prime: $\mathbb{Z}_q[x]/f \simeq \mathbb{Z}_q \times \ldots \times \mathbb{Z}_q$.

Ideal/Polynomial-SIS [LM06,PR06]

Let $q \geq 2$, $\beta > 0$, $m > 0$. Let $f = x^n + 1 \in \mathbb{Z}[x]$ with $n = 2^k$.

Ideal-SIS$^f_{m,q,\beta}$

Given $(a_1, \ldots, a_m)$ uniform in $\mathbb{Z}_q[x]/f$, find $x_1, \ldots, x_m \in \mathbb{Z}[x]/f$ s.t.:

- $\sum_i x_i a_i = 0 \bmod q$,
- $0 < \|\mathbf{x}\| \leq \beta$, where $\mathbf{x} \in \mathbb{Z}^{mn}$ consists in the coeffs of the x_i's.

This is SIS, with matrix $\mathbf{A}$ made of stacked blocks $\mathrm{Rot}_f(a_i)$.
The j-th row of $\mathrm{Rot}_f(a_i)$ is made of the coefficients of $x^{j-1} \cdot a_i \bmod f$.

Why this f?

f is irreducible $\Rightarrow$ $\mathbb{Q}[x]/f$ is a field.
For $q = 1 \bmod (2n)$ prime: $\mathbb{Z}_q[x]/f \simeq \mathbb{Z}_q \times \ldots \times \mathbb{Z}_q$.

Ideal/Polynomial-SIS [LM06,PR06]

Let $q \geq 2$, $\beta > 0$, $m > 0$. Let $f = x^n + 1 \in \mathbb{Z}[x]$ with $n = 2^k$.

Ideal-SIS$^f_{m,q,\beta}$

Given $(a_1, \ldots, a_m)$ uniform in $\mathbb{Z}_q[x]/f$, find $x_1, \ldots, x_m \in \mathbb{Z}[x]/f$ s.t.:

- $\sum_i x_i a_i = 0 \bmod q$,
- $0 < \|\mathbf{x}\| \leq \beta$, where $\mathbf{x} \in \mathbb{Z}^{mn}$ consists in the coeffs of the x_i's.

This is SIS, with matrix $\mathbf{A}$ made of stacked blocks $\mathrm{Rot}_f(a_i)$.
The j-th row of $\mathrm{Rot}_f(a_i)$ is made of the coefficients of $x^{j-1} \cdot a_i \bmod f$.

Why this f?

f is irreducible $\Rightarrow$ $\mathbb{Q}[x]/f$ is a field.
For $q = 1 \bmod (2n)$ prime: $\mathbb{Z}_q[x]/f \simeq \mathbb{Z}_q \times \ldots \times \mathbb{Z}_q$.

Ideal/Polynomial-LWE [SSTX09]

Let $q \geq 2$, $\alpha > 0$. Let $f = x^n + 1 \in \mathbb{Z}[x]$ with $n = 2^k$.

Search P-LWE^f

Given $(a_1, \ldots, a_m)$ and $(a_1 \cdot s + e_1, \ldots, a_m \cdot s + e_m)$, find s.

- s uniform in $\mathbb{Z}_q[x]/f$
- All a_i's uniform in $\mathbb{Z}_q[x]/f$
- The coefficients of the e_i's are sampled from $\nu_{\alpha q}$

Hardness of P-SIS / P-LWE

There is a reduction from SVP_γ **for ideals of $\mathbb{Z}[x]/f$** to P-SIS^f.
The approximation factor γ is proportional to β.

There is a quantum reduction from SVP_γ **for ideals of $\mathbb{Z}[x]/f$** to search P-LWE^f.
The approximation factor γ is proportional to $1/\alpha$.

- Vacuous if SVP_γ for ideals of $\mathbb{Z}[x]/f$ is easy
- Ideal-SVP_γ is currently easier than SVP_γ for large γ [CDW17,PHS19]

Hardness of P-SIS / P-LWE

There is a reduction from SVP_γ **for ideals of $\mathbb{Z}[x]/f$** to P-SIS^f.
The approximation factor γ is proportional to β.

There is a quantum reduction from SVP_γ **for ideals of $\mathbb{Z}[x]/f$** to search P-LWE^f.
The approximation factor γ is proportional to $1/\alpha$.

- Vacuous if SVP_γ for ideals of $\mathbb{Z}[x]/f$ is easy
- Ideal-SVP_γ is currently easier than SVP_γ for large γ [CDW17,PHS19]

Ring-LWE [LPR10]

Let $q \geq 2$, $\alpha > 0$, $f \in \mathbb{Z}[x]$ monic irreducible of degree n.

K: number field defined by f.
$\mathcal{O}_K$: its ring of integers. $\mathcal{O}_K{}^\vee$: its dual ideal.
$\sigma_1, \ldots, \sigma_n$: the Minkowski embeddings.

As complex embeddings come by pairs of conjugates,

the σ_k's give a bijection σ from $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$ to $\mathbb{R}^n$.

Search Ring-LWE^f

Given $(a_1, \ldots, a_m)$ and $(a_1 \cdot s + e_1, \ldots, a_m \cdot s + e_m)$, find s.

- s uniform in $\mathcal{O}_K{}^\vee / q\mathcal{O}_K{}^\vee$
- All a_i's uniform in $\mathcal{O}_K / q\mathcal{O}_K$
- The $\sigma(e_i)$'s are sampled from $\nu_{\alpha q}$

Decision Ring-LWE: distinguish uniform (a_i, b_i)'s from (a_i, b_i)'s as above

Ring-LWE [LPR10]

Let $q \geq 2$, $\alpha > 0$, $f \in \mathbb{Z}[x]$ monic irreducible of degree n.

K: number field defined by f.
$\mathcal{O}_K$: its ring of integers. $\mathcal{O}_K{}^\vee$: its dual ideal.
$\sigma_1, \ldots, \sigma_n$: the Minkowski embeddings.

As complex embeddings come by pairs of conjugates,
the σ_k's give a bijection σ from $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$ to $\mathbb{R}^n$.

Search Ring-LWE^f

Given $(a_1, \ldots, a_m)$ and $(a_1 \cdot s + e_1, \ldots, a_m \cdot s + e_m)$, find s.

- s uniform in $\mathcal{O}_K{}^\vee / q\mathcal{O}_K{}^\vee$
- All a_i's uniform in $\mathcal{O}_K / q\mathcal{O}_K$
- The $\sigma(e_i)$'s are sampled from $\nu_{\alpha q}$

Decision Ring-LWE: distinguish uniform (a_i, b_i)'s from (a_i, b_i)'s as above

Ring-LWE [LPR10]

Let $q \geq 2$, $\alpha > 0$, $f \in \mathbb{Z}[x]$ monic irreducible of degree n.

K: number field defined by f.
$\mathcal{O}_K$: its ring of integers. $\mathcal{O}_K{}^\vee$: its dual ideal.
$\sigma_1, \ldots, \sigma_n$: the Minkowski embeddings.

As complex embeddings come by pairs of conjugates,
the σ_k's give a bijection σ from $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$ to $\mathbb{R}^n$.

Search Ring-LWE^f

Given $(a_1, \ldots, a_m)$ and $(a_1 \cdot s + e_1, \ldots, a_m \cdot s + e_m)$, find s.

- s uniform in $\mathcal{O}_K{}^\vee / q\mathcal{O}_K{}^\vee$
- All a_i's uniform in $\mathcal{O}_K / q\mathcal{O}_K$
- The $\sigma(e_i)$'s are sampled from $\nu_{\alpha q}$

Decision Ring-LWE: distinguish uniform (a_i, b_i)'s from (a_i, b_i)'s as above

Hardness of Ring-LWE

LPR10 : For all f, there is a reduction from ApproxSVP for $\mathcal{O}_K$-ideals to search Ring-LWE^f.
For f cyclotomic, there is a reduction from search to decision Ring-LWE^f.

PRS17 : For all f, there is a reduction from ApproxSVP for $\mathcal{O}_K$-ideals to decision Ring-LWE^f.

The landscape is complex

Selected open problems

- What are the precise relationships between P-LWE, Ring-LWE and Module-LWE? [AD17,RSW18]
- What do the attacks on Ideal-SVP mean? [CDW17,PHS19]
- Is the relevant worst-case problem SVP for $\mathcal{O}_K$-modules? [LS15]
- Can we go from a K to a K'? [GHPS13]
- Are some K better or worse than others?

Plan for this lecture

1. Signing from SIS
2. Improving efficiency
3. **NTRU**

NTRU (adapted from [HPS98])

Notations: $R = \mathbb{Z}[x]/(x^n+1)$ $\quad R_q = \mathbb{Z}_q[x]/(x^n+1)$

Keygen: Sample f, g in R with coeffs in $\{-1, 0, 1\}$.
$sk = f$, $pk = h := g/f \bmod q$.

Encrypt: $M \in R$ with coeffs in $\{0, 1\}$. Sample s and e small.
$C = 2(h \cdot s + e) + M \bmod q$.

Decrypt: $(C \cdot f \bmod q) \bmod 2$ is $M \cdot f \bmod 2$
Divide by f mod 2.

(This requires f invertible mod q and mod 2)

Correct as long as $\|2(g \cdot s + e \cdot f)\|_\infty < q/2$ with probability ≈ 1

NTRU (adapted from [HPS98])

Notations: $R = \mathbb{Z}[x]/(x^n+1)$ $R_q = \mathbb{Z}_q[x]/(x^n+1)$

Keygen: Sample f, g in R with coeffs in $\{-1, 0, 1\}$.
$sk = f$, $pk = h := g/f \bmod q$.

Encrypt: $M \in R$ with coeffs in $\{0, 1\}$. Sample s and e small.
$C = 2(h \cdot s + e) + M \bmod q$.

Decrypt: $(C \cdot f \bmod q) \bmod 2$ is $M \cdot f \bmod 2$
Divide by $f \bmod 2$.

(This requires f invertible mod q and mod 2)

Correct as long as $\|2(g \cdot s + e \cdot f)\|_\infty < q/2$ with probability ≈ 1

NTRU (adapted from [HPS98])

Notations: $R = \mathbb{Z}[x]/(x^n+1)$ $R_q = \mathbb{Z}_q[x]/(x^n+1)$

Keygen: Sample f, g in R with coeffs in $\{-1, 0, 1\}$.
$sk = f$, $pk = h := g/f \bmod q$.

Encrypt: $M \in R$ with coeffs in $\{0, 1\}$. Sample s and e small.
$C = 2(h \cdot s + e) + M \bmod q$.

Decrypt: $(C \cdot f \bmod q) \bmod 2$ is $M \cdot f \bmod 2$
Divide by f mod 2.

(This requires f invertible mod q and mod 2)

Correct as long as $\|2(g \cdot s + e \cdot f)\|_\infty < q/2$ with probability ≈ 1

The design is versatile

- $f = x^n + 1$, q and "2" may be changed
- Use diverse types of rounding or noises
- Use small or big coefficients for f, g, s, e

Security boils down to two intractability assumptions:

- Indistinguishability of $h = g/f \bmod q$ from uniform in R_q.
  May be waived, but at a significant cost [SS11]
  Can be solved efficiently for large q and small f and g [ABD16,CJL16,KF17]
- Indistinguishability of ciphertext from uniform (i.e., Ring-LWE).

The design is versatile

- $f = x^n + 1$, q and "2" may be changed
- Use diverse types of rounding or noises
- Use small or big coefficients for f, g, s, e

Security boils down to two intractability assumptions:

- Indistinguishability of $h = g/f \bmod q$ from uniform in R_q.

  May be waived, but at a significant cost [SS11]

  Can be solved efficiently for large q and small f and g [ABD16,CJL16,KF17]
- Indistinguishability of ciphertext from uniform (i.e., Ring-LWE).

NTRU key security

Breaking the key is solving unique-SVP for a rank-2 module lattice.

$$M := \{x_1, x_2 \in R^2 : x_1 \cdot h = x_2 \bmod q\}$$

- For a uniform h, we would expect $\lambda_1(M) \approx \sqrt{n \cdot q}$
- But $(f, g) \in M$ is shorter than that

Partial hardness results [PS21]

Under specific (and incompatible) parameter restrictions:

- worst-case ideal-SVP reduces to average-case search NTRU [PS21]
- average-case search NTRU reduces to decision NTRU [PS21]

NTRU key security

Breaking the key is solving unique-SVP for a rank-2 module lattice.

$$M := \{x_1, x_2 \in R^2 : x_1 \cdot h = x_2 \bmod q\}$$

- For a uniform h, we would expect $\lambda_1(M) \approx \sqrt{n \cdot q}$
- But $(f, g) \in M$ is shorter than that

Partial hardness results [PS21]

Under specific (and incompatible) parameter restrictions:

- worst-case ideal-SVP reduces to average-case search NTRU [PS21]
- average-case search NTRU reduces to decision NTRU [PS21]

Plan for this lecture

1. Signing from SIS
2. Improving efficiency
3. NTRU

Wrapping up

Lattices are conjectured to provide hard worst-case problems.

SIS/LWE are a-c variants no easier than some w-c lattice problems.

- There is no fundamental weakness in SIS/LWE.
- The reductions are not meant for setting parameters, but for ensuring that there is no fundamental flaw.

SIS/LWE can be viewed as linear algebra problems.

- It leads to simple cryptographic design.
- It enables advanced cryptographic constructions.

To improve efficiency, use algebraic lattices.

- Does it impact computational intractability?
- Plenty of problems involving algebraic number theory.

Wrapping up

Lattices are conjectured to provide hard worst-case problems.

SIS/LWE are a-c variants no easier than some w-c lattice problems.

- There is no fundamental weakness in SIS/LWE.
- The reductions are not meant for setting parameters, but for ensuring that there is no fundamental flaw.

SIS/LWE can be viewed as linear algebra problems.

- It leads to simple cryptographic design.
- It enables advanced cryptographic constructions.

To improve efficiency, use algebraic lattices.

- Does it impact computational intractability?
- Plenty of problems involving algebraic number theory.

Wrapping up

Lattices are conjectured to provide hard worst-case problems.

SIS/LWE are a-c variants no easier than some w-c lattice problems.

- There is no fundamental weakness in SIS/LWE.
- The reductions are not meant for setting parameters, but for ensuring that there is no fundamental flaw.

SIS/LWE can be viewed as linear algebra problems.

- It leads to simple cryptographic design.
- It enables advanced cryptographic constructions.

To improve efficiency, use algebraic lattices.

- Does it impact computational intractability?
- Plenty of problems involving algebraic number theory.

Wrapping up

Lattices are conjectured to provide hard worst-case problems.

SIS/LWE are a-c variants no easier than some w-c lattice problems.

- There is no fundamental weakness in SIS/LWE.
- The reductions are not meant for setting parameters, but for ensuring that there is no fundamental flaw.

SIS/LWE can be viewed as linear algebra problems.

- It leads to simple cryptographic design.
- It enables advanced cryptographic constructions.

To improve efficiency, use algebraic lattices.

- Does it impact computational intractability?
- Plenty of problems involving algebraic number theory.

Bibliography

ACPS09 B. Applebaum, D. Cash, C. Peikert, A. Sahai: Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. CRYPTO 2009.

Ajtai96 M. Ajtai: Generating Hard Instances of Lattice Problems. STOC 1996.

BKSW18 Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen: Learning with Errors and Extrapolated Dihedral Cosets. Public Key Cryptography 2018.

BLPRS13 Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé: Classical hardness of learning with errors. STOC 2013.

CDW17 R. Cramer, L. Ducas, B. Wesolowski: Short Stickelberger Class Relations and Application to Ideal-SVP. EUROCRYPT 2017.

GHPS13 C. Gentry, S. Halevi, C. Peikert, N. P. Smart: Field switching in BGV-style homomorphic encryption. J. Comput. Secur. 2013.

GPV08 C. Gentry, C. Peikert, V. Vaikuntanathan: Trapdoors for hard lattices and new cryptographic constructions. STOC 2008.

HPS98 J. Hoffstein, J. Pipher, J. H. Silverman: NTRU: A Ring-Based Public Key Cryptosystem. ANTS 1998.

Lyu09 V. Lyubashevsky: Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. ASIACRYPT 2009.

Lyu12 V. Lyubashevsky: Lattice Signatures without Trapdoors. EUROCRYPT 2012.

LM06 V. Lyubashevsky, D. Micciancio: Generalized Compact Knapsacks Are Collision Resistant. ICALP 2006.

LPR10 V. Lyubashevsky, C. Peikert, O. Regev: On Ideal Lattices and Learning with Errors over Rings. EUROCRYPT 2010.

LPS10 V. Lyubashevsky, A. Palacio, G. Segev: Public-Key Cryptographic Primitives Provably as Secure as Subset Sum. TCC 2010.

LS15 A. Langlois, D. Stehlé: Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr. 2015.

Bibliography

Peikert09 C. Peikert: Public-key cryptosystems from the worst-case shortest vector problem. STOC 2009.

PHS19 A. Pellet-Mary, G. Hanrot, D. Stehlé: Approx-SVP in Ideal Lattices with Pre-processing. EUROCRYPT 2019.

PR06 C. Peikert, A. Rosen: Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices. TCC 2006.

PRS17 C. Peikert, O. Regev, N. Stephens-Davidowitz: Pseudorandomness of ring-LWE for any ring and modulus. STOC 2017.

PS21 A. Pellet-Mary, D. Stehlé: On the Hardness of the NTRU Problem. ASIACRYPT 2021.

Regev05 O. Regev: On lattices, learning with errors, random linear codes, and cryptography. STOC 2005.

SSTX09 D. Stehlé, R. Steinfeld, K. Tanaka, K. Xagawa: Efficient Public Key Encryption Based on Ideal Lattices. ASIACRYPT 2009.