Introduction to lattice-based cryptography

Damien Stehlé

ENS de Lyon

Aussois, March 2019

Plan for this lecture

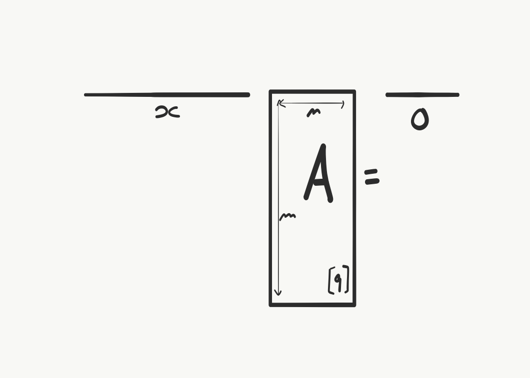
1. **Signing from SIS**
2. Improving efficiency
3. NTRU

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

The Small Integer Solution Problem

Given a uniform $A \in \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m \setminus \mathbf{0}$ such that:

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



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 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 $A \in \mathbb{Z}_q^{m\times n}$, find $\mathbf{x} \in \mathbb{Z}^m \setminus \mathbf{0}$ such that:

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

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

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

Why is it hard to invert?

- Let A be a SIS instance.
- Sample $\mathbf{x} \hookleftarrow U(\{-B,\ldots,B\})^m$, set $\mathbf{y} = \mathbf{x}^T \cdot A$.
- Adversary gets 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 $A \in \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m \setminus \mathbf{0}$ such that:

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

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

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

Why is it hard to invert?

- Let A be a SIS instance.
- Sample $\mathbf{x} \hookleftarrow U(\{-B, \ldots, B\})^m$, set $\mathbf{y} = \mathbf{x}^T \cdot A$.
- Adversary gets 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 $A \in \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m \setminus \mathbf{0}$ such that:

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

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

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

Why is it hard to invert?

- Let A be a SIS instance.
- Sample $\mathbf{x} \hookleftarrow U(\{-B, \ldots, B\})^m$, set $\mathbf{y} = \mathbf{x}^T \cdot A$.
- Adversary gets 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 SIS

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

Prover generates a blinding equation:

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

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

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

Proof of knowledge for SIS

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

Prover generates a blinding equation:

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

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

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

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

Proof of knowledge for SIS

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

Prover generates a blinding equation:

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

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

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

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

Proof of knowledge for SIS

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

Prover generates a blinding equation:

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

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

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

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

Proof of knowledge for SIS

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

Prover generates a blinding equation:

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

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**.

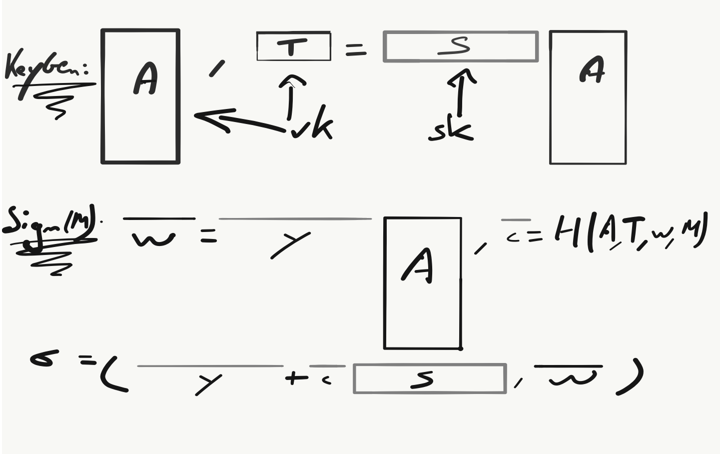
Prover replies with $\mathbf{y} + c \cdot \mathbf{s}$.

Verifier checks whether

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

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 $\sigma_1^T A = \mathbf{w}^T + \mathbf{c}^T T$.

This signature scheme is insecure but can be fixed

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

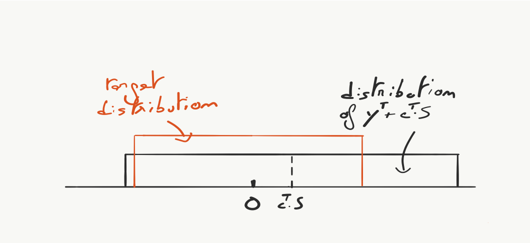
$\sigma_1^T = \mathbf{y}^T + \mathbf{c}^T \cdot S$ conditioned on $\mathbf{c}$ and S, has center $\mathbf{c}^T \cdot S$.

This signature scheme is insecure but can be fixed

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

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

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**

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

$\Rightarrow$ No need for a signing key anymore!

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

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

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

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**

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

$\Rightarrow$ No need for a signing key anymore!

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

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

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

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**

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

$\Rightarrow$ No need for a signing key anymore!

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

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

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

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: use LWE rather than SIS
  - Shorter $S \Rightarrow$ shorter $\mathbf{y} \Rightarrow$ smaller signatures
  - Security proof can be made tight
  - Security proof can be done in the quantum random oracle model (eprint 2015/755)

- Precise comparison to GPV-type signatures.
- Efficient signature without the random oracle heuristic?
- Efficient Schnorr-type signature with security proof in the quantum random oracle model?

Further remarks

- Setting parameters requires work. Compromises between:
  - Security
  - Probability of rejection (and hence signing time)
  - Size of signatures

- Further improvement: use LWE rather than SIS
  - Shorter $S \Rightarrow$ shorter $\mathbf{y} \Rightarrow$ smaller signatures
  - Security proof can be made tight
  - Security proof can be done in the quantum random oracle model (eprint 2015/755)

- Precise comparison to GPV-type signatures.
- Efficient signature without the random oracle heuristic?
- Efficient Schnorr-type signature with security proof in the quantum random oracle model?

Plan for this lecture

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

It's all slow

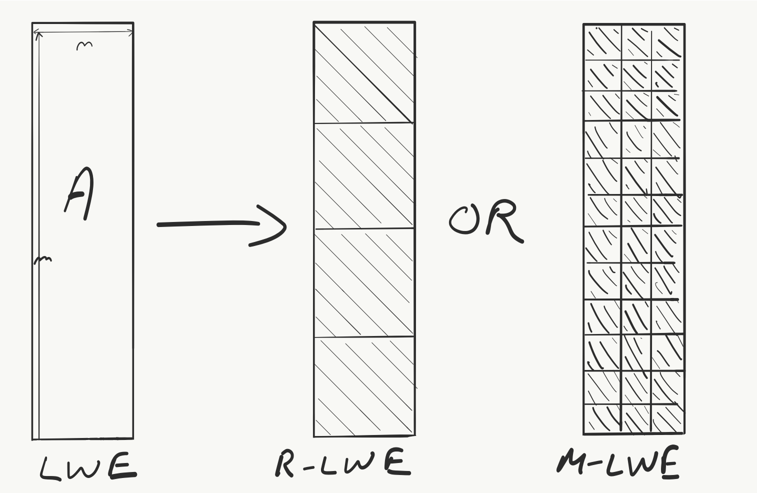
Public key contains a uniformly sampled matrix A.

- Share A among users
  (but maybe an adversary can work on A to break all keys)
- Store only the seed of the randomness used to sample 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 same encryption scheme as the one we saw work. 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 $q = 1$ $[2n]$ 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 $q = 1$ $[2n]$ 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 $n = 2^k$.

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

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 $q = 1$ $[2n]$ 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 actually easier than SVP_γ!
  [CDW17,PHS19], 2016/885, 2019/215

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 actually easier than SVP_γ!
  [CDW17,PHS19], 2016/885, 2019/215

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 than others? See Wouter's talk!
- What to think about MP-LWE? [Lyubashevsky16,RSSS17]

It matters! All these Round 2 NIST candidates rely on algebraic lattices:

Dilithium, Falcon, Tesla,

Kyber, LAC, NewHope, NTRU, NTRUPrime, Round5, SABER, ThreeBears

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 than others? See Wouter's talk!
- What to think about MP-LWE? [Lyubashevsky16,RSSS17]

It matters! All these Round 2 NIST candidates rely on algebraic lattices:

Dilithium, Falcon, Tesla,

Kyber, LAC, NewHope, NTRU, NTRUPrime, Round5, SABER, ThreeBears

Plan for this lecture

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

NTRU — a personal variant of [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 $|2(g \cdot s + e \cdot f)| < q/2$ with probability ≈ 1

NTRU — a personal variant of [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 $|2(g \cdot s + e \cdot f)| < q/2$ with probability ≈ 1

NTRU — a personal variant of [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 $|2(g \cdot s + e \cdot f)| < q/2$ 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 done efficiently for large q [ABD16,CJL16,KF17]
- Indistinguishability of ciphertext from uniform, i.e., Ring-LWE-like.

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 done efficiently for large q [ABD16,CJL16,KF17]
- Indistinguishability of ciphertext from uniform, i.e., Ring-LWE-like.

My favorite NTRU open problem

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

For arbitrary lattices, BDD reduces to unique-SVP in 1 more dimension, and unique-SVP reduces to BDD in same dimension.

Is unique-SVP for rank-2 modules computationally closer to:

- BDD in rank-1 modules, i.e., ideal lattices?

  (some weaknesses are known)
- or BDD in rank-2 modules?

  (some equivalence with Ring-LWE known [LS15,AD17])

My favorite NTRU open problem

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

For arbitrary lattices, BDD reduces to unique-SVP in 1 more dimension, and unique-SVP reduces to BDD in same dimension.

Is unique-SVP for rank-2 modules computationally closer to:

- BDD in rank-1 modules, i.e., ideal lattices?
  (some weaknesses are known)
- or BDD in rank-2 modules?
  (some equivalence with Ring-LWE known [LS15,AD17])

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 hard 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 weakness.

SIS and LWE can be viewed linear algebra problems.

- Leads to simple cryptographic design.
- Allows advanced cryptographic constructions.

To get faster schemes, 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 hard 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 weakness.

SIS and LWE can be viewed linear algebra problems.

- Leads to simple cryptographic design.
- Allows advanced cryptographic constructions.

To get faster schemes, 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 hard 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 weakness.

SIS and LWE can be viewed linear algebra problems.

- Leads to simple cryptographic design.
- Allows advanced cryptographic constructions.

To get faster schemes, 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 hard 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 weakness.

SIS and LWE can be viewed linear algebra problems.

- Leads to simple cryptographic design.
- Allows advanced cryptographic constructions.

To get faster schemes, use algebraic lattices.

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