Ideal Lattices

Damien Stehlé

ENS de Lyon

Berkeley, 07/07/2015

Lattice-based cryptography: elegant but impractical

- Lattice-based cryptography is fascinating: simple, (presumably) post-quantum, expressive
- But it is very **slow**

Recall the SIS hash function:

$$\begin{array}{ccc} \{0,1\}^m & \to & \mathbb{Z}_q^n \\ \mathbf{x} & \mapsto & \mathbf{x}^T \cdot \mathbf{A} \end{array}$$

- Need $m = \Omega(n \log q)$ to compress
- q is $n^{O(1)}$, $\mathbf{A}$ is uniform in $\mathbb{Z}_q^{m \times n}$

$\Rightarrow \widetilde{O}(n^2)$ space and cost

- Example parameters: $n \approx 2^6$, $m \approx n \cdot 2^4$, $\log_2 q \approx 2^3$

Lattice-based cryptography: elegant but impractical

- Lattice-based cryptography is fascinating: simple, (presumably) post-quantum, expressive
- But it is very **slow**

Recall the SIS hash function:

$$\begin{array}{ccc} \{0,1\}^m & \rightarrow & \mathbb{Z}_q^n \\ \mathbf{x} & \mapsto & \mathbf{x}^T \cdot \mathbf{A} \end{array}$$

- Need $m = \Omega(n \log q)$ to compress
- q is $n^{O(1)}$, $\mathbf{A}$ is uniform in $\mathbb{Z}_q^{m \times n}$

$\Rightarrow \quad \widetilde{O}(n^2)$ space and cost

- Example parameters: $n \approx 2^6$, $m \approx n \cdot 2^4$, $\log_2 q \approx 2^3$

Lattice-based cryptography: elegant but impractical

- Lattice-based cryptography is fascinating:
  simple, (presumably) post-quantum, expressive
- But it is very **slow**

Recall the SIS hash function:

$$\begin{array}{ccc} \{0,1\}^m & \rightarrow & \mathbb{Z}_q^n \\ \mathbf{x} & \mapsto & \mathbf{x}^T \cdot \mathbf{A} \end{array}$$

- Need $m = \Omega(n \log q)$ to compress
- q is $n^{O(1)}$, $\mathbf{A}$ is uniform in $\mathbb{Z}_q^{m \times n}$

$\Rightarrow \widetilde{O}(n^2)$ space and cost

- Example parameters: $n \approx 2^6$, $m \approx n \cdot 2^4$, $\log_2 q \approx 2^3$

Lattice-based cryptography: elegant but impractical

- Lattice-based cryptography is fascinating: simple, (presumably) post-quantum, expressive
- But it is very **slow**

Recall the SIS hash function:

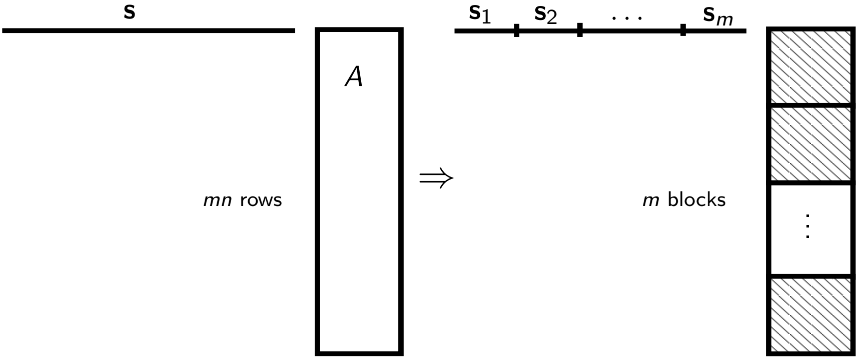
$$\begin{array}{ccc} \{0,1\}^m & \to & \mathbb{Z}_q^n \\ \mathbf{x} & \mapsto & \mathbf{x}^T \cdot \mathbf{A} \end{array}$$

- Need $m = \Omega(n \log q)$ to compress
- q is $n^{O(1)}$, $\mathbf{A}$ is uniform in $\mathbb{Z}_q^{m \times n}$

$\Rightarrow \; \widetilde{O}(n^2)$ space and cost

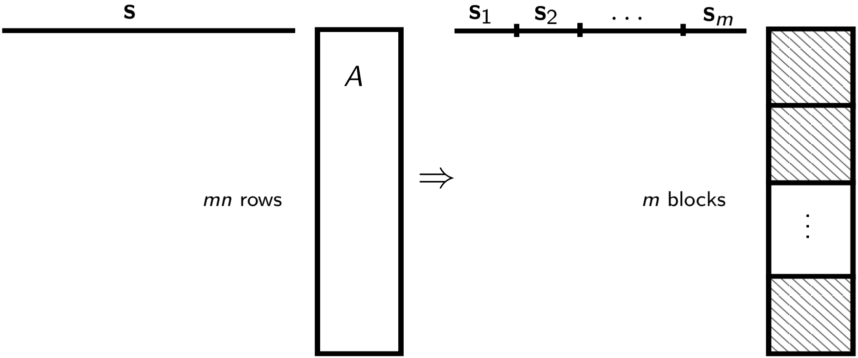
- Example parameters: $n \approx 2^6$, $m \approx n \cdot 2^4$, $\log_2 q \approx 2^3$

Speeding up linear algebra



- Matrix **A** is structured by block
- Structured matrices ⇒ much less space
- Structured matrices ≡ polynomials ≡ fast algorithms
- For $n \approx 2^6$, $m \approx 2^4$, $\log_2 q \approx 2^3$: 2^{19} vs 2^{13} bits

Speeding up linear algebra



- Matrix **A** is structured by block
- Structured matrices ⇒ much less space
- Structured matrices ≡ polynomials ≡ fast algorithms
- For $n \approx 2^6, m \approx 2^4, \log_2 q \approx 2^3$: 2^{19} vs 2^{13} bits

Structured lattices in crypto: historical perspective

- [NTRU'96,'98,'01]: Encryption and signature, heuristic security

- [Micciancio03]: One-way hash function with cyclic lattices
- [LyMi06,PeRo06]: **Ring-SIS**, collision-resistant hashing
- [Lyu08,Lyu12,DDLL13]: Schnorr-like Ring-SIS signature

- [Gentry09]: Fully homomorphic encryption
- [SSTX09]: Fast encryption based on ideal lattices
- [LyPeRe10]: **Ring-LWE**

- [GaGeHa13]: was a candidate cryptographic **multilinear map**

Structured lattices in crypto: historical perspective

- [NTRU'96,'98,'01]: Encryption and signature, heuristic security

- [Micciancio03]: One-way hash function with cyclic lattices
- [LyMi06,PeRo06]: **Ring-SIS**, collision-resistant hashing
- [Lyu08,Lyu12,DDLL13]: Schnorr-like Ring-SIS signature

- [Gentry09]: Fully homomorphic encryption
- [SSTX09]: Fast encryption based on ideal lattices
- [LyPeRe10]: **Ring-LWE**

- [GaGeHa13]: was a candidate cryptographic **multilinear map**

Structured lattices in crypto: historical perspective

- [NTRU'96,'98,'01]: Encryption and signature, heuristic security

- [Micciancio03]: One-way hash function with cyclic lattices
- [LyMi06,PeRo06]: **Ring-SIS**, collision-resistant hashing
- [Lyu08,Lyu12,DDLL13]: Schnorr-like Ring-SIS signature

- [Gentry09]: Fully homomorphic encryption
- [SSTX09]: Fast encryption based on ideal lattices
- [LyPeRe10]: **Ring-LWE**

- [GaGeHa13]: was a candidate cryptographic **multilinear map**

Roadmap

Goals of this talk

- Introduce Ring-SIS and Ring-LWE
- Describe the lattices that lurk behind

Roadmap

Goals of this talk

- Introduce Ring-SIS and Ring-LWE
- Describe the lattices that lurk behind

1- **Ideal lattices**

2- Ring-SIS

3- Ring-LWE

4- Other lattices from algebraic number theory

Some algebra

Number field

Let $\zeta \in \mathbb{C}$ algebraic with minimum polynomial $P \in \mathbb{Q}[X]$. Let

$$K \ := \ \sum_{i=0}^{n-1} \mathbb{Q} \cdot \zeta^i \ \subseteq \ \mathbb{C}$$

with $n = \deg P$. This is a field, and $K \cong \mathbb{Q}[X]/P$.

Ring of integers of K

The ring of integers $R = \mathcal{O}_K$ is the set of $\sum y_i \cdot \zeta^i \in K$ that are roots of monic polynomials with integer coefficients.

$$\mathbb{Z}[X]/P \ \cong \ \sum_{i=0}^{n-1} \mathbb{Z} \cdot \zeta^i \ \subseteq \ R.$$

In general, the inclusion is strict.
But there always exist $(\zeta_i)_i$ such that $R = \sum_i \mathbb{Z} \cdot \zeta_i$.

In general, finding a $\mathbb{Z}$-basis of R from P is expensive

Some algebra

Number field

Let $\zeta \in \mathbb{C}$ algebraic with minimum polynomial $P \in \mathbb{Q}[X]$. Let

$$K \ := \ \sum_{i=0}^{n-1} \mathbb{Q} \cdot \zeta^i \ \subseteq \ \mathbb{C}$$

with $n = \deg P$. This is a field, and $K \cong \mathbb{Q}[X]/P$.

Ring of integers of K

The ring of integers $R = \mathcal{O}_K$ is the set of $\sum y_i \cdot \zeta^i \in K$ that are roots of monic polynomials with integer coefficients.

$$\mathbb{Z}[X]/P \ \cong \ \sum_{i=0}^{n-1} \mathbb{Z} \cdot \zeta^i \ \subseteq \ R.$$

In general, the inclusion is strict.
But there always exist $(\zeta_i)_i$ such that $R = \sum_i \mathbb{Z} \cdot \zeta_i$.

In general, finding a $\mathbb{Z}$-basis of R from P is expensive

Cyclotomic fields

Cyclotomic polynomial

Φ_m is the unique irreducible polynomial dividing $X^m - 1$ which is not dividing any $X^k - 1$ for $k < m$.

$$\Phi_m(X) \;=\; \prod_{k:gcd(k,m)=1}(X - e^{\frac{2ik\pi}{m}}).$$

- If m is a power of 2, then $\Phi_m = 1 + X^{m/2}$
- If m is prime, then $\Phi_m = \frac{X^m - 1}{X - 1}$

Cyclotomic field

The mth cyclotomic field is $K(e^{\frac{2i\pi}{m}}) \;\cong\; \mathbb{Q}[X]/\Phi_m$.

Why cyclotomic fields?

- More is known, and they tend to be simpler to deal with
- E.g.: $R \;=\; \sum_{i=0}^{n-1} \mathbb{Z} \cdot \zeta^i \;\cong\; \mathbb{Z}[x]/\Phi_m$

Cyclotomic fields

Cyclotomic polynomial

Φ_m is the unique irreducible polynomial dividing $X^m - 1$ which is not dividing any $X^k - 1$ for $k < m$.

$$\Phi_m(X) \ = \ \prod_{k:gcd(k,m)=1}(X - e^{\frac{2ik\pi}{m}}).$$

- If m is a power of 2, then $\Phi_m = 1 + X^{m/2}$
- If m is prime, then $\Phi_m = \frac{X^m - 1}{X - 1}$

Cyclotomic field

The mth cyclotomic field is $K(e^{\frac{2i\pi}{m}}) \ \cong \ \mathbb{Q}[X]/\Phi_m$.

Why cyclotomic fields?

- More is known, and they tend to be simpler to deal with
- E.g.: $R \ = \ \sum_{i=0}^{n-1} \mathbb{Z} \cdot \zeta^i \ \cong \ \mathbb{Z}[x]/\Phi_m$

Cyclotomic fields

Cyclotomic polynomial

Φ_m is the unique irreducible polynomial dividing $X^m - 1$ which is not dividing any $X^k - 1$ for $k < m$.

$$\Phi_m(X) \ = \ \prod_{k:gcd(k,m)=1}(X - e^{\frac{2ik\pi}{m}}).$$

- If m is a power of 2, then $\Phi_m = 1 + X^{m/2}$
- If m is prime, then $\Phi_m = \frac{X^m-1}{X-1}$

Cyclotomic field

The mth cyclotomic field is $K(e^{\frac{2i\pi}{m}}) \ \cong \ \mathbb{Q}[X]/\Phi_m$.

Why cyclotomic fields?

- More is known, and they tend to be simpler to deal with
- E.g.: $R \ = \ \sum_{i=0}^{n-1} \mathbb{Z} \cdot \zeta^i \ \cong \ \mathbb{Z}[x]/\Phi_m$

Ideals

Ideal of $\mathcal{O}_K$

$I \subseteq R$ is an (integral) ideal if $\forall a, b \in I$, $\forall r \in R$:

$$a + b \in I \quad \text{and} \quad r \cdot a \in I.$$

If $I \neq \{0\}$, then R/I is a finite ring and we let $\mathcal{N}(I) = |R/I|$.

Principal ideal

If $g \in R$, then $(g) = g \cdot R$ is an ideal, called principal ideal.

- For large n, most ideals are not principal.
- Every ideal is of the form $\sum_{i \leq n} g_i \cdot \mathbb{Z}$ for some $g_i \in R$.
- Every ideal is generated by 2 elements:

$$I = g_1 \cdot R + g_2 \cdot R \quad \text{for some } g_1, g_2 \in R$$

Ideals

Ideal of $\mathcal{O}_K$

$I \subseteq R$ is an (integral) ideal if $\forall a, b \in I$, $\forall r \in R$:

$$a + b \in I \quad \text{and} \quad r \cdot a \in I.$$

If $I \neq \{0\}$, then R/I is a finite ring and we let $\mathcal{N}(I) = |R/I|$.

Principal ideal

If $g \in R$, then $(g) = g \cdot R$ is an ideal, called principal ideal.

- For large n, most ideals are not principal.
- Every ideal is of the form $\sum_{i \leq n} g_i \cdot \mathbb{Z}$ for some $g_i \in R$.
- Every ideal is generated by 2 elements:

$$I = g_1 \cdot R + g_2 \cdot R \quad \text{for some } g_1, g_2 \in R$$

Number fields and geometry

We have $K \subseteq \mathbb{C}$... this is geometrically boring

Polynomial embedding σ_P

Using $K \cong \mathbb{Q}[X]/P$, we can identify elements of K with polynomials of degree $< n$, and hence with elements of $\mathbb{Q}^n$.

Canonical embedding σ_C

Let $(\zeta_i)_i$ be the roots of P. For $g \in \mathbb{Q}[X]/P$, we define

$$\forall i \leq n: \quad \sigma_i(g) = g(\zeta_i) \in \mathbb{C}$$

$\sigma_C := (\sigma_i)_i$ sends K to a $\mathbb{Q}$-vector subspace of $\mathbb{C}^n$ of dimension n.

This is multi-evaluation!

- Easy to compute
- $+$ and $\times$ in K are mapped to componentwise $+$ and $\times$ in $\mathbb{C}^n$

Number fields and geometry

We have $K \subseteq \mathbb{C}$... this is geometrically boring

Polynomial embedding σ_P

Using $K \cong \mathbb{Q}[X]/P$, we can identify elements of K with polynomials of degree $< n$, and hence with elements of $\mathbb{Q}^n$.

Canonical embedding σ_C

Let $(\zeta_i)_i$ be the roots of P. For $g \in \mathbb{Q}[X]/P$, we define

$$\forall i \leq n : \quad \sigma_i(g) = g(\zeta_i) \in \mathbb{C}$$

$\sigma_C := (\sigma_i)_i$ sends K to a $\mathbb{Q}$-vector subspace of $\mathbb{C}^n$ of dimension n.

This is multi-evaluation!

- Easy to compute
- $+$ and $\times$ in K are mapped to componentwise $+$ and $\times$ in $\mathbb{C}^n$

Number fields and geometry

We have $K \subseteq \mathbb{C}$... this is geometrically boring

Polynomial embedding σ_P

Using $K \cong \mathbb{Q}[X]/P$, we can identify elements of K with polynomials of degree $< n$, and hence with elements of $\mathbb{Q}^n$.

Canonical embedding σ_C

Let $(\zeta_i)_i$ be the roots of P. For $g \in \mathbb{Q}[X]/P$, we define

$$\forall i \leq n: \quad \sigma_i(g) = g(\zeta_i) \in \mathbb{C}$$

$\sigma_C := (\sigma_i)_i$ sends K to a $\mathbb{Q}$-vector subspace of $\mathbb{C}^n$ of dimension n.

This is multi-evaluation!

- Easy to compute
- $+$ and $\times$ in K are mapped to componentwise $+$ and $\times$ in $\mathbb{C}^n$

σ_P versus σ_C

- Multiplication is (mathematically) simpler for σ_C
- Products make norms grow less for σ_C:
  - $\frac{\|\sigma_P(g_1 \cdot g_2)\|}{\|\sigma_P(g_1)\| \cdot \|\sigma_P(g_2)\|}$ can be very large even if P is small,
  - $\frac{\|\sigma_C(g_1 \cdot g_2)\|}{\|\sigma_C(g_1)\| \cdot \|\sigma_C(g_2)\|} \leq 1$
- For the power-of-2 cyclotomic field of degree n:

$$\forall g \in K: \quad \|\sigma_P(g)\| = \frac{1}{\sqrt{n}} \cdot \|\sigma_C(g)\|$$

Ideal lattices

Ideal lattice

Let K a number field and σ an add-homomorphism from K to $\mathbb{R}^n$.
Then $I \subseteq R$ ideal $\Rightarrow$ $\sigma(I) \subseteq \mathbb{R}^n$ lattice.

By default, one uses σ_C to look at the geometry of ideals

Ideal-SVP

Let $(K_i)_i$ be a sequence a number fields of growing degrees n_i.
An Ideal-SVP instance is an ideal I of R_i.
One has to find $b \in I \setminus \{0\}$ minimizing $\|\sigma_C(b)\|$.

This is SVP restricted to ideals of $(R_i)_i$.

E.g., we can study SVP for ideals of power-of-2 cyclotomic fields.

Ideal lattices

Ideal lattice

Let K a number field and σ an add-homomorphism from K to $\mathbb{R}^n$.
Then $I \subseteq R$ ideal $\Rightarrow$ $\sigma(I) \subseteq \mathbb{R}^n$ lattice.

By default, one uses σ_C to look at the geometry of ideals

Ideal-SVP

Let $(K_i)_i$ be a sequence a number fields of growing degrees n_i.
An Ideal-SVP instance is an ideal I of R_i.
One has to find $b \in I \setminus \{0\}$ minimizing $\|\sigma_C(b)\|$.

This is SVP restricted to ideals of $(R_i)_i$.

E.g., we can study SVP for ideals of power-of-2 cyclotomic fields.

Are ideal lattice problems any easier than lattice problems?

Property 1. $b \in I$ small $\Rightarrow$ $\zeta^i \cdot b$ small, for all i.

(For σ_P and power-of-2 cyclotomics, these are the famous negacyclic shifts)

Property 2. λ_1 approximately known. For power-of-2 cyclotomics

$$\sqrt{n} \cdot \mathcal{N}(I)^{1/n} \leq \lambda_1(I) \leq n \cdot \mathcal{N}(I)^{1/n}$$

- RHS. Minkowski's theorem $(\det I = \sqrt{n}^n \cdot \mathcal{N}(I))$.
- LHS. Take b reaching λ_1. Then
  - $(b) \subseteq I$
  - $(b \cdot \zeta^i)_i$ is a basis of (b), made of vectors of norms $\|b\|$

  $\Rightarrow \mathcal{N}(I) \leq \mathcal{N}((b)) = \sqrt{n}^{-n} \cdot \det(b) \leq \sqrt{n}^{-n} \|b\|^n$

Apart from these two properties, no other known weakness for lattice problems restricted to ideal lattices, in the worst case.

Are ideal lattice problems any easier than lattice problems?

Property 1. $b \in I$ small $\Rightarrow$ $\zeta^i \cdot b$ small, for all i.

(For σ_P and power-of-2 cyclotomics, these are the famous negacyclic shifts)

Property 2. λ_1 approximately known. For power-of-2 cyclotomics

$$\sqrt{n} \cdot \mathcal{N}(I)^{1/n} \leq \lambda_1(I) \leq n \cdot \mathcal{N}(I)^{1/n}$$

- RHS. Minkowski's theorem (det $I = \sqrt{n}^n \cdot \mathcal{N}(I)$).
- LHS. Take b reaching λ_1. Then
  - $(b) \subseteq I$
  - $(b \cdot \zeta^i)_i$ is a basis of (b), made of vectors of norms $\|b\|$

$\Rightarrow \mathcal{N}(I) \leq \mathcal{N}((b)) = \sqrt{n}^{-n} \cdot \det\ (b) \leq \sqrt{n}^{-n} \|b\|^n$

Apart from these two properties, no other known weakness for lattice problems restricted to ideal lattices, in the worst case.

Are ideal lattice problems any easier than lattice problems?

Property 1. $b \in I$ small $\Rightarrow$ $\zeta^i \cdot b$ small, for all i.

(For σ_P and power-of-2 cyclotomics, these are the famous negacyclic shifts)

Property 2. λ_1 approximately known. For power-of-2 cyclotomics

$$\sqrt{n} \cdot \mathcal{N}(I)^{1/n} \leq \lambda_1(I) \leq n \cdot \mathcal{N}(I)^{1/n}$$

- RHS. Minkowski's theorem (det $I = \sqrt{n}^n \cdot \mathcal{N}(I)$).
- LHS. Take b reaching λ_1. Then
  - $(b) \subseteq I$
  - $(b \cdot \zeta^i)_i$ is a basis of (b), made of vectors of norms $\|b\|$

$\Rightarrow$ $\mathcal{N}(I) \leq \mathcal{N}((b)) = \sqrt{n}^{-n} \cdot \det\,(b) \leq \sqrt{n}^{-n} \|b\|^n$

Apart from these two properties, no other known weakness for lattice problems restricted to ideal lattices, in the worst case.

Are ideal lattice problems any easier than lattice problems?

Apart from these two properties, no other known weakness for lattice problems restricted to ideal lattices, in the worst case.

... but no proof that no other structural weakness exists.

Some problems become easy for some families of ideal lattices, at least for cyclotomic fields.

Gentry-Szydlo — see Alice's talk

If $I = (g)$ and we are given $B^t B$ for the basis B of I corresponding to the $\zeta^i \cdot g$'s, then we may recover g in polynomial time.

SPIP — see Chris' talk

If $I = (g)$ with g "exceptionally" small, then we may recover g in subexponential time.

Are ideal lattice problems any easier than lattice problems?

Apart from these two properties, no other known weakness for lattice problems restricted to ideal lattices, in the worst case.

... but no proof that no other structural weakness exists.

Some problems become easy for some families of ideal lattices, at least for cyclotomic fields.

Gentry-Szydlo — see Alice's talk

If $I = (g)$ and we are given $B^t B$ for the basis B of I corresponding to the $\zeta^i \cdot g$'s, then we may recover g in polynomial time.

SPIP — see Chris' talk

If $I = (g)$ with g "exceptionally" small, then we may recover g in subexponential time.

Roadmap

1- Ideal lattices

2- **Ring-SIS**

3- Ring-LWE

4- Other lattices from algebraic number theory

Two rings

$$R \cong \mathbb{Z}[x]/(x^n+1) \quad \text{and} \quad R_q = \mathbb{Z}_q[x]/(x^n+1) = R/qR$$

If $f \in R$ is known to have small coeffs, then $(f \bmod q)$ reveals f

Multiplication in R_q and linear algebra:

$$[a_0\ a_1\ \ldots\ a_{n-1}] \cdot \begin{bmatrix} b_0 & b_1 & \ldots & b_{n-1} \\ -b_{n-1} & b_0 & \ldots & b_{n-2} \\ \vdots & & \vdots & \\ -b_1 & -b_2 & \ldots & b_0 \end{bmatrix} = [c_0\ c_1\ \ldots\ c_{n-1}],$$

with $c(x) = a(x) \cdot b(x) \bmod (x^n+1)$

- Quasi-linear time multiplication
- It's even practical, for $q = 1 \bmod 2n$ (number-theory transform)

Two rings

$$R \cong \mathbb{Z}[x]/(x^n+1) \quad \text{and} \quad R_q = \mathbb{Z}_q[x]/(x^n+1) = R/qR$$

If $f \in R$ is known to have small coeffs, then (f mod q) reveals f

Multiplication in R_q and linear algebra:

$$[a_0\ a_1\ \ldots\ a_{n-1}] \cdot \begin{bmatrix} b_0 & b_1 & \ldots & b_{n-1} \\ -b_{n-1} & b_0 & \ldots & b_{n-2} \\ \vdots & & \vdots & \\ -b_1 & -b_2 & \ldots & b_0 \end{bmatrix} = [c_0\ c_1\ \ldots\ c_{n-1}],$$

with $c(x) = a(x) \cdot b(x) \bmod (x^n+1)$

- Quasi-linear time multiplication
- It's even practical, for $q = 1 \bmod 2n$ (number-theory transform)

Two rings

$$R \cong \mathbb{Z}[x]/(x^n+1) \quad \text{and} \quad R_q = \mathbb{Z}_q[x]/(x^n+1) = R/qR$$

If $f \in R$ is known to have small coeffs, then (f mod q) reveals f

Multiplication in R_q and linear algebra:

$$[a_0\ a_1\ \ldots\ a_{n-1}] \cdot \begin{bmatrix} b_0 & b_1 & \ldots & b_{n-1} \\ -b_{n-1} & b_0 & \ldots & b_{n-2} \\ \vdots & & \vdots & \\ -b_1 & -b_2 & \ldots & b_0 \end{bmatrix} = [c_0\ c_1\ \ldots\ c_{n-1}],$$

with $c(x) = a(x) \cdot b(x) \bmod (x^n+1)$

- Quasi-linear time multiplication
- It's even practical, for $q = 1 \bmod 2n$ (number-theory transform)

Two rings

$$R \cong \mathbb{Z}[x]/(x^n+1) \quad \text{and} \quad R_q = \mathbb{Z}_q[x]/(x^n+1) = R/qR$$

If $f \in R$ is known to have small coeffs, then (f mod q) reveals f

Multiplication in R_q and linear algebra:

$$[a_0\ a_1\ \dots\ a_{n-1}] \cdot \begin{bmatrix} b_0 & b_1 & \dots & b_{n-1} \\ -b_{n-1} & b_0 & \dots & b_{n-2} \\ \vdots & & \vdots & \\ -b_1 & -b_2 & \dots & b_0 \end{bmatrix} = [c_0\ c_1\ \dots\ c_{n-1}],$$

with $c(x) = a(x) \cdot b(x) \bmod (x^n+1)$

- Quasi-linear time multiplication
- It's even practical, for $q = 1 \bmod 2n$ (number-theory transform)

The Ring-SIS problem

SIS

Given $\mathbf{a}_i, \ldots, \mathbf{a}_m \leftarrow U(\mathbb{Z}_q^n)$, find $\mathbf{s} \in \mathbb{Z}^m$ s.t.

$$0 < \|\mathbf{s}\| \leq \beta \;\text{ and }\; \sum s_i \cdot \mathbf{a}_i = \mathbf{0} \mod q$$

Ring-SIS

Given $a_1, \ldots, a_m \leftarrow U(R_q)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \;\text{ and }\; \sum s_i \cdot a_i = 0 \mod q$$

- Here $\sigma_C(\mathbf{s}) = (\ \sigma_C(s_1)| \ldots |\sigma_C(s_m)\ ) \in \mathbb{C}^{nm}$
- The m of Ring-SIS should be taken n times smaller than that of SIS, for fair comparison
- Ring-SIS leads to fast signatures

The Ring-SIS problem

SIS

Given $\mathbf{a}_i, \ldots, \mathbf{a}_m \leftarrow U(\mathbb{Z}_q^n)$, find $\mathbf{s} \in \mathbb{Z}^m$ s.t.

$$0 < \|\mathbf{s}\| \leq \beta \text{ and } \sum s_i \cdot \mathbf{a}_i = \mathbf{0} \mod q$$

Ring-SIS

Given $a_1, \ldots, a_m \leftarrow U(R_q)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \text{ and } \sum s_i \cdot a_i = 0 \bmod q$$

- Here $\sigma_C(\mathbf{s}) = (\ \sigma_C(s_1)| \ldots |\sigma_C(s_m)\ ) \in \mathbb{C}^{nm}$
- The m of Ring-SIS should be taken n times smaller than that of SIS, for fair comparison
- Ring-SIS leads to fast signatures

The Ring-SIS problem

SIS

Given $\mathbf{a}_i, \ldots, \mathbf{a}_m \leftarrow U(\mathbb{Z}_q^n)$, find $\mathbf{s} \in \mathbb{Z}^m$ s.t.

$$0 < \|\mathbf{s}\| \leq \beta \text{ and } \sum s_i \cdot \mathbf{a}_i = \mathbf{0} \mod q$$

Ring-SIS

Given $a_1, \ldots, a_m \leftarrow U(R_q)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \text{ and } \sum s_i \cdot a_i = 0 \bmod q$$

- Here $\sigma_C(\mathbf{s}) = (\ \sigma_C(s_1)| \ldots |\sigma_C(s_m)\ ) \in \mathbb{C}^{nm}$
- The m of Ring-SIS should be taken n times smaller than that of SIS, for fair comparison
- Ring-SIS leads to fast signatures

Ring-SIS and ideal lattices

Worst-case to average-case reduction [LyMi06,PeRo06,PeRo07]

Any ppt **Ring-SIS** algorithm succeeding with non-negligible probability leads to a ppt **Ideal-SVP**$_\gamma$ algorithm, with $\gamma, q \gg \sqrt{n}\beta$

- This result is for $R = \mathbb{Z}[x]/(x^n + 1)$ with n a power of 2
- It extends to any sequence of rings of integers R_n of degree n number field K_n, assuming that:
  - R_n is known,
  - $|\det \sigma_C(R_n)| \leq n^{O(n)}$.

A weak variant of Ring-SIS

Ring-SIS

Given $a_1, \ldots, a_m \leftarrow U(R_q)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \quad \text{and} \quad \sum s_i a_i = 0 \bmod q$$

Take $R = \mathbb{Z}[X]/(X^n - 1)$.

- We have $X^n - 1 = (X-1) \cdot Q(X)$ for $Q(X) = 1 + \ldots + X^{n-1}$
- By the CRT: $R \cong \mathbb{Z}[X]/(X-1) \times \mathbb{Z}[X]/Q(X)$

We can solve mod $X - 1$ and mod $Q(X)$, and CRT-reconstruct.

- Mod Q: Choose $s_i = 0$ for all i
- Mod $X - 1$: fix $s_1 = 1$ for all i

With probability $1/q$, we have $\sum s_i a_i = 0 \bmod (q, X-1)$.

A weak variant of Ring-SIS

Ring-SIS

Given $a_1, \ldots, a_m \leftarrow U(R_q)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \quad \text{and} \quad \sum s_i a_i = 0 \bmod q$$

Take $R = \mathbb{Z}[X]/(X^n - 1)$.

- We have $X^n - 1 = (X-1) \cdot Q(X)$ for $Q(X) = 1 + \ldots + X^{n-1}$
- By the CRT: $R \cong \mathbb{Z}[X]/(X-1) \times \mathbb{Z}[X]/Q(X)$

We can solve mod $X - 1$ and mod $Q(X)$, and CRT-reconstruct.

- Mod Q: Choose $s_i = 0$ for all i
- Mod $X - 1$: fix $s_1 = 1$ for all i

  With probability $1/q$, we have $\sum s_i a_i = 0 \bmod (q, X-1)$.

Roadmap

1- Ideal lattices

2- Ring-SIS

3- **Ring-LWE**

4- Other lattices from algebraic number theory

Challenge distributions

LWE challenge distribution $A_{\mathbf{s},\phi}$

For $\mathbf{s} \in \mathbb{Z}_q^n$ secret and ϕ a small (error) distribution over $\mathbb{Z}$, a sample from $A_{\mathbf{s},\phi}$ is of the form

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^{n+1} \text{ with } \mathbf{a} \leftarrow U(\mathbb{Z}_q^n),\ e \leftarrow \phi$$

For a cost $\widetilde{O}(n)$, we give out **one $\mathbb{Z}_q$-hint** on $\mathbf{s}$

Ring-LWE challenge distribution $A^R_{s,\phi}$

For $s \in R_q$ secret and ϕ a small (error) distribution over R, a sample from $A^R_{s,\phi}$ is of the form:

$$(a, a \cdot s + e) \in R_q^2 \text{ with } a \leftarrow U(R_q),\ e \leftarrow \phi$$

For a cost $\widetilde{O}(n)$, we give out n **($\mathbb{Z}_q$)-hints** on s.

Challenge distributions

LWE challenge distribution $A_{\mathbf{s},\phi}$

For $\mathbf{s} \in \mathbb{Z}_q^n$ secret and ϕ a small (error) distribution over $\mathbb{Z}$, a sample from $A_{\mathbf{s},\phi}$ is of the form

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^{n+1} \text{ with } \mathbf{a} \leftarrow U(\mathbb{Z}_q^n), \; e \leftarrow \phi$$

For a cost $\widetilde{O}(n)$, we give out **one $\mathbb{Z}_q$-hint** on $\mathbf{s}$

Ring-LWE challenge distribution $A^R_{s,\phi}$

For $s \in R_q$ secret and ϕ a small (error) distribution over R, a sample from $A^R_{s,\phi}$ is of the form:

$$(a, a \cdot s + e) \in R_q^2 \text{ with } a \leftarrow U(R_q), \; e \leftarrow \phi$$

For a cost $\widetilde{O}(n)$, we give out n **$(\mathbb{Z}_q)$-hints** on s.

Challenge distributions

LWE challenge distribution $A_{\mathbf{s},\phi}$

For $\mathbf{s} \in \mathbb{Z}_q^n$ secret and ϕ a small (error) distribution over $\mathbb{Z}$, a sample from $A_{\mathbf{s},\phi}$ is of the form

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^{n+1} \text{ with } \mathbf{a} \leftarrow U(\mathbb{Z}_q^n),\ e \leftarrow \phi$$

For a cost $\widetilde{O}(n)$, we give out **one $\mathbb{Z}_q$-hint** on $\mathbf{s}$

Ring-LWE challenge distribution $A^R_{s,\phi}$

For $s \in R_q$ secret and ϕ a small (error) distribution over R, a sample from $A^R_{s,\phi}$ is of the form:

$$(a, a \cdot s + e) \in R_q^2 \text{ with } a \leftarrow U(R_q),\ e \leftarrow \phi$$

For a cost $\widetilde{O}(n)$, we give out n **($\mathbb{Z}_q$)-hints** on s.

Challenge distributions

LWE challenge distribution $A_{\mathbf{s},\phi}$

For $\mathbf{s} \in \mathbb{Z}_q^n$ secret and ϕ a small (error) distribution over $\mathbb{Z}$, a sample from $A_{\mathbf{s},\phi}$ is of the form

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{Z}_q^{n+1} \quad \text{with} \quad \mathbf{a} \leftarrow U(\mathbb{Z}_q^n),\ e \leftarrow \phi$$

For a cost $\widetilde{O}(n)$, we give out **one $\mathbb{Z}_q$-hint** on $\mathbf{s}$

Ring-LWE challenge distribution $A_{s,\phi}^R$

For $s \in R_q$ secret and ϕ a small (error) distribution over R, a sample from $A_{s,\phi}^R$ is of the form:

$$(a, a \cdot s + e) \in R_q^2 \quad \text{with} \quad a \leftarrow U(R_q),\ e \leftarrow \phi$$

For a cost $\widetilde{O}(n)$, we give out n **($\mathbb{Z}_q$)-hints** on s.

The Ring-LWE problem, search version

Search Ring-LWE

Set ϕ and take $s \in R_q$. The goal is to find s, given arbitrarily many samples $(a, a \cdot s + e)$ from $A^R_{s,\phi}$.

Hardness of search Ring-LWE [LyPeRe10]

Let Φ be the set of distributions ϕ s.t. for all i, $\sigma_i(\phi)$ is an independent 1-dim Gaussian with standard deviation $\approx \alpha q$.

Any ppt **search Ring-LWE** algorithm for all $\phi \in \Phi$ leads to a **quantum** ppt algorithm for **Ideal-SVP**$_\gamma$, with $\gamma, q \geq n^{O(1)}/\alpha$.

- Same assumptions on $(R_n)_n$ as for Ring-SIS
- Note that we have a distribution ensemble
- We do not know how to get a classical reduction for small q

The Ring-LWE problem, search version

Search Ring-LWE

Set ϕ and take $s \in R_q$. The goal is to find s, given arbitrarily many samples $(a, a \cdot s + e)$ from $A^R_{s,\phi}$.

Hardness of search Ring-LWE [LyPeRe10]

Let Φ be the set of distributions ϕ s.t. for all i, $\sigma_i(\phi)$ is an independent 1-dim Gaussian with standard deviation $\approx \alpha q$.

Any ppt **search Ring-LWE** algorithm for all $\phi \in \Phi$ leads to a **quantum** ppt algorithm for **Ideal-SVP**$_\gamma$, with $\gamma, q \geq n^{O(1)}/\alpha$.

- Same assumptions on $(R_n)_n$ as for Ring-SIS
- Note that we have a distribution ensemble
- We do not know how to get a classical reduction for small q

Search to decision reduction

Decision Ring-LWE

Sample ϕ and $s \leftarrow U(R_q)$. With non-negligible probability over ϕ and s, we have to distinguish between $A^R_{s,\phi}$ and $U(R_q^2)$

Decision Ring-LWE is more suited for cryptographic design

Hardness of decision Ring-LWE [LyPeRe10]

Let ϕ sampled s.t. for all i, $\sigma_i(\phi)$ is an independent Gaussian with standard deviation $\approx \alpha q$.
Let R be the ring of integers of the cyclotomic field of order m, and set $q = 1 \bmod m$ prime.
Then **search Ring-LWE** reduces to **decision Ring-LWE**.

The random choice of ϕ is not very important

Why these algebraic/arithmetic conditions?

"Let R be the ring of integers of the cyclotomic field of order m, and choose $q = 1 \bmod m$ prime."

With this q:

- $\Phi_m(X)$ splits into n distinct linear factors mod q.
- By the CRT: $R_q \cong (\mathbb{Z}_q)^n$, as rings.

Field automorphisms:

- $\tau_k : X \mapsto X^k$ for any k coprime with m
- τ_k behaves nicely with Ring-LWE samples:

$$\tau_k(as + e) = \tau_k(a)\tau_k(s) + \tau_k(e), \quad \text{with } \tau_k(e) \text{ small}$$

- Any CRT slot is sent to any other by some τ_k

Why these algebraic/arithmetic conditions?

"Let R be the ring of integers of the cyclotomic field of order m, and choose $q = 1 \bmod m$ prime."

With this q:

- $\Phi_m(X)$ splits into n distinct linear factors mod q.
- By the CRT: $R_q \cong (\mathbb{Z}_q)^n$, as rings.

Field automorphisms:

- $\tau_k : X \mapsto X^k$ for any k coprime with m
- τ_k behaves nicely with Ring-LWE samples:

$$\tau_k(as+e) = \tau_k(a)\tau_k(s) + \tau_k(e), \quad \text{with } \tau_k(e) \text{ small}$$

- Any CRT slot is sent to any other by some τ_k

Why these algebraic/arithmetic conditions?

"Let R be the ring of integers of the cyclotomic field of order m, and choose $q = 1 \bmod m$ prime."

With this q:

- $\Phi_m(X)$ splits into n distinct linear factors mod q.
- By the CRT: $R_q \cong (\mathbb{Z}_q)^n$, as rings.

Field automorphisms:

- $\tau_k : X \mapsto X^k$ for any k coprime with m
- τ_k behaves nicely with Ring-LWE samples:

$$\tau_k(as + e) = \tau_k(a)\tau_k(s) + \tau_k(e), \quad \text{with } \tau_k(e) \text{ small}$$

- Any CRT slot is sent to any other by some τ_k

Conditions on q

The choice of q seems necessary for reducing search Ring-LWE to decision Ring-LWE. However...

Modulus switching for Ring-LWE [LaSt14]

Let $q \approx q'$. Then Ring-LWE(q) reduces to Ring-LWE(q').

Arithmetic properties of q, q' play no role

Proof idea: $(a, b) \in (R_q)^2 \mapsto (\lfloor \frac{q'}{q} a \rceil, \lfloor \frac{q'}{q} b \rceil) \in (R_{q'})^2$.

- Use Gaussian rounding to ensure uniformity of $\lfloor \frac{q'}{q} a \rceil$
- Use a small secret s, to prevent noise blow-up

Conditions on q

The choice of q seems necessary for reducing search Ring-LWE to decision Ring-LWE. However...

Modulus switching for Ring-LWE [LaSt14]

Let $q \approx q'$. Then Ring-LWE(q) reduces to Ring-LWE(q').

Arithmetic properties of q, q' play no role

Proof idea: $(a, b) \in (R_q)^2 \quad \mapsto \quad (\lfloor \frac{q'}{q} a \rceil, \lfloor \frac{q'}{q} b \rceil) \in (R_{q'})^2$.

- Use Gaussian rounding to ensure uniformity of $\lfloor \frac{q'}{q} a \rceil$
- Use a small secret s, to prevent noise blow-up

Conditions on q

The choice of q seems necessary for reducing search Ring-LWE to decision Ring-LWE. However...

Modulus switching for Ring-LWE [LaSt14]

Let $q \approx q'$. Then Ring-LWE(q) reduces to Ring-LWE(q').

Arithmetic properties of q, q' play no role

Proof idea: $(a, b) \in (R_q)^2 \mapsto (\lfloor \frac{q'}{q} a \rfloor, \lfloor \frac{q'}{q} b \rfloor) \in (R_{q'})^2$.

- Use Gaussian rounding to ensure uniformity of $\lfloor \frac{q'}{q} a \rfloor$
- Use a small secret s, to prevent noise blow-up

Weak variant Ring-LWE

Take Ring-LWE with $R = \mathbb{Z}[X]/(X^n - 1)$.

- Get samples $(a_i, b_i)_{i \leq m}$ for some m
- Use the weak Ring-SIS variant solver, to find $x_1, \ldots, x_m \in R$ small and not all zero, such that $\sum_i x_i a_i = 0 \bmod q$
- If $b_i \approx a_i \cdot s_i$ for all i, then $\sum_i x_i b_i \bmod q$ is small
- If b_i is uniform, then $\sum_i x_i b_i \bmod (q, X-1)$ is uniform

More on weak variants of Ring-LWE in Kristin's talk!

Roadmap

1- Ideal lattices

2- Ring-SIS

3- Ring-LWE

4- **Other lattices from algebraic number theory**

Ring-SIS/Ring-LWE lattices

Ring-SIS

Given $a_1, \ldots, a_m \leftarrow U(R_q)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \quad \text{and} \quad \sum s_i \cdot a_i = 0 \bmod q$$

Ring-SIS is about finding **s** small and non-zero in

$$M(a_1, \ldots, a_m) = \{\mathbf{x} \in R^m : \textstyle\sum_i x_i \cdot a_i = 0 \bmod q\}.$$

This set is a rank m module over R.

- We don't know how to express Ring-SIS as an ideal lattice problem
- We could imagine that ideal lattice problems turn out to be easy, while Ring-SIS remains hard

Ring-SIS/Ring-LWE lattices

Ring-SIS

Given $a_1, \ldots, a_m \leftarrow U(R_q)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \quad \text{and} \quad \sum s_i \cdot a_i = 0 \bmod q$$

Ring-SIS is about finding **s** small and non-zero in

$$M(a_1, \ldots, a_m) = \{\mathbf{x} \in R^m : \textstyle\sum_i x_i \cdot a_i = 0 \bmod q\}.$$

This set is a rank m module over R.

- We don't know how to express Ring-SIS as an ideal lattice problem
- We could imagine that ideal lattice problems turn out to be easy, while Ring-SIS remains hard

Module lattices

Module lattices

A module lattice in K^m is a set of the form

$$M = \sum_{j \leq k} I_j \cdot \mathbf{b}_j,$$

where the I_j's are ideals and the $\mathbf{b}_j$'s are K-linearly independent

- Ideal lattices: $k = 1$
- Euclidean lattices: $R = \mathbb{Z}$

Reductions from Ideal-SVP to Ring-SIS/Ring-LWE can be extended to reductions from Module-SVP to Module-SIS/Module-LWE

Module-SIS [LaSt14]

Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \leftarrow U(R_q^k)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \quad \text{and} \quad \sum s_i \cdot \mathbf{a}_i = 0 \bmod q$$

Module lattices

Module lattices

A module lattice in K^m is a set of the form

$$M = \sum_{j \leq k} I_j \cdot \mathbf{b}_j,$$

where the I_j's are ideals and the $\mathbf{b}_j$'s are K-linearly independent

- Ideal lattices: $k = 1$
- Euclidean lattices: $R = \mathbb{Z}$

Reductions from Ideal-SVP to Ring-SIS/Ring-LWE can be extended to reductions from Module-SVP to Module-SIS/Module-LWE

Module-SIS [LaSt14]

Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \leftarrow U(R_q^k)$, find $s_1, \ldots, s_m \in R$ s.t.

$$0 < \|\sigma_C(\mathbf{s})\| \leq \beta \quad \text{and} \quad \sum s_i \cdot \mathbf{a}_i = 0 \bmod q$$

Log unit lattice – More in Chris' talk

Units

Units u are invertible elements in R. We have: $\prod_i \sigma_i(u) = 1$

Dirichlet's theorem: $R^\times \cong \langle g \rangle \times \mathbb{Z}^d$

Every unit u is of the form

$$g_0^k \cdot u_1^{k_1} \cdot \ldots \cdot u_{d-1}^{k_d}, \quad k_i \in \mathbb{Z},$$

where $\langle g \rangle \subset \mathbb{C}$ is finite, the $\langle u_i \rangle$'s are independent and infinite, and $d = n/2 - 1$ in the case of cyclotomic fields

The log-unit lattice is $\left\{ \begin{pmatrix} \log|\sigma_1(u)| \\ \vdots \\ \log|\sigma_n(u)| \end{pmatrix} : u \in R^\times \right\} \subseteq \mathbb{R}^n$.

It is related to the multiplicative structure of R

Log unit lattice – More in Chris' talk

Units

Units u are invertible elements in R. We have: $\prod_i \sigma_i(u) = 1$

Dirichlet's theorem: $R^\times \cong \langle g \rangle \times \mathbb{Z}^d$

Every unit u is of the form

$$g_0^k \cdot u_1^{k_1} \cdot \ldots \cdot u_{d-1}^{k_d}, \quad k_i \in \mathbb{Z},$$

where $\langle g \rangle \subset \mathbb{C}$ is finite, the $\langle u_i \rangle$'s are independent and infinite, and $d = n/2 - 1$ in the case of cyclotomic fields

The log-unit lattice is $\left\{ \begin{pmatrix} \log|\sigma_1(u)| \\ \vdots \\ \log|\sigma_n(u)| \end{pmatrix} : u \in R^\times \right\} \subseteq \mathbb{R}^n.$

It is related to the multiplicative structure of R

Open problems

More hardness guarantees?

- Reduction from lattice problems to ideal lattice problems?
- Or to Ring-LWE/Ring-SIS?
- Classical reduction from ideal lattice problems to Ring-LWE?

More constructions?

- Adapting to Ring-SIS/Ring-LWE all SIS/LWE constructions, with the expected efficiency gain?
- A multilinear map, **provably** secure under the assumption that lattice problems for ideal lattices are hard in the worst case?

More attacks? Can we better exploit the multiplicative structure?

Open problems

More hardness guarantees?

- Reduction from lattice problems to ideal lattice problems?
- Or to Ring-LWE/Ring-SIS?
- Classical reduction from ideal lattice problems to Ring-LWE?

More constructions?

- Adapting to Ring-SIS/Ring-LWE all SIS/LWE constructions, with the expected efficiency gain?
- A multilinear map, **provably** secure under the assumption that lattice problems for ideal lattices are hard in the worst case?

More attacks? Can we better exploit the multiplicative structure?

Open problems

More hardness guarantees?

- Reduction from lattice problems to ideal lattice problems?
- Or to Ring-LWE/Ring-SIS?
- Classical reduction from ideal lattice problems to Ring-LWE?

More constructions?

- Adapting to Ring-SIS/Ring-LWE all SIS/LWE constructions, with the expected efficiency gain?
- A multilinear map, **provably** secure under the assumption that lattice problems for ideal lattices are hard in the worst case?

More attacks? Can we better exploit the multiplicative structure?

Very partial bibliography

Books:

- P. Samuel: Algebraic theory of numbers
- H. Cohen: A course in computational algebraic theory
- H. Cohen: Advanced topics in computational number theory
- L. C. Washington: Introduction to cyclotomic fields

Selection of articles:

- C. Peikert and A. Rosen: Lattices that Admit Logarithmic Worst-Case to Average-Case Connection Factors
- V. Lybashevsky, C. Peikert and O. Regev: On Ideal Lattices and Learning with Errors Over Rings

Questions?