Structured variants of LWE
(and SIS and NTRU)

Wouter Castryck
(contains joint work with Carl Bootland, Ilia Iliashenko, Alan Szepieniec, Frederik Vercauteren)

KU Leuven
Dept. of Mathematics & COSIC
Ghent University
The LWE problem: solve a linear system

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{m-1}
\end{pmatrix} \approx \begin{pmatrix}
    a_{10} & a_{11} & \ldots & a_{1,n-1} \\
    a_{20} & a_{21} & \ldots & a_{2,n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m0} & a_{m1} & \ldots & a_{m,n-1}
\end{pmatrix} \cdot \begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix}
\]

over a finite field $\mathbb{F}_p$ for a secret $(s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_p^n$ where
1. Learning With Errors [Reg05]

The **LWE** problem: solve a linear system

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{m-1}
\end{pmatrix} \approx
\begin{pmatrix}
    a_{10} & a_{11} & \cdots & a_{1,n-1} \\
    a_{20} & a_{21} & \cdots & a_{2,n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m0} & a_{m1} & \cdots & a_{m,n-1}
\end{pmatrix}
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix}
\]

over a finite field \( \mathbb{F}_p \) for a secret \((s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_p^n\) where

- each equation is perturbed by a “small” error, i.e.

\[
b_i = a_{i0}s_0 + a_{i1}s_1 + \cdots + a_{i,n-1}s_{n-1} + e_i,
\]
1. Learning With Errors [Reg05]

The **LWE** problem: solve a linear system

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{m-1}
\end{pmatrix}
\approx
\begin{pmatrix}
  a_{10} & a_{11} & \cdots & a_{1,n-1} \\
  a_{20} & a_{21} & \cdots & a_{2,n-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{m0} & a_{m1} & \cdots & a_{m,n-1}
\end{pmatrix}
\begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix}
\]

over a finite field $\mathbb{F}_p$ for a secret $(s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_p^n$ where

- each equation is perturbed by a “small” error, i.e.

  \[
  b_i = a_{i0}s_0 + a_{i1}s_1 + \cdots + a_{i,n-1}s_{n-1} + e_i,
  \]

- the $a_{ij} \in \mathbb{F}_p$ are chosen uniformly at random,
1. Learning With Errors [Reg05]

The **LWE** problem: solve a linear system

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{m-1}
\end{pmatrix}
\approx
\begin{pmatrix}
    a_{10} & a_{11} & \ldots & a_{1,n-1} \\
    a_{20} & a_{21} & \ldots & a_{2,n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m0} & a_{m1} & \ldots & a_{m,n-1}
\end{pmatrix}
\cdot
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix}
\]

over a finite field \( \mathbb{F}_p \) for a secret \((s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_p^n\) where

- each equation is perturbed by a “small” error, i.e.

  \[
b_i = a_{i0}s_0 + a_{i1}s_1 + \cdots + a_{i,n-1}s_{n-1} + e_i,
  \]

- the \(a_{ij} \in \mathbb{F}_p\) are chosen uniformly at random,

- \(m > n\).
1. Learning With Errors [Reg05]

The **LWE** problem: solve a linear system

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{m-1}
\end{pmatrix}
= 
\begin{pmatrix}
    a_{10} & a_{11} & \cdots & a_{1,n-1} \\
    a_{20} & a_{21} & \cdots & a_{2,n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m0} & a_{m1} & \cdots & a_{m,n-1}
\end{pmatrix}
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix} +
\begin{pmatrix}
    e_0 \\
    e_1 \\
    \vdots \\
    e_{m-1}
\end{pmatrix}
\]

over a finite field \(\mathbb{F}_p\) for a secret \((s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_p^n\) where

- each equation is perturbed by a “small” error, i.e.

\[
b_i = a_{i0}s_0 + a_{i1}s_1 + \cdots + a_{i,n-1}s_{n-1} + e_i,
\]

- the \(a_{ij} \in \mathbb{F}_p\) are chosen uniformly at random,

- \(m > n\).
1. Learning With Errors [Reg05]

The errors $e_i$ are sampled independently from a discretized Gaussian with standard deviation $\sigma \gtrsim \sqrt{n}$:

When viewed jointly, the error vector

$$\begin{pmatrix} e_0 \\ \vdots \\ e_{m-1} \end{pmatrix}$$

is sampled from a spherical Gaussian.
1. Learning With Errors [Reg05]

Known attacks for $q = \text{poly}(n)$:

- **Trial and error:**
  $2^{O(n \log n)}$ time and $O(n)$ samples.

- A. Blum, A. Kalai, H. Wasserman ‘03:
  $2^{O(n)}$ time and $2^{O(n)}$ samples.

- S. Arora, R. Ge ‘11:
  $2^{O(\sigma^2 \log n)}$ time and $2^{O(\sigma^2 \log n)}$ samples.
1. Learning With Errors [Reg05]

Known attacks for $q = \text{poly}(n)$:

- Trial and error:
  
  $2^{O(n \log n)}$ time and $O(n)$ samples.

- A. Blum, A. Kalai, H. Wasserman ‘03:
  
  $2^{O(n)}$ time and $2^{O(n)}$ samples.

- S. Arora, R. Ge ‘11:
  
  $2^{O(\sigma^2 \log n)}$ time and $2^{O(\sigma^2 \log n)}$ samples.

Idea: if all errors (almost) certainly lie in $\{-T, \ldots, T\}$, then

$$\prod_{j=-T}^{T} (a_{i,0}s_0 + a_{i,1}s_1 + \cdots + a_{i,n-1}s_{n-1} - b_i - j) = 0.$$
1. Learning With Errors [Reg05]
Known attacks for $q = \text{poly}(n)$:

- Trial and error:
  $2^{O(n \log n)}$ time and $O(n)$ samples.

- A. Blum, A. Kalai, H. Wasserman ‘03:
  $2^{O(n)}$ time and $2^{O(n)}$ samples.

- S. Arora, R. Ge ‘11:
  $2^{O(\sigma^2 \log n)}$ time and $2^{O(\sigma^2 \log n)}$ samples.
  Idea: if all errors (almost) certainly lie in $\{-T, \ldots, T\}$, then
  \[
  \prod_{j=-T}^{T} (a_{i,0}s_0 + a_{i,1}s_1 + \cdots + a_{i,n-1}s_{n-1} - b_i - j) = 0.
  \]
  View as linear system of equations in $\approx n^{2T}$ monomials.
LWE is tightly related to classical lattice problems.

- Can be thought of as an instance of BDD inside the lattice

\[
\left( \mathbb{Z}/p\mathbb{Z} \right)^m \cap \{ \mathbf{w} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}^n : \mathbf{w} \equiv A\cdot \mathbf{s} \mod p \} \cap \mathbb{Z}^m.
\]
LWE is tightly related to classical lattice problems.

- Can be thought of as an instance of BDD inside the lattice

\[
(p\mathbb{Z})^m \cap \{ w \in \mathbb{Z}^m | \exists s \in \mathbb{Z}^n : w \equiv A \cdot s \mod p \} \cap \mathbb{Z}^m.
\]

- Proven to be at least as hard as quantum SIVP.
1. Learning With Errors (LWE)

Features:

- hardness reduction from famous lattice problems,
- versatile building block for cryptography, enabling exciting applications (post-quantum crypto, FHE, ...)

\[
\begin{bmatrix}
    b_0 \\
    b_1 \\
    ... \\
    b_{m-1}
\end{bmatrix} \approx 
\begin{bmatrix}
    a_{10} \\
    a_{11} \\
    ... \\
    a_{1,n-1} \\
    a_{20} \\
    a_{21} \\
    ... \\
    a_{m,0} \\
    a_{m,1} \\
    ... \\
    a_{m,n-1}
\end{bmatrix} \cdot 
\begin{bmatrix}
    s_0 \\
    s_1 \\
    ... \\
    s_{n-1}
\end{bmatrix}.
\]

↑ ↑ ↑

\[m \log p + n \log p + n \log p\]
1. Learning With Errors (LWE)

Features:
- hardness reduction from famous lattice problems,
- versatile building block for cryptography, enabling exciting applications (post-quantum crypto, FHE, ...)

Drawback: key size.
- To hide the secret one needs an entire linear system:

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{m-1}
\end{pmatrix}
\approx
\begin{pmatrix}
    a_{10} & a_{11} & \ldots & a_{1,n-1} \\
    a_{20} & a_{21} & \ldots & a_{2,n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m0} & a_{m1} & \ldots & a_{m,n-1}
\end{pmatrix}
\cdot
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix}
\]

\[m \log p \approx mn \log p \approx n \log p\]
2. Ring-based LWE?

Idea:

- Identify key space

\[ \mathbb{F}_p^n \quad \text{with} \quad \frac{\mathbb{Z}[x]}{(p, f(x))} \]

for some monic deg \( n \) polynomial \( f(x) \in \mathbb{Z}[x] \), by viewing

\( (s_0, s_1, \ldots, s_{n-1}) \) as \( s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-1} x^{n-1} \).
2. Ring-based LWE?

Idea:

► Identify key space

\[ \mathbb{F}_p^n \text{ with } \frac{\mathbb{Z}[x]}{(p, f(x))} \]

for some monic deg \( n \) polynomial \( f(x) \in \mathbb{Z}[x] \), by viewing

\((s_0, s_1, \ldots, s_{n-1})\) as \( s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-1} x^{n-1} \).

► Replace every block of \( n \) eqns by a block of the form

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{n-1}
\end{pmatrix}
\approx
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix}
\text{ with } A_a \text{ the matrix of multiplication by some random } a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.\]
2. Ring-based LWE?

Idea:

- Identify key space $\mathbb{F}_p^n$ with $\mathbb{Z}[x]/(p, f(x))$ for some monic degree $n$ polynomial $f(x) \in \mathbb{Z}[x]$, by viewing $(s_0, s_1, \ldots, s_{n-1})$ as $s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-1} x^{n-1}$.

- Replace every block of $n$ eqns by a block of the form

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} \approx A_{a} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}$$

with $A_a$ the matrix of multiplication by some random $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$.

- Store $a(x)$ rather than $A_a$: saves factor $n$. 

Example:

- If \( f(x) = x^n - 1 \), then \( A_a \) is a **circulant matrix**

\[
\begin{pmatrix}
  a_0 & a_{n-1} & \ldots & a_2 & a_1 \\
  a_1 & a_0 & \ldots & a_3 & a_2 \\
  a_2 & a_1 & \ldots & a_4 & a_3 \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  a_{n-1} & a_{n-2} & \ldots & a_1 & a_0 \\
\end{pmatrix}
\]

of which it suffices to store the first column.
2. Ring-based LWE?

Example:

- if \( f(x) = x^n - 1 \), then \( A_a \) is a circulant matrix

\[
\begin{pmatrix}
a_0 & a_{n-1} & \ldots & a_2 & a_1 \\
a_1 & a_0 & \ldots & a_3 & a_2 \\
a_2 & a_1 & \ldots & a_4 & a_3 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
a_{n-1} & a_{n-2} & \ldots & a_1 & a_0
\end{pmatrix}
\]

of which it suffices to store the first column.

- Bad example, because of . . .
3. Ring-based LWE?

Potential threat:

smallness preserving homomorphisms to smaller rings.

▶ Suppose e.g. that $f(1) \equiv 0 \mod p$, then

$$R_p := \frac{\mathbb{Z}[x]}{(p, f(x))} \rightarrow \mathbb{F}_p : r(x) \mapsto r(1) = r_0 + r_1 + \cdots + r_{n-1},$$

is a well-defined ring homomorphism.
3. Ring-based LWE?

Potential threat:

smallness preserving homomorphisms to smaller rings.

- Suppose e.g. that $f(1) \equiv 0 \mod p$, then

$$R_p := \frac{\mathbb{Z}[x]}{(p, f(x))} \rightarrow \mathbb{F}_p : r(x) \mapsto r(1) = r_0 + r_1 + \cdots + r_{n-1},$$

is a well-defined ring homomorphism.

- Our ring-based LWE samples

$$b(x) = a(x) \cdot s(x) + e(x)$$

evaluate to

$$b(1) = a(1) \cdot s(1) + e(1).$$
3. Ring-based LWE?

Potential threat:
smallness preserving homomorphisms to smaller rings.

- Suppose e.g. that \( f(1) \equiv 0 \mod p \), then

\[
R_p := \frac{\mathbb{Z}[x]}{(p, f(x))} \rightarrow \mathbb{F}_p : r(x) \mapsto r(1) = r_0 + r_1 + \cdots + r_{n-1},
\]

is a well-defined ring homomorphism.

- Our ring-based LWE samples

\[
b(x) = a(x) \cdot s(x) + e(x)
\]

evaluate to

\[
b(1) = a(1) \cdot s(1) + e(1).
\]

- For each guess for \( s(1) \in \mathbb{F}_p \), analyze distribution of \( e(1) \).
3. Ring-based LWE?

Potential threat:

- smallness preserving homomorphisms to smaller rings.

▶ Suppose e.g. that \( f(1) \equiv 0 \mod p \), then

\[
R_p := \frac{\mathbb{Z}[x]}{(p, f(x))} \rightarrow \mathbb{F}_p : r(x) \mapsto r(1) = r_0 + r_1 + \cdots + r_{n-1},
\]

is a well-defined ring homomorphism.

▶ Our ring-based LWE samples

\[
b(x) = a(x) \cdot s(x) + e(x)
\]
evaluate to

\[
b(1) = a(1) \cdot s(1) + e(1).
\]

▶ For each guess for \( s(1) \in \mathbb{F}_p \), analyze distribution of \( e(1) \).

▶ Non-uniformity might reveal \( s(1) \).
3. Ring-based LWE?

A lattice point of view:
3. Ring-based LWE?

A lattice point of view:
3. Ring-based LWE?

A lattice point of view:
3. Ring-based LWE?

A lattice point of view:
3. Ring-based LWE?

Safety measure: restrict to irreducible \( f(x) \in \mathbb{Z}[x] \).

- Rules out examples like \( x^n - 1 \).
- Resulting problem is often called Poly-LWE [SSTX09].
- Notice: our ‘parent ring’

\[
R = \frac{\mathbb{Z}[x]}{(f(x))}
\]

is an order in the number field \( K = \mathbb{Q}[x]/(f(x)) \).
3. Ring-based LWE?

Safety measure: restrict to irreducible $f(x) \in \mathbb{Z}[x]$.

- Rules out examples like $x^n - 1$.
- Resulting problem is often called Poly-LWE [SSTX09].
- Notice: our ‘parent ring’

\[
R = \frac{\mathbb{Z}[x]}{(f(x))}
\]

is an order in the number field $K = \mathbb{Q}[x]/(f(x))$.

Does this really solve our problem?

- No! E.g., $f(x) = x^n + (p - 1)$ suffers from same problem.
- Possible to make examples where $K/\mathbb{Q}$ is Galois [EHL14].
  $\sim s(1)$ is enough to reconstruct $s$ completely!
3. Ring-based LWE?

Safety measure: restrict to irreducible $f(x) \in \mathbb{Z}[x]$.

- Rules out examples like $x^n - 1$.
- Resulting problem is often called Poly-LWE [SSTX09].
- Notice: our ‘parent ring’

$$R = \frac{\mathbb{Z}[x]}{(f(x))}$$

is an order in the number field $K = \mathbb{Q}[x]/(f(x))$.

Does this really solve our problem?

- No! E.g., $f(x) = x^n + (p - 1)$ suffers from same problem.
- Possible to make examples where $K/\mathbb{Q}$ is Galois [EHL14].
  $\rightsquigarrow \mathbf{s}(1)$ is enough to reconstruct $\mathbf{s}$ completely!

Ring-LWE: choose more ‘canonical’ error distribution [LPR12].
4. Ring-LWE [LPR12]

Direct ring-based analogue of LWE-sample would read

\[
\begin{pmatrix}
b_0 \\
b_1 \\
\vdots \\
b_{n-1}
\end{pmatrix}
= \begin{pmatrix}
a \\
a \\
\vdots \\
a
\end{pmatrix}
\cdot 
\begin{pmatrix}
s_0 \\
s_1 \\
\vdots \\
s_{n-1}
\end{pmatrix}
+ 
\begin{pmatrix}
e_0 \\
e_1 \\
\vdots \\
e_{n-1}
\end{pmatrix}
\]

with the \( e_i \) sampled independently from

\[ N(0, \sigma) \]

for some fixed small \( \sigma = \sigma(n) \).

This is not Ring-LWE!
4. Ring-LWE [LPR12]

So what is Ring-LWE? Samples look like

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix}
= A_a \cdot
\begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix}
+ \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
\]
4. Ring-LWE [LPR12]
So what is Ring-LWE? Samples look like

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix} = A_a \cdot \begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
\]

where

- \( B \) is the **canonical embedding** matrix,
- \( A_{f'(x)} \) compensates for the fact that one actually picks secrets from the **dual**.
4. Ring-LWE [LPR12]

So what is Ring-LWE? Samples look like

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix} = A_a \cdot \begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
\]

where

- \( B \) is the canonical embedding matrix,
- \( A_{f'(x)} \) compensates for the fact that one actually picks secrets from the dual.

At least as hard as quantum Ideal-SIVP.
4. Ring-LWE [LPR12]

So what is Ring-LWE? Samples look like

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix}
= A_a \cdot
\begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix}
+ A_{f'(x)} \cdot B^{-1} \cdot
\begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
\]

where

- \( B \) is the canonical embedding matrix,
- \( A_{f'(x)} \) compensates for the fact that one actually picks secrets from the dual.

At least as hard as quantum Ideal-SIVP.

Note:
- factor \( A_{f'(x)} \cdot B^{-1} \) might skew the error distribution,
4. Ring-LWE [LPR12]  
So what is Ring-LWE? Samples look like

\[
\begin{pmatrix}
 b_0 \\
 b_1 \\
 \vdots \\
 b_{n-1}
\end{pmatrix}
= A_a \cdot \begin{pmatrix}
 s_0 \\
 s_1 \\
 \vdots \\
 s_{n-1}
\end{pmatrix}
+ A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix}
 e_0 \\
 e_1 \\
 \vdots \\
 e_{n-1}
\end{pmatrix}
\]

where

- \(B\) is the canonical embedding matrix,
- \(A_{f'(x)}\) compensates for the fact that one actually picks secrets from the dual.

At least as hard as quantum Ideal-SIVP.

Note:

- factor \(A_{f'(x)} \cdot B^{-1}\) might skew the error distribution,
- but also scales it!
4. Ring-LWE [LPR12]

...but also scales it!

\[
\begin{pmatrix}
 b_0 \\
 b_1 \\
 \vdots \\
 b_{n-1}
\end{pmatrix}
= A_a \cdot \begin{pmatrix}
 s_0 \\
 s_1 \\
 \vdots \\
 s_{n-1}
\end{pmatrix}
+ A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix}
 e_0 \\
 e_1 \\
 \vdots \\
 e_{n-1}
\end{pmatrix}
\]

Indeed, one has

- \(\det A_{f'(x)} = \Delta\) with

\[
\Delta = |\text{disc } f(x)|,
\]

\(\leftarrow\) typically huge
4. Ring-LWE [LPR12]

...but also scales it!

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix}
= A_a \cdot 
\begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix}
+ A_{f'(x)} \cdot B^{-1} \cdot 
\begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
\]

Indeed, one has

- \( \det A_{f'(x)} = \Delta \) with
  \[
  \Delta = |\text{disc } f(x)|, \quad \leftarrow \text{typically huge}
  \]
- \( \det B^{-1} = 1/\sqrt{\Delta} \).
4. Ring-LWE [LPR12]

... but also scales it!

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix}
= A_a \cdot \begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
\]

Indeed, one has

\[
\det A_{f'(x)} = \Delta \quad \text{with}
\]

\[
\Delta = |\text{disc } f(x)|, \quad \leftarrow \text{typically huge}
\]

\[
\det B^{-1} = 1/\sqrt{\Delta}.
\]

So “on average”, each \( e_i \) is scaled up by \( \sqrt{\Delta}^{1/n} \) ... 

\[
\leftarrow \quad \text{... but remember: skewness.}
\]
4. Ring-LWE [LPR12]

Main example: 2-power cyclotomics $f(x) = x^n + 1$ with $n = 2^k$.

$$
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix} = A_a \cdot \begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix} + A_{f'}(x) \cdot B^{-1} \cdot \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
$$

- $f'(x) = nx^{n-1} = n \times \text{unit}$, so

  $$A_{f'}(x) = n \times \text{orthogonal matrix},$$

- all singular values of $B$ are $\sqrt{n}$, so

  $$B^{-1} = \frac{1}{\sqrt{n}} \times \text{orthogonal matrix},$$
4. Ring-LWE [LPR12]

Main example: 2-power cyclotomies $f(x) = x^n + 1$ with $n = 2^k$.

$$
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix}
= \begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix}
+ \sqrt{n} \cdot \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
$$

▶ $f'(x) = nx^{n-1} = n \times \text{unit}$, so

$$A_{f'}(x) = n \times \text{orthogonal matrix},$$

▶ all singular values of $B$ are $\sqrt{n}$, so

$$B^{-1} = \frac{1}{\sqrt{n}} \times \text{orthogonal matrix},$$

Therefore Ring-LWE = Poly-LWE in this case.
5. A wrong instantiation

Recall: successful attack on Ring-LWE

\[ \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + A f'(x) \cdot B^{1/2} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}. \]

But:
\[ \det B^{-1} = \frac{1}{\sqrt{\Delta}}, \text{ so the errors get squeezed.} \]
\[ \text{To compensate, they scale up the errors by a factor } \sqrt{\frac{\Delta}{n}}. \]
5. A wrong instantiation

Recall: successful attack on Ring-LWE

\[ \Downarrow \]
quantum solution to SIVP in ideal lattices.

[۴۶۲۱۵] announced successful evaluation-at-1 attack

\[ \sim \] but for convenience picked non-dual secrets:

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix} = A_a \cdot \begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix} + \overbrace{A_{r(x)}} B^{-1} \cdot \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}.
\]
5. A wrong instantiation

Recall: successful attack on Ring-LWE

\[ \Downarrow \]

quantum solution to SIVP in ideal lattices.

[ELOS15] announced successful evaluation-at-1 attack

\[ \rightsquigarrow \] but for convenience picked non-dual secrets:

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{n-1}
\end{pmatrix} = A_a \cdot \begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix} + A_f(x) \cdot B^{-1} \cdot \begin{pmatrix}
    e_0 \\
    e_1 \\
    \vdots \\
    e_{n-1}
\end{pmatrix}.
\]

But:

\[ \text{det } B^{-1} = \frac{1}{\sqrt{\Delta}}, \text{ so the errors get squeezed.} \]
5. A wrong instantiation

Recall: successful attack on Ring-LWE

\[ \Downarrow \]

quantum solution to SIVP in ideal lattices.

[ELOS15] announced successful evaluation-at-1 attack

\[ \sim \] but for convenience picked non-dual secrets:

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{n-1}
\end{pmatrix}
= A_a \cdot 
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix}
+ A_{f'(x)} \cdot 
\begin{pmatrix}
    e_0 \\
    e_1 \\
    \vdots \\
    e_{n-1}
\end{pmatrix}.
\]

But:

- \[ \det B^{-1} = 1/\sqrt{\Delta}, \] so the errors get squeezed.

- To compensate, they scale up the errors by a factor \( \sqrt{\Delta}^{1/n} \).
5. A wrong instantiation

Issue:

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{n-1}
\end{pmatrix}
= A_a \cdot 
\begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{n-1}
\end{pmatrix}
+ \sqrt{\Delta^{1/n}} B^{-1} \cdot 
\begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{n-1}
\end{pmatrix}
\]

▶ The factor \( \sqrt{\Delta^{1/n}} \) compensates for \( B^{-1} \) only “on average”.

Aussois, March 22, 2019
5. A wrong instantiation

Issue:

\[
\begin{pmatrix}
 b_0 \\
 b_1 \\
 \vdots \\
 b_{n-1}
\end{pmatrix}
= \begin{pmatrix}
 s_0 \\
 s_1 \\
 \vdots \\
 s_{n-1}
\end{pmatrix}
+ \sqrt{\Delta}^{1/n} \begin{pmatrix}
 e_0 \\
 e_1 \\
 \vdots \\
 e_{n-1}
\end{pmatrix}.
\]

- The factor $\sqrt{\Delta}^{1/n}$ compensates for $B^{-1}$ only “on average”.
- In some coordinates $B^{-1}$ could scale down much more.

Compensation factor is insufficient

$\Rightarrow$ merely rounding yields exact equations in the secret!
5. A wrong instantiation

- Concrete example: $f(x) = x^{256} + 8190$, $p = 8191$.
- Standard deviations even form a geometric series!

Error distribution in each coordinate (experimental):

![Graph showing error distribution in each coordinate](image_url)
5. A wrong instantiation

- Concrete example: $f(x) = x^{256} + 8190$, $p = 8191$.
- Standard deviations even form a geometric series!

Error distribution in each coordinate (experimental):
Recall: LWE is about solving a noisy system of linear equations

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{m-1}
\end{pmatrix}
= \begin{pmatrix}
    a_{10} & a_{11} & \ldots & a_{1,n-1} \\
    a_{20} & a_{21} & \ldots & a_{2,n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m0} & a_{m1} & \ldots & a_{m,n-1}
\end{pmatrix}
\cdot
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix}
+ \begin{pmatrix}
    e_0 \\
    e_1 \\
    \vdots \\
    e_{m-1}
\end{pmatrix}
\]

in \( \mathbb{F}_p^n \).
6. Module-LWE [LS15]

Recall: LWE is about solving a noisy system of linear equations

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{m-1}
\end{pmatrix}
= \begin{pmatrix}
    a_{10} & a_{11} & \cdots & a_{1,n-1} \\
    a_{20} & a_{21} & \cdots & a_{2,n-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m0} & a_{m1} & \cdots & a_{m,n-1}
\end{pmatrix}
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{n-1}
\end{pmatrix}
+ \begin{pmatrix}
    e_0 \\
    e_1 \\
    \vdots \\
    e_{m-1}
\end{pmatrix}
\]

in \( \mathbb{F}_p^n \).

In Ring-LWE we replace \( A \) by a matrix of multiplication \( A_a \) with

\[
a \in R_p = \frac{\mathbb{Z}[x]}{(p, f(x))} \cong \mathbb{F}_p^n.
\]
6. Module-LWE [LS15]

Let $n = \ell \cdot \ell'$. Module-LWE is about solving a noisy system

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{k-1}
\end{pmatrix}
= \begin{pmatrix}
  a_{10} & a_{11} & \cdots & a_{1,\ell-1} \\
  a_{20} & a_{21} & \cdots & a_{2,\ell-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{k0} & a_{k1} & \cdots & a_{k,\ell-1}
\end{pmatrix}
\begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{\ell-1}
\end{pmatrix}
+ \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{k-1}
\end{pmatrix}
\]

in $R_{\ell}^p$, where $R_{\ell}^p = \mathbb{Z}[x]/(f(x))$, $f(x)$ is monic irreducible of degree $\ell'$, and all $e_i$ are sampled as in Ring-LWE.
6. Module-LWE [LS15]

Let \( n = \ell \cdot \ell' \). Module-LWE is about solving a noisy system

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{k-1}
\end{pmatrix} = \begin{pmatrix}
  a_{10} & a_{11} & \cdots & a_{1,\ell-1} \\
  a_{20} & a_{21} & \cdots & a_{2,\ell-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{k0} & a_{k1} & \cdots & a_{k,\ell-1}
\end{pmatrix} \cdot \begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{\ell-1}
\end{pmatrix} + \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{k-1}
\end{pmatrix}
\]

in \( R^\ell_p \), where

\[
R_p = \frac{\mathbb{Z}[x]}{(f(x))}, \quad f(x) \text{ monic irreducible of degree } \ell',
\]

and all \( e_i \) are sampled as in Ring-LWE.
6. Module-LWE [LS15]

Let $n = \ell \cdot \ell'$. Module-LWE is about solving a noisy system

$$
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{k-1}
\end{pmatrix} =
\begin{pmatrix}
    a_{10} & a_{11} & \cdots & a_{1,\ell-1} \\
    a_{20} & a_{21} & \cdots & a_{2,\ell-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{k0} & a_{k1} & \cdots & a_{k,\ell-1}
\end{pmatrix} \cdot
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{\ell-1}
\end{pmatrix} +
\begin{pmatrix}
    e_0 \\
    e_1 \\
    \vdots \\
    e_{k-1}
\end{pmatrix}
$$

in $R^\ell_p$, where

$$R_p = \frac{\mathbb{Z}[x]}{(f(x))}, \quad f(x) \text{ monic irreducible of degree } \ell',$$

and all $e_i$ are sampled as in Ring-LWE.

This fills $A$ blockwise with matrices of multiplication.
6. Module-LWE [LS15]

Let \( n = \ell \cdot \ell' \). Module-LWE is about solving a noisy system

\[
\begin{pmatrix}
    b_0 \\
    b_1 \\
    \vdots \\
    b_{k-1}
\end{pmatrix}
= \begin{pmatrix}
    a_{10} & a_{11} & \cdots & a_{1,\ell-1} \\
    a_{20} & a_{21} & \cdots & a_{2,\ell-1} \\
     & & \ddots & \vdots \\
    a_{k0} & a_{k1} & \cdots & a_{k,\ell-1}
\end{pmatrix}
\begin{pmatrix}
    s_0 \\
    s_1 \\
    \vdots \\
    s_{\ell-1}
\end{pmatrix}
+ \begin{pmatrix}
    e_0 \\
    e_1 \\
    \vdots \\
    e_{k-1}
\end{pmatrix}
\]

in \( R_p^\ell \), where

\[
R_p = \frac{\mathbb{Z}[x]}{(f(x))}, \quad f(x) \text{ monic irreducible of degree } \ell',
\]

and all \( e_i \) are sampled as in Ring-LWE.

This fills \( A \) blockwise with matrices of multiplication.

At least as hard as quantum Module-SIVP.
Matrix version of the NTRU problem:

- Consider two $n \times n$ matrices

\[ A = (a_{ij}), \quad B = (b_{ij}) \in \mathbb{F}_p^{n \times n} \]

with $a_{ij}, b_{ij}$ sampled randomly from a narrow distribution. If $\det B = 0$, start over.
Matrix version of the NTRU problem:

- Consider two $n \times n$ matrices

$$A = (a_{ij}), \quad B = (b_{ij}) \quad \in \mathbb{F}_p^{n \times n}$$

with $a_{ij}, b_{ij}$ sampled randomly from a narrow distribution. If $\det B = 0$, start over.

- Compute

$$H = AB^{-1} \in \mathbb{F}_p^{n \times n}.$$
7. Variants of NTRU [HPS98], [CG05]

Matrix version of the NTRU problem:

- Consider two \( n \times n \) matrices

\[
A = (a_{ij}), \quad B = (b_{ij}) \quad \in \mathbb{F}_p^{n \times n}
\]

with \( a_{ij}, b_{ij} \) sampled randomly from a narrow distribution. If \( \det B = 0 \), start over.

- Compute

\[
H = AB^{-1} \in \mathbb{F}_p^{n \times n}.
\]

- Problem: given \( H \), find small \( A, B \in \mathbb{F}_p^{n \times n} \) with \( H = AB^{-1} \).
7. Variants of NTRU [HPS98], [CG05]

Matrix version of the NTRU problem:

- Consider two $n \times n$ matrices

$$A = (a_{ij}), \quad B = (b_{ij}) \in \mathbb{F}_p^{n \times n}$$

with $a_{ij}, b_{ij}$ sampled randomly from a narrow distribution. If $\det B = 0$, start over.

- Compute

$$H = AB^{-1} \in \mathbb{F}_p^{n \times n}.$$

- Problem: given $H$, find small $A, B \in \mathbb{F}_p^{n \times n}$ with $H = AB^{-1}$.

Best-known version of the NTRU problem:

- Replace $A, B$ by matrices of multiplication $A_a, B_b$ for small

$$a, b \in R_p = \mathbb{Z}[x]/(f(x)), \quad f(x) \text{ monic irr. of deg } n.$$
7. Variants of NTRU [HPS98], [CG05]

Module version of NTRU:

Let \( n = \ell \times \ell' \). Consider two \( \ell \times \ell \) matrices

\[
A = (a_{ij}), \quad B = (b_{ij}) \quad \in \quad R^{\ell \times \ell}_p
\]

with

\[
a_{ij}, b_{ij} \in R_p = \mathbb{Z}[x]/(f(x)), \quad f(x) \text{ monic irr. of deg } \ell'
\]

sampled randomly from a narrow distribution. If \( B \) not invertible, start over.
7. Variants of NTRU [HPS98], [CG05]

Module version of NTRU:

- Let \( n = \ell \times \ell' \). Consider two \( \ell \times \ell \) matrices

\[
A = (a_{ij}), \quad B = (b_{ij}) \in \mathbb{R}_{p}^{\ell \times \ell}
\]

with

\[
a_{ij}, b_{ij} \in \mathbb{R}_{p} = \mathbb{Z}[x]/(f(x)), \quad f(x) \text{ monic irr. of deg } \ell'
\]

sampled randomly from a narrow distribution.

If \( B \) not invertible, start over.

- Compute

\[
H = AB^{-1} \in \mathbb{R}_{p}^{\ell \times \ell}.
\]
Module version of NTRU:

Let $n = \ell \times \ell'$. Consider two $\ell \times \ell$ matrices

$$A = (a_{ij}), \quad B = (b_{ij}) \in R_p^{\ell \times \ell}$$

with

$$a_{ij}, b_{ij} \in R_p = \mathbb{Z}[x]/(f(x)), \quad f(x) \text{ monic irr. of deg } \ell'$$

sampled randomly from a narrow distribution. If $B$ not invertible, start over.

Compute

$$H = AB^{-1} \in R_p^{\ell \times \ell}.$$ 

Problem: given $H$, find small $A, B \in R_p^{\ell \times \ell}$ with $H = AB^{-1}$. 
Remark: if \( \ell \) is small, e.g.,

\[
H = \frac{A}{B} = \begin{pmatrix}
  a_{11} & a_{12} \\
  a_{21} & a_{22} \\
  b_{11} & b_{12} \\
  b_{21} & b_{22}
\end{pmatrix} \in \mathbb{R}^{2 \times 2}
\]

which is an NTRU-instance in \( \mathbb{R}^2 \). May suffice to recover \( A \), \( B \).
7. Variants of NTRU [HPS98], [CG05]

Remark: if \( \ell \) is small, e.g.,

\[
H = \frac{A}{B} = \begin{pmatrix}
    a_{11} & a_{12} \\
    a_{21} & a_{22}
\end{pmatrix}
\begin{pmatrix}
    b_{11} & b_{12} \\
    b_{21} & b_{22}
\end{pmatrix}
\in \mathbb{R}^{2\times 2}
\]

then taking determinants yields

\[
\det H = \frac{\det A}{\det B} = \frac{a_{11}a_{22} - a_{21}a_{12}}{b_{11}b_{22} - b_{21}b_{12}}
\]

which is an NTRU-instance in \( \mathbb{R}_p \); may suffice to recover \( A, B \).
The SIS problem is about finding a small solution in $\mathbb{F}_p^m \setminus \{0\}$ to

$$
\begin{pmatrix}
    a_{10} & a_{11} & \ldots & a_{1,m-1} \\
    a_{20} & a_{21} & \ldots & a_{2,m-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{n0} & a_{n1} & \ldots & a_{n,m-1}
\end{pmatrix}
\cdot
\begin{pmatrix}
    x_0 \\
    x_1 \\
    \vdots \\
    x_{m-1}
\end{pmatrix} = 0
$$

where $n < m$ and the $a_{ij} \in \mathbb{F}_p$ are chosen uniformly at random.
8. Variants of SIS [Aj96], [LM06], [PR06], [LS15]

The SIS problem is about finding a small solution in $\mathbb{F}_p^m \setminus \{0\}$ to

$$
\begin{pmatrix}
    a_{10} & a_{11} & \ldots & a_{1,m-1} \\
    a_{20} & a_{21} & \ldots & a_{2,m-1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{n0} & a_{n1} & \ldots & a_{n,m-1}
\end{pmatrix}
\cdot
\begin{pmatrix}
    x_0 \\
    x_1 \\
    \vdots \\
    x_{m-1}
\end{pmatrix}
= 0
$$

where $n < m$ and the $a_{ij} \in \mathbb{F}_p$ are chosen uniformly at random.

One defines:

- **Ring-SIS** (assume $m = kn$):
  - Find small $x_i \in R_p = \mathbb{Z}[x]/(f(x))$ with $\deg f(x) = n$ such that
    $$(a_1 \ldots a_k) \cdot (x_1 \ldots x_k)^T = 0$$
    with $a_i \in R_p$ random.
8. Variants of SIS [Aj96], [LM06], [PR06], [LS15]

The SIS problem is about finding a small solution in $\mathbb{F}_p^m \setminus \{0\}$ to

$$
\begin{pmatrix}
a_{10} & a_{11} & \ldots & a_{1,m-1} \\
a_{20} & a_{21} & \ldots & a_{2,m-1} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n0} & a_{n1} & \ldots & a_{n,m-1}
\end{pmatrix} \cdot
\begin{pmatrix}
x_0 \\
x_1 \\
\vdots \\
x_{m-1}
\end{pmatrix} = 0
$$

where $n < m$ and the $a_{ij} \in \mathbb{F}_p$ are chosen uniformly at random.

One defines:

- **Ring-SIS** (assume $m = kn$):
  - Find small $x_i \in R_p = \mathbb{Z}[x]/(f(x))$ with $\deg f(x) = n$ such that
    $$
    (a_1 \ldots a_k) \cdot (x_1 \ldots x_k)^T = 0
    $$
    with $a_i \in R_p$ random.

- **Module-SIS**: similar (fill matrix with blocks)

Proven to be at least as hard as —/Ideal/Module-SIVP.
The SIS problem is about finding a small solution in $\mathbb{F}_p^m \setminus \{0\}$ to

$$\begin{pmatrix}
a_{10} & a_{11} & \ldots & a_{1,m-1} \\
a_{20} & a_{21} & \ldots & a_{2,m-1} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n0} & a_{n1} & \ldots & a_{n,m-1} \\
\end{pmatrix} \cdot \begin{pmatrix}
x_0 \\
x_1 \\
\vdots \\
x_{m-1} \\
\end{pmatrix} = 0$$

where $n < m$ and the $a_{ij} \in \mathbb{F}_p$ are chosen uniformly at random.

One defines:

- **Ring-SIS** (assume $m = kn$):
  - Find small $x_i \in \mathbb{Z}[x]/(f(x))$ with $\deg f(x) = n$ such that

  $$\begin{pmatrix}a_1 & \ldots & a_k\end{pmatrix} \cdot \begin{pmatrix}x_1 & \ldots & x_k\end{pmatrix}^T = 0$$

  with $a_i \in \mathbb{R}_p$ random.

- **Module-SIS**: similar (fill matrix with blocks)

Proven to be at least as hard as —/Ideal/Module-SIVP.
9. Don’t push it

Reconsider Module-LWE, where one is to solve a noisy system

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{k-1}
\end{pmatrix}
= \begin{pmatrix}
  a_{10} & a_{11} & \cdots & a_{1,\ell-1} \\
  a_{20} & a_{21} & \cdots & a_{2,\ell-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{k0} & a_{k1} & \cdots & a_{k,\ell-1}
\end{pmatrix}
\cdot
\begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{\ell-1}
\end{pmatrix}
+ \begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{k-1}
\end{pmatrix}
\]

over \( \mathbb{R}_p^\ell \).
9. Don’t push it

Reconsider Module-LWE, where one is to solve a noisy system

\[
\begin{pmatrix}
  b_0 \\
  b_1 \\
  \vdots \\
  b_{k-1}
\end{pmatrix} =
\begin{pmatrix}
  a_{10} & a_{11} & \cdots & a_{1,\ell-1} \\
  a_{20} & a_{21} & \cdots & a_{2,\ell-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{k0} & a_{k1} & \cdots & a_{k,\ell-1}
\end{pmatrix}
\begin{pmatrix}
  s_0 \\
  s_1 \\
  \vdots \\
  s_{\ell-1}
\end{pmatrix} +
\begin{pmatrix}
  e_0 \\
  e_1 \\
  \vdots \\
  e_{k-1}
\end{pmatrix}
\]

over \( \mathbb{R}_p^{\ell} \).

What if we push it, identify key space

\[
\begin{pmatrix}
  R_\ell^p
\end{pmatrix}
\text{ with }
\frac{R[y]}{(p, g(y))}
\]

for some monic deg \( \ell \) polynomial \( g(y) \in R[y] \), by viewing

\[
(s_0, s_1, \ldots, s_{\ell-1}) \quad \text{as} \quad s_0 + s_1 y + s_2 y^2 + \cdots + s_{\ell-1} y^{\ell-1},
\]

and replace \( A \) with \( A_{a(y)} \) for random \( a(y) \)?
9. Don’t push it

Can be a bad idea:

- [PTP15] suggest to work with

\[ f(x) = x^{\ell'} + 1, \quad \ell' = 2^{k'}, \quad g(y) = y^\ell + 1, \quad \ell = 2^k, \]

which amounts to working in the ring

\[ \mathbb{Z}[x, y] / (p, x^{\ell'} + 1, y^\ell + 1) \]

and identifying

\[ (s_{00}, s_{01}, \ldots, s_{\ell'-1,\ell-1}) \in \mathbb{F}_p^n \quad \text{with} \quad \sum_{0 \leq i \leq \ell', 0 \leq j \leq \ell} s_{ij} x^i y^j. \]
9. Don’t push it

Can be a bad idea:

- [PTP15] suggest to work with

\[ f(x) = x^{\ell'} + 1, \quad \ell' = 2^{k'}, \quad g(y) = y^\ell + 1, \quad \ell = 2^k, \]

which amounts to working in the ring

\[
\mathbb{Z}[x, y] / (p, x^{\ell'} + 1, y^\ell + 1)
\]

and identifying

\[
(s_{00}, s_{01}, \ldots, s_{\ell'-1,\ell-1}) \in \mathbb{F}_p^n \quad \text{with} \quad \sum_{0 \leq i \leq \ell', \quad 0 \leq j \leq \ell} s_{ij} x^i y^j.
\]

- Assume (wlog) that \( \ell' \geq \ell \), then \( x^{\ell'}/\ell \) is a root of \( y^\ell + 1 \).
9. Don’t push it

Can be a bad idea:

- So we have a smallness preserving homomorphism

\[
\frac{\mathbb{Z}[x, y]}{(p, x^{\ell'} + 1, y^\ell + 1)} \to \frac{\mathbb{Z}[x]}{(p, x^{\ell'} + 1)} : s(x, y) \mapsto s(x, x^{\ell'}/\ell)
\]

and solving smaller-dim’l Ring-LWE reveals \( s(x, x^{\ell'}/\ell) \).

- By varying the roots \( x^{\ell'}/\ell, x^{3\ell'}/\ell, x^{5\ell'}/\ell, \ldots \) we retrieve all of \( s(x, y) \) through simple linear algebra.
9. Don’t push it

Can be a bad idea:

- So we have a smallness preserving homomorphism

\[ \frac{\mathbb{Z}[x, y]}{(p, x^{\ell'} + 1, y^{\ell} + 1)} \rightarrow \frac{\mathbb{Z}[x]}{(p, x^{\ell'} + 1)} : s(x, y) \mapsto s(x, x^{\ell'}/\ell) \]

and solving smaller-dim’l Ring-LWE reveals \( s(x, x^{\ell'}/\ell) \).

- By varying the roots \( x^{\ell'}/\ell, x^{3\ell'}/\ell, x^{5\ell'}/\ell, \ldots \) we retrieve all of \( s(x, y) \) through simple linear algebra.

In general:

- if the two ring structures are independent, then essentially reduce to Ring-LWE,
- if the two ring structures are dependent, then suffer from the above reduction.
9. Don’t push it

Can be a bad idea:

- So we have a smallness preserving homomorphism

\[ \frac{\mathbb{Z}[x, y]}{(p, x^{\ell'} + 1, y^\ell + 1)} \rightarrow \frac{\mathbb{Z}[x]}{(p, x^{\ell'} + 1)} : s(x, y) \mapsto s(x, x^{\ell'/\ell}) \]

and solving smaller-dim’l Ring-LWE reveals \( s(x, x^{\ell'/\ell}) \).

- By varying the roots \( x^{\ell'/\ell}, x^{3\ell'/\ell}, x^{5\ell'/\ell}, \ldots \) we retrieve all of \( s(x, y) \) through simple linear algebra.

In general:

- if the two ring structures are \textit{independent}, then essentially reduce to Ring-LWE,
- if the two ring structures are \textit{dependent}, then suffer from the above reduction.

Does not seem interesting track...
9. Don’t push it

Example/remark: consider a Module-NTRU sample

\[ H = A_{a(y)}A_{b(y)}^{-1} \in R_{p}^{2 \times 2}, \quad R = \frac{\mathbb{Z}[x]}{(x^{n/2} + 1)} \]

with matrices of multiplication by

\[ a(y), b(y) \in \frac{R[y]}{(p, y^2 - x)} = \frac{\mathbb{Z}[x, y]}{(p, x^{n/2} + 1, y^2 - x)} \cong \frac{\mathbb{Z}[y]}{(p, y^n + 1)}. \]

This becomes a standard Ring-LWE sample.
9. Don’t push it

Example/remark: consider a Module-NTRU sample

$$H = A_{a(y)}A_{b(y)}^{-1} \in R_p^{2 \times 2}, \quad R = \frac{\mathbb{Z}[x]}{(x^{n/2} + 1)}$$

with matrices of multiplication by

$$a(y), b(y) \in \frac{R[y]}{(p, y^2 - x)} = \frac{\mathbb{Z}[x, y]}{(p, x^{n/2} + 1, y^2 - x)} \cong \frac{\mathbb{Z}[y]}{(p, y^n + 1)}.$$  

This becomes a standard Ring-LWE sample.

Interpretation of the determinant reduction:

$$\det H = \frac{\det A_{a(y)}}{\det A_{b(y)}} = \frac{N(a(y))}{N(b(y))}$$

$$\leadsto$$ used in [ABD16] to attack overstretched NTRU.
10. Polynomial ciphertext modulus

Return to ring-based LWE and take a step back... We start with our parent ring $R = \mathbb{Z}[x]/(f(x))$ with $f(x)$ monic of degree $n$. Note:

- Free $\mathbb{Z}$-module with basis $1, x, \ldots, x^{n-1}$.
- Smallness is defined at this level. E.g., coefficients from spherical Gaussian.

Next we quotient out by a ciphertext modulus to end up in $R_p = \mathbb{Z}[x]/(p, f(x))$ $\text{Rep}(R_p) = \{ \sum_{0 \leq i < n} a_i x^i | 0 \leq a_i < p \}$ where:

- small elt.'s are reductions mod $p$ of small elt.'s of $R$ (easy to recognize when isolated),
- all computations are reduced into $\text{Rep}(R_p)$ (wrap around $\mapsto$ hard to recognize in expressions).
10. Polynomial ciphertext modulus

Return to ring-based LWE and take a step back...

We start with our parent ring $R = \mathbb{Z}[x]/(f(x))$
with $f(x)$ monic of degree $n$.

Note:

- Free $\mathbb{Z}$-module with basis $1, x, \ldots, x^{n-1}$.

- **Smallness** is defined at this level.

  E.g., coefficients from spherical Gaussian.
10. Polynomial ciphertext modulus

Return to ring-based LWE and take a step back...

We start with our parent ring \( R = \mathbb{Z}[x]/(f(x)) \)
with \( f(x) \) monic of degree \( n \).

Note:
- Free \( \mathbb{Z} \)-module with basis \( 1, x, \ldots, x^{n-1} \).
- Smallness is defined at this level.
  E.g., coefficients from spherical Gaussian.

Next we quotient out by a ciphertext modulus to end up in

\[
R_p = \mathbb{Z}[x]/(p, f(x)) \quad \text{Rep}(R_p) = \left\{ \sum_{0 \leq i < n} a_i x^i \mid 0 \leq a_i < p \right\}
\]

where:
- small elt.’s are reductions mod \( p \) of small elt.’s of \( R \)
  (easy to recognize when isolated),
- all computations are reduced into \( \text{Rep}(R_p) \)
  (wrap around ⇝ hard to recognize in expressions)
10. Polynomial ciphertext modulus

What if we replace $p$ by a polynomial modulus?

- Pick monic polynomial $f(x) \in \mathbb{Z}[x]$ defining the parent ring:

  $$R = \mathbb{Z}[x]/(f(x)).$$
10. Polynomial ciphertext modulus

What if we replace $p$ by a polynomial modulus?

- Pick monic polynomial $f(x) \in \mathbb{Z}[x]$ defining the parent ring:

$$R = \mathbb{Z}[x]/(f(x)).$$

- Choose error distribution to define smallness.
10. Polynomial ciphertext modulus

What if we replace \( p \) by a polynomial modulus?

- Pick monic polynomial \( f(x) \in \mathbb{Z}[x] \) defining the parent ring:
  \[
  R = \mathbb{Z}[x]/(f(x)).
  \]

- Choose error distribution to define smallness.

- Pick \( g(x) \in \mathbb{Z}[x] \) coprime with \( f(x) \) and assume that
  \[
  (f(x), g(x)) = (a, r(x)) \quad \text{for} \quad a \in \mathbb{Z} \text{ and monic } r(x) \in \mathbb{Z}[x]
  \]
  (true for about 60.8\% of all polynomial pairs \( f(x) \) and \( g(x) \)).

This gives an easy set of representatives:

\[
\text{Rep}(R_{g(x)}) = \left\{ \sum_{0 \leq i < \deg r(x)} a_i x^i \mid 0 \leq a_i < a \right\}.
\]

in which all results are to be reduced.
10. Polynomial ciphertext modulus

What if we replace $p$ by a polynomial modulus?

▶ Pick monic polynomial $f(x) \in \mathbb{Z}[x]$ defining the parent ring:

$$R = \mathbb{Z}[x]/(f(x)).$$

▶ Choose error distribution to define smallness.

▶ Pick $g(x) \in \mathbb{Z}[x]$ coprime with $f(x)$ and assume that

$$(f(x), g(x)) = (a, r(x)) \quad \text{for } a \in \mathbb{Z} \text{ and monic } r(x) \in \mathbb{Z}[x]$$

(true for about 60.8% of all polynomial pairs $f(x)$ and $g(x)$).

This gives an easy set of representatives:

$$\text{Rep}(R_{g(x)}) = \left\{ \sum_{0 \leq i < \deg r(x)} a_i x^i \mid 0 \leq a_i < a \right\}.$$ 

in which all results are to be reduced.

▶ Recognizing small elements seems ad hoc exercise.
10. Polynomial ciphertext modulus

Example:

- Parent ring: \( R = \mathbb{Z}[x]/(f(x)) \) with \( f(x) = x^n - 1 \).
10. Polynomial ciphertext modulus

Example:

- Parent ring: $R = \mathbb{Z}[x]/(f(x))$ with $f(x) = x^n - 1$.
- Smallness: samples from an extremely narrow Gaussian, so that all coefficients are 0 with just a few $\pm 1$'s.
10. Polynomial ciphertext modulus

Example:

► Parent ring: $R = \mathbb{Z}[x]/(f(x))$ with $f(x) = x^n - 1$.

► Smallness: samples from an extremely narrow Gaussian, so that all coefficients are 0 with just a few $\pm 1$'s.

► Now quotient out by $x - 2$ to get ciphertext ring

$$R_{x-2} = \mathbb{Z}[x]/(x^n - 1, x - 2) = \mathbb{Z}[x]/(2^n - 1, x - 2) \cong \mathbb{Z}/(2^n - 1)$$

which comes with representatives

$$\text{Rep}(R_{x-2}) = \{ a \in \mathbb{Z} | 0 \leq a < 2^n - 1 \}$$
10. Polynomial ciphertext modulus

Example:

- Parent ring: \( R = \mathbb{Z}[x]/(f(x)) \) with \( f(x) = x^n - 1 \).
- Smallness: samples from an extremely narrow Gaussian, so that all coefficients are 0 with just a few \( \pm 1 \)'s.
- Now quotient out by \( x - 2 \) to get ciphertext ring

\[
R_{x-2} = \frac{\mathbb{Z}[x]}{(x^n - 1, x - 2)} = \frac{\mathbb{Z}[x]}{(2^n - 1, x - 2)} \cong \frac{\mathbb{Z}}{(2^n - 1)}
\]

which comes with representatives

\[
\text{Rep}(R_{x-2}) = \{ a \in \mathbb{Z} \mid 0 \leq a < 2^n - 1 \}
\]

- Easy to recognize small elements (Hamming weight)

Note that \( R_{x-2} \) is totally invulnerable to evaluation-at-1.

Essentially the Mersenne based system from [AJPS17].
10. Polynomial ciphertext modulus

Example:

- Parent ring: $R = \mathbb{Z}[x]/(f(x))$ with $f(x) = x^n - 1$.
- Smallness: samples from an extremely narrow Gaussian, so that all coefficients are 0 with just a few ±1’s.
- Now quotient out by $x - 2$ to get ciphertext ring

$$R_{x-2} = \frac{\mathbb{Z}[x]}{(x^n - 1, x - 2)} \cong \frac{\mathbb{Z}[x]}{(2^n - 1, x - 2)} \cong \frac{\mathbb{Z}}{(2^n - 1)}$$

which comes with representatives

$$\text{Rep}(R_{x-2}) = \{ a \in \mathbb{Z} \mid 0 \leq a < 2^n - 1 \}$$

- Easy to recognize small elements (Hamming weight)
- Note that $R_{x-2}$ is totally invulnerable to evaluation-at-1.
10. Polynomial ciphertext modulus

Example:

- Parent ring: \( R = \mathbb{Z}[x]/(f(x)) \) with \( f(x) = x^n - 1 \).
- Smallness: samples from an extremely narrow Gaussian, so that all coefficients are 0 with just a few ±1’s.
- Now quotient out by \( x - 2 \) to get ciphertext ring

\[
R_{x-2} = \frac{\mathbb{Z}[x]}{(x^n - 1, x - 2)} = \frac{\mathbb{Z}[x]}{(2^n - 1, x - 2)} \cong \frac{\mathbb{Z}}{(2^n - 1)}
\]

which comes with representatives

\[
\text{Rep}(R_{x-2}) = \{ a \in \mathbb{Z} \mid 0 \leq a < 2^n - 1 \}
\]

- Easy to recognize small elements (Hamming weight)
- Note that \( R_{x-2} \) is totally invulnerable to evaluation-at-1.
- Essentially the Mersenne based system from [AJPS17].
11. A recipe for constructing hard problems

1. Select the parent ring $R = \mathbb{Z}[x]/(f(x))$.

2. Select error distribution.

3. Select ciphertext modulus $g(x)$ subject to constraints.

4. Select the rank of the module.

5. Select your hard problem family:
   Module-LWE, Module-NTRU or Module-SIS.
11. A recipe for constructing hard problems

1. Select the parent ring $R = \mathbb{Z}[x]/(f(x))$.

   \[ R = \mathbb{Z} \quad (= \mathbb{Z}[x]/(x)) \]

2. Select error distribution.

   Gaussian

3. Select ciphertext modulus $g(x)$ subject to constraints.

   \[ g(x) = p \]

4. Select the rank of the module.

   rank $n$, so work in $R_p^n$

5. Select your hard problem family:

   Module-LWE, Module-NTRU or Module-SIS.
11. A recipe for constructing hard problems

1. Select the parent ring $R = \mathbb{Z}[x]/(f(x))$.
   
   $R = \mathbb{Z}[x]/(x^n + 1) \quad (n = 2^k)$

2. Select error distribution.
   
   spherical Gaussian

3. Select ciphertext modulus $g(x)$ subject to constraints.
   
   $g(x) = p$

4. Select the rank of the module.
   
   rank 1, so work in $R_p$

5. Select your hard problem family:
   
   Module-LWE, Module-NTRU or Module-SIS.
11. A recipe for constructing hard problems

1. Select the parent ring $R = \mathbb{Z}[x]/(f(x))$.
   
   $R = \mathbb{Z}[x]/(x^q - x - 1)$

2. Select error distribution.
   
   coefficients uniform in $\{0, \pm 1\}$ with fixed weight

3. Select ciphertext modulus $g(x)$ subject to constraints.
   
   $g(x) = p$

4. Select the rank of the module.
   
   rank 1, so work in $R_p$

5. Select your hard problem family:
   
   Module-LWE, Module-NTRU or Module-SIS.

NTRU Prime
11. A recipe for constructing hard problems

1. Select the parent ring $R = \mathbb{Z}[x]/(f(x))$.
   \[ R = \mathbb{Z}[x]/(x^D - x^{D/2} - 1) \]

2. Select error distribution.
   coefficients sampled from \{0, ±1\}

3. Select ciphertext modulus $g(x)$ subject to constraints.
   \[ g(x) = x - 2 \]

4. Select the rank of the module.
   small rank $n \in \{2, 3, 4\}$, so work in $R^n_{x-2}$

5. Select your hard problem family:
   Module-LWE, Module-NTRU or Module-SIS.

Three Bears (I-MLWE)
11. A recipe for constructing hard problems

1. Select the parent ring $R = \mathbb{Z}[x]/(f(x))$.
   \[ R = \mathbb{Z}[x]/(x^n + 1) \quad (n = 2^k) \]

2. Select error distribution.
   spherical binomial

3. Select ciphertext modulus $g(x)$ subject to constraints.
   \[ g(x) = p \]

4. Select the rank of the module.
   small rank $n \in \{2, 3, 4\}$, so work in $R_p^n$

5. Select your hard problem family:
   Module-LWE, Module-NTRU or Module-SIS.

Kyber
Questions?