

A direct Search-LWE attack

Robin Frot,
László Koltai,
Daniel Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

A direct Search-LWE attack

Robin Frot, László Koltai, Daniel Zentai

Harvey's Consultancy Services ZRT, Hungary

NuTMiC 2026 - September 21st

Some notations

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

- Let $N = 2^l$ be a power of 2 for some $l \in \mathbb{N}$.

Some notations

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

- Let $N = 2^l$ be a power of 2 for some $l \in \mathbb{N}$.
- Let q be a prime number.

Some notations

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

- Let $N = 2^l$ be a power of 2 for some $l \in \mathbb{N}$.
- Let q be a prime number.
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$ the ring of cyclotomic integers.

Some notations

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

- Let $N = 2^l$ be a power of 2 for some $l \in \mathbb{N}$.
- Let q be a prime number.
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$ the ring of cyclotomic integers.
- $\mathcal{R}_q = \mathbb{F}_q[X]/(X^N + 1) = \mathcal{R}/q\mathcal{R}$

Some notations

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

- Let $N = 2^l$ be a power of 2 for some $l \in \mathbb{N}$.
- Let q be a prime number.
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$ the ring of cyclotomic integers.
- $\mathcal{R}_q = \mathbb{F}_q[X]/(X^N + 1) = \mathcal{R}/q\mathcal{R}$
- For $x \in \mathbb{Z}$, $\lfloor x \rfloor_q$ is the representative of x modulo q in $[-(q-1)/2, (q-1)/2]$. It generalizes to $\mathcal{R}$ by doing it coefficient-wise.

Some notations

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

- Let $N = 2^l$ be a power of 2 for some $l \in \mathbb{N}$.
- Let q be a prime number.
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$ the ring of cyclotomic integers.
- $\mathcal{R}_q = \mathbb{F}_q[X]/(X^N + 1) = \mathcal{R}/q\mathcal{R}$
- For $x \in \mathbb{Z}$, $\lfloor x \rfloor_q$ is the representative of x modulo q in $[-(q-1)/2, (q-1)/2]$. It generalizes to $\mathcal{R}$ by doing it coefficient-wise.
- If $c \in \mathcal{R}_q$, $\tilde{c}$ is the only lift of c in $\mathcal{R}$ such that $\lfloor \tilde{c} \rfloor_q = \tilde{c}$, i.e., $\tilde{c}$ has coefficients in the aforementioned interval.

Some notations

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

- Let $N = 2^l$ be a power of 2 for some $l \in \mathbb{N}$.
- Let q be a prime number.
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$ the ring of cyclotomic integers.
- $\mathcal{R}_q = \mathbb{F}_q[X]/(X^N + 1) = \mathcal{R}/q\mathcal{R}$
- For $x \in \mathbb{Z}$, $\lfloor x \rfloor_q$ is the representative of x modulo q in $[-(q-1)/2, (q-1)/2]$. It generalizes to $\mathcal{R}$ by doing it coefficient-wise.
- If $c \in \mathcal{R}_q$, $\tilde{c}$ is the only lift of c in $\mathcal{R}$ such that $\lfloor \tilde{c} \rfloor_q = \tilde{c}$, i.e., $\tilde{c}$ has coefficients in the aforementioned interval. This is not a group homomorphism.

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

■ $b = as + e$, where $a, s, e \in \mathcal{R}_q$.

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László Koltai,
Daniel Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László Koltai,
Daniel Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László Koltai,
Daniel Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Decision problem: Given a pair (a, b) , is it uniform or RLWE?

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice
reduction
Step 2: lift and
reduction
Step 3: solving
the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Decision problem: Given a pair (a, b) , is it uniform or RLWE?

Search problem: Given a RLWE pair (a, b) , find s .

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László Koltai,
Daniel Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice reduction
Step 2: lift and reduction
Step 3: solving the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Decision problem: Given a pair (a, b) , is it uniform or RLWE?

Search problem: Given a RLWE pair (a, b) , find s .

Why care about RLWE?

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice
reduction
Step 2: lift and
reduction
Step 3: solving
the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Decision problem: Given a pair (a, b) , is it uniform or RLWE?

Search problem: Given a RLWE pair (a, b) , find s .

Why care about RLWE?

- It is conjectured to be quantum secure.

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice
reduction
Step 2: lift and
reduction
Step 3: solving
the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Decision problem: Given a pair (a, b) , is it uniform or RLWE?

Search problem: Given a RLWE pair (a, b) , find s .

Why care about RLWE?

- It is conjectured to be quantum secure.
- It is the underlying problem behind several (Fully) Homomorphic Encryption schemes e.g. BGV, NTRU, CKKS...

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Decision problem: Given a pair (a, b) , is it uniform or RLWE?

Search problem: Given a RLWE pair (a, b) , find s .

The novelty of our method:

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Decision problem: Given a pair (a, b) , is it uniform or RLWE?

Search problem: Given a RLWE pair (a, b) , find s .

The novelty of our method: To solve the search problem, previous attacks involved a Search-to-Decision reduction.

Ring Learning with Errors

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

The RLWE distribution on $\mathcal{R}_q^2$ consists of pairs (a, b) such that:

- $b = as + e$, where $a, s, e \in \mathcal{R}_q$.
- a is chosen uniformly in $\mathcal{R}_q$.
- s and e are usually "small".

Decision problem: Given a pair (a, b) , is it uniform or RLWE?

Search problem: Given a RLWE pair (a, b) , find s .

The novelty of our method: To solve the search problem, previous attacks involved a Search-to-Decision reduction. In our attack we directly solve the Search-RLWE problem without reducing it to a decision problem.

Lattices

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

Lattices

A direct
Search-LWE
attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some
definitions

Notations

RLWE

Lattices

Direct search
attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

A lattice L is a discrete subgroup of $\mathbb{R}^n$.

Lattices

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

A lattice L is a discrete subgroup of $\mathbb{R}^n$.

Examples:

Lattices

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

A lattice L is a discrete subgroup of $\mathbb{R}^n$.

Examples:

$$\blacksquare \mathbb{Z}^n \subset \mathbb{R}^n$$

Lattices

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

A lattice L is a discrete subgroup of $\mathbb{R}^n$.

Examples:

- $\mathbb{Z}^n \subset \mathbb{R}^n$
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1) \subset \mathbb{R}[X]/(X^N + 1) \simeq \mathbb{R}^N$

Lattices

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

A lattice L is a discrete subgroup of $\mathbb{R}^n$.

Examples:

- $\mathbb{Z}^n \subset \mathbb{R}^n$
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1) \subset \mathbb{R}[X]/(X^N + 1) \simeq \mathbb{R}^N$
- If $B = \{b_1, \dots, b_k\} \subset \mathbb{R}^n$ is a set of linearly independent vectors, then

$$L(B) = \{a_1 b_1 + \dots + a_k b_k \mid a_i \in \mathbb{Z}\}$$

Lattices

A direct Search-LWE attack

Robin Frot,
László Koltai,
Daniel Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

A lattice L is a discrete subgroup of $\mathbb{R}^n$.

Examples:

- $\mathbb{Z}^n \subset \mathbb{R}^n$
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1) \subset \mathbb{R}[X]/(X^N + 1) \simeq \mathbb{R}^N$
- If $B = \{b_1, \dots, b_k\} \subset \mathbb{R}^n$ is a set of linearly independent vectors, then

$$L(B) = \{a_1 b_1 + \dots + a_k b_k \mid a_i \in \mathbb{Z}\}$$

Every lattice L is of the form $L(B)$, for some set of linearly independent vectors $B \subset \mathbb{R}^n$. We call such a set basis of the lattice L .

Lattices

A direct Search-LWE attack

Robin Frot,
László Koltai,
Daniel Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

A lattice L is a discrete subgroup of $\mathbb{R}^n$.

Examples:

- $\mathbb{Z}^n \subset \mathbb{R}^n$
- $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1) \subset \mathbb{R}[X]/(X^N + 1) \simeq \mathbb{R}^N$
- If $B = \{b_1, \dots, b_k\} \subset \mathbb{R}^n$ is a set of linearly independent vectors, then

$$L(B) = \{a_1 b_1 + \dots + a_k b_k \mid a_i \in \mathbb{Z}\}$$

Every lattice L is of the form $L(B)$, for some set of linearly independent vectors $B \subset \mathbb{R}^n$. We call such a set basis of the lattice L .

A basis of $\mathcal{R}$ in $\mathbb{R}[X]/(X^N + 1)$ is $\{1, X, X^2, \dots, X^{N-1}\}$.

Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

Given a basis $B = (b_1, \dots, b_n)$,

Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

Given a basis $B = (b_1, \dots, b_n)$, a lattice reduction algorithm (LLL, BKZ, ...) outputs a basis $B' = (b'_1, \dots, b'_n)$ of smaller, "almost orthogonal" vectors.

Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

Given a basis $B = (b_1, \dots, b_n)$, a lattice reduction algorithm (LLL, BKZ, ...) outputs a basis $B' = (b'_1, \dots, b'_n)$ of smaller, "almost orthogonal" vectors. Generally, one expects

$$\|b'_1\| \ll C^n \det(B)^{\frac{1}{n}}.$$

Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

Given a basis $B = (b_1, \dots, b_n)$, a lattice reduction algorithm (LLL, BKZ, ...) outputs a basis $B' = (b'_1, \dots, b'_n)$ of smaller, "almost orthogonal" vectors. Generally, one expects

$$\|b'_1\| \ll C^n \det(B)^{\frac{1}{n}}.$$

Similar bounds hold for the remaining basis vectors.

Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

Given a basis $B = (b_1, \dots, b_n)$, a lattice reduction algorithm (LLL, BKZ, ...) outputs a basis $B' = (b'_1, \dots, b'_n)$ of smaller, "almost orthogonal" vectors. Generally, one expects

$$\|b'_1\| \ll C^n \det(B)^{\frac{1}{n}}.$$

Similar bounds hold for the remaining basis vectors.

Remark: Let us denote by $\lambda_1(L)$ the minimal length of the non-zero vectors of the lattice L , i.e.

$$\lambda_1(L) = \min\{\|v\| \mid v \in L, v \neq 0\}.$$

Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

Given a basis $B = (b_1, \dots, b_n)$, a lattice reduction algorithm (LLL, BKZ, ...) outputs a basis $B' = (b'_1, \dots, b'_n)$ of smaller, "almost orthogonal" vectors. Generally, one expects

$$\|b'_1\| \ll C^n \det(B)^{\frac{1}{n}}.$$

Similar bounds hold for the remaining basis vectors.

Remark: Let us denote by $\lambda_1(L)$ the minimal length of the non-zero vectors of the lattice L , i.e.

$$\lambda_1(L) = \min\{\|v\| \mid v \in L, v \neq 0\}.$$

By the theorem of Minkowsky we have:

$$\lambda_1(L(B)) \leq \det(B)^{1/n}$$

Step 1: Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and
reduction

Step 3: solving
the system

Let $(a, b = as + e)$ be a RLWE instance, $\tilde{a}$ a lift of a in $\mathcal{R}$

Step 1: Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

Let $(a, b = as + e)$ be a RLWE instance, $\tilde{a}$ a lift of a in $\mathcal{R}$ and

$$\begin{pmatrix} qI_N & A \\ 0 & I_N \end{pmatrix} \in M_{2N}(\mathbb{Z})$$

be a lattice base, where A is the multiplication by $\tilde{a}$.

Step 1: Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

Let $(a, b = as + e)$ be a RLWE instance, $\tilde{a}$ a lift of a in $\mathcal{R}$ and

$$\begin{pmatrix} qI_N & A \\ 0 & I_N \end{pmatrix} \in M_{2N}(\mathbb{Z})$$

be a lattice base, where A is the multiplication by $\tilde{a}$. A reduced vector $(\epsilon_0, \dots, \epsilon_{N-1}, m_0, \dots, m_{N-1})^T$ of this lattice gives two polynomials ϵ and m such that

Step 1: Lattice reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

Let $(a, b = as + e)$ be a RLWE instance, $\tilde{a}$ a lift of a in $\mathcal{R}$ and

$$\begin{pmatrix} qI_N & A \\ 0 & I_N \end{pmatrix} \in M_{2N}(\mathbb{Z})$$

be a lattice base, where A is the multiplication by $\tilde{a}$. A reduced vector $(\epsilon_0, \dots, \epsilon_{N-1}, m_0, \dots, m_{N-1})^T$ of this lattice gives two polynomials ϵ and m such that

$$m\tilde{a} + q\epsilon = z \in \mathcal{R}$$

$$z, m = O(q^{1-\delta})$$

where $\delta \leq 1/2$.

Step 2: lift and reduction

Let us assume that $s, e = O(q^{\delta/2})$ and let $\tilde{b}$ be the lift of b .

A direct
Search-LWE
attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some
definitions

Notations

RLWE

Lattices

Direct search
attack

Step 1: Lattice
reduction

**Step 2: lift and
reduction**

Step 3: solving
the system

Step 2: lift and reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice
reduction

**Step 2: lift and
reduction**

Step 3: solving
the system

Let us assume that $s, e = O(q^{\delta/2})$ and let $\tilde{b}$ be the lift of b .
We have

$$\tilde{b} \in \tilde{a}\tilde{s} + \tilde{e} + q\mathcal{R}$$

$$\tilde{b} = \tilde{a}\tilde{s} + \tilde{e} + qd$$

and

Step 2: lift and reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice reduction

Step 2: lift and reduction

Step 3: solving the system

Let us assume that $s, e = O(q^{\delta/2})$ and let $\tilde{b}$ be the lift of b .
We have

$$\tilde{b} \in \tilde{a}\tilde{s} + \tilde{e} + q\mathcal{R}$$

$$\tilde{b} = \tilde{a}\tilde{s} + \tilde{e} + qd$$

and

$$m\tilde{b} \in z\tilde{s} + m\tilde{e} + q\mathcal{R}.$$

$$m\tilde{b} = m\tilde{a}\tilde{s} + m\tilde{e} + mqd$$

$$= z\tilde{s} - q\epsilon\tilde{s} + m\tilde{e} + qdm$$

$$= z\tilde{s} + m\tilde{e} + qd^*$$

Step 2: lift and reduction

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice
reduction
Step 2: lift and
reduction
Step 3: solving
the system

Let us assume that $s, e = O(q^{\delta/2})$ and let $\tilde{b}$ be the lift of b .
We have

$$\tilde{b} \in \tilde{a}\tilde{s} + \tilde{e} + q\mathcal{R}$$

$$\tilde{b} = \tilde{a}\tilde{s} + \tilde{e} + qd$$

and

$$m\tilde{b} \in z\tilde{s} + m\tilde{e} + q\mathcal{R}.$$

$$\begin{aligned} m\tilde{b} &= m\tilde{a}\tilde{s} + m\tilde{e} + mqd \\ &= z\tilde{s} - q\epsilon\tilde{s} + m\tilde{e} + qdm \\ &= z\tilde{s} + m\tilde{e} + qd^* \end{aligned}$$

Finally, since $z\tilde{s}, m\tilde{e} = O(q^{1-\delta/2})$, we have

$$\lfloor m\tilde{b} \rfloor_q = z\tilde{s} + m\tilde{e} \in \mathcal{R}.$$

Step 3: solving the system

A direct Search-LWE attack

Robin Frot,
László Koltai,
Daniel Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice reduction
Step 2: lift and reduction
Step 3: solving the system

Assume that we found 2 relations as in the last slide (from 2 reduced basis vectors):

$$b_1 = z_1 \tilde{s} + m_1 \tilde{e}$$

$$b_2 = z_2 \tilde{s} + m_2 \tilde{e},$$

Step 3: solving the system

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations
RLWE
Lattices

Direct search attack

Step 1: Lattice
reduction
Step 2: lift and
reduction
Step 3: solving
the system

Assume that we found 2 relations as in the last slide (from 2 reduced basis vectors):

$$b_1 = z_1 \tilde{s} + m_1 \tilde{e}$$

$$b_2 = z_2 \tilde{s} + m_2 \tilde{e},$$

then

$$\tilde{s} = (m_2 b_1 - m_1 b_2)(m_2 z_1 - m_1 z_2)^{-1}$$

(recall that $\mathcal{R} \subset \mathbb{Q}[X]/(X^N + 1)$ is a field)
and $s = \tilde{s} \bmod q$.

A direct Search-LWE attack

Robin Frot,
László
Koltai,
Daniel
Zentai

Some definitions

Notations

RLWE

Lattices

Direct search attack

Step 1: Lattice
reduction

Step 2: lift and
reduction

Step 3: solving
the system

Thank you for your attention!