On algebraic variants of the LWE problem

Damien Stehlé

Based on joint works with M. Rosca, A. Sakzad, R. Steinfeld and A. Wallet
Figures borrowed from M. Rosca and A. Wallet

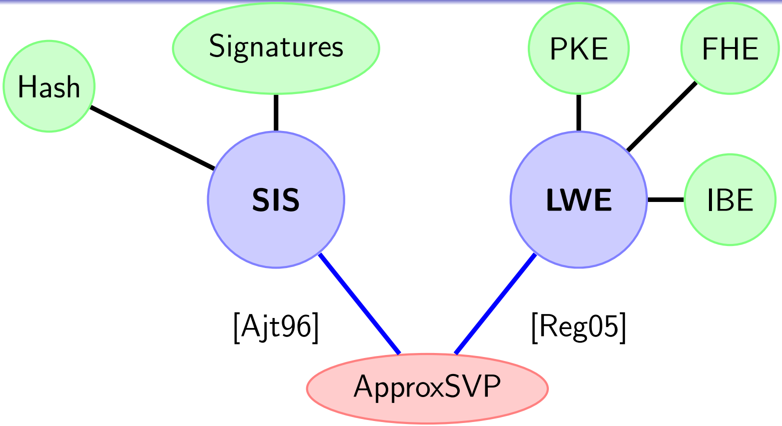
ENS de Lyon, Bitdefender, U. Monash

CAEN, June 2018

ENS DE LYON

erc

What is this talk about



SIS and LWE are lattice problems that are convenient for cryptographic design.

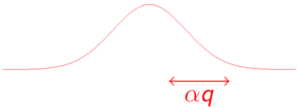
We'll focus on "efficient" variants of LWE.

LWE [Reg05]

LWE parameters: $m \geq n \geq 1$, $q \geq 2$ and $\alpha > 0$.

$$\left(\underbrace{\mathbf{A}}_{n}{}^{m} \, , \, \mathbf{A}\,\mathbf{s} + \mathbf{e} \right) \xrightarrow{\text{find}} \mathbf{s}$$

- $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$,
- $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^{n})$,
- $\mathbf{e} \hookleftarrow D_{\alpha q}^{m}$.

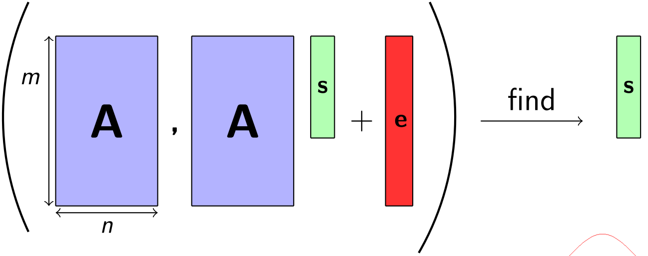


Gaussian error distribution $D_{\alpha q}$

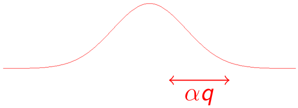
Typical parameters: n proportional to the bit-security, $q = n^{\Theta(1)}$, $m = \Theta(n \log q)$, $\alpha \approx \sqrt{n}/q$.

LWE [Reg05]

LWE parameters: $m \geq n \geq 1$, $q \geq 2$ and $\alpha > 0$.



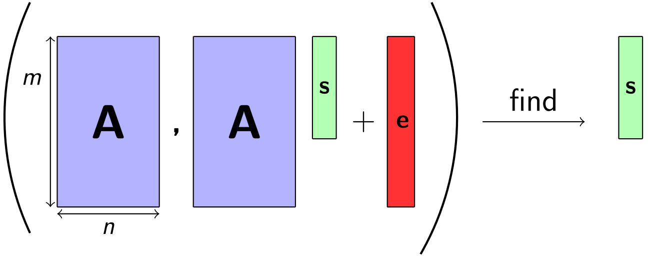
- $\boxed{\mathbf{A}} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$,
- $\boxed{\mathbf{s}} \hookleftarrow U(\mathbb{Z}_q^{n})$,
- $\boxed{\mathbf{e}} \hookleftarrow D_{\alpha q}^{m}$.



Gaussian error distribution $D_{\alpha q}$

Typical parameters: n proportional to the bit-security,
$q = n^{\Theta(1)}$, $m = \Theta(n \log q)$, $\alpha \approx \sqrt{n}/q$.

Search LWE as a Closest Vector Problem variant



- **A** defines the Construction-A lattice

$$L_q(\mathbf{A}) = \mathbf{A}\mathbb{Z}_q^n + q\mathbb{Z}^m.$$

- $\mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ is a point near that lattice.
- Finding **s** is finding the closest vector in $L_q(\mathbf{A})$.

LWE is CVP for a uniformly sampled Construction-A lattice, a random lattice vector and a Gaussian lattice offset.

Hardness and "inefficiency" of LWE

Best known attack for most parameter ranges: lattice reduction.

$$\text{Time} \approx \exp\left(\frac{n \log q}{\log^2 \alpha} \log\left(\frac{n \log q}{\log^2 \alpha}\right)\right)$$

- Representing an LWE instance is quadratic in the bit-security.
- One then performs (at least) matrix-vector multiplications...

Frodo: submission to the NIST post-quantum standardization process
public-key and ciphertexts $\approx$ 10 kB
encryption and decryption $\approx$ 2 million cycles

(for security similar to brute-forcing AES-128)

Hardness and "inefficiency" of LWE

Best known attack for most parameter ranges: lattice reduction.

$$\text{Time} \approx \exp\left(\frac{n \log q}{\log^2 \alpha} \log\left(\frac{n \log q}{\log^2 \alpha}\right)\right)$$

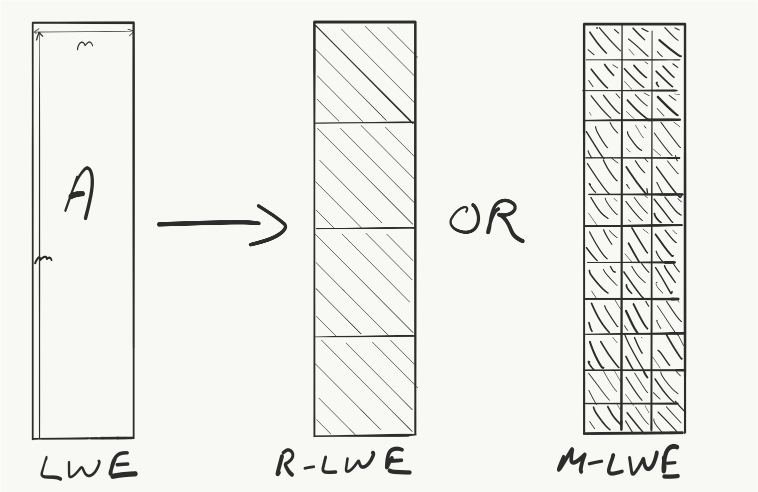
- Representing an LWE instance is quadratic in the bit-security.
- One then performs (at least) matrix-vector multiplications...

Frodo: submission to the NIST post-quantum standardization process
public-key and ciphertexts $\approx$ 10 kB
encryption and decryption $\approx$ 2 million cycles
(for security similar to brute-forcing AES-128)

Road-map

- The Learning With Errors problem
- **Algebraic variants of the LWE problem**
- On Polynomial-LWE and Ring-LWE
- The Middle-Product-LWE problem

Take structured matrices!



Polynomial-LWE [SSTX09]

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

Search P-LWE^f

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

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

This is LWE, with matrix $\mathbf{A}$ made of stacked blocks $\mathrm{Rot}_f(a_i)$.

The j-th row of $\mathrm{Rot}_f(a_i)$ is made of the coefficients of $x^{j-1} \cdot a_i \bmod f$.

Polynomial-LWE [SSTX09]

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

Search P-LWE^f

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

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

This is LWE, with matrix $\mathbf{A}$ made of stacked blocks $\mathrm{Rot}_f(a_i)$.

The j-th row of $\mathrm{Rot}_f(a_i)$ is made of the coefficients of $x^{j-1} \cdot a_i \bmod f$.

Polynomial-LWE [SSTX09]

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

Search P-LWE^f

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

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

This is LWE, with matrix $\mathbf{A}$ made of stacked blocks $\mathrm{Rot}_f(a_i)$.

The j-th row of $\mathrm{Rot}_f(a_i)$ is made of the coefficients of $x^{j-1} \cdot a_i \bmod f$.

Why is P-LWE useful?

Search P-LWE^f

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

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

One $(a_i, a_i \cdot s + e_i)$ encodes n correlated LWE samples:

$$(\mathrm{Rot}_f(a_i), \mathrm{Rot}_f(a_i) \cdot s + e_i) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n.$$

This requires $2n$ elements of $\mathbb{Z}_q$ instead of $n^2 + n$.
It takes $\widetilde{O}$ operations over $\mathbb{Z}_q$ to compute $a_i \cdot s + e_i$, instead of $\Theta(n^2)$.

Ring-LWE [LPR10]

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

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

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

Search Ring-LWE^f

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

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

Ring-LWE [LPR10]

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

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

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

Search Ring-LWE^f

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

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

Ring-LWE vs Primal-Ring-LWE

Search Ring-LWE^f

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

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

Search Primal-Ring-LWE^f

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

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

What does it mean to be small?

Search Ring-LWE^f

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

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

- We should be able to recover e_i from $e_i \bmod q{\mathcal{O}_K}^\vee$.
- It shouldn't fold in any direction if reduced mod $q{\mathcal{O}_K}^\vee$.

We implicitly assume we have a good basis of $q{\mathcal{O}_K}^\vee$.

- Not too small either, as else the problem becomes easy.

One may do subtle things with the noise distributions.

Here, we'll be happy enough if the $\sigma(e_i)$'s are small.

What does it mean to be small?

Search Ring-LWE^f

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

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

- We should be able to recover e_i from e_i mod $q{\mathcal{O}_K}^\vee$.
- It shouldn't fold in any direction if reduced mod $q{\mathcal{O}_K}^\vee$.

  We implicitly assume we have a good basis of $q{\mathcal{O}_K}^\vee$.
- Not too small either, as else the problem becomes easy.

One may do subtle things with the noise distributions.

Here, we'll be happy enough if the $\sigma(e_i)$'s are small.

What does it mean to be small?

Search Ring-LWE^f

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

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

- We should be able to recover e_i from e_i mod $q{\mathcal{O}_K}^\vee$.
- It shouldn't fold in any direction if reduced mod $q{\mathcal{O}_K}^\vee$.

  We implicitly assume we have a good basis of $q{\mathcal{O}_K}^\vee$.
- Not too small either, as else the problem becomes easy.

  One may do subtle things with the noise distributions.

  Here, we'll be happy enough if the $\sigma(e_i)$'s are small.

A messy landscape...

At least 3 problem families:

- P-LWE^f
- R-LWE^f
- primal-R-LWE^f

Plus Module-LWE^f, a trade-off between these and LWE

Plus the decision versions

A messy landscape...

At least 3 problem families:

- P-LWE^f
- R-LWE^f
- primal-R-LWE^f

Plus Module-LWE^f, a trade-off between these and LWE
Plus the decision versions

A messy landscape...

At least 3 problem families:

- P-LWE^f
- R-LWE^f
- primal-R-LWE^f

Plus Module-LWE^f, a trade-off between these and LWE
Plus the decision versions

- How are these problems related?
- Is there a relationship between $*$-LWE^f and $*$-LWE^g?
- Can we find one ring to rule them all?

A messy landscape...

At least 3 problem families:

- P-LWE^f
- R-LWE^f
- primal-R-LWE^f

Plus Module-LWE^f, a trade-off between these and LWE
Plus the decision versions

- **How are these problems related?**
- Is there a relationship between $*$-LWE^f and $*$-LWE^g?
- **Can we find one ring to rule them all?**

Do we care?

These algebraic variants do lead to efficient schemes:

NIST p.-q. submissions: Ding, HILA5, KINDI, Kyber, LAC, LIMA, Lizard, Newhope, Saber

Somewhere between 5 and 10 times better than LWE-based Frodo

Most of these use $f = x^n + 1$ with f a power of 2.

For this f, the three problems are identical, and the results have been known for almost 10 years.

Do we care?

These algebraic variants do lead to efficient schemes:

NIST p.-q. submissions: Ding, HILA5, KINDI, Kyber, LAC, LIMA, Lizard, Newhope, Saber

Somewhere between 5 and 10 times better than LWE-based Frodo

Most of these use $f = x^n + 1$ with f a power of 2.

For this f, the three problems are identical, and the results have been known for almost 10 years.

Road-map

- The Learning With Errors problem
- Algebraic variants of the LWE problem
- **On Polynomial-LWE and Ring-LWE**

Joint work with M. Rosca and A. Wallet, Eurocrypt 2018.

- The Middle-Product-LWE problem

From dual to primal

A useful lemma from [LPR10]

Let $t \in ({\mathcal{O}_K}^\vee)^{-1}$ with $t{\mathcal{O}_K}^\vee$ coprime to (q). Then '$\times t$' is an $\mathcal{O}_K$-module isomorphism from ${\mathcal{O}_K}^\vee / q{\mathcal{O}_K}^\vee$ to $\mathcal{O}_K / q\mathcal{O}_K$.

If we have a R-LWE sample $(a_i, b_i = a_i \cdot s + e_i)$, we can multiply the right hand side by t.

We get $(a_i', b_i') = (a_i, a_i(ts) + (te_i))$.

- ts is now uniform in $\mathcal{O}_K / q\mathcal{O}_K$
- This is a primal R-LWE sample, with noise term $e_i' = te_i$

But is e_i' small? It is if t is small.

From dual to primal

A useful lemma from [LPR10]

Let $t \in (\mathcal{O}_K{}^\vee)^{-1}$ with $t\mathcal{O}_K{}^\vee$ coprime to (q). Then '$\times t$' is an $\mathcal{O}_K$-module isomorphism from $\mathcal{O}_K{}^\vee / q\mathcal{O}_K{}^\vee$ to $\mathcal{O}_K / q\mathcal{O}_K$.

If we have a R-LWE sample $(a_i, b_i = a_i \cdot s + e_i)$,
we can multiply the right hand side by t.

We get $(a_i', b_i') = (a_i, a_i(ts) + (te_i))$.

- ts is now uniform in $\mathcal{O}_K / q\mathcal{O}_K$
- This is a primal R-LWE sample, with noise term $e_i' = te_i$

But is e_i' small? It is if t is small.

From dual to primal

A useful lemma from [LPR10]

Let $t \in ({\mathcal{O}_K}^\vee)^{-1}$ with $t{\mathcal{O}_K}^\vee$ coprime to (q). Then '$\times t$' is an $\mathcal{O}_K$-module isomorphism from ${\mathcal{O}_K}^\vee / q{\mathcal{O}_K}^\vee$ to $\mathcal{O}_K / q\mathcal{O}_K$.

If we have a R-LWE sample $(a_i, b_i = a_i \cdot s + e_i)$,
we can multiply the right hand side by t.

We get $(a_i', b_i') = (a_i, a_i(ts) + (te_i))$.

- ts is now uniform in $\mathcal{O}_K / q\mathcal{O}_K$
- This is a primal R-LWE sample, with noise term $e_i' = te_i$

But is e_i' small? It is if t is small.

Make the noise small!

Goal

Show that there exists $t \in (\mathcal{O}_K{}^\vee)^{-1}$ small with $t\mathcal{O}_K{}^\vee$ coprime to (q)

- We consider the Gaussian distribution over $(\mathcal{O}_K{}^\vee)^{-1}$
- We show that short vectors are not all trapped in a $(\mathcal{O}_K{}^\vee)^{-1} \cdot J$, for a divisor J of (q).
- Tools: inclusion-exclusion and lattice smoothing

From primal R-LWE to P-LWE

We are given $(a_i, a_i \cdot s + e_i)$ with

- a_i and s in $\mathcal{O}_K$
- e_i with small Minkowski embeddings

We want a related $(a_i', a_i's' + e_i')$ with

- a_i' and s' in $\mathbb{Z}[x]/f$
- e_i' with small coefficients

From primal R-LWE to P-LWE

We are given $(a_i, a_i \cdot s + e_i)$ with

- a_i and s in $\mathcal{O}_K$
- e_i with small Minkowski embeddings

We want a related $(a_i', a_i's' + e_i')$ with

- a_i' and s' in $\mathbb{Z}[x]/f$
- e_i' with small coefficients

Handling the algebra

- $\mathcal{O} := \mathbb{Z}[x]/f$ is an order of $\mathcal{O}_K$.
- Sometimes, they are the same!

The conductor ideal

$\mathcal{C}_{\mathcal{O}} = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}$ is an $\mathcal{O}_K$-ideal and an $\mathcal{O}$-ideal.

If (q) and $\mathcal{C}_{\mathcal{O}}$ are coprime,
if $t \in \mathcal{C}_{\mathcal{O}}$ is such that $t\mathcal{C}_{\mathcal{O}}^{-1}$ and (q) are coprime,
then "$\times t$" is a ring isomorphism from $\mathcal{O}_K/q\mathcal{O}_K$ to $\mathcal{O}/q\mathcal{O}$.

We proceed as in the dual to primal case, using a small t.

Handling the algebra

- $\mathcal{O} := \mathbb{Z}[x]/f$ is an order of $\mathcal{O}_K$.
- Sometimes, they are the same!

The conductor ideal

$\mathcal{C}_{\mathcal{O}} = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}$ is an $\mathcal{O}_K$-ideal and an $\mathcal{O}$-ideal.

If (q) and $\mathcal{C}_{\mathcal{O}}$ are coprime,
if $t \in \mathcal{C}_{\mathcal{O}}$ is such that $t\mathcal{C}_{\mathcal{O}}^{-1}$ and (q) are coprime,
then "$\times t$" is a ring isomorphism from $\mathcal{O}_K/q\mathcal{O}_K$ to $\mathcal{O}/q\mathcal{O}$.

We proceed as in the dual to primal case, using a small t.

Handling the algebra

- $\mathcal{O} := \mathbb{Z}[x]/f$ is an order of $\mathcal{O}_K$.
- Sometimes, they are the same!

The conductor ideal

$\mathcal{C}_{\mathcal{O}} = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}$ is an $\mathcal{O}_K$-ideal and an $\mathcal{O}$-ideal.

If (q) and $\mathcal{C}_{\mathcal{O}}$ are coprime,
if $t \in \mathcal{C}_{\mathcal{O}}$ is such that $t\mathcal{C}_{\mathcal{O}}^{-1}$ and (q) are coprime,
then "$\times t$" is a ring isomorphism from $\mathcal{O}_K/q\mathcal{O}_K$ to $\mathcal{O}/q\mathcal{O}$.

We proceed as in the dual to primal case, using a small t.

Handling the algebra

- $\mathcal{O} := \mathbb{Z}[x]/f$ is an order of $\mathcal{O}_K$.
- Sometimes, they are the same!

The conductor ideal

$\mathcal{C}_{\mathcal{O}} = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}$ is an $\mathcal{O}_K$-ideal and an $\mathcal{O}$-ideal.

If (q) and $\mathcal{C}_{\mathcal{O}}$ are coprime,
if $t \in \mathcal{C}_{\mathcal{O}}$ is such that $t\mathcal{C}_{\mathcal{O}}^{-1}$ and (q) are coprime,
then "$\times t$" is a ring isomorphism from $\mathcal{O}_K/q\mathcal{O}_K$ to $\mathcal{O}/q\mathcal{O}$.

We proceed as in the dual to primal case, using a small t.

Handling the geometry

Relation between the embeddings

For $e \in \mathbb{R}[x]/f$, computing the Minkowski embedding is multiplying the coefficient vector by

$$\mathbf{V}_f = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & & \dots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{bmatrix},$$

where the α_j's are the roots of f.

We want to know if a noise that has small Minkowski embedding also has small coefficients.

Goal: Show that $\|\mathbf{V}_f^{-1}\|$ is small.

Handling the geometry

Relation between the embeddings

For $e \in \mathbb{R}[x]/f$, computing the Minkowski embedding is multiplying the coefficient vector by

$$\mathbf{V}_f = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & & \ldots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{bmatrix},$$

where the α_j's are the roots of f.

We want to know if a noise that has small Minkowski embedding also has small coefficients.

Goal: Show that $\|\mathbf{V}_f^{-1}\|$ is small.

Root separation

$\|\mathbf{V}_f^{-1}\|$ can be large only if the roots α_j of f are close.

[This can be $2^{\Omega(n)}$, even when f has small coeffs [BM04].]

(1) $f := x^n - c \in \mathbb{Z}[x]$ is great.

(2) Let $P = \sum_{i=1}^{n/2} p_i x^i \in \mathbb{Z}[x]$.

Perturbation: $g := f + P$

For 'small' P, the roots don't move much.

Theorem (Rouché)

If $|P(z)| < |f(z)|$ on a circle, then f and $f + P$ have the same numbers of zeros inside this circle.

Root separation

$\|\mathbf{V}_f^{-1}\|$ can be large only if the roots α_j of f are close.

[This can be $2^{\Omega(n)}$, even when f has small coeffs [BM04].]

(1) $f := x^n - c \in \mathbb{Z}[x]$ is great.

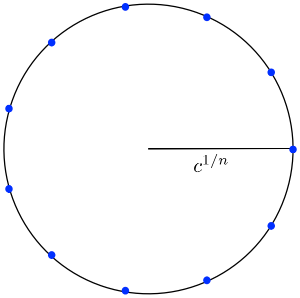
(2) Let $P = \sum_{i=1}^{n/2} p_i x^i \in \mathbb{Z}[x]$.

Perturbation: $g := f + P$

For 'small' P, the roots don't move much.

Theorem (Rouché)

If $|P(z)| < |f(z)|$ on a circle, then f and $f + P$ have the same numbers of zeros inside this circle.



Root separation

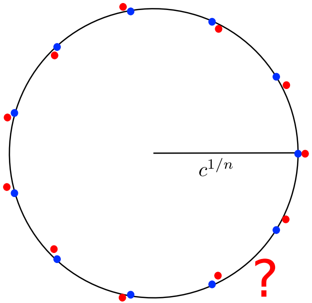
$\|\mathbf{V}_f^{-1}\|$ can be large only if the roots α_j of f are close.

[This can be $2^{\Omega(n)}$, even when f has small coeffs [BM04].]

(1) $f := x^n - c \in \mathbb{Z}[x]$ is great.
(2) Let $P = \sum_{i=1}^{n/2} p_i x^i \in \mathbb{Z}[x]$.

Perturbation: $g := f + P$

For 'small' P, the roots don't move much.



Theorem (Rouché)

If $|P(z)| < |f(z)|$ on a circle, then f and $f + P$ have the same numbers of zeros inside this circle.

Root separation

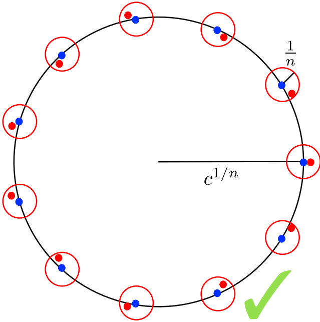
$\|\mathbf{V}_f^{-1}\|$ can be large only if the roots α_j of f are close.

[This can be $2^{\Omega(n)}$, even when f has small coeffs [BM04].]

(1) $f := x^n - c \in \mathbb{Z}[x]$ is great.
(2) Let $P = \sum_{i=1}^{n/2} p_i x^i \in \mathbb{Z}[x]$.

Perturbation: $g := f + P$

For 'small' P, the roots don't move much.



Theorem (Rouché)

If $|P(z)| < |f(z)|$ on a circle, then f and $f + P$ have the same numbers of zeros inside this circle.

Road-map

- The Learning With Errors problem
- Algebraic variants of the LWE problem
- On Polynomial-LWE and Ring-LWE
- **The Middle-Product-LWE problem**

Joint work with M. Rosca, A. Sakzad and R. Steinfeld, Crypto 2017.

Middle product

Let $a \in \mathbb{Z}[x]$ of degree $< n$ and $s \in \mathbb{Z}[x]$ of degree $< 2n - 1$.

- Their product has $3n - 2$ non-trivial coefficients.
- We define $a \circ_n s$ as the middle n coefficients.

$$a \odot_n s := \left\lfloor \frac{(a \cdot b) \bmod x^{2n-1}}{x^{n-1}} \right\rfloor .$$

MP was studied in computer algebra for accelerating computations on polynomials and power series [Sho99,HQZ04].

MP-LWE

Let $q \geq 2$, $\alpha > 0$.

Search MP-LWE

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

- s uniform in $\mathbb{Z}_q[x]$ of degree $< 2n - 1$.
- All a_i's uniform in $\mathbb{Z}_q[x]$ of degree $< n$
- The coefficients of the e_i's are sampled from $D_{\alpha q}$

Titanium: A NIST candidate based on MP-LWE

MP-LWE

Let $q \geq 2$, $\alpha > 0$.

Search MP-LWE

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

- s uniform in $\mathbb{Z}_q[x]$ of degree $< 2n - 1$.
- All a_i's uniform in $\mathbb{Z}_q[x]$ of degree $< n$
- The coefficients of the e_i's are sampled from $D_{\alpha q}$

Titanium: A NIST candidate based on MP-LWE

Hardness of MP-LWE

$$\text{P-LWE}^{f}_{m,q,\alpha} \text{ reduces to } \text{MP-LWE}_{q,\beta}$$

for **any** monic $f \in \mathbb{Z}[x]$ s.t.

- $\deg(f) = n$
- $\gcd(f_0, q) = 1$
- β grows linearly with α and $\mathrm{EF}(f)$

[This extends [Lyu16] from the SIS to the LWE setup]

As long as P-LWE^f is hard for one f, MP-LWE is hard.

Hardness of MP-LWE

$\text{P-LWE}^f_{m,q,\alpha}$ reduces to $\text{MP-LWE}_{q,\beta}$

for **any** monic $f \in \mathbb{Z}[x]$ s.t.

- $\deg(f) = n$
- $\gcd(f_0, q) = 1$
- β grows linearly with α and $\text{EF}(f)$

[This extends [Lyu16] from the SIS to the LWE setup]

As long as P-LWE^f is hard for one f, MP-LWE is hard.

Proof sketch

$$\mathrm{Rot}_f(b) = \mathrm{Rot}_f(a) \times \mathrm{Rot}_f(s) + \mathrm{Rot}_f(e)$$

Take first column

$$M_f \, b = \mathrm{Rot}_f(a) \times M_f \, s + M_f \, e$$

Decompose $\mathrm{Rot}_f(a)$

$$b' = \mathrm{Toep}(a) \, \mathrm{Rot}_f(1) \times M_f \, s + M_f \, e$$

Rename

$$b' = \mathrm{Toep}(a) \times s' + e'$$

Proof sketch

$$\mathrm{Rot}_f(b) = \mathrm{Rot}_f(a) \times \mathrm{Rot}_f(s) + \mathrm{Rot}_f(e)$$

Take first column

$$M_f \; b = \mathrm{Rot}_f(a) \times M_f \; s + M_f \; e$$

Decompose $\mathrm{Rot}_f(a)$

$$b' = \mathrm{Toep}(a) \; \mathrm{Rot}_f(1) \times M_f \; s + M_f \; e$$

Rename

$$b' = \mathrm{Toep}(a) \times s' + e'$$

Proof sketch

$$\mathrm{Rot}_f(b) = \mathrm{Rot}_f(a) \times \mathrm{Rot}_f(s) + \mathrm{Rot}_f(e)$$

Take first column

$$M_f \; b = \mathrm{Rot}_f(a) \times M_f \; s + M_f \; e$$

Decompose $\mathrm{Rot}_f(a)$

$$b' = \mathrm{Toep}(a) \; \mathrm{Rot}_f(1) \times M_f \; s + M_f \; e$$

Rename

$$b' = \mathrm{Toep}(a) \times s' + e'$$

Proof sketch

$$\mathrm{Rot}_f(b) = \mathrm{Rot}_f(a) \times \mathrm{Rot}_f(s) + \mathrm{Rot}_f(e)$$

Take first column

$$M_f \; b = \mathrm{Rot}_f(a) \times M_f \; s + M_f \; e$$

Decompose $\mathrm{Rot}_f(a)$

$$b' = \mathrm{Toep}(a) \; \mathrm{Rot}_f(1) \times M_f \; s + M_f \; e$$

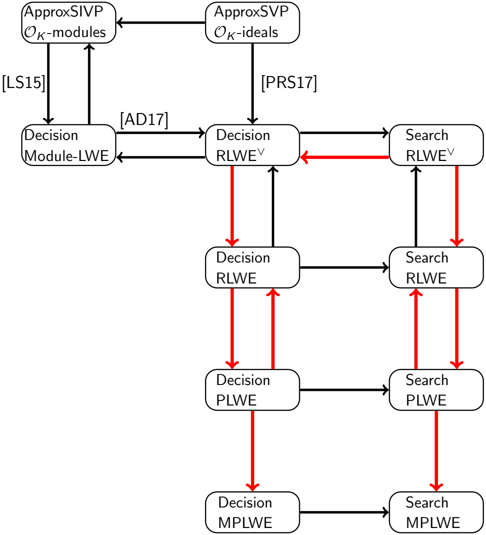
Rename

$$b' = \mathrm{Toep}(a) \times s' + e'$$

Road-map

- The Learning With Errors problem
- Algebraic variants of the LWE problem
- On Polynomial-LWE and Ring-LWE
- The Middle-Product-LWE problem

Landscape overview



The search to decision reduction for RLWE$^\vee$ relies on [PRS17] and a left-over hash lemma over ${\mathcal{O}_K}^\vee / q{\mathcal{O}_K}^\vee$.

Some reductions

- are non-uniform
- require small EF
- require small $\|\mathbf{V}_f\|$

Open problems

$\Rightarrow$ Clean the landscape further.

$\Rightarrow$ Relate PLWE^f to PLWE^g.

$\Rightarrow$ Get a search to decision reduction for MP-LWE.

$\Rightarrow$ Get a reduction from MP-LWE to P-LWE.

$\Rightarrow$ Better understand MP-LWE.