Middle-Product Learning With Errors

Miruna Rosca

LATCA Workshop, Bertinoro

- **Middle-Product Learning With Errors**
  Miruna Rosca, Amin Sakzad, Damien Stehlé, Ron Steinfeld
  In proceedings of CRYPTO 2017

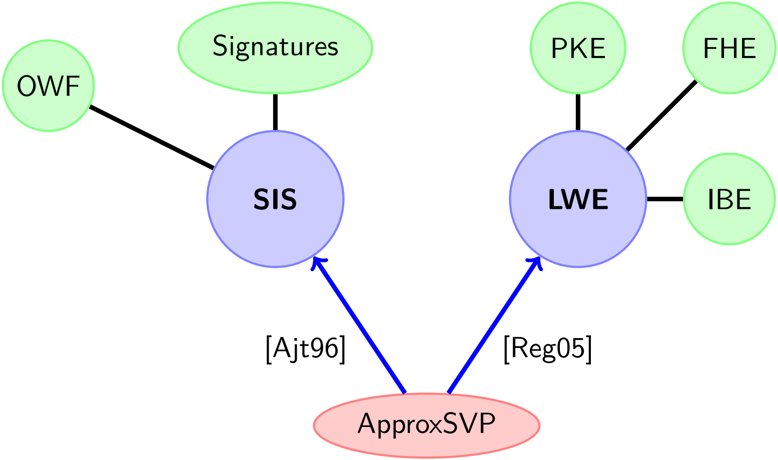
- **Middle-Product Learning With Errors**
  Miruna Rosca, Amin Sakzad, Damien Stehlé, Ron Steinfeld
  In proceedings of CRYPTO 2017

Related works:

- **Titanium: Proposal for a NIST Post-Quantum Public-key Encryption and KEM Standard**
  Ron Steinfeld, Amin Sakzad, Raymond Kuo Zhao
- **On the Ring-LWE and Polynomial-LWE problems**
  Miruna Rosca, Damien Stehlé, Alexandre Wallet
  In proceedings of EUROCRYPT 2018

Lattices and crypto

Lattice-based cryptography



LWE: a quick reminder

Let $n \geq 1$, $q \geq 2$, $\alpha \in (0,1)$ and $\mathbb{R}_q := \mathbb{R}/q\mathbb{Z}$
Let $D_{\alpha \cdot q}$ be the Gaussian on $\mathbb{R}$ of standard deviation $\alpha \cdot q$

$\mathrm{LWE}^n_{q,\alpha}(s)$ for $s \in \mathbb{Z}_q^n$

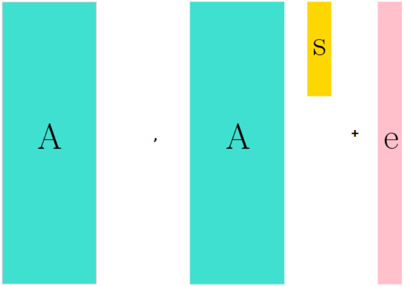
- sample $a \hookleftarrow U(\mathbb{Z}_q^n)$ and $e \hookleftarrow D_{\alpha \cdot q}$
- return $(a, b = \langle a, s \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{R}_q$

(decision) $\mathrm{LWE}^n_{q,\alpha}$

With non-negligible probability over $s \hookleftarrow U(\mathbb{Z}_q^n)$, distinguish between oracle access to

$$\mathrm{LWE}^n_{q,\alpha}(s) \quad \text{and} \quad U(\mathbb{Z}_q^n \times \mathbb{R}_q)$$

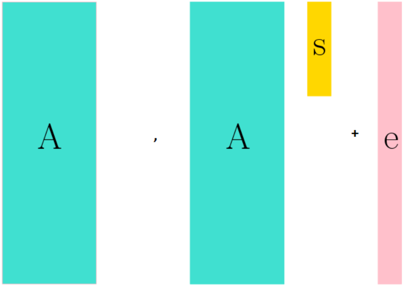
LWE with matrices



Decision: Distinguish the LWE distribution from the uniform one.
Search: Find **s**.

Search is BDD on $\Lambda_q(A) = \{y \in \mathbb{Z}^m : y = A \cdot s \bmod q \text{ for some } s \in \mathbb{Z}^n\}$

LWE with matrices



Decision: Distinguish the LWE distribution from the uniform one.
Search: Find **s**.

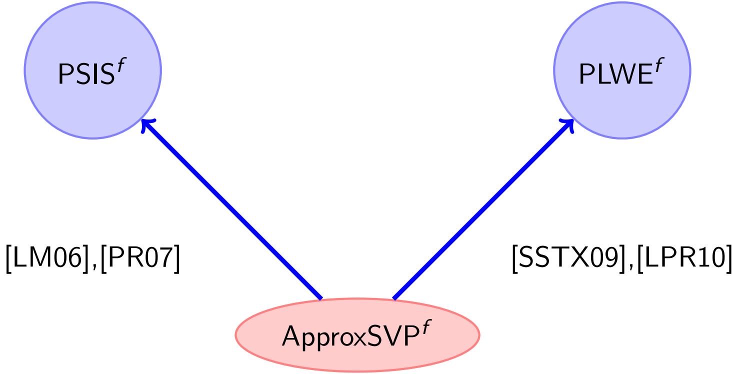
Search is BDD on $\Lambda_q(A) = \{y \in \mathbb{Z}^m : y = A \cdot s \bmod q \text{ for some } s \in \mathbb{Z}^n\}$

Pro: all known ApproxSVP algorithms are exponential in the dimension n

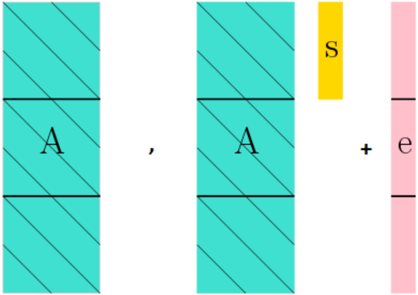
Con: large keys and slow computations because of the matrices involved

How to fix it?

Put some extra algebraic structure on the objects!



PLWE with matrices



Pro: faster cryptographic applications since we work with structured matrices

Con: how hard is ApproxSVP^f?

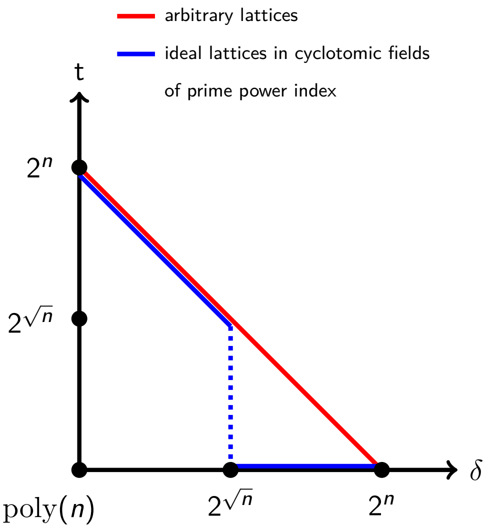
ApproxSVP could be easy for some f' s

- [BS15]: quantum poly. time algorithm to find a generator of a **principal ideal** in any number field

  The case of cyclotomics of prime power index:

- [CDPR16]: quantum poly. time algorithm to find a **short** generator of a **principal ideal** for $2^{O(\sqrt{n})}$ approx. factor

- [CDW17]: quantum poly. time algorithm to solve ApproxSVP for **all ideals** for $2^{O(\sqrt{n})}$ approx. factor



[New result: Alice Pellet--Mary and Damien Stehlé]

A potential weak f risk

- PLWE may still be hard
- impact on the hardness foundation of PLWE
- two solutions:
  - use non-cyclotomic polynomials: [BCLvV16], [PRSD17]
  - use problems which are provably at least as hard as PLWE^f (or PSIS^f) for **a wide class** of polynomials f

How to hedge against the weak f risk?

[Lyu16]: PSIS over $\mathbb{Z}_q[x]$

$\mathrm{PSIS}^{f}_{k,\beta}$

Given $a_1, \ldots, a_k \leftarrow \mathbb{Z}_q[x]/f$, find a nontrivial sol. for $\sum_i a_i z_i = 0$ **mod** f such that $||z_i||_\infty \leq \beta$.

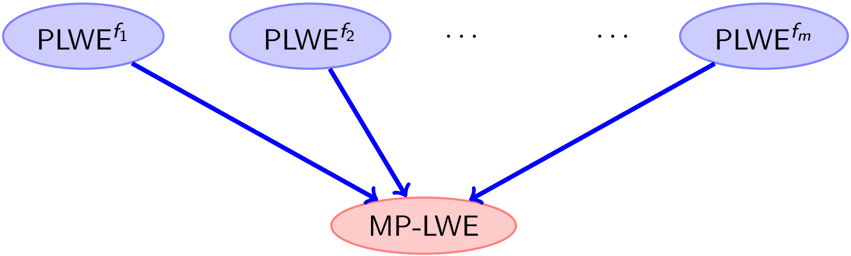
$\mathrm{PSIS}^{<n}_{k,\beta,d}$

Given $a_1, \ldots, a_k \leftarrow \mathbb{Z}_q^{<n}[x]$, find a nontrivial sol. for $\sum_i a_i z_i = 0$ such that $||z_i||_\infty \leq \beta$ and $\deg z_i < d$.

$\mathrm{PSIS}^{f}_{k,\beta}$ reduces to $\mathrm{PSIS}^{<n}_{k,\beta,d}$ for **any** polynomial f s.t. $d \leq \deg(f) \leq n$.

Our result: the LWE case

- we introduce MP-LWE, by making use of the middle product of polynomials
- we give a reduction from (decision) PLWE^f to (decision) MP-LWE for a wide class of polynomials f



Middle Product of two polynomials

Let R be a ring, $a \in R^{<n}[x]$ and $b \in R^{<2n-1}[x]$ two polynomials.

- Their product is:

$$
\begin{aligned}
& c_0 + \cdots + c_{n-2}x^{n-2} \\
& + c_{n-1}x^{n-1} + c_n x^n + \cdots + c_{2n-2}x^{2n-2} \\
& + c_{2n-1}x^{2n-1} + \cdots + c_{3n-3}x^{3n-3} \in R^{<3n-2}[x]
\end{aligned}
$$

- Their n-**middle** product is:

$$
\boldsymbol{a \odot_n b := c_{n-1} + c_n \cdot x + \ldots + c_{2n-2} \cdot x^{n-1}} \in R^{<n}[x]
$$

[The definition generalizes to any d middle coefficients]

Matrix interpretation of the middle product

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} & 0 & \dots & \dots & 0 \\ 0 & a_0 & \dots & a_{n-2} & a_{n-1} & \dots & \dots & 0 \\ \vdots & & \ddots & & & \ddots & & \\ \vdots & & & \ddots & & & \ddots & \\ 0 & 0 & \dots & 0 & a_0 & \dots & a_{n-2} & a_{n-1} \end{bmatrix} \cdot \begin{bmatrix} b_{2n-2} \\ b_{2n-3} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ b_0 \end{bmatrix} = \begin{bmatrix} c_{2n-2} \\ c_{2n-3} \\ \vdots \\ \vdots \\ c_{n-1} \end{bmatrix}$$

PLWE and MP-LWE distributions

$D_{\alpha \cdot q}$: Gaussian on $\mathbb{R}^{<n}[x]$ with standard deviation $\alpha \cdot q$.

$\mathrm{P}^f_{q,\alpha}(s)$ for a polynomial f of degree n and $s \in \mathbb{Z}_q[x]/f$

- sample $a \hookleftarrow U(\mathbb{Z}_q[x]/f)$ and $e \hookleftarrow D_{\alpha \cdot q}$
- return $(a, b = a \cdot s + e) \in \mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f$

$\mathrm{MP}^n_{q,\alpha}(s)$ for $s \in \mathbb{Z}_q^{<2n-1}[x]$

- sample $a \hookleftarrow U(\mathbb{Z}_q^{<n}[x])$ and $e \hookleftarrow D_{\alpha \cdot q}$
- return $(a, b = a \odot_n s + e) \in \mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<n}[x]$

* We use the notation $\mathbb{R}_q := \mathbb{R}/q\mathbb{Z}$

PLWE and MP-LWE problems

(decision) $\mathrm{PLWE}^f_{q,\alpha}$

With non-negligible probability over $s \hookleftarrow U(\mathbb{Z}_q[x]/f)$, distinguish between

$$\mathrm{P}^f_{q,\alpha}(s) \quad \text{and} \quad U(\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f)$$

(decision) $\mathrm{MP\text{-}LWE}^n_{q,\alpha}$

With non-negligible probability over $s \hookleftarrow U(\mathbb{Z}_q^{<2n-1})$, distinguish between

$$\mathrm{MP}^n_{q,\alpha}(s) \quad \text{and} \quad U(\mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<n}[x])$$

Hardness of MP-LWE

Let $n, S > 0$, $q \geq 2$, and $\alpha \in (0, 1)$.

$$\boxed{\mathrm{PLWE}^{f}_{q,\alpha} \text{ reduces to } \mathrm{MP\text{-}LWE}^{n}_{q,\alpha\cdot n\cdot S}}$$

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

- $\deg f = n$
- $\gcd(f_0, q) = 1$
- $\mathrm{EF}(f) := \max\left\{ \frac{||g \bmod f||_\infty}{||g||_\infty} : g \in \mathbb{Z}^{<2n-1}[x] \setminus \{0\} \right\} < S$

Proof idea

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

Proof idea

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

Take first column

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

Proof idea

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

Take first column

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

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

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

Proof idea

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

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

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

Does b' really correspond to an MP-LWE sample?

Randomize the secret s' (self-reducibility)

$$b'' = \mathrm{Toep}(a) \times t + b'$$

Remove the dependency on f in e' (covariance compensation)

$$b^* = e^* + b''$$

PKE from MP-LWE

Public-Key Encryption from MP-LWE

Let q be an odd integer.

KeyGen(1^λ) :

- $sk := s \hookleftarrow U(\mathbb{Z}_q^{<2n-1}[x])$
- for $i \leq t = O(\log q)$
  - $a_i \hookleftarrow U(\mathbb{Z}_q^{<n}[x])$
  - $e_i \hookleftarrow \lfloor D_{\alpha q} \rceil^n$
  - $b_i = a_i \odot_n s + 2 \cdot e_i$
- pk $:= (a_i, b_i)_i$

Public-Key Encryption from MP-LWE

Let $\mu \in \{0,1\}^{<n/2}[x]$ be a message.

Encrypt(μ) :

- for $i \leq t$, sample $r_i \hookleftarrow U(\{0,1\}^{<n/2+1}[x])$
- return $c = (c_1, c_2)$ with:

$$c_1 = \sum r_i \cdot a_i \ , \quad c_2 = \mu + \sum r_i \odot_{n/2} b_i .$$

Decrypt(c) : return the message

$$\mu' = (c_2 - c_1 \odot_{n/2} s \bmod q) \bmod 2.$$

Correctness

For all polynomials of compatible degrees:

$$\boxed{r \odot_{n/2} (a \odot_n s) = (r \cdot a) \odot_{n/2} s}$$

$$\begin{aligned} c_2 - c_1 \odot s &= \mu + \sum r_i \odot b_i - (\sum r_i \cdot a_i) \odot s \\ &= \mu + \sum (r_i \odot (a_i \odot s + 2 \cdot e_i) - (r_i \cdot a_i) \odot s) \\ &= \mu + 2 \sum r_i \odot e_i \end{aligned}$$

* If $||\mu + 2 \sum r_i \odot e_i||_\infty < q/2$, then we can recover μ.

Security

- replace the public key with a truly uniform one (that's fine, thanks to the MP-LWE assumption)
- use the generalized Leftover Hash Lemma to prove that

$$(a_i, b_i)_i, \ \ \sum r_i \cdot a_i, \ \ \sum r_i \odot_{n/2} b_i$$

and

$$(a_i, b_i)_i, \ \ \sum r_i \cdot a_i, \quad u$$

are statistically close.

Related works

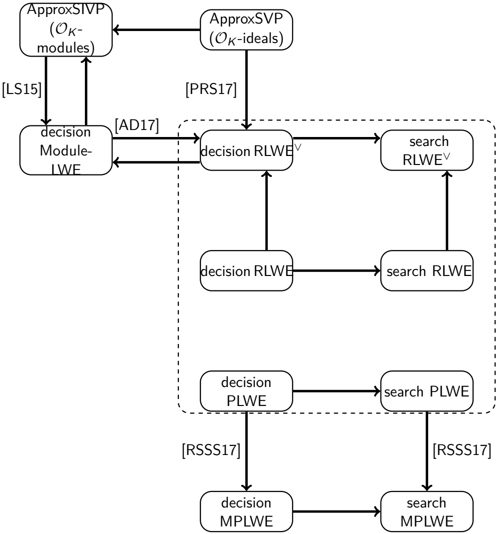
NIST proposal based on MP-LWE: Titanium [SSZ18]

- choose parameters via the reduction
- the case of Std128:
  - parameters for Titanium-CPA: $n = 1024$, $t = 9$, $q = 86017$
  - parameters for Titanium-CCA: $n = 1024$, $t = 10$, $q = 118273$

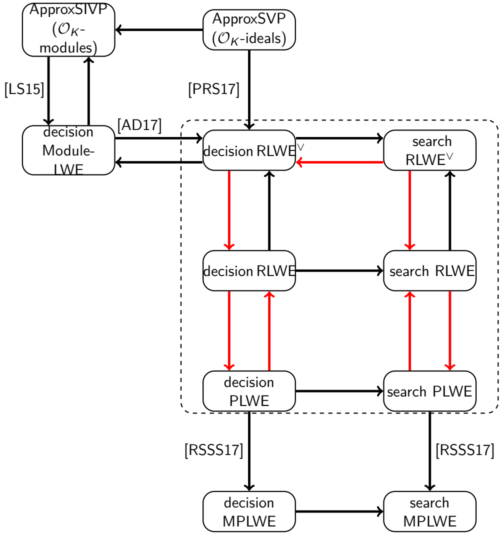
  - size of the family of polynomials f: 3^{256}
  - size of the keys: $|\mathsf{pk}| = 14$ KB, $|\mathsf{sk}| = 0.032$ KB, $|\mathsf{ct}| = 3$ KB

- small differences from [RSSS17]:
  - coefficients of r_i can be bigger than 1
  - the error is from a difference of two binomials

On variants of Ring-LWE and PLWE [RSW18]



On variants of Ring-LWE and PLWE [RSW18]



Open problems

- reduce MP-LWE to PLWE
- get a search MP-LWE to decision MP-LWE reduction
- give an algebraic meaning of MP-LWE
- build more advanced primitives from MP-LWE

Thank you.