

# Middle-Product Learning With Errors

Miruna Roşca, Amin Sakzad, Damien Stehlé and Ron Steinfeld

CRYPTO 2017



# Preview

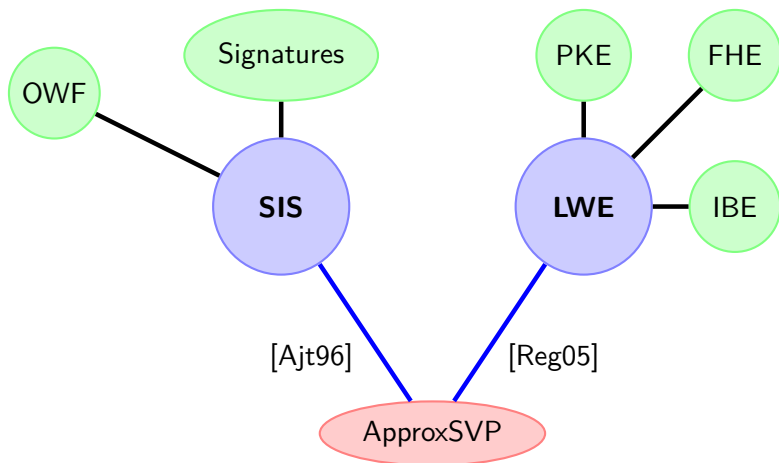
We define an LWE variant which:

- is **at least as hard** as **exponentially many** PLWE instances
- allows **efficient** public key encryption



# Intro

# Lattice based cryptography

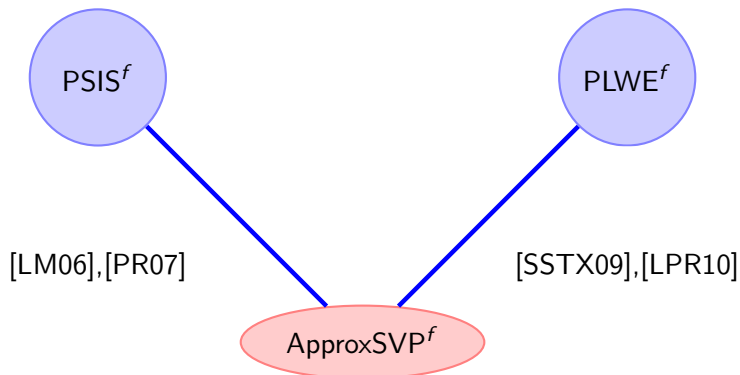


**Advantage:** all known algorithms are exponential in dimension  $n$

Major **drawbacks:** large keys and slow computations

# How to fix this?

Put some extra algebraic structure on the objects!



# 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

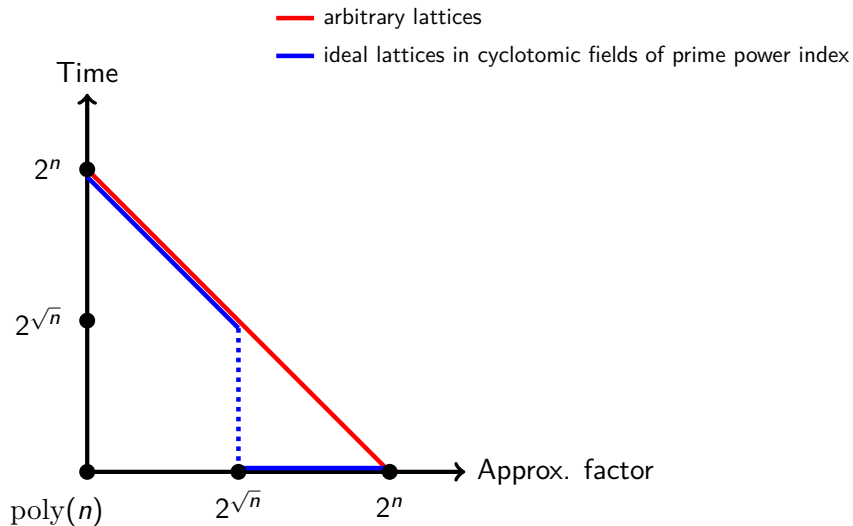
## The case of cyclotomics of prime power index:

- [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

## The case of multiquadratics:

- [BBdVLvV17]: quasipoly. time algorithm to find a **short** generator of a **principal ideal**

# ApproxSVP



# What should be done?

- use non-cyclotomic polynomials: [BCLvV16], [PRSD17]
- use problems which are provably at least as hard as  $\text{PSIS}^f$  or  $\text{PLWE}^f$  for **a wide class** of polynomials  $f$ : [Lyu16]



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

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

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

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

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

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

# Our contribution: the LWE case

- we introduce MP-LWE, by making use of the middle product of polynomials
- we give a reduction from (decision) PLWE<sup>*f*</sup> 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 **middle** product is:

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

# Matrix interpretation of the middle product

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

\* all the results generalize to **any**  $d$  middle coefficients

# PLWE and MP-LWE distributions

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

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

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

$MP_{q,\alpha}^n(s)$  for  $s \in \mathbb{Z}_q^{\leq 2n-1}[x]$

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

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

# PLWE and MP-LWE problems

(decision)  $\text{PLWE}_{q,\alpha}^f$

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

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

(decision)  $\text{MP-LWE}_{q,\alpha}^n$

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

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

# Hardness of MP-LWE

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

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

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

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



# Proof idea

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

# Proof idea

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

Take first column

$$\boxed{M_f} \begin{array}{|c} b \end{array} = \boxed{\text{Rot}_f(a)} \times \boxed{M_f} \begin{array}{|c} s \end{array} + \boxed{M_f} \begin{array}{|c} e \end{array}$$

# Proof idea

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

Take first column

$$\boxed{M_f} \begin{matrix} | \\ b \end{matrix} = \boxed{\text{Rot}_f(a)} \times \boxed{M_f} \begin{matrix} | \\ s \end{matrix} + \boxed{M_f} \begin{matrix} | \\ e \end{matrix}$$

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

$$\begin{matrix} | \\ b' \end{matrix} = \text{Toep}(a) \boxed{\text{Rot}_f(1)} \times \boxed{M_f} \begin{matrix} | \\ s \end{matrix} + \boxed{M_f} \begin{matrix} | \\ e \end{matrix}$$

# Proof idea

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

Take first column

$$\boxed{M_f} \begin{array}{|c|} \hline b \\ \hline \end{array} = \boxed{\text{Rot}_f(a)} \times \boxed{M_f} \begin{array}{|c|} \hline s \\ \hline \end{array} + \boxed{M_f} \begin{array}{|c|} \hline e \\ \hline \end{array}$$

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

$$\begin{array}{|c|} \hline b' \\ \hline \end{array} = \text{Toep}(a) \times \boxed{\text{Rot}_f(1)} \times \boxed{M_f} \begin{array}{|c|} \hline s \\ \hline \end{array} + \boxed{M_f} \begin{array}{|c|} \hline e \\ \hline \end{array}$$

Rename

$$\begin{array}{|c|} \hline b' \\ \hline \end{array} = \text{Toep}(a) \times \begin{array}{|c|} \hline s' \\ \hline \end{array} + \begin{array}{|c|} \hline e' \\ \hline \end{array}$$

# Application of MP-LWE

# Public-Key Encryption from MP-LWE

Let  $q$  be an odd integer.

$\text{KeyGen}(1^\lambda)$  :

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

# Public-Key Encryption from MP-LWE

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

Encrypt( $\mu$ ) :

- for  $i \leq t$ , sample  $r_i \leftarrow U(\{0, 1\}^{\leq n/2+1}[x])$
- 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

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

For all polynomials of compatible degrees:

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

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

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



- 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

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

are statistically close.

- build other cryptographic primitives using MP-LWE
- better understand the link between PLWE and Ring-LWE
- give an algebraic interpretation of the middle product

Thank you.