Middle-Product Learning with Rounding Problem and its Applications

Shi Bai[1] **Katharina Boudgoust**[2] Dipayan Das[3] Adeline Roux-Langlois[2] Weiqiang Wen[2] Zhenfei Zhang[4]

[1] Department of Mathematical Sciences, Florida Atlantic University.

[2] Univ Rennes, CNRS, IRISA.

[3] Department of Mathematics, National Institute of Technology, Durgapur.

[4] Algorand.

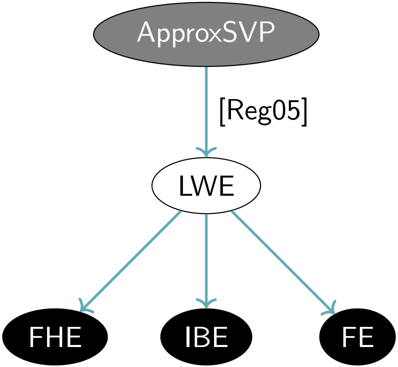
Monash Cybersecurity Seminar, 3rd December 2019, Melbourne, Australia

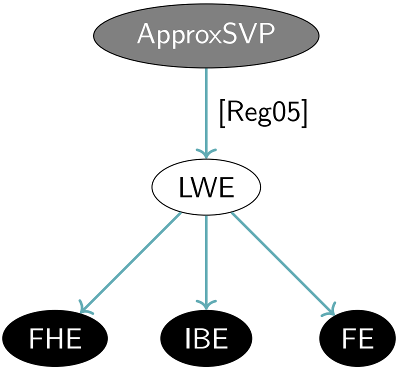
We define a Learning With Errors (LWE) variant which

- is at least as hard as **exponentially many** P-LWE instances,
- is **deterministic** and
- can be used to build **efficient** public key encryption.

Introduction

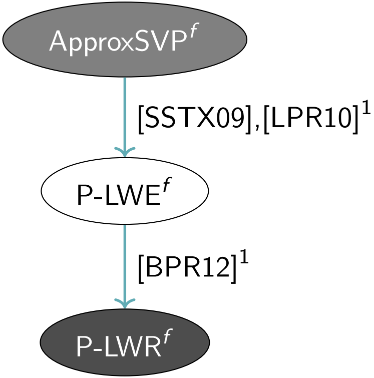
Intro





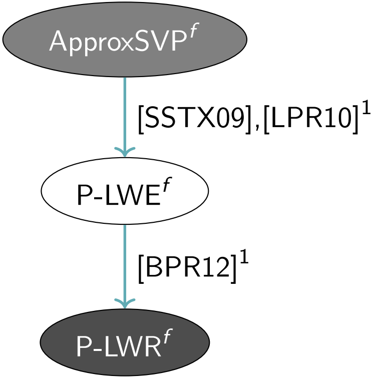
Advantage:		security based on **all** Euclidean lattices
Disadvantages:	(1)	large public keys
	(2)	Gaussian sampling

Two ideas: structured and deterministic variants



[1] For simplicity, take the power-of-two cyclotomic case, where P-LWE and R-LWE (resp. P-LWR and R-LWR) coincide.

Two ideas: structured and deterministic variants

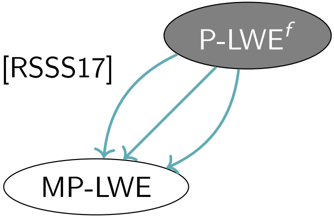


Disadvantages: (1) security based on **restricted** class of lattices, **depending** on f

(2) **decisional** P-LWR: super-polynomial modulus

[1] For simplicity, take the power-of-two cyclotomic case, where P-LWE and R-LWE (resp. P-LWR and R-LWR) coincide.

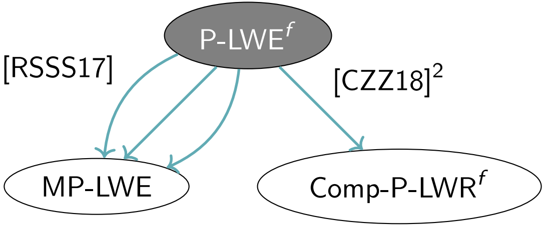
Previous work:



Solution: (1) Middle-Product LWE
reduction for **exponentially** many f

[2] For the sake of lucidity, we simplified the graph. In fact, their reduction was shown for the corresponding ring variants.

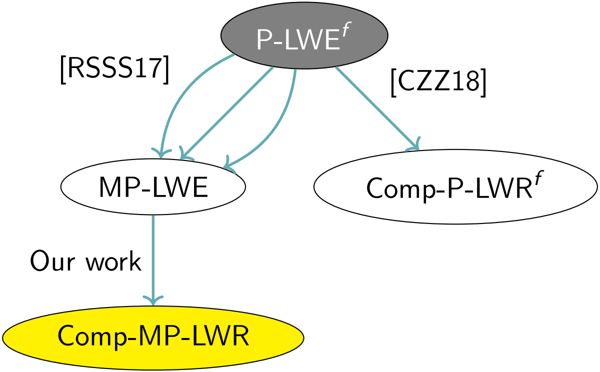
Previous work:



Solution: (1) Middle-Product LWE
reduction for **exponentially** many f
(2) Computational P-LWR^f
allows **provable secure** PKE

[2] For the sake of lucidity, we simplified the graph. In fact, their reduction was shown for the corresponding ring variants.

Our work



Contributions

We define:

(1) Computational Middle-Product Learning with Rounding Problem (Comp-MP-LWR)

We show:

(2) Efficient reduction from MP-LWE to Comp-MP-LWR

We construct:

(3) Public Key Encryption based on Comp-MP-LWR

Computational Middle-Product Learning with Rounding

Middle-Product

Given polynomials $a = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}^{<n}[x]$, $b = \sum_{i=0}^{2n-2} b_i x^i \in \mathbb{Z}^{<2n-1}[x]$.

Their product is

$$\begin{aligned} a \cdot b = c_0 + \cdots + c_{n-2} x^{n-2} \\ + \mathbf{c_{n-1}} x^{n-1} + \mathbf{c_n} x^n + \cdots + \mathbf{c_{2n-2}} x^{2n-2} \\ + c_{2n-1} x^{2n-1} + \cdots + c_{3n-3} x^{3n-3} \in \mathbb{Z}^{<3n-2}[x]. \end{aligned}$$

Their **middle-product** is

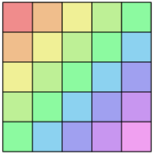
$$a \odot_n b = \mathbf{c_{n-1}} + \mathbf{c_n} x + \cdots + \mathbf{c_{2n-2}} x^{n-1} \in \mathbb{Z}^{<n}[x].$$

Matrix representation of the middle-product

Given a polynomial $b = \sum_{i=0}^{2n-2} b_i x^i \in \mathbb{Z}^{<2n-1}[x]$.

Its **Hankel matrix** is

$$\text{Hankel}(b) = \begin{pmatrix} b_0 & b_1 & \dots & b_{n-1} \\ b_1 & b_2 & \dots & b_n \\ & & \iddots & \\ b_{n-1} & b_n & \dots & b_{2n-2} \end{pmatrix} \in \mathbb{Z}^{n \times n}.$$



For any $a \in \mathbb{Z}^{<n}[x]$ it yields

$$a \odot_n b = \text{Hankel}(b) \cdot \overline{\mathbf{a}},$$

where $\overline{\mathbf{a}} = (a_{n-1}, \dots, a_0)^T$.

Image: wikipedia.de

Let χ be a distribution on $\mathbb{R}^{<n}[x]$ (e.g., Gaussian)

Definition (MP-LWE$_{q,n,\chi}$ distribution for $s \in \mathbb{Z}_q^{<2n-1}[x]$)

Sample $a \leftarrow U\left(\mathbb{Z}_q^{<n}[x]\right)$ and $e \leftarrow \chi$.

Return $(a, b = a \odot_n s + e) \in \mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<n}[x]$

Middle-Product LWE+LWR

Let χ be a distribution on $\mathbb{R}^{<n}[x]$ (e.g., Gaussian)

Definition (MP-LWE$_{q,n,\chi}$ distribution for $s \in \mathbb{Z}_q^{<2n-1}[x]$)

Sample $a \leftarrow U\left(\mathbb{Z}_q^{<n}[x]\right)$ and $e \leftarrow \chi$.

Return $(a, b = a \odot_n s + e) \in \mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<n}[x]$

Given $p < q$ and $y \in \mathbb{Z}_q$. Rounding $\lfloor y \rceil_p = \left\lfloor \frac{p}{q} \cdot y \right\rceil \bmod p$.

Definition (MP-LWR$_{p,q,n}$ distribution for $s \in \mathbb{Z}_q^{<2n-1}[x]$)

Sample $a \leftarrow U\left(\mathbb{Z}_q^{<n}[x]\right)$.

Return $(a, \lfloor b \rceil_p = \lfloor a \odot_n s \rceil_p) \in \mathbb{Z}_q^{<n}[x] \times \mathbb{R}_p^{<n}[x]$

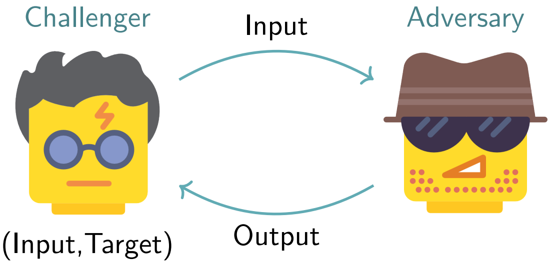
Intuition

Challenger

Adversary

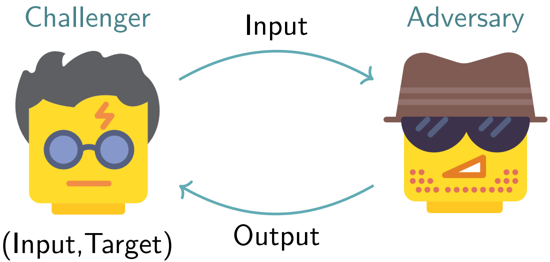
Images: flaticon.com

Intuition



Images: flaticon.com

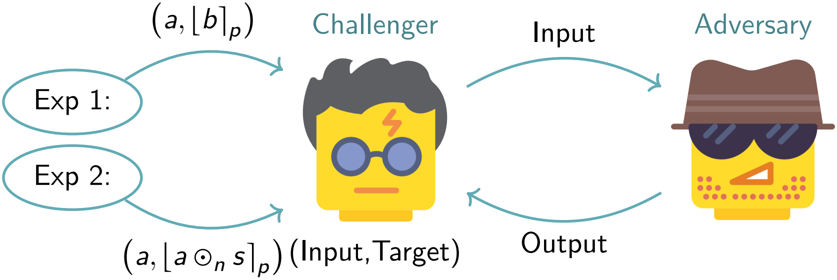
Intuition



Output=Target?

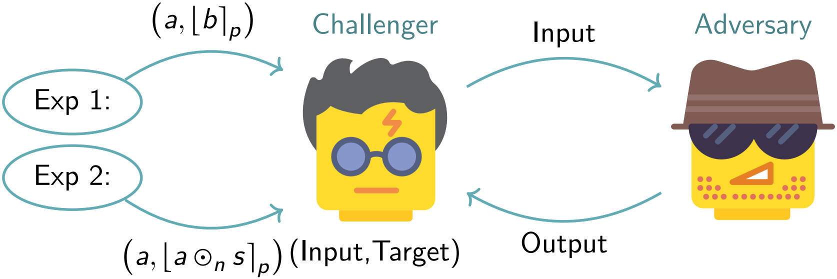
Images: flaticon.com

Intuition



Output=Target?

Intuition

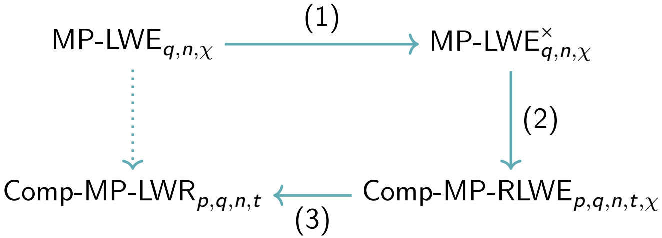


Output=Target?

Assumption (Comp-MP-LWR)

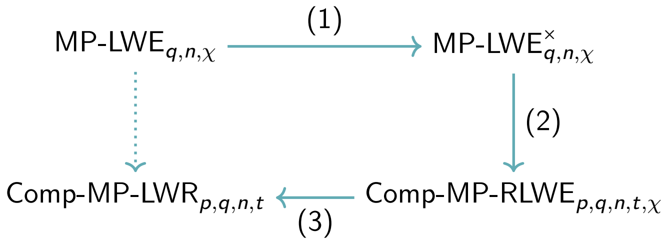
The adversary can't obtain more information from the MP-LWR distribution than from the rounded uniform distribution.

Reduction

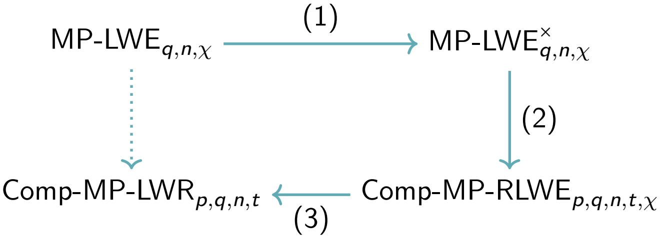


$\text{MP-LWE}_{q,n,\chi}$
(1)
$\text{MP-LWE}^{\times}_{q,n,\chi}$
(2)
$\text{Comp-MP-LWR}_{p,q,n,t}$
(3)
$\text{Comp-MP-RLWE}_{p,q,n,t,\chi}$

Reduction



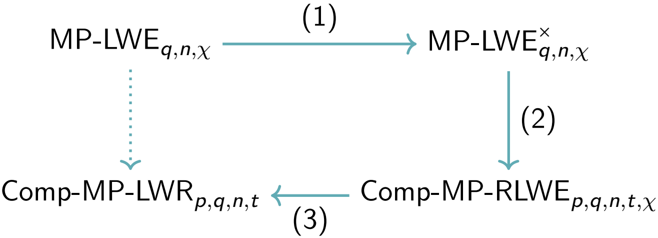
(1) If secret s with **full-rank** Hankel matrix:
(e.g., for q prime, happens with probability $\geq 1 - 1/q$)
a uniform $\Rightarrow$ $a \odot_n s = \text{Hankel}(s) \cdot \overline{\mathbf{a}}$ uniform



(1) If secret s with **full-rank** Hankel matrix:
(e.g., for q prime, happens with probability $\geq 1 - 1/q$)
a uniform $\Rightarrow$ $a \odot_n s = \text{Hankel}(s) \cdot \overline{\mathbf{a}}$ uniform

(2) Round second component of MP-LWE sample

Reduction

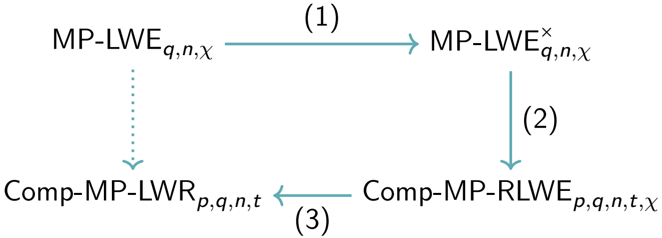


(1) If secret s with **full-rank** Hankel matrix:
(e.g., for q prime, happens with probability $\geq 1 - 1/q$)
a uniform $\Rightarrow$ $a \odot_n s = \text{Hankel}(s) \cdot \overline{\mathbf{a}}$ uniform

(2) Round second component of MP-LWE sample

(3) Using Rényi divergence:
fix number of samples t **a priori**

Reduction



The reduction is **dimension-preserving** and works for **polynomial-sized** modulus q.

Elements sampled from χ are bounded by B with probability at least δ, s.t.

$$q > 2pBnt \text{ and } \delta \geq 1 - \frac{1}{tn}.$$

PKE based on Comp-MP-LWR

Public Key Encryption from Comp-MP-LWR

High level: Adapt encryption scheme from [CZZ18] to middle-product setting.

Public Key Encryption from Comp-MP-LWR

Message $\mu \in \{0,1\}^{n/2}$ and random oracle $H\colon \{0,1\}^{n/2} \to \{0,1\}^{n/2}$

Public Key Encryption from Comp-MP-LWR

Message $\mu \in \{0,1\}^{n/2}$ and random oracle $H: \{0,1\}^{n/2} \to \{0,1\}^{n/2}$

$\mathrm{REC}(y, \langle x \rangle_2) = \lfloor x \rceil_2$, if $|x - y| < \frac{q}{8}$ (for more details, see [Pei14])

Public Key Encryption from Comp-MP-LWR

Message $\mu \in \{0,1\}^{n/2}$ and random oracle $H\colon \{0,1\}^{n/2} \to \{0,1\}^{n/2}$

$\mathrm{REC}(y, \langle x \rangle_2) = \lfloor x \rceil_2$, if $|x - y| < \frac{q}{8}$ (for more details, see [Pei14])

KeyGen(1^λ). Sample $s \leftarrow U\left(\mathbb{Z}_q^{<2n-1}[x]\right)$ s.t. $\mathrm{rank}(\mathrm{Hankel}(s)) = n$ and $a_i \leftarrow U\left(\mathbb{Z}_q^{<n}[x]\right)$ for $1 \leq i \leq t$.

$$\mathbf{pk} = \left(a_i, b_i = \lfloor a_i \odot_n s \rceil_p\right)_{i \leq t} \text{ and } \mathbf{sk} = s.$$

Public Key Encryption from Comp-MP-LWR

Message $\mu \in \{0,1\}^{n/2}$ and random oracle $H: \{0,1\}^{n/2} \to \{0,1\}^{n/2}$

$\mathrm{REC}(y, \langle x \rangle_2) = \lfloor x \rceil_2$, if $|x - y| < \frac{q}{8}$ (for more details, see [Pei14])

KeyGen(1^λ). Sample $s \leftarrow U\left(\mathbb{Z}_q^{<2n-1}[x]\right)$ s.t. $\mathrm{rank}(\mathrm{Hankel}(s)) = n$ and $a_i \leftarrow U\left(\mathbb{Z}_q^{<n}[x]\right)$ for $1 \le i \le t$.

$$\mathbf{pk} = \left(a_i, b_i = \lfloor a_i \odot_n s \rceil_p\right)_{i \le t} \text{ and } \mathbf{sk} = s.$$

Enc(μ, pk). Sample $r_i \leftarrow U\left(\{0,1\}^{<n/2+1}[x]\right)$ for $1 \le i \le t$. Set

$$c_1 = \sum_{i \le t} r_i a_i \quad \text{and} \quad v = \sum_{i \le t} r_i \odot_{n/2} b_i.$$

Further set $c_2 = \langle v \rangle_2$ and $c_3 = H(\lfloor v \rceil_2) \oplus \mu$.

Public Key Encryption from Comp-MP-LWR

Message $\mu \in \{0,1\}^{n/2}$ and random oracle $H\colon \{0,1\}^{n/2} \to \{0,1\}^{n/2}$

$\mathrm{REC}(y, \langle x \rangle_2) = \lfloor x \rceil_2$, if $|x - y| < \frac{q}{8}$ (for more details, see [Pei14])

KeyGen(1^λ). Sample $s \leftarrow U\left(\mathbb{Z}_q^{<2n-1}[x]\right)$ s.t. $\mathrm{rank}(\mathrm{Hankel}(s)) = n$ and $a_i \leftarrow U\left(\mathbb{Z}_q^{<n}[x]\right)$ for $1 \le i \le t$.

$$\mathbf{pk} = \left(a_i, b_i = \lfloor a_i \odot_n s \rceil_p\right)_{i \le t} \text{ and } \mathbf{sk} = s.$$

Enc(μ, pk). Sample $r_i \leftarrow U\left(\{0,1\}^{<n/2+1}[x]\right)$ for $1 \le i \le t$. Set

$$c_1 = \sum_{i \le t} r_i a_i \quad \text{and} \quad v = \sum_{i \le t} r_i \odot_{n/2} b_i.$$

Further set $c_2 = \langle v \rangle_2$ and $c_3 = H(\lfloor v \rceil_2) \oplus \mu$.

Dec(c_1, c_2, c_3, sk). Compute $w = c_1 \odot_{n/2} s$ and return $\mu' = c_3 \oplus H(\mathrm{REC}(w, c_2))$.

KeyGen(1^λ). **pk** $= \left(a_i, b_i = \lfloor a_i \odot_n s \rceil_p\right)_{i \leq t}$ and **sk** $= s$.

Enc(μ, pk). Sample $r_i \leftarrow U\left(\{0,1\}^{<n/2+1}[x]\right)$ for $1 \leq i \leq t$. Set

$$c_1 = \sum_{i \leq t} r_i a_i \quad \text{and} \quad v = \sum_{i \leq t} r_i \odot_{n/2} b_i.$$

Further set $c_2 = \langle v \rangle_2$ and $c_3 = H(\lfloor v \rceil_2) \oplus \mu$.

Dec(c_1, c_2, c_3, sk). Compute $w = c_1 \odot_{n/2} s$ and return $\mu' = c_3 \oplus H(\mathrm{REC}(w, c_2))$.

For **correctness**, reconciliation mechanism has to work:

$$\mathrm{REC}(w, \langle v \rangle_2) = \lfloor v \rceil_2 \text{ if } |w - v| < \frac{q}{8}$$

IND-CPA Security

pk $= (a_i, b_i)$, **sk** $= s$ and ciphertext $c = (c_1, c_2, c_3)$, where

$$c_1 = \sum r_i a_i, \quad v = \sum r_i \odot_{n/2} b_i, \quad c_2 = \langle v \rangle_2 \quad \text{and}$$

$$c_3 = H(\lfloor v \rceil_2) \oplus \mu.$$

Sequence of steps:

- Distinguishing advantage of IND-CPA game upper bounded by advantage of computing preimage $\lfloor v \rceil_2$ of H,

IND-CPA Security

pk $= \left(a_i, \$\right)$, **sk** $= s$ and ciphertext $c = (c_1, c_2, c_3)$, where

$$c_1 = \sum r_i a_i, \quad v = \sum r_i \odot_{n/2} \$, \quad c_2 = \langle v \rangle_2 \quad \text{and}$$

$$c_3 = H(\lfloor v \rceil_2) \oplus \mu.$$

Sequence of steps:

- Distinguishing advantage of IND-CPA game upper bounded by advantage of computing preimage $\lfloor v \rceil_2$ of H,
- Replace second component of **pk** by rounded uniform samples (use Comp-MP-LWR assumption),

IND-CPA Security

pk $= (a_i, \$)$, **sk** $= s$ and ciphertext $c = (c_1, c_2, c_3)$, where

$$c_1 = \sum r_i a_i, \quad v = \boxed{\$}, \quad c_2 = \langle \boxed{\$} \rangle_2 \quad \text{and}$$

$$c_3 = H(\lfloor \boxed{\$} \rceil_2) \oplus \mu.$$

Sequence of steps:

- Distinguishing advantage of IND-CPA game upper bounded by advantage of computing preimage $\lfloor v \rceil_2$ of H,
- Replace second component of **pk** by rounded uniform samples (use Comp-MP-LWR assumption),
- Replace v by uniform sample, thus c_2 is also uniform (use Generalized LHL),

IND-CPA Security

pk $= (a_i, \$)$, **sk** $= s$ and ciphertext $c = (c_1, c_2, c_3)$, where

$$c_1 = \sum r_i a_i, \quad v = \boxed{\$}, \quad c_2 = \langle \boxed{\$} \rangle_2 \quad \text{and}$$

$$c_3 = H(\lfloor \boxed{\$} \rceil_2) \oplus \mu.$$

Sequence of steps:

- Distinguishing advantage of IND-CPA game upper bounded by advantage of computing preimage $\lfloor v \rceil_2$ of H,
- Replace second component of **pk** by rounded uniform samples (use Comp-MP-LWR assumption),
- Replace v by uniform sample, thus c_2 is also uniform (use Generalized LHL),
- As c_1 and c_2 are independent, adversary can only **guess** preimage of H.

Open Questions

- Reduction from **decisional** MP-LWE to **decisional** MP-LWR[3],
- Alternatively: **search-to-decision** reduction for MP-LWR,
- PKE based on MP-LWR in the **standard model**,
- Using **small** secret to gain in **efficiency**.

[3] Carries over to other structured LWR variants.

Thank you

References I

A. Banerjee, C. Peikert, and A. Rosen, **Pseudorandom functions and lattices**, Advances in Cryptology - EUROCRYPT 2012, Proceedings, 2012, pp. 719–737.

L. Chen, Z. Zhang, and Z. Zhang, **On the hardness of the computational ring-lwr problem and its applications**, Advances in Cryptology - ASIACRYPT 2018, Proceedings, Part I, 2018, pp. 435–464.

V. Lyubashevsky, C. Peikert, and O. Regev, **On ideal lattices and learning with errors over rings**, Advances in Cryptology - EUROCRYPT 2010, Proceedings, 2010, pp. 1–23.

C. Peikert, **Lattice cryptography for the internet**, Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Proceedings, 2014, pp. 197–219.

References II

- O. Regev, **On lattices, learning with errors, random linear codes, and cryptography**, Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, 2005, pp. 84–93.
- M. Rosca, A. Sakzad, D. Stehlé, and R. Steinfeld, **Middle-product learning with errors**, Advances in Cryptology - CRYPTO 2017, Proceedings, Part III, 2017, pp. 283–297.
- D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa, **Efficient public key encryption based on ideal lattices**, Advances in Cryptology - ASIACRYPT 2009, Proceedings, 2009, pp. 617–635.