# Algebraically Structured LWE, Revisited

Chris Peikert    Zachary Pepin

University of Michigan

TCC 2019

# 'Algebraic' Learning With Errors

- A foundation of efficient lattice crypto: Ring-LWE, Module-LWE, Polynomial-LWE, Order-LWE, Middle-Product-LWE, ...

# ‘Algebraic’ Learning With Errors

- A foundation of efficient lattice crypto: Ring-LWE, Module-LWE, Polynomial-LWE, Order-LWE, Middle-Product-LWE, ...
- Hardness supported by a web of reductions, from worst-case problems on algebraic lattices and among the problems themselves
  [SSTX'09,LPR'10,LS'15,L'16,PRS'17,RSSS'17,AD'17,RSW'18,BBPS'18,...]

# ‘Algebraic’ Learning With Errors

- A foundation of efficient lattice crypto: Ring-LWE, Module-LWE, Polynomial-LWE, Order-LWE, Middle-Product-LWE, . . .
- Hardness supported by a web of reductions, from worst-case problems on algebraic lattices and among the problems themselves
  [SSTX’09,LPR’10,LS’15,L’16,PRS’17,RSSS’17,AD’17,RSW’18,BBPS’18,. . . ]

# 'Algebraic' Learning With Errors

- A foundation of efficient lattice crypto: Ring-LWE, Module-LWE, Polynomial-LWE, Order-LWE, Middle-Product-LWE, ...
- Hardness supported by a web of reductions, from worst-case problems on algebraic lattices and among the problems themselves
  [SSTX'09,LPR'10,LS'15,L'16,PRS'17,RSSS'17,AD'17,RSW'18,BBPS'18,...]
- But these reductions are often difficult to understand and use:

# 'Algebraic' Learning With Errors

- A foundation of efficient lattice crypto: Ring-LWE, Module-LWE, Polynomial-LWE, Order-LWE, Middle-Product-LWE, ...
- Hardness supported by a web of reductions, from worst-case problems on algebraic lattices and among the problems themselves
  [SSTX'09,LPR'10,LS'15,L'16,PRS'17,RSSS'17,AD'17,RSW'18,BBPS'18,...]
- But these reductions are often difficult to understand and use:
  - Several steps between problems of interest
  - Complex analysis and parameters
  - Frequently large blowup and distortion of error distributions, across different metrics
  - Sometimes non-uniform advice that appears hard to compute

# Prior Hardness of Ring-LWE and MP-LWE

$$\begin{tikzcd} \text{(dual) } \mathcal{O}_K\text{-LWE} \\ \text{worst-case approx-}\mathcal{O}_K\text{-SIVP} \arrow[u, dashed, "{\text{[LPR'10,PRS'17]}}"] \end{tikzcd}$$

# Prior Hardness of Ring-LWE and MP-LWE

(primal) $\mathcal{O}_K$-LWE

[LPR'10,DD'12,RSW'18] complex & non-uniform; expands error

(dual) $\mathcal{O}_K$-LWE

[LPR'10,PRS'17]

worst-case approx-$\mathcal{O}_K$-SIVP

# Prior Hardness of Ring-LWE and MP-LWE

(primal) $\mathbb{Z}[\alpha]$-LWE

[RSW'18]

complex & non-uniform;
expands error by $\geq \|V_\alpha\|, \|V_\alpha^{-1}\|$

(primal) $\mathcal{O}_K$-LWE

[LPR'10,DD'12,RSW'18]

complex & non-uniform;
expands error

(dual) $\mathcal{O}_K$-LWE

[LPR'10,PRS'17]

worst-case approx-$\mathcal{O}_K$-SIVP

# Prior Hardness of Ring-LWE and MP-LWE

MP-LWE$_{n,d}$

[RSSS'17] for any $\alpha$ s.t. $d \leq \deg(\alpha) \leq n$, expands error by $\geq d \cdot \mathsf{EF}(\alpha)$

(primal) $\mathbb{Z}[\alpha]$-LWE

[RSW'18] complex & non-uniform; expands error by $\geq \|V_\alpha\|, \|V_\alpha^{-1}\|$

(primal) $\mathcal{O}_K$-LWE

[LPR'10,DD'12,RSW'18] complex & non-uniform; expands error

(dual) $\mathcal{O}_K$-LWE

[LPR'10,PRS'17]

worst-case approx-$\mathcal{O}_K$-SIVP

# Our Contributions

## Definitions

1. A unified $\mathcal{L}$-LWE problem class covering all proposed algebraic LWEs (over number-field rings)

# Our Contributions

## Definitions

1. A unified $\mathcal{L}$-LWE problem class covering all proposed algebraic LWEs (over number-field rings)
2. A unified Generalized-LWE problem class covering all proposed LWEs (over commutative rings)

# Our Contributions

## Definitions

1. A unified $\mathcal{L}$-LWE problem class covering all proposed algebraic LWEs (over number-field rings)
2. A unified Generalized-LWE problem class covering all proposed LWEs (over commutative rings)

## Reductions

- Simpler, tighter reductions among algebraic and general LWEs

# Our Contributions

## Definitions

1. A unified $\mathcal{L}$-LWE problem class covering all proposed algebraic LWEs (over number-field rings)
2. A unified Generalized-LWE problem class covering all proposed LWEs (over commutative rings)

## Reductions

- Simpler, tighter reductions among algebraic and general LWEs
  - All have easy-to-analyze effects on the error distribution
  - Some are even error preserving

# Our Contributions

## Definitions

1. A unified $\mathcal{L}$-LWE problem class covering all proposed algebraic LWEs (over number-field rings)
2. A unified Generalized-LWE problem class covering all proposed LWEs (over commutative rings)

## Reductions

- Simpler, tighter reductions among algebraic and general LWEs
  - All have easy-to-analyze effects on the error distribution
  - Some are even error preserving
- Error-preserving $\mathcal{L}$-LWE $\leq \mathcal{L}'$-LWE under mild conditions on $\mathcal{L}' \subseteq \mathcal{L}$.

# Our Contributions

## Definitions

1. A unified $\mathcal{L}$-LWE problem class covering all proposed algebraic LWEs (over number-field rings)
2. A unified Generalized-LWE problem class covering all proposed LWEs (over commutative rings)

## Reductions

- Simpler, tighter reductions among algebraic and general LWEs
  - ⋆ All have easy-to-analyze effects on the error distribution
  - ⋆ Some are even error preserving
- Error-preserving $\mathcal{L}$-LWE $\leq \mathcal{L}'$-LWE under mild conditions on $\mathcal{L}' \subseteq \mathcal{L}$.
- For any order $\mathcal{L} = \mathbb{Z}[\alpha]$ with $d \leq \deg(\alpha) \leq n$,

$$\mathbb{Z}[\alpha]\text{-LWE} \leq \text{MP-LWE}_{n,d}$$

  with error expansion $\|V_\alpha\|$.

# New Hardness of MP-LWE

MP-LWE$_{n,d}$

↑ $d \leq \deg(\alpha) \leq n$,
expands by $\geq d \cdot \mathsf{EF}(\alpha)$

(primal) $\mathbb{Z}[\alpha]$-LWE

↑ complex & non-uniform;
expands by $\geq \|V_\alpha\|, \|V_\alpha^{-1}\|$

(primal) $\mathcal{O}_K$-LWE

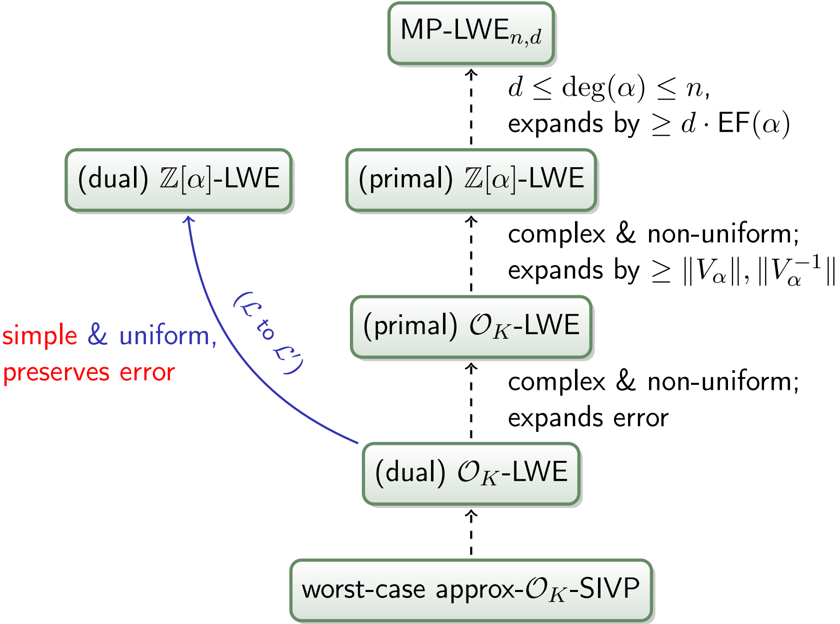
↑ complex & non-uniform;
expands error

(dual) $\mathcal{O}_K$-LWE

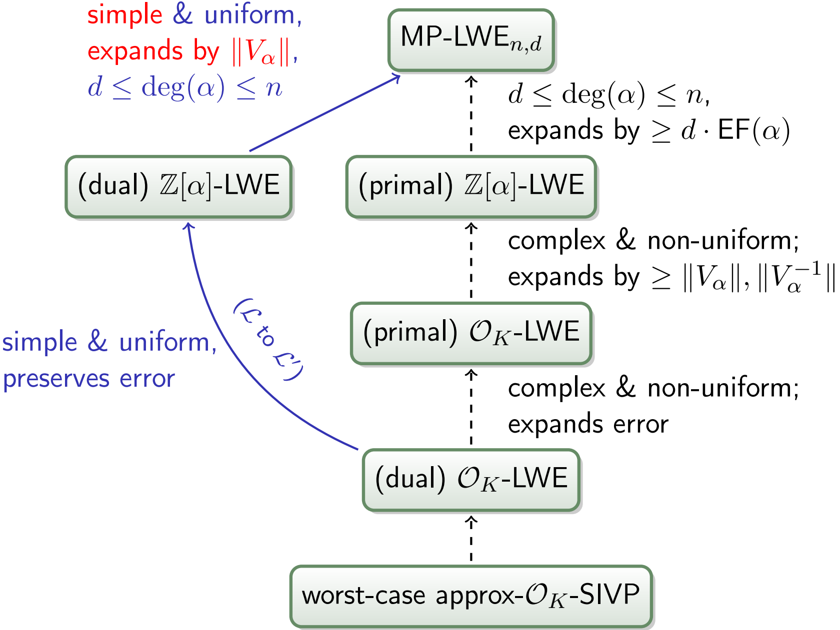
↑

worst-case approx-$\mathcal{O}_K$-SIVP

# New Hardness of MP-LWE



# New Hardness of MP-LWE



# Ring-LWE and Variants

## Ring-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $R = \mathcal{O}_K$ be its ring of integers.
  (E.g., $R \cong \mathbb{Z}[x]/(x^n + 1)$ for $n = 2^k$.)

# Ring-LWE and Variants

## Ring-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $R = \mathcal{O}_K$ be its ring of integers.
  (E.g., $R \cong \mathbb{Z}[x]/(x^n + 1)$ for $n = 2^k$.)
- $R$-LWE$_q$ for secret $s \in R_q^\vee$ concerns 'noisy random products'
  $$\big(a \leftarrow R_q \ , \ b \approx s \cdot a \in R_q^\vee\big).$$

# Ring-LWE and Variants

## Ring-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $R = \mathcal{O}_K$ be its ring of integers.
  (E.g., $R \cong \mathbb{Z}[x]/(x^n + 1)$ for $n = 2^k$.)
- $R$-LWE$_q$ for secret $s \in R_q^\vee$ concerns 'noisy random products'
  $$\big(a \leftarrow R_q\ ,\ b \approx s \cdot a \in R_q^\vee\big).$$

## Order-LWE

- Same, but $R = \mathcal{O}$ is some arbitrary order of $K$ (not necessarily $\mathcal{O}_K$).

# Ring-LWE and Variants

## Ring-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $R = \mathcal{O}_K$ be its ring of integers.
  (E.g., $R \cong \mathbb{Z}[x]/(x^n + 1)$ for $n = 2^k$.)
- $R$-LWE$_q$ for secret $s \in R_q^\vee$ concerns 'noisy random products'
  $$\big(a \leftarrow R_q \ , \ b \approx s \cdot a \in R_q^\vee\big).$$

## Order-LWE

- Same, but $R = \mathcal{O}$ is some arbitrary order of $K$ (not necessarily $\mathcal{O}_K$).

## Poly-LWE

- Same, but $R = \mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/f(x)$ and $s, a, s \cdot a \in R_q$ (no dual $R_q^\vee$).

# New Unified Problem: $\mathcal{L}$-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $\mathcal{L} \subset K$ any (full-rank) lattice.

# New Unified Problem: $\mathcal{L}$-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $\mathcal{L} \subset K$ any (full-rank) lattice.
- The coefficient ring of $\mathcal{L}$, which is an order of $K$, is

$$\mathcal{O}^{\mathcal{L}} := \{x \in K : x\mathcal{L} \subseteq \mathcal{L}\} = (\mathcal{L} \cdot \mathcal{L}^{\vee})^{\vee}.$$

# New Unified Problem: $\mathcal{L}$-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $\mathcal{L} \subset K$ any (full-rank) lattice.
- The coefficient ring of $\mathcal{L}$, which is an order of $K$, is

$$\mathcal{O}^{\mathcal{L}} := \{x \in K : x\mathcal{L} \subseteq \mathcal{L}\} = (\mathcal{L} \cdot \mathcal{L}^{\vee})^{\vee}.$$

Note: if $\mathcal{L}$ is an order $\mathcal{O}$ or its dual $\mathcal{O}^{\vee}$, then $\mathcal{O}^{\mathcal{L}} = \mathcal{O}$.

# New Unified Problem: $\mathcal{L}$-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $\mathcal{L} \subset K$ any (full-rank) lattice.
- The coefficient ring of $\mathcal{L}$, which is an order of $K$, is

$$\mathcal{O}^{\mathcal{L}} := \{x \in K : x\mathcal{L} \subseteq \mathcal{L}\} = (\mathcal{L} \cdot \mathcal{L}^\vee)^\vee.$$

Note: if $\mathcal{L}$ is an order $\mathcal{O}$ or its dual $\mathcal{O}^\vee$, then $\mathcal{O}^{\mathcal{L}} = \mathcal{O}$.

## The $\mathcal{L}$-LWE Problem

# New Unified Problem: $\mathcal{L}$-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $\mathcal{L} \subset K$ any (full-rank) lattice.
- The coefficient ring of $\mathcal{L}$, which is an order of $K$, is

$$\mathcal{O}^{\mathcal{L}} := \{x \in K : x\mathcal{L} \subseteq \mathcal{L}\} = (\mathcal{L} \cdot \mathcal{L}^\vee)^\vee.$$

Note: if $\mathcal{L}$ is an order $\mathcal{O}$ or its dual $\mathcal{O}^\vee$, then $\mathcal{O}^{\mathcal{L}} = \mathcal{O}$.

## The $\mathcal{L}$-LWE Problem

- $\mathcal{L}$-LWE$_q$ for secret $s \in \mathcal{L}_q^\vee$ concerns noisy products

$$\left(a \leftarrow \mathcal{O}_q^{\mathcal{L}}\ ,\ b \approx s \cdot a \in \mathcal{L}_q^\vee\right).$$

# New Unified Problem: $\mathcal{L}$-LWE

- Let $K = \mathbb{Q}(\alpha)$ be a number field and $\mathcal{L} \subset K$ any (full-rank) lattice.
- The coefficient ring of $\mathcal{L}$, which is an order of $K$, is

$$\mathcal{O}^{\mathcal{L}} := \{x \in K : x\mathcal{L} \subseteq \mathcal{L}\} = (\mathcal{L} \cdot \mathcal{L}^\vee)^\vee.$$

Note: if $\mathcal{L}$ is an order $\mathcal{O}$ or its dual $\mathcal{O}^\vee$, then $\mathcal{O}^{\mathcal{L}} = \mathcal{O}$.

## The $\mathcal{L}$-LWE Problem

- $\mathcal{L}$-LWE$_q$ for secret $s \in \mathcal{L}_q^\vee$ concerns noisy products

$$\left(a \leftarrow \mathcal{O}_q^{\mathcal{L}} \ , \ b \approx s \cdot a \in \mathcal{L}_q^\vee\right).$$

- Generalizes:

| | |
|---|---|
| Ring-LWE | by taking $\mathcal{L} = \mathcal{O}_K$ to be the full ring of integers |
| Order-LWE | by taking $\mathcal{L} = \mathcal{O}$ to be an order of $K$ |
| Poly-LWE | by taking $\mathcal{L} = \mathbb{Z}[\alpha]^\vee$ for some $\alpha \in \mathcal{O}_K$ |
| Module-LWE | by allowing $a, s$ to be vectors |

# Our $\mathcal{L}$-LWE Reductions

**Theorem 1: $\mathcal{L}$ to $\mathcal{L}'$**

- Let $\mathcal{L}' \subseteq \mathcal{L} \subset K$ be lattices with respective coefficient rings $\mathcal{O}' \subseteq \mathcal{O}$, and $|\mathcal{L}/\mathcal{L}'|$ coprime to $q$. (E.g., $\mathcal{L}' = \mathcal{O}' \subseteq \mathcal{L} = \mathcal{O}$.)

# Our $\mathcal{L}$-LWE Reductions

**Theorem 1: $\mathcal{L}$ to $\mathcal{L}'$**

- Let $\mathcal{L}' \subseteq \mathcal{L} \subset K$ be lattices with respective coefficient rings $\mathcal{O}' \subseteq \mathcal{O}$, and $|\mathcal{L}/\mathcal{L}'|$ coprime to $q$. (E.g., $\mathcal{L}' = \mathcal{O}' \subseteq \mathcal{L} = \mathcal{O}$.)

  Then there is a tight error-preserving reduction

$$\mathcal{L}\text{-LWE}_q \leq \mathcal{L}'\text{-LWE}_q \ .$$

# Our $\mathcal{L}$-LWE Reductions

**Theorem 1: $\mathcal{L}$ to $\mathcal{L}'$**

- Let $\mathcal{L}' \subseteq \mathcal{L} \subset K$ be lattices with respective coefficient rings $\mathcal{O}' \subseteq \mathcal{O}$, and $|\mathcal{L}/\mathcal{L}'|$ coprime to $q$. (E.g., $\mathcal{L}' = \mathcal{O}' \subseteq \mathcal{L} = \mathcal{O}$.)

  Then there is a tight error-preserving reduction

  $$\mathcal{L}\text{-LWE}_q \leq \mathcal{L}'\text{-LWE}_q \ .$$

- Proof: easy using the natural inclusions $\mathcal{L}_q^\vee \to (\mathcal{L}')_q^\vee$ and $\mathcal{O}'_q \to \mathcal{O}_q$, which are bijections.

# Our $\mathcal{L}$-LWE Reductions

## Theorem 1: $\mathcal{L}$ to $\mathcal{L}'$

- Let $\mathcal{L}' \subseteq \mathcal{L} \subset K$ be lattices with respective coefficient rings $\mathcal{O}' \subseteq \mathcal{O}$, and $|\mathcal{L}/\mathcal{L}'|$ coprime to $q$. (E.g., $\mathcal{L}' = \mathcal{O}' \subseteq \mathcal{L} = \mathcal{O}$.)

  Then there is a tight error-preserving reduction

  $$\mathcal{L}\text{-LWE}_q \leq \mathcal{L}'\text{-LWE}_q \ .$$

- Proof: easy using the natural inclusions $\mathcal{L}_q^\vee \to (\mathcal{L}')_q^\vee$ and $\mathcal{O}'_q \to \mathcal{O}_q$, which are bijections.

## Theorem 2: $\mathcal{O}'$ to $\mathcal{O}$-Module

- Let $\mathcal{O}$ be any number-field order and $\mathcal{O}' = \mathcal{O}[X]/f(X)$ for any monic irreducible $f(X) \in \mathcal{O}[X]$ of degree $d$.

# Our $\mathcal{L}$-LWE Reductions

## Theorem 1: $\mathcal{L}$ to $\mathcal{L}'$

- Let $\mathcal{L}' \subseteq \mathcal{L} \subset K$ be lattices with respective coefficient rings $\mathcal{O}' \subseteq \mathcal{O}$, and $|\mathcal{L}/\mathcal{L}'|$ coprime to $q$. (E.g., $\mathcal{L}' = \mathcal{O}' \subseteq \mathcal{L} = \mathcal{O}$.)

  Then there is a tight error-preserving reduction

  $$\mathcal{L}\text{-LWE}_q \leq \mathcal{L}'\text{-LWE}_q \ .$$

- Proof: easy using the natural inclusions $\mathcal{L}_q^\vee \to (\mathcal{L}')_q^\vee$ and $\mathcal{O}'_q \to \mathcal{O}_q$, which are bijections.

## Theorem 2: $\mathcal{O}'$ to $\mathcal{O}$-Module

- Let $\mathcal{O}$ be any number-field order and $\mathcal{O}' = \mathcal{O}[X]/f(X)$ for any monic irreducible $f(X) \in \mathcal{O}[X]$ of degree $d$.

  Then there is a tight "effectively error-preserving" reduction

  $$\mathcal{O}'\text{-LWE}_q \leq \mathcal{O}\text{-Module-LWE}_q^d \ .$$

# Our $\mathcal{L}$-LWE Reductions

## Theorem 1: $\mathcal{L}$ to $\mathcal{L}'$

- Let $\mathcal{L}' \subseteq \mathcal{L} \subset K$ be lattices with respective coefficient rings $\mathcal{O}' \subseteq \mathcal{O}$, and $|\mathcal{L}/\mathcal{L}'|$ coprime to $q$. (E.g., $\mathcal{L}' = \mathcal{O}' \subseteq \mathcal{L} = \mathcal{O}$.)

  Then there is a tight error-preserving reduction

  $$\mathcal{L}\text{-LWE}_q \leq \mathcal{L}'\text{-LWE}_q \ .$$

- Proof: easy using the natural inclusions $\mathcal{L}_q^\vee \to (\mathcal{L}')_q^\vee$ and $\mathcal{O}'_q \to \mathcal{O}_q$, which are bijections.

## Theorem 2: $\mathcal{O}'$ to $\mathcal{O}$-Module

- Let $\mathcal{O}$ be any number-field order and $\mathcal{O}' = \mathcal{O}[X]/f(X)$ for any monic irreducible $f(X) \in \mathcal{O}[X]$ of degree $d$.

  Then there is a tight "effectively error-preserving" reduction

  $$\mathcal{O}'\text{-LWE}_q \leq \mathcal{O}\text{-Module-LWE}_q^d \ .$$

- Proof: $\mathcal{O}'$ is a rank-$d$ $\mathcal{O}$-module. Keep just first coordinate of $b \approx s \cdot a$.

# Middle-Product-LWE

## MP-LWE

- For $s \in \mathbb{Z}_q^{<n+d-1}[x]$ and $a \in \mathbb{Z}_q^{<n}[x]$, the

  middle product $s \odot_d a$

  is the middle $d$ coefficients of $s \cdot a \in \mathbb{Z}_q^{<2(n-1)+d}[x]$.

# Middle-Product-LWE

## MP-LWE

- For $s \in \mathbb{Z}_q^{<n+d-1}[x]$ and $a \in \mathbb{Z}_q^{<n}[x]$, the

$$\text{middle product } s \odot_d a$$

  is the middle $d$ coefficients of $s \cdot a \in \mathbb{Z}_q^{<2(n-1)+d}[x]$.

- MP-LWE$_{n,d,q}$ for secret $s$ concerns 'noisy random middle products'

$$(a \leftarrow \mathbb{Z}_q^{<n}[x]\ ,\ b \approx s \odot_d a \in \mathbb{Z}_q^{<d}[x]).$$

# Middle-Product-LWE

## MP-LWE

- For $s \in \mathbb{Z}_q^{<n+d-1}[x]$ and $a \in \mathbb{Z}_q^{<n}[x]$, the

$$\text{middle product } s \odot_d a$$

is the middle $d$ coefficients of $s \cdot a \in \mathbb{Z}_q^{<2(n-1)+d}[x]$.

- MP-LWE$_{n,d,q}$ for secret $s$ concerns 'noisy random middle products'

$$(a \leftarrow \mathbb{Z}_q^{<n}[x]\ ,\ b \approx s \odot_d a \in \mathbb{Z}_q^{<d}[x]).$$

## Theorem 3: $\mathbb{Z}[\alpha]$-to-MP Reduction

- For any order $\mathcal{L} = \mathbb{Z}[\alpha]$ with $d \leq \deg(\alpha) \leq n$, we have

$$\mathbb{Z}[\alpha]\text{-LWE}_q \leq \text{MP-LWE}_{n,d,q}$$

with error expansion $\|V_\alpha\|$ of, e.g., spherical Gaussians.

# Middle-Product-LWE

## MP-LWE

- For $s \in \mathbb{Z}_q^{<n+d-1}[x]$ and $a \in \mathbb{Z}_q^{<n}[x]$, the

$$\text{middle product } s \odot_d a$$

is the middle $d$ coefficients of $s \cdot a \in \mathbb{Z}_q^{<2(n-1)+d}[x]$.

- MP-LWE$_{n,d,q}$ for secret $s$ concerns 'noisy random middle products'

$$(a \leftarrow \mathbb{Z}_q^{<n}[x]\ ,\ b \approx s \odot_d a \in \mathbb{Z}_q^{<d}[x]).$$

## Theorem 3: $\mathbb{Z}[\alpha]$-to-MP Reduction

- For any order $\mathcal{L} = \mathbb{Z}[\alpha]$ with $d \leq \deg(\alpha) \leq n$, we have

$$\mathbb{Z}[\alpha]\text{-LWE}_q \leq \text{MP-LWE}_{n,d,q}$$

with error expansion $\|V_\alpha\|$ of, e.g., spherical Gaussians.

- Proof sketch: rest of the talk...

# New Problem: Generalized-LWE

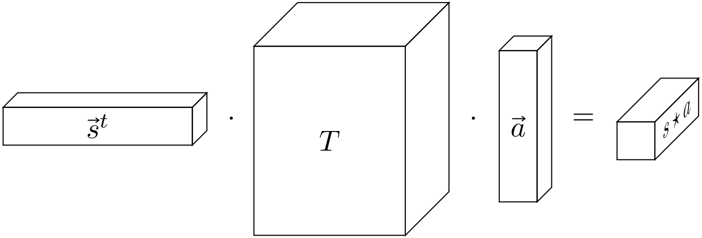
- In every LWE problem, the 'product' $s \star a$ is a fixed $\mathcal{R}$-bilinear form over, e.g., $\mathcal{R} = \mathbb{Z}_q$ or $R_q$.

# New Problem: Generalized-LWE

- In every LWE problem, the 'product' $s \star a$ is a fixed $\mathcal{R}$-bilinear form over, e.g., $\mathcal{R} = \mathbb{Z}_q$ or $R_q$.
- Fixing bases for $s, a, s \star a$, the bilinear form may be represented as a fixed 3-dimensional tensor $T$:

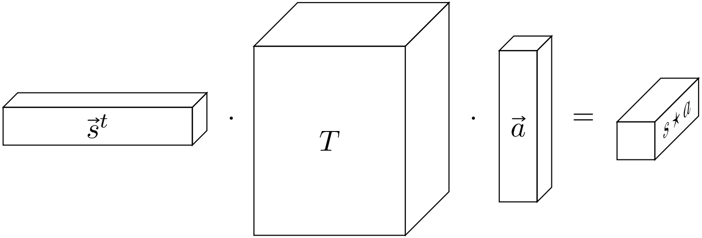
# New Problem: Generalized-LWE

- In every LWE problem, the 'product' $s \star a$ is a fixed $\mathcal{R}$-bilinear form over, e.g., $\mathcal{R} = \mathbb{Z}_q$ or $R_q$.
- Fixing bases for $s, a, s \star a$, the bilinear form may be represented as a fixed 3-dimensional tensor $T$:

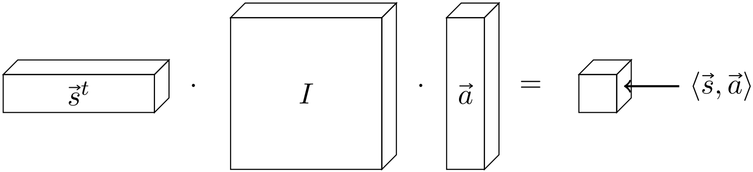


## New Problem: Generalized-LWE

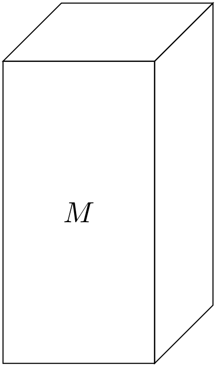
- In every LWE problem, the 'product' $s \star a$ is a fixed $\mathcal{R}$-bilinear form over, e.g., $\mathcal{R} = \mathbb{Z}_q$ or $R_q$.
- Fixing bases for $s, a, s \star a$, the bilinear form may be represented as a fixed 3-dimensional tensor $T$:



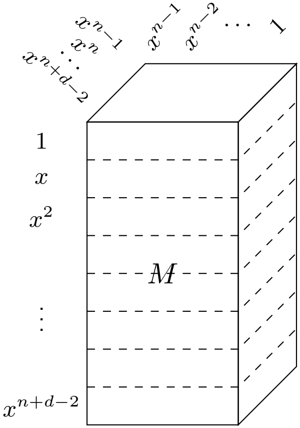

- Plain LWE:



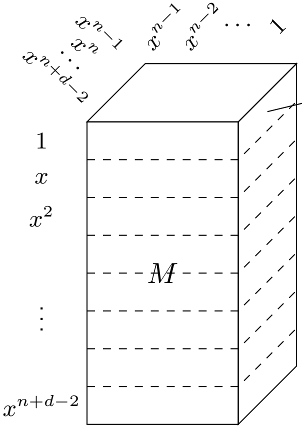
# Middle-Product-LWE$_{n,d}$ Tensor



# Middle-Product-LWE$_{n,d}$ Tensor

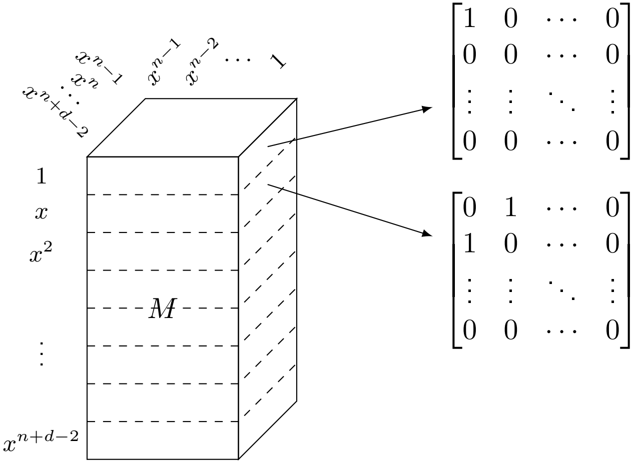


# Middle-Product-LWE$_{n,d}$ Tensor

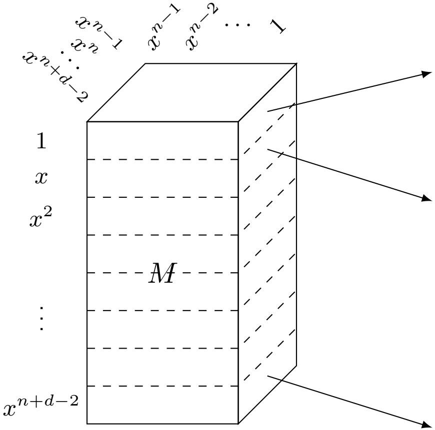



$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

# Middle-Product-LWE$_{n,d}$ Tensor



# Middle-Product-LWE$_{n,d}$ Tensor



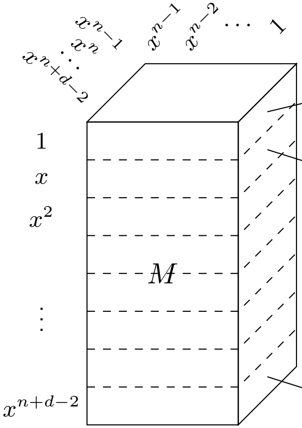

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

$$\vdots$$

$$\begin{bmatrix} 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}$$

# Middle-Product-LWE$_{n,d}$ Tensor




$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

$$\vdots$$

$$\begin{bmatrix} 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}$$

a full basis of $d \times n$ Hankel matrices:

entry $j, k$ given by $j + k$

(constant on anti-diagonals)

# $\mathbb{Z}[\alpha]$-LWE $\leq$ MP-LWE Reduction

- Goal: transformation mapping $\mathbb{Z}[\alpha]$-LWE samples to MP-LWE$_{n,d}$ samples, and uniform ones to uniform ones.

# $\mathbb{Z}[\alpha]$-LWE $\leq$ MP-LWE Reduction

- Goal: transformation mapping $\mathbb{Z}[\alpha]$-LWE samples to MP-LWE$_{n,d}$ samples, and uniform ones to uniform ones.

- Say $d = \deg(\alpha) = n$ for simplicity. The (dual) $\mathbb{Z}[\alpha]$-LWE tensor $T$ is

$$T_{i,j,k} = \mathrm{Tr}(p_i^\vee \cdot p_j \cdot p_k) = \mathrm{Tr}(p_i^\vee \cdot \alpha^{j+k}),$$

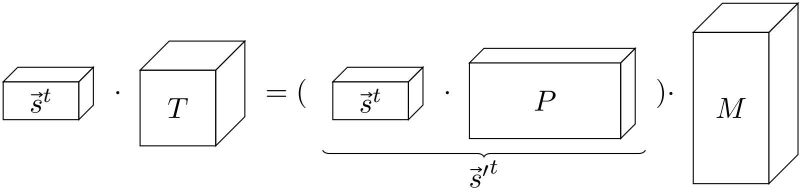
where $\vec{p} = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ is the power basis of $\mathbb{Z}[\alpha]$.

# $\mathbb{Z}[\alpha]$-LWE $\leq$ MP-LWE Reduction

- Goal: transformation mapping $\mathbb{Z}[\alpha]$-LWE samples to MP-LWE$_{n,d}$ samples, and uniform ones to uniform ones.
- Say $d = \deg(\alpha) = n$ for simplicity. The (dual) $\mathbb{Z}[\alpha]$-LWE tensor $T$ is

$$T_{i,j,k} = \mathrm{Tr}(p_i^\vee \cdot p_j \cdot p_k) = \mathrm{Tr}(p_i^\vee \cdot \alpha^{j+k}),$$

  where $\vec{p} = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ is the power basis of $\mathbb{Z}[\alpha]$.
- So, each 'layer' $T_{i\cdot\cdot}$ is a Hankel matrix, and we can factor:



# $\mathbb{Z}[\alpha]$-LWE $\leq$ MP-LWE Reduction

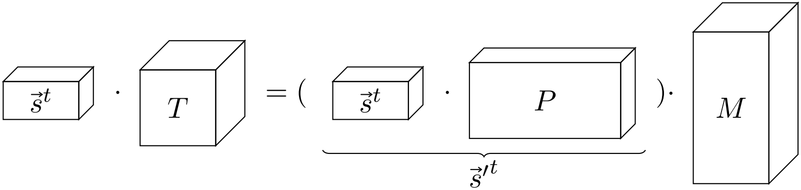
- Goal: transformation mapping $\mathbb{Z}[\alpha]$-LWE samples to MP-LWE$_{n,d}$ samples, and uniform ones to uniform ones.

- Say $d = \deg(\alpha) = n$ for simplicity. The (dual) $\mathbb{Z}[\alpha]$-LWE tensor $T$ is

$$T_{i,j,k} = \mathrm{Tr}(p_i^\vee \cdot p_j \cdot p_k) = \mathrm{Tr}(p_i^\vee \cdot \alpha^{j+k}),$$

  where $\vec{p} = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ is the power basis of $\mathbb{Z}[\alpha]$.

- So, each 'layer' $T_{i\cdot\cdot}$ is a Hankel matrix, and we can factor:




- Generally: $T$-LWE $\leq$ $M$-LWE for any $T, M$ that factor as above.

# Final Thoughts

- It is easy to use Ring-LWE as a foundation for the hardness of various algebraic LWE problems, via simple and tight reductions.

# Final Thoughts

- It is easy to use Ring-LWE as a foundation for the hardness of various algebraic LWE problems, via simple and tight reductions.
- Open: what other LWE problems have reductions from problems over multiple rings simultaneously?

# Final Thoughts

- It is easy to use Ring-LWE as a foundation for the hardness of various algebraic LWE problems, via simple and tight reductions.
- Open: what other LWE problems have reductions from problems over multiple rings simultaneously?
- Open: hardness of Ring-LWE (over some fixed ring) based on multiple "unrelated" LWE problems?

# Final Thoughts

- It is easy to use Ring-LWE as a foundation for the hardness of various algebraic LWE problems, via simple and tight reductions.
- Open: what other LWE problems have reductions from problems over multiple rings simultaneously?
- Open: hardness of Ring-LWE (over some fixed ring) based on multiple "unrelated" LWE problems?

Thanks!