A Too$\lambda\kappa$it for Ri$\nu\gamma$-$\Lambda\Omega$E $\kappa\rho$y$\pi\tau o\gamma\rho\alpha\phi$

Vadim Lyubashevsky[1] $\boxed{\text{Chris Peikert}^{2}}$ Oded Regev[3]

[1]INRIA & ENS Paris

[2]Georgia Tech

[3]Courant Institute, NYU

Eurocrypt 2013
27 May

A Toolkit for Ring-LWE Cryptography

Vadim Lyubashevsky[1] Chris Peikert[2] Oded Regev[3]

[1]INRIA & ENS Paris

[2]Georgia Tech

[3]Courant Institute, NYU

Eurocrypt 2013
27 May

Lattice- and Ring-Based Cryptography

- Offers worst-case hardness [Ajtai'96,...], asymptotic efficiency & parallelism, and (apparent) quantum resistance.

Lattice- and Ring-Based Cryptography

- Offers worst-case hardness [Ajtai'96,...], asymptotic efficiency & parallelism, and (apparent) quantum resistance.
- Many exciting developments in recent years:
  - ⋆ Encryption [R'05,PW'08,PVW'08,ACPS'09,...]
  - ⋆ Signatures [LM'08,GPV'08,L'09,CHKP'10,B'10,GKV'10,BF'11ab,L'12,...]
  - ⋆ (H)IBE & FE [GPV'08,CHKP'10,ABB'10,AFV'11,...]
  - ⋆ FHE [G'09,vDGHV'10,SV'11,BV'11ab,BGV'12,B'12,...]
  - ⋆ Multi-linear maps [GGH'13,CLT'13,...]

Lattice- and Ring-Based Cryptography

- Offers worst-case hardness [Ajtai'96,...], asymptotic efficiency & parallelism, and (apparent) quantum resistance.
- Many exciting developments in recent years:
  - ⋆ Encryption [R'05,PW'08,PVW'08,ACPS'09,...]
  - ⋆ Signatures [LM'08,GPV'08,L'09,CHKP'10,B'10,GKV'10,BF'11ab,L'12,...]
  - ⋆ (H)IBE & FE [GPV'08,CHKP'10,ABB'10,AFV'11,...]
  - ⋆ FHE [G'09,vDGHV'10,SV'11,BV'11ab,BGV'12,B'12,...]
  - ⋆ Multi-linear maps [GGH'13,CLT'13,...]
- Most modern schemes are based on the SIS/LWE problems [A'96,R'05] and/or their ring variants [M'02,PR'06,LM'06,LPR'10].

Lattice- and Ring-Based Cryptography

- Offers worst-case hardness [Ajtai'96,...], asymptotic efficiency & parallelism, and (apparent) quantum resistance.
- Many exciting developments in recent years:
  - ⋆ Encryption [R'05,PW'08,PVW'08,ACPS'09,...]
  - ⋆ Signatures [LM'08,GPV'08,L'09,CHKP'10,B'10,GKV'10,BF'11ab,L'12,...]
  - ⋆ (H)IBE & FE [GPV'08,CHKP'10,ABB'10,AFV'11,...]
  - ⋆ FHE [G'09,vDGHV'10,SV'11,BV'11ab,BGV'12,B'12,...]
  - ⋆ Multi-linear maps [GGH'13,CLT'13,...]
- Most modern schemes are based on the SIS/LWE problems [A'96,R'05] and/or their ring variants [M'02,PR'06,LM'06,LPR'10].
  - ✗ SIS/LWE aren't quite practical: $\Omega(n^2)$ key sizes and runtimes
  - ✔ Ring-based primitives are! $\tilde{O}(n)$ complexity

LWE Over Rings, Over-Simplified [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1 + X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

LWE Over Rings, Over-Simplified [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- For $s \leftarrow R_q$, pairs $\{(a_i\ ,\ b_i)\} \stackrel{c}{\approx}$ uniform $\{(a_i\ ,\ b_i)\}$:

$$
\begin{array}{ccc}
a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q \\
a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q \\
 & \vdots &
\end{array}
$$

LWE Over Rings, Over-Simplified [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- For $s \leftarrow R_q$, pairs $\{(a_i\ ,\ b_i)\} \overset{c}{\approx}$ uniform $\{(a_i\ ,\ b_i)\}$:

$$
\begin{aligned}
a_1 \leftarrow R_q \quad &, \quad b_1 = a_1 \cdot s + e_1 \in R_q \\
a_2 \leftarrow R_q \quad &, \quad b_2 = a_2 \cdot s + e_2 \in R_q \\
&\vdots
\end{aligned}
$$

- Error ("noise") terms $e(X) \in R$ are "short." What could this mean?

LWE Over Rings, Over-Simplified [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- For $s \leftarrow R_q$, pairs $\{(a_i\ ,\ b_i)\} \overset{c}{\approx}$ uniform $\{(a_i\ ,\ b_i)\}$:

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q \\ & \vdots & \end{array}$$

- Error ("noise") terms $e(X) \in R$ are "short." What could this mean?

$$e(X) = \sum_{j=0}^{n-1} e_j X^j \quad \longleftrightarrow \quad (e_0, e_1, \ldots, e_{n-1}) \in \mathbb{Z}^n.$$

LWE Over Rings, Over-Simplified [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- For $s \leftarrow R_q$, pairs $\{(a_i\ ,\ b_i)\} \overset{c}{\approx}$ uniform $\{(a_i\ ,\ b_i)\}$:

$$
\begin{aligned}
a_1 \leftarrow R_q \quad &, \quad b_1 = a_1 \cdot s + e_1 \in R_q \\
a_2 \leftarrow R_q \quad &, \quad b_2 = a_2 \cdot s + e_2 \in R_q \\
&\vdots
\end{aligned}
$$

- Error ("noise") terms $e(X) \in R$ are "short." What could this mean?

$$
e(X) = \sum_{j=0}^{n-1} e_j X^j \quad \longleftrightarrow \quad (e_0, e_1, \ldots, e_{n-1}) \in \mathbb{Z}^n.
$$

- Applications need $(+,\cdot)$-combinations of errors to remain short, so we can "decode" them modulo q. Significantly affects security.

LWE Over Rings, Over-Simplified [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- For $s \leftarrow R_q$, pairs $\{(a_i\ ,\ b_i)\} \overset{c}{\approx}$ uniform $\{(a_i\ ,\ b_i)\}$:

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q \\ & \vdots & \end{array}$$

- Error ("noise") terms $e(X) \in R$ are "short." What could this mean?

$$e(X) = \sum_{j=0}^{n-1} e_j X^j \quad \longleftrightarrow \quad (e_0, e_1, \ldots, e_{n-1}) \in \mathbb{Z}^n.$$

- Applications need $(+,\cdot)$-combinations of errors to remain short, so we can "decode" them modulo q. Significantly affects security.

$$\|e + e'\| \leq \|e\| + \|e'\| \qquad \|e \cdot e'\| \leq \sqrt{n} \cdot \|e\| \cdot \|e'\|.$$

LWE Over Rings, Over-Simplified [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- For $s \leftarrow R_q$, pairs $\{(a_i\ ,\ b_i)\} \overset{c}{\approx}$ uniform $\{(a_i\ ,\ b_i)\}$:

$$\begin{aligned} a_1 \leftarrow R_q \quad &, \quad b_1 = a_1 \cdot s + e_1 \in R_q \\ a_2 \leftarrow R_q \quad &, \quad b_2 = a_2 \cdot s + e_2 \in R_q \\ &\vdots \end{aligned}$$

- Error ("noise") terms $e(X) \in R$ are "short." What could this mean?

$$e(X) = \sum_{j=0}^{n-1} e_j X^j \quad \longleftrightarrow \quad (e_0, e_1, \ldots, e_{n-1}) \in \mathbb{Z}^n.$$

- Applications need $(+, \cdot)$-combinations of errors to remain short, so we can "decode" them modulo q. Significantly affects security.

$$\|e + e'\| \leq \|e\| + \|e'\| \qquad \|e \cdot e'\| \leq \sqrt{n} \cdot \|e\| \cdot \|e'\|.$$

("Expansion factor" $\sqrt{n}$ is worst-case, often quite loose.)

More Rings, Please!

- Rings $\mathbb{Z}[X]/(1 + X^{2^k})$ don't meet all our needs.

More Rings, Please!

- Rings $\mathbb{Z}[X]/(1+X^{2^k})$ don't meet all our needs.
  - ✗ They are rare — might make keys unnecessarily large in practice.

More Rings, Please!

- Rings $\mathbb{Z}[X]/(1+X^{2^k})$ don't meet all our needs.
  - ✗ They are rare — might make keys unnecessarily large in practice.
  - ✗✗ Many schemes cannot use them at all!

    E.g., SIMD homom. encryption [SV'11] and applications [GHS'12abc]

More Rings, Please!

- Rings $\mathbb{Z}[X]/(1+X^{2^k})$ don't meet all our needs.
  - ✗ They are rare — might make keys unnecessarily large in practice.
  - ✗✗ Many schemes cannot use them at all!

    E.g., SIMD homom. encryption [SV'11] and applications [GHS'12abc]

- The mth cyclotomic ring: $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ where

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega_m^i) \in \mathbb{Z}[X], \quad \omega_m = e^{2\pi\sqrt{-1}/m} \in \mathbb{C}.$$

  Note: $\Phi_m(X)$ divides $(X^m - 1)$, has degree $n = \varphi(m) = \deg(\Phi_m)$.

  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

More Rings, Please!

- Rings $\mathbb{Z}[X]/(1+X^{2^k})$ don't meet all our needs.
  - ✗ They are rare — might make keys unnecessarily large in practice.
  - ✗✗ Many schemes cannot use them at all!
    E.g., SIMD homom. encryption [SV'11] and applications [GHS'12abc]

- The mth cyclotomic ring: $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ where

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega_m^i) \in \mathbb{Z}[X], \quad \omega_m = e^{2\pi\sqrt{-1}/m} \in \mathbb{C}.$$

  Note: $\Phi_m(X)$ divides $(X^m - 1)$, has degree $n = \varphi(m) = \deg(\Phi_m)$.

  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

- Examples: $\Phi_{2^{k+1}}(X) = 1 + X^{2^k}$, $\quad \Phi_9(X) = 1 + X^3 + X^6$.

More Rings, Please!

- Rings $\mathbb{Z}[X]/(1+X^{2^k})$ don't meet all our needs.
  - ✗ They are rare — might make keys unnecessarily large in practice.
  - ✗✗ Many schemes cannot use them at all!
    E.g., SIMD homom. encryption [SV'11] and applications [GHS'12abc]

- The mth cyclotomic ring: $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ where

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega_m^i) \in \mathbb{Z}[X], \quad \omega_m = e^{2\pi\sqrt{-1}/m} \in \mathbb{C}.$$

  Note: $\Phi_m(X)$ divides $(X^m - 1)$, has degree $n = \varphi(m) = \deg(\Phi_m)$.

  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

- Examples: $\Phi_{2^{k+1}}(X) = 1 + X^{2^k}$, $\quad \Phi_9(X) = 1 + X^3 + X^6$.

✔ Ring-LWE (appropriately defined) is hard in any cyclotomic [LPR'10]

…assuming problems on ideal lattices are quantum-hard in the worst case.

The Form of Cyclotomic Polynomials

- For prime p,

$$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1} \quad \text{and} \quad \Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}).$$

The Form of Cyclotomic Polynomials

- For prime p,

  $$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1} \quad \text{and} \quad \Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}).$$

  Mod-$\Phi_{p^e}(X)$ reduction is efficient; small(ish) expansion factor.

The Form of Cyclotomic Polynomials

- For prime p,

  $$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1} \quad \text{and} \quad \Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}).$$

  Mod-$\Phi_{p^e}(X)$ reduction is efficient; small(ish) expansion factor.

  But still not enough: e.g., SIMD FHE likes $m = 3 \cdot 7 \cdot 19 \cdot 73$.

The Form of Cyclotomic Polynomials

- For prime p,

  $$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1} \quad \text{and} \quad \Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}).$$

  Mod-$\Phi_{p^e}(X)$ reduction is efficient; small(ish) expansion factor.

  But still not enough: e.g., SIMD FHE likes $m = 3 \cdot 7 \cdot 19 \cdot 73$.

- What about non-prime power m?

The Form of Cyclotomic Polynomials

- For prime p,

  $$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1} \quad \text{and} \quad \Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}).$$

  Mod-$\Phi_{p^e}(X)$ reduction is efficient; small(ish) expansion factor.

  But still not enough: e.g., SIMD FHE likes $m = 3 \cdot 7 \cdot 19 \cdot 73$.

- What about non-prime power m?
  - ✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$

The Form of Cyclotomic Polynomials

- For prime p,

  $$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1} \quad \text{and} \quad \Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}).$$

  Mod-$\Phi_{p^e}(X)$ reduction is efficient; small(ish) expansion factor.

  But still not enough: e.g., SIMD FHE likes $m = 3 \cdot 7 \cdot 19 \cdot 73$.

- What about non-prime power m?
  - ✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$
  - ✗✗ $\Phi_{105}(X)$: degree 48; 33 monomials with $\{-2, -1, 1\}$-coefficients

The Form of Cyclotomic Polynomials

- For prime p,

  $$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1} \quad \text{and} \quad \Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}).$$

  Mod-$\Phi_{p^e}(X)$ reduction is efficient; small(ish) expansion factor.

  But still not enough: e.g., SIMD FHE likes $m = 3 \cdot 7 \cdot 19 \cdot 73$.

- What about non-prime power m?
  - ✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$
  - ✗✗ $\Phi_{105}(X)$: degree 48; 33 monomials with $\{-2, -1, 1\}$-coefficients
  - ✗✗✗ $\Phi_{3 \cdot 7 \cdot 19 \cdot 73}(X)$: highly irregular; large coeffs

The Form of Cyclotomic Polynomials

- For prime p,

  $$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1} \quad \text{and} \quad \Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}).$$

  Mod-$\Phi_{p^e}(X)$ reduction is efficient; small(ish) expansion factor.

  But still not enough: e.g., SIMD FHE likes $m = 3 \cdot 7 \cdot 19 \cdot 73$.

- What about non-prime power m?

  ✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$

  ✗✗ $\Phi_{105}(X)$: degree 48; 33 monomials with $\{-2, -1, 1\}$-coefficients

  ✗✗✗ $\Phi_{3 \cdot 7 \cdot 19 \cdot 73}(X)$: highly irregular; large coeffs

Yuck!!!

✗ Irregular $\Phi_m(X)$ induces cumbersome, slower operations modulo $\Phi_m(X)$

✗ Large expansion factors — up to super-polynomial $n^{\omega(1)}$ [Erdős'46]

✗ Provable & concrete security also degrade with expansion factor: pay twice!

Our Contributions

A toolkit of simple, fast algorithms and tight error analyses for working with ring-LWE in arbitrary cyclotomics

Our Contributions

A toolkit of simple, fast algorithms and tight error analyses for working with ring-LWE in arbitrary cyclotomics

Fast Algorithms: ring operations $(+, \cdot)$; noise generation & decoding; conversions among the best representations for each task.
$\Longrightarrow$ Runtimes: $O(n)$ per prime divisor of m, or $O(n \log n)$.

Our Contributions

A toolkit of simple, fast algorithms and tight error analyses
for working with ring-LWE in arbitrary cyclotomics

Fast Algorithms: ring operations $(+, \cdot)$; noise generation & decoding; conversions among the best representations for each task.
$\implies$ Runtimes: $O(n)$ per prime divisor of m, or $O(n \log n)$.

Tight Analysis: same noise growth and worst-case hardness in *all cyclotomics*; optimal noise tolerance in decoding.
$\implies$ No dependence on the form of m.

Our Contributions

A toolkit of simple, fast algorithms and tight error analyses
for working with ring-LWE in arbitrary cyclotomics

Fast Algorithms: ring operations $(+, \cdot)$; noise generation & decoding;
conversions among the best representations for each task.
$\Longrightarrow$ Runtimes: $O(n)$ per prime divisor of m, or $O(n \log n)$.

Tight Analysis: same noise growth and worst-case hardness in
all cyclotomics; optimal noise tolerance in decoding.
$\Longrightarrow$ No dependence on the form of m.

Key Ideas

1. In algorithms, use tensorial representations of ring elements.
   - ✔ No reduction modulo $\Phi_m(X)$ — in fact, don't need $\Phi_m(X)$ at all!

Our Contributions

A toolkit of simple, fast algorithms and tight error analyses for working with ring-LWE in arbitrary cyclotomics

Fast Algorithms: ring operations $(+, \cdot)$; noise generation & decoding; conversions among the best representations for each task.
$\implies$ Runtimes: $O(n)$ per prime divisor of m, or $O(n \log n)$.

Tight Analysis: same noise growth and worst-case hardness in *all cyclotomics*; optimal noise tolerance in decoding.
$\implies$ No dependence on the form of m.

Key Ideas

1. In algorithms, use tensorial representations of ring elements.
   - ✔ No reduction modulo $\Phi_m(X)$ — in fact, don't need $\Phi_m(X)$ at all!
2. In analysis, use canonical embedding to define geometry.

Our Contributions

A toolkit of simple, fast algorithms and tight error analyses for working with ring-LWE in arbitrary cyclotomics

Fast Algorithms: ring operations $(+, \cdot)$; noise generation & decoding; conversions among the best representations for each task.
$\implies$ Runtimes: $O(n)$ per prime divisor of m, or $O(n \log n)$.

Tight Analysis: same noise growth and worst-case hardness in *all cyclotomics*; optimal noise tolerance in decoding.
$\implies$ No dependence on the form of m.

Key Ideas

1. In algorithms, use tensorial representations of ring elements.
   - ✔ No reduction modulo $\Phi_m(X)$ — in fact, don't need $\Phi_m(X)$ at all!
2. In analysis, use canonical embedding to define geometry.
3. Use decoding basis of dual ideal $R^\vee$ for noise generation & decoding.
   - ✔ Corresponds to the "true" definition of ring-LWE.

Tensorial Decomposition and the “Powerful” Basis

- Recall: $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ and $\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}})$.

Tensorial Decomposition and the "Powerful" Basis

- Recall: $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ and $\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}})$.

Ancient Theorem [Kummer, 1840s]

- Let $m = \prod_\ell m_\ell$ be the prime-power factorization of m.

  Then the mth cyclotomic ring $R = \mathbb{Z}[X]/\Phi_m(X)$ is isomorphic to the tensor product of all the m_ℓth cyclotomic rings:

  $$R \cong \mathbb{Z}[X_1, X_2, \ldots]/(\Phi_{m_1}(X_1), \Phi_{m_2}(X_2), \ldots).$$

  Isomorphism identifies X_ℓ with X^{m/m_ℓ}.

Tensorial Decomposition and the "Powerful" Basis

- Recall: $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ and $\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}})$.

Ancient Theorem [Kummer, 1840s]

- Let $m = \prod_\ell m_\ell$ be the prime-power factorization of m.

  Then the mth cyclotomic ring $R = \mathbb{Z}[X]/\Phi_m(X)$ is isomorphic to the tensor product of all the m_ℓth cyclotomic rings:

  $$R \cong \mathbb{Z}[X_1, X_2, \ldots]/(\Phi_{m_1}(X_1), \Phi_{m_2}(X_2), \ldots).$$

  Isomorphism identifies X_ℓ with X^{m/m_ℓ}.

The Powerful Basis

- It's the natural $\mathbb{Z}$-basis $\{X_1^{j_1} X_2^{j_2} \cdots\} = \bigotimes_\ell \{X_\ell^{j_\ell}\}, \ 0 \leq j_\ell < \varphi(m_\ell)$.

Tensorial Decomposition and the "Powerful" Basis

- Recall: $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ and $\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}})$.

Ancient Theorem [Kummer, 1840s]

- Let $m = \prod_\ell m_\ell$ be the prime-power factorization of m.

  Then the mth cyclotomic ring $R = \mathbb{Z}[X]/\Phi_m(X)$ is isomorphic to the tensor product of all the m_ℓth cyclotomic rings:

  $$R \cong \mathbb{Z}[X_1, X_2, \ldots]/(\Phi_{m_1}(X_1), \Phi_{m_2}(X_2), \ldots).$$

  Isomorphism identifies X_ℓ with X^{m/m_ℓ}.

The Powerful Basis

- It's the natural $\mathbb{Z}$-basis $\{X_1^{j_1} X_2^{j_2} \cdots\} = \bigotimes_\ell \{X_\ell^{j_\ell}\}, \; 0 \le j_\ell < \varphi(m_\ell)$.
- It is not the "power" basis $\{1, X, X^2, \ldots, X^{\varphi(m)-1}\}$ of $\mathbb{Z}[X]/\Phi_m(X)$.

  E.g., for $m = 15$ it's $\{X^j\}$ for $j \in \{0, 3, 5, 6, 8, 9, 11, 14\}$.

If You Remember Only One Thing From This Talk. . .

Tensorial decomposition with the powerful basis is algebraically, computationally, and geometrically preferable to $\mathbb{Z}[X]/\Phi_m(X)$ with the power basis.

If You Remember Only One Thing From This Talk. . .

Tensorial decomposition with the powerful basis is algebraically, computationally, and geometrically preferable to $\mathbb{Z}[X]/\Phi_m(X)$ with the power basis.

Algebra: Exposes fine-grained structure of the ring and its relationships with other cyclotomic rings.

If You Remember Only One Thing From This Talk. . .

Tensorial decomposition with the powerful basis is algebraically, computationally, and geometrically preferable to $\mathbb{Z}[X]/\Phi_m(X)$ with the power basis.

Algebra: Exposes fine-grained structure of the ring and its relationships with other cyclotomic rings.

E.g.: has applications in "ring-switching" [GHPS'12] and new bootstrapping [AP'13] algorithms for FHE.

If You Remember Only One Thing From This Talk...

Tensorial decomposition with the powerful basis is algebraically, computationally, and geometrically preferable to $\mathbb{Z}[X]/\Phi_m(X)$ with the power basis.

Algebra: Exposes fine-grained structure of the ring and its relationships with other cyclotomic rings.

E.g.: has applications in "ring-switching" [GHPS'12] and new bootstrapping [AP'13] algorithms for FHE.

Algorithms: Efficiently reduces all operations to the prime-power case, by dealing with each X_ℓ independently.

If You Remember Only One Thing From This Talk...

Tensorial decomposition with the powerful basis is algebraically, computationally, and geometrically preferable to $\mathbb{Z}[X]/\Phi_m(X)$ with the power basis.

Algebra: Exposes fine-grained structure of the ring and its relationships with other cyclotomic rings.

E.g.: has applications in "ring-switching" [GHPS'12] and new bootstrapping [AP'13] algorithms for FHE.

Algorithms: Efficiently reduces all operations to the prime-power case, by dealing with each X_ℓ independently.

E.g.: simple, fast conversions to/from "evaluation (CRT) representation," via sequence of prime-power FFTs.

If You Remember Only One Thing From This Talk...

Tensorial decomposition with the powerful basis is algebraically, computationally, and geometrically preferable to $\mathbb{Z}[X]/\Phi_m(X)$ with the power basis.

Algebra: Exposes fine-grained structure of the ring and its relationships with other cyclotomic rings.

E.g.: has applications in "ring-switching" [GHPS'12] and new bootstrapping [AP'13] algorithms for FHE.

Algorithms: Efficiently reduces all operations to the prime-power case, by dealing with each X_ℓ independently.

E.g.: simple, fast conversions to/from "evaluation (CRT) representation," via sequence of prime-power FFTs.

Geometry: Norms, singular values, Gram-Schmidt orthogonalization, dual basis, etc. all behave well under tensoring.

If You Remember Only One Thing From This Talk...

Tensorial decomposition with the powerful basis is algebraically, computationally, and geometrically preferable to $\mathbb{Z}[X]/\Phi_m(X)$ with the power basis.

Algebra: Exposes fine-grained structure of the ring and its relationships with other cyclotomic rings.

E.g.: has applications in "ring-switching" [GHPS'12] and new bootstrapping [AP'13] algorithms for FHE.

Algorithms: Efficiently reduces all operations to the prime-power case, by dealing with each X_ℓ independently.

E.g.: simple, fast conversions to/from "evaluation (CRT) representation," via sequence of prime-power FFTs.

Geometry: Norms, singular values, Gram-Schmidt orthogonalization, dual basis, etc. all behave well under tensoring.

E.g.: powerful basis is better-conditioned than power basis.

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \ldots, X^{p-2}\}$.

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \ldots, X^{p-2}\}$.
- Geometrically, associating elements with their coeff vectors is strange:

$$
\begin{aligned}
X^j &\longleftrightarrow (0,\ldots,0,1,0,\ldots,0), \quad (j = 0,\ldots,p-2) \\
X^{p-1} &\longleftrightarrow (-1,-1,\ldots,-1)
\end{aligned}
$$

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \ldots, X^{p-2}\}$.
- Geometrically, associating elements with their coeff vectors is strange:

$$\begin{aligned} X^j &\longleftrightarrow (0,\ldots,0,1,0,\ldots,0), \quad (j = 0,\ldots,p-2) \\ X^{p-1} &\longleftrightarrow (-1,-1,\ldots,-1) \end{aligned}$$

We want a basis-independent geometry.

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \ldots, X^{p-2}\}$.
- Geometrically, associating elements with their coeff vectors is strange:

$$\begin{aligned} X^j &\longleftrightarrow (0, \ldots, 0, 1, 0, \ldots, 0), \quad (j = 0, \ldots, p-2) \\ X^{p-1} &\longleftrightarrow (-1, -1, \ldots, -1) \end{aligned}$$

  We want a basis-independent geometry.
- The canonical embedding $\sigma\colon R \to \mathbb{C}^{p-1}$ evaluates at all roots of Φ_p:

$$\sigma(e(X)) = \big(e(\omega_p^1),\, e(\omega_p^2),\, \ldots,\, e(\omega_p^{p-1})\big)$$

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \ldots, X^{p-2}\}$.
- Geometrically, associating elements with their coeff vectors is strange:

$$\begin{aligned} X^j &\longleftrightarrow (0,\ldots,0,1,0,\ldots,0), \quad (j = 0,\ldots,p-2) \\ X^{p-1} &\longleftrightarrow (-1,-1,\ldots,-1) \end{aligned}$$

  We want a basis-independent geometry.
- The canonical embedding $\sigma \colon R \to \mathbb{C}^{p-1}$ evaluates at all roots of Φ_p:

$$\sigma(e(X)) = \big(e(\omega_p^1),\, e(\omega_p^2),\, \ldots,\, e(\omega_p^{p-1})\big)$$

  Define all geometric quantities using σ: e.g., $\|e\|_2 := \|\sigma(e)\|_2$.

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \ldots, X^{p-2}\}$.
- Geometrically, associating elements with their coeff vectors is strange:

$$\begin{aligned} X^j &\longleftrightarrow (0, \ldots, 0, 1, 0, \ldots, 0), \quad (j = 0, \ldots, p-2) \\ X^{p-1} &\longleftrightarrow (-1, -1, \ldots, -1) \end{aligned}$$

  We want a basis-independent geometry.

- The canonical embedding $\sigma \colon R \to \mathbb{C}^{p-1}$ evaluates at all roots of Φ_p:

$$\sigma(e(X)) = \big(e(\omega_p^1),\, e(\omega_p^2),\, \ldots,\, e(\omega_p^{p-1})\big)$$

  Define all geometric quantities using σ: e.g., $\|e\|_2 := \|\sigma(e)\|_2$.

Nice Features of the Canonical Embedding

✔ $\|X^j\|_\infty = 1$ and $\|X^j\|_2 = \sqrt{p-1}$ for all j.

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \ldots, X^{p-2}\}$.
- Geometrically, associating elements with their coeff vectors is strange:

$$\begin{aligned} X^j &\longleftrightarrow (0,\ldots,0,1,0,\ldots,0), \quad (j = 0,\ldots,p-2) \\ X^{p-1} &\longleftrightarrow (-1,-1,\ldots,-1) \end{aligned}$$

  We want a basis-independent geometry.
- The canonical embedding $\sigma \colon R \to \mathbb{C}^{p-1}$ evaluates at all roots of Φ_p:

$$\sigma(e(X)) = \big(e(\omega_p^1),\, e(\omega_p^2),\, \ldots,\, e(\omega_p^{p-1})\big)$$

  Define all geometric quantities using σ: e.g., $\|e\|_2 := \|\sigma(e)\|_2$.

Nice Features of the Canonical Embedding

- ✔ $\|X^j\|_\infty = 1$ and $\|X^j\|_2 = \sqrt{p-1}$ for all j.
- ✔ Under σ, both $+$ and $\cdot$ are coordinate-wise: $\sigma(a \cdot b) = \sigma(a) \odot \sigma(b)$.

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \dots, X^{p-2}\}$.
- Geometrically, associating elements with their coeff vectors is strange:

$$\begin{array}{rcl} X^j & \longleftrightarrow & (0,\dots,0,1,0,\dots,0), \quad (j = 0,\dots,p-2) \\ X^{p-1} & \longleftrightarrow & (-1,-1,\dots,-1) \end{array}$$

  We want a basis-independent geometry.
- The canonical embedding $\sigma \colon R \to \mathbb{C}^{p-1}$ evaluates at all roots of Φ_p:

$$\sigma(e(X)) = \big(e(\omega_p^1),\, e(\omega_p^2),\, \dots,\, e(\omega_p^{p-1})\big)$$

  Define all geometric quantities using σ: e.g., $\|e\|_2 := \|\sigma(e)\|_2$.

Nice Features of the Canonical Embedding

- ✔ $\|X^j\|_\infty = 1$ and $\|X^j\|_2 = \sqrt{p-1}$ for all j.
- ✔ Under σ, both $+$ and $\cdot$ are coordinate-wise: $\sigma(a \cdot b) = \sigma(a) \odot \sigma(b)$.

  Makes expansion very easy to analyze: e.g., $\|a \cdot b\|_2 \leq \|a\|_\infty \cdot \|b\|_2$.

Geometry of the Ring

- Consider $R = \mathbb{Z}[X]/\Phi_p(X)$ with power basis $\{1, X, X^2, \ldots, X^{p-2}\}$.
- Geometrically, associating elements with their coeff vectors is strange:

$$\begin{aligned} X^j &\longleftrightarrow (0,\ldots,0,1,0,\ldots,0), \quad (j = 0,\ldots,p-2) \\ X^{p-1} &\longleftrightarrow (-1,-1,\ldots,-1) \end{aligned}$$

  We want a basis-independent geometry.
- The canonical embedding $\sigma \colon R \to \mathbb{C}^{p-1}$ evaluates at all roots of Φ_p:

$$\sigma(e(X)) = \big(e(\omega_p^1),\, e(\omega_p^2),\, \ldots,\, e(\omega_p^{p-1})\big)$$

  Define all geometric quantities using σ: e.g., $\|e\|_2 := \|\sigma(e)\|_2$.

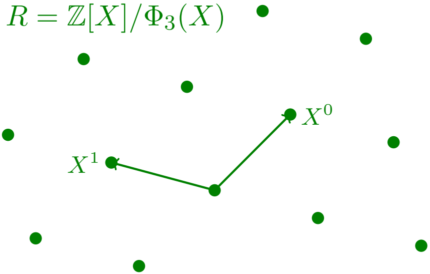
Nice Features of the Canonical Embedding

- ✔ $\|X^j\|_\infty = 1$ and $\|X^j\|_2 = \sqrt{p-1}$ for all j.
- ✔ Under σ, both $+$ and $\cdot$ are coordinate-wise: $\sigma(a \cdot b) = \sigma(a) \odot \sigma(b)$.

  Makes expansion very easy to analyze: e.g., $\|a \cdot b\|_2 \le \|a\|_\infty \cdot \|b\|_2$.
- ✔ Ring-LWE is provably hard with (spherical) Gaussian noise under σ.

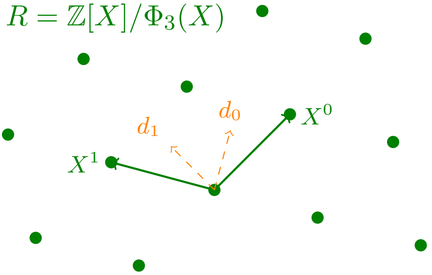
Dual Ideal $R^\vee$ and Decoding Basis

- $R = \mathbb{Z}[X]/\Phi_p(X)$ under embedding σ is a lattice in $\mathbb{C}^{p-1}$.



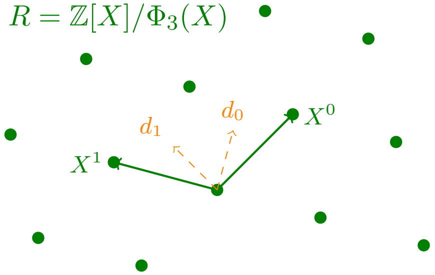
Dual Ideal $R^\vee$ and Decoding Basis

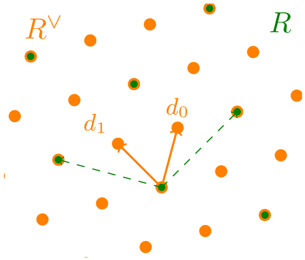
- $R = \mathbb{Z}[X]/\Phi_p(X)$ under embedding σ is a lattice in $\mathbb{C}^{p-1}$.
- Its dual $R^\vee$ has $\mathbb{Z}$-basis $\{d_j\}$, given by $\langle \sigma(d_j)\,,\, \sigma(X^{j'}) \rangle = \delta_{j,j'}$.
  We call $\{d_j\}$ the decoding basis. (It also has a tensor form...)



Dual Ideal $R^\vee$ and Decoding Basis

- $R = \mathbb{Z}[X]/\Phi_p(X)$ under embedding σ is a lattice in $\mathbb{C}^{p-1}$.
- Its dual $R^\vee$ has $\mathbb{Z}$-basis $\{d_j\}$, given by $\langle \sigma(d_j)\,,\, \sigma(X^{j'}) \rangle = \delta_{j,j'}$.
  We call $\{d_j\}$ the decoding basis. (It also has a tensor form...)
- $R^\vee$ is a (fractional) ideal, and $pR^\vee \subseteq R \subseteq R^\vee$, with $pR^\vee \approx R$.





Dual Ideal $R^\vee$ and Decoding Basis

- In "true" ring-LWE, errors are Gaussian over $R^\vee$.

Dual Ideal $R^\vee$ and Decoding Basis

- In "true" ring-LWE, errors are Gaussian over $R^\vee$.
- In decryption, we need to recover $e \in R^\vee$, given $\bar{e} = e \bmod qR^\vee$.

Dual Ideal $R^\vee$ and Decoding Basis

- In "true" ring-LWE, errors are Gaussian over $R^\vee$.
- In decryption, we need to recover $e \in R^\vee$, given $\bar{e} = e \bmod qR^\vee$.
  How: represent $\bar{e}$ in decoding basis with $\mathbb{Z}_q$-coeffs, then "lift" to $\mathbb{Z}$.

Dual Ideal $R^\vee$ and Decoding Basis

- In "true" ring-LWE, errors are Gaussian over $R^\vee$.
- In decryption, we need to recover $e \in R^\vee$, given $\bar{e} = e \bmod qR^\vee$.
  How: represent $\bar{e}$ in decoding basis with $\mathbb{Z}_q$-coeffs, then "lift" to $\mathbb{Z}$.

Key Facts

- For short $e \in R^\vee$ (under σ), coeffs in decoding basis $\{d_j\}$ are small:

$$e = \sum\nolimits_j e_j d_j \quad (e_j \in \mathbb{Z}) \implies |e_j| = \left|\langle \sigma(e) \,,\, \sigma(X^j) \rangle\right| \leq \|e\| \cdot \sqrt{n}.$$

Dual Ideal $R^\vee$ and Decoding Basis

- In "true" ring-LWE, errors are Gaussian over $R^\vee$.
- In decryption, we need to recover $e \in R^\vee$, given $\bar{e} = e \bmod qR^\vee$.
  How: represent $\bar{e}$ in decoding basis with $\mathbb{Z}_q$-coeffs, then "lift" to $\mathbb{Z}$.

Key Facts

- For short $e \in R^\vee$ (under σ), coeffs in decoding basis $\{d_j\}$ are small:

$$e = \sum\nolimits_j e_j d_j \quad (e_j \in \mathbb{Z}) \implies |e_j| = \left|\left\langle \sigma(e)\, ,\, \sigma(X^j) \right\rangle\right| \leq \|e\| \cdot \sqrt{n}.$$

- Moreover, $|e_j|$ are optimally small given "density" of $R^\vee$,
  because powerful basis $\{X^j\}$ is optimally short given density of R.

Dual Ideal $R^\vee$ and Decoding Basis

- In "true" ring-LWE, errors are Gaussian over $R^\vee$.
- In decryption, we need to recover $e \in R^\vee$, given $\bar{e} = e \bmod qR^\vee$.
  How: represent $\bar{e}$ in decoding basis with $\mathbb{Z}_q$-coeffs, then "lift" to $\mathbb{Z}$.

Key Facts

- For short $e \in R^\vee$ (under σ), coeffs in decoding basis $\{d_j\}$ are small:

$$e = \sum\nolimits_j e_j d_j \quad (e_j \in \mathbb{Z}) \implies |e_j| = \left|\langle \sigma(e)\,, \sigma(X^j) \rangle\right| \leq \|e\| \cdot \sqrt{n}.$$

- Moreover, $|e_j|$ are optimally small given "density" of $R^\vee$, because powerful basis $\{X^j\}$ is optimally short given density of R.
- By contrast, such optimal decoding is not possible for R/qR, because $R^\vee$ lacks optimally short elements for its density.

Dual Ideal $R^\vee$ and Decoding Basis

- In "true" ring-LWE, errors are Gaussian over $R^\vee$.
- In decryption, we need to recover $e \in R^\vee$, given $\bar{e} = e \bmod qR^\vee$.
  How: represent $\bar{e}$ in decoding basis with $\mathbb{Z}_q$-coeffs, then "lift" to $\mathbb{Z}$.

Key Facts

- For short $e \in R^\vee$ (under σ), coeffs in decoding basis $\{d_j\}$ are small:

$$e = \sum_j e_j d_j \quad (e_j \in \mathbb{Z}) \implies |e_j| = \left|\langle \sigma(e)\,,\, \sigma(X^j)\rangle\right| \leq \|e\| \cdot \sqrt{n}.$$

- Moreover, $|e_j|$ are optimally small given "density" of $R^\vee$, because powerful basis $\{X^j\}$ is optimally short given density of R.
- By contrast, such optimal decoding is not possible for R/qR, because $R^\vee$ lacks optimally short elements for its density.
- **Bottom line:** using $R^\vee$ is actually beneficial in applications!

  (And "advanced" applications benefit even more from its algebraic properties.)

Concluding Thoughts

- The "right" choices of

mathematical objects	and	representations
(canonical embedding, $R^\vee$)		(tensor bases)

come together perfectly, yielding:

Concluding Thoughts

- The "right" choices of

mathematical objects	and	representations
(canonical embedding, $R^\vee$)		(tensor bases)

come together perfectly, yielding:

provable hardness,

Concluding Thoughts

- The "right" choices of

mathematical objects	and	representations
(canonical embedding, $R^\vee$)		(tensor bases)

come together perfectly, yielding:

provable hardness, fast algorithms,

Concluding Thoughts

- The "right" choices of

mathematical objects	and	representations
(canonical embedding, $R^\vee$)		(tensor bases)

  come together perfectly, yielding:

  provable hardness, fast algorithms, tight analysis — no compromises.

Concluding Thoughts

- The "right" choices of

mathematical objects	and	representations
(canonical embedding, $R^\vee$)		(tensor bases)

  come together perfectly, yielding:

  provable hardness, fast algorithms, tight analysis — no compromises.

- Much more in the paper: "regularity" lemma, (homomorphic) encryption schemes, implementation advice, ...

Concluding Thoughts

- The "right" choices of

mathematical objects (canonical embedding, $R^\vee$)	and	representations (tensor bases)

  come together perfectly, yielding:

  provable hardness, fast algorithms, tight analysis — no compromises.

- Much more in the paper: "regularity" lemma, (homomorphic) encryption schemes, implementation advice, ...

- Implementations coming soon!

Concluding Thoughts

- The "right" choices of

mathematical objects	and	representations
(canonical embedding, $R^\vee$)		(tensor bases)

  come together perfectly, yielding:

  provable hardness, fast algorithms, tight analysis — no compromises.

- Much more in the paper: "regularity" lemma, (homomorphic) encryption schemes, implementation advice, ...

- Implementations coming soon!

Thanks!

Full version: ePrint #2013/293
http://eprint.iacr.org/2013/293