Ring Switching and Bootstrapping FHE

Chris Peikert

School of Computer Science
Georgia Tech

Oberwolfach Crypto Workshop
29 July 2014

Agenda

1. A homomorphic encryption tool: ring switching

2. An application: (practical!) bootstrapping FHE in $\tilde{O}(\lambda)$ time

Bibliography:

GHPS'12 C. Gentry, S. Halevi, C. Peikert, N. Smart, "Ring Switching in BGV-Style Homomorphic Encryption," SCN'12 / JCS'13.

AP'13 J. Alperin-Sheriff, C. Peikert, "Practical Bootstrapping in Quasilinear Time," CRYPTO'13.

Part 1:

Ring Switching

Notation

- Let $R^{(\ell)}/\cdots/R^{(2)}/R^{(1)}/\mathbb{Z}$ be a tower of cyclotomic ring extensions.

Notation

- Let $R^{(\ell)}/\cdots/R^{(2)}/R^{(1)}/\mathbb{Z}$ be a tower of cyclotomic ring extensions.

- Let's go slower.

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).
  - ★ $\mathcal{O}_1 = \mathbb{Z}[1] = \mathbb{Z}$. $\mathbb{Z}$-basis $\{1\}$.

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).
  - ⋆ $\mathcal{O}_1 = \mathbb{Z}[1] = \mathbb{Z}$. $\mathbb{Z}$-basis $\{1\}$.
  - ⋆ $\mathcal{O}_2 = \mathbb{Z}[-1] = \mathbb{Z}$.

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).
  - ⋆ $\mathcal{O}_1 = \mathbb{Z}[1] = \mathbb{Z}$. $\mathbb{Z}$-basis $\{1\}$.
  - ⋆ $\mathcal{O}_2 = \mathbb{Z}[-1] = \mathbb{Z}$.
  - ⋆ $\mathcal{O}_4 \cong \mathbb{Z}[i] \cong \mathbb{Z}[X]/(1 + X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_4\}$.

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).
  - ⋆ $\mathcal{O}_1 = \mathbb{Z}[1] = \mathbb{Z}$. $\mathbb{Z}$-basis $\{1\}$.
  - ⋆ $\mathcal{O}_2 = \mathbb{Z}[-1] = \mathbb{Z}$.
  - ⋆ $\mathcal{O}_4 \cong \mathbb{Z}[i] \cong \mathbb{Z}[X]/(1 + X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_4\}$.
  - ⋆ $\mathcal{O}_3 = \mathbb{Z}[\zeta_3] \cong \mathbb{Z}[X]/(1 + X + X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_3\}$.

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).
  - ⋆ $\mathcal{O}_1 = \mathbb{Z}[1] = \mathbb{Z}$. $\mathbb{Z}$-basis $\{1\}$.
  - ⋆ $\mathcal{O}_2 = \mathbb{Z}[-1] = \mathbb{Z}$.
  - ⋆ $\mathcal{O}_4 \cong \mathbb{Z}[i] \cong \mathbb{Z}[X]/(1 + X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_4\}$.
  - ⋆ $\mathcal{O}_3 = \mathbb{Z}[\zeta_3] \cong \mathbb{Z}[X]/(1 + X + X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_3\}$.
  - ⋆ $\mathcal{O}_5 = \mathbb{Z}[\zeta_5] \cong \mathbb{Z}[X]/(1 + X + X^2 + X^3 + X^4)$, $\mathbb{Z}$-basis $\{1, \zeta, \zeta^2, \zeta^3\}$.

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).
  - ★ $\mathcal{O}_1 = \mathbb{Z}[1] = \mathbb{Z}$. $\mathbb{Z}$-basis $\{1\}$.
  - ★ $\mathcal{O}_2 = \mathbb{Z}[-1] = \mathbb{Z}$.
  - ★ $\mathcal{O}_4 \cong \mathbb{Z}[i] \cong \mathbb{Z}[X]/(1+X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_4\}$.
  - ★ $\mathcal{O}_3 = \mathbb{Z}[\zeta_3] \cong \mathbb{Z}[X]/(1+X+X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_3\}$.
  - ★ $\mathcal{O}_5 = \mathbb{Z}[\zeta_5] \cong \mathbb{Z}[X]/(1+X+X^2+X^3+X^4)$, $\mathbb{Z}$-basis $\{1, \zeta, \zeta^2, \zeta^3\}$.

Facts

1. For prime p, $\mathcal{O}_p \cong \mathbb{Z}[X]/(\underbrace{1+X+\cdots+X^{p-1}}_{\Phi_p(X)})$; $\{1, \zeta, \ldots, \zeta^{p-2}\}$.

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).
  - ⋆ $\mathcal{O}_1 = \mathbb{Z}[1] = \mathbb{Z}$. $\mathbb{Z}$-basis $\{1\}$.
  - ⋆ $\mathcal{O}_2 = \mathbb{Z}[-1] = \mathbb{Z}$.
  - ⋆ $\mathcal{O}_4 \cong \mathbb{Z}[i] \cong \mathbb{Z}[X]/(1+X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_4\}$.
  - ⋆ $\mathcal{O}_3 = \mathbb{Z}[\zeta_3] \cong \mathbb{Z}[X]/(1+X+X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_3\}$.
  - ⋆ $\mathcal{O}_5 = \mathbb{Z}[\zeta_5] \cong \mathbb{Z}[X]/(1+X+X^2+X^3+X^4)$, $\mathbb{Z}$-basis $\{1, \zeta, \zeta^2, \zeta^3\}$.

Facts

1. For prime p, $\mathcal{O}_p \cong \mathbb{Z}[X]/(\underbrace{1+X+\cdots+X^{p-1}}_{\Phi_p(X)})$; $\{1, \zeta, \ldots, \zeta^{p-2}\}$.
2. For prime power p^e, $\mathcal{O}_{p^e} \cong \mathbb{Z}[X]/(\Phi_p(X^{p^{e-1}}))$; $\{1, \zeta, \ldots, \zeta^{\varphi(p^e)-1}\}$.

Cyclotomic Rings

- Define $\mathcal{O}_k = \mathbb{Z}[\zeta_k]$, where ζ_k has order k (so $\zeta_k^k = 1$).
  - ⋆ $\mathcal{O}_1 = \mathbb{Z}[1] = \mathbb{Z}$. $\mathbb{Z}$-basis $\{1\}$.
  - ⋆ $\mathcal{O}_2 = \mathbb{Z}[-1] = \mathbb{Z}$.
  - ⋆ $\mathcal{O}_4 \cong \mathbb{Z}[i] \cong \mathbb{Z}[X]/(1 + X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_4\}$.
  - ⋆ $\mathcal{O}_3 = \mathbb{Z}[\zeta_3] \cong \mathbb{Z}[X]/(1 + X + X^2)$, $\mathbb{Z}$-basis $\{1, \zeta_3\}$.
  - ⋆ $\mathcal{O}_5 = \mathbb{Z}[\zeta_5] \cong \mathbb{Z}[X]/(1 + X + X^2 + X^3 + X^4)$, $\mathbb{Z}$-basis $\{1, \zeta, \zeta^2, \zeta^3\}$.

Facts

1. For prime p, $\mathcal{O}_p \cong \mathbb{Z}[X]/(\underbrace{1 + X + \cdots + X^{p-1}}_{\Phi_p(X)})$; $\{1, \zeta, \ldots, \zeta^{p-2}\}$.
2. For prime power p^e, $\mathcal{O}_{p^e} \cong \mathbb{Z}[X]/(\Phi_p(X^{p^{e-1}}))$; $\{1, \zeta, \ldots, \zeta^{\varphi(p^e)-1}\}$.
3. For distinct primes $p_1, p_2, \ldots$,
$$\mathcal{O}_{p_1^{e_1} p_2^{e_2} \cdots} \cong \mathbb{Z}[X_1, X_2, \ldots]/(\Phi_{p_1}(X_1^{p_1^{e_1-1}}), \Phi_{p_2}(X_2^{p_2^{e_2-1}}), \ldots).$$

Cyclotomic Extensions

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via
$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$

Cyclotomic Extensions

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via
$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$
- Example: tower of quadratic extensions $\mathcal{O}_k/\mathcal{O}_{k/2}/\cdots/\mathcal{O}_4/\mathbb{Z}$:

Cyclotomic Extensions

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via

$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$

- Example: tower of quadratic extensions $\mathcal{O}_k/\mathcal{O}_{k/2}/\cdots/\mathcal{O}_4/\mathbb{Z}$:

$$\begin{array}{ccc}
\zeta_k^2 = \zeta_{k/2} & \mathcal{O}_k = \mathcal{O}_{k/2}[\zeta_k] & \mathcal{O}_{k/2}\text{-basis } B'_k = \{1, \zeta_k\} \\
 & \vdots & \\
\zeta_8^2 = \zeta_4 & \mathcal{O}_8 = \mathcal{O}_4[\zeta_8] & \mathcal{O}_4\text{-basis } B'_8 = \{1, \zeta_8\} \\
 & | & \\
\zeta_4^2 = \zeta_2 & \mathcal{O}_4 = \mathcal{O}_2[\zeta_4] & \mathcal{O}_2\text{-basis } B'_4 = \{1, \zeta_4\} \\
 & | & \\
\zeta_2^2 = 1 & \mathcal{O}_2 = \mathbb{Z}[\zeta_2] = \mathbb{Z} & \mathbb{Z}\text{-basis } B'_2 = \{1\}
\end{array}$$

Cyclotomic Extensions

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via
$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$
- Example: tower of quadratic extensions $\mathcal{O}_k/\mathcal{O}_{k/2}/\cdots/\mathcal{O}_4/\mathbb{Z}$:
$$\begin{array}{ccc}
\zeta_k^2 = \zeta_{k/2} & \mathcal{O}_k = \mathcal{O}_{k/2}[\zeta_k] & \mathcal{O}_{k/2}\text{-basis } B'_k = \{1, \zeta_k\} \\
& \vdots & \\
\zeta_8^2 = \zeta_4 & \mathcal{O}_8 = \mathcal{O}_4[\zeta_8] & \mathcal{O}_4\text{-basis } B'_8 = \{1, \zeta_8\} \\
& | & \\
\zeta_4^2 = \zeta_2 & \mathcal{O}_4 = \mathcal{O}_2[\zeta_4] & \mathcal{O}_2\text{-basis } B'_4 = \{1, \zeta_4\} \\
& | & \\
\zeta_2^2 = 1 & \mathcal{O}_2 = \mathbb{Z}[\zeta_2] = \mathbb{Z} & \mathbb{Z}\text{-basis } B'_2 = \{1\}
\end{array}$$
- "Product" $\mathbb{Z}$-basis of $\mathcal{O}_k$:
$$B_k := B'_k \cdot B_{k/2} = B'_k \cdot B'_{k/2} \cdots B'_2$$

Cyclotomic Extensions

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via
$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$
- Example: tower of quadratic extensions $\mathcal{O}_k/\mathcal{O}_{k/2}/\cdots/\mathcal{O}_4/\mathbb{Z}$:

$$\begin{array}{ccc}
\zeta_k^2 = \zeta_{k/2} & \mathcal{O}_k = \mathcal{O}_{k/2}[\zeta_k] & \mathcal{O}_{k/2}\text{-basis } B'_k = \{1, \zeta_k\} \\
 & \vdots & \\
\zeta_8^2 = \zeta_4 & \mathcal{O}_8 = \mathcal{O}_4[\zeta_8] & \mathcal{O}_4\text{-basis } B'_8 = \{1, \zeta_8\} \\
 & | & \\
\zeta_4^2 = \zeta_2 & \mathcal{O}_4 = \mathcal{O}_2[\zeta_4] & \mathcal{O}_2\text{-basis } B'_4 = \{1, \zeta_4\} \\
 & | & \\
\zeta_2^2 = 1 & \mathcal{O}_2 = \mathbb{Z}[\zeta_2] = \mathbb{Z} & \mathbb{Z}\text{-basis } B'_2 = \{1\}
\end{array}$$

- "Product" $\mathbb{Z}$-basis of $\mathcal{O}_k$:
$$B_k := B'_k \cdot B_{k/2} = B'_k \cdot B'_{k/2} \cdots B'_2 = \{1, \zeta, \zeta^2, \ldots, \zeta^{k/2-1}\}.$$

Cyclotomic Extensions: Trace

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via

$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$

Cyclotomic Extensions: Trace

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via
$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$
- The trace $\mathrm{Tr} = \mathrm{Tr}_{R'/R} \colon R' \to R$ is a "universal" R-linear function:

Cyclotomic Extensions: Trace

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via
$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$
- The trace $\mathrm{Tr} = \mathrm{Tr}_{R'/R} \colon R' \to R$ is a "universal" R-linear function:
  1. R-linear: for any $r_j \in R$ and $r'_j \in R'$,
  $$\mathrm{Tr}(r_1 \cdot r'_1 + r_2 \cdot r'_2) = r_1 \cdot \mathrm{Tr}(r'_1) + r_2 \cdot \mathrm{Tr}(r'_2).$$

Cyclotomic Extensions: Trace

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via

$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$

- The trace $\mathrm{Tr} = \mathrm{Tr}_{R'/R} \colon R' \to R$ is a "universal" R-linear function:

  1. R-linear: for any $r_j \in R$ and $r'_j \in R'$,

  $$\mathrm{Tr}(r_1 \cdot r'_1 + r_2 \cdot r'_2) = r_1 \cdot \mathrm{Tr}(r'_1) + r_2 \cdot \mathrm{Tr}(r'_2).$$

  2. Universal: <u>any</u> R-linear function $L \colon R' \to R$ can be written as

  $$L(x) = \mathrm{Tr}(r'_L \cdot x)$$

  for some r'_L depending only on L.

Cyclotomic Extensions: Trace

- If $k \mid k'$, can view $R = \mathbb{Z}[\zeta_k]$ as a subring of $R' = \mathbb{Z}[\zeta_{k'}]$, via
$$\zeta_k \mapsto \zeta_{k'}^{(k'/k)}. \qquad \text{(still has order } k\text{)}$$
- The trace $\mathrm{Tr} = \mathrm{Tr}_{R'/R} \colon R' \to R$ is a "universal" R-linear function:
  1. R-linear: for any $r_j \in R$ and $r'_j \in R'$,
  $$\mathrm{Tr}(r_1 \cdot r'_1 + r_2 \cdot r'_2) = r_1 \cdot \mathrm{Tr}(r'_1) + r_2 \cdot \mathrm{Tr}(r'_2).$$
  2. Universal: <u>any</u> R-linear function $L \colon R' \to R$ can be written as
  $$L(x) = \mathrm{Tr}(r'_L \cdot x)$$
  for some r'_L depending only on L.
- Any R-linear function is uniquely defined by its values on an R-basis $\{b'_j\}$ of R', and vice versa:
$$\mathrm{Tr}\left(\sum_j r_j \cdot b'_j\right) = \sum_j r_j \cdot \mathrm{Tr}(b'_j).$$

Homomorphic Encryption over Rings [LPR'10,BV'11,BGV'12]

- Let $R := \mathcal{O}_k$, e.g., $\mathbb{Z}[X]/(1 + X^{k/2})$ for k a power of 2.

Homomorphic Encryption over Rings [LPR'10,BV'11,BGV'12]

- Let $R := \mathcal{O}_k$, e.g., $\mathbb{Z}[X]/(1 + X^{k/2})$ for k a power of 2.

  Denote $R_q := R/qR = \mathbb{Z}_q[X]/(1 + X^{k/2})$ for any integer q.

Homomorphic Encryption over Rings [LPR'10,BV'11,BGV'12]

- Let $R := \mathcal{O}_k$, e.g., $\mathbb{Z}[X]/(1 + X^{k/2})$ for k a power of 2.

  Denote $R_q := R/qR = \mathbb{Z}_q[X]/(1 + X^{k/2})$ for any integer q.

- Plaintext ring is R_2, ciphertext ring is R_q for some $q \gg 2$.

Homomorphic Encryption over Rings [LPR'10,BV'11,BGV'12]

- Let $R := \mathcal{O}_k$, e.g., $\mathbb{Z}[X]/(1 + X^{k/2})$ for k a power of 2.

  Denote $R_q := R/qR = \mathbb{Z}_q[X]/(1 + X^{k/2})$ for any integer q.

- Plaintext ring is R_2, ciphertext ring is R_q for some $q \gg 2$.

- Encryption of $\mu \in R_2$ under $s \in R$ is some $c = (c_0, c_1) \in R_q^2$ satisfying

$$c_0 + c_1 \cdot s \approx \frac{q}{2}\mu \pmod{qR}.$$

  - ⋆ Thanks to this relation we can do $+$ and $\times$ homomorphically.
  - ⋆ Semantic security follows from hardness of ring-LWE over R
    $\Leftarrow$ (quantum) worst-case hardness of approx-SVP on ideal lattices in R.

Homomorphic Encryption over Rings [LPR'10,BV'11,BGV'12]

- Let $R := \mathcal{O}_k$, e.g., $\mathbb{Z}[X]/(1+X^{k/2})$ for k a power of 2.

  Denote $R_q := R/qR = \mathbb{Z}_q[X]/(1+X^{k/2})$ for any integer q.

- Plaintext ring is R_2, ciphertext ring is R_q for some $q \gg 2$.

- Encryption of $\mu \in R_2$ under $s \in R$ is some $c = (c_0, c_1) \in R_q^2$ satisfying

$$c_0 + c_1 \cdot s \approx \tfrac{q}{2}\mu \pmod{qR}.$$

  - ⋆ Thanks to this relation we can do $+$ and $\times$ homomorphically.
  - ⋆ Semantic security follows from hardness of ring-LWE over R
    $\Leftarrow$ (quantum) worst-case hardness of approx-SVP on ideal lattices in R.

- "Unpacked" plaintext $\mu \in \mathbb{Z}_2 \subseteq R_2$ (just a constant polynomial).

Homomorphic Encryption over Rings [LPR'10,BV'11,BGV'12]

- Let $R := \mathcal{O}_k$, e.g., $\mathbb{Z}[X]/(1+X^{k/2})$ for k a power of 2.
  Denote $R_q := R/qR = \mathbb{Z}_q[X]/(1+X^{k/2})$ for any integer q.
- Plaintext ring is R_2, ciphertext ring is R_q for some $q \gg 2$.
- Encryption of $\mu \in R_2$ under $s \in R$ is some $c = (c_0, c_1) \in R_q^2$ satisfying

$$c_0 + c_1 \cdot s \approx \tfrac{q}{2}\mu \pmod{qR}.$$

  - ⋆ Thanks to this relation we can do $+$ and $\times$ homomorphically.
  - ⋆ Semantic security follows from hardness of ring-LWE over R
    $\Leftarrow$ (quantum) worst-case hardness of approx-SVP on ideal lattices in R.
- "Unpacked" plaintext $\mu \in \mathbb{Z}_2 \subseteq R_2$ (just a constant polynomial).
  "Packed" plaintext uses more of R_2, e.g., multiple "slots" [SV'11].

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate
  - any R-linear $L\colon R'_2 \to R_2$ (i.e., map $\mu' \in R'_2$ to $\mu = L(\mu') \in R_2$)

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate
  - any R-linear $L\colon R'_2 \to R_2$ (i.e., map $\mu' \in R'_2$ to $\mu = L(\mu') \in R_2$)
  - by mapping the ciphertext c' over R' to some c over R,

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate
  - any R-linear $L \colon R'_2 \to R_2$ (i.e., map $\mu' \in R'_2$ to $\mu = L(\mu') \in R_2$)
  - by mapping the ciphertext c' over R' to some c over R,
  - assuming hardness of R-LWE.

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate
  - any R-linear $L \colon R'_2 \to R_2$ (i.e., map $\mu' \in R'_2$ to $\mu = L(\mu') \in R_2$)
  - by mapping the ciphertext c' over R' to some c over R,
  - assuming hardness of R-LWE.

So What?

- "Fresh" ciphertexts need small noise $\Rightarrow$ large ring degree for security.
- Noise increases as we do homomorphic operations, so we can securely switch to smaller ring dimension, yielding smaller ciphertexts and faster operations.
- Also important for minimizing complexity of decryption for bootstrapping (cf. "dimension reduction" [BV'11]).
- We'll see another cool application later...

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate
  - any R-linear $L \colon R'_2 \to R_2$ (i.e., map $\mu' \in R'_2$ to $\mu = L(\mu') \in R_2$)
  - by mapping the ciphertext c' over R' to some c over R,
  - assuming hardness of R-LWE.

- Proof: Given $c' = (c'_0, c'_1)$, let $c_i = \mathrm{Tr}(r'_L \cdot c'_i)$.

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate
  - ⋆ any R-linear $L\colon R'_2 \to R_2$ (i.e., map $\mu' \in R'_2$ to $\mu = L(\mu') \in R_2$)
  - ⋆ by mapping the ciphertext c' over R' to some c over R,
  - ⋆ assuming hardness of R-LWE.

- Proof: Given $c' = (c'_0, c'_1)$, let $c_i = \mathrm{Tr}(r'_L \cdot c'_i)$.

$$c'_0 + s' \cdot c'_1 \approx \tfrac{q}{2} \cdot \mu' \pmod{qR'}$$

$$\Longrightarrow \mathrm{Tr}(r'_L \cdot c'_0) + \mathrm{Tr}(s' \cdot r'_L \cdot c'_1) \approx \tfrac{q}{2} \cdot \mathrm{Tr}(r'_L \cdot \mu') \pmod{qR}$$

$$?? \Longrightarrow c_0 + s' \cdot c_1 \approx \tfrac{q}{2} \cdot \mu \pmod{qR}.$$

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate
  - any R-linear $L\colon R'_2 \to R_2$ (i.e., map $\mu' \in R'_2$ to $\mu = L(\mu') \in R_2$)
  - by mapping the ciphertext c' over R' to some c over R,
  - assuming hardness of R-LWE.

- Proof: Given $c' = (c'_0, c'_1)$, let $c_i = \mathrm{Tr}(r'_L \cdot c'_i)$.

$$c'_0 + s \cdot c'_1 \approx \tfrac{q}{2} \cdot \mu' \pmod{qR'}$$

$$\implies \mathrm{Tr}(r'_L \cdot c'_0) + \mathrm{Tr}(s \cdot r'_L \cdot c'_1) \approx \tfrac{q}{2} \cdot \mathrm{Tr}(r'_L \cdot \mu') \pmod{qR}$$

$$\implies c_0 + s \cdot c_1 \approx \tfrac{q}{2} \cdot \mu \pmod{qR}.$$

- First "key-switch" from $s' \in R'$ to $s \in R$.

Ring Switching

Theorem [GHPS'12]

- For any cyclotomic rings R'/R, we can homomorphically evaluate
  - any R-linear $L \colon R'_2 \to R_2$ (i.e., map $\mu' \in R'_2$ to $\mu = L(\mu') \in R_2$)
  - by mapping the ciphertext c' over R' to some c over R,
  - assuming hardness of R-LWE.

- Proof: Given $c' = (c'_0, c'_1)$, let $c_i = \mathrm{Tr}(r'_L \cdot c'_i)$.

$$c'_0 + s \cdot c'_1 \approx \tfrac{q}{2} \cdot \mu' \pmod{qR'}$$

$$\implies \mathrm{Tr}(r'_L \cdot c'_0) + \mathrm{Tr}(s \cdot r'_L \cdot c'_1) \approx \tfrac{q}{2} \cdot \mathrm{Tr}(r'_L \cdot \mu') \pmod{qR}$$

$$\implies c_0 + s \cdot c_1 \approx \tfrac{q}{2} \cdot \mu \pmod{qR}.$$

- First "key-switch" from $s' \in R'$ to $s \in R$.

  Theorem: R'-LWE with secret in R is as hard as R-LWE.

Part 2:

Bootstrapping

Fully Homomorphic Encryption [RAD'78,Gen'09]

- FHE lets you do this:

$$\boxed{\mu} \longrightarrow \boxed{\mathsf{Eval}\Big(f\ ,\ \boxed{\mu}\Big)} \longrightarrow \boxed{f(\mu)}$$

where $|f(\mu)|$ and decryption time don't depend on $|f|$.

A cryptographic "holy grail."

Fully Homomorphic Encryption [RAD'78,Gen'09]

- FHE lets you do this:

$$\boxed{\mu} \longrightarrow \boxed{\mathsf{Eval}\left(f\ ,\ \boxed{\mu}\right)} \longrightarrow \boxed{f(\mu)}$$

  where $|f(\mu)|$ and decryption time don't depend on $|f|$.

  A cryptographic "holy grail."

- Naturally occurring schemes are "somewhat homomorphic" (SHE): they can only evaluate functions of an *a priori* bounded depth.

$$\boxed{\mu} \to \boxed{\mathsf{Eval}\left(f, \boxed{\mu}\right)} \to \boxed{f(\mu)} \to \boxed{\mathsf{Eval}\left(g, \boxed{f(\mu)}\right)} \to \boxed{g(f(\mu))}$$

Bootstrapping: SHE $\to$ FHE [Gen'09]

- Homomorphically evaluates the SHE decryption function to "refresh" a ciphertext $\boxed{\mu}$, allowing further homomorphic operations.

$$\boxed{sk} \longrightarrow \boxed{\mathsf{Eval}\Big(\ f(\cdot) = \mathsf{Dec}(\ \cdot\ ,\ \boxed{\mu})\Big)} \longrightarrow \boxed{\mu}$$

Bootstrapping: SHE $\rightarrow$ FHE [Gen'09]

- Homomorphically evaluates the SHE decryption function to "refresh" a ciphertext $\boxed{\mu}$, allowing further homomorphic operations.

$$\boxed{sk} \longrightarrow \boxed{\mathsf{Eval}\Big(f(\cdot) = \mathsf{Dec}(\,\cdot\,,\ \boxed{\mu})\Big)} \longrightarrow \boxed{\mu}$$

  - ⋆ The only known way of obtaining unbounded FHE.
  - ⋆ Goal: Efficiency! Minimize depth d and size s of decryption "circuit."
  - ⋆ Most efficient SHEs [BGV'12] can evaluate in time $\tilde{O}(d \cdot s \cdot \lambda)$.

Bootstrapping: SHE $\to$ FHE [Gen'09]

- Homomorphically evaluates the SHE decryption function to "refresh" a ciphertext $\boxed{\mu}$, allowing further homomorphic operations.

$$\boxed{sk} \longrightarrow \boxed{\mathsf{Eval}\Big(\ f(\cdot) = \mathsf{Dec}(\ \cdot\ ,\ \boxed{\mu})\Big)} \longrightarrow \boxed{\mu}$$

  - ★ The only known way of obtaining unbounded FHE.
  - ★ Goal: Efficiency! Minimize depth d and size s of decryption "circuit."
  - ★ Most efficient SHEs [BGV'12] can evaluate in time $\tilde{O}(d \cdot s \cdot \lambda)$.

- Intensive study, many techniques [G'09,GH'11a,GH'11b,GHS'12b,AP'13,BV'14,AP'14], but still very inefficient – the main bottleneck in FHE, by far.

Bootstrapping: SHE → FHE [Gen'09]

- Homomorphically evaluates the SHE decryption function to "refresh" a ciphertext $\boxed{\mu}$, allowing further homomorphic operations.

$$\boxed{sk} \longrightarrow \boxed{\mathsf{Eval}\Big(\, f(\cdot) = \mathsf{Dec}(\,\cdot\,,\ \boxed{\mu})\Big)} \longrightarrow \boxed{\mu}$$

  - ★ The only known way of obtaining unbounded FHE.
  - ★ Goal: Efficiency! Minimize depth d and size s of decryption "circuit."
  - ★ Most efficient SHEs [BGV'12] can evaluate in time $\tilde{O}(d \cdot s \cdot \lambda)$.

- Intensive study, many techniques [G'09,GH'11a,GH'11b,GHS'12b,AP'13,BV'14,AP'14], but still very inefficient – the main bottleneck in FHE, by far.

- Prior asymptotically efficient methods on "packed" ciphertexts [GHS'12a,GHS'12b] are very complex, and are practically worse than asymptotically slower methods.

Milestones in Bootstrapping

[Gen'09]: $\tilde{O}(\lambda^4)$ runtime

Milestones in Bootstrapping

[Gen'09]: $\tilde{O}(\lambda^4)$ runtime

[BGV'12]: $\tilde{O}(\lambda^2)$ runtime, or $\tilde{O}(\lambda)$ amortized over λ ciphertexts

Milestones in Bootstrapping

[Gen'09]: $\tilde{O}(\lambda^4)$ runtime

[BGV'12]: $\tilde{O}(\lambda^2)$ runtime, or $\tilde{O}(\lambda)$ amortized over λ ciphertexts

Mainly via improved SHE homomorphic capacity.

Amortized method requires "exotic" rings, emulating $\mathbb{Z}_2$ arithmetic in $\mathbb{Z}_p$.

Milestones in Bootstrapping

[Gen'09]: $\tilde{O}(\lambda^4)$ runtime

[BGV'12]: $\tilde{O}(\lambda^2)$ runtime, or $\tilde{O}(\lambda)$ amortized over λ ciphertexts

Mainly via improved SHE homomorphic capacity.

Amortized method requires "exotic" rings, emulating $\mathbb{Z}_2$ arithmetic in $\mathbb{Z}_p$.

[GHS'12b]: $\tilde{O}(\lambda)$ runtime, for "packed" plaintexts. Declare victory?

Milestones in Bootstrapping

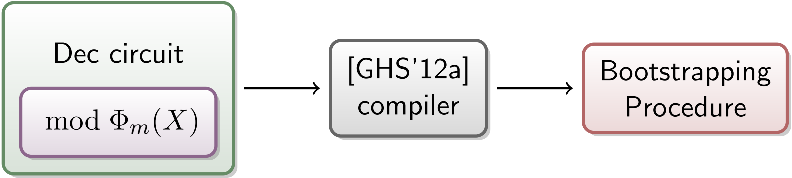
[Gen'09]: $\tilde{O}(\lambda^4)$ runtime

[BGV'12]: $\tilde{O}(\lambda^2)$ runtime, or $\tilde{O}(\lambda)$ amortized over λ ciphertexts

Mainly via improved SHE homomorphic capacity.

Amortized method requires "exotic" rings, emulating $\mathbb{Z}_2$ arithmetic in $\mathbb{Z}_p$.

[GHS'12b]: $\tilde{O}(\lambda)$ runtime, for "packed" plaintexts. Declare victory?



Milestones in Bootstrapping

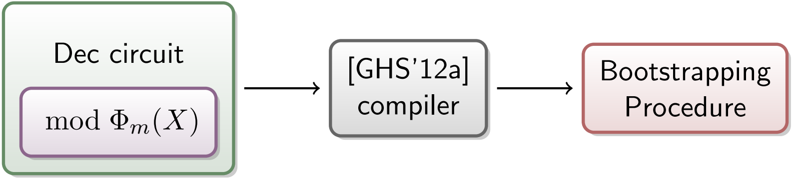
[Gen'09]: $\tilde{O}(\lambda^4)$ runtime

[BGV'12]: $\tilde{O}(\lambda^2)$ runtime, or $\tilde{O}(\lambda)$ amortized over λ ciphertexts

Mainly via improved SHE homomorphic capacity.

Amortized method requires "exotic" rings, emulating $\mathbb{Z}_2$ arithmetic in $\mathbb{Z}_p$.

[GHS'12b]: $\tilde{O}(\lambda)$ runtime, for "packed" plaintexts. Declare victory?



✗ Log-depth mod-$\Phi_m(X)$ circuit is complex, w/large hidden constants.

Milestones in Bootstrapping

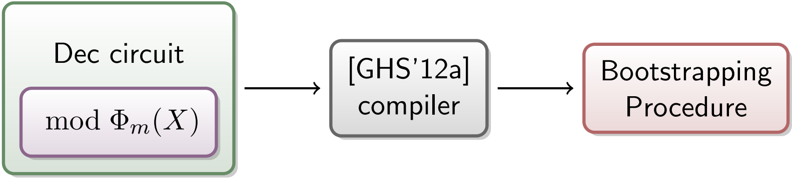
[Gen'09]: $\tilde{O}(\lambda^4)$ runtime

[BGV'12]: $\tilde{O}(\lambda^2)$ runtime, or $\tilde{O}(\lambda)$ amortized over λ ciphertexts

Mainly via improved SHE homomorphic capacity.

Amortized method requires "exotic" rings, emulating $\mathbb{Z}_2$ arithmetic in $\mathbb{Z}_p$.

[GHS'12b]: $\tilde{O}(\lambda)$ runtime, for "packed" plaintexts. Declare victory?



✗ Log-depth mod-$\Phi_m(X)$ circuit is complex, w/large hidden constants.

✗✗ [GHS'12a] compiler is very complex, w/large polylog overhead.

Our Results

Practical bootstrapping algorithms with quasi-linear $\tilde{O}(\lambda)$ runtimes:

Our Results

Practical bootstrapping algorithms with quasi-linear $\tilde{O}(\lambda)$ runtimes:

1. For "unpacked" (single-bit) plaintexts:
   - ✔ Extremely simple!
   - ✔ Uses only power-of-2 cyclotomic rings (fast, easy to implement).

Our Results

Practical bootstrapping algorithms with quasi-linear $\tilde{O}(\lambda)$ runtimes:

1. For "unpacked" (single-bit) plaintexts:
   - ✔ Extremely simple!
   - ✔ Uses only power-of-2 cyclotomic rings (fast, easy to implement).
   - ⋆ Cf. [BGV'12]: $\tilde{O}(\lambda)$ amortized across λ ciphertexts, exotic rings.

Our Results

Practical bootstrapping algorithms with quasi-linear $\tilde{O}(\lambda)$ runtimes:

1. For "unpacked" (single-bit) plaintexts:
   - ✔ Extremely simple!
   - ✔ Uses only power-of-2 cyclotomic rings (fast, easy to implement).
   - ⋆ Cf. [BGV'12]: $\tilde{O}(\lambda)$ amortized across λ ciphertexts, exotic rings.

2. For "packed" (many-bit) plaintexts:

Our Results

Practical bootstrapping algorithms with quasi-linear $\tilde{O}(\lambda)$ runtimes:

1. For "unpacked" (single-bit) plaintexts:
   - ✔ Extremely simple!
   - ✔ Uses only power-of-2 cyclotomic rings (fast, easy to implement).
   - ⋆ Cf. [BGV'12]: $\tilde{O}(\lambda)$ amortized across λ ciphertexts, exotic rings.

2. For "packed" (many-bit) plaintexts:
   - ⋆ Based on an enhancement of ring-switching to non-subrings.

Our Results

Practical bootstrapping algorithms with quasi-linear $\tilde{O}(\lambda)$ runtimes:

1. For "unpacked" (single-bit) plaintexts:
   - ✔ Extremely simple!
   - ✔ Uses only power-of-2 cyclotomic rings (fast, easy to implement).
   - ⋆ Cf. [BGV'12]: $\tilde{O}(\lambda)$ amortized across λ ciphertexts, exotic rings.

2. For "packed" (many-bit) plaintexts:
   - ⋆ Based on an enhancement of ring-switching to non-subrings.
   - ✔ Seems quite practical, avoids both main inefficiencies of [GHS'12b]: no homomorphic reduction modulo $\Phi_m(X)$, no generic compilation.

Our Results

Practical bootstrapping algorithms with quasi-linear $\tilde{O}(\lambda)$ runtimes:

1. For "unpacked" (single-bit) plaintexts:
   - ✔ Extremely simple!
   - ✔ Uses only power-of-2 cyclotomic rings (fast, easy to implement).
   - ⋆ Cf. [BGV'12]: $\tilde{O}(\lambda)$ amortized across λ ciphertexts, exotic rings.

2. For "packed" (many-bit) plaintexts:
   - ⋆ Based on an enhancement of ring-switching to non-subrings.
   - ✔ Seems quite practical, avoids both main inefficiencies of [GHS'12b]: no homomorphic reduction modulo $\Phi_m(X)$, no generic compilation.
   - ✔ Special purpose, completely algebraic description – no "circuits."

Our Results

Practical bootstrapping algorithms with quasi-linear $\tilde{O}(\lambda)$ runtimes:

1. For "unpacked" (single-bit) plaintexts:
   - ✔ Extremely simple!
   - ✔ Uses only power-of-2 cyclotomic rings (fast, easy to implement).
   - ⋆ Cf. [BGV'12]: $\tilde{O}(\lambda)$ amortized across λ ciphertexts, exotic rings.

2. For "packed" (many-bit) plaintexts:
   - ⋆ Based on an enhancement of ring-switching to non-subrings.
   - ✔ Seems quite practical, avoids both main inefficiencies of [GHS'12b]: no homomorphic reduction modulo $\Phi_m(X)$, no generic compilation.
   - ✔ Special purpose, completely algebraic description – no "circuits."
   - ✔ Decouples the algebraic structure of SHE plaintext ring from the ring structure needed for bootstrapping.

Bootstrapping Packed Ciphertexts: Overview

1. Prepare: view c as a "noiseless" encryption of plaintext

$$v = c_0 + c_1 \cdot s = \sum_j v_j \cdot b_j \in R_q. \qquad (\mathbb{Z}\text{-basis } \{b_j\} \text{ of } R)$$

Recall: $v \approx \frac{q}{2} \cdot \mu$, so $\mu = \lfloor v \rceil := \sum_j \lfloor v_j \rceil \cdot b_j \in R_2$.

Bootstrapping Packed Ciphertexts: Overview

1. Prepare: view c as a "noiseless" encryption of plaintext

$$v = c_0 + c_1 \cdot s = \sum_j v_j \cdot b_j \in R_q. \qquad (\mathbb{Z}\text{-basis } \{b_j\} \text{ of } R)$$

Recall: $v \approx \frac{q}{2} \cdot \mu$, so $\mu = \lfloor v \rceil := \sum_j \lfloor v_j \rceil \cdot b_j \in R_2$.

2. Homomorphically map $\mathbb{Z}_q$-coeffs v_j to "$\mathbb{Z}_q$-slots" of certain ring S_q:

$$\sum v_j \cdot b_j \in R_q \quad \longmapsto \quad \sum v_j \cdot c_j \in S_q.$$

(Change of basis, analogous to homomorphic DFT.)

Bootstrapping Packed Ciphertexts: Overview

1. Prepare: view c as a "noiseless" encryption of plaintext

$$v = c_0 + c_1 \cdot s = \sum_j v_j \cdot b_j \in R_q. \qquad (\mathbb{Z}\text{-basis } \{b_j\} \text{ of } R)$$

Recall: $v \approx \frac{q}{2} \cdot \mu$, so $\mu = \lfloor v \rceil := \sum_j \lfloor v_j \rceil \cdot b_j \in R_2$.

2. Homomorphically map $\mathbb{Z}_q$-coeffs v_j to "$\mathbb{Z}_q$-slots" of certain ring S_q:

$$\sum v_j \cdot b_j \in R_q \quad \longmapsto \quad \sum v_j \cdot c_j \in S_q.$$

(Change of basis, analogous to homomorphic DFT.)

3. Batch-round: homom'ly apply $\lfloor \cdot \rceil$ on all $\mathbb{Z}_q$-slots at once [SV'11]:

$$\sum v_j \cdot c_j \in S_q \quad \longmapsto \quad \sum \lfloor v_j \rceil \cdot c_j \in S_2.$$

Bootstrapping Packed Ciphertexts: Overview

1. Prepare: view c as a "noiseless" encryption of plaintext

$$v = c_0 + c_1 \cdot s = \sum_j v_j \cdot b_j \in R_q. \qquad (\mathbb{Z}\text{-basis } \{b_j\} \text{ of } R)$$

   Recall: $v \approx \frac{q}{2} \cdot \mu$, so $\mu = \lfloor v \rceil := \sum_j \lfloor v_j \rceil \cdot b_j \in R_2$.

2. Homomorphically map $\mathbb{Z}_q$-coeffs v_j to "$\mathbb{Z}_q$-slots" of certain ring S_q:

$$\sum v_j \cdot b_j \in R_q \quad \longmapsto \quad \sum v_j \cdot c_j \in S_q.$$

   (Change of basis, analogous to homomorphic DFT.)

3. Batch-round: homom'ly apply $\lfloor \cdot \rceil$ on all $\mathbb{Z}_q$-slots at once [SV'11]:

$$\sum v_j \cdot c_j \in S_q \quad \longmapsto \quad \sum \lfloor v_j \rceil \cdot c_j \in S_2.$$

4. Homomorphically reverse-map $\mathbb{Z}_2$-slots back to B-coeffs:

$$\sum \lfloor v_j \rceil \cdot c_j \in S_2 \quad \longmapsto \quad \sum \lfloor v_j \rceil \cdot b_j = \mu \in R_2.$$

   (Akin to homomorphic DFT^{-1}.)

Algebra: Slots and CRT Sets

- Let $1 = \ell_0 | \ell_1 | \ell_2 | \cdots$ (all odd), and $S^{(i)} = \mathcal{O}_{\ell_i} = \mathbb{Z}[\zeta_{\ell_i}]$.

  So we have a cyclotomic tower $S^{(i)} / S^{(i-1)} / \cdots / \mathbb{Z}$.

Algebra: Slots and CRT Sets

- Let $1 = \ell_0 | \ell_1 | \ell_2 | \cdots$ (all odd), and $S^{(i)} = \mathcal{O}_{\ell_i} = \mathbb{Z}[\zeta_{\ell_i}]$.

  So we have a cyclotomic tower $S^{(i)}/S^{(i-1)}/\cdots/\mathbb{Z}$.

- In $S = S^{(i)}$, 2 factors into distinct prime ideals, like so:

$$
\begin{tikzcd}
S^{(2)} = \mathcal{O}_{91} \arrow[d, dash] \\
S^{(1)} = \mathcal{O}_{7} \arrow[d, dash] \\
\mathbb{Z} = \mathcal{O}_{1}
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
\mathfrak{p}_{1,1} \arrow[dr, dash] & \mathfrak{p}_{1,2} \arrow[d, dash] & \mathfrak{p}_{1,3} \arrow[dl, dash] & & \mathfrak{p}_{2,1} \arrow[dr, dash] & \mathfrak{p}_{2,2} \arrow[d, dash] & \mathfrak{p}_{2,3} \arrow[dl, dash] \\
& \mathfrak{p}_1 \arrow[drr, dash] & & & & \mathfrak{p}_2 \arrow[dll, dash] & \\
& & & 2 & & &
\end{tikzcd}
$$

Algebra: Slots and CRT Sets

- Let $1 = \ell_0 | \ell_1 | \ell_2 | \cdots$ (all odd), and $S^{(i)} = \mathcal{O}_{\ell_i} = \mathbb{Z}[\zeta_{\ell_i}]$.

  So we have a cyclotomic tower $S^{(i)} / S^{(i-1)} / \cdots / \mathbb{Z}$.

- In $S = S^{(i)}$, 2 factors into distinct prime ideals, like so:

$$
\begin{tikzcd}
S^{(2)} = \mathcal{O}_{91} \arrow[d, dash] \\
S^{(1)} = \mathcal{O}_{7} \arrow[d, dash] \\
\mathbb{Z} = \mathcal{O}_{1}
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
\mathfrak{p}_{1,1} \arrow[dr, dash] & \mathfrak{p}_{1,2} \arrow[d, dash] & \mathfrak{p}_{1,3} \arrow[dl, dash] & & \mathfrak{p}_{2,1} \arrow[dr, dash] & \mathfrak{p}_{2,2} \arrow[d, dash] & \mathfrak{p}_{2,3} \arrow[dl, dash] \\
& \mathfrak{p}_{1} \arrow[drr, dash] & & & & \mathfrak{p}_{2} \arrow[dll, dash] & \\
& & & 2 & & &
\end{tikzcd}
$$

- By Chinese Rem Thm, $S_2 \cong \bigoplus_j (S/\mathfrak{p}_j)$ via natural homomorphism.

Algebra: Slots and CRT Sets

- Let $1 = \ell_0 | \ell_1 | \ell_2 | \cdots$ (all odd), and $S^{(i)} = \mathcal{O}_{\ell_i} = \mathbb{Z}[\zeta_{\ell_i}]$.

  So we have a cyclotomic tower $S^{(i)} / S^{(i-1)} / \cdots / \mathbb{Z}$.
- In $S = S^{(i)}$, 2 factors into distinct prime ideals, like so:

$$\begin{array}{c} S^{(2)} = \mathcal{O}_{91} \\ | \\ S^{(1)} = \mathcal{O}_7 \\ | \\ \mathbb{Z} = \mathcal{O}_1 \end{array} \qquad \begin{tikzcd}[arrows=dash] \mathfrak{p}_{1,1} \arrow[dr] & \mathfrak{p}_{1,2} \arrow[d] & \mathfrak{p}_{1,3} \arrow[dl] & & \mathfrak{p}_{2,1} \arrow[dr] & \mathfrak{p}_{2,2} \arrow[d] & \mathfrak{p}_{2,3} \arrow[dl] \\ & \mathfrak{p}_1 \arrow[drr] & & & & \mathfrak{p}_2 \arrow[dll] & \\ & & & 2 & & & \end{tikzcd}$$

- By Chinese Rem Thm, $S_2 \cong \bigoplus_j (S/\mathfrak{p}_j)$ via natural homomorphism.

  "CRT set:" $C = \{c_j\} \subset S$ s.t. $c_j = 1 \pmod{\mathfrak{p}_j}$, $= 0 \pmod{\mathfrak{p}_{\neq j}}$.

  Map $v_j \in \mathbb{Z}_2 \mapsto v_j \cdot c_j \in S_2$ embeds $\mathbb{Z}_2$ into jth "slot" of S_2.

Algebra: Slots and CRT Sets

- Let $1 = \ell_0 | \ell_1 | \ell_2 | \cdots$ (all odd), and $S^{(i)} = \mathcal{O}_{\ell_i} = \mathbb{Z}[\zeta_{\ell_i}]$.
  So we have a cyclotomic tower $S^{(i)} / S^{(i-1)} / \cdots / \mathbb{Z}$.
- In $S = S^{(i)}$, 2 factors into distinct prime ideals, like so:

$$\begin{array}{c} S^{(2)} = \mathcal{O}_{91} \\ | \\ S^{(1)} = \mathcal{O}_7 \\ | \\ \mathbb{Z} = \mathcal{O}_1 \end{array}$$

$$\begin{tikzcd}[column sep=small]
\mathfrak{p}_{1,1} \arrow[dr, dash] & \mathfrak{p}_{1,2} \arrow[d, dash] & \mathfrak{p}_{1,3} \arrow[dl, dash] & & \mathfrak{p}_{2,1} \arrow[dr, dash] & \mathfrak{p}_{2,2} \arrow[d, dash] & \mathfrak{p}_{2,3} \arrow[dl, dash] \\
& \mathfrak{p}_1 \arrow[drr, dash] & & & & \mathfrak{p}_2 \arrow[dll, dash] & \\
& & & 2 & & &
\end{tikzcd}$$

- By Chinese Rem Thm, $S_2 \cong \bigoplus_j (S/\mathfrak{p}_j)$ via natural homomorphism.
  "CRT set:" $C = \{c_j\} \subset S$ s.t. $c_j = 1 \pmod{\mathfrak{p}_j}$, $= 0 \pmod{\mathfrak{p}_{\neq j}}$.
  Map $v_j \in \mathbb{Z}_2 \mapsto v_j \cdot c_j \in S_2$ embeds $\mathbb{Z}_2$ into jth "slot" of S_2.
- Can factor $C_i = C'_i \cdot C_{i-1}$: let $c'_k = 1 \pmod{\mathfrak{p}_{\star,k}}$, $= 0 \pmod{\mathfrak{p}_{\star,\neq k}}$.

Algebra: Slots and CRT Sets

- Let $1 = \ell_0 | \ell_1 | \ell_2 | \cdots$ (all odd), and $S^{(i)} = \mathcal{O}_{\ell_i} = \mathbb{Z}[\zeta_{\ell_i}]$.
  So we have a cyclotomic tower $S^{(i)} / S^{(i-1)} / \cdots / \mathbb{Z}$.
- In $S = S^{(i)}$, 2 factors into distinct prime ideals, like so:

$$\begin{tikzcd}[row sep=small]
S^{(2)} = \mathcal{O}_{91} \arrow[d, dash] \\
S^{(1)} = \mathcal{O}_7 \arrow[d, dash] \\
\mathbb{Z} = \mathcal{O}_1
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
\mathfrak{p}_{1,1} \arrow[dr, dash] & \mathfrak{p}_{1,2} \arrow[d, dash] & \mathfrak{p}_{1,3} \arrow[dl, dash] & & \mathfrak{p}_{2,1} \arrow[dr, dash] & \mathfrak{p}_{2,2} \arrow[d, dash] & \mathfrak{p}_{2,3} \arrow[dl, dash] \\
& \mathfrak{p}_1 \arrow[drr, dash] & & & & \mathfrak{p}_2 \arrow[dll, dash] & \\
& & & 2 & & &
\end{tikzcd}$$

- By Chinese Rem Thm, $S_2 \cong \bigoplus_j (S/\mathfrak{p}_j)$ via natural homomorphism.
  "CRT set:" $C = \{c_j\} \subset S$ s.t. $c_j = 1 \pmod{\mathfrak{p}_j}$, $= 0 \pmod{\mathfrak{p}_{\neq j}}$.
  Map $v_j \in \mathbb{Z}_2 \mapsto v_j \cdot c_j \in S_2$ embeds $\mathbb{Z}_2$ into jth "slot" of S_2.
- Can factor $C_i = C'_i \cdot C_{i-1}$: let $c'_k = 1 \pmod{\mathfrak{p}_{\star,k}}$, $= 0 \pmod{\mathfrak{p}_{\star,\neq k}}$.
- Similarly for $S_q \cong \bigoplus_j (S/\mathfrak{p}_j^{\lg q})$.

Mapping Coeffs to Slots: Overview

- Choose S so that S_q has $\geq n = \deg(R/\mathbb{Z})$ $\mathbb{Z}_q$-slots, via:

$$(v_j) \in \mathbb{Z}_q^n \longmapsto \sum v_j \cdot c_j \bmod q$$

for an appropriate CRT set $C = \{c_j\} \subset S$ of size n.

Mapping Coeffs to Slots: Overview

- Choose S so that S_q has $\geq n = \deg(R/\mathbb{Z})$ $\mathbb{Z}_q$-slots, via:

$$(v_j) \in \mathbb{Z}_q^n \longmapsto \sum v_j \cdot c_j \bmod q$$

for an appropriate CRT set $C = \{c_j\} \subset S$ of size n.

- Our goal: homomorphically map $\sum v_j \cdot b_j \in R_q \longmapsto \sum v_j \cdot c_j \in S_q$.

Mapping Coeffs to Slots: Overview

- Choose S so that S_q has $\geq n = \deg(R/\mathbb{Z})$ $\mathbb{Z}_q$-slots, via:

$$(v_j) \in \mathbb{Z}_q^n \longmapsto \sum v_j \cdot c_j \bmod q$$

for an appropriate CRT set $C = \{c_j\} \subset S$ of size n.

- Our goal: homomorphically map $\sum v_j \cdot b_j \in R_q \longmapsto \sum v_j \cdot c_j \in S_q$.

Equivalently, evaluate the $\mathbb{Z}$-linear map $L \colon R \to S$ defined by

$$L(b_j) = c_j.$$

Mapping Coeffs to Slots: Overview

- Choose S so that S_q has $\geq n = \deg(R/\mathbb{Z})$ $\mathbb{Z}_q$-slots, via:

$$(v_j) \in \mathbb{Z}_q^n \longmapsto \sum v_j \cdot c_j \bmod q$$

  for an appropriate CRT set $C = \{c_j\} \subset S$ of size n.

- Our goal: homomorphically map $\sum v_j \cdot b_j \in R_q \longmapsto \sum v_j \cdot c_j \in S_q$.

  Equivalently, evaluate the $\mathbb{Z}$-linear map $L\colon R \to S$ defined by

$$L(b_j) = c_j.$$

- Ring-switching lets us evaluate any R'-linear map $L\colon R \to R'$

Mapping Coeffs to Slots: Overview

- Choose S so that S_q has $\geq n = \deg(R/\mathbb{Z})$ $\mathbb{Z}_q$-slots, via:

$$(v_j) \in \mathbb{Z}_q^n \longmapsto \sum v_j \cdot c_j \bmod q$$

  for an appropriate CRT set $C = \{c_j\} \subset S$ of size n.

- Our goal: homomorphically map $\sum v_j \cdot b_j \in R_q \longmapsto \sum v_j \cdot c_j \in S_q$.

  Equivalently, evaluate the $\mathbb{Z}$-linear map $L \colon R \to S$ defined by

$$L(b_j) = c_j.$$

- Ring-switching lets us evaluate any R'-linear map $L \colon R \to R'$

  ...but only for a subring $R' \subseteq R$.

Mapping Coeffs to Slots: Overview

- Choose S so that S_q has $\geq n = \deg(R/\mathbb{Z})$ $\mathbb{Z}_q$-slots, via:

$$(v_j) \in \mathbb{Z}_q^n \longmapsto \sum v_j \cdot c_j \bmod q$$

for an appropriate CRT set $C = \{c_j\} \subset S$ of size n.

- Our goal: homomorphically map $\sum v_j \cdot b_j \in R_q \longmapsto \sum v_j \cdot c_j \in S_q$.

Equivalently, evaluate the $\mathbb{Z}$-linear map $L \colon R \to S$ defined by

$$L(b_j) = c_j.$$

- Ring-switching lets us evaluate any R'-linear map $L \colon R \to R'$

. . . but only for a subring $R' \subseteq R$.

Goal for Remainder of Talk

- Extend ring-switching to (efficiently) handle $\mathbb{Z}$-linear maps $L \colon R \to S$.

Algebra: Combining Cyclotomic Rings

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$. Let $d = \gcd(k, \ell)$ and $m = \mathrm{lcm}(k, \ell)$.

Algebra: Combining Cyclotomic Rings

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$. Let $d = \gcd(k, \ell)$ and $m = \operatorname{lcm}(k, \ell)$.

$$\begin{tikzcd}
 & T = R + S = \mathcal{O}_m \text{ (“compositum”)} \arrow[dl, dash] \arrow[dr, dash] & \\
R \arrow[dr, dash] & & S \arrow[dl, dash] \\
 & E = R \cap S = \mathcal{O}_d &
\end{tikzcd}$$

Algebra: Combining Cyclotomic Rings

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$. Let $d = \gcd(k, \ell)$ and $m = \operatorname{lcm}(k, \ell)$.

$$\begin{tikzcd}[column sep=small]
 & T = R + S = \mathcal{O}_m \ \text{(“compositum”)} \arrow[dl, dash] \arrow[dr, dash] & \\
R \arrow[dr, dash] & & S \arrow[dl, dash] \\
 & E = R \cap S = \mathcal{O}_d &
\end{tikzcd}$$

Easy Lemma

- For any E-linear $L \colon R \to S$, there is an S-linear $\bar{L} \colon T \to S$ that agrees with L on R.

Algebra: Combining Cyclotomic Rings

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$. Let $d = \gcd(k, \ell)$ and $m = \operatorname{lcm}(k, \ell)$.

$$\begin{tikzcd}[column sep=small]
 & T = R + S = \mathcal{O}_m \quad (\text{“compositum”}) \arrow[dl, dash] \arrow[dr, dash] & \\
R \arrow[dr, dash] & & S \arrow[dl, dash] \\
 & E = R \cap S = \mathcal{O}_d &
\end{tikzcd}$$

Easy Lemma

- For any E-linear $L\colon R \to S$, there is an S-linear $\bar{L}\colon T \to S$ that agrees with L on R.
- Proof: define $\bar{L}$ by $\bar{L}(r \cdot s) = L(r) \cdot s \in S$.

Enhanced Ring-Switching: First Attempt

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$ be s.t. $\gcd(k, \ell) = 1$, $\mathrm{lcm}(k, \ell) = k\ell$.

Enhanced Ring-Switching: First Attempt

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$ be s.t. $\gcd(k, \ell) = 1$, $\mathrm{lcm}(k, \ell) = k\ell$.

$$\begin{tikzcd}
 & T = \mathcal{O}_{k\ell} \arrow[dr, "\bar{L}"] & \\
R \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "L", "\text{(induced)}"'] \arrow[dr, dash] & & S \arrow[dl, dash] \\
 & E = \mathbb{Z} &
\end{tikzcd}$$

Enhanced Ring-Switching: First Attempt

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$ be s.t. $\gcd(k,\ell) = 1$, $\mathrm{lcm}(k,\ell) = k\ell$.

$$\begin{tikzcd}
 & T = \mathcal{O}_{k\ell} \arrow[dr, "\bar{L}"] & \\
R \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "L", "\text{(induced)}"'] \arrow[dr, dash] & & S \\
 & E = \mathbb{Z} \arrow[ur, dash] &
\end{tikzcd}$$

- To homom'ly eval. $\mathbb{Z}$-linear $L \colon R \to S$ on an encryption of $v \in R_q$,

Enhanced Ring-Switching: First Attempt

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$ be s.t. $\gcd(k, \ell) = 1$, $\operatorname{lcm}(k, \ell) = k\ell$.

$$\begin{tikzcd}
& T = \mathcal{O}_{k\ell} \arrow[dr, "\bar{L}"] & \\
R \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "L", "\text{(induced)}"'] \arrow[dr, dash] & & S \arrow[dl, dash] \\
& E = \mathbb{Z} &
\end{tikzcd}$$

- To homom'ly eval. $\mathbb{Z}$-linear $L \colon R \to S$ on an encryption of $v \in R_q$,
  1. Trivially embed ciphertext $R \to T$ (still encrypts v).
  2. Homomorphically apply S-linear $\bar{L} \colon T \to S$ using ring-switching.
  - ✔ We now have an encryption of $\bar{L}(v) = L(v)$!

Enhanced Ring-Switching: First Attempt

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$ be s.t. $\gcd(k, \ell) = 1$, $\mathrm{lcm}(k, \ell) = k\ell$.

$$
\begin{tikzcd}
 & T = \mathcal{O}_{k\ell} \arrow[dr, "\bar{L}"] & \\
R \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "L", "\text{(induced)}"'] & & S \\
 & E = \mathbb{Z} \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}
$$

- To homom'ly eval. $\mathbb{Z}$-linear $L \colon R \to S$ on an encryption of $v \in R_q$,
  1. Trivially embed ciphertext $R \to T$ (still encrypts v).
  2. Homomorphically apply S-linear $\bar{L} \colon T \to S$ using ring-switching.

  ✔ We now have an encryption of $\bar{L}(v) = L(v)$!

✗✗ Problem: degree of T is quadratic, therefore so is runtime & space.

Enhanced Ring-Switching: First Attempt

- Let $R = \mathcal{O}_k$, $S = \mathcal{O}_\ell$ be s.t. $\gcd(k,\ell) = 1$, $\operatorname{lcm}(k,\ell) = k\ell$.

$$\begin{tikzcd}
 & T = \mathcal{O}_{k\ell} \arrow[dr, "\bar{L}"] & \\
R \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "L", "\text{(induced)}"'] \arrow[dr, dash] & & S \arrow[dl, dash] \\
 & E = \mathbb{Z} &
\end{tikzcd}$$

- To homom'ly eval. $\mathbb{Z}$-linear $L \colon R \to S$ on an encryption of $v \in R_q$,
  1. Trivially embed ciphertext $R \to T$ (still encrypts v).
  2. Homomorphically apply S-linear $\bar{L} \colon T \to S$ using ring-switching.
  - ✔ We now have an encryption of $\bar{L}(v) = L(v)$!

✗✗ Problem: degree of T is quadratic, therefore so is runtime & space. This is inherent if we treat L as a generic $\mathbb{Z}$-linear map!

Enhanced Ring-Switching, Efficiently

Key Ideas

- The $\mathbb{Z}$-linear $L\colon R \to S$ given by $L(b_j) = c_j$ is "highly structured," because B, C are product sets.

Enhanced Ring-Switching, Efficiently

Key Ideas

- The $\mathbb{Z}$-linear $L \colon R \to S$ given by $L(b_j) = c_j$ is "highly structured," because B, C are product sets.
- Gradually map B to C through a sequence of "hybrid rings" $H^{(i)}$, via $E^{(i)}$-linear functions that each send a factor of B to one of C.

$$
\begin{tikzcd}
 & T^{(1)} \arrow[dr] & & T^{(2)} \arrow[dr] & \\
B \subset R = H^{(0)} \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "E^{(1)}\text{-linear}", "\text{(induced)}"'] \arrow[dr, dash] & & H^{(1)} \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "E^{(2)}\text{-linear}", "\text{(induced)}"'] \arrow[dr, dash] & & H^{(2)} = S \supset C \\
 & E^{(1)} \arrow[ur, dash] & & E^{(2)} \arrow[ur, dash] &
\end{tikzcd}
$$

Enhanced Ring-Switching, Efficiently

Key Ideas

- The $\mathbb{Z}$-linear $L\colon R \to S$ given by $L(b_j) = c_j$ is "highly structured," because B, C are product sets.
- Gradually map B to C through a sequence of "hybrid rings" $H^{(i)}$, via $E^{(i)}$-linear functions that each send a factor of B to one of C.
- Ensure small compositums $T^{(i)} = H^{(i-1)} + H^{(i)}$ via large gcd's: replace prime factors of k with those of ℓ, one at a time.

$$\begin{tikzcd}
 & T^{(1)} \arrow[dr] & & T^{(2)} \arrow[dr] & \\
B \subset R = H^{(0)} \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "E^{(1)}\text{-linear}", "\text{(induced)}"'] \arrow[dr, dash] & & H^{(1)} \arrow[ur, "\text{embed}"] \arrow[rr, dashed, "E^{(2)}\text{-linear}", "\text{(induced)}"'] \arrow[dr, dash] & & H^{(2)} = S \supset C \\
 & E^{(1)} \arrow[ur, dash] & & E^{(2)} \arrow[ur, dash] &
\end{tikzcd}$$

Toy Example

- $R = \mathcal{O}_8$, basis $B = B'_8 \cdot B'_4 = \{1, \zeta_8\} \cdot \{1, \zeta_4\}$.

Toy Example

- $R = \mathcal{O}_8$, basis $B = B'_8 \cdot B'_4 = \{1, \zeta_8\} \cdot \{1, \zeta_4\}$.
- $S = \mathcal{O}_{7\cdot 13}$, CRT set $C = C'_7 \cdot C'_{91} = \{c_1, c_2\} \cdot \{c'_1, c'_2, c'_3\}$.

Toy Example

- $R = \mathcal{O}_8$, basis $B = B'_8 \cdot B'_4 = \{1, \zeta_8\} \cdot \{1, \zeta_4\}$.
- $S = \mathcal{O}_{7\cdot 13}$, CRT set $C = C'_7 \cdot C'_{91} = \{c_1, c_2\} \cdot \{c'_1, c'_2, c'_3\}$.

$$
\begin{tikzcd}
\begin{array}{c} B'_8 \cdot B'_4 \\ \subset \mathcal{O}_8 \end{array} \arrow[rr, dashed, "B'_8 \to C'_7", "\text{fix } B'_4"'] \arrow[dr, no head] & & \begin{array}{c} B'_4 \cdot C'_7 \\ \subset \mathcal{O}_{4\cdot 7} \end{array} \arrow[rr, dashed, "B'_4 \to C'_{91}", "\text{fix } C'_7"'] \arrow[dr, no head] & & \begin{array}{c} C'_7 \cdot C'_{91} \\ \subset \mathcal{O}_{7\cdot 13} \end{array} \\
& \mathcal{O}_4 \arrow[ur, no head] & & \mathcal{O}_7 \arrow[ur, no head] &
\end{tikzcd}
$$

Toy Example

- $R = \mathcal{O}_8$, basis $B = B'_8 \cdot B'_4 = \{1, \zeta_8\} \cdot \{1, \zeta_4\}$.
- $S = \mathcal{O}_{7\cdot 13}$, CRT set $C = C'_7 \cdot C'_{91} = \{c_1, c_2\} \cdot \{c'_1, c'_2, c'_3\}$.

$$
\begin{tikzcd}
\begin{array}{c} B'_8 \cdot B'_4 \\ \subset \mathcal{O}_8 \end{array} \arrow[rr, dashed, "B'_8 \to C'_7", "\text{fix } B'_4"'] \arrow[dr, no head] & & \begin{array}{c} B'_4 \cdot C'_7 \\ \subset \mathcal{O}_{4\cdot 7} \end{array} \arrow[rr, dashed, "B'_4 \to C'_{91}", "\text{fix } C'_7"'] \arrow[dl, no head] \arrow[dr, no head] & & \begin{array}{c} C'_7 \cdot C'_{91} \\ \subset \mathcal{O}_{7\cdot 13} \end{array} \arrow[dl, no head] \\
& \mathcal{O}_4 & & \mathcal{O}_7 &
\end{tikzcd}
$$

- In general, switch through $\leq \log(\deg(R/\mathbb{Z})) = \log(\lambda)$ hybrid rings, one for each prime factor of k.

Final Thoughts

- Gradually converting B to C via hybrid rings is roughly analogous to a log-depth FFT butterfly network.

Final Thoughts

- Gradually converting B to C via hybrid rings is roughly analogous to a log-depth FFT butterfly network.
- Technique should also be useful for homomorphically evaluating other signal-processing transforms having "sparse decompositions."

Final Thoughts

- Gradually converting B to C via hybrid rings is roughly analogous to a log-depth FFT butterfly network.
- Technique should also be useful for homomorphically evaluating other signal-processing transforms having “sparse decompositions.”
- Practical implementation and evaluation are underway.

Final Thoughts

- Gradually converting B to C via hybrid rings is roughly analogous to a log-depth FFT butterfly network.
- Technique should also be useful for homomorphically evaluating other signal-processing transforms having "sparse decompositions."
- Practical implementation and evaluation are underway.

Thanks!