Lattice-based Obfuscation from NTRU and Equivocal LWE

Valerio Cini[1], Russell W. F. Lai[2], **Ivy K. Y. Woo**[2]

ia.cr/2025/1129

[1] Bocconi University, Italy
[2] **Aalto University, Finland**

CRYPTO, 21 August 2025

Content

Indistinguishability Obfuscation

- Algorithms: $\mathsf{Obf}(\Gamma) \to \tilde{\Gamma}$, $\mathsf{Eval}(\tilde{\Gamma}, x) \to y = \Gamma(x)$
- Security: For any $\Gamma_0 \equiv \Gamma_1$, $\mathsf{Obf}(\Gamma_0) \approx_c \mathsf{Obf}(\Gamma_1)$
- Efficiency: $|\tilde{\Gamma}| = \mathsf{poly}(|\Gamma|, \lambda)$
- Construction from "well-founded" assumptions by Jain, Lin, and Sahai [JLS21; JLS22], but not post-quantum secure

EXponentially-efficient iO

- Relaxed efficiency: $|\tilde{\Gamma}| = o(|\text{truth table}|) \cdot \text{poly}(\lambda)$
- [LPST16]: XiO + LWE $\implies$ iO
- Many XiO attempts from lattices, all based on heuristics or novel/highly-tailored assumptions; most assumptions cryptanalysed [HJL21; JLLS23]

EXponentially-efficient iO

- Relaxed efficiency: $|\tilde{\Gamma}| = o(|\text{truth table}|) \cdot \text{poly}(\lambda)$
- [LPST16]: XiO + LWE $\Longrightarrow$ iO
- Many XiO attempts from lattices, all based on heuristics or novel/highly-tailored assumptions; most assumptions cryptanalysed [HJL21; JLLS23]
- Our goal: Lattice-based XiO from self-contained + reasonable assumptions
- Starting point: XiO template of Brakerski, Döttling, Garg, and Malavolta [BDGM20]

Ingredients to [BDGM20]'s XiO Template

1. Fully-homomorphic encryption (FHE)

2. Learning with Errors (LWE)-based encoding

Ingredients to [BDGM20]'s XiO Template

1. Fully-homomorphic encryption (FHE)
   - From $\mathrm{ctxt}_{\mathbf{x}}$ encrypting $\mathbf{x}$, can derive $\mathrm{ctxt}_{f(\mathbf{x})}$ for any function f
   - Secret key sk = vector $\mathbf{s}$
   - Decrypt = evaluate linear function $\mathbf{L}_{\mathrm{ctxt}}$ in $\mathbf{s}$, then rounding:

$$\mathrm{Dec}(\cdot, \mathrm{ctxt}) : \; \mathbf{s} \mapsto \mathrm{Dec}(\mathbf{s}, \mathrm{ctxt}) = \mathrm{round}(\mathbf{L}_{\mathrm{ctxt}} \cdot \mathbf{s})$$

2. Learning with Errors (LWE)-based encoding

Ingredients to [BDGM20]'s XiO Template

1. Fully-homomorphic encryption (FHE)
   - From $\mathsf{ctxt}_{\mathbf{x}}$ encrypting $\mathbf{x}$, can derive $\mathsf{ctxt}_{f(\mathbf{x})}$ for any function f
   - Secret key sk = vector $\mathbf{s}$
   - Decrypt $=$ evaluate linear function $\mathbf{L}_{\mathsf{ctxt}}$ in $\mathbf{s}$, then rounding:

$$\mathsf{Dec}(\cdot, \mathsf{ctxt}) : \ \mathbf{s} \mapsto \mathsf{Dec}(\mathbf{s}, \mathsf{ctxt}) = \mathsf{round}(\mathbf{L}_{\mathsf{ctxt}} \cdot \mathbf{s})$$

2. Learning with Errors (LWE)-based encoding
   - Given $\mathbf{B}$ random wide matrix, $\mathbf{RB} + \mathbf{E} \bmod q \approx_c \$$ for random $\mathbf{R}$, Gaussian $\mathbf{E}$

$$\Longrightarrow \mathbf{C} = \mathbf{RB} + \mathbf{E} + \mathsf{Encode}(\mathbf{s}) \bmod q \approx_c \$$$

   - LWE secret $\mathbf{R}$ allows to recover $\mathbf{s}$:

$$\mathbf{s} = \mathsf{Decode}(\mathbf{C} - \mathbf{RB} \bmod q)$$

Ingredients to [BDGM20]'s XiO Template

1. Fully-homomorphic encryption (FHE)
   - From $\text{ctxt}_{\mathbf{x}}$ encrypting $\mathbf{x}$, can derive $\text{ctxt}_{f(\mathbf{x})}$ for any function f
   - Secret key sk = vector $\mathbf{s}$
   - Decrypt $=$ evaluate linear function $\mathbf{L}_{\text{ctxt}}$ in $\mathbf{s}$, then rounding:

$$\text{Dec}(\cdot, \text{ctxt}) : \ \mathbf{s} \mapsto \text{Dec}(\mathbf{s}, \text{ctxt}) = \text{round}(\mathbf{L}_{\text{ctxt}} \cdot \mathbf{s})$$

2. Learning with Errors (LWE)-based encoding
   - Given $\mathbf{B}$ random wide matrix, $\mathbf{RB} + \mathbf{E} \bmod q \approx_c \$$ for random $\mathbf{R}$, Gaussian $\mathbf{E}$

$$\Longrightarrow \mathbf{C} = \mathbf{RB} + \mathbf{E} + \text{Encode}(\mathbf{s}) \bmod q \approx_c \$$$

   - Homomorphic for low-norm linear transforms, i.e. if $\mathbf{L}$ is low-norm matrix then

$$\mathbf{LC} \approx \mathbf{LRB} + \text{Encode}(\mathbf{Ls}) \bmod q$$

   - LWE secret $\mathbf{R}$ allows to recover $\mathbf{s}$:

$$\mathbf{s} = \text{Decode}(\mathbf{C} - \mathbf{RB} \bmod q) \qquad \mathbf{Ls} = \text{Decode}(\mathbf{LC} - \mathbf{LRB} \bmod q)$$

[BDGM20]'s XiO Template

- Circuit Γ, truth table $\mathbf{Y}$, size $|\mathbf{Y}| = h \cdot k$
- $\mathsf{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathsf{ctxt}, \mathbf{B}, \mathbf{C}, \hat{\mathbf{R}})$
  - FHE ctxt encrypting Γ ; secret key $= \mathbf{s}$
  - $\mathbf{B}$: random wide matrix
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathsf{Encode}(\mathbf{s}) \bmod q$
  - Decryption hint $\hat{\mathbf{R}}$

[BDGM20]'s XiO Template

- Circuit Γ, truth table $\mathbf{Y}$, size $|\mathbf{Y}| = h \cdot k$
- $\mathrm{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathrm{ctxt}, \mathbf{B}, \mathbf{C}, \hat{\mathbf{R}})$
  - FHE ctxt encrypting Γ ; secret key $= \mathbf{s}$
  - $\mathbf{B}$: random wide matrix
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathrm{Encode}(\mathbf{s}) \bmod q$
  - Decryption hint $\hat{\mathbf{R}}$
    - For each input x, evaluate universal circuit $U(\cdot, x)$ on ctxt
      $\to$ Obtain FHE $\mathrm{ctxt}_{\Gamma(x)}$ encrypting $\Gamma(x)$
    - Evaluate linear part $\mathbf{L}$ of $\mathrm{FHE.Dec}(\cdot, (\mathrm{ctxt}_{\Gamma(x)})_x)$ on $\mathbf{C}$, obtain

$$\mathbf{L}\mathbf{C} \approx \underbrace{\mathbf{L}\mathbf{R}}_{\hat{\mathbf{R}}}\mathbf{B} + \mathrm{Encode}(\mathbf{Y}) \bmod q$$

- $\mathrm{Eval}(\tilde{\Gamma}, x)$: Re-derive $\mathbf{L}\mathbf{C} \bmod q$ from $(\mathrm{ctxt}, \mathbf{C})$, obtain $\mathrm{Decode}(\mathbf{L}\mathbf{C} - \hat{\mathbf{R}}\mathbf{B} \bmod q) = \mathbf{Y}$

[BDGM20]'s XiO Template

- Circuit Γ, truth table $\mathbf{Y}$, size $|\mathbf{Y}| = h \cdot k$
- $\mathrm{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathrm{ctxt}, \mathbf{B}, \mathbf{C}, \hat{\mathbf{R}})$
  - FHE ctxt encrypting Γ ; secret key $= \mathbf{s}$
  - $\mathbf{B}$: random wide matrix
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathrm{Encode}(\mathbf{s}) \bmod q$
  - Decryption hint $\hat{\mathbf{R}} = \boxed{\mathbf{L}}\ \boxed{\mathbf{R}}$
- $|\mathrm{Encode}(\mathbf{Y})| = O(hk) > O(h) + O(k) = |\hat{\mathbf{R}}| + |\mathbf{B}| \Rightarrow$ Compression ✓

$$\mathbf{LC} \approx h\,\boxed{\hat{\mathbf{R}}}\ \overset{k}{\boxed{\mathbf{B}}} + h\,\overset{k}{\boxed{\mathrm{Encode}(\mathbf{Y})}} \mod q$$

[BDGM20]'s XiO Template

- Circuit Γ, truth table $\mathbf{Y}$, size $|\mathbf{Y}| = h \cdot k$
- $\mathrm{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathrm{ctxt}, \mathbf{B}, \mathbf{C}, \hat{\mathbf{R}})$ ✗
  - FHE ctxt encrypting Γ ; secret key $= \mathbf{s}$
  - $\mathbf{B}$: random wide matrix
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathrm{Encode}(\mathbf{s}) \bmod q$
  - Decryption hint $\hat{\mathbf{R}} = \boxed{\mathbf{L}}\ \boxed{\mathbf{R}}$
- $|\mathrm{Encode}(\mathbf{Y})| = O(hk) > O(h) + O(k) = |\hat{\mathbf{R}}| + |\mathbf{B}| \Rightarrow$ Compression ✓
- Issues with $\hat{\mathbf{R}}$:
  - Give out $\hat{\mathbf{R}} \to$ Trivial attack, find $\mathbf{R}$ from $(\mathbf{L}, \hat{\mathbf{R}} = \mathbf{L}\mathbf{R})$, then recover $\mathbf{s}$ from $\mathbf{C}$ ✗

[BDGM20]'s XiO Template

- Circuit Γ, truth table $\mathbf{Y}$, size $|\mathbf{Y}| = h \cdot k$
- $\mathrm{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathrm{ctxt}, \mathbf{B}, \mathbf{C}, \mathrm{mask}(\hat{\mathbf{R}}))$ ...?
  - FHE ctxt encrypting Γ ; secret key $= \mathbf{s}$
  - $\mathbf{B}$: random wide matrix
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathrm{Encode}(\mathbf{s}) \bmod q$
  - Decryption hint $\hat{\mathbf{R}} = \boxed{\mathbf{L}}\ \boxed{\mathbf{R}}$
- $|\mathrm{Encode}(\mathbf{Y})| = O(hk) > O(h) + O(k) = |\hat{\mathbf{R}}| + |\mathbf{B}| \Rightarrow$ Compression ✓
- Issues with $\hat{\mathbf{R}}$:
  - Give out $\hat{\mathbf{R}} \to$ Trivial attack, find $\mathbf{R}$ from $(\mathbf{L}, \hat{\mathbf{R}} = \mathbf{L}\mathbf{R})$, then recover $\mathbf{s}$ from $\mathbf{C}$ ✗
  - Innovative ways to mask $\hat{\mathbf{R}}$ [BDGM20; WW21; GP21; DQV+21; BDGM22]

    $\to$ Heuristic security/ Assumption cryptanalysed ✗ [HJL21; JLLS23]

Idea to new decryption hint

Recap:

- $\mathsf{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathsf{ctxt}, \mathbf{B}, \mathbf{C}, ?)$
  - FHE ctxt of Γ; $\mathsf{sk} = \mathbf{s}$
  - $\mathbf{B}$: wide matrix
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathsf{Encode}(\mathbf{s}) \bmod q$
  - $\hat{\mathbf{R}} = \mathbf{L}\mathbf{R} \bmod q$, thus $\mathbf{L}\mathbf{C} \approx \hat{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$
- $\mathsf{Eval}(\tilde{\Gamma}, x)$: Re-derive $\mathbf{L}\mathbf{C}$ from $(\mathsf{ctxt}, \mathbf{C})$, obtain truth table $\mathsf{Decode}(\mathbf{L}\mathbf{C} - \hat{\mathbf{R}}\mathbf{B} \bmod q) = \mathbf{Y}$
- Give out $\hat{\mathbf{R}} \to$ Trivial attack ✗; Give out $\mathsf{mask}(\hat{\mathbf{R}}) \to$ No proof from plausible assumption ✗

Idea to new decryption hint

Recap:

- $\mathsf{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathsf{ctxt}, \mathbf{B}, \mathbf{C}, ?)$
  - FHE ctxt of Γ; $\mathsf{sk} = \mathbf{s}$
  - $\mathbf{B}$: wide matrix
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathsf{Encode}(\mathbf{s}) \bmod q$
  - $\hat{\mathbf{R}} = \mathbf{L}\mathbf{R} \bmod q$, thus $\mathbf{L}\mathbf{C} \approx \hat{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$
- $\mathsf{Eval}(\tilde{\Gamma}, x)$: Re-derive $\mathbf{L}\mathbf{C}$ from $(\mathsf{ctxt}, \mathbf{C})$, obtain truth table $\mathsf{Decode}(\mathbf{L}\mathbf{C} - \hat{\mathbf{R}}\mathbf{B} \bmod q) = \mathbf{Y}$
- Give out $\hat{\mathbf{R}} \to$ Trivial attack ✗; Give out $\mathsf{mask}(\hat{\mathbf{R}}) \to$ No proof from plausible assumption ✗

- Observations:
  - Correctness needs $\hat{\mathbf{R}}$ s.t. $\mathbf{L}\mathbf{C} \approx \hat{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$, unique w.h.p. if $\mathbf{B}$ uniform
  - Prior attempts: (randomness for) masking to $\hat{\mathbf{R}}$ leaked elsewhere in obfuscation

Idea to new decryption hint

Recap:

- $\mathsf{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathsf{ctxt}, \mathbf{B}, \mathbf{C}, \tilde{\mathbf{R}})$
  - FHE ctxt of Γ; $\mathsf{sk} = \mathbf{s}$
  - $\mathbf{B}$: wide matrix sampled from special distribution
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathsf{Encode}(\mathbf{s}) \bmod q$
  - $\hat{\mathbf{R}} = \mathbf{L}\mathbf{R} \bmod q$, thus $\mathbf{L}\mathbf{C} \approx \hat{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$
  - Sample random $\tilde{\mathbf{R}}$ s.t. $\mathbf{L}\mathbf{C} \approx \tilde{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$
- $\mathsf{Eval}(\tilde{\Gamma}, x)$: Re-derive $\mathbf{L}\mathbf{C}$ from $(\mathsf{ctxt}, \mathbf{C})$, obtain truth table $\mathsf{Decode}(\mathbf{L}\mathbf{C} - \tilde{\mathbf{R}}\mathbf{B} \bmod q) = \mathbf{Y}$
- Give out $\hat{\mathbf{R}} \to$ Trivial attack ✗; Give out $\mathsf{mask}(\hat{\mathbf{R}}) \to$ No proof from plausible assumption ✗

- Observations:
  - Correctness needs $\hat{\mathbf{R}}$ s.t. $\mathbf{L}\mathbf{C} \approx \hat{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$, unique w.h.p. if $\mathbf{B}$ uniform
  - Prior attempts: (randomness for) masking to $\hat{\mathbf{R}}$ leaked elsewhere in obfuscation
- Idea: Let $\mathbf{B}$ s.t. there are many possible $\hat{\mathbf{R}}$, give out freshly sampled random one, e.g. $\tilde{\mathbf{R}}$

Lattice point of view

- For LWE sample $\mathbf{c}^\top = \mathbf{r}^\top\mathbf{B} + \mathbf{e}^\top \bmod q$,

  LWE solution = point on primal lattice $\Lambda_q(\mathbf{B}) = \{\mathbf{x}^\top : \exists \mathbf{r},\ \mathbf{x}^\top = \mathbf{r}^\top\mathbf{B} \bmod q\}$ close to $\mathbf{c}^\top$
- Uniform $\mathbf{B} \iff \Lambda_q(\mathbf{B})$ is "sparse" w.h.p. $\iff$ Unique lattice point close to $\mathbf{c}^\top$

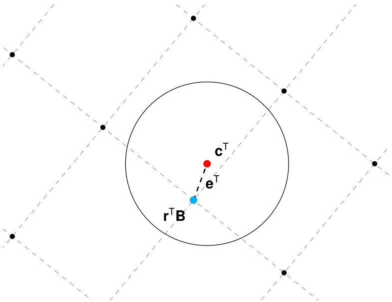


Figure: $\Lambda_q(\mathbf{B})$ for uniform $\mathbf{B}$. One lattice point within ball = unique LWE solution.

Lattice point of view

- For LWE sample $\mathbf{c}^\top = \mathbf{r}^\top\mathbf{B} + \mathbf{e}^\top \bmod q$,

  LWE solution = point on primal lattice $\Lambda_q(\mathbf{B}) = \{\mathbf{x}^\top : \exists \mathbf{r},\ \mathbf{x}^\top = \mathbf{r}^\top\mathbf{B} \bmod q\}$ close to $\mathbf{c}^\top$
- Uniform $\mathbf{B} \iff \Lambda_q(\mathbf{B})$ is "sparse" w.h.p. $\iff$ Unique lattice point close to $\mathbf{c}^\top$
- Idea: $\mathbf{B}$ s.t. $\Lambda_q(\mathbf{B})$ has a "dense" sublattice

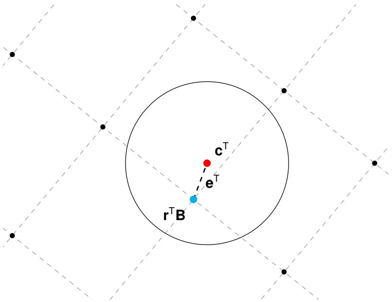


Figure: $\Lambda_q(\mathbf{B})$ for uniform $\mathbf{B}$. One lattice point within ball = unique LWE solution.

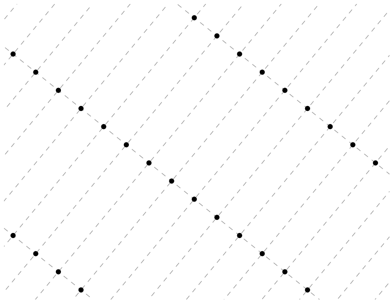


Figure: Lattice with dense sublattice.

Equivocal Distribution $\mathcal{E}$

- Want: Given LWE sample $\mathbf{c}^\top = \mathbf{r}^\top\mathbf{B} + \mathbf{e}^\top \bmod q$,
  - $\exists$ super-poly many LWE solutions $(\tilde{\mathbf{r}}, \tilde{\mathbf{e}})$ s.t. $\mathbf{c}^\top = \tilde{\mathbf{r}}^\top\mathbf{B} + \tilde{\mathbf{e}}^\top \bmod q$
  - $\mathbf{B}$ looks random, even given decryption hint

Equivocal Distribution $\mathcal{E}$

- Want: Given LWE sample $\mathbf{c}^\top = \mathbf{r}^\top\mathbf{B} + \mathbf{e}^\top \bmod q$,
  - $\exists$ super-poly many LWE solutions $(\tilde{\mathbf{r}}, \tilde{\mathbf{e}})$ s.t. $\mathbf{c}^\top = \tilde{\mathbf{r}}^\top\mathbf{B} + \tilde{\mathbf{e}}^\top \bmod q$
  - $\mathbf{B}$ looks random, even given decryption hint
- $\mathbf{B} \sim$ Equivocal distribution $\mathcal{E}$:
  1. **Dense Sublattice**: For any $\mathbf{c}$,

$$\text{min-entropy}\left(\tilde{\mathbf{r}}^\top\mathbf{B} \leftarrow\$ \text{ Guassian over } \Lambda_q(\mathbf{B}) \text{ centered at } \mathbf{c}\right) \geq \omega(\log\lambda)$$

$\tilde{\mathbf{r}}$:= “equivocation of $\mathbf{c}$”

  2. **Pseudorandom with Leakage**: For any low-norm $(\mathbf{c}_i)_i$,

$$\left\{ \mathbf{B}, (\mathbf{l}_i)_i \;\middle|\; \begin{array}{l} \mathbf{B} \leftarrow\$ \mathcal{E}; \quad x_i \leftarrow\$ \$ \\ \tilde{\mathbf{r}}_i = \text{equivocation of } \mathbf{c}_i \\ \mathbf{l}_i = x_i \cdot \tilde{\mathbf{r}}_i \bmod q \quad /\!/ \text{ leakage} \end{array} \right\} \approx_c \left\{ \mathbf{B}, (\mathbf{l}_i)_i \;\middle|\; \begin{array}{l} \mathbf{B} \leftarrow\$ \$; \quad \mathbf{x}_i \leftarrow\$ \$ \\ \hat{\mathbf{R}} \leftarrow\$ \$ \\ \mathbf{l}_i^\top = \mathbf{x}_i^\top \cdot \hat{\mathbf{R}} \bmod q \end{array} \right\}$$

Equivocal Distribution $\mathcal{E}$

- Want: Given LWE sample $\mathbf{c}^\mathsf{T} = \mathbf{r}^\mathsf{T}\mathbf{B} + \mathbf{e}^\mathsf{T} \bmod q$,
  - $\exists$ super-poly many LWE solutions $(\tilde{\mathbf{r}}, \tilde{\mathbf{e}})$ s.t. $\mathbf{c}^\mathsf{T} = \tilde{\mathbf{r}}^\mathsf{T}\mathbf{B} + \tilde{\mathbf{e}}^\mathsf{T} \bmod q$
  - $\mathbf{B}$ looks random, even given decryption hint
- $\mathbf{B} \sim$ Equivocal distribution $\mathcal{E}$:
  1. **Dense Sublattice**: For any $\mathbf{c}$,

$$\text{min-entropy}\Big(\tilde{\mathbf{r}}^\mathsf{T}\mathbf{B} \leftarrow\$ \text{ Guassian over } \Lambda_q(\mathbf{B}) \text{ centered at } \mathbf{c}\Big) \geq \omega(\log\lambda)$$

$\tilde{\mathbf{r}}$:= “equivocation of $\mathbf{c}$”

  2. **Pseudorandom with Leakage**: For any low-norm $(\mathbf{c}_i)_i$,

$$\left\{ \mathbf{B}, (\mathbf{l}_i)_i \;\middle|\; \begin{array}{l} \mathbf{B} \leftarrow\$ \mathcal{E}; \quad x_i \leftarrow\$ \$ \\ \tilde{\mathbf{r}}_i = \text{equivocation of } \mathbf{c}_i \\ \mathbf{l}_i = x_i \cdot \tilde{\mathbf{r}}_i \bmod q \quad / \text{ leakage} \end{array} \right\} \approx_c \left\{ \mathbf{B}, (\mathbf{l}_i)_i \;\middle|\; \begin{array}{l} \mathbf{B} \leftarrow\$ \$; \quad \mathbf{x}_i \leftarrow\$ \$ \\ \hat{\mathbf{R}} \leftarrow\$ \$ \\ \mathbf{l}_i^\mathsf{T} = \mathbf{x}_i^\mathsf{T} \cdot \hat{\mathbf{R}} \bmod q \end{array} \right\}$$

- Next: How to construct efficiently sampleable $\mathcal{E}$?

Primal Lattice Trapdoor

- Two algorithms:
  - $\mathsf{pTrapGen}(1^\lambda) \to (\mathbf{B},\ \mathsf{trapdoor})$
  - $\mathsf{Equivocate}(\mathsf{trapdoor},\ \mathbf{r},\ \mathbf{c}^\top = \mathbf{r}^\top\mathbf{B} + \mathbf{e}^\top \bmod q) \to \tilde{\mathbf{r}}$ s.t. $\mathbf{c}^\top = \tilde{\mathbf{r}}^\top\mathbf{B} + \tilde{\mathbf{e}}^\top \bmod q$

Primal Lattice Trapdoor

- Two algorithms:
  - $\mathsf{pTrapGen}(1^\lambda) \to (\mathbf{B},\ \mathsf{trapdoor})$
  - $\mathsf{Equivocate}(\mathsf{trapdoor},\ \mathbf{r},\ \mathbf{c}^\top = \mathbf{r}^\top\mathbf{B} + \mathbf{e}^\top \bmod q) \to \tilde{\mathbf{r}}$ s.t. $\mathbf{c}^\top = \tilde{\mathbf{r}}^\top\mathbf{B} + \tilde{\mathbf{e}}^\top \bmod q$
- I.e. sample lattice points from primal lattice

$$\Lambda_q(\mathbf{B}) = \left\{\mathbf{x}^\top : \exists\mathbf{r},\ \mathbf{x}^\top = \mathbf{r}^\top\mathbf{B} \bmod q\right\}$$

- Remark: Different from “standard” lattice trapdoor,
  which samples short vectors from kernel lattice $\Lambda_q^\perp(\mathbf{B}) = \{\mathbf{u} : \mathbf{B}\mathbf{u} = \mathbf{0} \bmod q\}$

Primal Lattice Trapdoor

- Two algorithms:
  - $\mathsf{pTrapGen}(1^\lambda) \to (\mathbf{B}, \text{ trapdoor})$
  - $\mathsf{Equivocate}(\text{trapdoor}, \ \mathbf{r}, \ \mathbf{c}^\top = \mathbf{r}^\top\mathbf{B} + \mathbf{e}^\top \bmod q) \to \tilde{\mathbf{r}} \ \text{ s.t. } \mathbf{c}^\top = \tilde{\mathbf{r}}^\top\mathbf{B} + \tilde{\mathbf{e}}^\top \bmod q$
- I.e. sample lattice points from primal lattice

$$\Lambda_q(\mathbf{B}) = \left\{\mathbf{x}^\top : \exists \mathbf{r}, \ \mathbf{x}^\top = \mathbf{r}^\top\mathbf{B} \bmod q\right\}$$

- Remark: Different from "standard" lattice trapdoor, which samples short vectors from kernel lattice $\Lambda_q^\perp(\mathbf{B}) = \{\mathbf{u} : \mathbf{B}\mathbf{u} = \mathbf{0} \bmod q\}$
- Desired properties:
  1. $\mathbf{B}$ equivocal (= $\Lambda_q(\mathbf{B})$ has dense sublattice + $\mathbf{B}$ Pseudorandom with Leakage)
  2. Equivocated LWE secret $\tilde{\mathbf{r}}$ satisfies

$$\tilde{\mathbf{r}}^\top\mathbf{B} \bmod q \ \approx_s \ \text{Gaussian over } \Lambda_q(\mathbf{B}) \text{ centered at } \mathbf{c} \bmod q$$

NTRU

(Decisional) NTRU Assumption

For $\mathbf{f} \leftarrow\$ \mathcal{D}_{\mathcal{R}^m,\chi}$ Gaussian, $d \leftarrow\$ \mathcal{R}_q^\times$ random (short) invertible,

$$\mathbf{b} = d^{-1} \cdot \mathbf{f} \bmod q \qquad \approx_c \qquad \mathbf{b} \leftarrow\$ \text{ uniform over } \mathcal{R}_q^m$$

- $\mathbf{f}^\top$: hidden short vector in $\Lambda_q(\mathbf{b}^\top)$
  - $\mathbf{f}^\top = d \cdot \mathbf{b}^\top \bmod q$
  - $\mathbf{b}$ pseudorandom $\Rightarrow$ Cannot tell if $\Lambda_q(\mathbf{b}^\top)$ has exceptionally short vectors

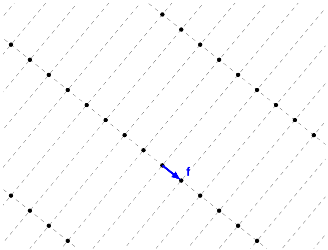
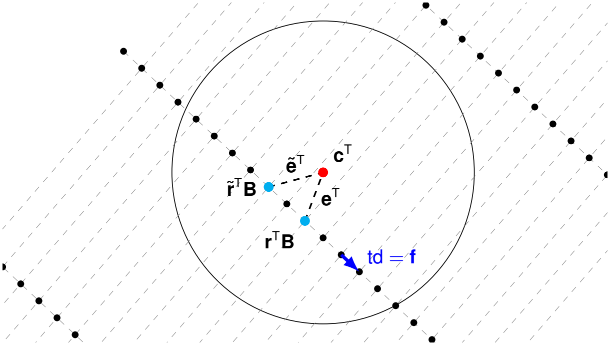


Figure: $\Lambda_q(\mathbf{b}^\top)$ for NTRU $\mathbf{b} = d^{-1} \cdot \mathbf{f} \bmod q$

Primal Lattice Trapdoor – Visualisation

- How $\Lambda_q(\mathbf{B})$ looks like:



- $(\mathbf{r}, \mathbf{e}), (\tilde{\mathbf{r}}, \tilde{\mathbf{e}})$ (and any lattice point within circle) are LWE solutions to $\mathbf{c}$:

$$\mathbf{c}^{\top} = \mathbf{r}^{\top}\mathbf{B} + \mathbf{e}^{\top} = \tilde{\mathbf{r}}^{\top}\mathbf{B} + \tilde{\mathbf{e}}^{\top} \bmod q$$

- Secret short vector $\mathbf{f}$ as trapdoor, allows sampling along dense line(/hyperplane)

Primal Lattice Trapdoor from NTRU

$(\mathbf{B}, \mathrm{td}) \leftarrow \mathrm{pTrapGen}(1^t, 1^k, q)$	$\tilde{\mathbf{r}}^\top \leftarrow \mathrm{Equivocate}(\mathrm{td}, \mathbf{r}, \mathbf{c}, s)$
$\mathbf{d} \leftarrow\$\ \mathcal{R}_q^t : \mathbf{d}^\top \mathcal{R}_q^t = \mathcal{R}_q$	$\mathbf{s} := s/\sigma(\bar{\mathbf{f}}^\top \mathbf{f})$ // component-wise inversion
$\mathbf{f} \leftarrow\$\ \mathcal{D}_{\mathcal{R}^k, \chi_f} : \mathbf{f}^\top \mathcal{R}^k = \mathcal{R}$	$\mathbf{e}_{\mathbb{L}} :=$ Projection of $\mathbf{c}^\top - \mathbf{r}^\top \mathbf{B} \bmod q$ on $\mathrm{Span}(\mathcal{L}(\mathbf{f}^\top))$
$\mathbf{B} \leftarrow\$\ \mathcal{R}_q^{t \times k} : \mathbf{d}^\top \mathbf{B} = \mathbf{f}^\top \bmod q$	$c \cdot \mathbf{1}_k := \mathbf{e}_{\mathbb{L}} / \mathbf{f}$ // component-wise inversion
return $(\mathbf{B}, \mathrm{td} = (\mathbf{B}, \mathbf{f}, \mathbf{d}))$	$p \leftarrow\$\ \mathcal{D}_{\mathcal{R}, \mathbf{s}, c}$
	return $\tilde{\mathbf{r}}^\top := \mathbf{r}^\top + p \cdot \mathbf{d}^\top \bmod q$

Primal Lattice Trapdoor from NTRU

$(\mathbf{B}, \mathrm{td}) \leftarrow \mathrm{pTrapGen}(1^t, 1^k, q)$	$\tilde{\mathbf{r}}^\top \leftarrow \mathrm{Equivocate}(\mathrm{td}, \mathbf{r}, \mathbf{c}, s)$
$\mathbf{d} \leftarrow\$ \mathcal{R}_q^t : \mathbf{d}^\top \mathcal{R}_q^t = \mathcal{R}_q$	$\mathbf{s} := s/\sigma(\bar{\mathbf{f}}^\top \mathbf{f})$ / component-wise inversion
$\mathbf{f} \leftarrow\$ \mathcal{D}_{\mathcal{R}^k, \chi_f} : \mathbf{f}^\top \mathcal{R}^k = \mathcal{R}$	$\mathbf{e}_{\mathbb{L}} :=$ Projection of $\mathbf{c}^\top - \mathbf{r}^\top \mathbf{B} \bmod q$ on $\mathrm{Span}(\mathcal{L}(\mathbf{f}^\top))$
$\mathbf{B} \leftarrow\$ \mathcal{R}_q^{t \times k} : \mathbf{d}^\top \mathbf{B} = \mathbf{f}^\top \bmod q$	$c \cdot \mathbf{1}_k := \mathbf{e}_{\mathbb{L}}/\mathbf{f}$ / component-wise inversion
return $(\mathbf{B}, \mathrm{td} = (\mathbf{B}, \mathbf{f}, \mathbf{d}))$	$p \leftarrow\$ \mathcal{D}_{\mathcal{R}, \mathbf{s}, c}$
	return $\tilde{\mathbf{r}}^\top := \mathbf{r}^\top + p \cdot \mathbf{d}^\top \bmod q$

- $\mathbf{B}$ equivocal:
  - $\mathbf{f}$ is short vector in $\Lambda_q(\mathbf{B}) \Longrightarrow \mathcal{R}$-span of $\mathbf{f}$ is dense sublattice
  - $\mathbf{B}$ Pseudorandom with Leakage: proof under NTRU assumption
- $\tilde{\mathbf{r}}^\top \mathbf{B} \bmod q \approx$ Gaussian over $\Lambda_q(\mathbf{B})$ centered at $\mathbf{c} \bmod q$: statistical proof

Putting together: XiO Construction

- $\mathsf{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathsf{ctxt}, \mathbf{B}, \mathbf{C}, ?)$:
  - FHE ctxt of Γ; $\mathsf{sk} = \mathbf{s}$
  - $\mathbf{B}$: random matrix
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathsf{Encode}(\mathbf{s}) \bmod q$
  - $\hat{\mathbf{R}} = \mathbf{L}\mathbf{R} \bmod q$, thus $\mathbf{L}\mathbf{C} \approx \hat{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$

Putting together: XiO Construction

- $\mathrm{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathrm{ctxt}, \mathbf{B}, \mathbf{C}, \tilde{\mathbf{R}})$:
  - FHE ctxt of Γ; $\mathrm{sk} = \mathbf{s}$
  - $\mathbf{B}$: Equivocal, sampled by pTrapGen
  - $\mathbf{C} = \mathbf{R}\mathbf{B} + \mathbf{E} + \mathrm{Encode}(\mathbf{s}) \bmod q$
  - $\hat{\mathbf{R}} = \mathbf{L}\mathbf{R} \bmod q$, thus $\mathbf{L}\mathbf{C} \approx \hat{\mathbf{R}}\mathbf{B} + \mathrm{Encode}(\mathbf{Y}) \bmod q$
  - Sample random $\tilde{\mathbf{R}}$ s.t. $\mathbf{L}\mathbf{C} \approx \tilde{\mathbf{R}}\mathbf{B} + \mathrm{Encode}(\mathbf{Y}) \bmod q$ by Equivocate
- $\mathrm{Eval}(\tilde{\Gamma}, x)$: Re-derive $\mathbf{L}\mathbf{C}$ from $(\mathrm{ctxt}, \mathbf{C})$, obtain truth table $\mathrm{Decode}(\mathbf{L}\mathbf{C} - \tilde{\mathbf{R}}\mathbf{B} \bmod q) = \mathbf{Y}$

Putting together: XiO Construction

- $\mathsf{Obf}(\Gamma) \to \tilde{\Gamma} = (\mathsf{ctxt}, \mathbf{B}, \mathbf{C}, \tilde{\mathbf{R}})$:
  - FHE ctxt of Γ; $\mathsf{sk} = \mathbf{s}$
  - $\mathbf{B}$: Equivocal, sampled by pTrapGen
  - $\mathbf{C} = \mathbf{RB} + \mathbf{E} + \mathsf{Encode}(\mathbf{s}) \bmod q$
  - $\hat{\mathbf{R}} = \mathbf{LR} \bmod q$, thus $\mathbf{LC} \approx \hat{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$
  - Sample random $\tilde{\mathbf{R}}$ s.t. $\mathbf{LC} \approx \tilde{\mathbf{R}}\mathbf{B} + \mathsf{Encode}(\mathbf{Y}) \bmod q$ by Equivocate
- $\mathsf{Eval}(\tilde{\Gamma}, x)$: Re-derive $\mathbf{LC}$ from $(\mathsf{ctxt}, \mathbf{C})$, obtain truth table $\mathsf{Decode}(\mathbf{LC} - \tilde{\mathbf{R}}\mathbf{B} \bmod q) = \mathbf{Y}$
- Security: Equivocal LWE assumption
  - Based on equivocal distribution $\mathcal{E}$
  - Non-interactive ✓; independent of circuit to be ofuscated ✓; no random oracle ✓
  - Hint $\tilde{\mathbf{R}}\mathbf{B} \bmod q \sim$ Gaussian with public description ✓
  - Cryptanalysis on assumption: see paper

Summary

- Equivocal Distribution & Primal Lattice Trapdoor
- Trapdoor construction from NTRU
- Above + Equivocal LWE assumption $\Longrightarrow$ XiO
- `ia.cr/2025/1129`

Ivy K. Y. Woo
Aalto University, Finland
ivy.woo@aalto.fi
ivyw.ooo
research.cs.aalto.fi/crypto

Thank You!

References I

[BDGM20] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. "Candidate iO from Homomorphic Encryption Schemes". In: *EUROCRYPT 2020, Part I*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12105. LNCS. Springer, Cham, May 2020, pp. 79–109. DOI: 10.1007/978-3-030-45721-1_4.

[BDGM22] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. "Factoring and Pairings Are Not Necessary for IO: Circular-Secure LWE Suffices". In: *ICALP 2022*. Ed. by Mikolaj Bojanczyk, Emanuela Merelli, and David P. Woodruff. Vol. 229. LIPIcs. Schloss Dagstuhl, July 2022, 28:1–28:20. DOI: 10.4230/LIPIcs.ICALP.2022.28.

[DQV+21] Lalita Devadas, Willy Quach, Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. "Succinct LWE Sampling, Random Polynomials, and Obfuscation". In: *TCC 2021, Part II*. Ed. by Kobbi Nissim and Brent Waters. Vol. 13043. LNCS. Springer, Cham, Nov. 2021, pp. 256–287. DOI: 10.1007/978-3-030-90453-1_9.

[GP21] Romain Gay and Rafael Pass. "Indistinguishability obfuscation from circular security". In: *53rd ACM STOC*. Ed. by Samir Khuller and Virginia Vassilevska Williams. ACM Press, June 2021, pp. 736–749. DOI: 10.1145/3406325.3451070.

References II

[HJL21] Samuel B. Hopkins, Aayush Jain, and Huijia Lin. "Counterexamples to New Circular Security Assumptions Underlying iO". In: *CRYPTO 2021, Part II*. Ed. by Tal Malkin and Chris Peikert. Vol. 12826. LNCS. Virtual Event: Springer, Cham, Aug. 2021, pp. 673–700. DOI: 10.1007/978-3-030-84245-1_23.

[JLLS23] Aayush Jain, Huijia Lin, Paul Lou, and Amit Sahai. "Polynomial-Time Cryptanalysis of the Subspace Flooding Assumption for Post-quantum $i\mathcal{O}$". In: *EUROCRYPT 2023, Part I*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14004. LNCS. Springer, Cham, Apr. 2023, pp. 205–235. DOI: 10.1007/978-3-031-30545-0_8.

[JLS21] Aayush Jain, Huijia Lin, and Amit Sahai. "Indistinguishability obfuscation from well-founded assumptions". In: *53rd ACM STOC*. Ed. by Samir Khuller and Virginia Vassilevska Williams. ACM Press, June 2021, pp. 60–73. DOI: 10.1145/3406325.3451093.

[JLS22] Aayush Jain, Huijia Lin, and Amit Sahai. "Indistinguishability Obfuscation from LPN over $\mathbb{F}_p$, DLIN, and PRGs in NC^0". In: *EUROCRYPT 2022, Part I*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13275. LNCS. Springer, Cham, May 2022, pp. 670–699. DOI: 10.1007/978-3-031-06944-4_23.

References III

[LPST16] Huijia Lin, Rafael Pass, Karn Seth, and Sidharth Telang. "Indistinguishability Obfuscation with Non-trivial Efficiency". In: *PKC 2016, Part II*. Ed. by Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang. Vol. 9615. LNCS. Springer, Berlin, Heidelberg, Mar. 2016, pp. 447–462. DOI: 10.1007/978-3-662-49387-8_17.

[WW21] Hoeteck Wee and Daniel Wichs. "Candidate Obfuscation via Oblivious LWE Sampling". In: *EUROCRYPT 2021, Part III*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12698. LNCS. Springer, Cham, Oct. 2021, pp. 127–156. DOI: 10.1007/978-3-030-77883-5_5.