How to Construct Indistinguishability Obfuscation? Part I

Russell W. F. Lai

Aalto University

Helsinki Algorithms & Theory Days, 2025.

Context

- Indistinguishability obfuscation (iO) is powerful – implies (almost) all of cryptography, assuming OWF.
- History:
  - 2001: Formal definition and impossibility of virtual black-box obfuscation [BGIRSVY01]
  - 2013: First candidate construction of iO [GGHRSW13], demonstration of usefulness [SW14]
  - 2014-2020: Breaking and fixing, constructions from progressively weaker assumptions, e.g. [BV15; AJ15; LPST16a; LPST16b; LV16; Lin17; LT17; AJLMS19]
  - 2021-2022: First constructions from "well-founded" assumptions [JLS21; JLS22], not post-quantum
  - 2020-2025: Breaking and fixing post-quantum constructions [BDGM20; WW21; GP21; HJL21; DQVWW21; BDGM22; JLLS23; CLW25; HJL25]
- Status quo:
  - All existing constructions require very long chains of transformations
  - No post-quantum construction from "well-founded" assumptions
  - No (remotely) practical construction
- Next talk: Latest attempt on post-quantum iO [CLW25]

Context

- Indistinguishability obfuscation (iO) is powerful – implies (almost) all of cryptography, assuming OWF.
- History:
  - 2001: Formal definition and impossibility of virtual black-box obfuscation [BGIRSVY01]
  - 2013: First candidate construction of iO [GGHRSW13], demonstration of usefulness [SW14]
  - 2014-2020: Breaking and fixing, constructions from progressively weaker assumptions, e.g. [BV15; AJ15; LPST16a; LPST16b; LV16; Lin17; LT17; AJLMS19]
  - 2021-2022: First constructions from “well-founded” assumptions [JLS21; JLS22], not post-quantum
  - 2020-2025: Breaking and fixing post-quantum constructions [BDGM20; WW21; GP21; HJL21; DQVWW21; BDGM22; JLLS23; CLW25; HJL25]
- Status quo:
  - All existing constructions require very long chains of transformations
  - No post-quantum construction from “well-founded” assumptions
  - No (remotely) practical construction
- Next talk: Latest attempt on post-quantum iO [CLW25]

Context

- Indistinguishability obfuscation (iO) is powerful – implies (almost) all of cryptography, assuming OWF.
- History:
  - 2001: Formal definition and impossibility of virtual black-box obfuscation [BGIRSVY01]
  - 2013: First candidate construction of iO [GGHRSW13], demonstration of usefulness [SW14]
  - 2014-2020: Breaking and fixing, constructions from progressively weaker assumptions, e.g. [BV15; AJ15; LPST16a; LPST16b; LV16; Lin17; LT17; AJLMS19]
  - 2021-2022: First constructions from “well-founded” assumptions [JLS21; JLS22], not post-quantum
  - 2020-2025: Breaking and fixing post-quantum constructions [BDGM20; WW21; GP21; HJL21; DQVWW21; BDGM22; JLLS23; CLW25; HJL25]
- Status quo:
  - All existing constructions require very long chains of transformations
  - No post-quantum construction from “well-founded” assumptions
  - No (remotely) practical construction
- Next talk: Latest attempt on post-quantum iO [CLW25]

Agenda

I will attempt to explain one of the construction chains:

$$\begin{aligned} \text{Next Talk} &\implies \text{XiO} \\ &\xRightarrow{\text{Succinct FE}} \text{Sublinear-size FE} \\ &\xRightarrow{\text{Succinct FE}} \text{Sublinear-time FE} \\ &\xRightarrow{\text{recursion}} \text{iO}. \end{aligned}$$

Note: Not a “well-founded assumptions” chain, but a chain with plausible post-quantum constructions.

Computation model

- We assume the (Boolean) circuit model of computation.
- Circuit families (to be obfuscated) are parametrised by input length $n \in \mathbb{N}$.
- A circuit is denoted as
$$\Gamma : \{0,1\}^n \to \{0,1\}^m.$$
- All circuits considered are $\mathrm{poly}(n)$ size. Therefore $|\mathrm{TruthTable}(\Gamma)| = 2^n \cdot m \leq 2^{\mathrm{poly}(n)}$.
- Cryptographic algorithms are parametrised by a security parameter $\lambda \in \mathbb{N}$. Setting $\lambda = 128$ means achieving 128-bit security.

Indistinguishability Obfuscation (iO)

Definition [BGIRSVY01]

An Indistinguishability Obfuscation (iO) is a pair of algorithms $(\mathsf{Obf}, \mathsf{Eval})$ such that

$$\tilde{\Gamma} \leftarrow \mathsf{Obf}(1^\lambda, \Gamma), \qquad y \leftarrow \mathsf{Eval}(\tilde{\Gamma}, x).$$

- Correctness: For any Γ, $x \in \{0,1\}^n$, $\mathsf{Eval}(\tilde{\Gamma}, x) = \Gamma(x)$.
- Indistinguishability: If $\Gamma_0 \equiv \Gamma_1$ then $\tilde{\Gamma}_0 \approx_c \tilde{\Gamma}_1$.
- Efficiency: $|\tilde{\Gamma}| \leq \mathsf{poly}(|\Gamma|, \lambda)$.

Q: Indistinguishability only for equivalent circuits. Why useful?

A: If $\Gamma_0 \approx_c \Gamma_0^\dagger \equiv \Gamma_1^\dagger \approx_c \Gamma_1$, then $\tilde{\Gamma}_0 \approx_c \tilde{\Gamma}_0^\dagger \approx_c \tilde{\Gamma}_1^\dagger \approx_c \tilde{\Gamma}_1$.

Indistinguishability Obfuscation (iO)

Definition [BGIRSVY01]

An Indistinguishability Obfuscation (iO) is a pair of algorithms $(\mathsf{Obf}, \mathsf{Eval})$ such that

$$\tilde{\Gamma} \leftarrow \mathsf{Obf}(1^{\lambda}, \Gamma), \qquad y \leftarrow \mathsf{Eval}(\tilde{\Gamma}, x).$$

- † Correctness: For any Γ, $x \in \{0,1\}^n$, $\mathsf{Eval}(\tilde{\Gamma}, x) = \Gamma(x)$.
- † Indistinguishability: If $\Gamma_0 \equiv \Gamma_1$ then $\tilde{\Gamma}_0 \approx_c \tilde{\Gamma}_1$.
- † Efficiency: $|\tilde{\Gamma}| \leq \mathsf{poly}(|\Gamma|, \lambda)$.

Q: Indistinguishability only for equivalent circuits. Why useful?

A: If $\Gamma_0 \approx_c \Gamma_0^{\dagger} \equiv \Gamma_1^{\dagger} \approx_c \Gamma_1$, then $\tilde{\Gamma}_0 \approx_c \tilde{\Gamma}_0^{\dagger} \approx_c \tilde{\Gamma}_1^{\dagger} \approx_c \tilde{\Gamma}_1$.

EXponentially-efficient iO (XiO)

- iO is trivial if we drop efficiency requirement:

$$\text{Construction: } \tilde{\Gamma} = \text{TruthTable}(\Gamma).$$

- What if we require $|\tilde{\Gamma}| \leq |\text{TruthTable}(\Gamma)|^{\alpha} \cdot \text{poly}(\lambda)$ with constant $\alpha < 1$?

Definition [LPST16a]

An **EXponentially-efficient iO (XiO)** is a pair of algorithms $(\text{Obf}, \text{Eval})$ such that

$$\tilde{\Gamma} \leftarrow \text{Obf}(1^{\lambda}, \Gamma), \qquad y \leftarrow \text{Eval}(\tilde{\Gamma}, x).$$

- Correctness: For any Γ, $x \in \{0,1\}^n$, $\text{Eval}(\text{Obf}(1^{\lambda}, \Gamma), x) = \Gamma(x)$.
- Indistinguishability: If $\Gamma_0 \equiv \Gamma_1$ then $\text{Obf}(\Gamma_0) \approx_c \text{Obf}(\Gamma_1)$.
- Non-trivial efficiency:
  - $|\tilde{\Gamma}| \leq |\text{TruthTable}(\Gamma)|^{\alpha} \cdot \text{poly}(\lambda)$,
  - $\text{Time}(\text{Obf}) \leq |\text{TruthTable}(\Gamma)| \cdot \text{poly}(\lambda)$.

EXponentially-efficient iO (XiO)

- iO is trivial if we drop efficiency requirement:

$$\text{Construction: } \tilde{\Gamma} = \mathsf{TruthTable}(\Gamma).$$

- What if we require $|\tilde{\Gamma}| \leq |\mathsf{TruthTable}(\Gamma)|^{\alpha} \cdot \mathsf{poly}(\lambda)$ with constant $\alpha < 1$?

Definition [LPST16a]

An **EXponentially-efficient iO (XiO)** is a pair of algorithms $(\mathsf{Obf}, \mathsf{Eval})$ such that

$$\tilde{\Gamma} \leftarrow \mathsf{Obf}(1^{\lambda}, \Gamma), \qquad y \leftarrow \mathsf{Eval}(\tilde{\Gamma}, x).$$

- Correctness: For any Γ, $x \in \{0,1\}^n$, $\mathsf{Eval}(\mathsf{Obf}(1^{\lambda}, \Gamma), x) = \Gamma(x)$.
- Indistinguishability: If $\Gamma_0 \equiv \Gamma_1$ then $\mathsf{Obf}(\Gamma_0) \approx_c \mathsf{Obf}(\Gamma_1)$.
- Non-trivial efficiency:
  - $|\tilde{\Gamma}| \leq |\mathsf{TruthTable}(\Gamma)|^{\alpha} \cdot \mathsf{poly}(\lambda)$,
  - $\mathsf{Time}(\mathsf{Obf}) \leq |\mathsf{TruthTable}(\Gamma)| \cdot \mathsf{poly}(\lambda)$.

XiO to iO

Theorem [LPST16a]

Assume the existence of XiO and the hardness of Learning with Errors (LWE), then iO exists.

The transformation goes through an intermediate notion called Functional Encryption (FE).

Functional Encryption (FE)

Definition

An FE is a tuple of algorithms $(\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ such that

- $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$: Generate master public and secret keys
- $\mathsf{sk}_\Gamma \leftarrow \mathsf{KGen}(\mathsf{msk}, \Gamma)$: Generate functional key for circuit $\Gamma : \{0,1\}^n \to \{0,1\}^m$
- $\mathsf{ctxt}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x)$: Encrypt $x \in \{0,1\}^n$
- $y \leftarrow \mathsf{Dec}(\mathsf{sk}_\Gamma, \mathsf{ctxt}_x)$: Decrypt and supposedly obtain $y = \Gamma(x)$

Security: Given $(\mathsf{sk}_\Gamma, \mathsf{ctxt}_x)$, can only learn $(\Gamma, \Gamma(x))$ but nothing else.

The XiO-to-iO transformation is very sensitive to the efficiency of Enc. We say that FE is ...

- "Sublinear-size" if $|\mathsf{ctxt}_x| \leq |\Gamma|^\alpha \cdot \mathsf{poly}(\lambda)$ and $\mathsf{Time}(\mathsf{Enc}) \leq |\mathsf{TruthTable}(\Gamma)| \cdot \mathsf{poly}(\lambda)$,
- "Sublinear-time" if $\mathsf{Time}(\mathsf{Enc})| \leq |\Gamma|^\alpha \cdot \mathsf{poly}(\lambda)$,
- "Succinct" if $\mathsf{Time}(\mathsf{Enc}) \leq m \cdot \mathsf{poly}(\lambda, \log |\Gamma|)$.

Functional Encryption (FE)

Definition

An FE is a tuple of algorithms $(\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ such that

- $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$: Generate master public and secret keys
- $\mathsf{sk}_\Gamma \leftarrow \mathsf{KGen}(\mathsf{msk}, \Gamma)$: Generate functional key for circuit $\Gamma : \{0,1\}^n \to \{0,1\}^m$
- $\mathsf{ctxt}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x)$: Encrypt $x \in \{0,1\}^n$
- $y \leftarrow \mathsf{Dec}(\mathsf{sk}_\Gamma, \mathsf{ctxt}_x)$: Decrypt and supposedly obtain $y = \Gamma(x)$

Security: Given $(\mathsf{sk}_\Gamma, \mathsf{ctxt}_x)$, can only learn $(\Gamma, \Gamma(x))$ but nothing else.

The XiO-to-iO transformation is very sensitive to the efficiency of Enc. We say that FE is ...

- "Sublinear-size" if $|\mathsf{ctxt}_x| \leq |\Gamma|^\alpha \cdot \mathsf{poly}(\lambda)$ and $\mathsf{Time}(\mathsf{Enc}) \leq |\mathsf{TruthTable}(\Gamma)| \cdot \mathsf{poly}(\lambda)$,
- "Sublinear-time" if $\mathsf{Time}(\mathsf{Enc})| \leq |\Gamma|^\alpha \cdot \mathsf{poly}(\lambda)$,
- "Succinct" if $\mathsf{Time}(\mathsf{Enc}) \leq m \cdot \mathsf{poly}(\lambda, \log|\Gamma|)$.

From XiO to iO

$$
\begin{aligned}
\text{LWE} &\Longrightarrow \text{Succinct FE} \\
\text{Next Talk} &\Longrightarrow \text{XiO} \\
&\overset{\text{Succinct FE}}{\Longrightarrow} \text{Sublinear-size FE} \\
&\overset{\text{Succinct FE}}{\Longrightarrow} \text{Sublinear-time FE} \\
&\overset{\text{recursion}}{\Longrightarrow} \text{iO}
\end{aligned}
$$

From XiO to iO

$$
\begin{aligned}
\text{LWE} &\Longrightarrow \text{Succinct FE} \\
\text{Next Talk} &\Longrightarrow \text{XiO} \\
&\xRightarrow{\text{Succinct FE}} \text{Sublinear-size FE} \\
&\xRightarrow{\text{Succinct FE}} \text{Sublinear-time FE} \\
&\xRightarrow{\text{recursion}} \text{iO}
\end{aligned}
$$

From XiO to iO

$$\text{LWE} \Longrightarrow \text{Succinct FE}$$

$$\text{Next Talk} \Longrightarrow \text{XiO}$$

$$\xRightarrow{\text{Succinct FE}} \text{Sublinear-size FE}$$

$$\xRightarrow{\text{Succinct FE}} \text{Sublinear-time FE}$$

$$\xRightarrow{\text{recursion}} \text{iO}$$

XiO + Succinct FE $\Longrightarrow$ Sublinear-size FE [LPST16a]

Goal: Construct Sublinear-size FE for $\Gamma : \{0,1\}^n \to \{0,1\}^m$.

- Setup(1^λ): Run Setup of SuccinctFE.
- KGen(msk, Γ):
  - Define $\Gamma^\dagger : (x, i) \mapsto i$-th bit of $\Gamma(x)$.
  - Output SuccinctFE secret key $\mathsf{sk}_\Gamma^\dagger$ of $\Gamma^\dagger$.
- Enc(mpk, x):
  - Output XiO $\tilde{\Pi}$ of $\Pi : i \mapsto \mathsf{SuccinctFE.Enc}(\mathsf{mpk}, (x, i))$.
- Dec$(\mathsf{sk}_\Gamma^\dagger, \mathsf{ctxt}_x)$:
  - Run $\mathsf{ctxt}_{x,i} \leftarrow \tilde{\Pi}(i)$ for all i.
  - Output $\mathsf{SuccinctFE.Dec}(\mathsf{sk}_\Gamma^\dagger, \mathsf{ctxt}_{x,i})$ for all i. // $\Gamma^\dagger(x, i) = i$-th bit of $\Gamma(x)$.

XiO + Succinct FE $\Longrightarrow$ Sublinear-size FE [LPST16a]

Goal: Construct Sublinear-size FE for $\Gamma : \{0,1\}^n \to \{0,1\}^m$.

- $\dagger$ $\mathrm{Enc}(\mathrm{mpk}, x)$:
  - $\ddagger$ Output XiO $\tilde{\Pi}$ of $\Pi : i \mapsto \mathrm{SuccinctFE.Enc}(\mathrm{mpk}, (x, i))$.

Proof of sublinear-size ciphertext:

$$
\begin{aligned}
\left|\mathrm{SuccinctFE.Enc}(\mathrm{mpk}, (x, i))\right| &\overset{\text{Succinct}}{\leq} 1 \cdot \mathrm{poly}(\lambda, \log|\Gamma|) \\
\left|\mathrm{TruthTable}(\Pi)\right| &= m \cdot \left|\mathrm{SuccinctFE.Enc}(\mathrm{mpk}, (x, i))\right| \\
&\leq m \cdot \mathrm{poly}(\lambda, \log|\Gamma|) \\
|\tilde{\Pi}| &\overset{\text{XiO}}{\leq} \left|\mathrm{TruthTable}(\Pi)\right|^{\alpha} \cdot \mathrm{poly}(\lambda) \\
&\leq m^{\alpha} \cdot \mathrm{poly}(\lambda, \log|\Gamma|) \\
&\leq |\Gamma|^{\alpha} \cdot \mathrm{poly}(\lambda), \text{ i.e. sublinear-size ciphertext}
\end{aligned}
$$

XiO + Succinct FE $\Longrightarrow$ Sublinear-size FE [LPST16a]

Goal: Construct Sublinear-size FE for $\Gamma : \{0,1\}^n \to \{0,1\}^m$.

- Enc(mpk, x):
  - Output XiO $\tilde{\Pi}$ of $\Pi : i \mapsto \mathsf{SuccinctFE.Enc}(\mathsf{mpk}, (x, i))$.

Proof of sublinear-size ciphertext:

$$
\begin{aligned}
|\mathsf{SuccinctFE.Enc}(\mathsf{mpk},(x,i))| &\overset{\text{Succinct}}{\leq} 1 \cdot \mathrm{poly}(\lambda, \log|\Gamma|) \\
|\mathsf{TruthTable}(\Pi)| &= m \cdot |\mathsf{SuccinctFE.Enc}(\mathsf{mpk},(x,i))| \\
&\leq m \cdot \mathrm{poly}(\lambda, \log|\Gamma|) \\
|\tilde{\Pi}| &\overset{\text{XiO}}{\leq} |\mathsf{TruthTable}(\Pi)|^{\alpha} \cdot \mathrm{poly}(\lambda) \\
&\leq m^{\alpha} \cdot \mathrm{poly}(\lambda, \log|\Gamma|) \\
&\leq |\Gamma|^{\alpha} \cdot \mathrm{poly}(\lambda), \text{ i.e. sublinear-size ciphertext}
\end{aligned}
$$

From XiO to iO

$$
\begin{aligned}
\text{LWE} &\Longrightarrow \text{Succinct FE} \\
\text{Next Talk} &\Longrightarrow \text{XiO} \\
&\xrightarrow{\text{Succinct FE}} \text{Sublinear-size FE} \\
&\xrightarrow{\text{Succinct FE}} \text{Sublinear-time FE} \\
&\xrightarrow{\text{recursion}} \text{iO}
\end{aligned}
$$

Sublinear-size FE + Succinct FE $\Longrightarrow$ Sublinear-time FE [LPST16b]

Goal: Construct Sublinear-time FE for $\Gamma : \{0,1\}^n \to \{0,1\}^m$.

- Setup(1^λ): Run Setup of SuccinctFE and SSizeFE.
- KGen(msk, Γ):
  - Generate SuccinctFE key $\mathsf{sk}_{\mathsf{Enc}}$ for $x \mapsto \mathsf{SSizeFE.Enc}(\mathsf{mpk}, x)$.
  - Generate SSizeFE key $\mathsf{sk}_\Gamma^\dagger$ for $x \mapsto \Gamma(x)$.
- Enc(mpk, x): Output SuccinctFE.Enc(mpk, x).
- Dec$(\mathsf{sk}_\Gamma, \mathsf{ctxt}_x)$:
  - Use SuccinctFE key $\mathsf{sk}_{\mathsf{Enc}}$ on ctxt_x to obtain an SSizeFE ciphertext $\mathsf{ctxt}_x^\dagger$.
  - Use SSizeFE key $\mathsf{sk}_\Gamma^\dagger$ on $\mathsf{ctxt}_x^\dagger$ to obtain $\Gamma(x)$.

Sublinear-size FE + Succinct FE $\implies$ Sublinear-time FE [LPST16b]

Goal: Construct Sublinear-time FE for $\Gamma : \{0,1\}^n \to \{0,1\}^m$ where $n \leq \mathrm{poly}(\lambda)$.

- $\mathsf{KGen}(\mathsf{msk}, \Gamma)$:
  - Generate SuccinctFE key $\mathsf{sk}_{\mathsf{Enc}}$ for $x \mapsto \mathsf{SSizeFE.Enc}(\mathsf{mpk}, x)$.
  - Generate SSizeFE key $\mathsf{sk}^{\dagger}_{\Gamma}$ for $x \mapsto \Gamma(x)$.
- $\mathsf{Enc}(\mathsf{mpk}, x)$: Output $\mathsf{SuccinctFE.Enc}(\mathsf{mpk}, x)$.

Proof of sublinear-time encryption:

$$|\mathsf{SSizeFE.Enc}(\mathsf{mpk}, x)| \overset{\text{SublinSize}}{\leq} |\Gamma|^{\alpha} \cdot \mathrm{poly}(\lambda) \ \ \forall x$$

$$\mathsf{Time}(\mathsf{SSizeFE.Enc}) \overset{\text{SublinSize}}{\leq} |\mathsf{TruthTable}(\Gamma)| \cdot \mathrm{poly}(\lambda)$$

$$\begin{aligned}\mathsf{Time}(\mathsf{SuccinctFE.Enc}) &\overset{\text{Succinct}}{\leq} |\mathsf{SSizeFE.Enc}(\mathsf{mpk}, x)| \cdot \mathrm{poly}(\lambda, \log \mathsf{Time}(\mathsf{SSizeFE.Enc})) \\ &\leq |\Gamma|^{\alpha} \cdot \mathrm{poly}(\lambda, \log |\mathsf{TruthTable}(\Gamma)|) \\ &\leq |\Gamma|^{\alpha} \cdot \mathrm{poly}(\lambda), \text{ i.e. sublinear-time encryption}\end{aligned}$$

Sublinear-size FE + Succinct FE $\implies$ Sublinear-time FE [LPST16b]

Goal: Construct Sublinear-time FE for $\Gamma : \{0,1\}^n \to \{0,1\}^m$ where $n \leq \text{poly}(\lambda)$.

- † $\mathsf{KGen}(\mathsf{msk}, \Gamma)$:
  - ‡ Generate SuccinctFE key $\mathsf{sk}_{\mathsf{Enc}}$ for $x \mapsto \mathsf{SSizeFE.Enc}(\mathsf{mpk}, x)$.
  - ‡ Generate SSizeFE key $\mathsf{sk}_\Gamma^\dagger$ for $x \mapsto \Gamma(x)$.
- † $\mathsf{Enc}(\mathsf{mpk}, x)$: Output $\mathsf{SuccinctFE.Enc}(\mathsf{mpk}, x)$.

Proof of sublinear-time encryption:

$$\left|\mathsf{SSizeFE.Enc}(\mathsf{mpk}, x)\right| \overset{\text{SublinSize}}{\leq} |\Gamma|^\alpha \cdot \text{poly}(\lambda) \;\; \forall x$$

$$\mathsf{Time}(\mathsf{SSizeFE.Enc}) \overset{\text{SublinSize}}{\leq} \left|\mathsf{TruthTable}(\Gamma)\right| \cdot \text{poly}(\lambda)$$

$$\begin{aligned}\mathsf{Time}(\mathsf{SuccinctFE.Enc}) &\overset{\text{Succinct}}{\leq} \left|\mathsf{SSizeFE.Enc}(\mathsf{mpk}, x)\right| \cdot \text{poly}(\lambda, \log \mathsf{Time}(\mathsf{SSizeFE.Enc})) \\ &\leq |\Gamma|^\alpha \cdot \text{poly}(\lambda, \log \left|\mathsf{TruthTable}(\Gamma)\right|) \\ &\leq |\Gamma|^\alpha \cdot \text{poly}(\lambda), \text{ i.e. sublinear-time encryption}\end{aligned}$$

From XiO to iO

$$
\begin{aligned}
\text{LWE} &\Longrightarrow \text{Succinct FE}\\
\text{Next Talk} &\Longrightarrow \text{XiO}\\
&\overset{\text{Succinct FE}}{\Longrightarrow} \text{Sublinear-size FE}\\
&\overset{\text{Succinct FE}}{\Longrightarrow} \text{Sublinear-time FE}\\
&\overset{\text{recursion}}{\Longrightarrow} \text{iO}
\end{aligned}
$$

Sublinear-time FE $\Longrightarrow$ iO [BV15; AJ15; LPST16b]

Goal: Construct iO for $\Gamma : \{0,1\}^n \to \{0,1\}^m$.

- $\mathsf{Obf}(1^\lambda, \Gamma)$:
  - Set up $n+1$ STimeFE key pairs. Generate $\mathsf{ctxt}_\epsilon \leftarrow \mathsf{Enc}^{(0)}(\mathsf{mpk}^{(0)}, \Gamma)$.
  - For $0 \le i < n$, generate a function key $\mathsf{sk}^{(i)}_{\mathsf{Enc}}$ for the following function:

$$(\Gamma, x_{[1:i]}) \mapsto (\mathsf{Enc}^{(i+1)}(\mathsf{mpk}^{(i+1)}, (\Gamma, x_{[1:i]} \| 0)), \mathsf{Enc}^{(i+1)}(\mathsf{mpk}^{(i+1)}, (\Gamma, x_{[1:i]} \| 1)))$$

  - Generate a function key $\mathsf{sk}^{(n)}_U$ for the universal circuit $U : (\Gamma, x) \mapsto \Gamma(x)$.
  - Output $(\mathsf{ctxt}_\epsilon, \mathsf{sk}^{(0)}_{\mathsf{Enc}}, \ldots, \mathsf{sk}^{(1)}_{\mathsf{Enc}}, \mathsf{sk}^{(n)}_U)$.
- $\mathsf{Eval}(\tilde{\Gamma}, x)$:
  - For $0 \le i < n$, run $\mathsf{ctxt}_{\Gamma, x_{[1:i+1]}} \leftarrow \mathsf{Dec}^{(i)}(\mathsf{sk}^{(i)}_{\mathsf{Enc}}, \mathsf{ctxt}_{\Gamma, x_{[1:i]}})$.
  - Output $y \leftarrow \mathsf{Dec}^{(n)}(\mathsf{sk}^{(n)}_U, \mathsf{ctxt}_{\Gamma, x})$.

Sublinear-time FE $\implies$ iO [BV15; AJ15; LPST16b]

- $\mathsf{Obf}(1^\lambda, \Gamma)$:
  - Set up $n+1$ STimeFE key pairs. Generate $\mathsf{ctxt}_\epsilon \leftarrow \mathsf{Enc}^{(0)}(\mathsf{mpk}^{(0)}, \Gamma)$.
  - For $0 \le i < n$, generate a function key $\mathsf{sk}^{(i)}_{\mathsf{Enc}}$ for the following function:

$$(\Gamma, x_{[1:i]}) \mapsto (\mathsf{Enc}^{(i+1)}(\mathsf{mpk}^{(i+1)}, (\Gamma, x_{[1:i]} \| 0)), \mathsf{Enc}^{(i+1)}(\mathsf{mpk}^{(i+1)}, (\Gamma, x_{[1:i]} \| 1)))$$

  - Generate a function key $\mathsf{sk}^{(n)}_U$ for the universal circuit $U : (\Gamma, x) \mapsto \Gamma(x)$.

Proof of efficiency:

$$\mathsf{Time}(\mathsf{Enc}^{(n)}) \overset{\text{SublinTime}}{\le} |U|^{\alpha^\dagger} \cdot \mathsf{poly}(\lambda) \le |\Gamma|^{\alpha} \cdot \mathsf{poly}(\lambda)$$

$$\mathsf{Time}(\mathsf{Enc}^{(n-1)}) \overset{\text{SublinTime}}{\le} \mathsf{Time}(\mathsf{Enc}^{(n)})^{\alpha} \cdot \mathsf{poly}(\lambda) = (|\Gamma|^{\alpha} \cdot \mathsf{poly}(\lambda))^{\alpha} \cdot \mathsf{poly}(\lambda) = |\Gamma|^{\alpha^2} \cdot \mathsf{poly}(\lambda)^{1+\alpha}$$

$$\mathsf{Time}(\mathsf{Enc}^{(0)}) \overset{\text{SublinTime}}{\le} |\Gamma|^{\alpha^{n+1}} \cdot \mathsf{poly}(\lambda)^{1+\alpha+\ldots+\alpha^n} \le |\Gamma|^{\alpha^{n+1}} \cdot \mathsf{poly}(\lambda)^{1/(1-\alpha)} \le \mathsf{poly}(\lambda)$$

Take Away

$$\begin{aligned} \text{LWE} &\implies \text{Succinct FE} \\ \text{Next Talk} &\implies \text{XiO} \\ &\xRightarrow{\text{Succinct FE}} \text{Sublinear-size FE} \\ &\xRightarrow{\text{Succinct FE}} \text{Sublinear-time FE} \\ &\xRightarrow{\text{recursion}} \text{iO} \end{aligned}$$

or

Size compression $\implies$ *time compression* $\implies$ *iO.*

Russell W. F. Lai
Aalto University, Finland
russell.lai@aalto.fi

russell-lai.hk
research.cs.aalto.fi/crypto

Thank You!

References I

[AJ15] Prabhanjan Ananth and Abhishek Jain. “Indistinguishability Obfuscation from Compact Functional Encryption”. In: *CRYPTO 2015, Part I*. 2015 (pages 2–4, 25, 26).

[AJLMS19] Prabhanjan Ananth, Aayush Jain, Huijia Lin, Christian Matt, and Amit Sahai. “Indistinguishability Obfuscation Without Multilinear Maps: New Paradigms via Low Degree Weak Pseudorandomness and Security Amplification”. In: *CRYPTO 2019, Part III*. 2019 (pages 2–4).

[BDGM20] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. “Candidate iO from Homomorphic Encryption Schemes”. In: *EUROCRYPT 2020, Part I*. 2020 (pages 2–4).

[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*. 2022 (pages 2–4).

[BGIRSVY01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. “On the (Im)possibility of Obfuscating Programs”. In: *CRYPTO 2001*. 2001 (pages 2–4, 7, 8).

References II

[BV15] Nir Bitansky and Vinod Vaikuntanathan. "Indistinguishability Obfuscation from Functional Encryption". In: *56th FOCS*. 2015 (pages 2–4, 25, 26).

[CLW25] Valerio Cini, Russell W. F. Lai, and Ivy K. Y. Woo. "Lattice-Based Obfuscation from NTRU and Equivocal LWE". In: *Advances in Cryptology – CRYPTO 2025*. 2025 (pages 2–4).

[DQVWW21] Lalita Devadas, Willy Quach, Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. "Succinct LWE Sampling, Random Polynomials, and Obfuscation". In: *TCC 2021, Part II*. 2021 (pages 2–4).

[GGHRSW13] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. "Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits". In: *54th FOCS*. 2013 (pages 2–4).

[GP21] Romain Gay and Rafael Pass. "Indistinguishability obfuscation from circular security". In: *53rd ACM STOC*. 2021 (pages 2–4).

[HJL21] Samuel B. Hopkins, Aayush Jain, and Huijia Lin. "Counterexamples to New Circular Security Assumptions Underlying iO". In: *CRYPTO 2021, Part II*. 2021 (pages 2–4).

References III

[HJL25] Yao-Ching Hsieh, Aayush Jain, and Huijia Lin. “Lattice-Based Post-quantum iO from Circular Security with Random Opening Assumption”. In: *Advances in Cryptology – CRYPTO 2025*. 2025 (pages 2–4).

[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*. 2023 (pages 2–4).

[JLS21] Aayush Jain, Huijia Lin, and Amit Sahai. “Indistinguishability obfuscation from well-founded assumptions”. In: *53rd ACM STOC*. 2021 (pages 2–4).

[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*. 2022 (pages 2–4).

[Lin17] Huijia Lin. “Indistinguishability Obfuscation from SXDH on 5-Linear Maps and Locality-5 PRGs”. In: *CRYPTO 2017, Part I*. 2017 (pages 2–4).

[LPST16a] Huijia Lin, Rafael Pass, Karn Seth, and Sidharth Telang. “Indistinguishability Obfuscation with Non-trivial Efficiency”. In: *PKC 2016, Part II*. 2016 (pages 2–4, 9–11, 17–19).

References IV

[LPST16b] Huijia Lin, Rafael Pass, Karn Seth, and Sidharth Telang. "Output-Compressing Randomized Encodings and Applications". In: *TCC 2016-A, Part I*. 2016 (pages 2–4, 21–23, 25, 26).

[LT17] Huijia Lin and Stefano Tessaro. "Indistinguishability Obfuscation from Trilinear Maps and Block-Wise Local PRGs". In: *CRYPTO 2017, Part I*. 2017 (pages 2–4).

[LV16] Huijia Lin and Vinod Vaikuntanathan. "Indistinguishability Obfuscation from DDH-Like Assumptions on Constant-Degree Graded Encodings". In: *57th FOCS*. 2016 (pages 2–4).

[SW14] Amit Sahai and Brent Waters. "How to use indistinguishability obfuscation: deniable encryption, and more". In: *46th ACM STOC*. 2014 (pages 2–4).

[WW21] Hoeteck Wee and Daniel Wichs. "Candidate Obfuscation via Oblivious LWE Sampling". In: *EUROCRYPT 2021, Part III*. 2021 (pages 2–4).