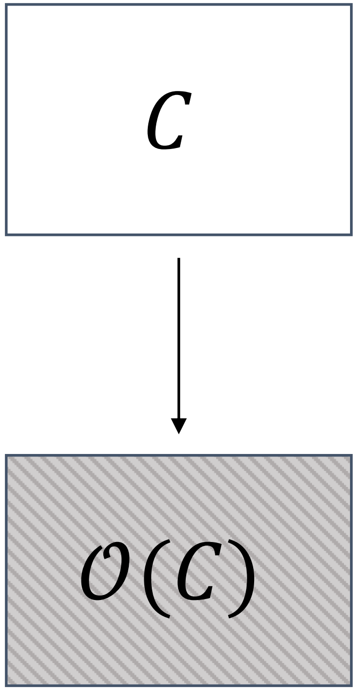
Obfuscation of Pseudo-Deterministic Quantum Circuits

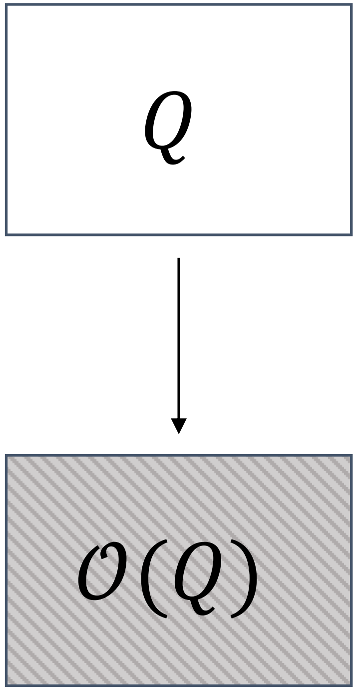
James Bartusek	UC Berkeley
Fuyuki Kitagawa	NTT Social Informatics Laboratories
Ryo Nishimaki	NTT Social Informatics Laboratories
Takashi Yamakawa	NTT Social Informatics Laboratories

Background: Classical obfuscation



- Scrambles a program to hide implementation details, while maintaining functionality
- A basic tool for *software protection*: useful against reverse-engineering, intellectual property theft, and piracy
- Indistinguishability obfuscation ($\forall\ C_1 \equiv C_2,\ \mathcal{O}(C_1) \approx_c \mathcal{O}(C_2)$) has become a “central hub” of cryptography: Fully-homomorphic encryption, functional encryption, public-key quantum money…
- Known from (pre-quantum) well-founded assumptions …, [Jain, Lin, Sahai 21], and exist post-quantum candidates

Background: Quantum obfuscation



- Definitions, impossibilities, applications [Alagic, Fefferman 16]
- Constructions:
  - Perfect obfuscation for limited circuit classes [Alagic, Jeffrey, Jordan 14], [Broadbent, Kazmi 20]
  - Obfuscation for circuits with logarithmically many non-Clifford gates, from post-quantum classical iO [BK20]
  - Obfuscation for null quantum circuits (and applications) in the classical oracle model [**B**, Malavolta 22]

Is it possible to obfuscate general-purpose quantum computation?

Main Result

Obfuscation of polynomial-size **pseudo-deterministic quantum circuits** in the classical oracle model (assuming learning with errors)

Pseudo-deterministic quantum circuit Q:

- Classical inputs and outputs
- For each input x, exists y s.t. $\mathrm{Pr}[Q(x) = y] = 1 - \mathrm{negl}$

Prominent example: Shor's algorithm

Main Result

Obfuscation of polynomial-size **pseudo-deterministic quantum circuits** in the classical oracle model (assuming learning with errors)

$$\mathrm{QuObf}(Q) \longrightarrow |\psi_Q\rangle, \mathrm{ClObf}(f_Q)$$

$$\mathrm{Eval}(|\psi_Q\rangle, \mathrm{ClObf}(f_Q), x) \longrightarrow Q(x)$$

$$\boxed{\mathrm{Adv}^{f_Q}(|\psi_Q\rangle) \approx \mathrm{Sim}^Q} \longleftarrow$$

Black-box obfuscation of Q

Main Result

Obfuscation of polynomial-size **pseudo-deterministic quantum circuits** in the classical oracle model (assuming learning with errors)

Candidate indistinguishability obfuscation of Q : $|\psi_Q\rangle, \mathrm{iO}(f_Q)$

$$\boxed{\mathrm{Adv}^{f_Q}(|\psi_Q\rangle) \approx \mathrm{Sim}^Q} \longleftarrow$$

Black-box obfuscation of Q

Main Result

Obfuscation of polynomial-size **pseudo-deterministic quantum circuits** in the classical oracle model (assuming learning with errors)

Applications
- Functional encryption for pseudo-deterministic quantum circuits
- Copy-protection for pseudo-deterministic quantum circuits

Starting point: Quantum fully-homomorphic encryption [Mahadev 18]

$$\mathrm{ct}_Q = \mathrm{Enc}(Q), x \xrightarrow{\text{Eval}} \mathrm{ct}_{Q(x)} = \mathrm{Enc}(Q(x))$$

$$\Downarrow$$

Can't give out sk in the clear

$$\mathrm{QuObf}(Q): \quad \mathrm{ct}_Q = \mathrm{Enc}(Q), \mathrm{ClObf}(\mathrm{P}_{\mathrm{Ver-then-decrypt}}[\mathrm{ct}_Q, \mathrm{sk}])$$

$\mathrm{P}_{\mathrm{Ver-then-decrypt}}[\mathrm{ct}_Q, \mathrm{sk}]$:

- Take $(x, \mathrm{ct}_{Q(x)}, \pi)$ as input
- Check that π is a proof that $\mathrm{ct}_{Q(x)} \leftarrow \mathrm{Eval}(\mathrm{ct}_Q, x)$
- If so, output $\mathrm{Dec}(\mathrm{sk}, \mathrm{ct}_{Q(x)})$

Main building block: Publicly-verifiable QFHE

- $\mathrm{Gen} \to (\mathrm{pk}, \mathrm{sk})$
- $\mathrm{Enc}(\mathrm{pk}, Q) \to \mathrm{ct}_Q, \mathrm{vk}$
- $\mathrm{Eval}(\mathrm{vk}, \mathrm{ct}_Q, x) \to \mathrm{ct}_{Q(x)}, \pi$
- $\boxed{\mathrm{Ver}(\mathrm{vk}, \mathrm{ct}_Q, x, \mathrm{ct}_{Q(x)}, \pi) \to \top/\bot}$
- $\mathrm{Dec}(\mathrm{sk}, \mathrm{ct}_{Q(x)}) \to Q(x)$

Must be classical

Soundness: for any QPT adversary $\mathrm{Adv}(\mathrm{vk}, \mathrm{ct}_Q) \to (x, \mathrm{ct}_{Q(x)}, \pi)$, if Ver accepts then $\mathrm{Dec}(\mathrm{sk}, \mathrm{ct}_{Q(x)}) = Q(x)$

[Alagic, Dulek, Schaffner, Speelman 17] VQFHE?

[Mahadev 18] classical verification?

Why is prior work insufficient?

1. [ADSS17] verification requires the QFHE secret key

2. [Mah18]
   - Not publicly verifiable
   - Only applies to *(pseudo)-deterministic* quantum computation (BQP)
   - Even if Q is (pseudo)-deterministic, $\mathrm{ct}_{Q(x)} \leftarrow \mathrm{Eval}(\mathrm{ct}_Q, x)$ is a randomized (sampBQP) computation

3. [Chung, Lee, Lin, Wu 22] construct classical verification for sampBQP computation, but with $1/\mathrm{poly}$ soundness

Improving on this is a nice open problem

High-level approach

QFHE evaluator with (ct_Q, x) interacts with classical oracle to produce output $\mathrm{ct}_{Q(x)}$ and proof π

1. Let $|\psi_x\rangle$ be the history state of the QFHE computation $(\mathrm{ct}_Q, x) \to \mathrm{ct}_{Q(x)}$. Evaluator commits to (many copies of) $|\psi_x\rangle$ using a *Pauli Functional Commitment* scheme.
   - Classical commitment to quantum state that supports opening to Z and X measurements
   - Used to overcome the issue that measurement protocol in Step 2 is not reusably sound
   - Require a "publicly-decodable" version: extend the [Brakerski, Christiano, Mahadev, Vazirani, Vidick 18] framework to support high-dimensional coset states

2. Evaluator and oracle interact to run a *measurement protocol* [Mah18, ACGH20, CLLW22, **B**21] on the copies of $|\psi_x\rangle$. Oracle obtains local Hamiltonian measurements from some copies and output samples $\{\mathrm{ct}^i_{Q(x)}\}_i$ from the others.

3. Oracle runs Hamiltonian verifier. If accepts, oracle runs Majority under QFHE $\{\mathrm{ct}^i_{Q(x)}\}_i \to \mathrm{ct}_{Q(x)}$ and returns $\mathrm{ct}_{Q(x)}$. Proof π: transcript between evaluator and oracle.

Open Problems

- The commitment key for our Pauli functional commitment is quantum. Can we make this classical?
- Can we prove security from (post-quantum) indistinguishability obfuscation?
- Can we obfuscate larger classes of quantum circuits?
  - Quantum sampling circuits?
  - Quantum maps?