Workshop on cryptography in the quantum age, Tuesday, 6 Nov 2018

Towards obfuscation using quantum homomorphic encryption

Christian Schaffner (QuSoft)

based on work-in-progress
with Gorjan Alagic,
Yfke Dulek, and
Florian Speelman

Suppose you find a fast algorithm for a hard problem.

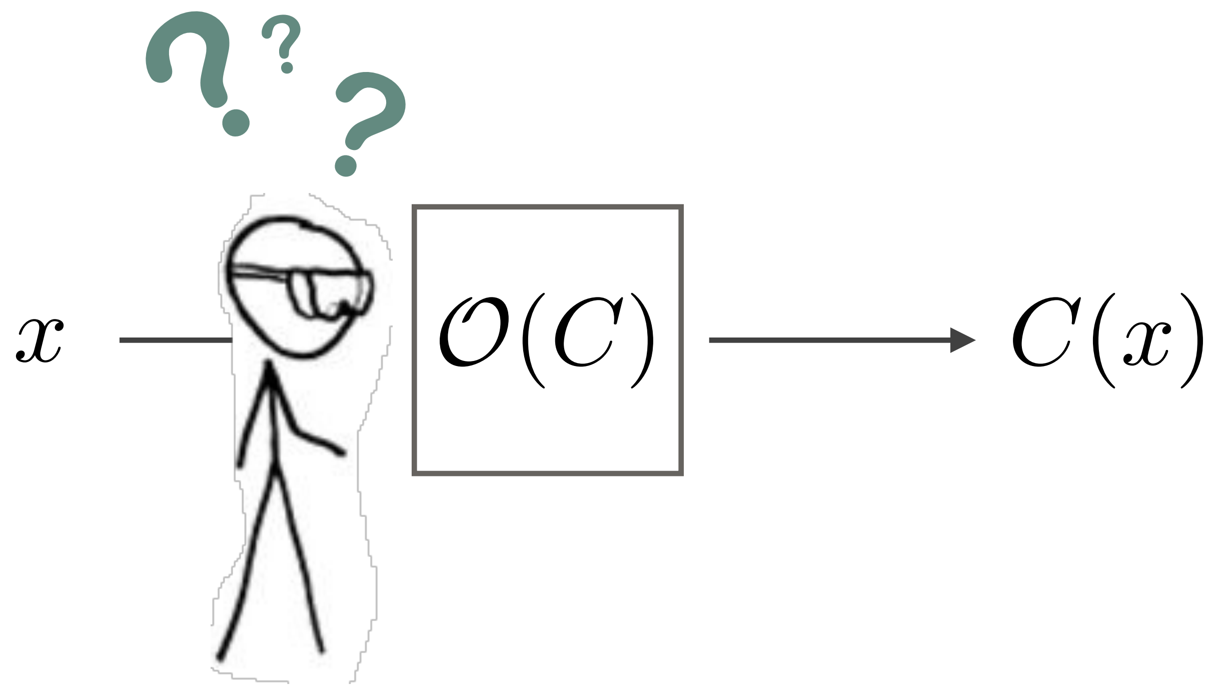
What do you do?

publish it!

or not?

obfuscation $\mathcal{O}(C)$ of a circuit C: an object that

- allows the efficient evaluation of C on any input
- reveals no information about C, except for what can be learned from oracle access to f_C



notoriously difficult to obtain in theory and practice

Outline

1. Obfuscation: definitions and (im)possibilities
2. Obfuscation from homomorphic encryption
3. The quantum story (work in progress)

1. Obfuscation:
definitions and (im)possibilities

Obfuscation: two definitions

- **Virtual black box**: for any PPT $\mathcal{A}$, there exists a PPT simulator $\mathcal{S}$ such that for all $C \in \mathfrak{C}$:

$$\left|\Pr[\mathcal{A}(\mathcal{O}(C)) = 1] - \Pr[\mathcal{S}^{C}(1^{|C|}) = 1]\right| \leq \mathrm{negl}(|C|)$$

  - impossible even for $\mathfrak{C} = \mathsf{TC}^0$ [BGI+01]

- **Indistinguishability** (iO): $\mathcal{O}(C)$ is indistinguishable from $\mathcal{O}(C')$ whenever $f_C = f_{C'}$

  - more promising (computationally) [GGH+13]

[BGI+01] Barak et al. On the (im)possibility of obfuscating programs (CRYPTO 2001)
[GGH+13] Garg et al. Candidate indistinguishability obfuscation and functional encryption for all circuits (FOCS 2013)

Why study black-box obfuscation?

- Impossible only if we assume $\mathcal{O}(C)$ is classical
  - It might still be possible to obfuscate a (classical) circuit C into a quantum state $\mathcal{O}(C)$
  - Related attempt: [AC12]
- Strongest definition (has the most applications)
- Cleanest definition (is easiest to work with)

[AC12] Aaronson and Christiano. Quantum money from hidden subspaces (Theory of Computing 2012)

2. Obfuscation from homomorphic encryption

Obfuscation for $\mathfrak{C}$ = P: ingredients

impossible, since $TC^0 \subseteq NC^1$

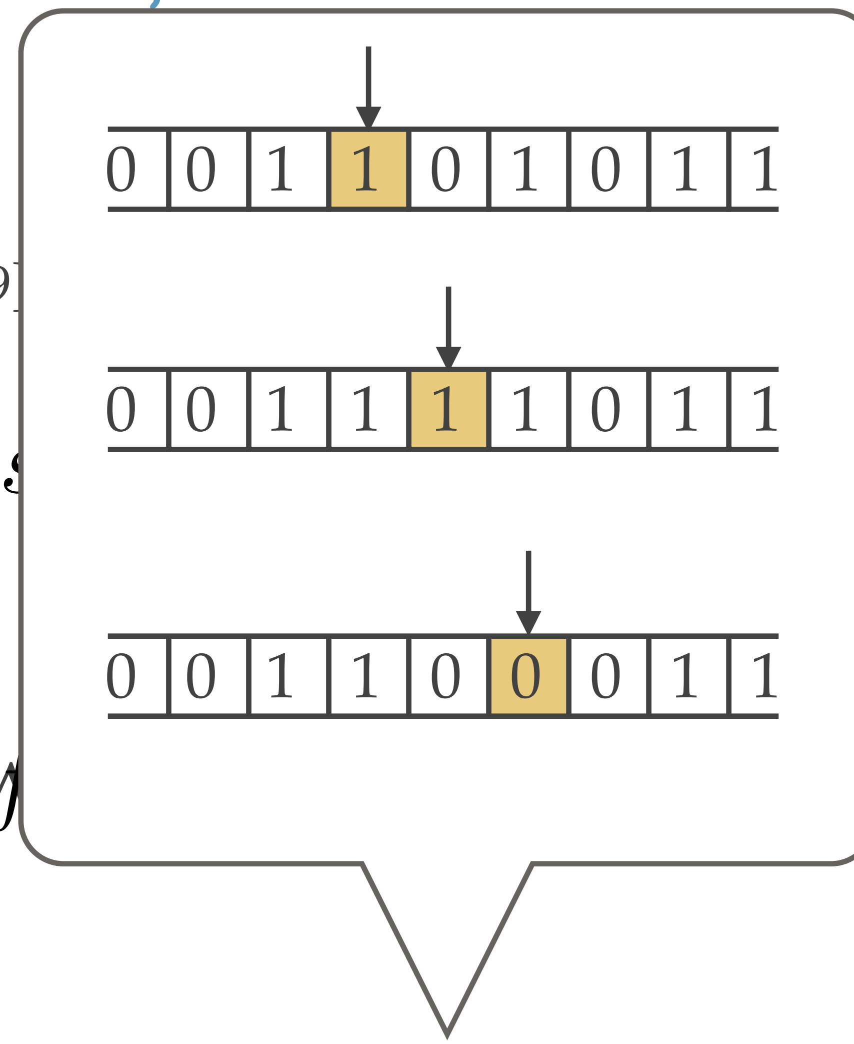
1. obfuscation for $\mathfrak{C} = \mathsf{NC}^1$

2. homomorphic encryption [Gen09]

KeyGen generates secret key s

Enc_{pk} anyone can encrypt

Dec_{sk} / Eval_{f} takes $\mathsf{Enc}(x)$ to $\mathsf{Enc}(y$



special requirements: verification (VerDec_{sk})

efficiency (VerDec_{sk} is NC^1)

[Gen09] Gentry. A fully homomorphic encryption scheme. (CRYPTO 2009)

Obfuscation for $\mathfrak{C} = \mathsf{P}$: construction

Definition

For all poly-size circuits C, define

$$\mathcal{O}_{\mathsf{P}}(C) := \left(\ (\mathsf{Enc}(C),\ \mathcal{O}_{\mathsf{NC}^1}(\mathsf{VerDec}) \ \right)$$

Usage

1. Encrypt your input: $\mathsf{Enc}(x)$

2. Compute $\mathsf{Eval}_{\mathsf{universal\_circuit}}(\mathsf{Enc}(C), \mathsf{Enc}(x)) \ = \ \mathsf{Enc}(C(x))$

3. Decrypt the result using $\mathcal{O}_{\mathsf{NC}^1}(\mathsf{VerDec})$

[BR14] Brakerski and Rothblum. Virtual black-box obfuscation for all circuits via generic graded encoding (Theory of Computing 2014)

Obfuscation for $\mathfrak{C}$ = P: security

- Recall security definition (virtual black box): for any PPT $\mathcal{A}$, there exists a PPT simulator $\mathcal{S}$ such that for all $C \in \mathfrak{C}$:

$$\left|\Pr[\mathcal{A}(\mathcal{O}(C)) = 1] - \Pr[S^C(1^{|C|}) = 1]\right| \leq \mathrm{negl}(|C|)$$

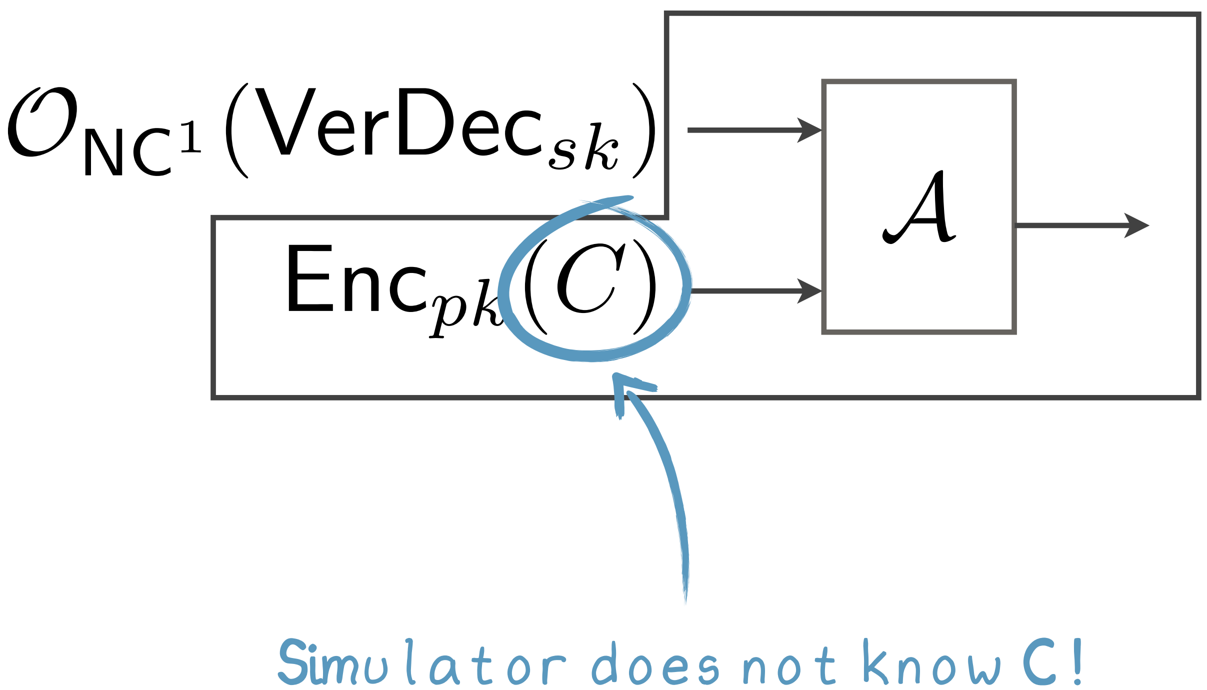
- Proof strategy: construct a simulator that trivially mimics $\mathcal{A}$, but that cannot exist. Then make several small changes ("hybrids") until it can exist.

Obfuscation for $\mathfrak{C} = \mathsf{P}$: security

Given adversary $\mathcal{A}$ for P-obfuscation, design simulator:

(1) $sk, pk \leftarrow \mathsf{KeyGen}$

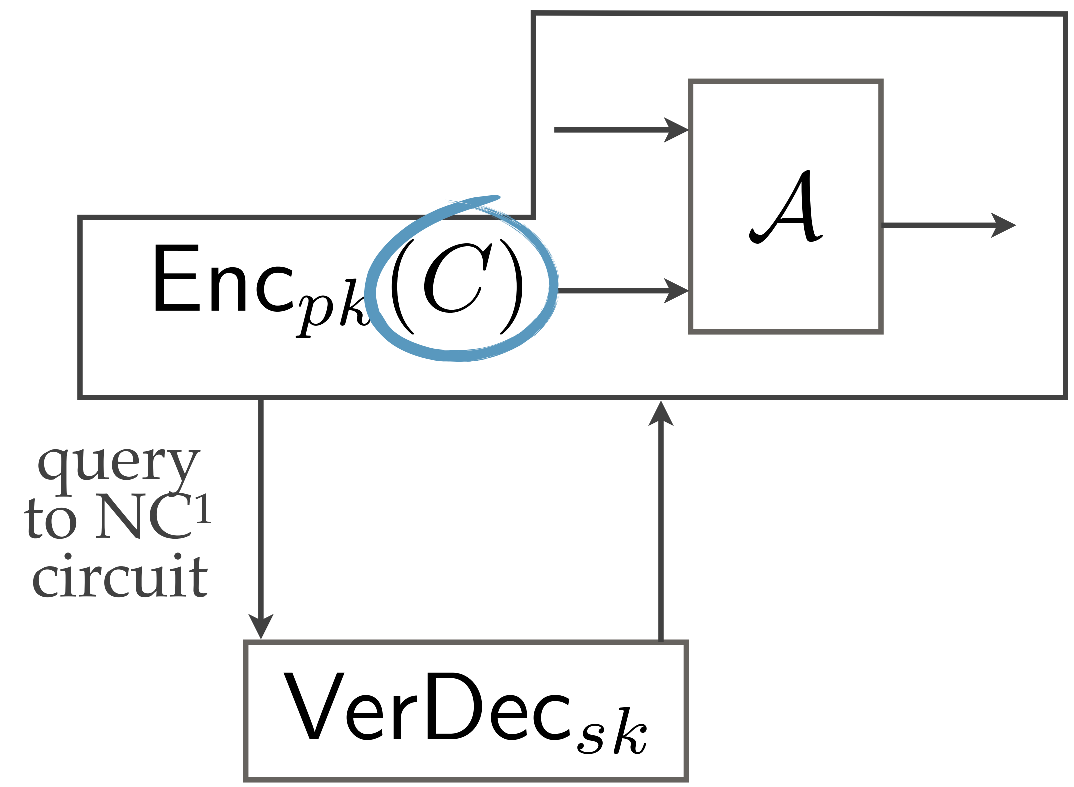
(2) Run the adv against NC¹ obf:



and output whatever it outputs

(1) $sk, pk \leftarrow \mathsf{KeyGen}$

(2) Run the NC¹ simulator for:



and output whatever it outputs

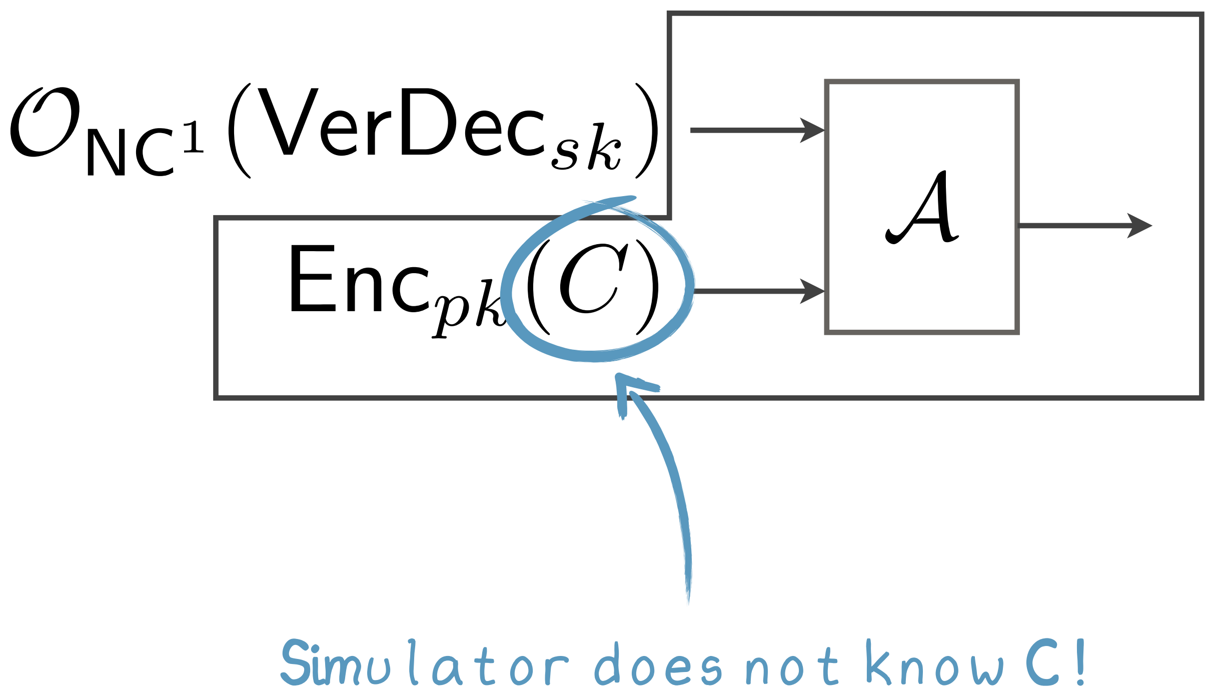
Indistinguishable by black-box obfuscation of NC¹

Obfuscation for $\mathfrak{C}$ = P: security

Given adversary $\mathcal{A}$ for P-obfuscation, design simulator:

(1) $sk, pk \leftarrow \mathsf{KeyGen}$

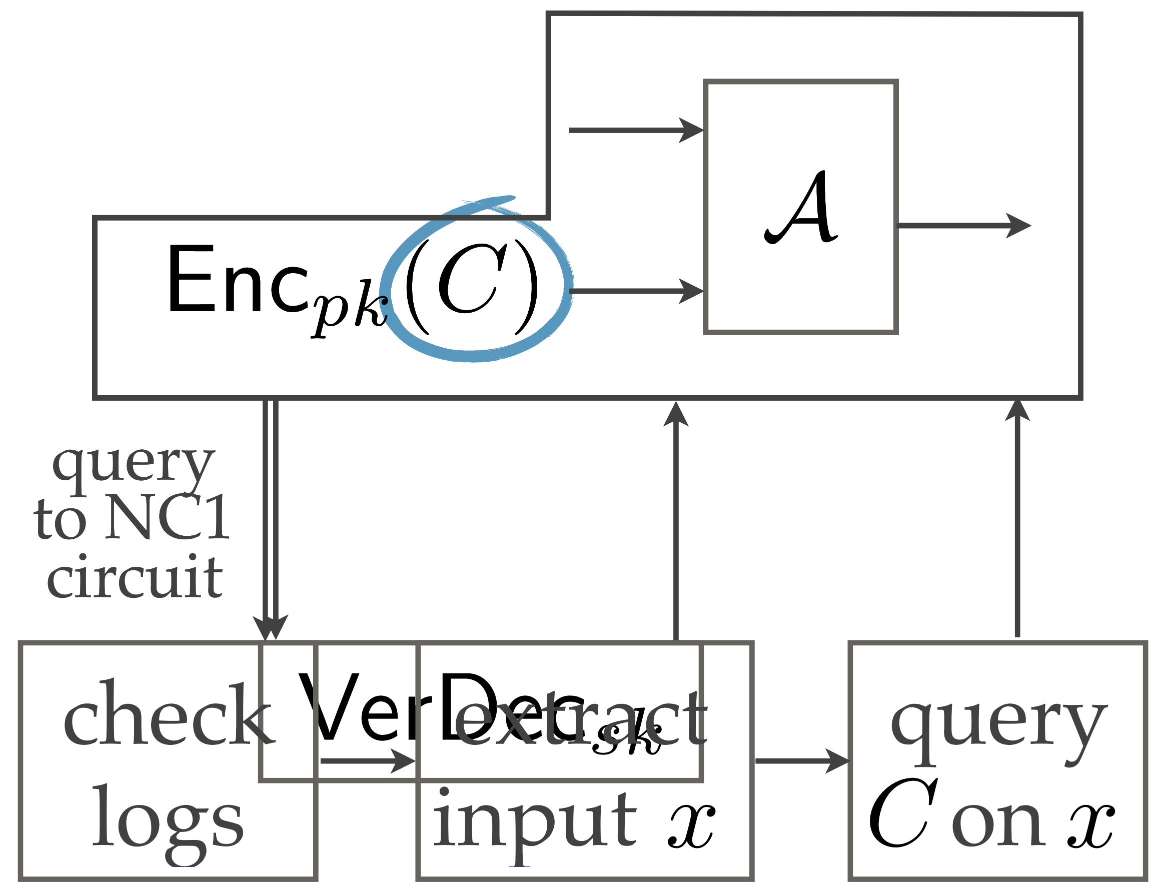
(2) Run the adv against NC¹ obf:



and output whatever it outputs

(1) $sk, pk \leftarrow \mathsf{KeyGen}$

(2) Run the NC¹ simulator for:



and output whatever it outputs

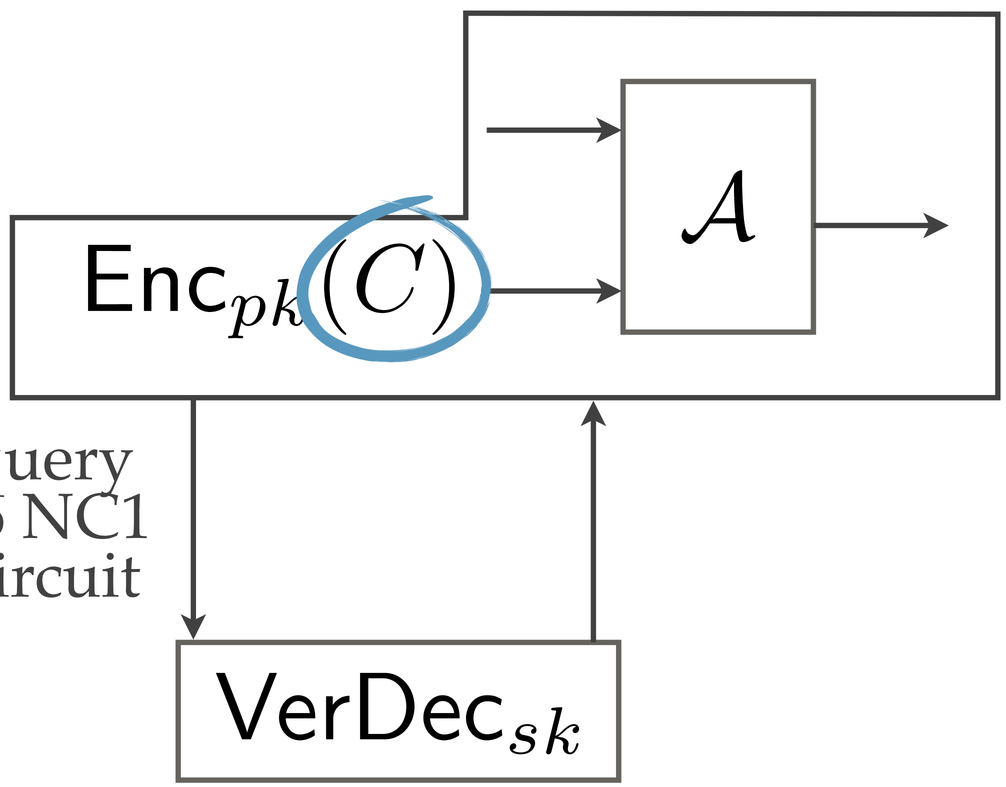
Indistinguishable by correctness of homomorphic encryption

Obfuscation for $\mathfrak{C} =$ P: security

Given adversary $\mathcal{A}$ for P-obfuscation, design simulator:

(1) $sk, pk \leftarrow$ KeyGen

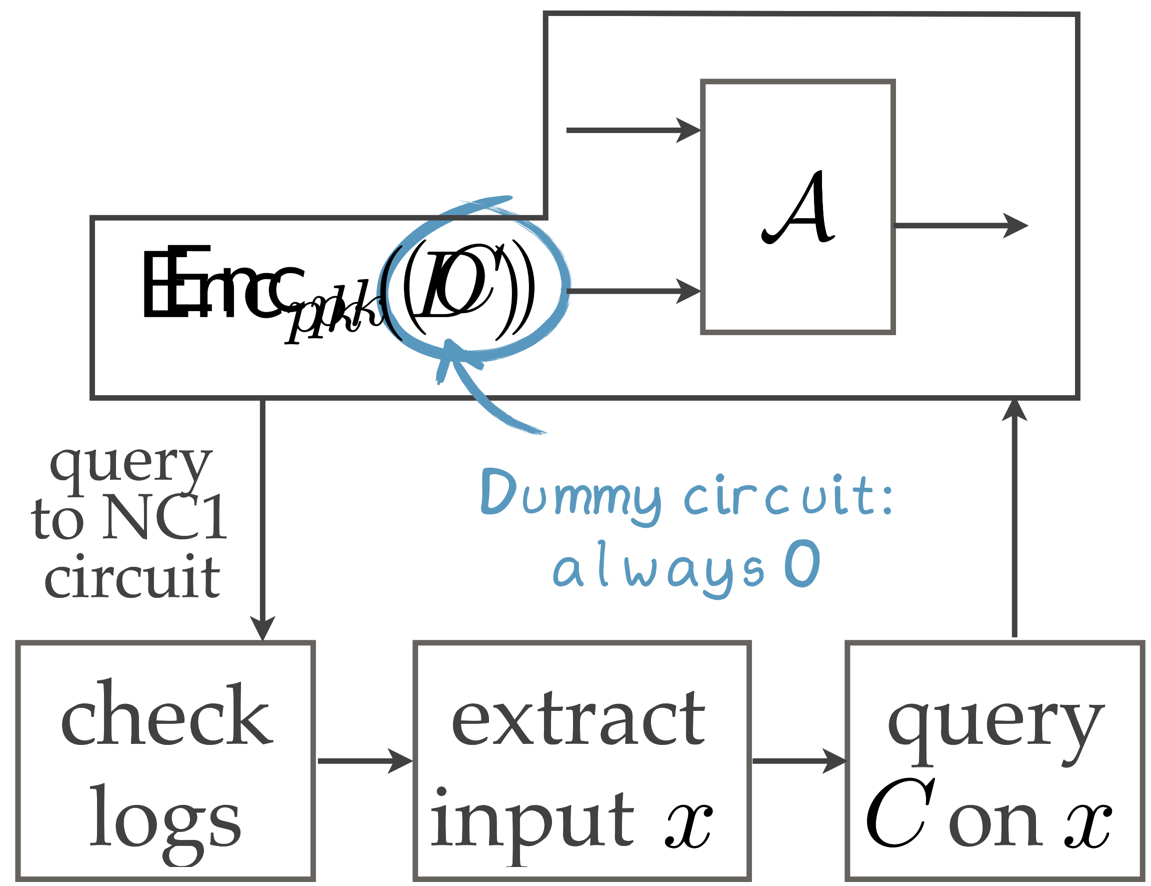
(2) Run the NC¹ simulator for:



and output whatever it outputs

(1) $sk, pk \leftarrow$ KeyGen

(2) Run the NC¹ simulator for:



and output whatever it outputs

Indistinguishable by security of homomorphic encryption

Obfuscation for $\mathfrak{C} = \mathsf{P}$: security

Simulator's output is indistinguishable from adversary's output by:

1. Obfuscation of NC^1 (remove $\mathcal{O}_{\mathsf{NC}^1}(\mathsf{VerDec}_{sk})$)
2. Correctness of HE (never decrypt $\mathcal{A}$'s output)
3. Security of HE (replace $\mathsf{Enc}(C)$ with $\mathsf{Enc}(D)$)

The quantum story
(work in progress)

Quantum obfuscation

- Recall classical definition (virtual black box):
  for any PPT QPT $\mathcal{A}$, there exists a PPT QPT simulator $\mathcal{S}$ such that for all $C \in \mathfrak{C}$:

$$\left|\Pr[\mathcal{A}(\mathcal{O}(C)) = 1] - \Pr[S^{C}(1^{|C|}) = 1]\right| \leq \text{negl}(|C|)$$

- Proven to be impossible only if the obfuscation has to be a (classical description of) a quantum circuit [AF16]

[AF16] Alagic and Fefferman. On quantum obfuscation (arXiv:1602.01771)

Main question

Can we obfuscate all poly-size quantum circuits?

Subquestion 1: *Can we **black-box** obfuscate all NC^1 (**classical**) circuits?*

Subquestion 2: *Can we lift black-box obfuscation of NC^1 to all poly-size **quantum** circuits?*

Subquestion 3: *Can we lift indistinguishability obfuscation of NC^1 to all poly-size **quantum** circuits?*

Obstacle 1: quantum HE

- We now want to obfuscate quantum circuits and run them on quantum input states.
- This requires homomorphic encryption of quantum states
  - Definition of quantum HE [BJ15]
  - Quantum HE (with decryption in NC^1) [DSS16]
  - Quantum HE with a classical client [Mah17]

[BJ15] Broadbent, Jeffery. Quantum homomorphic encryption for circuits with low T-gate complexity. (CRYPTO 2015)
[DSS16] Dulek, Schaffner, Speelman. Quantum homomorphic encryption for polynomial-sized circuits. (CRYPTO 2016)
[Mah17] Mahadev. Classical homomorphic encryption for quantum circuits. (FOCS 2018)

Obstacle 2: Verified decryption

- A quantum computation cannot trivially be verified: no-cloning and inherent randomness in the computation prevent the user from producing a computation log to submit to VerDec.
- Add verification by combining quantum authentication codes with homomorphic encryption. This allows Eval to produce a classical computation log. [ADSS17]

[ADSS17] Alagic, Dulek, Schaffner, Speelman. Quantum fully homomorphic encryption with verification (ASIACRYPT 2017).

Obstacle 3: key leakage

- New obstacle arises from authentication: adversary can extract information about the authentication key.

- Prevent key leakage: recent result [DS18]

[DS18] Dulek and Speelman. Quantum ciphertext authentication and key recycling with the trap code (TQC 2018).

Obstacle 4: ???

- Current status: candidate scheme without proof
- To do: bound the information that the adversary learns from querying VerDec_{sk}, possibly in superposition.

Summary

- Classically, one can lift obfuscation of NC^1 to obfuscation of P (using homomorphic encryption)
- We are trying to lift it to obfuscation of BQP, or, more generally, all poly-size quantum circuits
- We stumbled across many interesting research questions along the way!

Thank you

QuSoft

PhD/postdoc positions in quantum information available at QuSoft (Amsterdam)! See www.qusoft.org/jobs for more information.