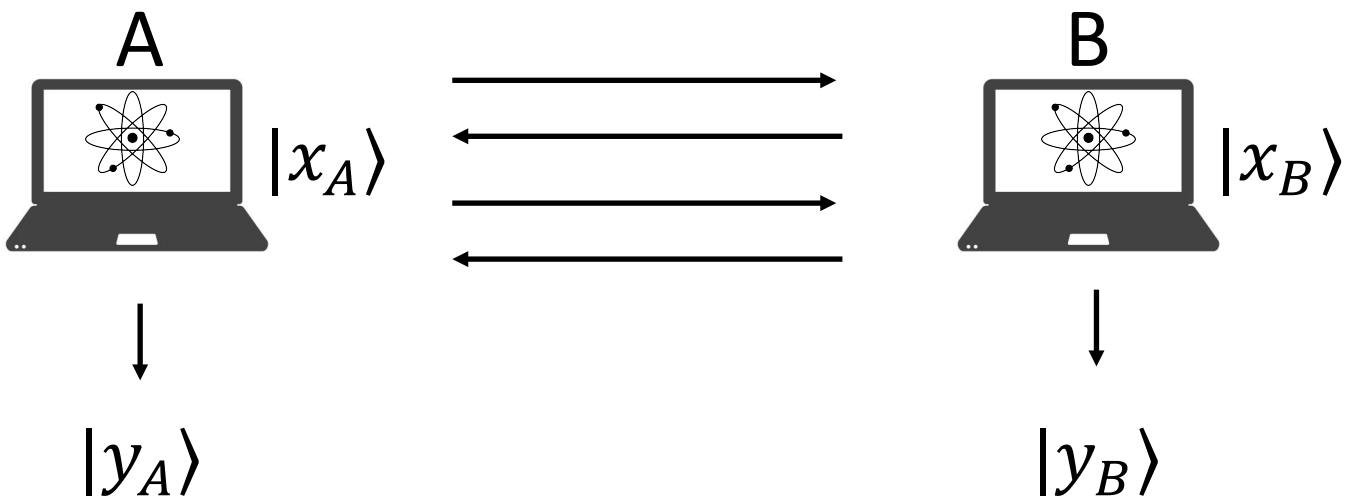
On the Round Complexity of Two-Party Quantum Computation

James Bartusek (UC Berkeley)
Andrea Coladangelo (UC Berkeley)
Dakshita Khurana (UIUC)
Fermi Ma (Princeton and NTT Research)

Secure Two-Party Quantum Computation

Assume access to shared random string (CRS model)



[DNS12]: Secure two-party *classical* computation implies secure two-party *quantum* computation

Number of rounds required by [DNS12] compiler grows with the *depth of the quantum circuit*

Goal: Compute $U|x_A\rangle|x_B\rangle = |y_A\rangle|y_B\rangle$

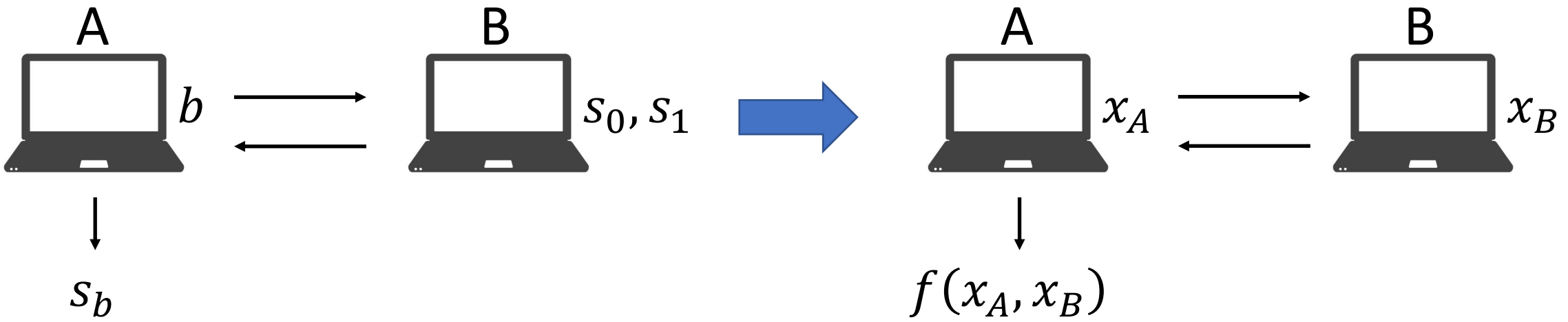
Security: Malicious A learns **only** $|y_A\rangle$
Malicious B learns **only** $|y_B\rangle$

In this work, we study the feasibility of two-round (round-optimal) maliciously-secure two-party quantum computation

Classical Two-Party Computation [Yao86]

Assuming **two-message** Oblivious Transfer:

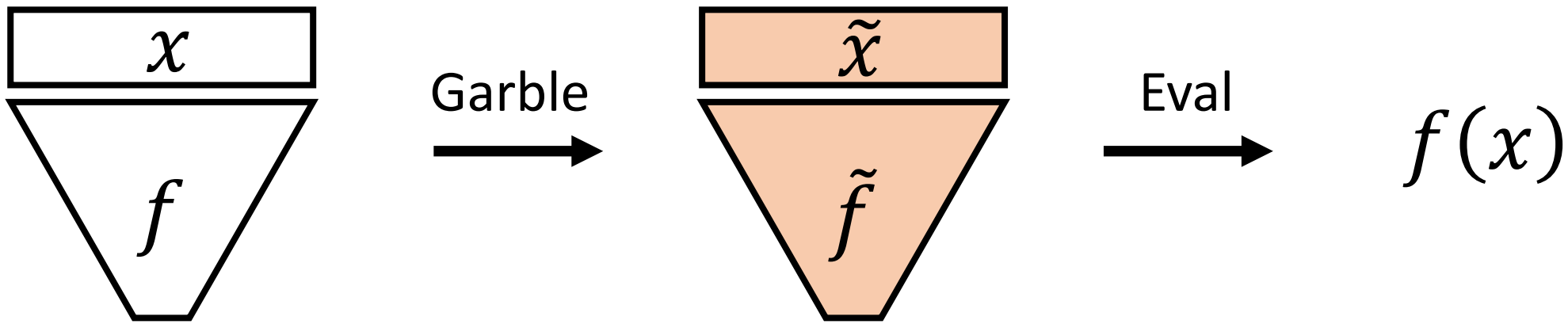
Any classical functionality f that delivers output to one party can be computed securely in **two messages**



Contribution #1: A Quantum Analogue of Yao's Protocol

Assuming two-message oblivious transfer, there exists a two-message protocol for computing any **quantum** functionality that delivers output to one party

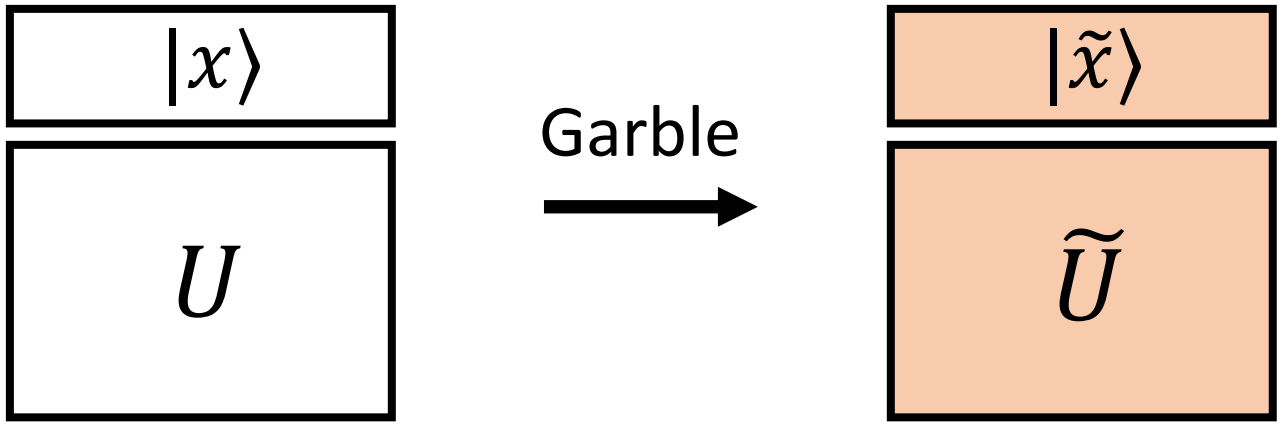
Classical Garbled Circuits



$$\mathrm{Sim}\big(f(x)\big) \approx \big(\tilde{f}, \tilde{x}\big)$$

Non-trivial when Garble has lower complexity than f

Quantum Garbled Circuits [BY20]



$U \to \tilde{U}$ is a *classical* operation

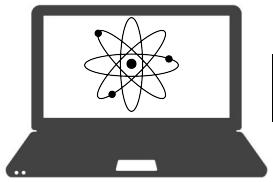
$|\tilde{x}\rangle = C|x\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$, where C is a random Clifford

$U|x_A\rangle|x_B\rangle = |y_A\rangle$

$|\hat{x}\rangle$: *Clifford Encoding* of $|x\rangle$

In parallel, run a classical 2PC that delivers $\widetilde{U}$ to A

A

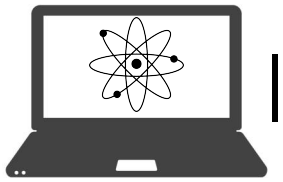


$|x_A\rangle$

$|\hat{x}_A\rangle$

$C|\hat{x}_A\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

B



$|x_B\rangle$

Eval with $\widetilde{U}$

$U|x_A\rangle|x_B\rangle$

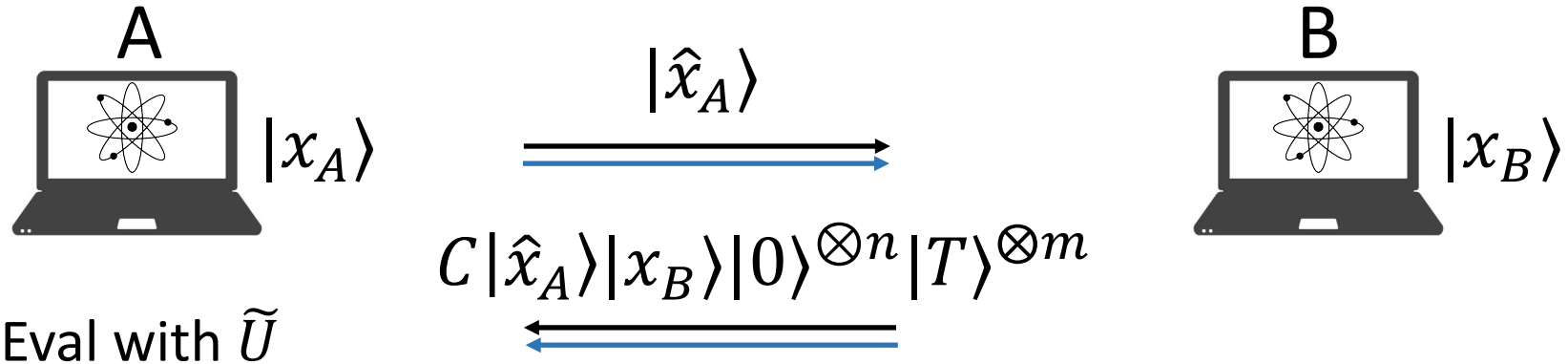
Quantum Garbling: $(U, |x\rangle) \rightarrow \left(\widetilde{U}, |\tilde{x}\rangle\right)$

- $U \rightarrow \widetilde{U}$ is a *classical* operation
- $|\tilde{x}\rangle = C|x\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$, where C is a random Clifford
- $\text{Eval}\left(\widetilde{U}, |\tilde{x}\rangle\right) \rightarrow U|x\rangle$

$U|x_A\rangle|x_B\rangle = |y_A\rangle$

$|\hat{x}\rangle$: *Clifford Encoding* of $|x\rangle$

In parallel, run a classical 2PC that delivers $\widetilde{U}$ to A



Tweak classical 2PC to

- Adjust for encrypted input $|\hat{x}_A\rangle$
- Build in checks ([DGJMS20]) that allow A to catch a B that does not prepare proper $|0\rangle$ and $|T\rangle$ states

Corollary

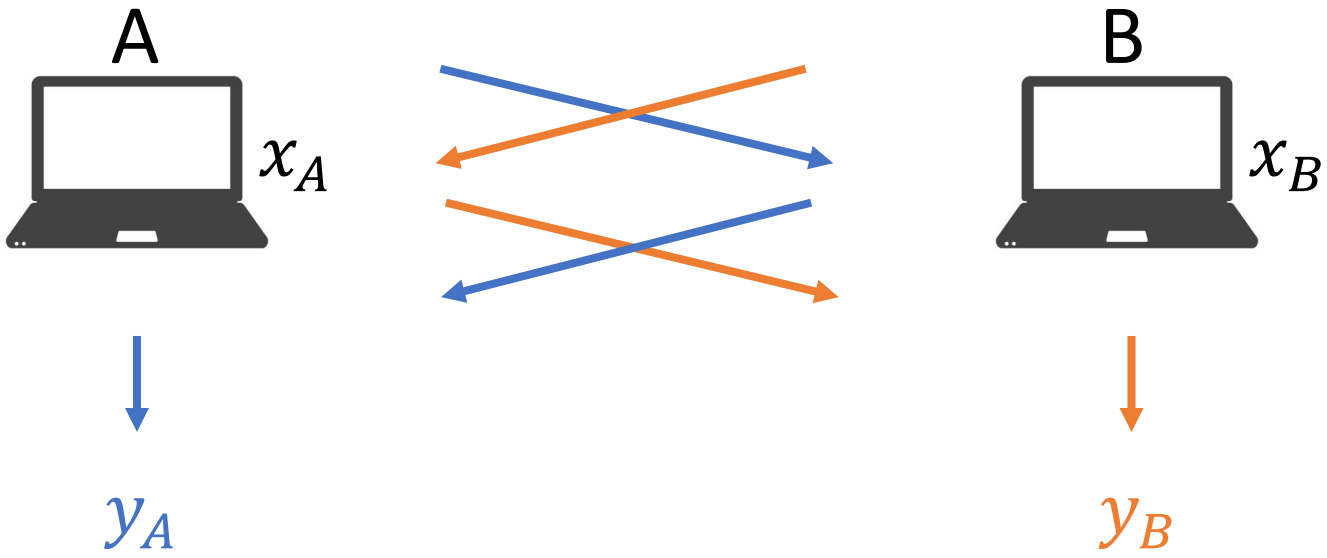
Assuming two-message oblivious transfer, there exists a Reusable Malicious Designated-Verifier NIZK for QMA

Improves the assumption compared to previous work on Reusable MDV-NIZK for QMA [Shm20]

What if both parties require output?

Classical approach:

$$f(x_A, x_B) = (y_A, y_B) \quad \rightarrow \quad \begin{matrix} f_A(x_A, x_B) = y_A \\ f_B(x_A, x_B) = y_B \end{matrix}$$



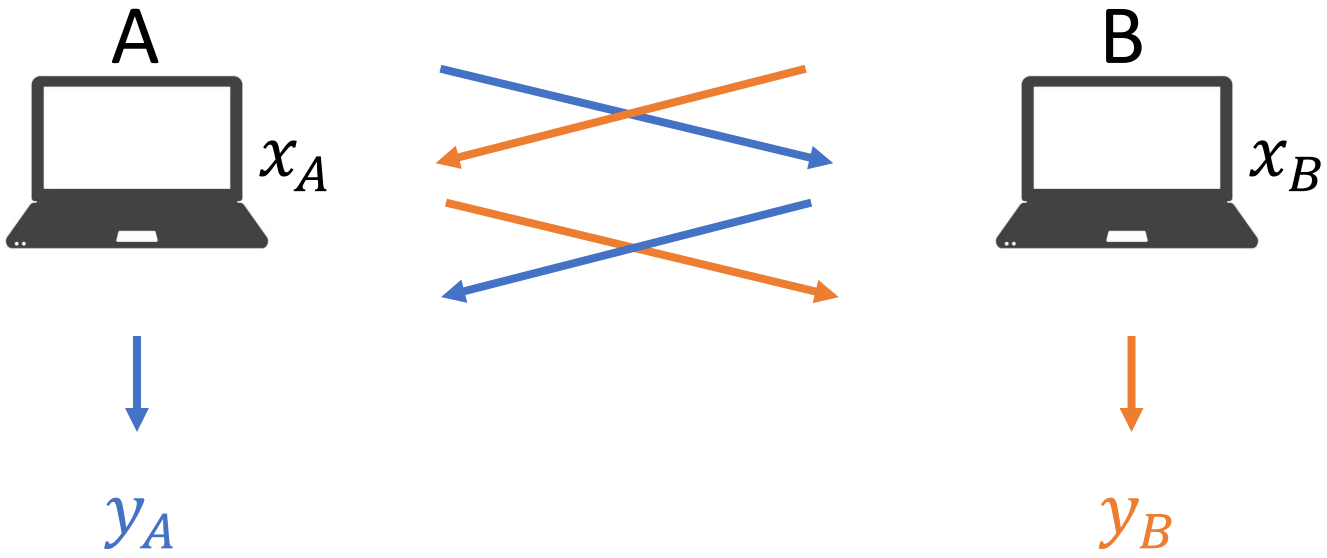
Difficulties in quantum setting:

- Can't in general **clone** quantum inputs

What if both parties require output?

Classical approach:

$$f(x_A, x_B; r) = (y_A, y_B) \longrightarrow \begin{matrix} f_A(x_A, x_B; r) = y_A \\ f_B(x_A, x_B; r) = y_B \end{matrix}$$



Difficulties in quantum setting:

- Can't in general **clone** quantum inputs
- Can't make the functionality **deterministic** by fixing the randomness

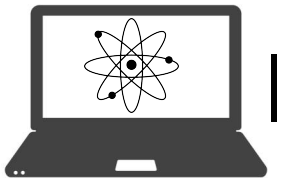
Contribution #2: Two-Round 2PQC with Pre-Processing

Assuming sub-exponentially secure Learning With Errors, there exists a two-round two-party quantum computation protocol with *input-independent* pre-processing

$$U|x_A\rangle|x_B\rangle = |y_A\rangle|y_B\rangle$$

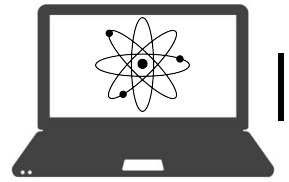
In parallel, run a classical 2PC that delivers $\widetilde{U}$ to A

A



$|x_A\rangle$

B



$|x_B\rangle$

$|\hat{x}_A\rangle$

$C|\hat{x}_A\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

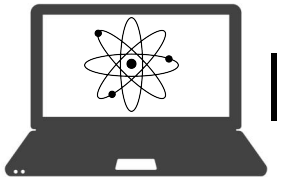
Eval with $\widetilde{U}$

$|y_A\rangle, |y_B\rangle$

$$U'|x_A\rangle|x_B\rangle = |y_A\rangle|\hat{y}_B\rangle$$

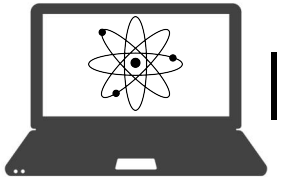
In parallel, run a classical 2PC that delivers $\widetilde{U'}$ to A

A



$|x_A\rangle$

B



$|x_B\rangle$

$|\hat{x}_A\rangle$

$C|\hat{x}_A\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

$|\hat{y}_B\rangle$

Eval with $\widetilde{U'}$

$|y_A\rangle, |\hat{y}_B\rangle$

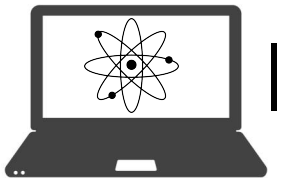
Decrypt

$|y_B\rangle$

$$U'|x_A\rangle|x_B\rangle = |y_A\rangle|\hat{y}_B\rangle$$

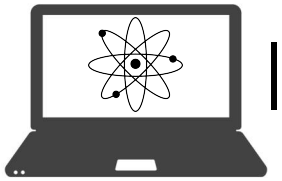
In parallel, run a classical 2PC that delivers $\widetilde{U'}$ to A

A



$|x_A\rangle$

B



$|x_B\rangle$

$|\hat{x}_A\rangle$

Eval with $\widetilde{U'}$

$\downarrow$

$|y_A\rangle, |\hat{y}_B\rangle$

$C|\hat{x}_A\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

$|\hat{y}_B\rangle$

Decrypt

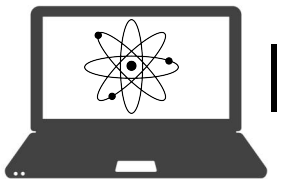
$\downarrow$

$|y_B\rangle$

$$U'|x_A\rangle|x_B\rangle = |y_A\rangle|\hat{y}_B\rangle$$

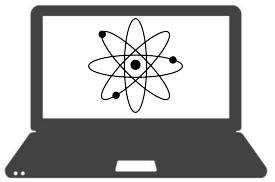
In parallel, run a classical 2PC that delivers $\widetilde{U'}$ to A

A



$|x_A\rangle$

B



$|\hat{x}_A\rangle$

$|x_B\rangle$

Eval with $\widetilde{U'}$

$|y_A\rangle, |\hat{y}_B\rangle$

$C|\hat{x}_A\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

$|\hat{y}_B\rangle$

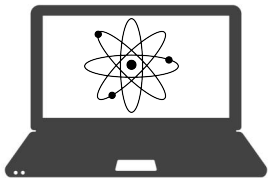
Decrypt

$|y_B\rangle$

$U'|x_A\rangle|x_B\rangle = |y_A\rangle|\hat{y}_B\rangle$

In parallel, run a classical 2PC that delivers $\widetilde{U'}$ to A

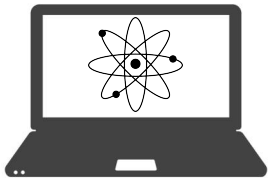
A



$|\mathrm{EPR_A}\rangle$

$|\mathrm{EPR_B}\rangle$

B



$|x_A\rangle$

$|x_B\rangle$

Eval with $\widetilde{U'}$

$|y_A\rangle, |\hat{y}_B\rangle$

$C|\mathrm{EPR_B}\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

$|\hat{y}_B\rangle$

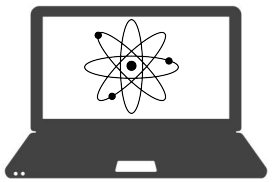
Decrypt

$|y_B\rangle$

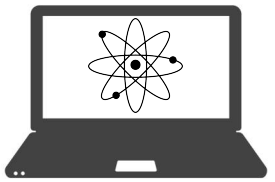
$$U'|x_A\rangle|x_B\rangle = |y_A\rangle|\hat{y}_B\rangle$$

In parallel, run a classical 2PC that delivers $\widetilde{U'}$ to A

A



B



$|\mathrm{EPR_B}\rangle$

$|x_A\rangle\,|\mathrm{EPR_A}\rangle \xrightarrow[\text{Bell}]{} (x,z)$

$|x_B\rangle$

$CX^xZ^z|x_A\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

Eval with $\widetilde{U'}$

$|\hat{y}_B\rangle$

Decrypt

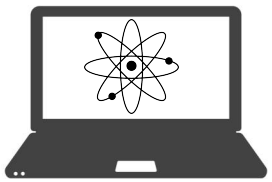
$|y_A\rangle, |\hat{y}_B\rangle$

$|y_B\rangle$

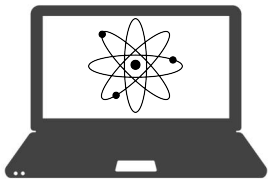
$$U'|x_A\rangle|x_B\rangle = |y_A\rangle|\hat{y}_B\rangle$$

In parallel, run a classical 2PC that delivers $\widetilde{U'X^xZ^z}$ to A

A



B



$|\mathrm{EPR_B}\rangle$

$|x_A\rangle\,|\mathrm{EPR_A}\rangle \xrightarrow[\text{Bell}]{} (x,z)$

$|x_B\rangle$

Eval with $\widetilde{U'X^xZ^z}$

$CX^xZ^z|x_A\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

$|y_A\rangle, |\hat{y}_B\rangle$

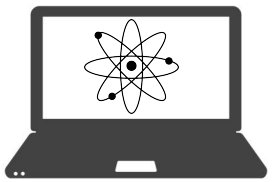
$|\hat{y}_B\rangle$

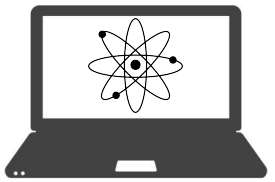
Decrypt

$|y_B\rangle$

$U'|x_A\rangle|x_B\rangle = |y_A\rangle|\hat{y}_B\rangle$

In parallel, run a classical 2PC that delivers $\widetilde{U'X^xZ^z}$ to A





$|\mathrm{EPR_B}\rangle$

$|x_A\rangle\,|\mathrm{EPR_A}\rangle \xrightarrow[\text{Bell}]{} (x,z)$

$|x_B\rangle$

Eval with $\widetilde{U'X^xZ^z}$

$CX^xZ^z|x_A\rangle|x_B\rangle|0\rangle^{\otimes n}|T\rangle^{\otimes m}$

$|y_A\rangle, |\hat{y}_B\rangle$

Challenge: (x,z) are not known in time to include in output of 2PC

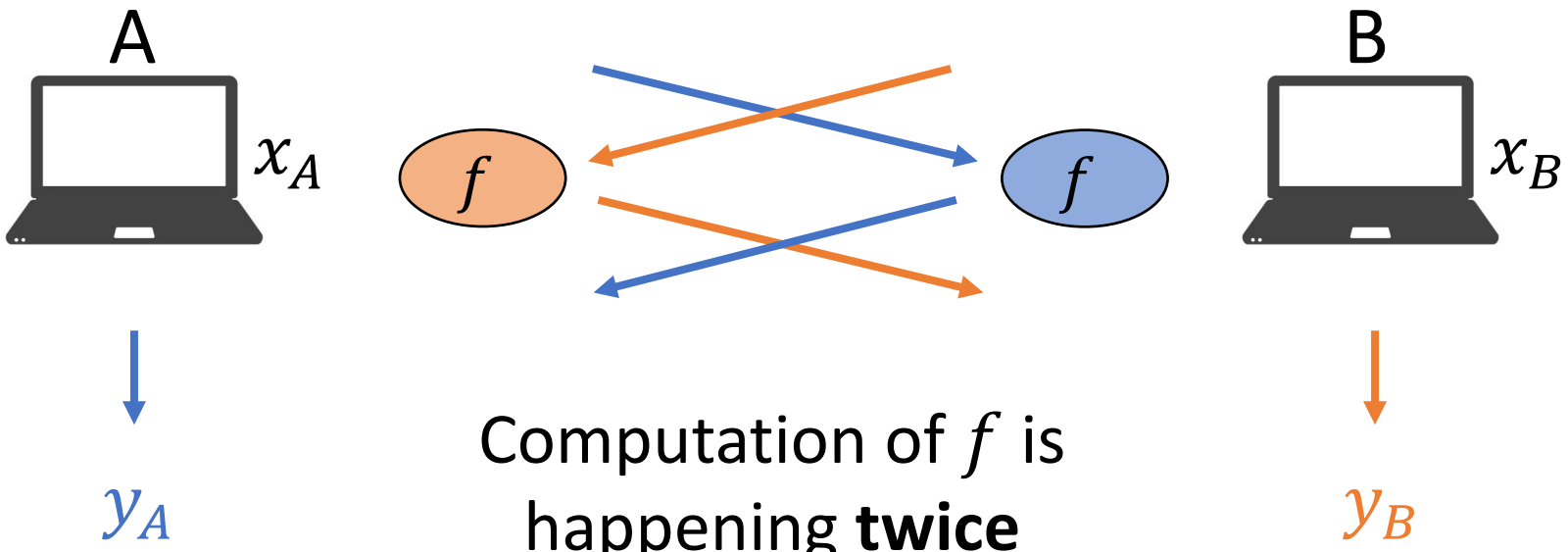
Solution (see paper for details):

- The 2PC outputs a *classical garbled circuit* that takes as input (x,z) and outputs $\widetilde{U'X^xZ^z}$
- Labels are encrypted with *quantum multi-key fully homomorphic encryption* [ABGKM20]

Contribution #3: On the possibility of two-round 2PQC

- Rule out two-round 2PQC with *oblivious simulation*, under a plausible quantum information-theoretic conjecture
- Give a “proof-of-concept” construction of two-round 2PQC from VBB obfuscation of quantum circuits

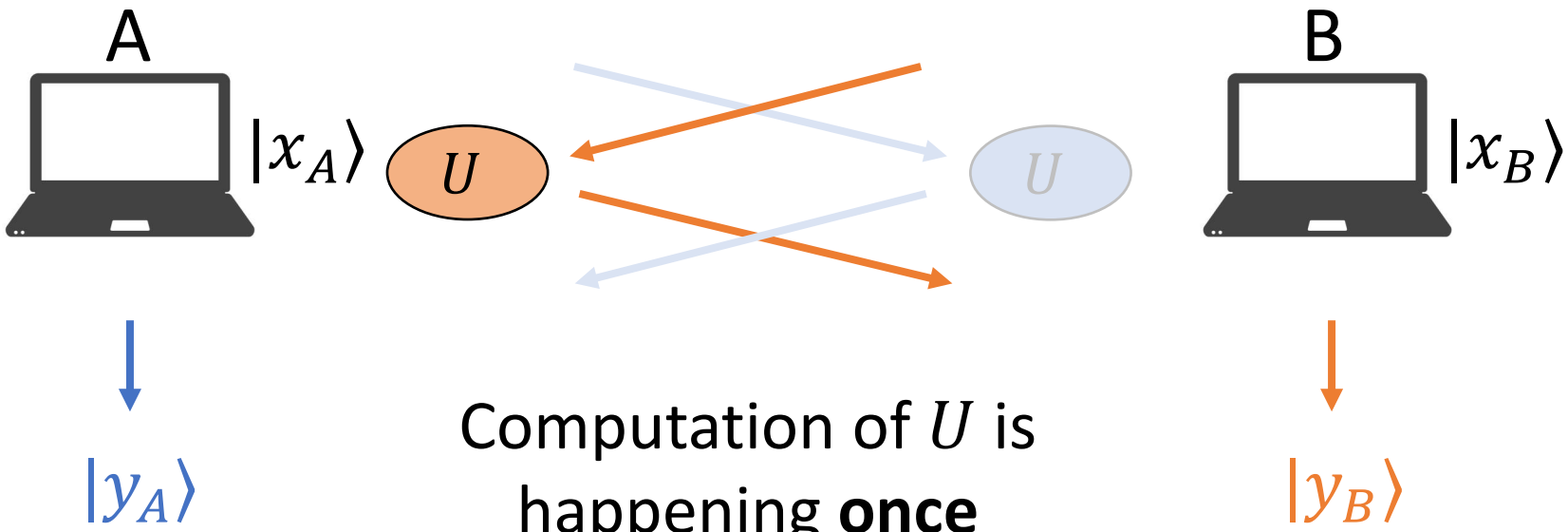
Classical setting:



Computation of f is happening **twice**

Idea for quantum setting: **either** A **or** B computes U, but parties can't distinguish which is the case

Facilitated by obfuscated programs in the CRS



Computation of U is happening **once**

Requires **non-oblivious** simulation
(simulator programs CRS differently depending on whether A or B is corrupted)

Thanks!