Cryptography in the Common Haar State Model: Feasibility Results and Separations

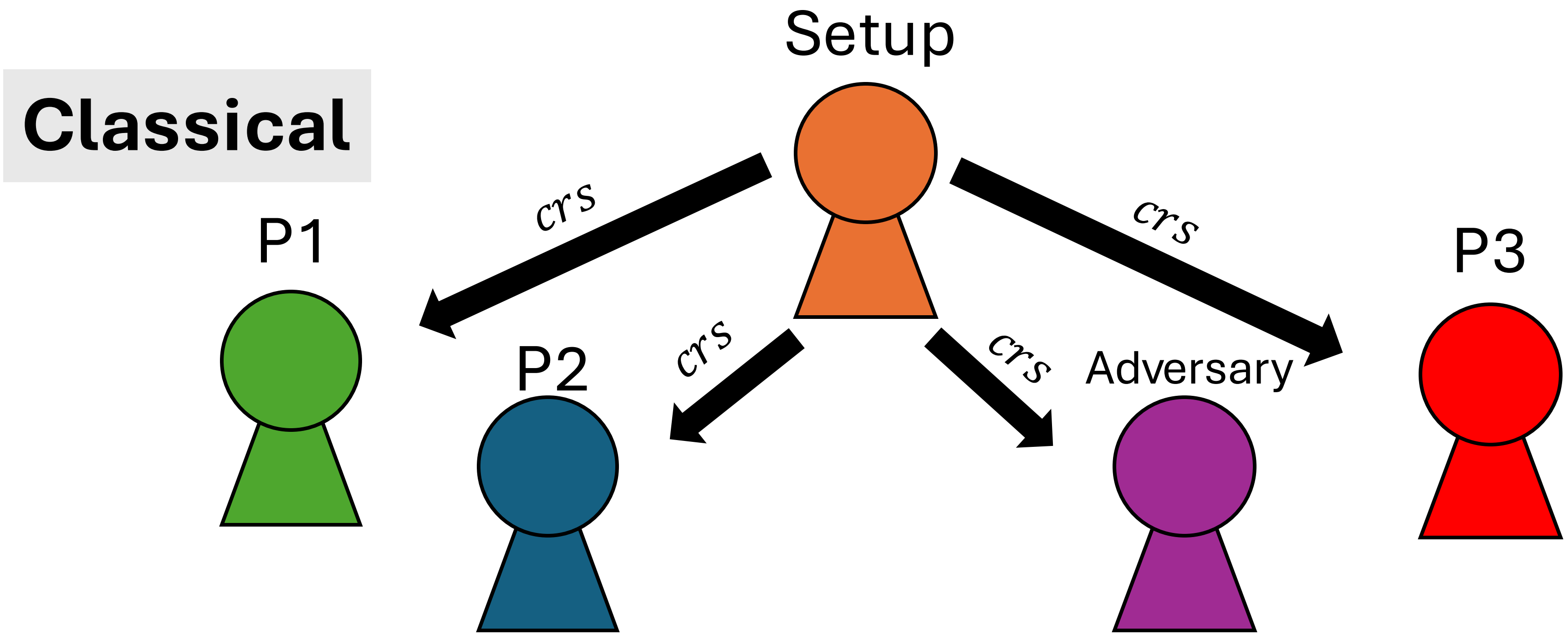
Prabhanjan Ananth (UCSB)

Aditya Gulati (UCSB)

Yao-Ting Lin (UCSB)

Introduction

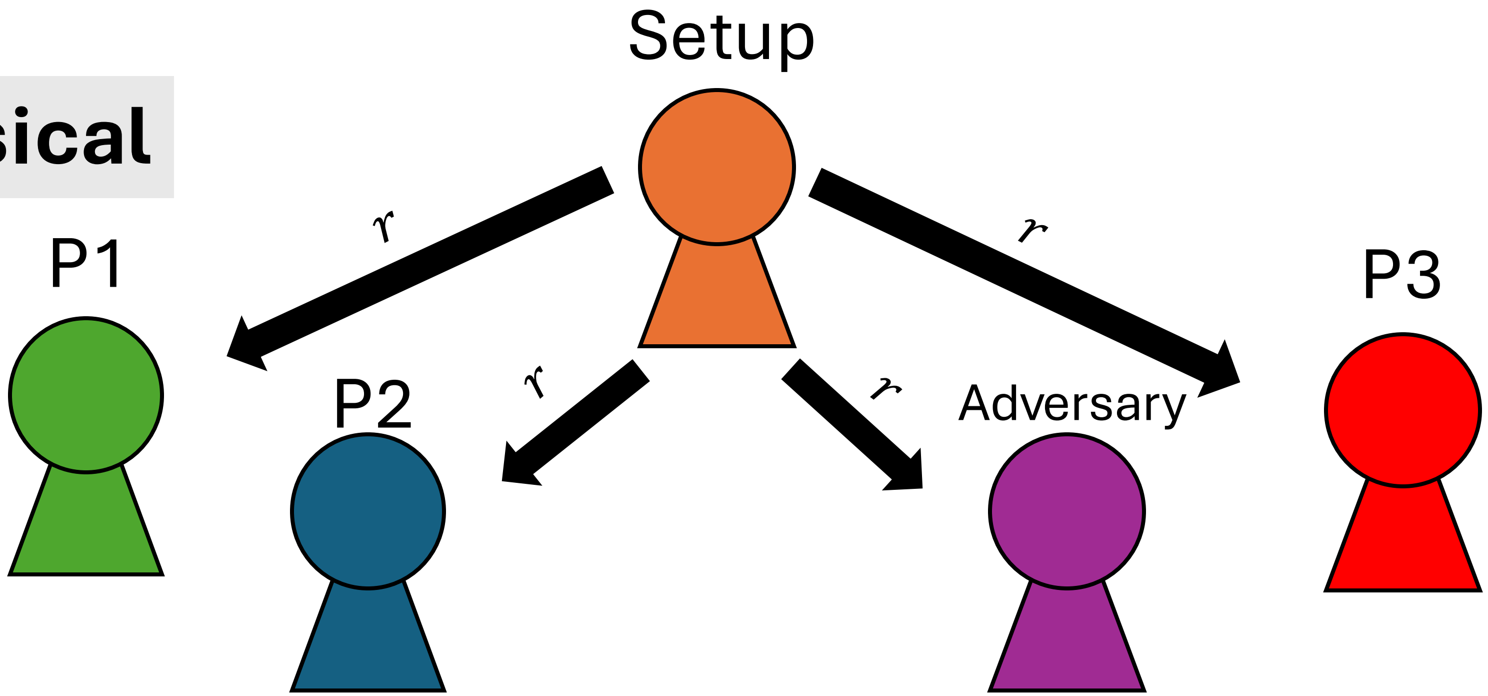
Common Reference String Model



- **Motivation:** Bypass impossibility results in the plain model
- Trusted setup outputs a **reference string** crs to each party, including the adversary
- **Applications:** NIZK, MPC, ...

Common Random String Model

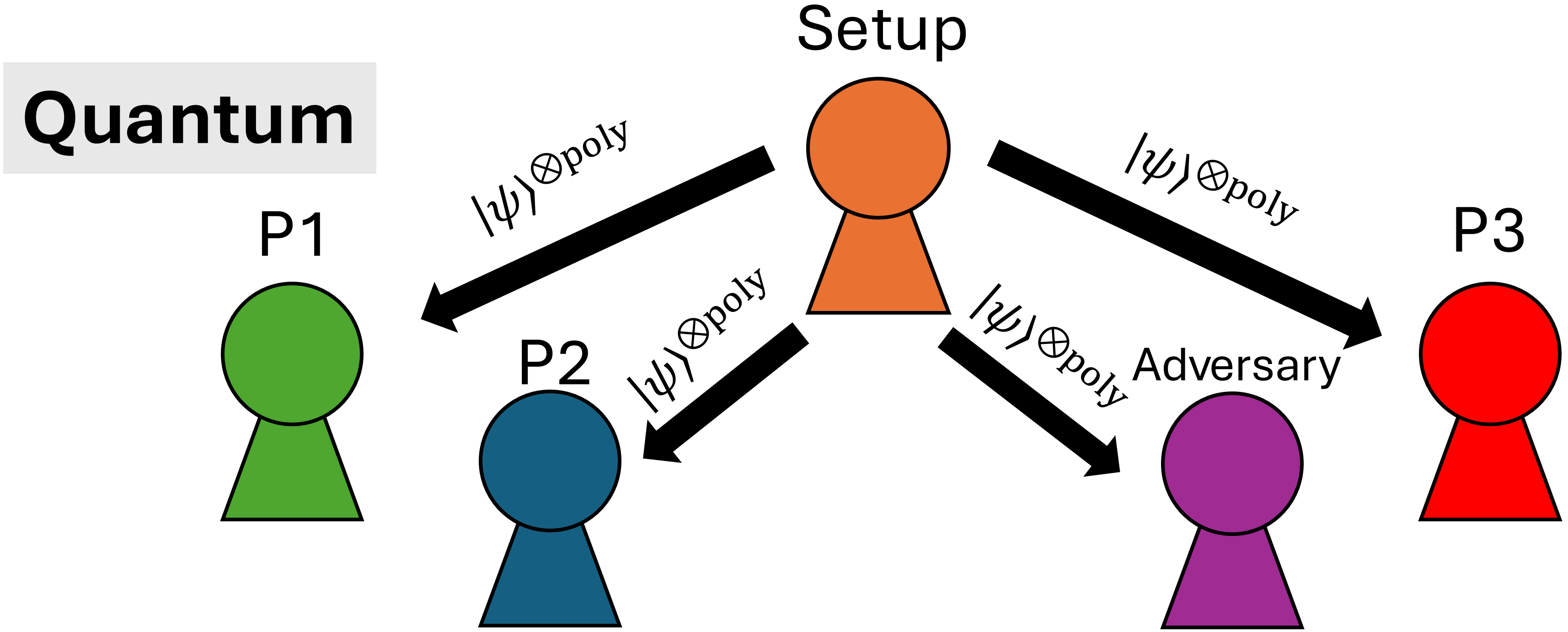
Classical



- Trusted setup outputs a **random string** r to each party, including the adversary
- Lack of structure $\Longrightarrow$ Easier to instantiate (e.g. lottery draw, cloud pattern)
- More desirable than the Common Reference String Model

Could Quantum be Useful?

Common Reference Quantum State Model



- [Morimae-Nehoran-Yamakawa'24] (see also [Qian'24]):

Stat.-hiding & Stat.-binding quantum commitments **exist** in the Common Reference Quantum State Model (quantum analogue of the Common **Reference** String Model)

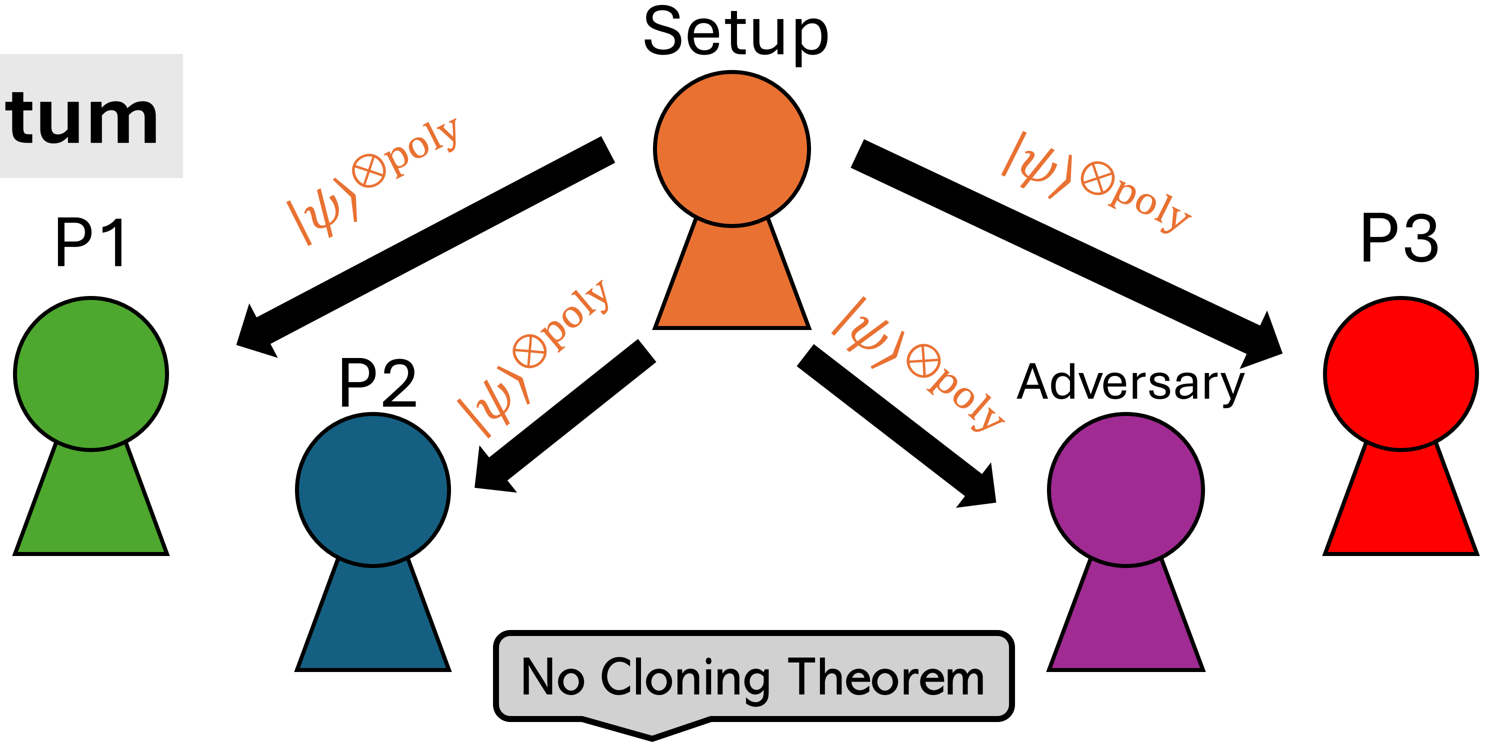
- Impossible in the Common Reference String Model

Our work: Common Haar State (CHS) Model

(quantum analogue of the Common **Random** String Model)

Definition: Common Haar State (CHS) Model

Quantum



- Trusted setup outputs **polynomial copies** of a **Haar random state** $|\psi\rangle$ to each party, including the adversary
- An independent and concurrent work by [Chen-Coladangelo-Sattath'24] also introduced the same model

Motivation

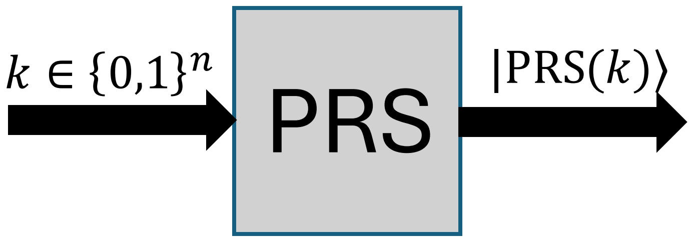
1. Bypassing impossibilities in the plain model
   - Some primitive that requires computational assumptions could be statistically secure in the CHS model

2. Modular approach for designing primitives
   - Instantiate the common Haar state by state designs or pseudorandom states (PRS) in the plain model

3. Black-box separations

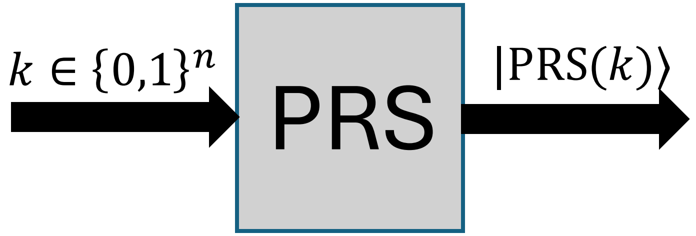
Background: Quantum Pseudorandom Primitives

- Pseudorandom States (PRS) Generator:
  - ➢ Defined by [Ji-Liu-Song'18]
  - ➢ Quantum analogue of PRG
  - ➢ Computationally indistinguishable from a Haar state, even when the adversary holds many copies
  - ➢ Stat.-secure, **stretch** PRS is **impossible** in the plain model



Background: Quantum Pseudorandom Primitives

- Pseudorandom States (PRS) Generator:
  - ➢ Defined by [Ji-Liu-Song'18]
  - ➢ Quantum analogue of PRG
  - ➢ Computationally indistinguishable from a Haar state, even when the adversary holds many copies
  - ➢ Stat.-secure, **stretch** PRS is **impossible** in the plain model



- Pseudorandom Function-Like State (PRFS) Generator:
  - ➢ Defined by [**Ananth**-Qian-Yuen'21]
  - ➢ Quantum analogue of PRF
  - ➢ Computationally indistinguishable from an oracle that outputs an i.i.d. Haar state $|\psi_x\rangle$ on input x

Our Results

Under the parameter regime that is impossible to achieve in the plain model

- Positive result: Bounded-query stat.-secure PRFS in the CHS model

Our Results

Under the parameter regime that is impossible to achieve in the plain model

- Positive result: Bounded-query stat.-secure PRFS in the CHS model
  - We construct PRFS that is secure against $O(n/\log^{1+\varepsilon}(n))$ number of queries in the CHS model for any $\varepsilon > 0$

Our Results

Under the parameter regime that is impossible to achieve in the plain model

- Positive result: Bounded-query stat.-secure PRFS in the CHS model
  - We construct PRFS that is secure against $O(n/\log^{1+\varepsilon}(n))$ number of queries in the CHS model for any $\varepsilon > 0$
  - First construction of PRFS with input length $\omega(\log n)$ from PRS in the plain model

Our Results

Under the parameter regime that is impossible to achieve in the plain model

- Positive result: Bounded-query stat.-secure PRFS in the CHS model

  - We construct PRFS that is secure against $O(n/\log^{1+\varepsilon}(n))$ number of queries in the CHS model for any $\varepsilon > 0$
  - First construction of PRFS with input length $\omega(\log n)$ from PRS in the plain model
  - It implies bounded-copy stat.-secure stretch PRS, stat.-hiding & stat.-binding quantum commitment in the CHS model

Our Results

Under the parameter regime that is impossible to achieve in the plain model

- Positive result: Bounded-query stat.-secure PRFS in the CHS model

  - We construct PRFS that is secure against $O(n/\log^{1+\varepsilon}(n))$ number of queries in the CHS model for any $\varepsilon > 0$

  - First construction of PRFS with input length $\omega(\log n)$ from PRS in the plain model

  - It implies bounded-copy stat.-secure stretch PRS, stat.-hiding & stat.-binding quantum commitment in the CHS model

  - Stronger results + simpler proof compared to [Chen-Coladangelo-Sattath'24]

Our Results

- Negative results:
  1. Optimality of our construction:
     - We break a class of PRS constructions using $O(n/\log n)$ copies
     - [Chen-Coladangelo-Sattath'24] break every construction of PRS in the CHS model using $O(n)$ copies

Our Results

- Negative results:
  1. Optimality of our construction:
     - We break a class of PRS constructions using $O(n/\log n)$ copies
     - [Chen-Coladangelo-Sattath'24] break every construction of PRS in the CHS model using $O(n)$ copies
  2. Impossibility of stat.-secure Quantum-Computation-Classical-Communication (QCCC) key agreement and commitment in the CHS model

Our Results

- Negative results:
  1. Optimality of our construction:
     - ➢ We break a class of PRS constructions using $O(n/\log n)$ copies
     - ➢ [Chen-Colada … of PRS in the CHS model using $O(n)$ copies

Each party performs local quantum computation and communicates classically

  2. Impossibility of stat… ecure Quantum-Computation-Classical-Communication (QCCC) key agreement and commitment in the CHS model

Our Results

- Negative results:
  1. Optimality of our construction:
     - ➢ We break a class of PRS constructions using $O(n/\log n)$ copies
     - ➢ [Chen-Colada… …of PRS in the CHS model using $O(n)$ copies

     Each party performs local quantum computation and communicates classically

  2. Impossibility of stat… …ecure Quantum-Computation-Classical-Communication (QCCC) key agreement and commitment in the CHS model
  3. Black-box separations between PRFS with output length $\omega(\log n)$ and { QCCC key agreement, QCCC commitment }

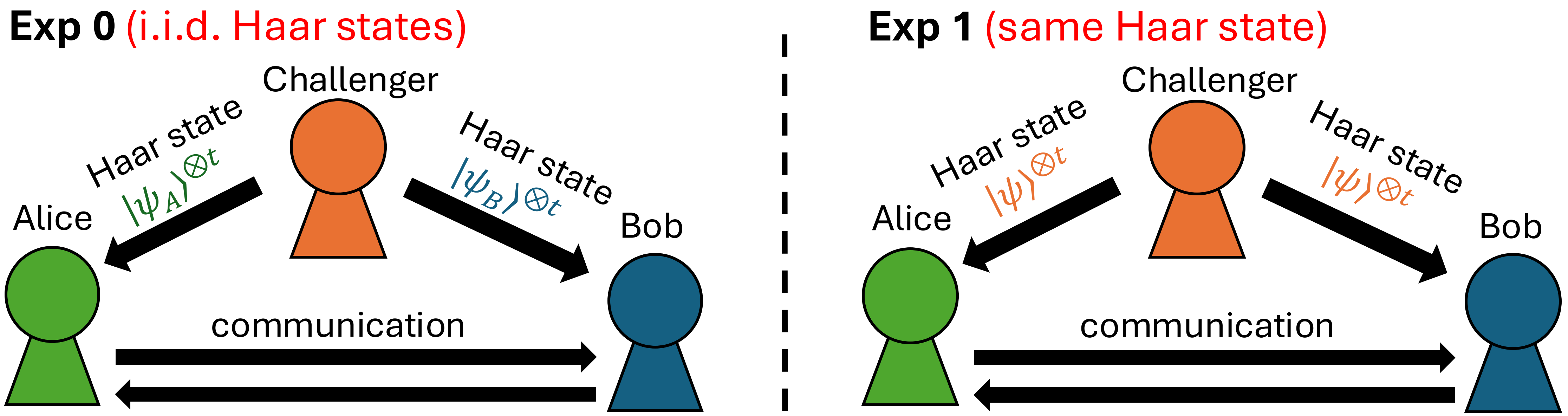
Our Results

- Negative results:
  1. Optimality of our construction:
     - We break a class of PRS constructions using
     - [Chen-Coladangelo-Sattath'24] break every $O(n)$ copies
  2. Impossibility of stat.-secure Quantum-Computation-Classical-Communication (QCCC) key agreement and commitment in the CHS model
  3. Black-box separations between PRFS with output length $\omega(\log n)$ and { QCCC key agreement, QCCC commitment }

Main technical tool:
LOCC Haar Indistinguishability

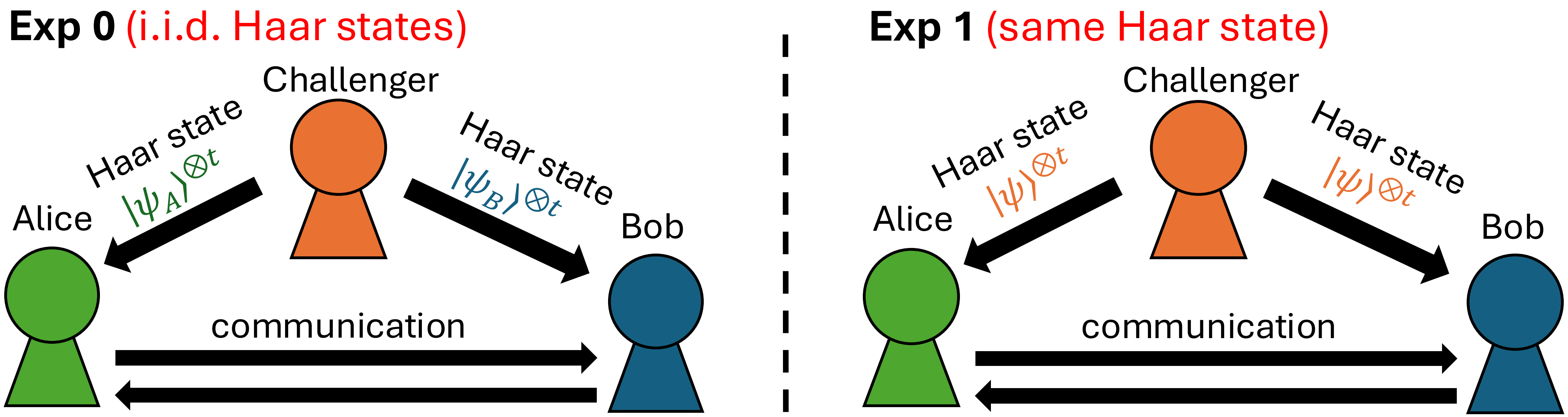
LOCC Haar Indistinguishability

Can two communicating parties w.h.p distinguish i.i.d. vs same Haar states?



LOCC Haar Indistinguishability

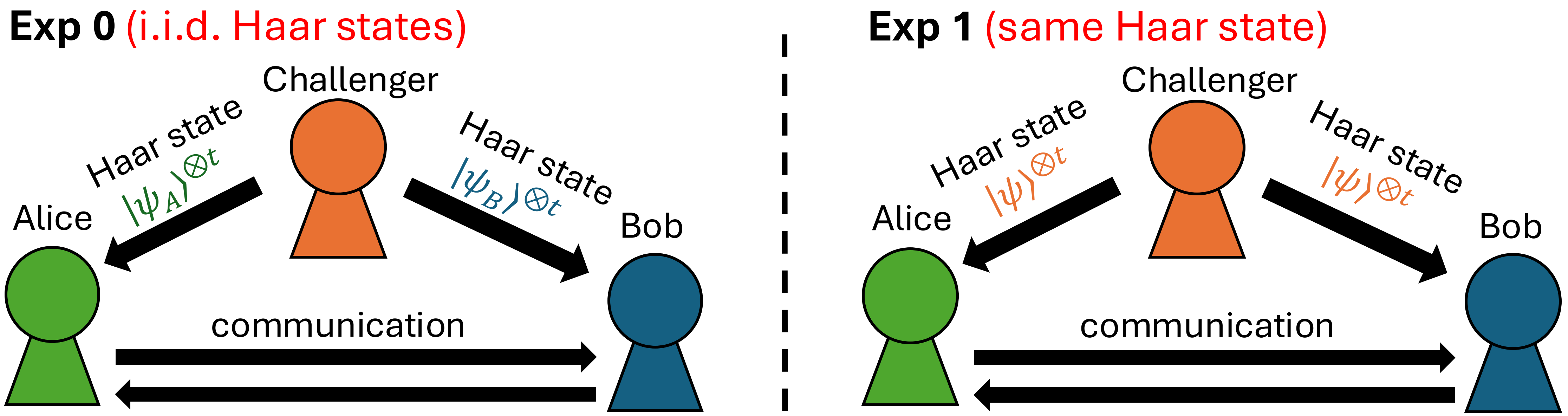
Can two communicating parties w.h.p distinguish i.i.d. vs same Haar states?



- If allow quantum communication: SWAP test $\Longrightarrow$ Easy

LOCC Haar Indistinguishability

Can two communicating parties w.h.p distinguish i.i.d. vs same Haar states?

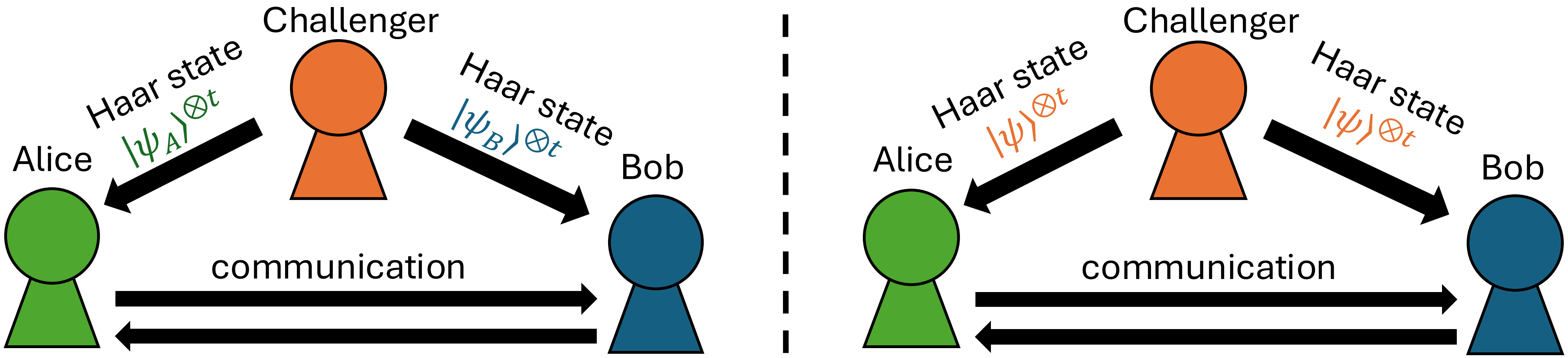


- If allow quantum communication: SWAP test $\Longrightarrow$ Easy
- Two-party adversary (Alice, Bob) (1) computationally unbounded (2) classical communication (3) no shared entanglement

LOCC Haar Indistinguishability

Can two communicating parties w.h.p distinguish i.i.d. vs same Haar states?

Exp 0 (i.i.d. Haar states) | **Exp 1** (same Haar state)



- If allow quantum communication: SWAP test $\Longrightarrow$ Easy
- Two-party adversary (Alice, Bob) (1) computationally unbounded (2) classical communication (3) no shared entanglement
- **Our work:** (Alice, Bob)'s distinguishing advantage is $O(t^2/2^n)$
  - Holds for Positive Partial Transpose (PPT) operators, which is a strict superset of LOCC operators
  - The bound is tight: ∃ (Alice, Bob) with advantage $\Omega(t^2/2^n)$

Our Construction of PRS

Our Construction of PRS

Construction:

On key $k \in \{0,1\}^n$ and m-qubit common Haar state $|\psi\rangle$,

$$|\mathrm{PRS}(k)\rangle := (Z^k \otimes \mathrm{id}_{m-n})|\psi\rangle$$

where $Z^k := Z^{k_1} \otimes Z^{k_2} \otimes \cdots \otimes Z^{k_n}$

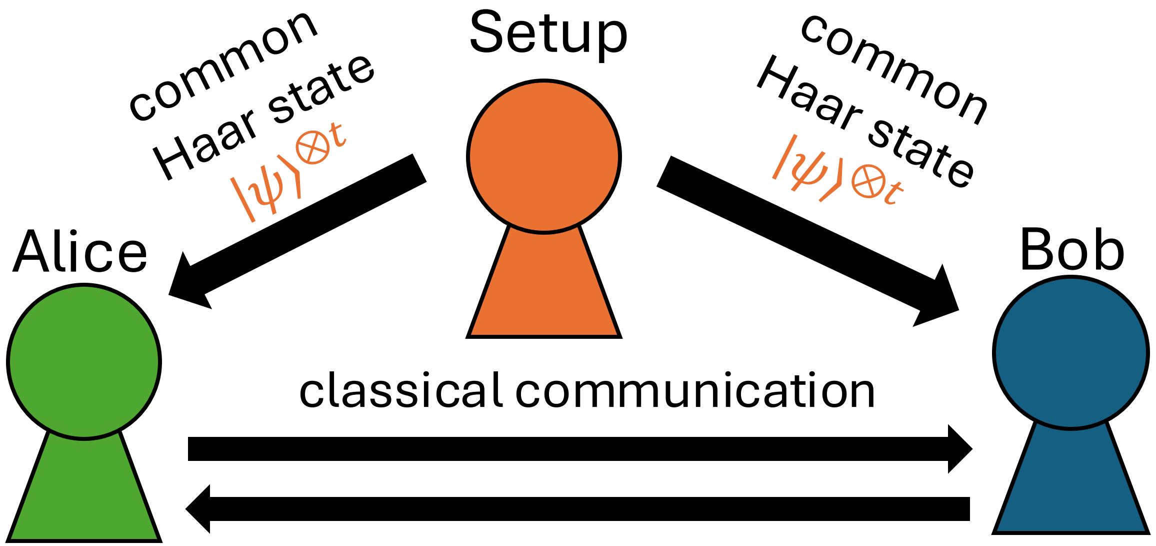
- Efficient generation
- Stretch
- Security: symmetric subspace + combinatorial arguments
- Work for $|\psi\rangle$ of **any** length $\geq$ key length

Impossibility of Interactive QCCC Primitives in the CHS model

A Framework for Proving Impossibilities in CHS model

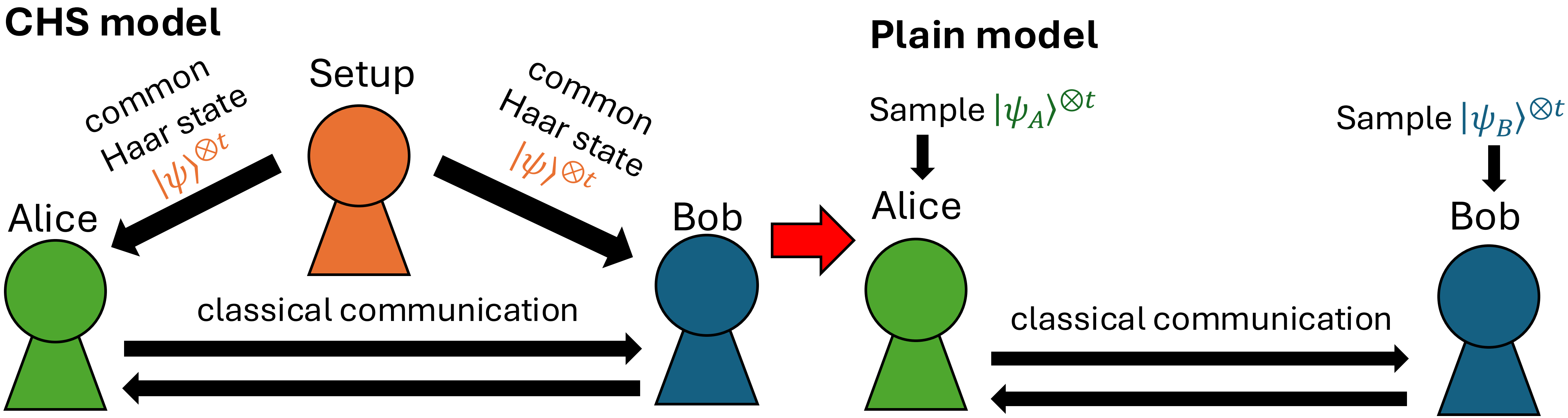
- Some stat.-secure QCCC protocol (e.g. key agreement, commitment) exists in the CHS model

CHS model



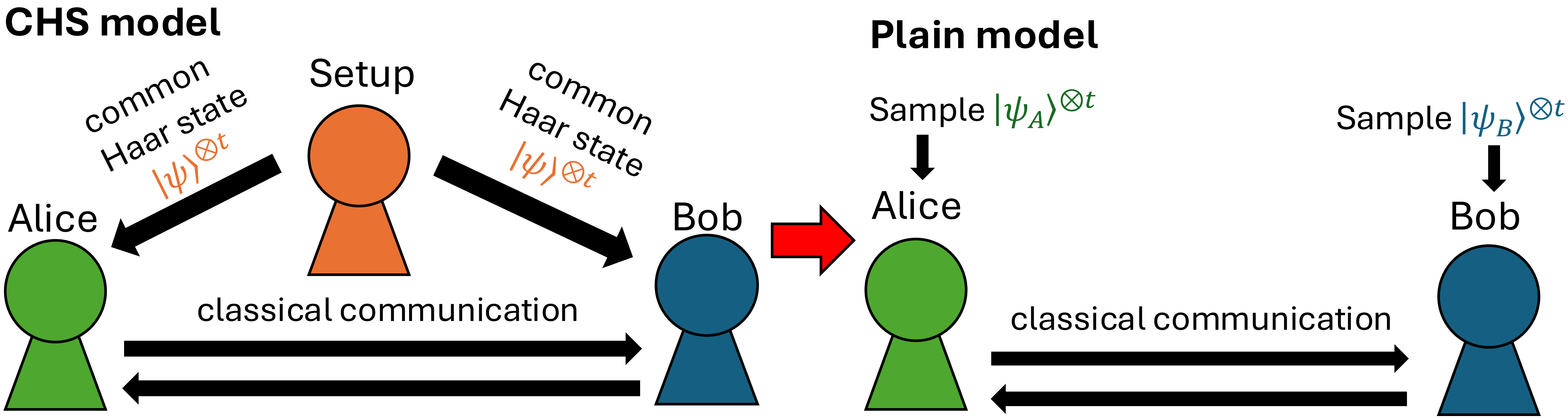
A Framework for Proving Impossibilities in CHS model

- Some stat.-secure QCCC protocol (e.g. key agreement, commitment) exists in the CHS model
- Define a new protocol in the **plain model** by replacing $|\psi\rangle$ with $|\psi_A\rangle$ and $|\psi_B\rangle$



A Framework for Proving Impossibilities in CHS model

- Some stat.-secure QCCC protocol (e.g. key agreement, commitment) exists in the CHS model
- Define a new protocol in the **plain model** by replacing $|\psi\rangle$ with $|\psi_A\rangle$ and $|\psi_B\rangle$
- By **LOCC Haar indistinguishability**, the new protocol in the plain model remains correct and statistically secure $\Longrightarrow$ Contradiction!



Separating Interactive QCCC Primitives from PRFS with Output Length $\omega(\log n)$

Separating Interactive QCCC Primitives from PRFS with Output Length $\omega(\log n)$

- PRS with output length $O(\log n)$ implies QCCC commitment [AGQY'22] [ALY'24]

Separating Interactive QCCC Primitives from PRFS with Output Length $\omega(\log n)$

- PRS with output length $O(\log n)$ implies QCCC commitment [AGQY'22] [ALY'24]
- **Our work:** consider a stronger variant of the CHS model that trivially implies PRFS:
  - Setup prepares a set of i.i.d. Haar states $\{|\psi_{k,x}\rangle\}_{k,x\in\{0,1\}^n}$
  - Party queries on (k, x) classically and gets one copy of $|\psi_{k,x}\rangle$

Separating Interactive QCCC Primitives from PRFS with Output Length $\omega(\log n)$

- PRS with output length $O(\log n)$ implies QCCC commitment [AGQY'22] [ALY'24]
- **Our work:** consider a stronger variant of the CHS model that trivially implies PRFS:
  - Setup prepares a set of i.i.d. Haar states $\{|\psi_{k,x}\rangle\}_{k,x\in\{0,1\}^n}$
  - Party queries on (k, x) classically and gets one copy of $|\psi_{k,x}\rangle$
- Define $|\mathrm{PRFS}(k,x)\rangle := |\psi_{k,x}\rangle$
- Using the same idea to rule out { QCCC key agreement, QCCC commitment } relative to $\{|\psi_{k,x}\rangle\}_{k,x\in\{0,1\}^n}$

Summary

- Common Haar State Model: a quantum analogue of the Common Random String Model
- Some stat.-secure primitives, which are impossible in the plain model, exist in the CHS model
- Separating interactive QCCC primitives from PRFS with super-logarithmic output length

Open Questions & Follow-Up Works

- Quantum Haar Random Oracle Model: Each party has access to a **Haar unitary** oracle
  - ➢Feasibilities & Limitations?
  - ➢Very recent works: [**Ananth**-Bostanci-**Gulati**-**Lin**'24], [Hhan-Yamada'24], …
- LOCC Haar Indistinguishability in the **oracle** setting ? $(A^U, B^U) \approx_{\mathrm{LOCC}} (A^U, B^V)$?

Thanks!