Verifiable blind observable estimation

Bo Yang, Elham Kashefi, Harold Ollivier

https://www.arxiv.org/abs/2510.08548

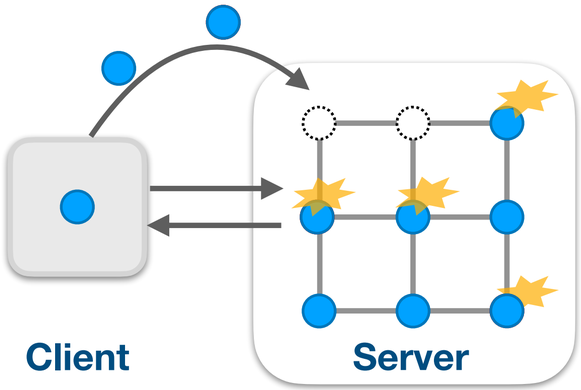


JIQ2026, Bordeaux, 16.01.2026

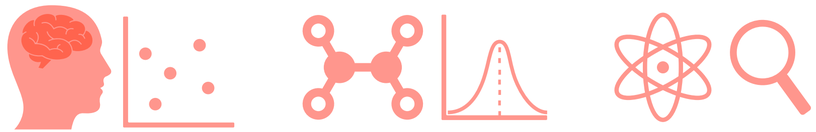
Our contribution

- The first **ideal resource** in abstract cryptography
- Overhead-free **secure verification protocol**

for **observable estimation tasks**



Secure certification



QML / simulation / metrology

key quantum applications

【Verification Protocols】

【Observable Estimation】

Towards ***secure verifiable*** near-term quantum advantage

Towards practical quantum utility

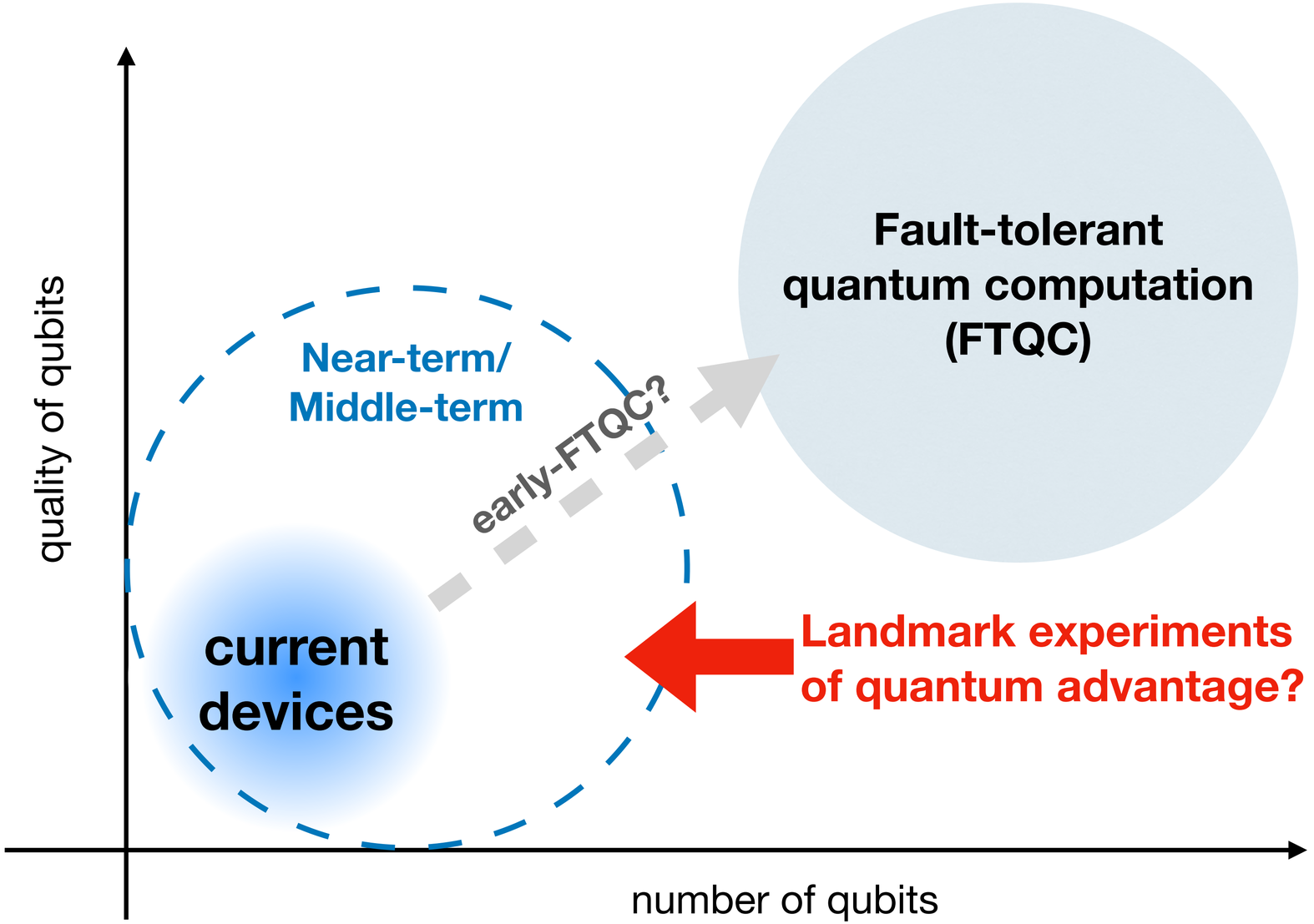
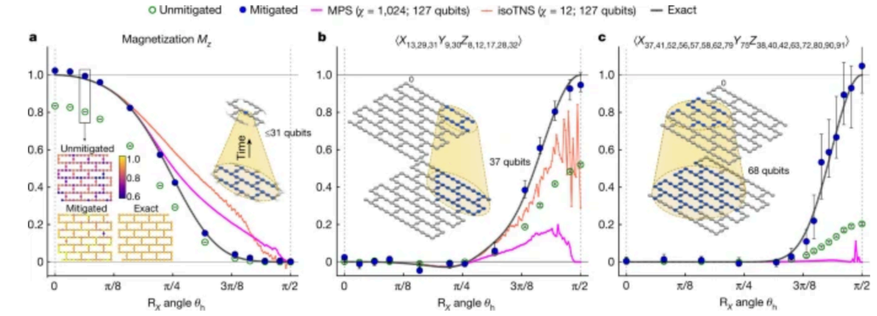
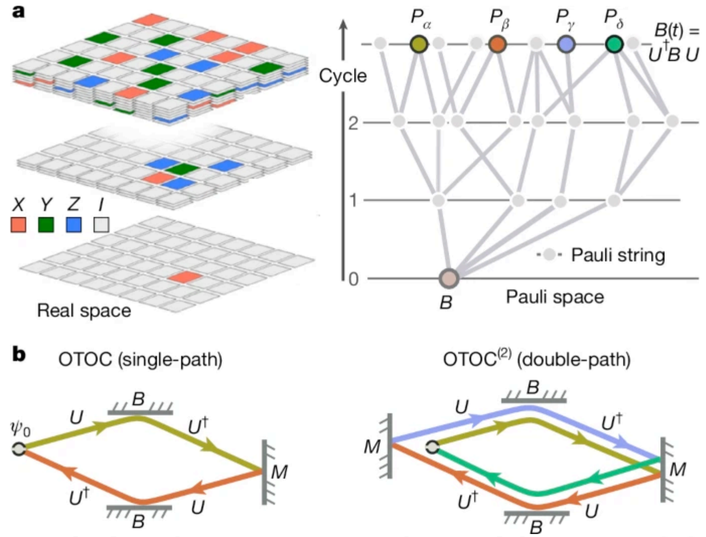


Fig. 3: Classically verifiable expectation values from 127-qubit, depth-15 Clifford and non-Clifford circuits.



[IBM's demonstration, Nature 2024]

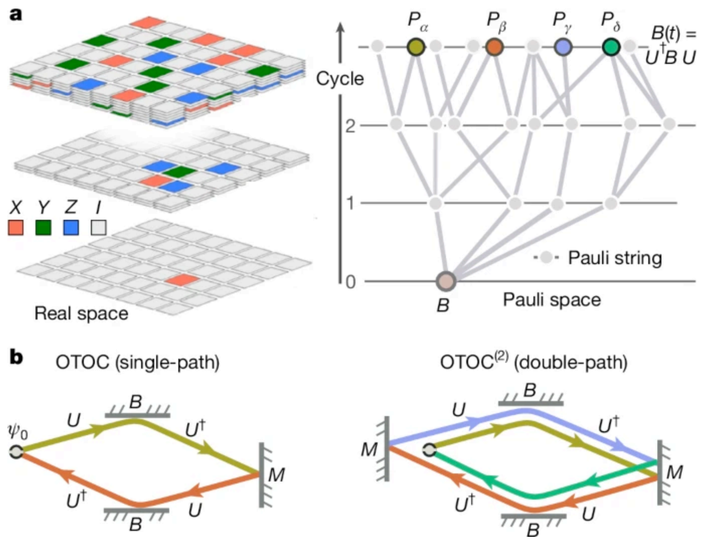


[Google's demonstration, Nature 2025]

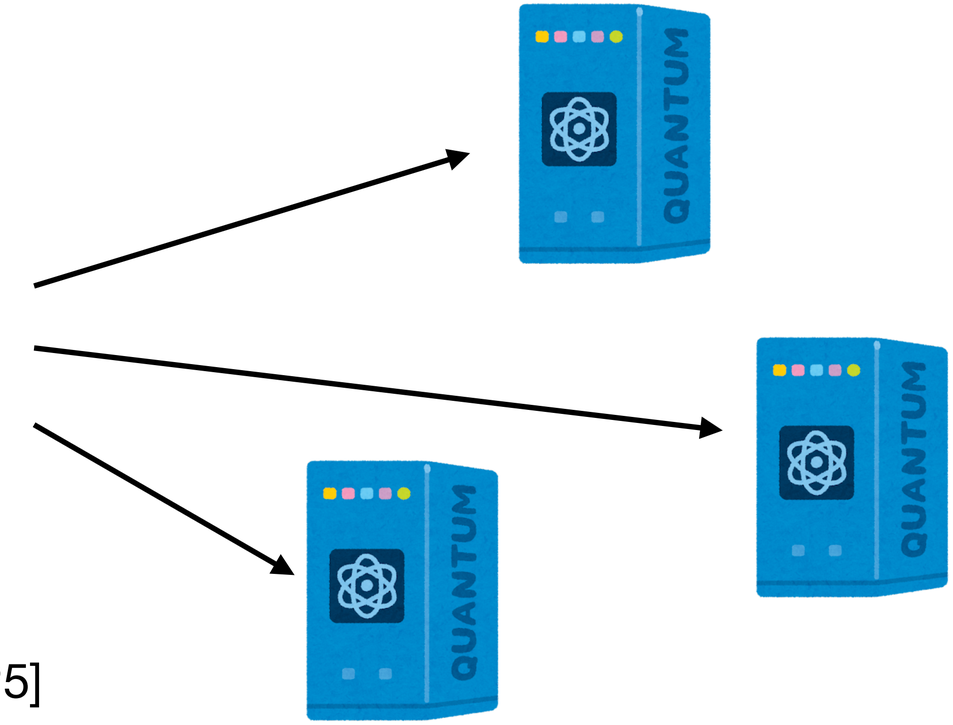
Verifiability of quantum advantage

Definition of **quantum advantage** [Lanes+25]

1. demonstrably superior to classical computational resources
2. **outputs can be rigorously validated**



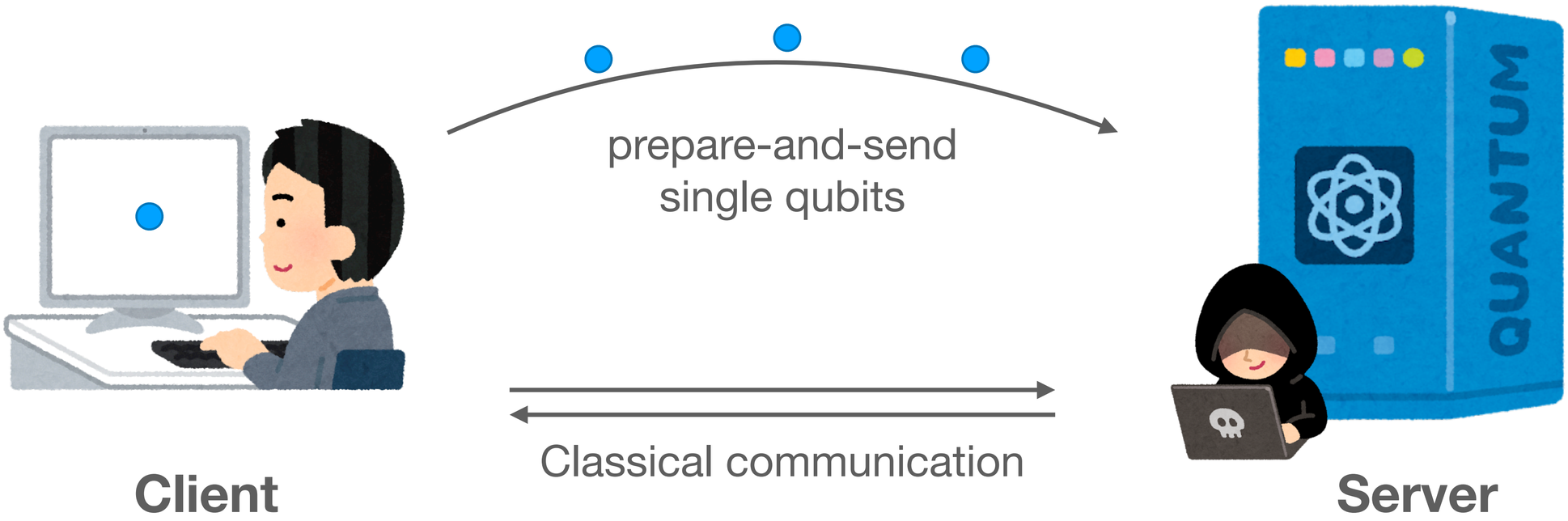
[Google's demonstration, Nature 2025]



Q. How to verify the outcome of classically intractable problem?

Secure delegated quantum computation

→ to <u>untrusted</u> and <u>unreliable</u> server

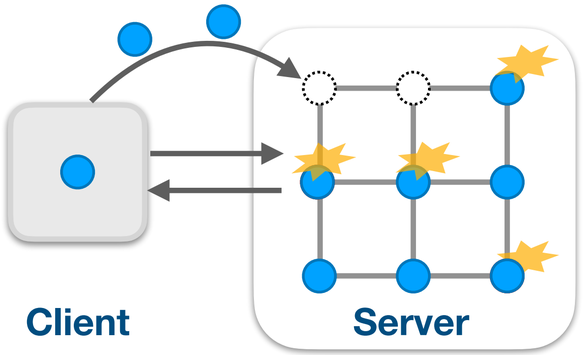


How to ensure the **integrity** and **confidentiality** of delegated quantum computation?

Universal **B**lind **Q**uantum **C**omputation (**UBQC**) [BFK09]

- Perfect blindness

Perfect security in abstract cryptography (AC)



The Client can prepare-and-send single qubits

Blindness:

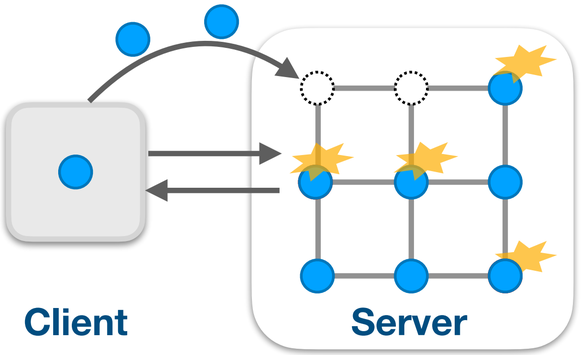
secret parameters in ●, $|+_\theta\rangle$,

Only Client can decode them within the MBQC process

Universal **B**lind **Q**uantum **C**omputation (**UBQC**) [BFK09]

- Perfect blindness

Perfect AC security

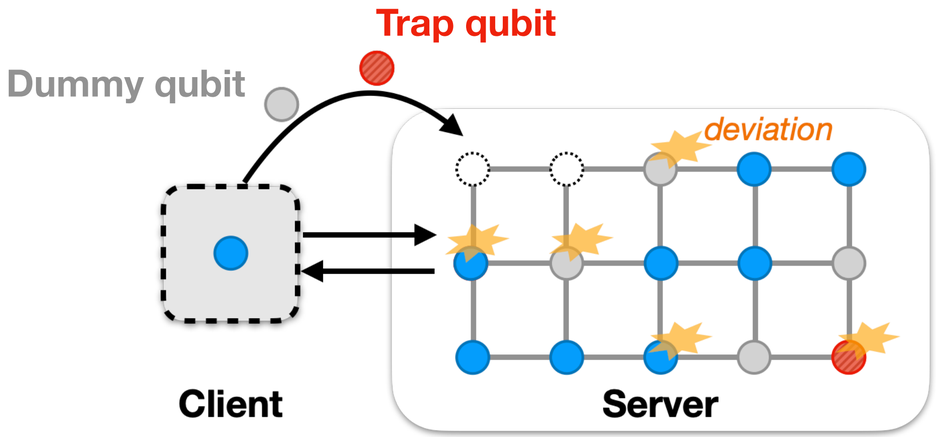


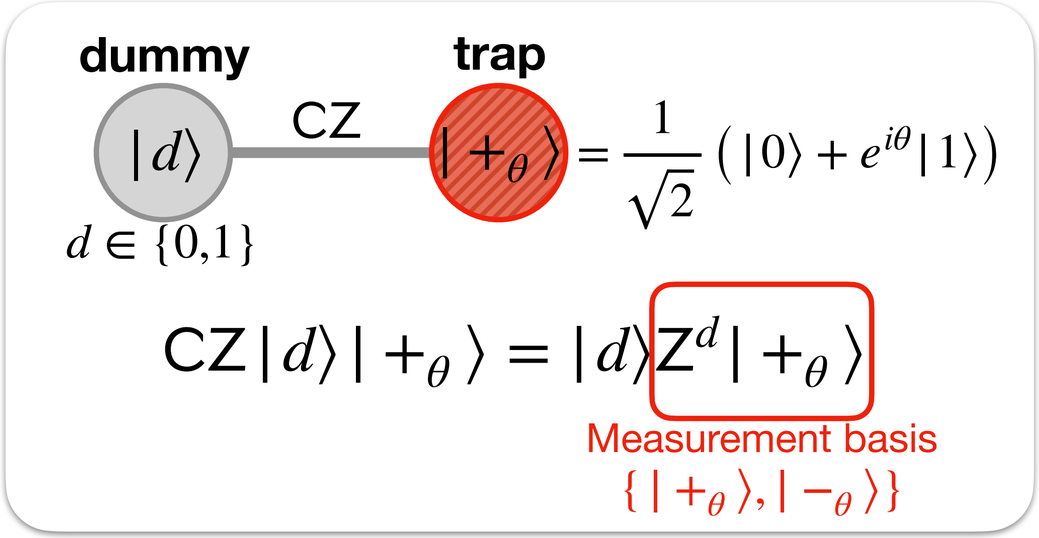
Verifiable **B**lind **Q**uantum **C**omputation (**VBQC**) [FK12]

- Perfect blindness
- Exponential verifiability

Exponential AC security

- Embed **traps** into MBQC
- **Require fault-tolerance for security amplification**
- Quantum output

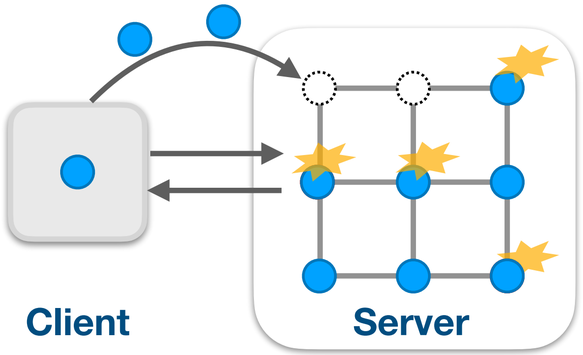




Universal **B**lind **Q**uantum **C**omputation (**UBQC**) [BFK09]

- Perfect blindness

Perfect AC security



Verifiable **B**lind **Q**uantum **C**omputation (**VBQC**) [FK12]

- Perfect blindness
- Exponential verifiability

Exponential AC security

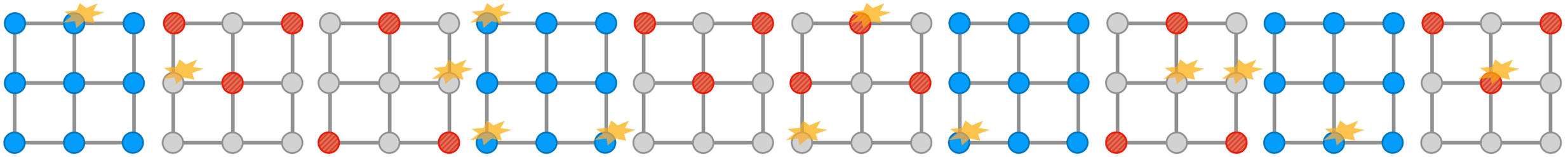
- Embed **traps** into MBQC
- **Require fault-tolerance for security amplification**
- Quantum output

Robust **VBQC** (**RVBQC**) [LMKO21]

- Perfect blindness
- Exponential verifiability

Exponential AC security

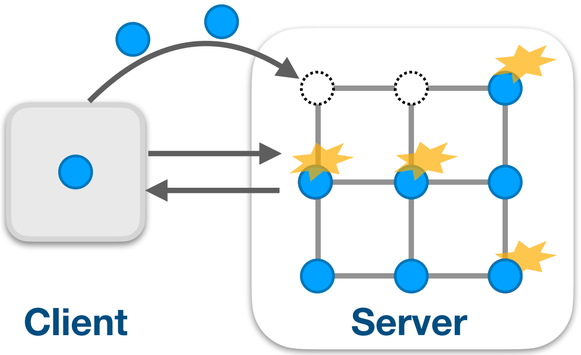
- Separated test/target runs
- **BQP decision problems**



Universal **B**lind **Q**uantum **C**omputation (**UBQC**) [BFK09]

- Perfect blindness

Perfect AC security



Verifiable **B**lind **Q**uantum **C**omputation (**VBQC**) [FK12]

- Perfect blindness
- Exponential verifiability

Exponential AC security

- Embed **traps** into MBQC
- **Require fault-tolerance for security amplification**
- Quantum output

Robust **VBQC** (**RVBQC**) [LMKO21]

- Perfect blindness
- Exponential verifiability

Exponential AC security

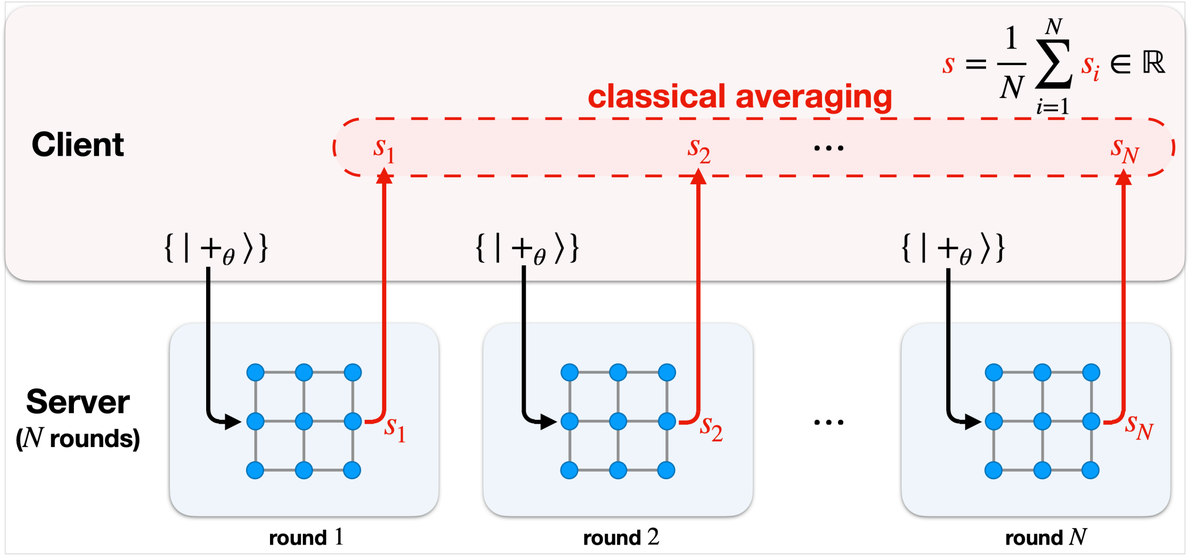
- Separated test/target runs
- **BQP decision problems**

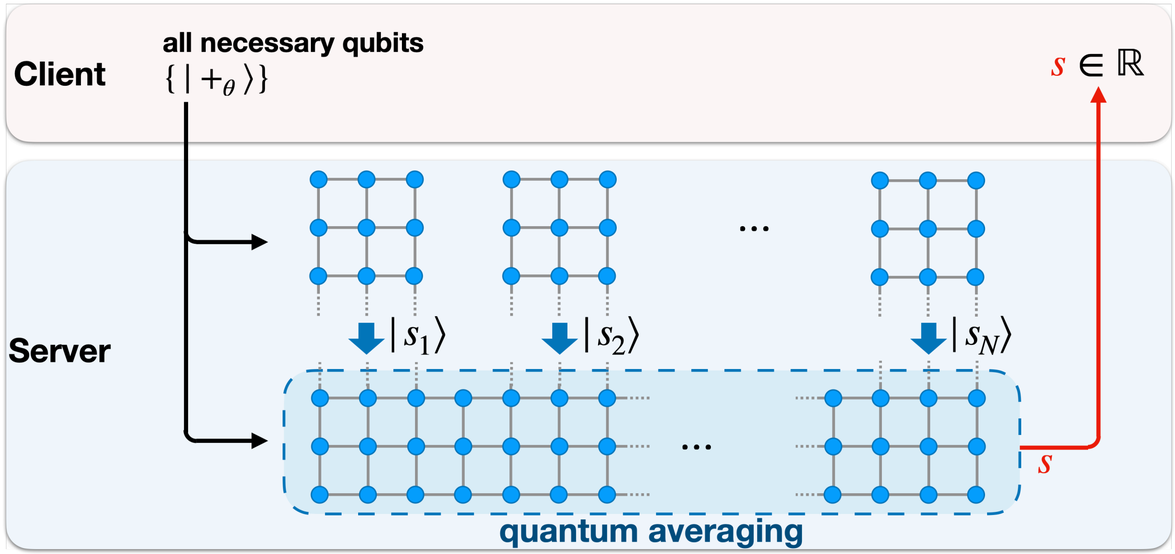
However…

Verifying **continuous-valued output** with RVBQC requires **additional circuit overhead**.

What is the issue?

→ Either inverse polynomial security or heavy space overhead





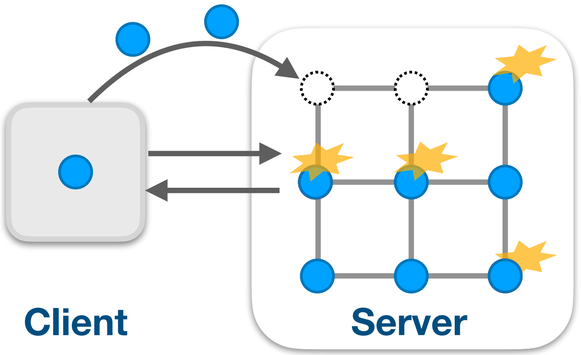
Only $\dfrac{N}{\mathrm{poly}(n)}$ security
with conventional security notion

Beyond near-term quantum overhead
to achieve $O(e^{-N})$ security

Universal **B**lind **Q**uantum **C**omputation (**UBQC**) [BFK09]

- Perfect blindness

Perfect AC security



Verifiable **B**lind **Q**uantum **C**omputation (**VBQC**) [FK12]

- Perfect blindness
- Exponential verifiability

Exponential AC security

- Embed **traps** into MBQC
- **Require QEC for security**
- Quantum output

Robust **VBQC** (**RVBQC**) [LMKO21]

- Perfect blindness
- Exponential verifiability

Exponential AC security

- Separated test/target runs
- **BQP decision problems**

Verifiable Blind Observable Estimation (VBOE) [YKO25]

- Perfect **blindness**
- Exponential **verifiability**

Exponential AC security

- Separated test/target runs
- **Observable estimation**

Task: observable estimation

Given: Observable O, number of samples N, and allowed estimation bias ϵ.

Target: To estimate $\mathrm{Tr}\left[\rho O\right]$ for a reference state ρ.

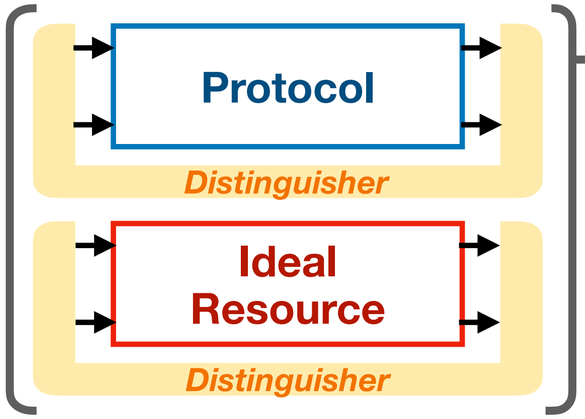
Without loss of generality,
$O := |+\rangle\langle+| - |-\rangle\langle-|$

Output: Empirical mean $\hat{o} = \frac{1}{N}\sum_{i=1}^{N} \hat{y}_i$, where $\hat{y}_i \in \{-1, 1\}$.

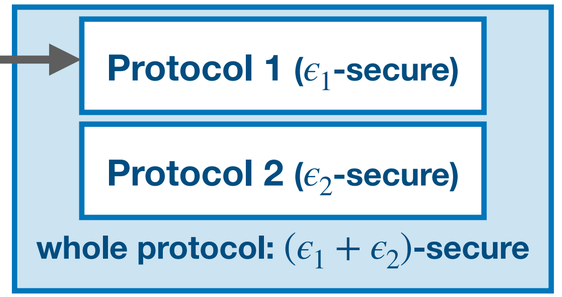
Performance: Estimation confidence $\Pr\left[\left|\hat{o} - \mathrm{Tr}\left[\rho O\right]\right| \geq \epsilon\right] \leq \delta$.

→ **“A protocol (ϵ, δ)-estimates $\mathrm{Tr}\left[\rho O\right]$”.**

Abstract cryptography

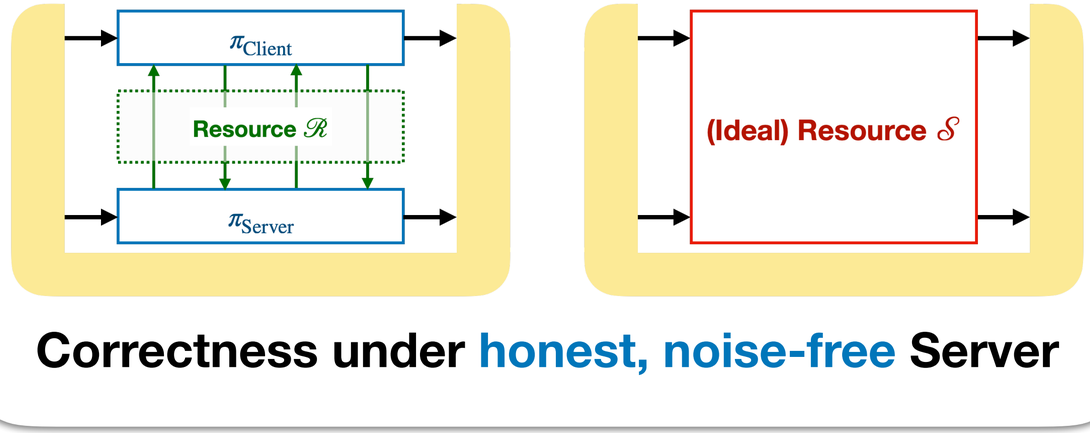


Protocol is "ϵ-secure"
if distinguishing advantage $< \epsilon$



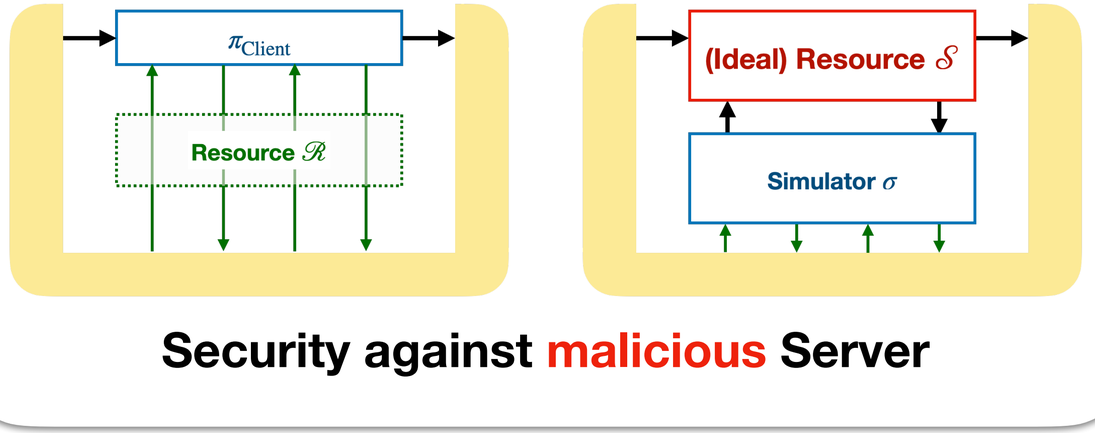
"composable security"

$$\pi_{\text{Client}} \mathcal{R} \pi_{\text{Server}} \approx_\epsilon \mathcal{S}$$



Correctness under honest, noise-free Server

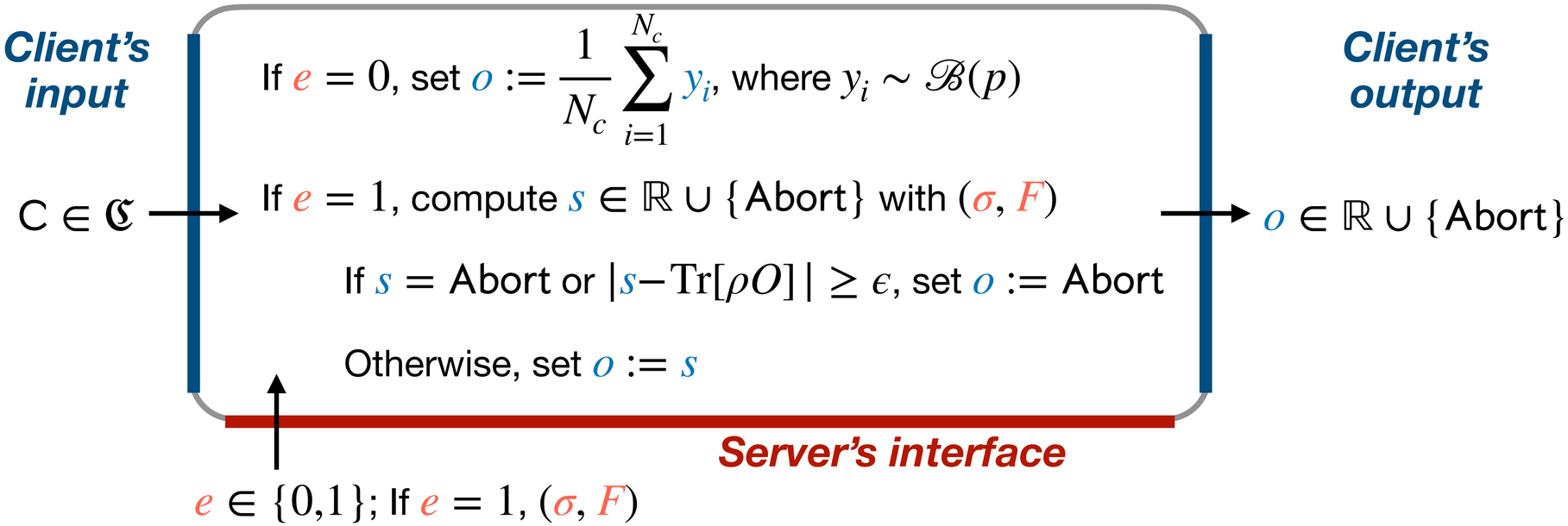
$$\pi_{\text{Client}} \mathcal{R} \approx_\epsilon \mathcal{S}\sigma$$



Security against malicious Server

Proposed ideal resource

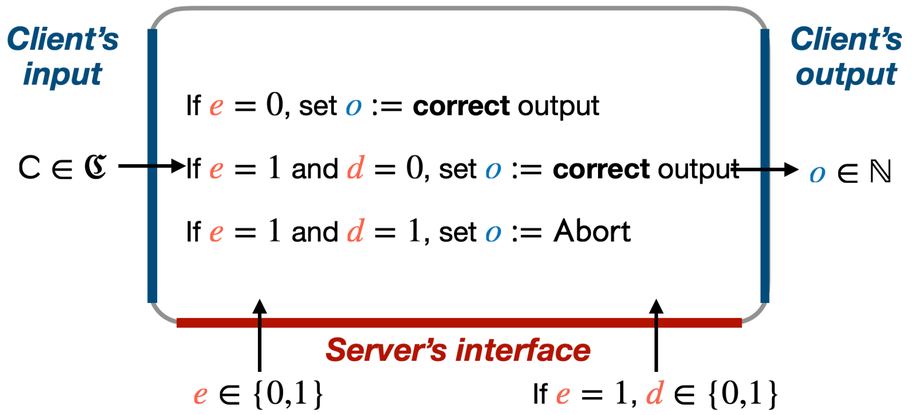
Secure Delegated Observable Estimation (SDOE)



→ **When accepted, the SDOE resource $(\epsilon, 0)$-estimates $\text{Tr}\left[\rho O\right]$.**

New conceptual tool in abstract cryptography

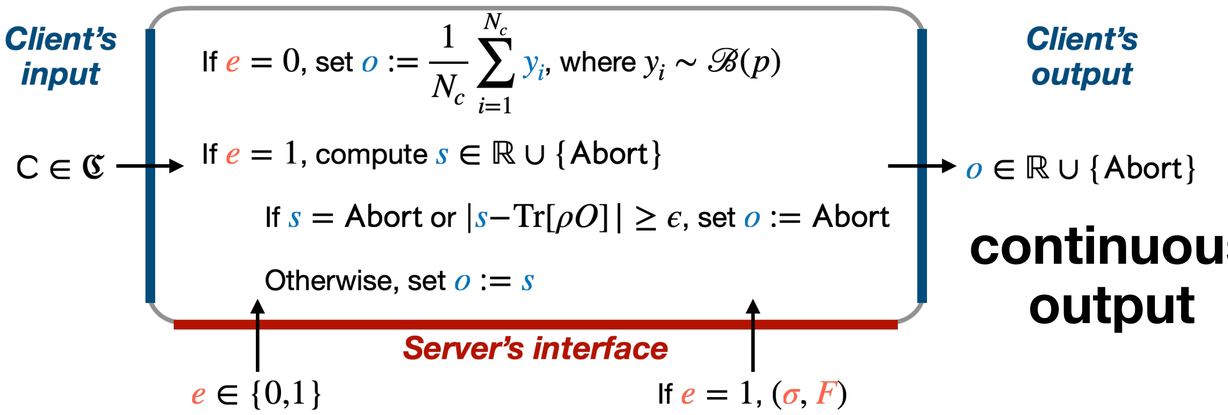
SDQC Resource [KKLO22], [DFPR14]



discrete output

Strictly correct discrete output

SDOE Resource [This work]



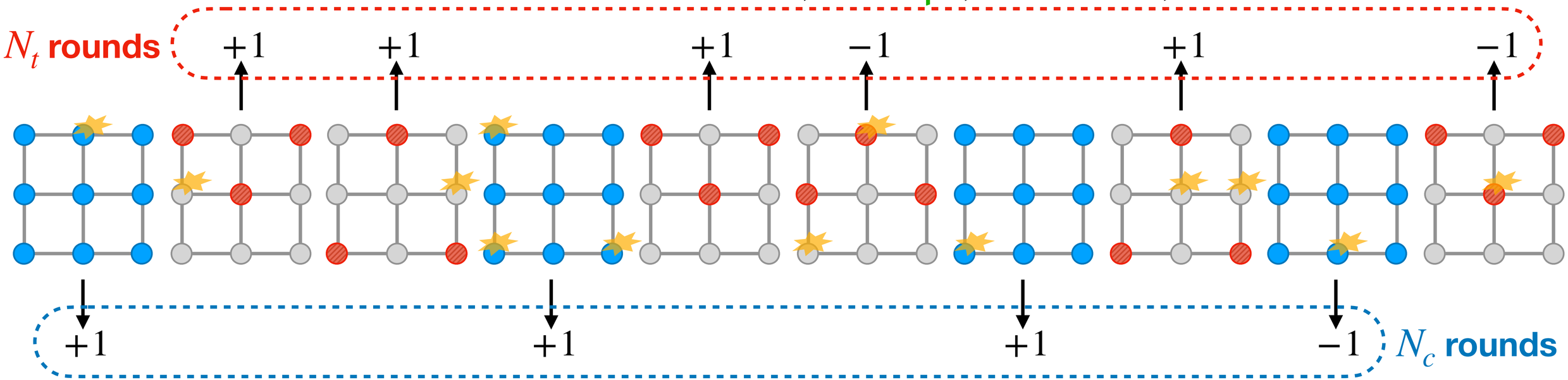
continuous output

Allowing **biased** output (up to an allowed extent)

Proposed secure protocol

Verifiable Blind Observable Estimation (VBOE)

Test rounds: if satisfied, Accept, otherwise, return Abort.



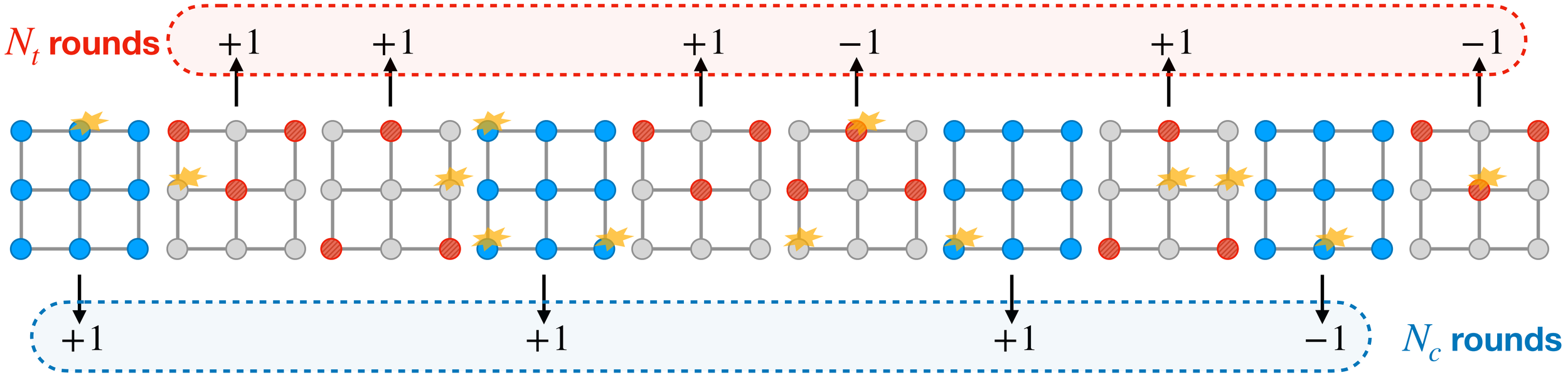
Computation rounds: If Accept, return $\tilde{o} = \frac{1}{N_c}\sum_{i=1}^{N_c} \tilde{y}_i$ to estimate $\mathrm{Tr}[\rho O]$.

Main theorem

Exponential composable security of VBOE

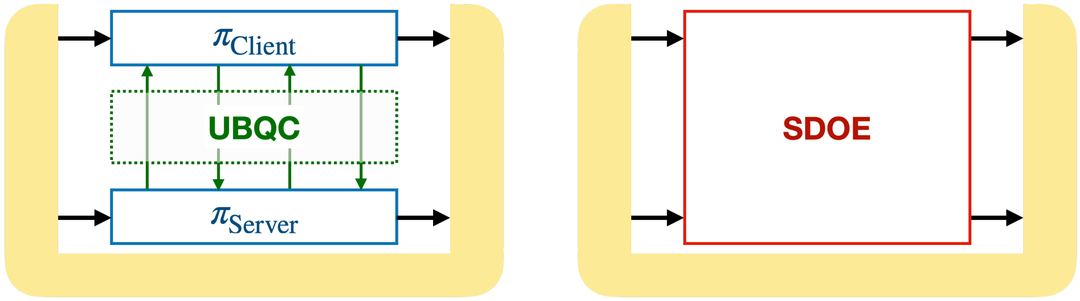
VBOE (ϵ, δ)-estimates $\mathrm{Tr}\left[\rho O\right]$ with exponentially small δ to N_c and N_t.

Exponentially small distinguishing advantage from SDOE,
i.e. $\delta = O\left(e^{-N_c} + e^{-N_t}\right)$.



Proof sketch

Correctness (vs honest, noise-free Server)

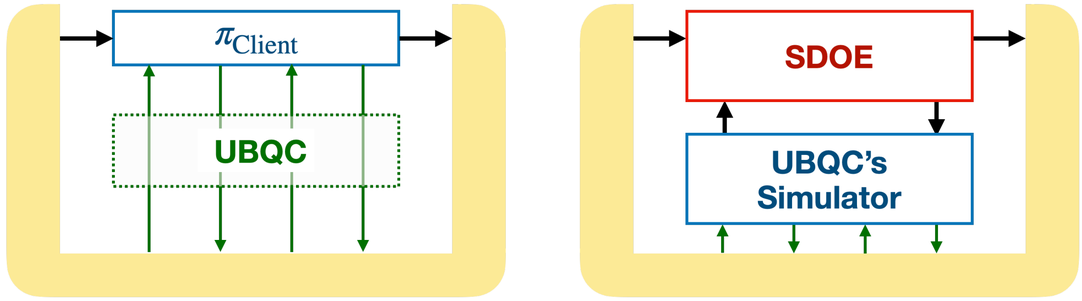


- VBOE always accepts
- SDOE further checks $\left|\hat{o} - \text{Tr}\left[\rho O\right]\right| \geq \epsilon$

↓ Difference in Accept/Abort probability

$$\Pr\left[\left|\hat{o} - \text{Tr}\left[\rho O\right]\right| \geq \epsilon\right] \leq 2\exp\left(-\frac{\epsilon^2}{2}N_c\right)$$

Security (vs malicious Server)



- Using composability of UBQC

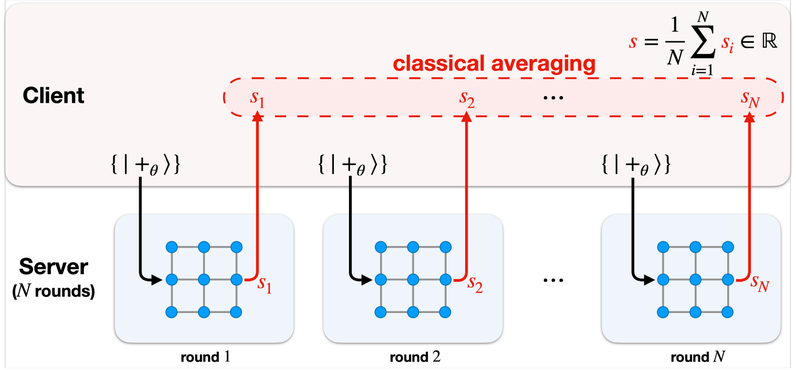
↓ Difference in Accept/Abort probability

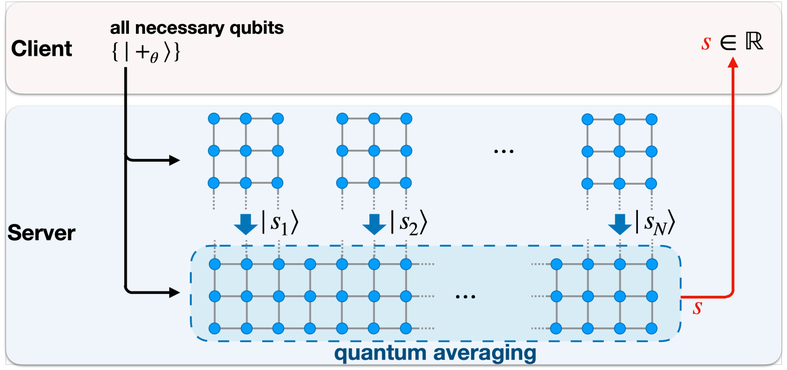
Distinguishability: $O\left(e^{-N_c} + e^{-N_t}\right)$

Impact of this work

Bridge between crypto-protocols and key quantum utility

- A new avenue for cryptographic **security analysis** of near-term quantum-classical hybrid **techniques with expectation values**
- The only known efficient **overhead-free** verification of near-term tasks with potential **quantum advantage**
- A convergence between foundational **cryptographic** theory and **physically** motivated quantum tasks

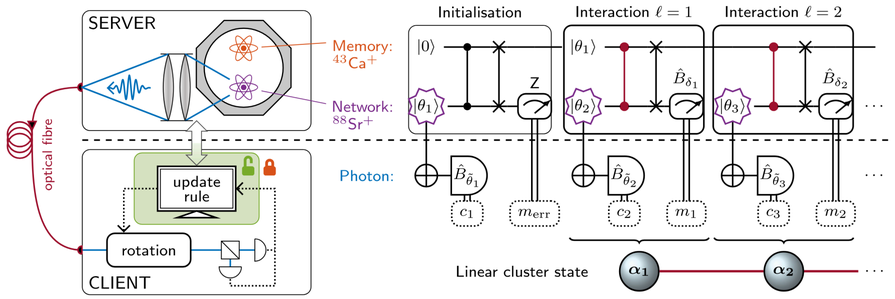




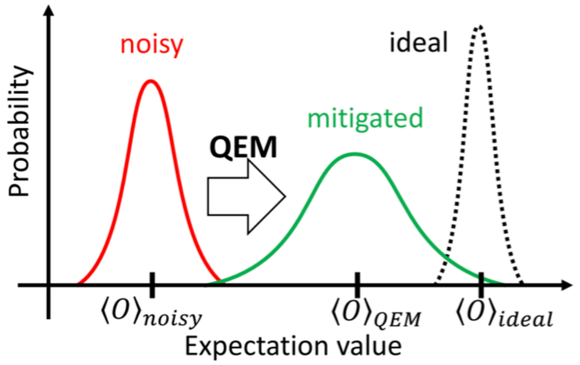
Future work

A broad class of applications of promising interest

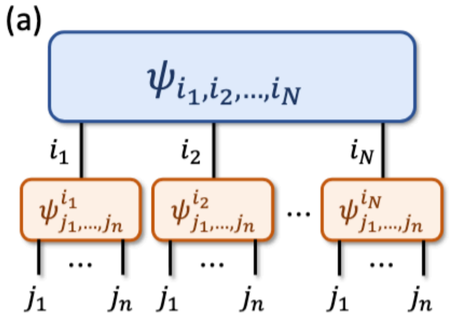
- Integration with **quantum error mitigation** and quantum-classical hybrid approaches
- Verifiable quantum advantage **experiments** on current hardware



Implementation in trapped-ion devices [Drmota et al. PRL2024]



Quantum error mitigation



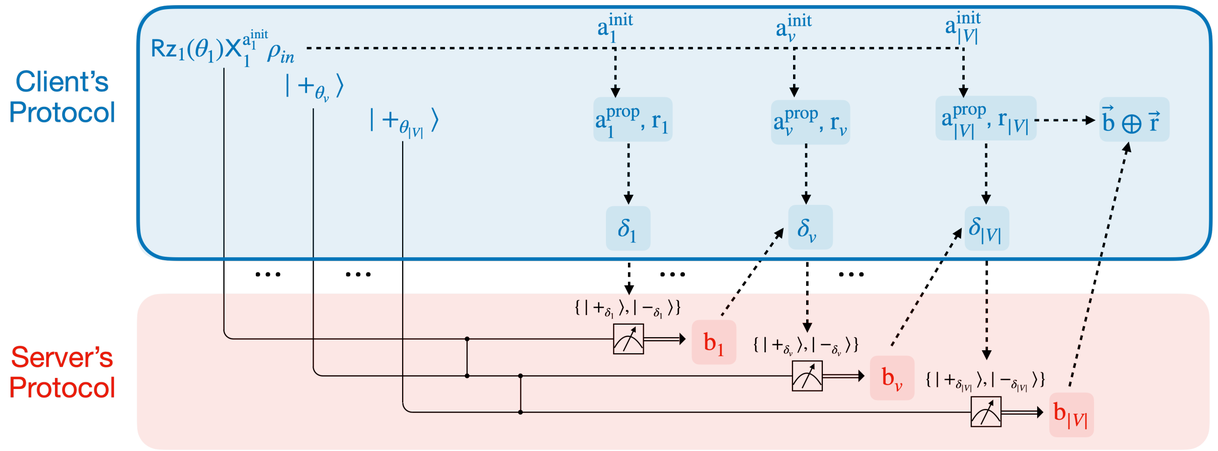
Hybrid tensor networks
[Harada et al. Quantum2025]

Link to our paper: https://www.arxiv.org/abs/2510.08548

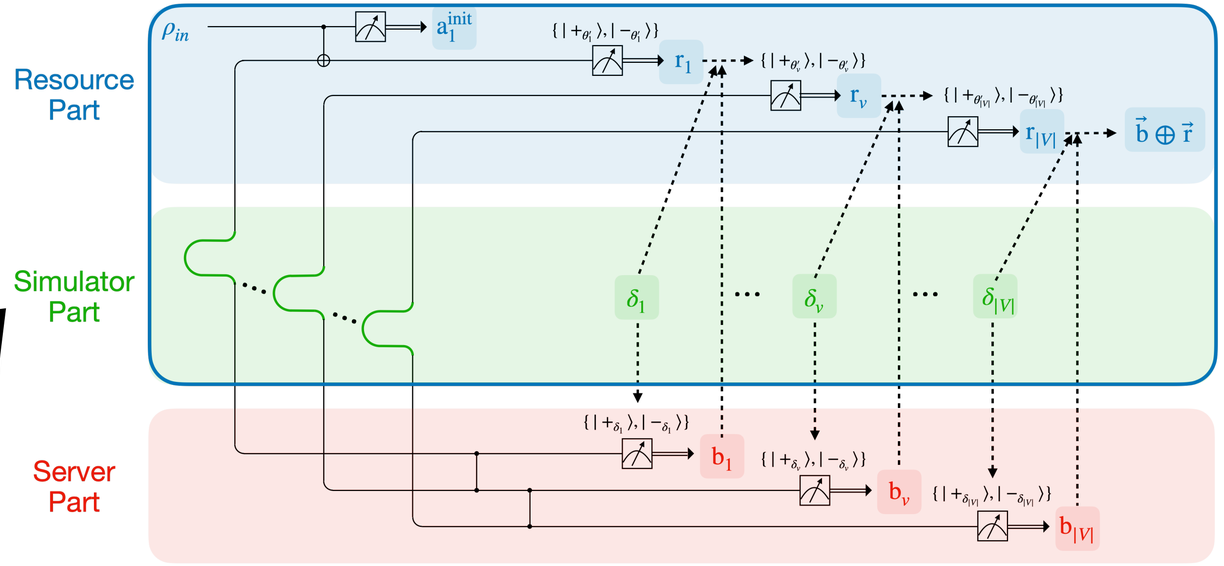
Appendix

https://scirate.com/arxiv/2510.08548

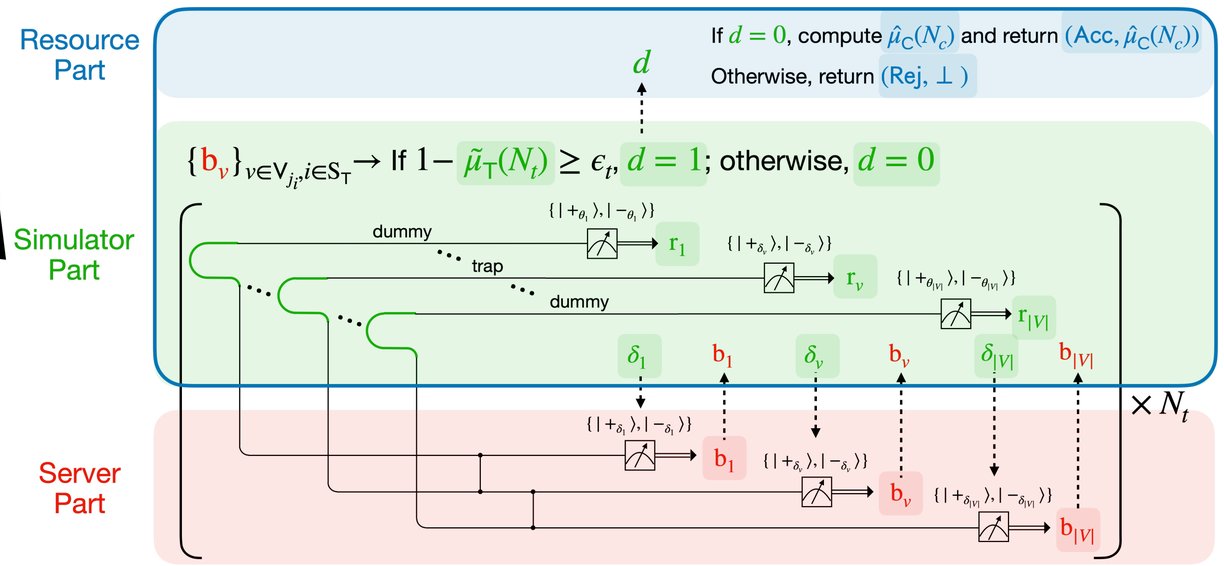
Separating Client's protocol of VBOE into **Resource Part** and **Simulator Part**



VBOE protocol



single computation round



test rounds