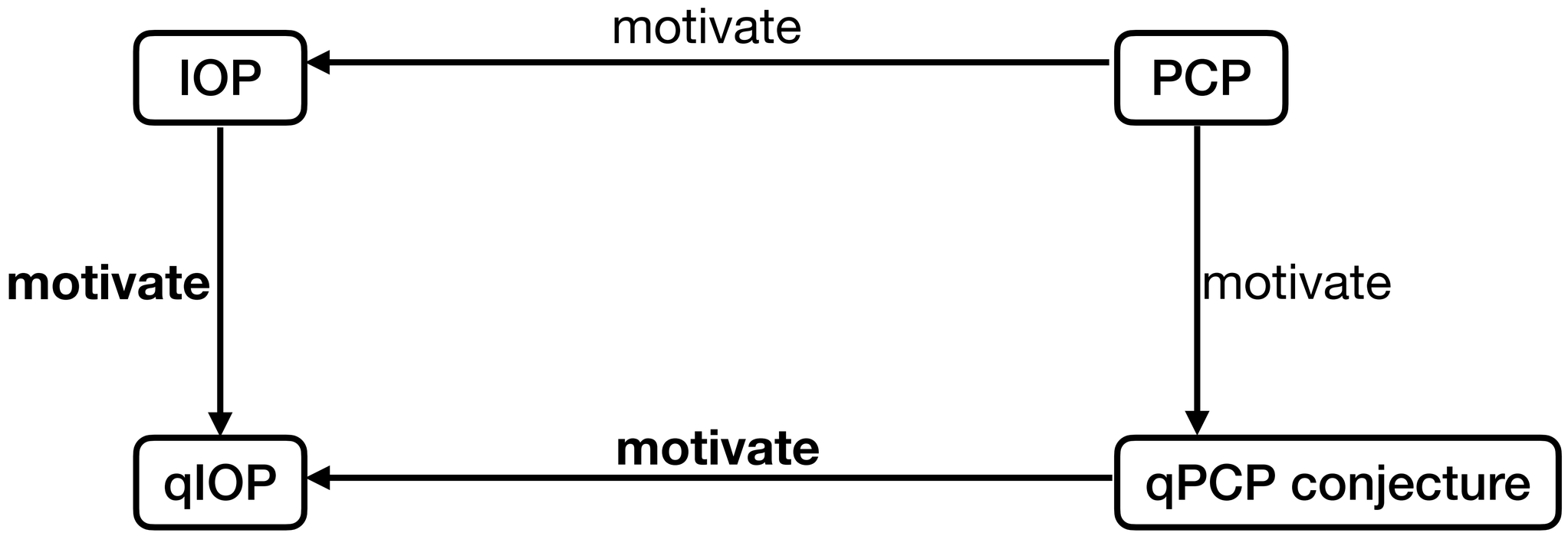
Probabilistically Checking Quantum Proofs, with Interaction

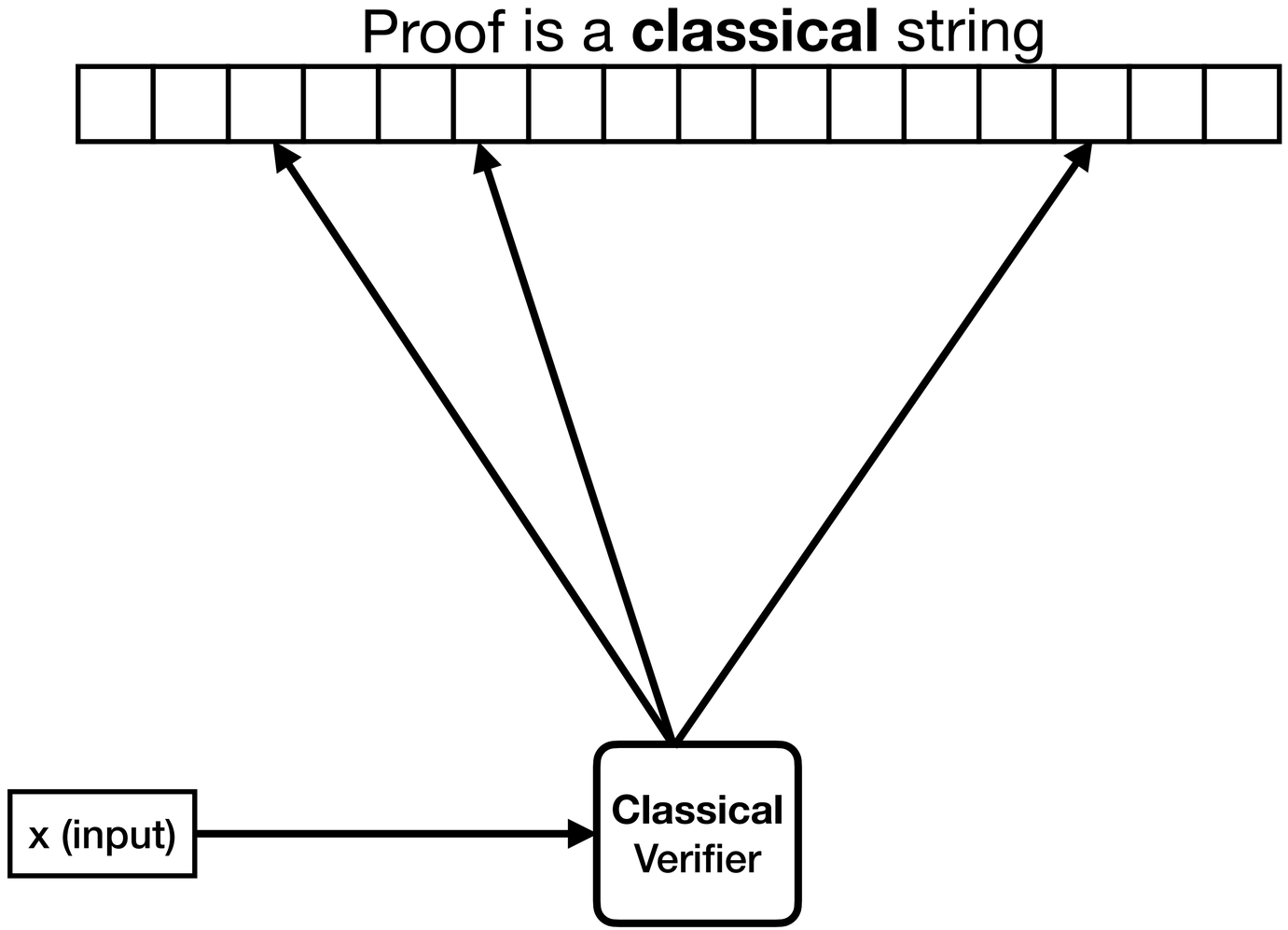
CCC 2026

Baocheng Sun (EPFL); work done while at WIS (co-authored with Thomas Vidick, WIS and EPFL)

Background


IOP
motivate
PCP
motivate
motivate
qIOP
motivate
qPCP conjecture

PCP Theorem

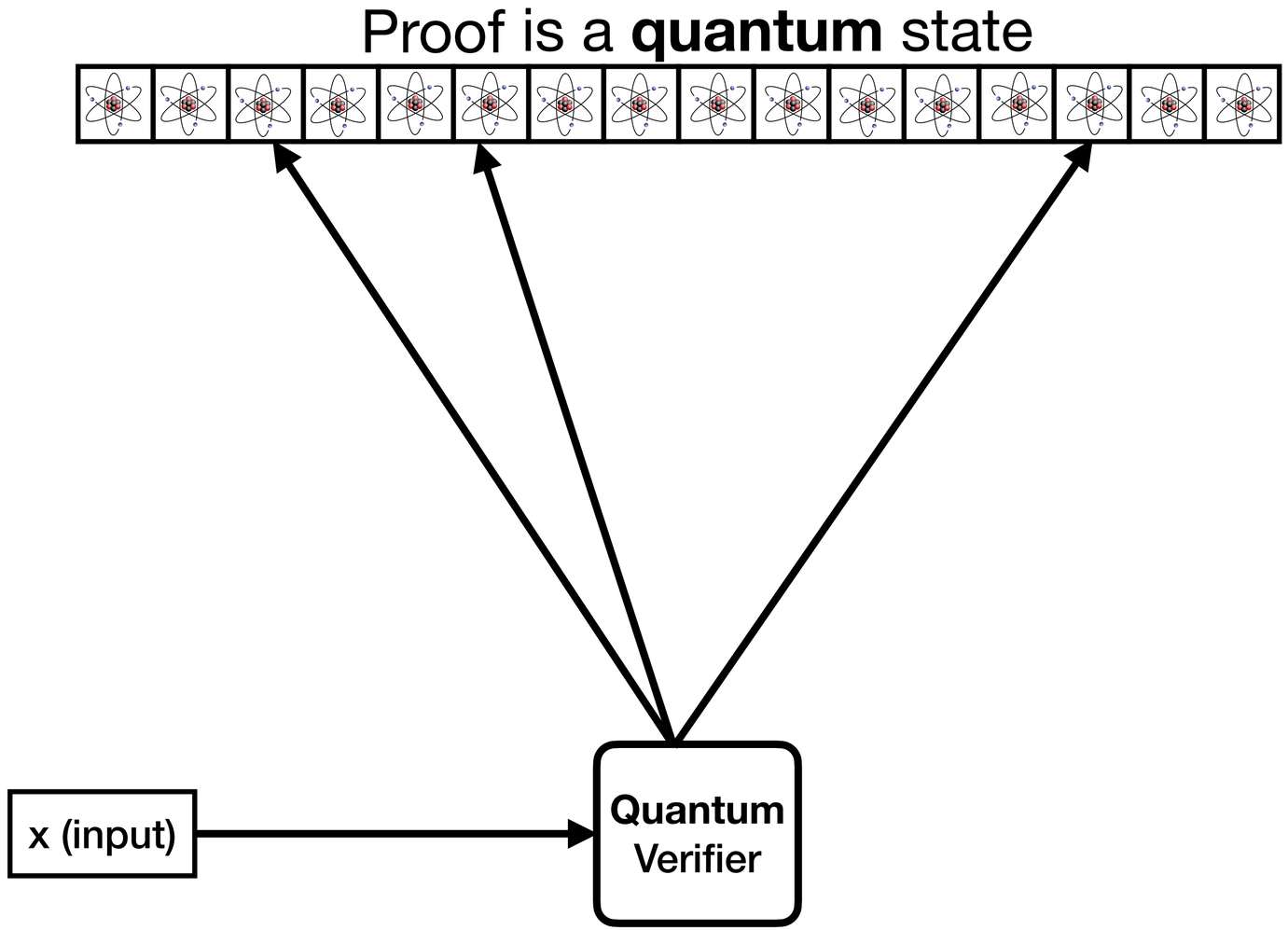


The length of the proof is poly(|x|)

query **O(1) classical bits**

$x \in \mathscr{L}$? $\mathscr{L}$ is an **NP** Language.

Quantum PCP Conjecture



The length of the proof is poly(|x|)

query **O(1) qubits**

$x \in \mathscr{L}$? $\mathscr{L}$ is an **QMA** Language.

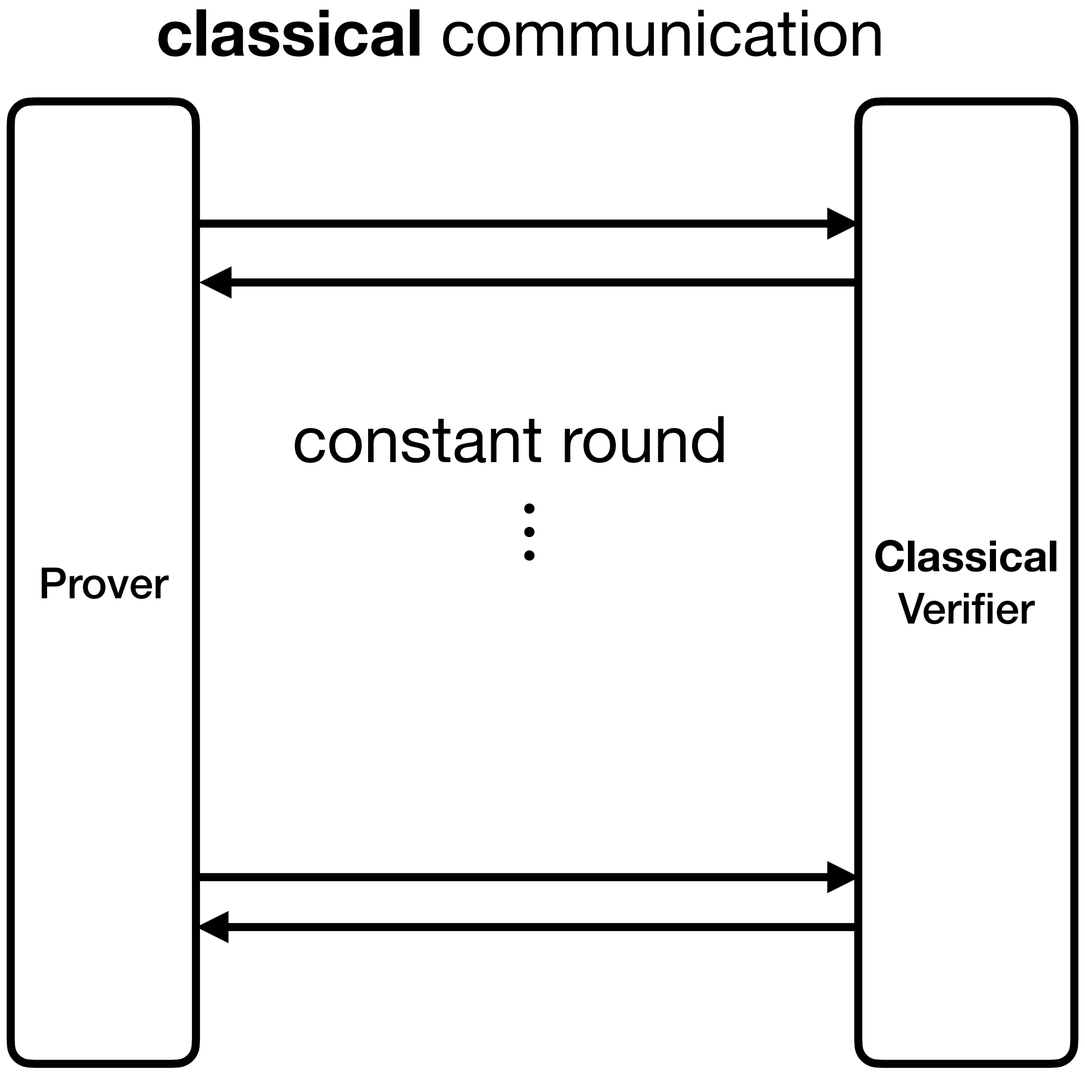
Wait, what do you mean by query?

Actually, it is not easy to provide a definition within an interactive context

If the classical (resp. quantum) verifier in PCP (resp. qPCP) invokes the following subroutine only once, we say it queries |S| bits (resp. qubits).

Classical	Quantum
Given $S \subseteq [n]$, apply a classical algorithm to the bits indexed by S along with some private bits.	Given $S \subseteq [n]$, apply a unitary to the prover's registers indexed by S, together with some private registers.

Interactive Oracle Proofs (IPs + PCPs)



communication complexity poly(|x|)

Each round the verifier query **O(1) bits**

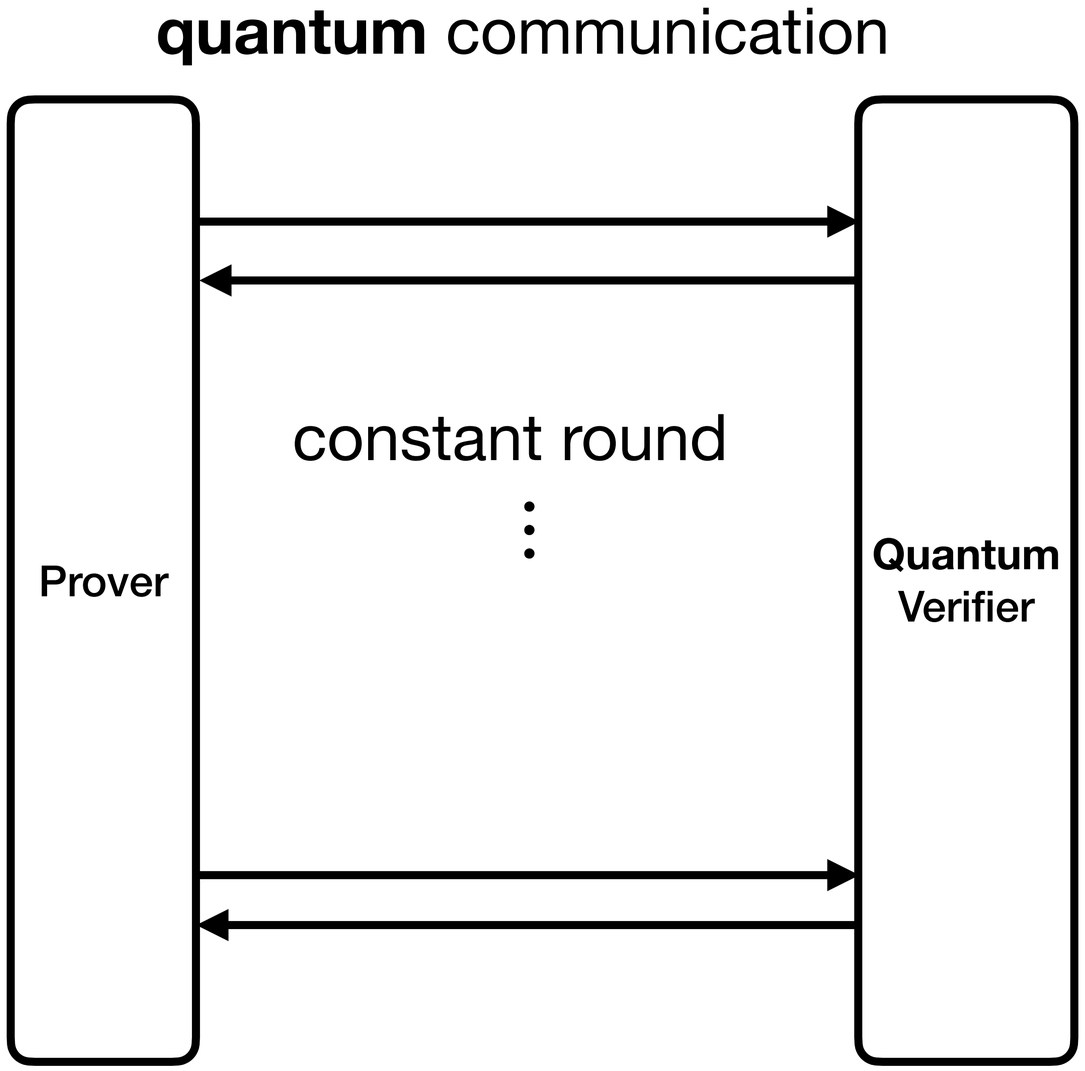
Moreover, the query set is chosen at the start of the protocol.

The honest prover is computationally efficient given access to the witness

$x \in \mathscr{L}$? $\mathscr{L}$ is an **NP** Language.

Our Models & Main Results

Quantum Interactive Oracle Proofs (IOPs + qPCPs)



communication complexity poly(|x|)

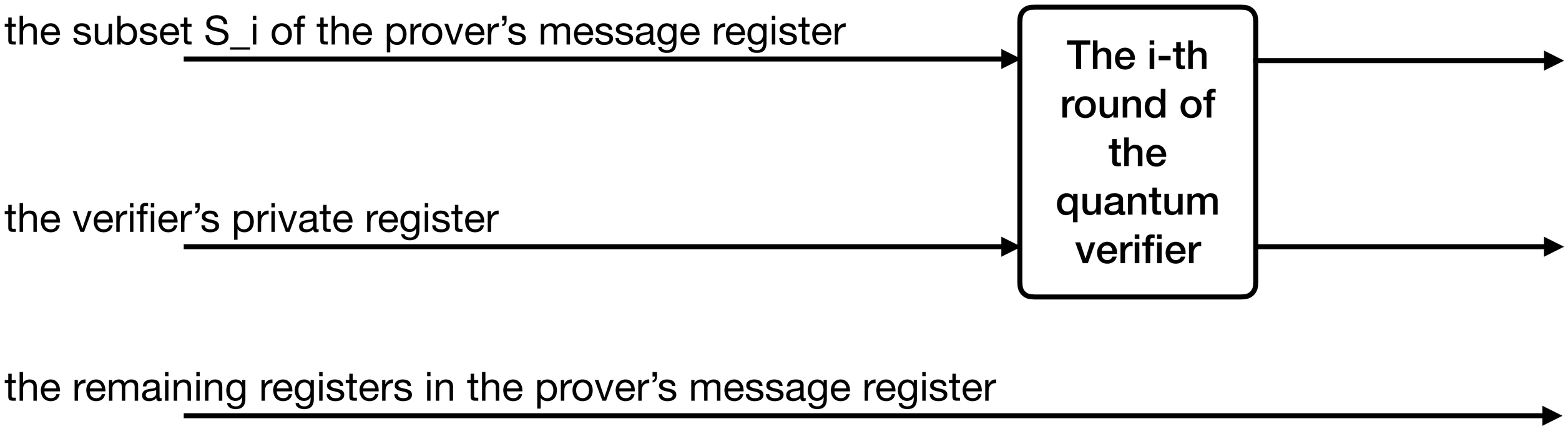
Each round the verifier query **O(1) qubits**

Moreover, the query set is chosen at the start of the protocol

The honest prover is computationally efficient given access to the witness

$x \in \mathscr{L}$? $\mathscr{L}$ is an **QMA** Language.

Recall the Definition of a Query



Extended Verifier Permissions

Classical	Quantum
Operating on a bit is detectable	Operating on a single qubit is not detectable

We allow the verifier to send the prover's message back! (and it should not be counted as the whole message being read.)

Our Previous Results (A Too Weak Model)

Should we allow any other type of messages?: If the verifier is allowed to **send general quantum messages** to the prover **(general model)**, then this is a **“simple”** construction of the desired qIOP system.

But we are not satisfied

The model grants the verifier too much power.

Baocheng Sun and Thomas Vidick. Quantum interactive oracle proofs. In Theory of Cryptography Conference (TCC). Springer-Verlag, 2025.

Our Previous Results (A Too Strong Model)

In the **more restricted model (strong model)**, where the verifier is only allowed to **return the prover's quantum messages** and **send classical messages**, we also construct a desired qIOP system except that the **communication complexity is exponential.**

But we are not satisfied

By definition, a qPCP implies a strong qIOP with the desired parameters.

This suggests that interesting results may also exist in models that are less restrictive.

Baocheng Sun and Thomas Vidick. Quantum interactive oracle proofs. In Theory of Cryptography Conference (TCC). Springer-Verlag, 2025.

Our Main Result

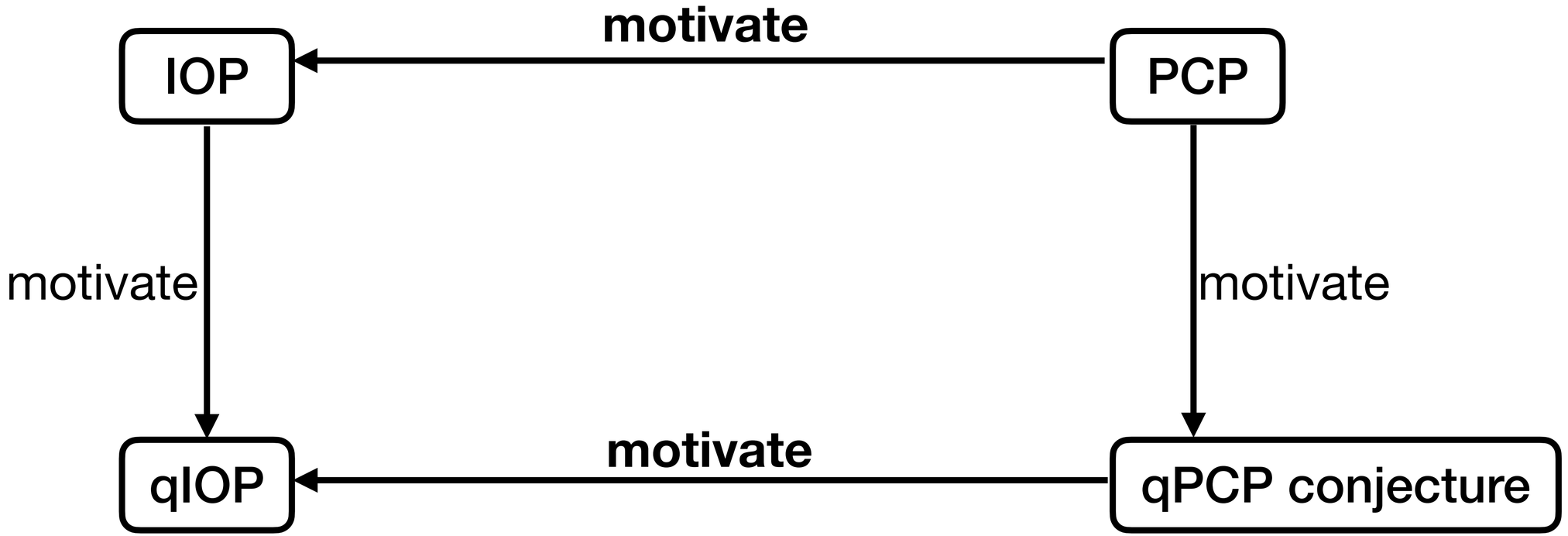
When we also allow the verifier to send back only a portion of the prover's message, either now or at a later time, without counting the complexity of that part (refined model), we construct a desired qIOP system with polylog queries, polylog rounds, and poly communication.

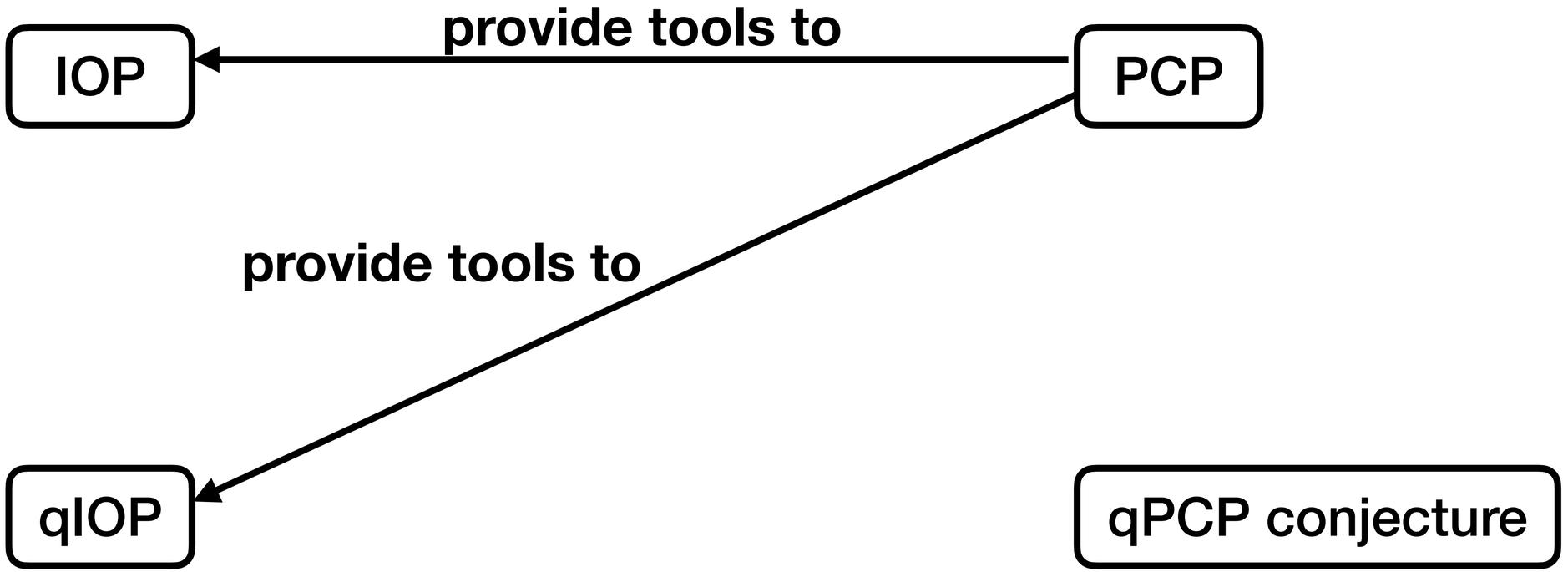
Moreover, if we have a good quantum LTC (constant relative rate, relative distance, and soundness, and constant-size parity checks), the query complexity and number of rounds in our protocol can also be reduced to constant.

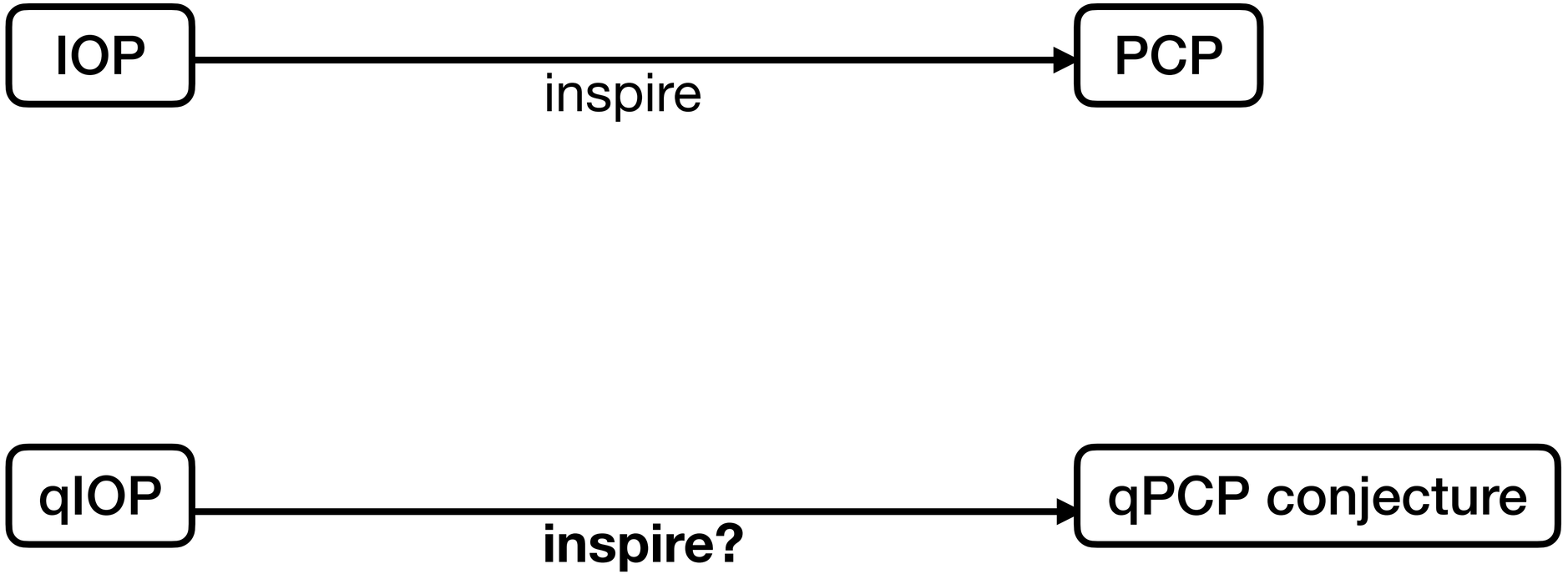
verifier is allowed to	send classical messages	send general quantum messages	return the prover's quantum messages	return only a portion of the prover's quantum messages, either now or at a later time
General model	Y	Y	Y	Y
Refined model	Y		Y	Y
Strong model	Y		Y	

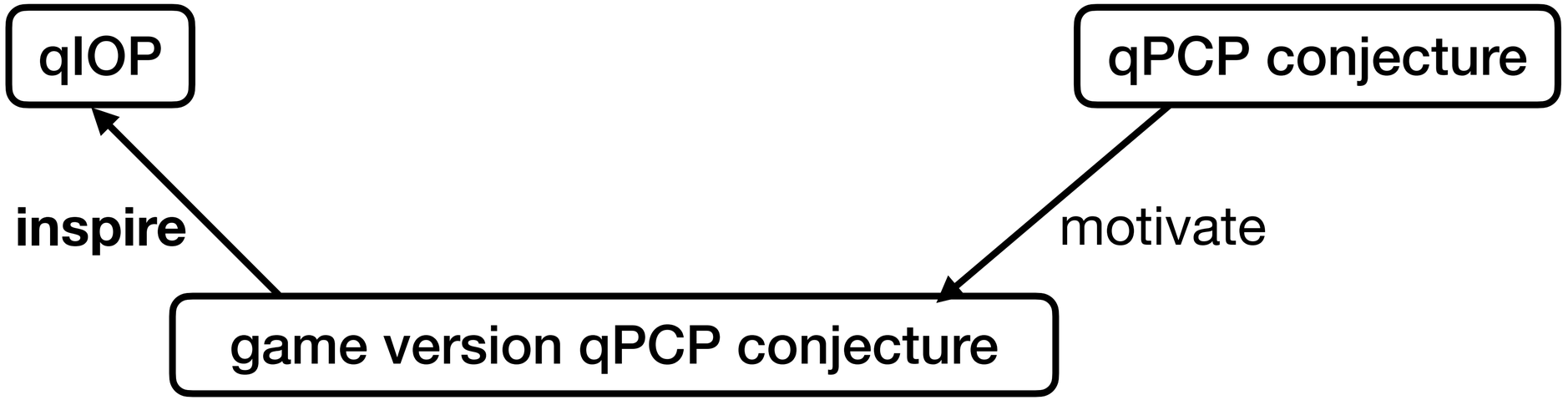
	Rounds	Query qubits	Communication complexity	Prover's efficiency
General model	O(1)	O(1)	poly	poly
Refined model	O(polylog)	O(polylog)	poly	poly
Strong model	O(1)	O(1)	exp∘poly	logarithmic depth

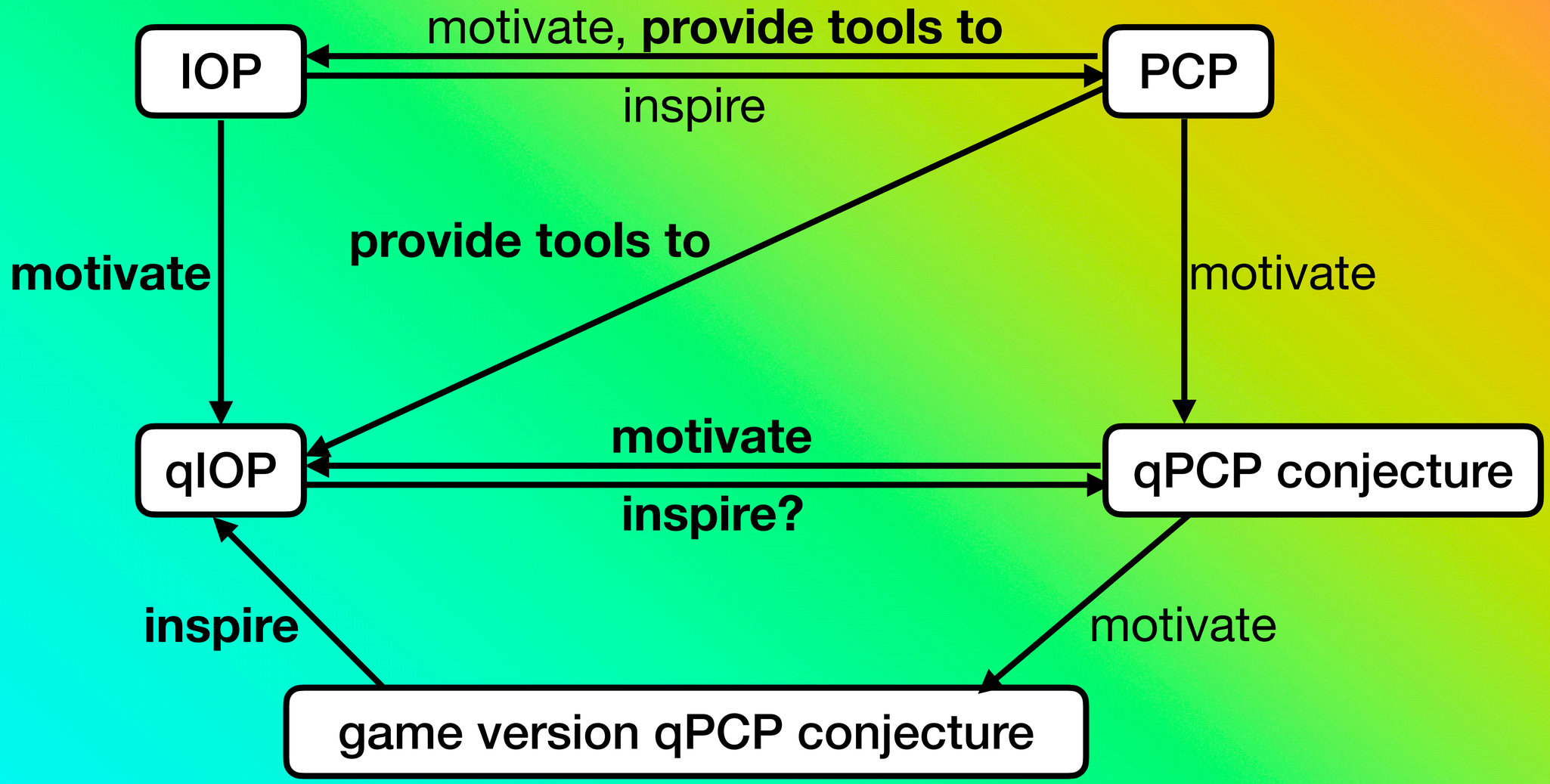
Related Works


motivate
IOP
PCP
motivate
motivate
motivate
qIOP
qPCP conjecture


provide tools to
IOP
PCP
provide tools to
qIOP
qPCP conjecture


IOP
inspire
PCP
qIOP
inspire?
qPCP conjecture


qIOP
qPCP conjecture
inspire
motivate
game version qPCP conjecture


IOP
motivate, provide tools to
PCP
inspire
motivate
provide tools to
motivate
qIOP
motivate
qPCP conjecture
inspire?
inspire
motivate
game version qPCP conjecture

Exponential-length classical PCP for QMA

QMA⊆NEXP=PCP[poly,O(1)]

But, this PCP construction is nowhere near efficient.

Delegating Quantum Computation

1. We have a very similar goal.
2. In most works on the subject, both the communication and the verifier are classical.
3. They can achieve polylog communication.
4. They also use many qubits tests from the game version of the qPCP literature.
5. But they rely on **crypto assumptions**.

Open Questions

Open Questions

1. Potential limitations on the quantum IOP model?
2. Compile quantum IOPs into quantum PCPs?
3. Construct quantum IOPs under restricted models with polynomial communication complexity?
4. Delegate quantum computation under minimal cryptographic assumptions?
5. Develop a cryptographic analogue of the quantum PCP theorem?
6. Design proof systems for QMA with classical communication?

Sketch of the Proofs

The QMA Complete Problem

Dual-Basis Projector Hamiltonian

$$H = \frac{1}{2}(\Pi^Z + \Pi^X)$$

where Π^Z and Π^X are normalized averages of **local** projections diagonal in the computational and Hadamard basis (Z and X basis) respectively.

$$H^{amp} = \frac{1}{2}(\Pi^{Z,amp} + \Pi^{X,amp})$$

where $\Pi^{Z,amp}$ and $\Pi^{X,amp}$ are normalized averages of **non-local** projections diagonal in the Z and X basis respectively.

Thiago Bergamaschi, Tony Metger, Thomas Vidick, and Tina Zhang. Derandomised tensor product gap amplification for quantum Hamiltonians. arXiv preprint arXiv:2510.01333, 2025.

Henry Ma and Anand Natarajan. Two bases suffice for QMA1-completeness. arXiv preprint arXiv:2509.24390, 2025.

Dual-Basis Projector Hamiltonian

- Start with a local hamiltonian with XZ-terms
- Build Kitaev's construction on the verification circuit of the XZ-hamiltonian
- For a gate in the Z basis, reading off the correct time is also done in the Z basis, but advancing the time is done in the X basis.

Henry Ma and Anand Natarajan. Two bases suffice for QMA1-completeness. arXiv preprint arXiv:2509.24390, 2025.

Dual-Basis Projector Hamiltonian

$$|\Phi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |\psi_t\rangle_{comp} \otimes |t\rangle_{clock} \qquad |\psi_t\rangle = U_t U_{t-1} \ldots U_1 |\psi_0\rangle \qquad |t\rangle_{clock} = |\underbrace{1 \ldots 11}_{t} \underbrace{00 \ldots 0}_{T-t}\rangle$$

$$H = H_{in} + H_{out} + H_{clock} + H_{prop}$$

$$H_{in} = \sum_{i \in ancilla} |1\rangle\langle 1|_i \otimes |0\rangle\langle 0|_{clock} \qquad H_{out} = |0\rangle\langle 0|_{accept} \otimes |T\rangle\langle T|_{clock} \qquad H_{prop} = \sum_{t=1}^{T} H_{prop,t}$$

$$H_{prop,t} = \frac{1}{2} |1\rangle\langle 1|_{t-1} \otimes \left(I_{comp} \otimes I_t - U_t \otimes X_t \right) \otimes |0\rangle\langle 0|_{t+1} \qquad if \quad U_t = U_t^\dagger$$

Henry Ma and Anand Natarajan. Two bases suffice for QMA1-completeness. arXiv preprint arXiv:2509.24390, 2025.

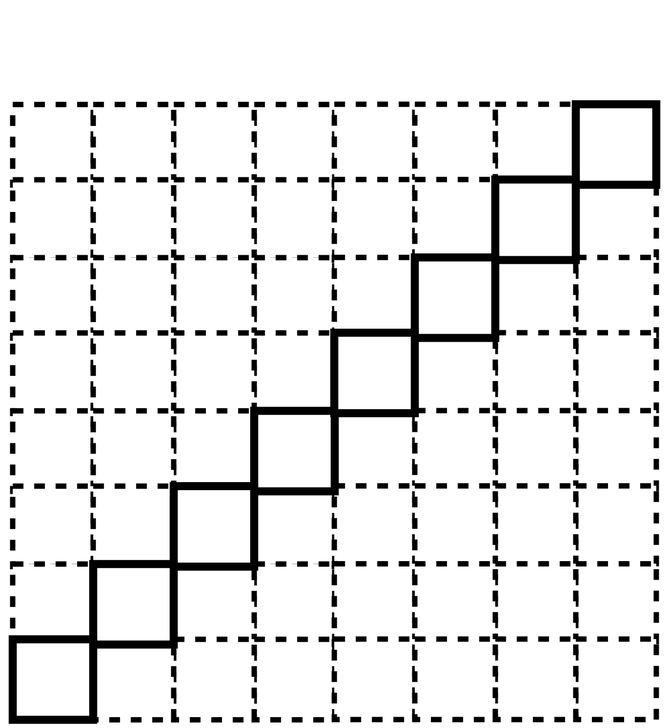
Dual-Basis Projector Hamiltonian

- So we simply introduce a second clock register in the X basis for time advancing.
- We move alternately, first a gate in the Z basis, then a gate in the X basis.
- The X and Z times can differ by at most one. When plotted on a 2D grid, the valid values occupy the squares along the diagonal.
- We do not directly check the consistency between the X and Z clocks. Instead, consistency is enforced naturally. If there is a mismatch between the Z-clock and the X-clock, the time-forwarding step, say an X flip, will produce an invalid Z-clock state.

Henry Ma and Anand Natarajan. Two bases suffice for QMA1-completeness. arXiv preprint arXiv:2509.24390, 2025.

Dual-Basis Projector Hamiltonian

$$U_t = \begin{cases} \text{diagonal in the } X\text{-basis}, & t \text{ is even} \\ \text{diagonal in the } Z\text{-basis}, & t \text{ is odd} \end{cases}$$

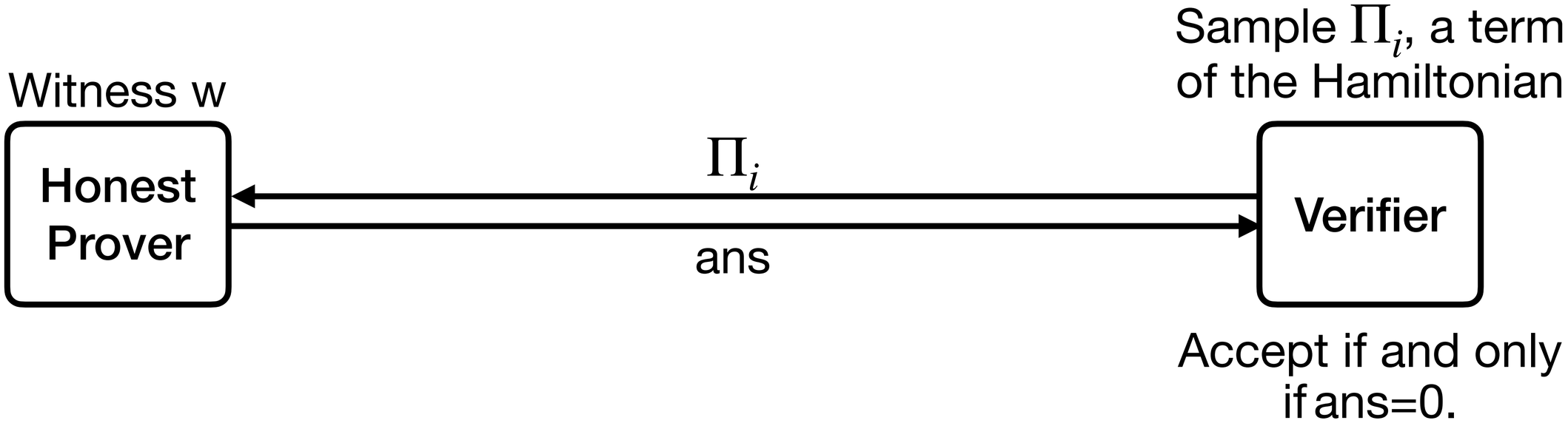


Henry Ma and Anand Natarajan. Two bases suffice for QMA1-completeness. arXiv preprint arXiv:2509.24390, 2025.

The Framework

Framework for Verifying Computation

With a flavor of MIP* (game version qPCP) techniques



Framework for Verifying Computation

With a flavor of MIP* (game version qPCP) techniques

- (Many qubits test) With some probability, the verifier runs a Many qubits test protocol.
- (Energy test) With some probability, the verifier runs a Energy test protocol.

The principle is that the verifier wants the prover to do something strong enough (which usually means "qubit" operations) that implies the energy test without cheating.

What Is a Qubit?

Course FSMP, Fall'20: Interactions with Quantum Devices, Thomas Vidick

A qubit is a triple $(|\psi\rangle, O_X, O_Z)$ such that

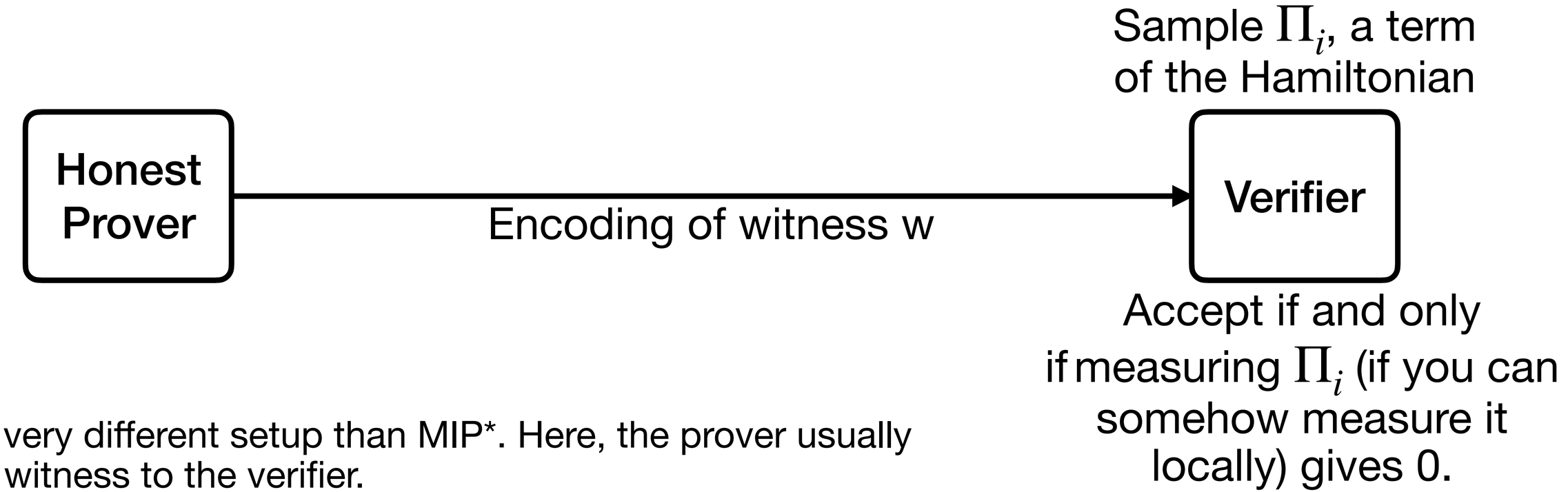
- $\||\psi\rangle\| = 1,$
- O_X and O_Z are Hermitian operators such that $\{O_X, O_Z\}|\psi\rangle = 0,$
- where $\{O_X, O_Z\} = O_X O_Z + O_X O_Z.$

$\Longleftrightarrow$

- $O_X =_{|\psi\rangle} V^\dagger X V$
- $O_Z =_{|\psi\rangle} V^\dagger Z V$
- where V is an isometry
- where $A =_{|\psi\rangle} B$ iff $\|(A - B)|\psi\rangle\| = 0$

Framework for Verifying Computation

With a flavor of PCP techniques



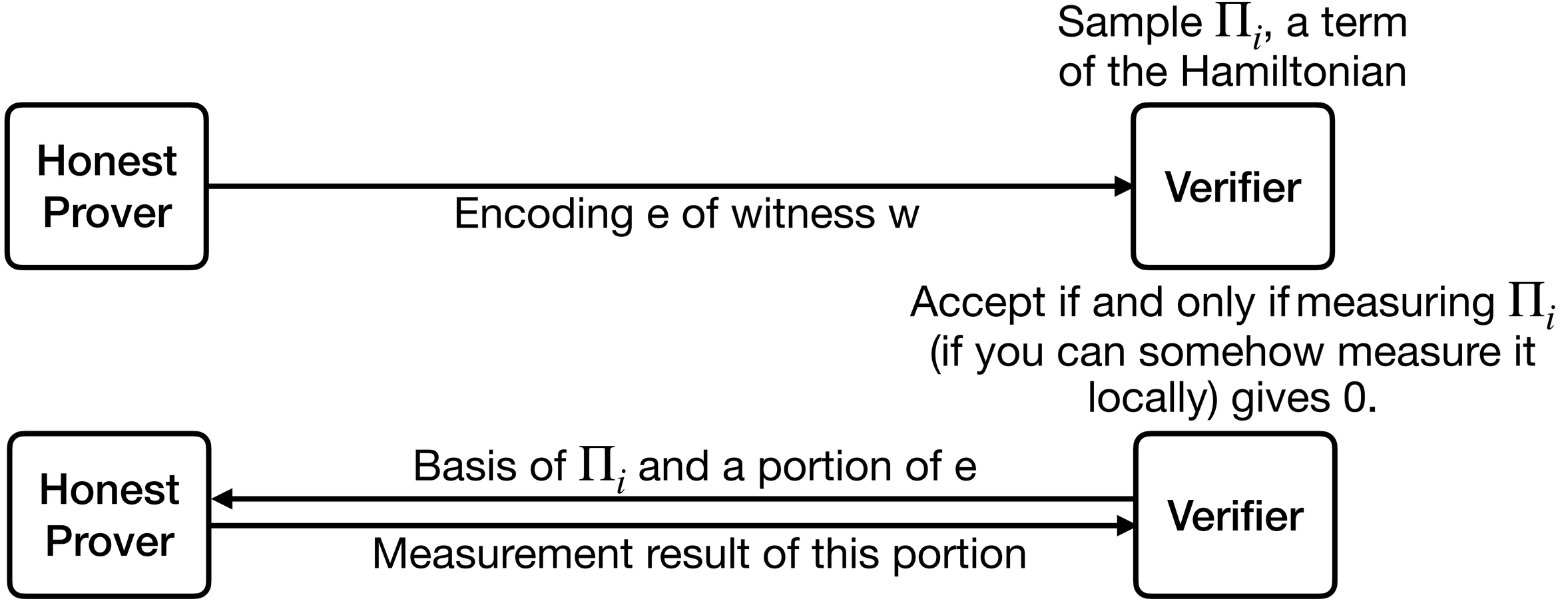
QIP is a very different setup than MIP*. Here, the prover usually sends a witness to the verifier.

For example, this means that the verifier can actually measure some qubits themselves (and this is a source of free “qubit”).

An Alternative Approach Towards Many Qubits Tests

- The prover sends the verifier the qLTC encoding of the quantum witness.
- The verifier sends the prover its choice of basis.
- The prover and verifier run the Global Measurement Extraction. In the honest case, at the end of the extraction both parties hold a copy of the qLTC codeword measured in the chosen basis (in some sense, our many-qubit test).
- The verifier sends the prover a term of the Hamiltonian, and the two run a PCPP (the energy test).

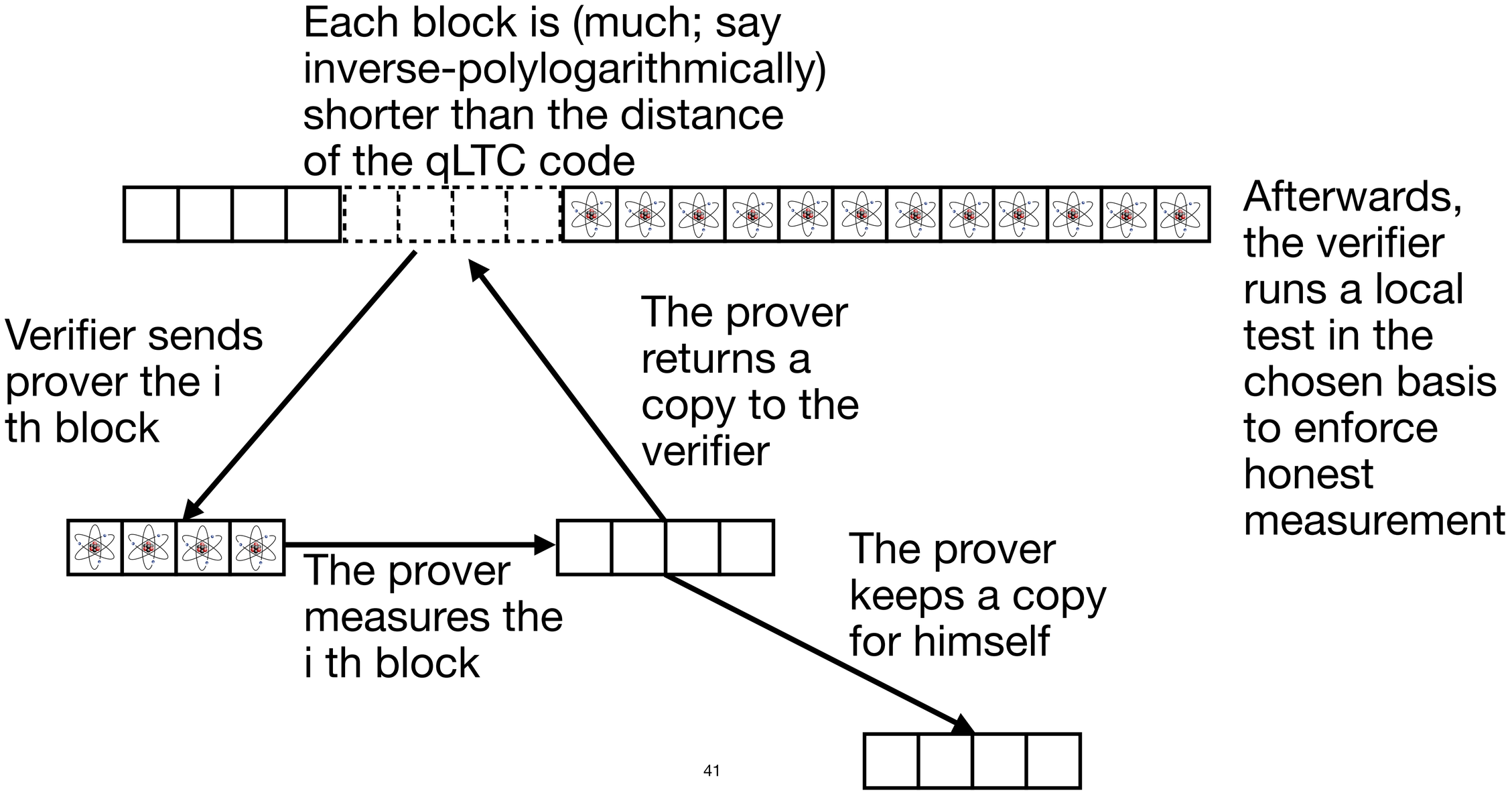
An Alternative Approach Towards Many Qubits Tests



The prover's behavior reflects key features of the desired qubit operation, as they are restricted from flipping too many measurement outcomes. So, we have a “qubit” in each position w.h.p. However, before the entire Global Measurement Extraction process finishes, we do not have any actual “qubits”.)

Global Measurement Extraction

ith round; 2nd round here



Thank you for your attention!

THIS PAGE IS INTENTIONALLY LEFT BLANK

THE FOLLOWING PAGES ARE DEPRECATED