Title: Non-interactive zero-knowledge arguments for QMA, with preprocessing

Speakers: Andrea Coladangelo

Series: Perimeter Institute Quantum Discussions

Date: September 30, 2020 - 4:00 PM

URL: http://pirsa.org/20090023

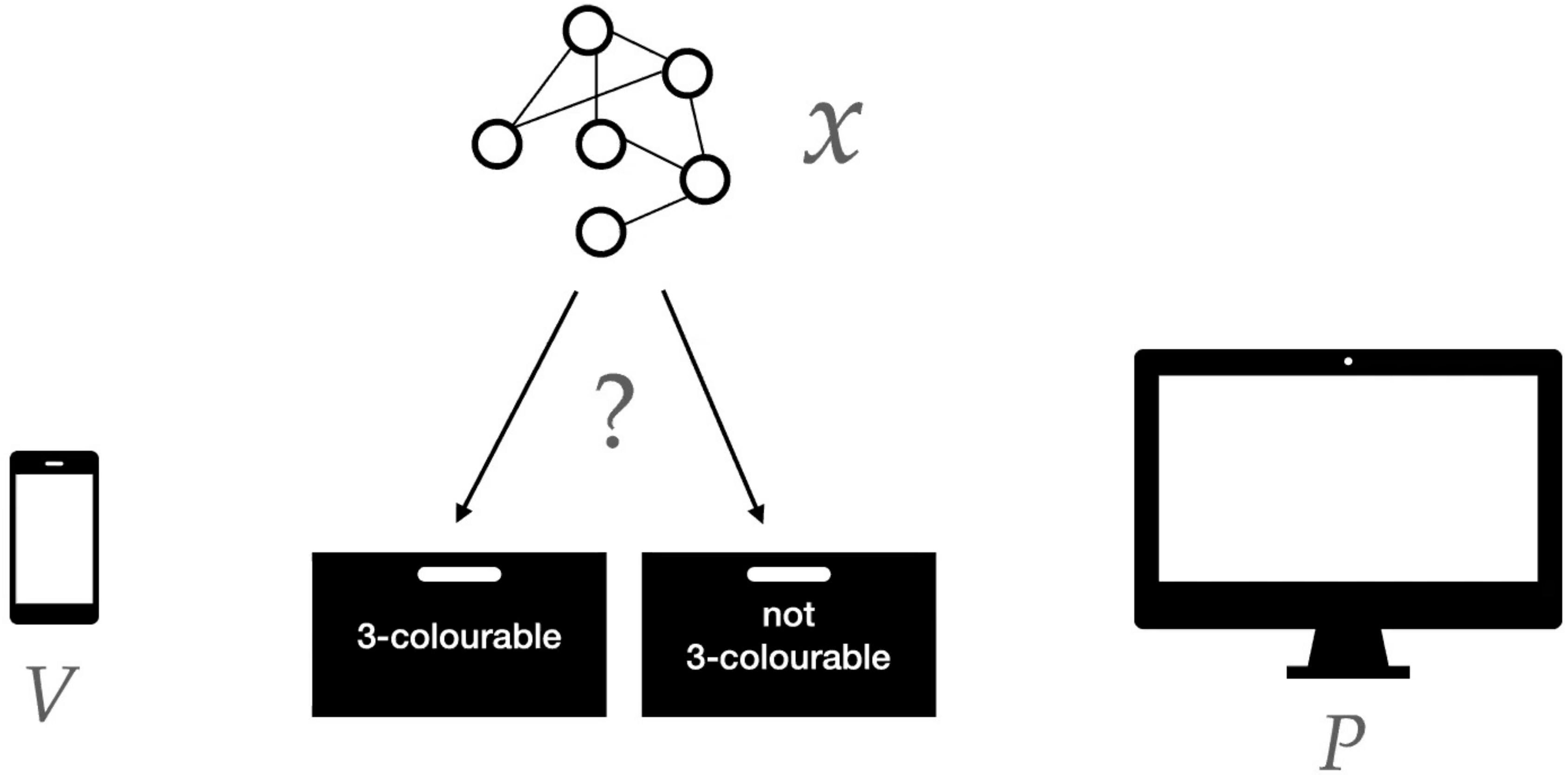
Abstract: Zero-knowledge proofs are one of the cornerstones of modern cryptography. It is well known that any language in NP admits a zero-knowledge proof. In the quantum setting, it is possible to go beyond NP. Zero-knowledge proofs for QMA have first been studied in a work of Broadbent et al (FOCS'16). There, the authors show that any language in QMA has an (interactive) zero-knowledge proof. In this talk, I will describe an idea, based on quantum teleportation, to remove interaction at the cost of adding an instance-independent preprocessing step. Assuming the Learning With Errors problem is hard for quantum computers, the resulting protocol is a non-interactive zero-knowledge argument for QMA, with a preprocessing step that consists of (i) the generation of a Common Reference String and (ii) a single (instance-independent) quantum message from the verifier to the prover.

This is joint work with Thomas Vidick and Tina Zhang

Non-interactive zero-knowledge arguments for QMA, with preprocessing

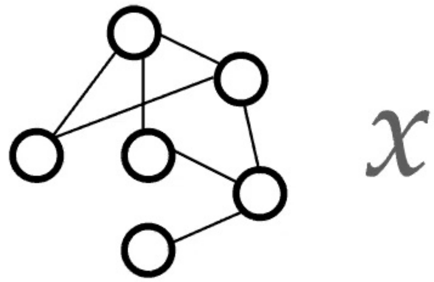
Andrea Coladangelo, Thomas Vidick, Tina Zhang

Proof–system for an NP problem



Argument

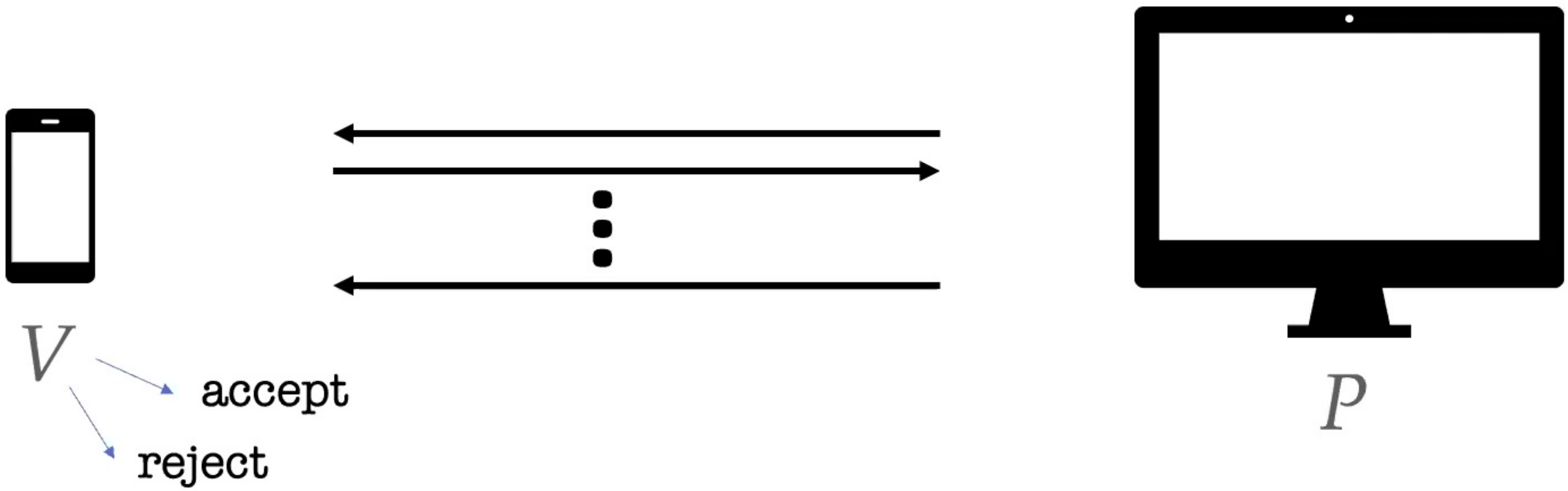
~~Proof~~-system for an NP problem



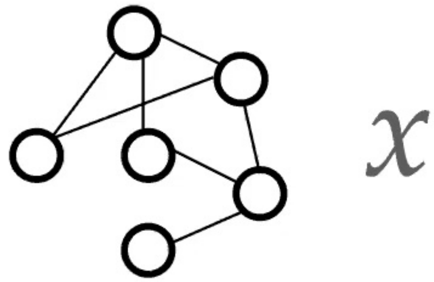
Completeness: If x is a **yes-instance**, P is accepted with probability 1.

Soundness: If x is **no-instance**, any P^* is accepted with probability at most $1 - 1/poly(n)$

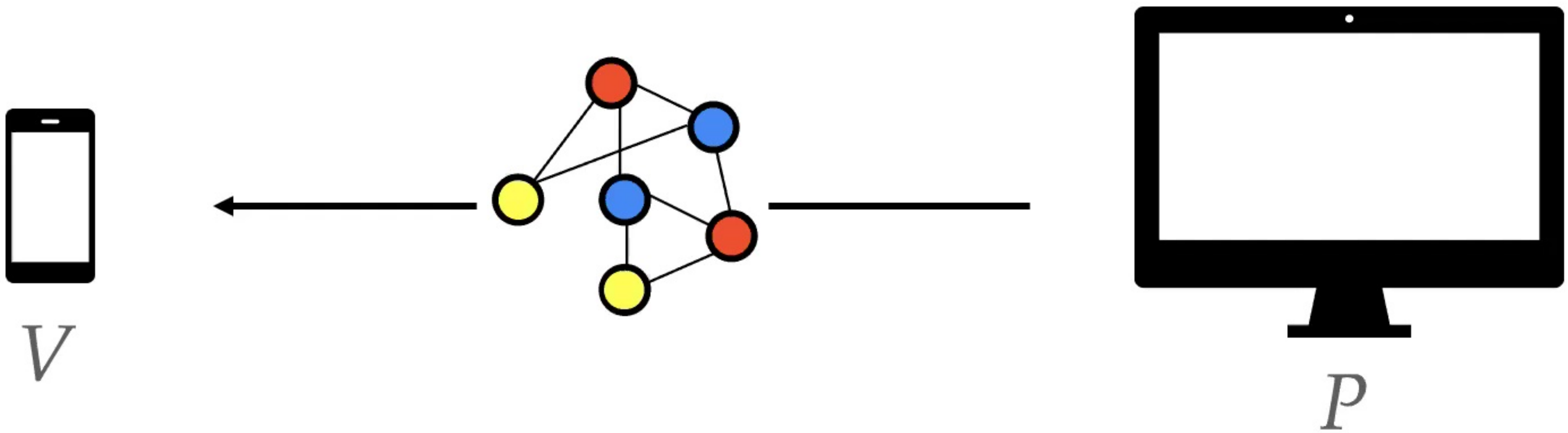
Computationally bounded



Proof–system for an NP problem

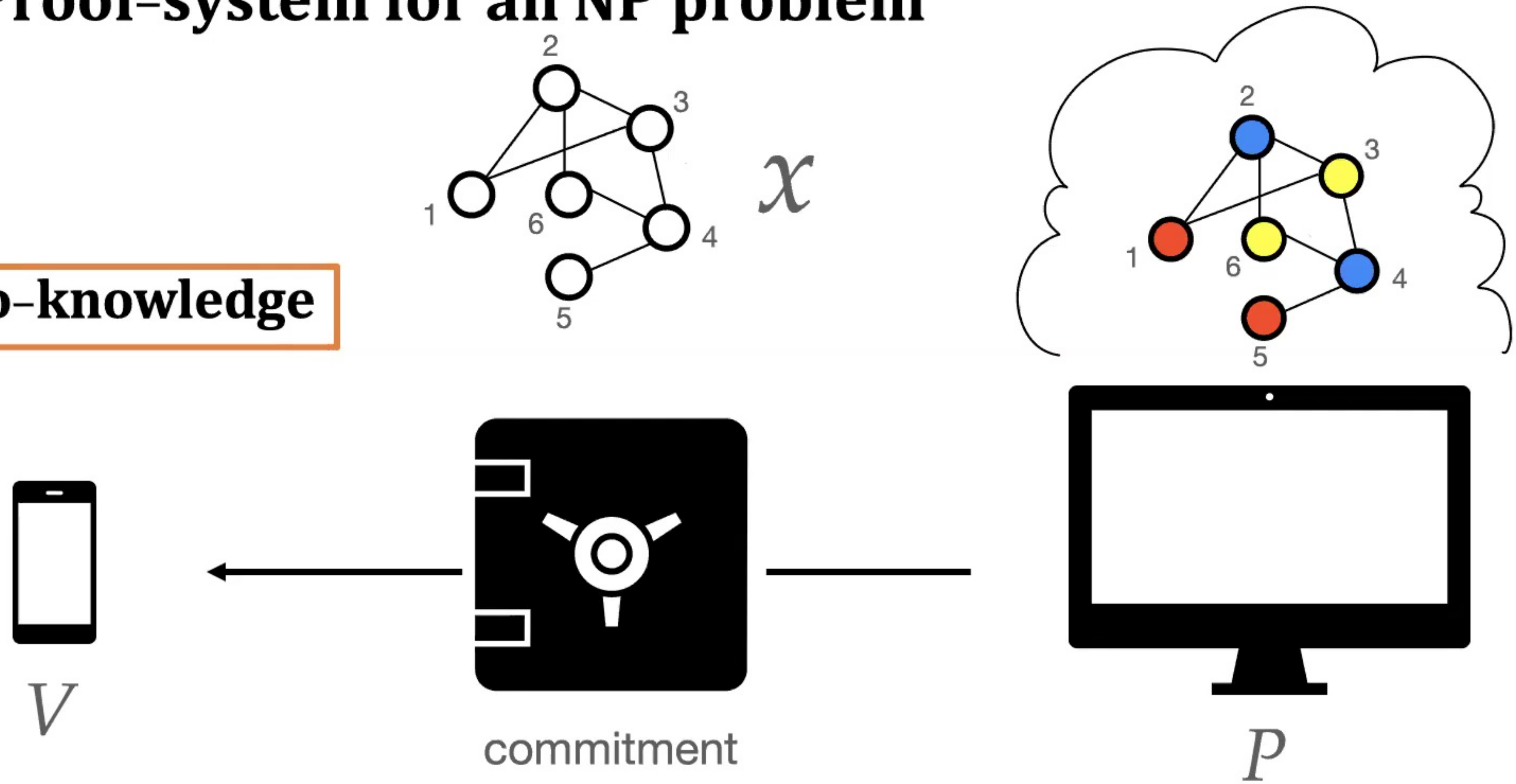


The trivial protocol

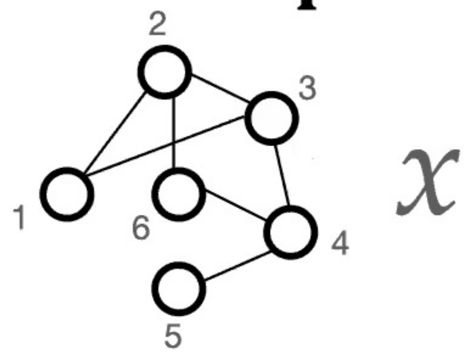


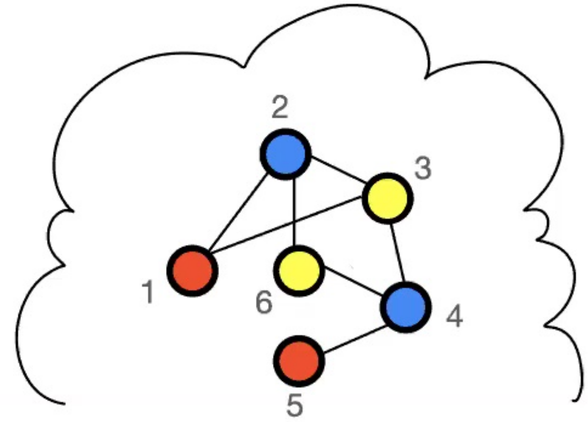
Proof-system for an NP problem

Zero-knowledge

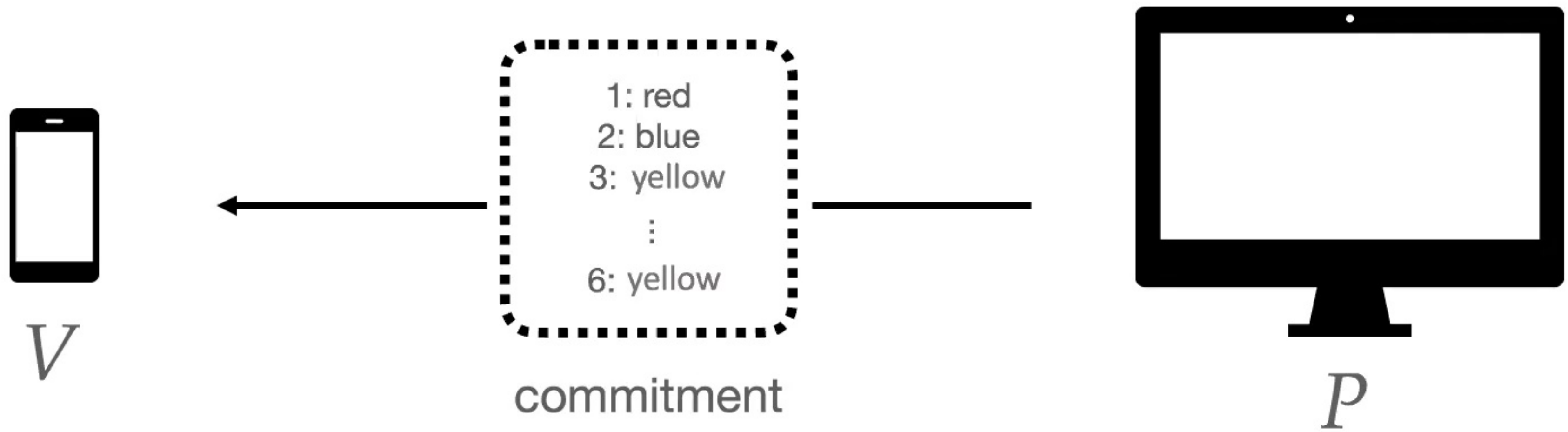


Proof-system for an NP problem

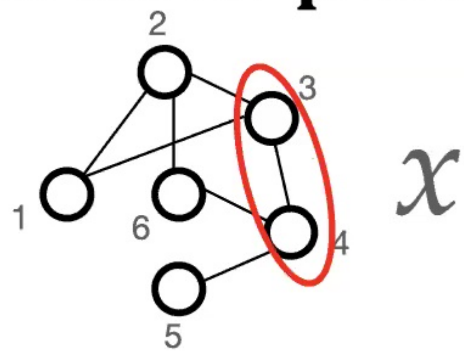


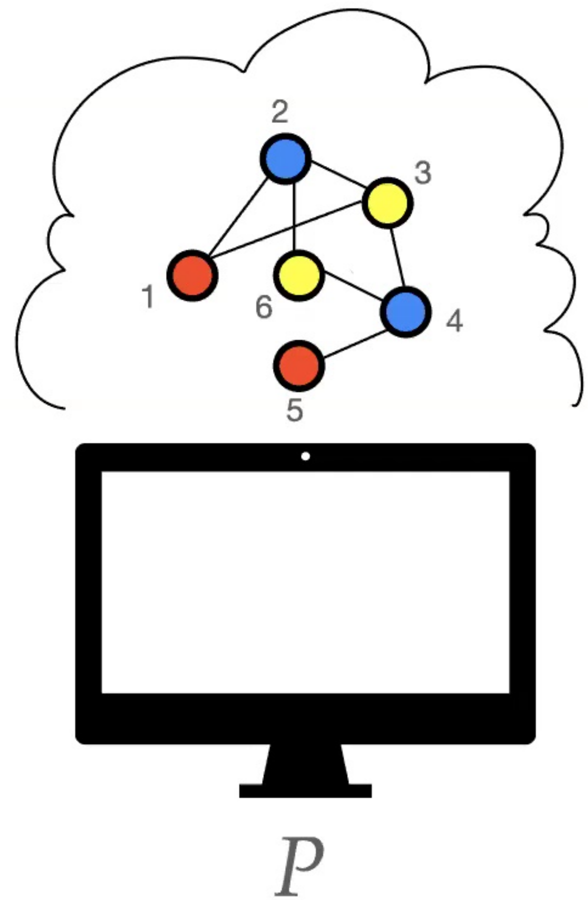


Zero-knowledge

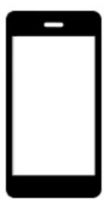


Proof-system for an NP problem



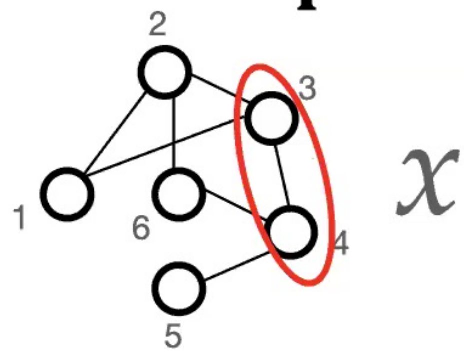


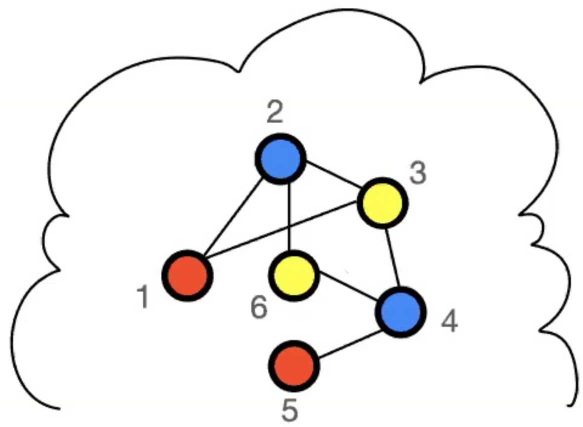
Zero-knowledge



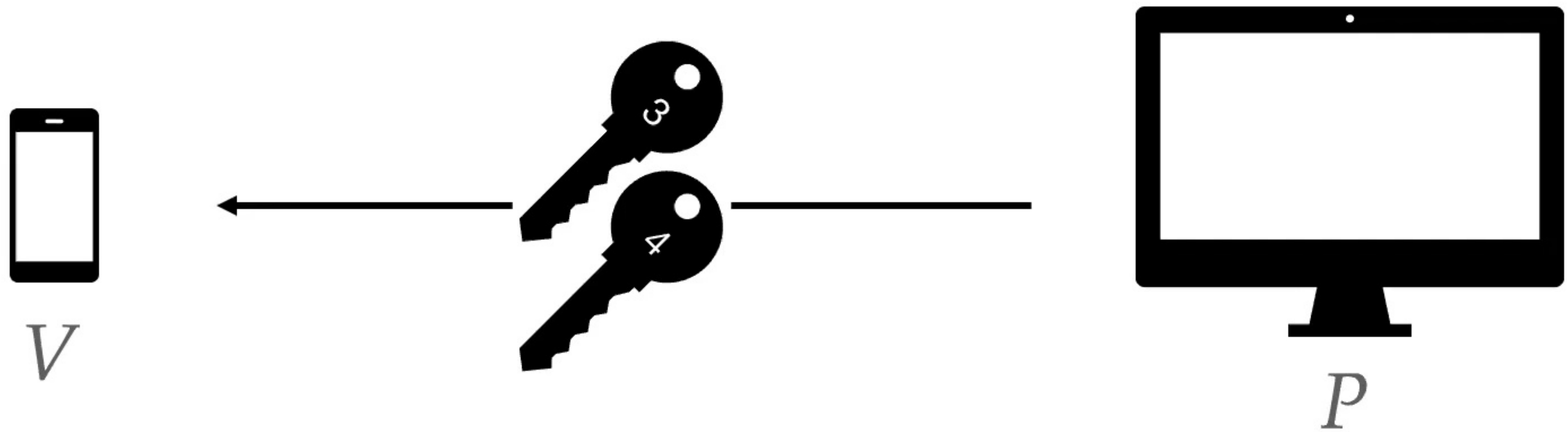
V

Proof-system for an NP problem

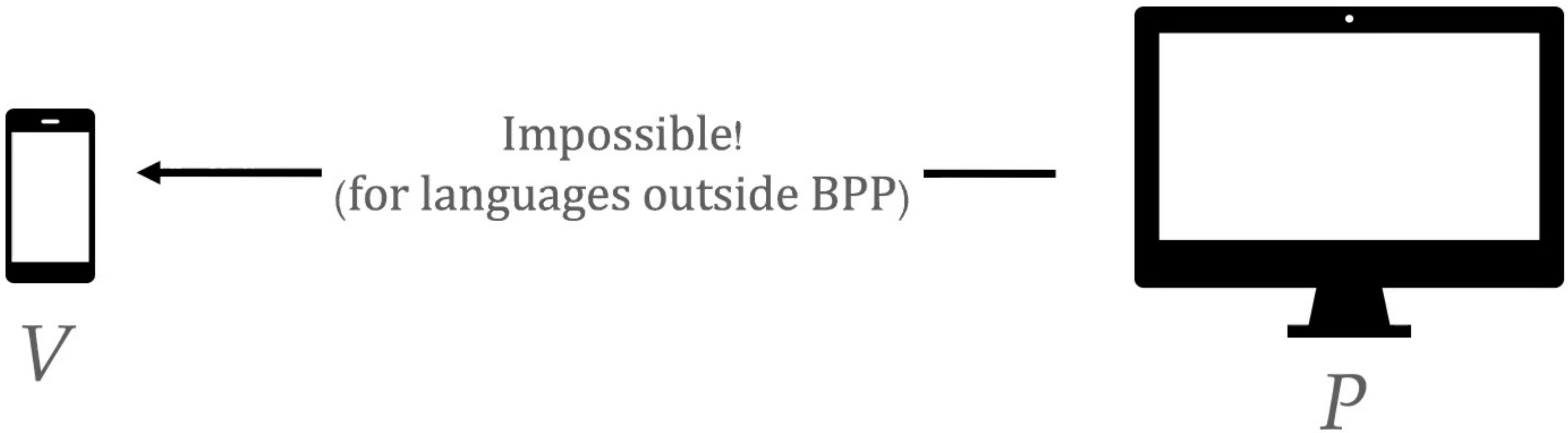




Zero-knowledge



Non–interactive zero–knowledge proof–systems

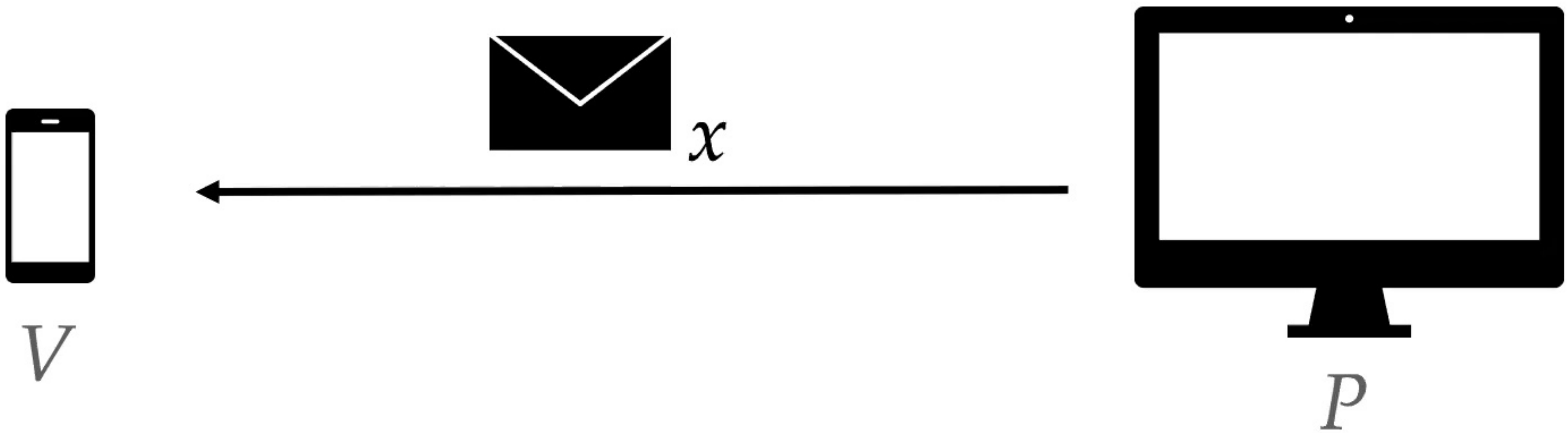


Non–interactive zero–knowledge proof–systems

Extended models:

CRS

01110010...

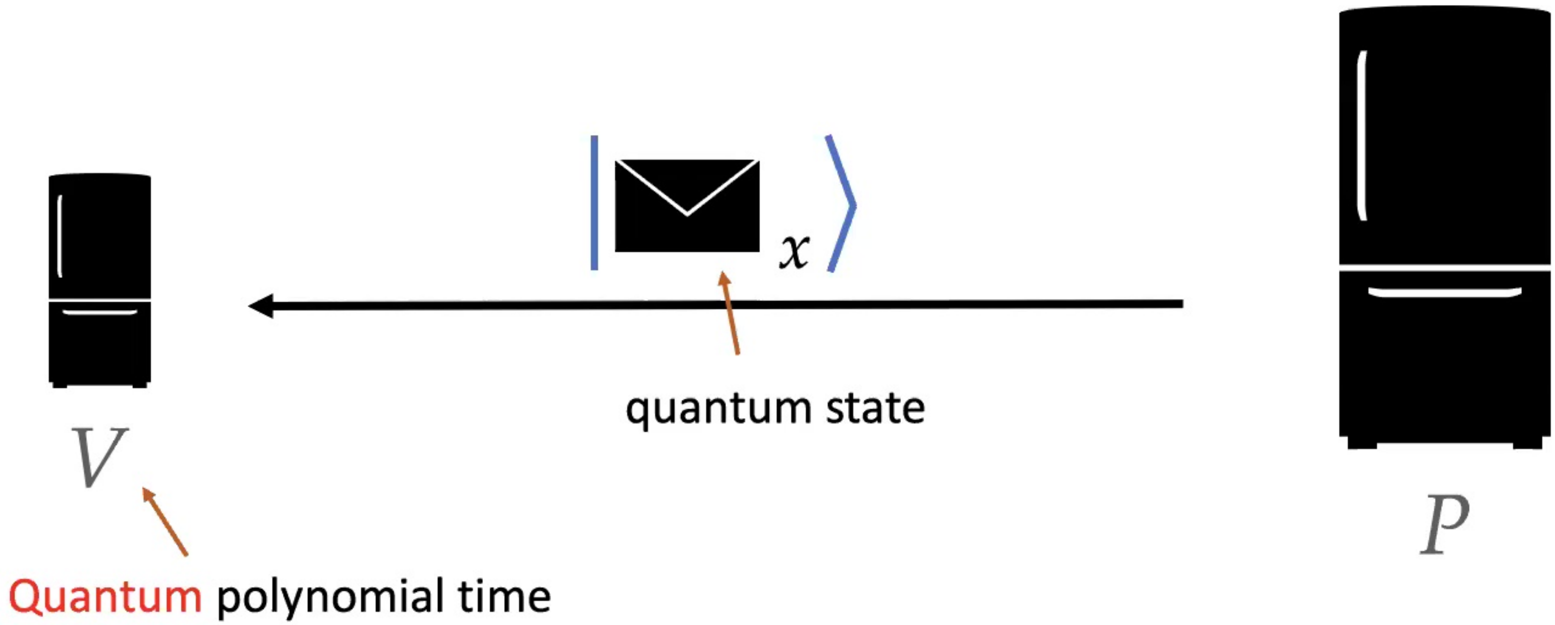


Beyond NP: ZK for QMA?

Local Hamiltonian Problem

Input: $x = H = \sum_r C_r$ (on n qubits)

Problem: Is lowest energy $< \alpha$ or $> \beta$?



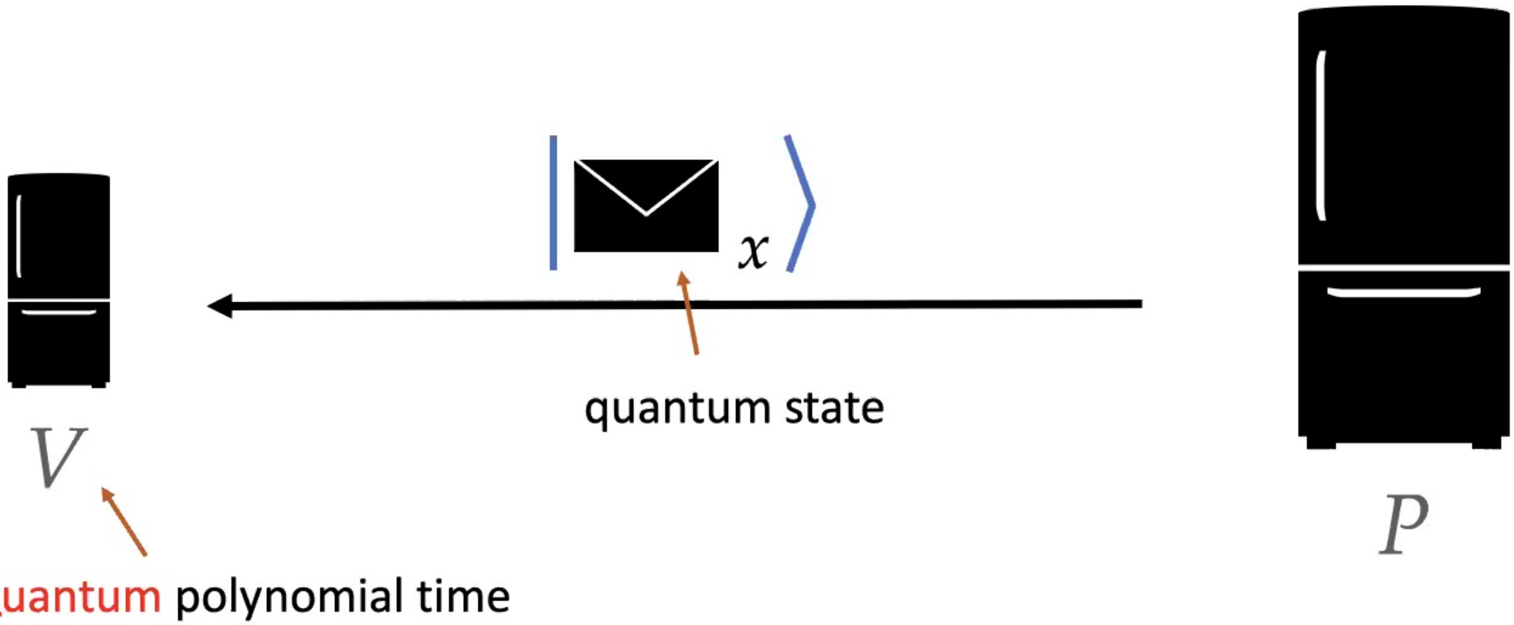
Beyond NP: ZK for QMA?

Input: $x = H = \sum_r C_r$ (on n qubits)

Problem: Is lowest energy $< \alpha$ or $> \beta$?

Local Hamiltonian Problem

Each C_r only acts on a constant number of qubits.



Beyond NP: ZK for QMA?

Local Hamiltonian Problem

Input: $x = H = \sum_r C_r$ (on n qubits)

Problem: Is lowest energy $< \alpha$ or $> \beta$?

Each C_r only acts on a constant number of qubits.

(Take $\alpha \approx 2^{-n}$ and $\beta \approx \frac{1}{poly(n)}$)

ground state

$|w\rangle$

V

P

V samples $r \leftarrow [m]$. Measures energy of $|w\rangle$ with respect to C_r and accepts if the energy is low.

Beyond NP: ZK for QMA?

Local Hamiltonian Problem

Input: $x = H = \sum_r C_r$ (on n qubits)

Problem: Is lowest energy $< \alpha$ or $> \beta$?

Each C_r only acts on a constant number of qubits.

(Take $\alpha \approx 2^{-n}$ and $\beta \approx \frac{1}{poly(n)}$)

ground state

$|w\rangle$

V

P

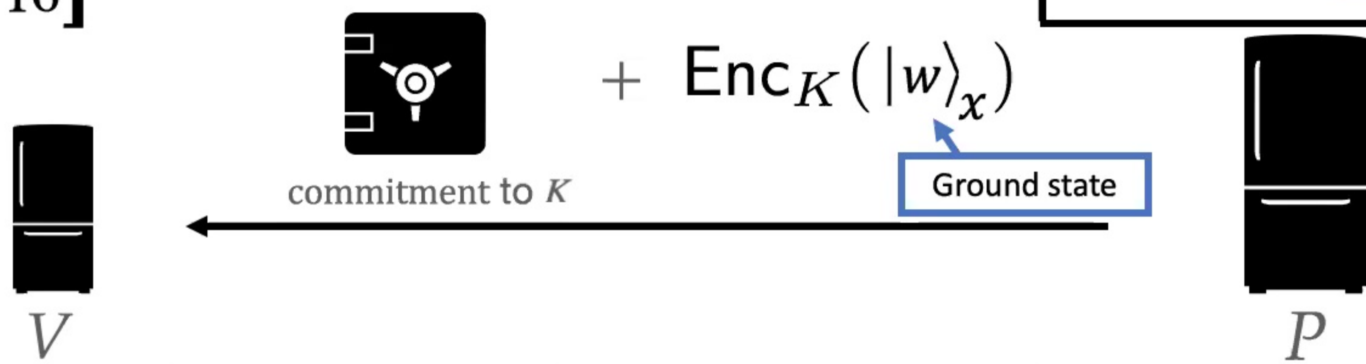
V samples $r \leftarrow [m]$. Measures energy of $|w\rangle$ with respect to C_r, i. e. makes the measurement $\{C_r, \mathrm{Id} - C_r\}$: accepts if outcome is latter.

Interactive ZK protocol for QMA [BJSW '16]

$x = H = \Sigma_r C_r$

$|w\rangle_x$ ← Ground state

Step 1:



Step 2:

V samples $r \leftarrow [m]$. Measures energy w. r. t C_r "homomorphically". Returns encoded outcome to P.

$r, \tilde{z}$

Step 3:

P checks validity of $\tilde{z}$. Proves that $\tilde{z}$ decodes to low energy under key K, using a ZK proof for NP.

⋮

$x = H = \Sigma_r\, C_r$

$|w\rangle_x$ ← Ground state

Interactive ZK protocol for QMA [BJSW '16]

commitment to K + $\mathrm{Enc}_K(|w\rangle_x)$ ← Ground state

Step 1:

V

P

Step 2: V samples $r \leftarrow [m]$. Measures energy w. r. t C_r "homomorphically" . Returns encoded outcome to P.

$r, \tilde{z}$ →

CRS

Step 3: P checks validity of $\tilde{z}$. Proves that $\tilde{z}$ decodes to low energy under key K, using a NIZK proof for NP.

←

How to make it non–interactive?

Main principle: quantum teleportation!

V measures encoded state before she receives it. . .

(Need EPR pairs + homomorphic encryption)

A closer look:

- Local Clifford Hamiltonian.
- The encoding Enc.
- Quantum teleportation.

Local Clifford Hamiltonian

Local Clifford Hamiltonian Problem

Input: $x = H = \sum_r C_r |0^k\rangle \langle 0^k| C_r^*$

Problem: Is lowest energy $< \alpha$ or $> \beta$?

The C_r's are k–qubit Clifford operators.

(Take $\alpha \approx 2^{-n}$ and $\beta \approx \frac{1}{poly(n)}$)

C is an n–qubit Clifford if for any $a, b \in \{0,1\}^n$, there are $a', b' \in \{0,1\}^n$ such that:

$$C\, X^a Z^b = X^{a'} Z^{b'}\, C$$

Local Clifford Hamiltonian

Local Clifford Hamiltonian Problem

Input: $x = H = \sum_r C_r |0^k\rangle\langle 0^k| C_r^*$

Problem: Is lowest energy $< \alpha$ or $> \beta$?

The C_r's are k–qubit Clifford operators.

(Take $\alpha \approx 2^{-n}$ and $\beta \approx \frac{1}{poly(n)}$)

ground state

$|w\rangle$

V samples $r \leftarrow [m]$. Applies C_r^* and measures.
Accepts if outcome is $\neq 0^k$.

P

$x = \sum_r C_r |0^k\rangle\langle 0^k| C_r^*$

$|w\rangle_x$ ← Ground state

Interactive ZK protocol for QMA [BJSW '16]

+ $\text{Enc}_K(|w\rangle_x)$

commitment to K

Ground state

Step 1:

V P

Step 2:

V samples $r \leftarrow [m]$. Applies C_r^* "homomorphically" and measures. Returns encoded outcome to P.

$r, \tilde{z}$

CRS

Step 3:

P checks validity of $\tilde{z}$. Proves that $\tilde{z}$ decodes to $\neq 0^k$ under key K, using a NIZK proof for NP.

The encoding Enc

Enc_K : 1 qubit $\rightarrow$ L qubits

(i) Measuring in standard basis reveals if state is a valid encoding under K.

(ii) **Homomorphic property**: Let C be a single–qubit Clifford, and $|\psi\rangle$ a single–qubit state. Then,

$$C^{\otimes L}\, \mathsf{Enc}_K(|\psi\rangle) = \mathsf{Enc}_{K'}(C|\psi\rangle)$$

where K' is efficiently computable given K and C.

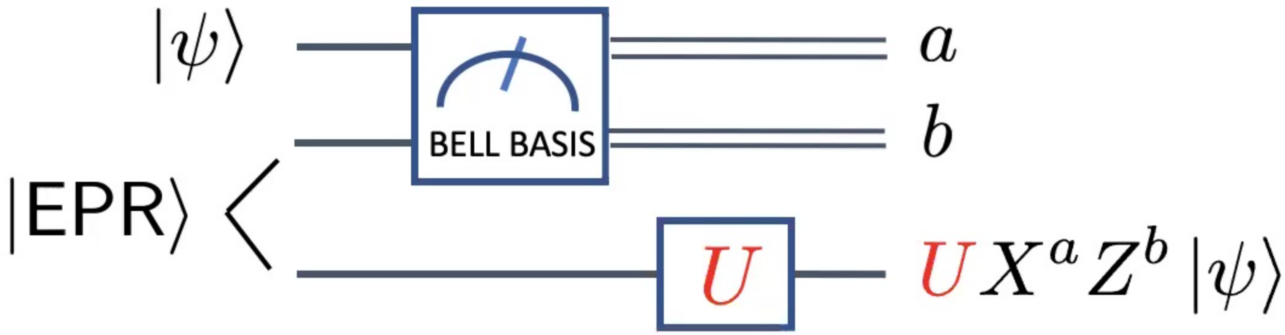
(iii) **Authentication property**: Let $K' \equiv K'(K, C)$.

$$\mathsf{Enc}_K(|\psi\rangle) \longrightarrow \mathsf{Enc}_{K'}(C'|\psi\rangle)$$

Hard for bounded adversaries

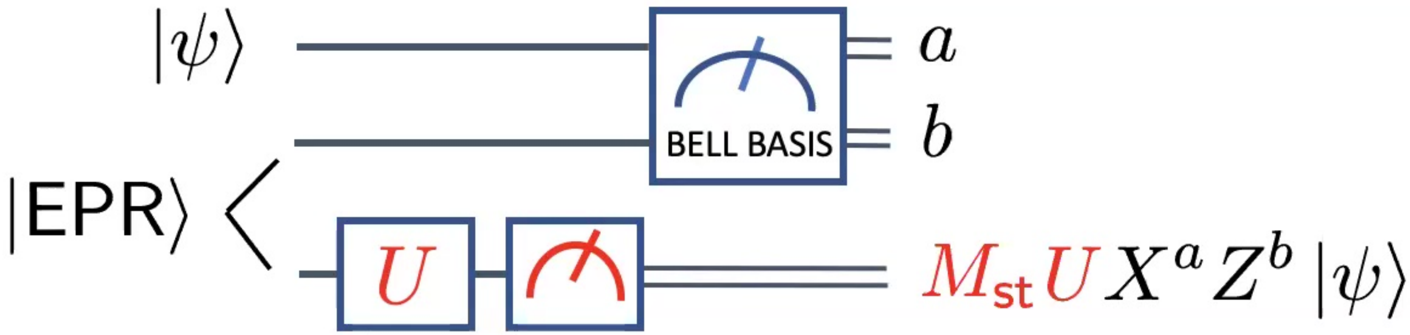
$$C' \neq C$$

Quantum teleportation



The Bell basis measurement and the application of U commute.

Quantum teleportation



$x = \sum_r C_r |0^k\rangle \langle 0^k| C_r^*$

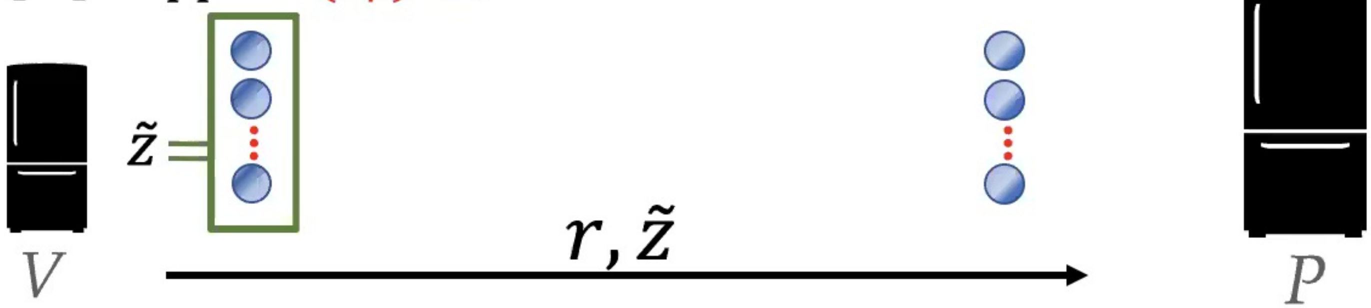
$|w\rangle_x$ ← Ground state

2-message protocol for QMA

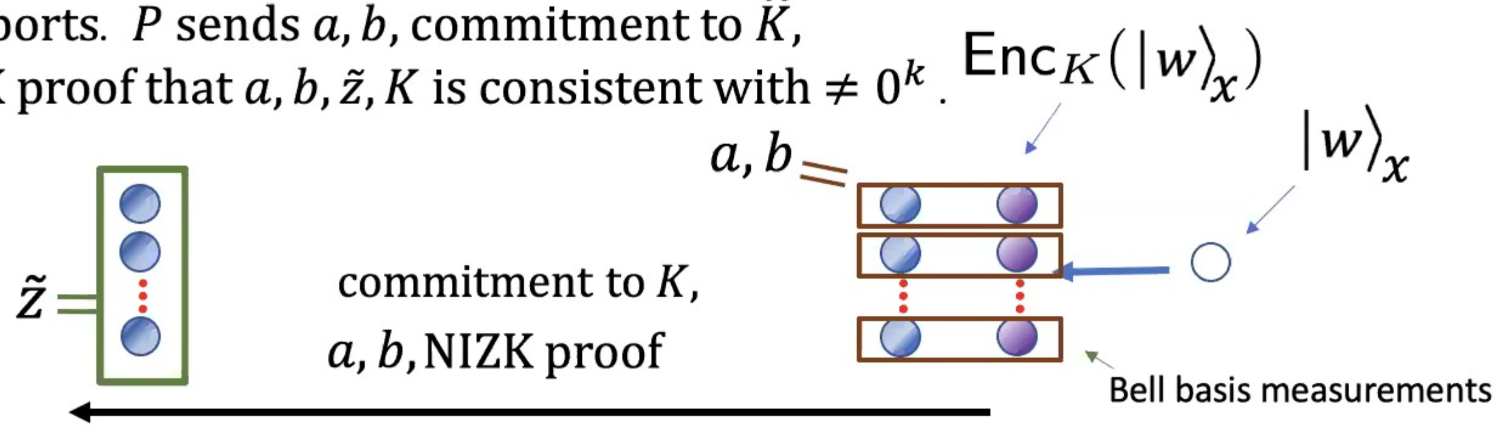
V creates EPR pairs. Sends second halves to P.

Samples $r \leftarrow [m]$. Applies $(C_r^*)^{\otimes L}$, then measures.

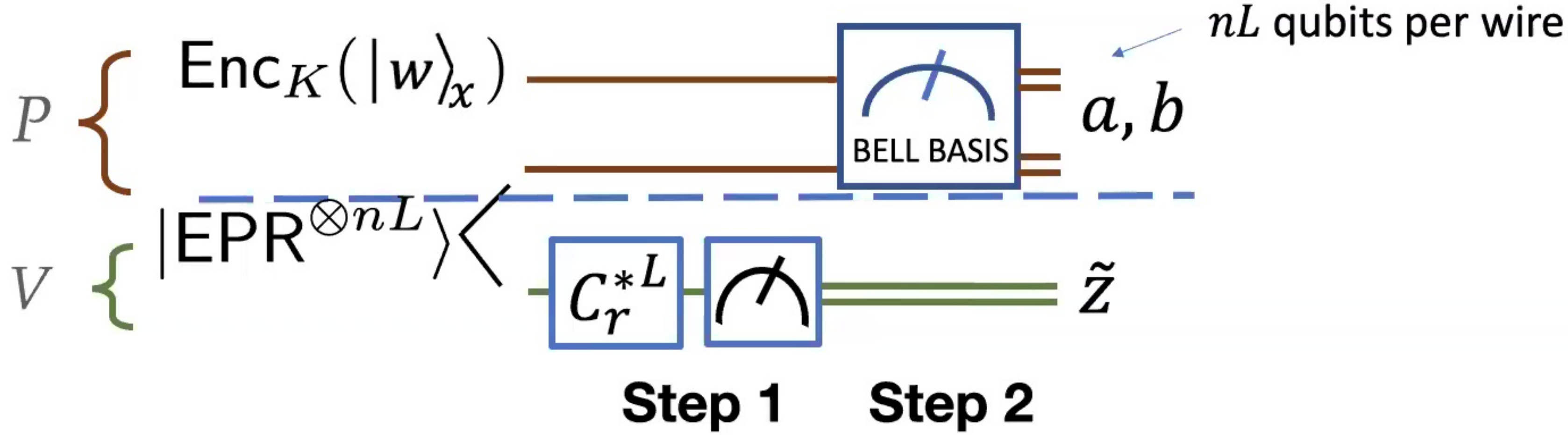
Step 1:



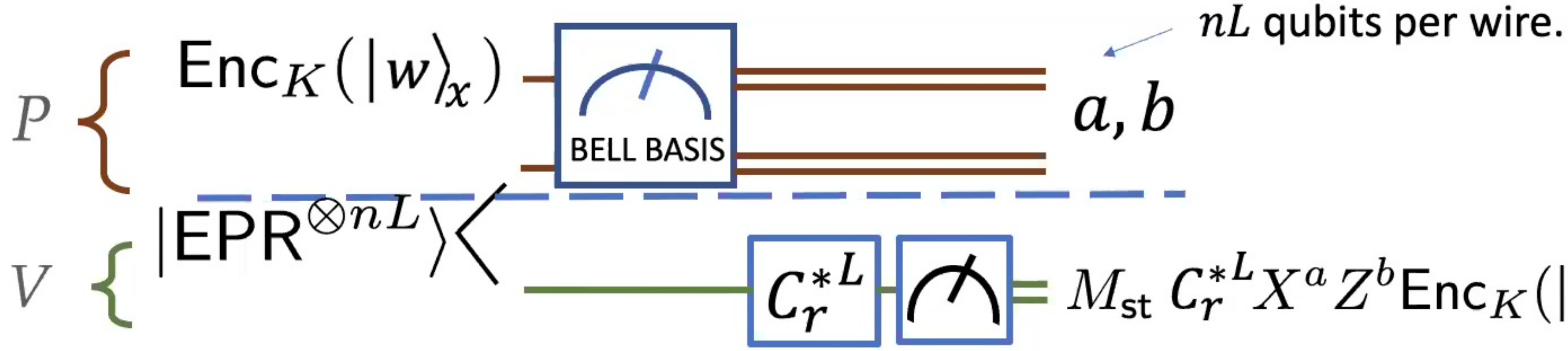
Step 2: P samples key K. Computes $\mathsf{Enc}_K(|w\rangle_x)$.
Teleports. P sends a, b, commitment to K,
NIZK proof that $a, b, \tilde{z}, K$ is consistent with $\neq 0^k$.



The protocol through the lens of teleportation



The protocol through the lens of teleportation

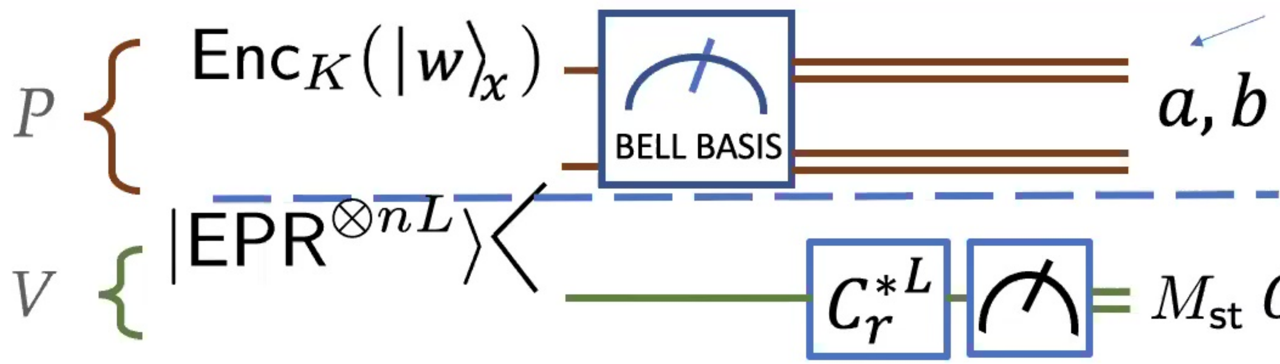


$$M_{\text{st}}\, C_r^{*L} X^a Z^b \text{Enc}_K(|w\rangle_x)$$

By definition of Clifford → $= M_{\text{st}} X^{a'} Z^{b'} \underbrace{C_r^{*L}\, \text{Enc}_K(|w\rangle_x)}$

By homomorphic property of Enc → $= M_{\text{st}} X^{a'} Z^{b'} \underbrace{\text{Enc}_{K'}(C_r^{*} |w\rangle_x)}$

The protocol through the lens of teleportation



$$M_{\mathrm{st}}\, C_r^{*L} X^a Z^b \mathrm{Enc}_K(|w\rangle_x)$$

By definition of Clifford → $= M_{\mathrm{st}} X^{a'} Z^{b'} C_r^{*L}\, \mathrm{Enc}_K(|w\rangle_x)$

By homomorphic property of Enc → $= M_{\mathrm{st}} X^{a'} Z^{b'} \mathrm{Enc}_{K'}(C_r^{*}|w\rangle_x)$

$$= a' \oplus M_{\mathrm{st}} \mathrm{Enc}_{K'}(C_r^{*}|w\rangle_x)$$

$x = \sum_r C_r |0^k\rangle\langle 0^k| C_r^*$

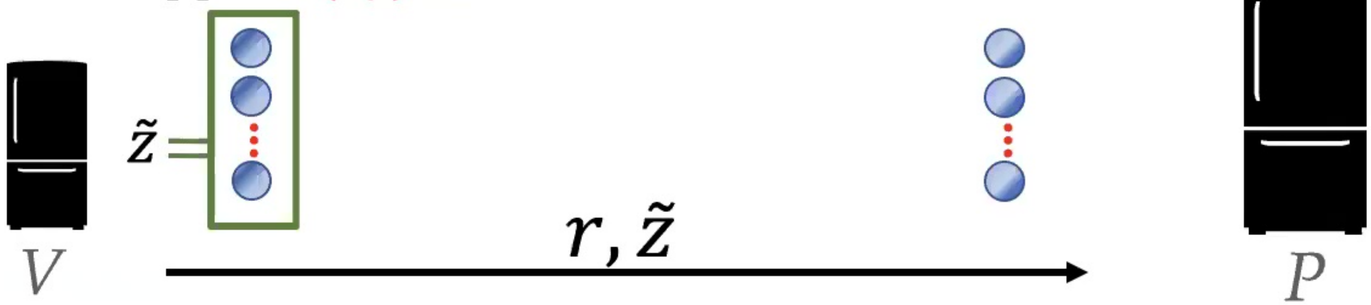
$|w\rangle_x$ ← Ground state

2-message protocol for QMA, with preprocessing

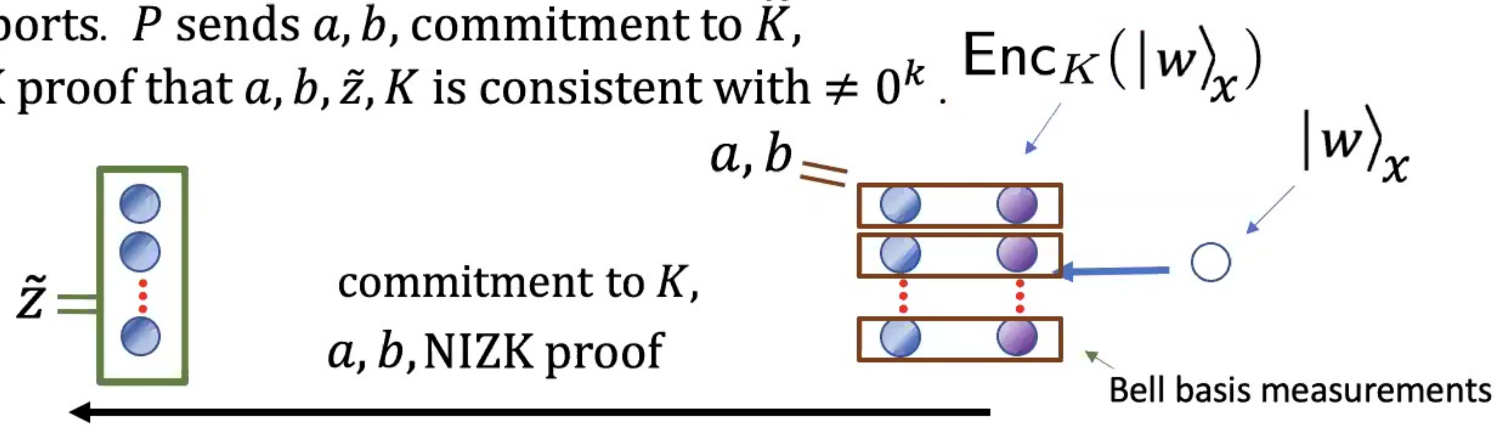
V creates EPR pairs. Sends second halves to P.

Samples $r \leftarrow [m]$. Applies $(C_r^*)^{\otimes L}$, then measures.

Step 1:



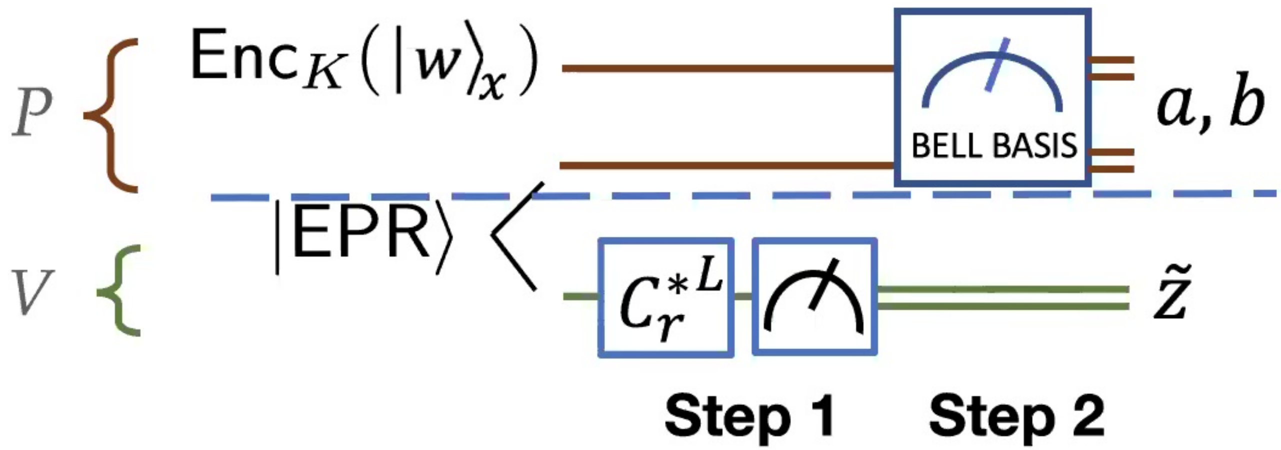
Step 2: P samples key K. Computes $\mathsf{Enc}_K(|w\rangle_x)$.
Teleports. P sends a, b, commitment to K,
NIZK proof that $a, b, \tilde{z}, K$ is consistent with $\neq 0^k$.



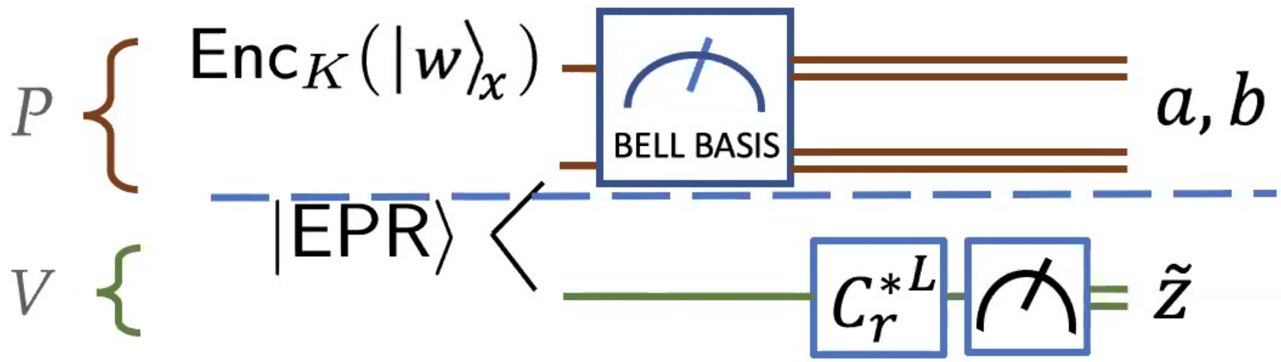
There is an issue (with soundness). .

r cannot be sent by V in the clear.

There is another issue (with soundness). .



There is another issue (with soundness). .



The two steps commute only if P’s action does not depend on $\tilde{z}$!

A fix for the issue

V does not send r and $\tilde{z}$ in the clear.

Instead, V sends a homomorphic encryption of r and $\tilde{z}$.

P “knows” everything under the hood of the encryption. So,
P **can compute the NIZK proof homomorphically**.

A fix for the issue

V does not send r and $\tilde{z}$ in the clear.

Instead, V sends a homomorphic encryption of r and $\tilde{z}$.

P "knows" everything under the hood of the encryption. So,
***P* can compute the NIZK proof homomorphically**.

Proof for QMA → argument for QMA

$x = \sum_r C_r |0^k\rangle \langle 0^k| C_r^*$

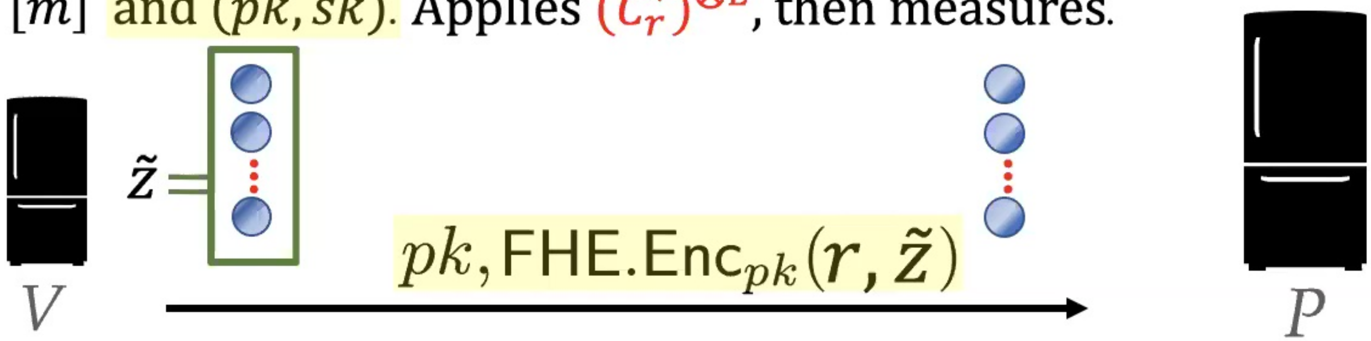
$|w\rangle_x$ ← Ground state

2–message protocol for QMA, with preprocessing

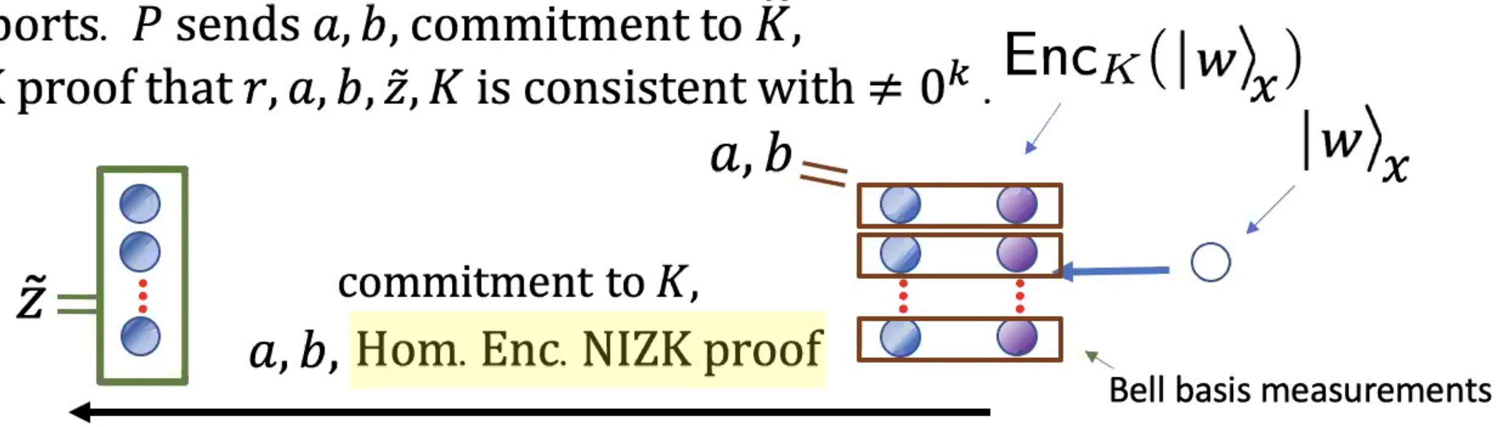
V creates EPR pairs. Sends second halves to P.

Samples $r \leftarrow [m]$ and (pk, sk). Applies $(C_r^*)^{\otimes L}$, then measures.

Step 1:



Step 2: P samples key K. Computes $\mathsf{Enc}_K(|w\rangle_x)$.
Teleports. P sends a, b, commitment to K,
Hom. Enc. of NIZK proof that $r, a, b, \tilde{z}, K$ is consistent with $\neq 0^k$.



Reductions to Hamiltonians

Current approach:

Instance x of a QMA problem
with verifying circuit Q

↓

Verifying circuit Q_x

↓

Local Clifford Hamiltonian $H(Q_x) = \sum_r C_r$

↓

Check that witness received from P has
low-energy with respect to $H(Q_x)$

Instance–independent approach:

QMA problem with verifying circuit Q

↓

Local Clifford Hamiltonian $H(Q) = \sum_r C_r$

Recap

Assuming LWE, we get a 2-message argument for QMA, in which the first message from V to P is *instance-independent*.

Related results: [Broabent & Grilo '19, Alagic et al '20]

Open question:

Can we have a truly non-interactive protocol for QMA in the CRS model (or in a model with shared EPR pairs?)

Thank you!