CLASSICAL VERIFICAITON OF QUANTUM COMPUTATIONS

→ $QPIP_k$ definition :
- Prover $\mathbb{P}$ capable of BQP computations.
- Verifier $\mathbb{V}$ capable of BPP computations + Quantum operations on "k" qubits

Unitary transformation, Measurements

- $\mathbb{P}, \mathbb{V}$ exchange poly($|x|$) classical messages, "k" qubits of quantum messages.

→ Result I : $QPIP_1 = BQP$

Two parts
(i) $QPIP_1 \subseteq BQP$ → Trivial proof.
(ii) $BQP \subseteq QPIP_1$ → [Morimae '15, '16]

- The proof uses [Kitaev '03] [Biamonte '08]'s results on QMA-completeness of the 5-LOCAL HAMILTONIAN and the 2-LOCAL HAMILTONIAN problems respectively.

- The idea is to convert an instance $x \in L$ of BQP to hamiltonian H_x (that is 2-local).
$\mathbb{P}$ determines the ground state of H_x and sends to $\mathbb{V}$ just the qubit that is to be measured. (only 2 times)
$\mathbb{V}$ accordingly determines the ground energy of this hamiltonian.

→ Result II : $QPIP_0 = BQP$ (true under certain LWE assumption)

Two parts
(i) $QPIP_0 \subseteq BQP$ → Trivial proof
(ii) $BQP \subseteq QPIP_0$ → [Mahadev '18] builds upon the proof of Result I.

- The reduction in previous proof involves a single measurement by $\mathbb{V}$ which is now outsourced to the $QPIP_0$ framework.

RESULT I : [Morimae '15 '16]

(proof of $BQP \subseteq QPIP_1$)

→ We make use of previous results
[Kitaev '03] QMA-completeness of 5-LOCAL HAMILTONIAN
[Kempe '05] QMA-completeness of 2-LOCAL HAMILTONIAN
[Biamonte '08] QMA-completeness of 2-LOCAL ZX HAMILTONIAN

→ - Take any $L \in BQP$.
- For an i/p instance $x \in L$?
- $L \in BQP \subseteq QMA \Rightarrow \neg L \in BQP \subseteq QMA$.
- Let V_x, $\overline{V_x}$ be the verification circuits of $L, \neg L$ resp.
- Since $L, \neg L \in BQP$, the verification certificate state for both of $V_x, \overline{V_x}$ will be an all $|0\rangle$ trivial state.

→ Reduce the instances $V_x, \overline{V_x}$ using reduction R
2-LOCAL ZX HAMILTONIAN instance H_x, $\overline{H_x}$ respectively

→ - Both $\mathbb{V}$ and $\mathbb{P}$ know $H_x, \overline{H_x}$
- $\mathbb{P}$ can construct the eigen state $|\eta\rangle$ (or $|\overline{\eta}\rangle$) of H_x (or $\overline{H_x}$) from the trivial certificate $|\xi\rangle = |0\rangle^{\otimes e}$.
(using reduction R)

→ - $\mathbb{P}$ uses $V_x, \overline{V_x}$ to find out if $x \in L$ or $x \in \neg L$.
- $\mathbb{P}$ conveys the information to $\mathbb{V}$ and will subsequently to try to prove his claim.
- If $x \in L$, they use V_x, H_x, $|\eta\rangle$
and if $x \in \neg L$, they use $\overline{V_x}$, $\overline{H_x}$, $|\overline{\eta}\rangle$.

→ - Using 2-LOCAL hamiltonian H_x (or $\overline{H_x}$) $\mathbb{V}$ decides which locations and bases to measure $|\eta\rangle$ (or $|\overline{\eta}\rangle$)
- $\mathbb{P}$ sends all the qubits of $|\eta\rangle$ (or $|\overline{\eta}\rangle$) to $\mathbb{V}$ one by one
- $\mathbb{V}$ performs the some measurements to decide.

In more detail.

2-LOCAL ZX HAMILTONIAN PROBLEM (Language L_{2H})

$$H_{ZX} = \sum_i h_i Z_i + \sum_i \Delta_i X_i + \sum_{i<j} J_{ij} Z_i X_j + \sum_{i<j} K_{ij} X_i Z_j$$

with $h_i, \Delta_i, J_{ij}, K_{ij} \in \mathbb{R}$

$x \in L_{2H} \Rightarrow \exists |\eta\rangle$ $\langle \eta | H_{ZX} | \eta \rangle \leq a$

$x \notin L_{2H} \Rightarrow \forall |\eta\rangle$ $\langle \eta | H_{ZX} | \eta \rangle \geq b$

$b - a \geq \frac{1}{\text{poly}|x|}$

→ Take $L \in BQP$, $(\neg L \in BQP)$
we want to show $L \in QPIP_1$ $(\because BQP \subseteq QPIP_1)$

For any instance $x \in L$? or $x \in \neg L$?
$\exists$ verification ckts V_x, $\bar{V}_x$ respectively:
with trivial verification certificates $|0\rangle^{\otimes w}$ $(\because L, \neg L \in BQP)$

→ Take a reduction $\mathcal{R}$: QMA $\longrightarrow$ 2-LOCAL HAMILTONIAN

$\mathcal{R} : V_x \longmapsto H_x$

$(|0\rangle^{\otimes w} \longrightarrow |\eta_0\rangle)$

→ $\mathbb{P}, \mathbb{V}$ know H_x
Only $\mathbb{P}$ knows $|\eta_0\rangle = R(|0\rangle^{\otimes w})$ because $\mathbb{V}$ has only one qubit.

→ $H_x = \sum_i h_i Z_i + \sum_i \Delta_i X_i + \sum_{i<j} J_{ij} Z_i X_j + \sum_{i<j} K_{ij} X_i Z_j$

(from defn of 2-LOCAL ZX hamiltonian)

$\Rightarrow H_x = \sum_S d_S S$ (where S is $Z_i, X_i, Z_i X_j$ or $X_i Z_j$ $_{i<j}$)

$\hookrightarrow$ is real

$$H_x' := H_x + \sum_s |d_s| I$$
$$= \sum_s |d_s| (I + \mathrm{sign}(d_s) S)$$
$$= \sum_s 2 |d_s| P_s \qquad \left[P_s = \frac{I + \mathrm{sign}(d_s) S}{2} \right]$$

$$H_x := \frac{1}{2 \sum_s |d_s|} H_x' = \sum_s \pi_s P_s$$

$\pi_s \to$ probability $= \dfrac{|d_s|}{\sum_s |d_s|}$

P_s is a projection operator on one or two qubits

It involves projection in $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}_{1,2}$ or $\{|+\rangle\langle +|$ or $|-\rangle\langle -|\}$ on exactly two qubits.

V measures in one of those projector for the required qubits. (one or two)
If the product of measurement equals $-\mathrm{sign}(d_s)$,

$$\langle \eta | \pi_s P_s | \eta \rangle = 0. \qquad (\text{or } \langle \bar{\eta} | \bar{\pi}_s \bar{P}_s | \bar{\eta} \rangle)$$

V returns "✓" else "X"

This procedure is repeated k times, $k = \mathrm{poly}(|x|)$.

If more than half of them result in "✓", V accepts $x \in L$
(or equivalently $x \notin L$)

Can we outsource this measurement step to the Prover? [Mahadev '18]

RESULT II : [Mahadev '18]

$BQP \subseteq QPIP_0$ (under certain assumptions)

→ KEY IDEA:

Develop a framework where $\mathbb{P}$ has a quantum state ρ, and $\mathbb{V}$ is able to measure ρ over a 2-local projection operator in Z, X bases. (denoted by h)

Importantly, the statistics of the measurement outcomes for this prover $\mathbb{P}$, $D_{\mathbb{P},h}$ should be close to the statistics of an actual measurement OF SOME STATE ρ' in the bases 'h' $D_{\rho',h}$ ($\rho = \rho'$ for honest provers)

$$D_{\mathbb{P},h} \sim D_{\rho',h}$$

→ For this purpose, we employ a MEASUREMENT PROTOCOL.

ROUGH IDEA:

- $\mathbb{V}$ prepares a basis of measurement 'h' according to the Pauli operator S,
  This basis is only for two qubits. $h_i = \begin{cases} 1 & X \text{ basis} \\ 0 & Z \text{ basis} \end{cases}$
  ($h_i = 0$ for other qubits)

- For ($i = 1$ to n):

  — <series of steps> —

  $\mathbb{V}$ decides to perform MEASUREMENT ROUND or TEST ROUND

  MEASUREMENT
  - steps for $\mathbb{V}$ to get measurement result.

  TEST
  - a check on malicious behaviour of $\mathbb{P}$.

SOME PREREQUISITES

TRAPDOOR CLAW-FREE FAMILIES: $\mathcal{F} = \{f_{k,b} : \mathcal{X} \to \mathcal{Y}\}_{b \in \{0,1\}}$

① $f_{k,0}, f_{k,1}$ are INJECTIVE and have the SAME RANGE
② INVERTIBLE using trapdoor t_k for BPP machine [For $y = f_{k,b}(x)$, $INV_{\mathcal{F}}(t_k, b, y) = x$]

(x_0, x_1) is a claw when $f_{k0}(x_0) = f_{k1}(x_1)$

③ CLAW-FREE: Hard for BQP to find $x_0, x_1 \in \mathcal{X}$ s.t. (x_0, x_1) is a claw.

④ ADAPTIVE-HARDCORE-BIT PROPERTY: Hard for BQP machine to find $b, x_b \in \{0,1\} \times \mathcal{X}$ and $d \in \{0,1\}^w$ s.t. $d \cdot (x_0 + x_1) = 0$ with non-negligible advantage over $\frac{1}{2}$.
↳ (x_0, x_1) is a claw.

⑤ EFFICIENTLY GENERATED: Efficient (BPP) algorithm $GEN_{\mathcal{F}}$

$$(k, t_k) \longleftarrow GEN_{\mathcal{F}}(1^\lambda)$$

⑥ Efficient BQP procedure $SAMP_{\mathcal{F}}$ that for i/p x, k, b gives

$$|x\rangle|0\rangle \xrightarrow[SAMP_{\mathcal{F}}(k,b)]{} |x\rangle|f_{k,b}(x)\rangle$$

TRAPDOOR INJECTIVE FXN FAMILIES: $\mathcal{G} = \{g_{k,b} : \mathcal{X} \to \mathcal{Y}\}_{b \in \{0,1\}}$

① $g_{k,b}$ is INJECTIVE and has DISJOINT range with $g_{k,b\oplus 1}$
② INVERTIBLE using a trapdoor t_k [For $y = g_{k,b}(x)$, $INV_{\mathcal{G}}(t_k, b, y) = x$] for BPP machine.
③ EFFICIENTLY GENERATED: Efficient (BPP) algorithm $GEN_{\mathcal{G}}$

$$(k, t_k) \longleftarrow GEN_{\mathcal{G}}(1^\lambda)$$

④ Efficient BQP procedure $SAMP_{\mathcal{G}}$ that for i/p x, k, b gives

$$|x\rangle|0\rangle \xrightarrow[SAMP_{\mathcal{G}}(k,b)]{} |x\rangle|g_{k,b}(x)\rangle$$

→ INJECTIVE INVARIANCE:
Given fxn key k, it is computationally hard (for BQP) to determine whether it is from a CLAW-FREE FAMILY or INJECTIVE FXN FAMILY.

→ Unfortunately we do not know to construct a TRAPDOOR CLAW-FREE FXN FAMILY.
We'll address this later.

→ For now, ASSUME a TRAPDOOR CLAW FREE FAMILY $\mathcal{F}$ exists which statisfies.
(i) conditions 1, 2, 3, 4, 5, 6 in prev. page
(ii) is injective invariant with a TRAPDOOR INJECTIVE FXN FAMILY $\mathcal{G}$.

→ Design a MEASUREMENT PROTOCOL under this assumption.

MEASUREMENT PROTOCOL

INITIAL CONDITIONS:

→ $\mathbb{V}$ decides the basis for measurement $h \in \{0,1\}^n$
$h_i = 0 \rightarrow Z$ basis, $h_i = 1 \rightarrow X$ basis

→ $\mathbb{P}$ has a state ρ

PROTOCOL:

For $i=1$ to n
$\mathbb{V}$ has $h_i = 0$ or 1
$\mathbb{P}$ has $\rho_i = \sum_b \alpha_b |b\rangle$ (not necessarily pure. but for illustration purpose)

(1) $\mathbb{V}$ samples k_i, t_{k_i} from $\mathcal{G}$ if $h_i=0$, from $\mathcal{F}$ if $h_i=1$. for $i=1$ to n

(2) $\mathbb{V}$ sends k_i to $\mathbb{P}$ for $i=1$ to n

(3) $\mathbb{P}$ constructs the following state using ρ_i

$$\underbrace{}_{}\frac{1}{\sqrt{|\mathcal{X}|}} \sum_b \sum_{x \in \mathcal{X}} \alpha_b |b\rangle |x\rangle |g_{k_b}(x)\rangle \quad \text{if } h_i = 0$$

$$\frac{1}{\sqrt{|\mathcal{X}|}} \sum_b \sum_{x \in \mathcal{X}} \alpha_b \underbrace{|b\rangle}_{①} \underbrace{|x\rangle}_{②} \underbrace{|f_{k_b}(x)\rangle}_{③} \quad \text{if } h_i = 1$$

Registers ① ② ③

(4) $\mathbb{P}$ measures register ③ to get result "y_i" for $i=1$ to n

(5) $\mathbb{P}$ commits to "y_i" by sending it to $\mathbb{V}$ for $i=1$ to n
→ Commitment string

The state in ①,② is now
$|b\rangle|x_{by}\rangle$ if $h_i=0$ $\quad \sum_b \alpha_b |b\rangle|x_{by}\rangle$ if $h_i=1$

(6) $\mathbb{V}$ decides to perform either a MEASUREMENT ROUND or TEST ROUND

The yellow coloured states in this page are only for illustrative purposes. and are true only when the i^{th} qubit is a pure state.

MEASUREMENT ROUND

(M1) $\mathbb{P}$ measures registers ①, ② in X basis. to get results b_i', d_i' resp. for $i=1$ to n.

(M2) $\mathbb{P}$ sends b_i', d_i' to $\mathbb{V}$ for $i=1$ to n

(M3) If $(h_i=0)$ $\mathbb{V}$ ignores b_i', d_i'
$\mathbb{V}$ Computes $b_i, x_{b_i,y} = INV_G(y_i, t_{k_i})$
$\mathbb{V}$ stores $m_i = b_i$

If $(h_i=1)$ $\mathbb{V}$ computes $x_{0y}, x_{1y} = INV_F(y_i, t_{k_i})$

$\mathbb{V}$ stores $m_i = b_i' \oplus d_i' \cdot (x_{0y} \oplus x_{1y})$

→ m_i is the measurement result. for $i=1$ to n

TEST ROUND

(T1) $\mathbb{P}$ measures registers ①, ② in Z basis to get results b_i', x_i' resp.

(T2) $\mathbb{P}$ sends b_i', x_i' to $\mathbb{V}$

for $i=1$ to n

(T3) If $(h_i=0)$ $\mathbb{V}$ computes $b_i, x_{b_i y} = \text{invert}(y_i, t_{k_i})$
$\mathbb{V}$ tests if $b_i, x_{b_i y} == b_i', x_i'$?

If $(h_i=1)$ $\mathbb{V}$ computes $x_{0y}, x_{1y} = \text{invert}(y_i, t_{k_i})$
$\mathbb{V}$ tests if $(x_i' == x_{0y}$ AND $b_i' == 0)$
OR
$(x_i' == x_{1y}$ AND $b_i' == 1)$?

for $i=1$ to n

→ $\mathbb{V}$ aborts the protocol (or rejects the input string) if the test fails.

ILLUSTRATION OF MEASUREMENT PROTOCOL

→ For illustration purpose, we take an honest prover $\mathbb{P}_0$ and the state ρ_i in its pure form.

$$\rho_i = \sum_b \alpha_b |b\rangle$$

CASE I : $h_i = 0$

After step (3), $\mathbb{P}_0$ has state $\frac{1}{\sqrt{|\mathcal{X}|}} \sum_b \sum_x \alpha_b |b\rangle |x\rangle |g_{k_b}(x)\rangle$

After step (5), $\mathbb{P}_0$ has $|b\rangle |x_{by}\rangle$ for some b
w.p. $|\alpha_0|^2, |\alpha_1|^2$ resp.

In MEASUREMENT ROUND:

After step (M1), $\mathbb{P}_0$'s result (b_i', d_i) is irrelevant

After step (M3), $m_i = 0$ or 1 w.p. $|\alpha_0|^2$, $|\alpha_1|^2$ resp.

$$\therefore \; D_{\mathbb{P}_0, h_i = 0} = \{|\alpha_0|^2, |\alpha_1|^2\}$$

$$= D_{\rho, h_i = 0} \qquad \{ \rho_i = \sum_b \alpha_b |b\rangle \}$$

The measurement probabilities match.

In TEST round,

After step (T1), $\mathbb{P}_0$ gets $b_i', x_i' = b, x_{by}$.

(T3), The test passes

CASE II: $h_i = 1$

After step (3), P_0's state is $\frac{1}{\sqrt{|\mathcal{X}|}}\sum_b\sum_x \alpha_b|b\rangle|x\rangle|f_{k_b}(x)\rangle$

step (5), P_0's state is $\sum_b \alpha_b|b\rangle|x_{by}\rangle$

In MEASUREMENT ROUND.

After step (M1), measuring in X basis

$\Updownarrow$

measuring $\sum_b \alpha_b H|b\rangle\otimes H|x_{by}\rangle$ in Z basis.

$$\sum_b \alpha_b H|b\rangle \otimes H X^{x_{by}}|0\rangle$$

$$= \sum_b \alpha_b H|b\rangle\otimes Z^{x_{by}} H|0\rangle$$

$$= \sum_{d\in\mathcal{X}}\sum_b \alpha_b H|b\rangle\otimes Z^{x_{by}}\frac{|d\rangle}{\sqrt{|\mathcal{X}|}}$$

$$= \sum_{d\in\mathcal{X}}\frac{1}{\sqrt{|\mathcal{X}|}}\sum_b \alpha_b(-1)^{d\cdot x_{by}} H|b\rangle\otimes|d\rangle$$

$$= \sum_{d\in\mathcal{X}}(H\otimes I)\sum_b(-1)^{d\cdot x_{by}}\alpha_b|b\rangle\otimes\frac{|d\rangle}{\sqrt{|\mathcal{X}|}}$$

$$= \sum_{d\in\mathcal{X}}(H\otimes I)\,(-1)^{d\cdot x_{0y}}\sum_b Z^{d\cdot(x_{0y}+x_{1y})}\alpha_b|b\rangle\otimes\frac{|d\rangle}{\sqrt{|\mathcal{X}|}}$$

$$= \sum_{d\in\mathcal{X}} H Z^{d\cdot(x_{0y}+x_{1y})}\left[\sum_b\alpha_b|b\rangle\right]\otimes Z^{x_{0y}}\frac{|d\rangle}{\sqrt{|\mathcal{X}|}}$$

$$= \sum_{d\in\mathcal{X}} X^{d\cdot(x_{0y}+x_{1y})}\, H\, |\psi\rangle\otimes Z^{x_{0y}}\frac{|d\rangle}{\sqrt{|\mathcal{X}|}}$$

Results in final state

$$\sum_{d\in\mathcal{X}} \frac{1}{\sqrt{|\mathcal{X}|}} \; X^{d\cdot(x_{0y}+x_{1y})} \left[\sum_b \alpha_b' |b\rangle\right] \otimes Z^{x_{0y}} |d\rangle$$

$\left[\alpha_0' \triangleq \frac{\alpha_0+\alpha_1}{\sqrt{2}}, \; \alpha_1' \triangleq \frac{\alpha_0-\alpha_1}{\sqrt{2}}\right]$

$$= \sum_{d\in\mathcal{X}} \sum_b \frac{\alpha_b'}{\sqrt{|\mathcal{X}|}} \; |b \oplus d\cdot(x_{0y}+x_{1y})\rangle \otimes |d\rangle$$

Measuring registers ①, ② to be b_i', d_i

$$b_i' = \begin{cases} 0 + d\cdot(x_{0y}+x_{1y}) & \text{w.p. } |\alpha_0'|^2 = \left|\frac{\alpha_0+\alpha_1}{\sqrt{2}}\right|^2 \\ 1 + d\cdot(x_{0y}+x_{1y}) & \text{w.p. } |\alpha_1'|^2 = \left|\frac{\alpha_0-\alpha_1}{\sqrt{2}}\right|^2 \end{cases}$$

After step (M3),

$$m_i' = b_i' + d\cdot(x_{0y}+x_{1y}) = \begin{cases} 0 & \text{w.p. } |\alpha_0'|^2 = \left|\frac{\alpha_0+\alpha_1}{\sqrt{2}}\right|^2 \\ 1 & \text{w.p. } |\alpha_1'|^2 = \left|\frac{\alpha_0-\alpha_1}{\sqrt{2}}\right|^2 \end{cases}$$

$$\Rightarrow \mathcal{D}_{\mathbb{P}, h_i=1} = \left\{ \left|\frac{\alpha_0+\alpha_1}{\sqrt{2}}\right|^2, \left|\frac{\alpha_0-\alpha_1}{\sqrt{2}}\right|^2 \right\}$$

$$= \mathcal{D}_{\mathcal{S}, h_i=1} \left\{ \mathcal{S}_i = \sum_b \alpha_b |b\rangle \right\}$$

The measurement probabilities match

In TEST ROUND,

After step (T1), $\mathbb{P}_0$ gets b_i', $x_i' = x_{b_i' y}$

In step (T3), $\mathbb{V}$'s test passes

The test passes.

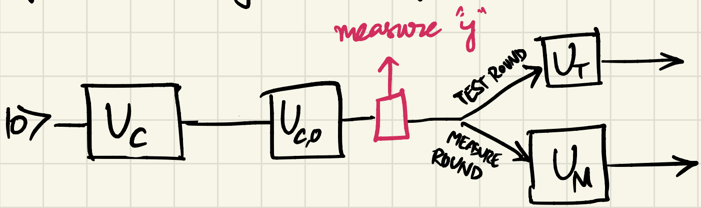
GENERAL PROVER BEHAVIOUR

FOR HONEST PROVER $\mathbb{P}_0$,

- Say performs U_{cp} unitary operation on an ancilliary state $|0\rangle$ to get state ξ, where he measures reg ③ in Z basis

FOR GENERAL PROVER $\mathbb{P}$,

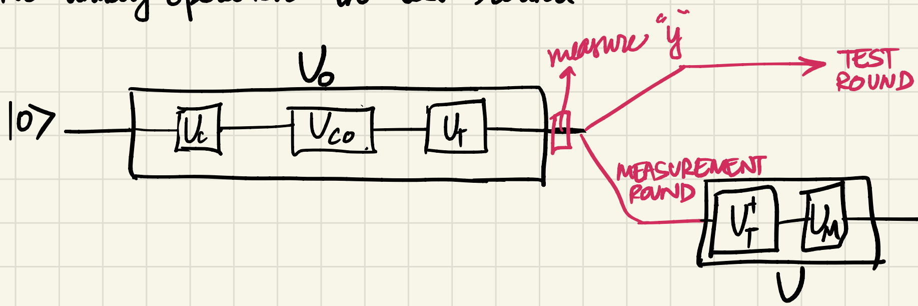
- Performs unitary U_c before U_{cp}
- Performs unitary U_T before test round (T1)
- Performs unitary U_M before measurement round (M1)



- U_T, U_M act only on regs ①,② So they commute with measuring "y" in reg③

EQUIVALENT BEHAVIOUR FOR GENERAL PROVER $\mathbb{P}$

- Performs $V_0 = U_T U_{co} U_c$ on initial state $|0\rangle$
- If it's a MEASUREMENT ROUND, $\mathbb{P}$ performs $U = U_M U_T^\dagger$ on his state at that time.
- No unitary operation in test round.



→ General prover P is characterised by (V_0, V)

$\Updownarrow$

$\mathbb{P}$ characterised by CPTP maps (S_0, S)

UNDERLYING QUANTUM STATES

How do the states evolve for general prover $\mathbb{P}$?

→ $\mathbb{P}$ begins with four registers.

Reg ① of length "n" of committed qubits $|b\rangle$
Reg ② of length "nw" of preimage registers $|x\rangle$
Reg ③ of length "nw" of commitment strings $|y\rangle$
Reg ④ all auxillary things.
fxn keys $|k\rangle$, ancillary bits, measurement results
$k^n = k_1 k_2 \dots k_n$

PROTOCOL Ⓐ

MEASUREMENT PROTOCOL Corresponding steps

(1) Initially $\mathbb{P}$ has an all zero state $|0\rangle^{\otimes e} \otimes |k\rangle$ (1),(2)

(2) $\mathbb{P}$ performs $V_0(|0\rangle^{\otimes e} \otimes |k\rangle) = V_{0k}(|0\rangle^{\otimes e}) \otimes |k\rangle$ (3)

$$\frac{1}{\sqrt{|\mathcal{X}|^n}} \sum_{b_1 b_2 \dots b_n} \sum_{x_1 x_2 \dots x_n} \alpha_{b_1 b_2 \dots b_n} |b_1 b_2 \dots b_n\rangle |x_1 x_2 \dots x_n\rangle \otimes$$

$$|g_{k_1 b_1}(x_1)\, f_{k_2 b_2}(x_2)\, f_{k_3 b_3}(x_3) \dots g_{k_n b_n}(x_n)\rangle |k\rangle |0\rangle^{\otimes e}$$

↳ $g_{k_i b_i}(x_i)$ or $f_{k_i b_i}(x_i)$ depending on $h_i = 0$ or 1

(3) $\mathbb{P}$ measures Reg ③ completely in Z basis to obtain (4)
$y^n = (y_1, y_2, \dots y_n) \in \mathcal{Y}^n$

(4) $\mathbb{P}$ sends y^n to $\mathbb{V}$ (5)

(5) TEST ROUND : $\mathbb{P}$ measures Reg ①,② and sends results to $\mathbb{V}$ one by one for $1 \le i \le n$ (T1), (T2)

MEASUREMENT ROUND:

(6) $\mathbb{P}$ applies unitary U to his state regs 1 & 2

(7) $\mathbb{P}$ measures regs 1 & 2 in X basis. (M1)
and sends the results b_i', d_i' to $\mathbb{V}$
one by one for $1 \leq i \leq n$.

→ $\mathbb{V}$ gets $m_i = b_i' \oplus d_i \cdot (x_{k_i 0} + x_{k_i 1})$ or b_i'
Return $(m_1 m_2 \ldots m_n)$ depending on $h_i = 0$ or 1

GOAL: To show that the measurement statistics obtained by $\mathbb{V}$ for prover $\mathbb{P}$ following PROTOCOL A $= D_{\mathbb{P},h}$

is equivalent to the measurement stats of measuring SOME quantum state ρ in basis h. : $D_{\rho,h}$

$D_{\mathbb{P}h} \sim D_{\rho h}$

Towards this goal we Prove

claim I
For $\mathbb{P}$ characterised by (U_0, U)

where U is trivial (U commutes with measurement of reg 1 in Z basis)

$\exists \rho$ s.t. $D_{\mathbb{P},h} \sim D_{\rho h}$

claim II
For all $\mathbb{P}'$ characterised by (U_0, U)

$\exists$ $\mathbb{P}$ characterised by $(\bar{U}_0, \bar{U})$ s.t. $\bar{U}$ is trivial.

and $D_{\mathbb{P}',h} \sim D_{\mathbb{P},h}$

PROOF OF CLAIM I

→ We construct a series of protocols which all return the same measurement statistics as ρ, Protocol Ⓐ

→ Protocol Ⓑ

1. For $1 \le i \le n$, sample $(k_i, t_{k_i}) \longleftarrow GEN_{\mathcal{F}}(1^\lambda)$
2. Designate reg①, reg②, reg③, reg④ like in protocol Ⓐ
3. Perform unitary U_0 on $|0\rangle^{\otimes e} \otimes |k\rangle$ to get

$$\frac{1}{\sqrt{|\mathcal{X}|^n}} \sum_{b_1 b_2 \cdots b_n} \sum_{x_1 x_2 \cdots x_n} \alpha_{b_1 b_2 \cdots b_n} |b_1 b_2 \cdots b_n\rangle |x_1 x_2 \cdots x_n\rangle \otimes |f_{k_1 b_1}(x_1) f_{k_2 b_2}(x_2) \cdots f_{k_n b_n}(x_n)\rangle$$

4. Measure reg③ completely to get y^n
5. Apply unitary U to regs ① & ②
6. Measure reg② in X basis to get $d_1 d_2 \cdots d_n \in \{0,1\}^w$
7. For $1 \le i \le n$, use t_{k_i} to get $x_{0 y_i}, x_{1 y_i}$
   Apply $Z^{d_i \cdot (x_{0y_i} + x_{1y_i})}$ to the i^{th} committed qubit in reg①

→ Define the resulting state as ρ.

→ Measure the resulting reg①, each qubit one by one to get m_i.
Return $(m_1, m_2, \cdots m_n)$

↳ with statistic $D_{\rho, h}$.

→ Observe that the state ρ prepared above is same irrespective of the bases states h.

→ Protocol C

1. For $1 \le i \le n$, sample $(k_i, t_{k_i}) \longleftarrow GEN_{\mathcal{F}}(1^{\lambda})$
2. If $h_i = 0$, forget t_{k_i}
3. Designate reg 1, reg 2, reg 3, reg 4 like in protocol A

4. Perform unitary U_0 on $|0\rangle^{\otimes e} \otimes |k\rangle$ to get

$$\frac{1}{\sqrt{|\mathcal{X}|^n}} \sum_{b_1 b_2 \cdots b_n} \sum_{x_1 x_2 \cdots x_n} \alpha_{b_1 b_2 \cdots b_n} |b_1 b_2 \cdots b_n\rangle |x_1 x_2 \cdots x_n\rangle \otimes |f_{k_1 b_1}(x_1) f_{k_2 b_2}(x_2) \cdots f_{k_n b_n}(x_n)\rangle$$

5 Measure reg 3 completely to get y^n
6 Apply unitary U to regs 1 & 2
7 Measure reg 2 in X basis to get $d_1 d_2 \cdots d_n \in \{0,1\}^w$
8 For $1 \le i \le n$,
→ If $(h_i = 1)$
use t_{k_i} to get $x_{0 y_i}, x_{1 y_i}$
Apply $Z^{d_i \cdot (x_{0y_i} + x_{1y_i})}$ to the i^{th} committed qubit in reg 1
→ If $(h_i = 0)$
Don't do anything.

→ Define the resulting state as $\rho_h^{(1)}$

→ Measure the resulting reg 1, each qubit one by one to get m_i.
Return $(m_1, m_2, \cdots m_n)$
↳ with statistic $D_{\rho_h^{(1)}, h}$

→ Unlike ρ of protocol B, $\rho_h^{(1)}$ here depends on the basis states.

→ Protocol B differs from Protocol C only at step 8 (of C), step 7 (of B) when $h_i = 0$.
where a Z operator is applied in protocol C.
But it doesn't make any difference in the measurement result, since we measure in Z basis itself.
⇒ $D_{\rho, h} = D_{\rho_h^{(1)}, h}$

→ Protocol (D)

1. For $1 \leq i \leq n$, $(k_i, t_{k_i}) \longleftarrow GEN_F(1^\lambda)$ if $h_i = 1$
$(k_i, t_{k_i}) \longleftarrow GEN_G(1^\lambda)$ if $h_i = 0$ and discard t_{k_i}
2. Designate reg(1), reg(2), reg(3), reg(4) like in protocol(A)
3. Perform unitary U_0 on $|0\rangle^{\otimes e} \otimes |k\rangle$ to get

$$\frac{1}{\sqrt{|\mathcal{X}|^n}} \sum_{b_1 b_2 \cdots b_n} \sum_{x_1 x_2 \cdots x_n} \alpha_{b_1 b_2 \cdots b_n} |b_1 b_2 \cdots b_n\rangle |x_1 x_2 \cdots x_n\rangle \otimes$$
$$|g_{k_1, b_1}(x_1) f_{k_2, b_2}(x_2) g(\cdot) \cdots f_{k_n, b_n}(x_n)\rangle$$

depends on h_i

4. Measure reg(3) completely to get y^n
5. Apply unitary U to regs (1) & (2)
6. Measure reg(2) in X basis to get $d_1 d_2 \cdots d_n \in \{0,1\}^w$
7. For $1 \leq i \leq n$,
→ If ($h_i = 1$)
use t_{k_i} to get $x_{0 y_i}$, $x_{1 y_i}$
Apply $Z^{d_i \cdot (x_{0 y_i} + x_{1 y_i})}$ to the i^{th} committed qubit in reg(1)
→ If ($h_i = 0$)
Don't do anything.

→ Define the resulting state as $\rho^{(2)}_{h}$

→ Measure the resulting reg(1), each qubit one by one to get m_i.
Return $(m_1, m_2, \cdots m_n)$
↳ with statistic $D_{\rho^{(2)}_h, h}$

→ $\rho^{(2)}_h$ also depends on the bases h.

→ Protocol (D) differs from Protocol (C) only at step 1, where the keys are sampled from F and G separately.
For $h_i = 0$, since t_{k_i} is unknown, from the computational indistinguishability of F, G, (INJECTIVE INVARIANCE property)

$$\left| D_{\rho^{(1)}_h, h} - D_{\rho^{(2)}_h, h} \right| \leq \lambda(n) \quad \Rightarrow \quad D_{\rho^{(1)}_h, h} \sim D_{\rho^{(2)}_h, h}$$

negligible fxn

→ So far, we have $D_{\rho,h} = D_{S_h^{(1)},h} \sim D_{S_h^{(2)},h} \overset{?}{=} D_{P,h}$

to prove

→ Compare Protocols Ⓓ and Protocol Ⓐ on a case by case basis.
The two differ in steps 6,7 (of Ⓓ) and step 7 (of Ⓐ)

Case I: $h_i = 0$.

Analysing Protocol Ⓐ, the result of step (7) and the measurement by V is

(if the state before step 5 is ρ') after measuring y_i

$m_i = b_i$ (which is obtained by $INV_G(t_{k_i}, y_i)$)

The state is $\sum_{b_i : k_i \in F} \alpha_{b_1 b_2 \dots b_n} |b_1 b_2 \dots b_n\rangle \otimes |x_{k_i y_i}\rangle$

$= |b_j\rangle \left(\sum_{i \neq j} \alpha_{b_1 b_2 \dots b_n} |b_1 b_2 \dots b_n\rangle \otimes |x \qquad \right)$

In Protocol Ⓓ, the measurement m_i is by measuring in Z basis,

$(Z \otimes H) U(\rho')$

Since U is trivial, measurement in Z basis shouldn't affect the measurement. (in reg ①)

So m_i is also same as measuring ρ' in Z basis directly, which results in outcome b_i exactly.

Case II: $h_i = 1$.

Protocol Ⓐ & Ⓓ differ at steps 7 and the measurement basis.

In Protocol Ⓐ,

we measure in X basis,

and then apply $X^{d_i \cdot (x_{k_i 0} + x_{k_i 1})}$ decoding operator

$\equiv$ measuring $X^{d_i \cdot (x_{k_i 0} + x_{k_i 1})} H(\rho)$ in Z basis

$\equiv$ $H Z^{d_i \cdot (x_{k_i 0} + x_{k_i 1})} (\rho)$ in Z basis.

$\equiv$ $Z^{d_i \cdot (x_{k_i 0} + x_{k_i 1})} (\rho)$ in X basis

which is what is happening in Protocol Ⓓ.

$$\Rightarrow \quad D_{S_h^{(2)},h} = D_{\mathbb{P},h} \qquad \blacksquare$$

From other previous results, $D_{S,h} = D_{S_h^{(1)},h} \sim D_{S_h^{(2)},h} = D_{\mathbb{P},h}$

$$\Rightarrow D_{S,h} \sim D_{\mathbb{P},h}.$$

Proof of Claim II

→ Crucially we have a prover $\mathbb{P}$ characterised by (U_0, S) who acc to Protocol Ⓐ, results in distribution $D_{\mathbb{P},h}$.
We would like to show that another prover $\mathbb{P}'$ characterised by (U_0, S') where S' is trivial, also results in distribution $D_{\mathbb{P}',h}$ same as $D_{\mathbb{P},h}$.

→ More formally,

For $S = \{B_\tau\}_\tau$ of prover $\mathbb{P}$ characterised by (U_0, S)
$\exists\ S_j = \{B'_{j,x,\tau}\}_{x\in\{0,1\},\tau}$ of prover $\mathbb{P}_j$ char. by (U_0, S_j)

s.t.
$$B_\tau = \sum_{x,z\in\{0,1\}} X^x Z^z \otimes B_{jxz\tau}$$
$$B'_{j,x,\tau} = \sum_{z\in\{0,1\}} Z^z \otimes B_{jxz\tau}$$
and $D_{\mathbb{P},h} = D_{\mathbb{P}_j,h}$

[$B_\tau, B_{jx\tau}$ are rearranged so that $X^x Z^z, Z^z$ act on the j^{th} qubit of reg ①].

→ Clearly S_j is trivial w.r.t. j^{th} qubit.

→ We can do this reduction one-by-one for every qubit, and the final CPTP map will be trivial wrt all qubits.

→ We do the proof for $j=1$.

Case I: $h_1 = 0$

$D_{\mathbb{P},h}, D_{\mathbb{P}_j,h}$ are trivially equal because, the attack S happens after measurement of "y" and doesn't affect the measurement output.

CASE II: $h_j = 1$

→ The state after step ④ should be

$$\sum_{b\in\{0,1\}} |b, x_{by}\rangle \underbrace{|\psi_{b,y,k}\rangle}_{} |y\rangle \qquad \text{s.t.} \quad f_{kb}(x_{by}) = y.$$

↳ correspond to the $i=2,3,\ldots n$ registers

if $\mathbb{P}$ (or $\mathbb{P}_j$) has to pass the TEST ROUND.

$$\rho_{yk} = \left[\sum_{b_1, b_2\in\{0,1\}} |b_1, x_{b_1 y}\rangle\langle b_2, x_{b_2 y}| \otimes |\psi_{b_1 yk}\rangle\langle\psi_{b_2 yk}|\right] \otimes |y\rangle\langle y|$$

→ Now, in measurement round, for prover $\mathbb{P}$, the state is step ⑥

$$\sum_{\tau} B_\tau \rho_{yk} B_\tau^\dagger$$

→ Measuring in X basis, ≡ Applying H gate and measuring in Z basis step ⑦

$$\sum_{\tau} (H^{\otimes l+1} \otimes I)\, B_\tau \rho_{yk} B_\tau^\dagger\, (H^{\otimes l+1} \otimes I)$$

→ Decoding operator XORing with $d\cdot(x_{0y} + x_{1y})$

$$\sum_{\tau} (X^{d\cdot(x_{0y}+x_{1y})} \otimes I)(H^{\otimes l+1} \otimes I)\, B_\tau \rho_{yk} B_\tau^\dagger\, (H^{\otimes l+1} \otimes I)(X^{d\cdot(x_{0y}+x_{1y})} \otimes I)$$

for the measurement results "d" on reg②

→ The distribution state is (applying projection operators

$$\sigma_{\mathbb{P},k} = \sum_{b,d,\tau} (|b\rangle\langle b| \otimes |d\rangle\langle d| \otimes I)(X^{d\cdot(x_{0y}+x_{1y})} \otimes I)(H^{\otimes l+1} \otimes I) B_\tau \rho_{yk}$$
$$B_\tau^\dagger (H^{\otimes l+1} \otimes I)(X^{d\cdot(x_{0y}+x_{1y})} \otimes I)(|b\rangle\langle b| \otimes |d\rangle\langle d| \otimes I)$$

$$= \sum_{bd\tau} O_{b,d\cdot(x_{0y}+x_{1y}),d,\tau}\ \rho_{yk}\ O^\dagger_{b,d\cdot(x_{0y}+x_{1y}),d,\tau}$$

where

$$O_{b,c,d,\tau} := (|b\rangle\langle b| \otimes |d\rangle\langle d| \otimes I)(X^c \otimes I)(H^{\otimes l+1} \otimes I) B_\tau$$

→ Say prover $\hat{P}_1$ is characterised by $(U_0, \{(Z \otimes I) S (Z \otimes I)\})$

→ Similarly the final distribution state for prover $\hat{P}_1$ is

$$\sigma_{\hat{P}_1,k} = \sum_{bd\tau} (|b\rangle\langle b| \otimes |d\rangle\langle d| \otimes I)(X^{d \cdot (x_{0y} + x_{1y})} \otimes I)(H^{\otimes l+1} \otimes I)$$

$$(Z \otimes I) B_\tau (Z \otimes I) \rho (Z \otimes I) B_\tau^\dagger (Z \otimes I)$$

$$(H^{\otimes l+1} \otimes I)(X^{d \cdot (x_{0y} + x_{1y})} \otimes I)(|b\rangle\langle b| \otimes |d\rangle\langle d| \otimes I)$$

$[HZ = XH]$

$$= \sum_{bd\tau} (|b\rangle\langle b| \otimes |d\rangle\langle d| \otimes I)(X^{d \cdot (x_{0y} + x_{1y}) \oplus c} \otimes I) B_\tau$$

$$(Z \otimes I) \rho (Z \otimes I)$$

$$B_\tau^\dagger (H^{\otimes l+1} \otimes I)(X^{d \cdot (x_{0y} + x_{1y}) + c} \otimes I)(|b\rangle\langle b| \otimes |d\rangle\langle d| \otimes I))$$

$$= \sum_{bd\tau} O_{b, d \cdot (x_{0y} + x_{1y}) + 1, d, \tau} (Z \otimes I) \rho (Z \otimes I) O^\dagger_{b, d \cdot (x_{0y} + x_{1y}) + 1, d, \tau}$$

→ We know prover P_1 is characterized by $(U_0, \{B'_{x\tau}\}_{x \in \{0,1\}, \tau})$

→ We have a Z-Pauli Twirl measurement result. (proved later)

When followed by Hadamard measurement, the CPTP attacks

$$\left\{\frac{1}{\sqrt{2}} (Z^x \otimes I) B_\tau (Z^x \otimes I)\right\}_{x \in \{0,1\}, \tau} \equiv \{B'_{x,\tau}\}_{x \in \{0,1\}, \tau}$$

→ So prover $\mathbb{P}_1$ is characterised by $\left(V_0, \left\{\frac{1}{\sqrt{2}}(Z^r\otimes I)B_\tau(Z^r\otimes I)\right\}_{r,\tau}\right)$

It looks like the CPTP of $\mathbb{P}_1$ is an average of $\mathbb{P}$ and of $\hat{\mathbb{P}}_1$.

$$\rightarrow \quad \sigma_{\mathbb{P}_1,h} = \frac{1}{2}\left(\sum_{bd\tau} O_{b,d\cdot(x_{0y}+x_{1y}),d,\tau}\, \rho_{yk}\, O^\dagger_{b,d\cdot(x_{0y}+x_{1y}),d,\tau}\right) + \frac{1}{2}\left(\sum_{bd\tau} O_{b,d\cdot(x_{0y}+x_{1y})+1,d,\tau}(Z\otimes I)\rho_{yk}(Z\otimes I)O^\dagger_{b,d\cdot(x_{0y}+x_{1y})+1,d,\tau}\right)$$

$$= \frac{1}{2}\left(\sigma_{\mathbb{P},h} + \sigma_{\hat{\mathbb{P}}_1,h}\right)$$

→ It suffices to show now that $\sigma_{\mathbb{P},h}$ is computationally indistinguishable from $\sigma_{\hat{\mathbb{P}}_1,h}$

$$\sigma_{0,k} := \sum_{bd\tau} O_{b,d\cdot(x_{0y}+x_{1y}),d,\tau}\, \rho_{yk}\, O^\dagger_{b,d\cdot(x_{0y}+x_{1y}),d,\tau}$$

$$\sigma_{1,k} := \sum_{bd\tau} O_{b,d\cdot(x_{0y}+x_{1y})+1,d,\tau}(Z\otimes I)\rho_{yk}(Z\otimes I)O^\dagger_{b,d\cdot(x_{0y}+x_{1y})+1,d,\tau}$$

$$\sigma_{r,k} = \sum_{bd\tau} O_{b,d\cdot(x_{0y}+x_{1y})+r,d,\tau}(Z^r\otimes I)\rho_{yk}(Z\otimes I)O^\dagger_{b,d+(x_{0y}+x_{1y})+r,d,\tau}$$

$$\sigma_r := \sum_k D_{V,h}(k)\,\sigma_{r,k}$$

$$\rightarrow \quad \rho_{yk} = \sum_{b_1 b_2} |b_1, x_{b_1 y}\rangle\langle b_2, x_{b_2 y}| \otimes |\psi_{b_1 yk}\rangle\langle\psi_{b_2 yk}| \otimes |y\rangle\langle y|$$

$$= \sum_b |b\rangle\langle b| \otimes |x_{by}\rangle\langle x_{by}| \otimes |\psi_{byk}\rangle\langle\psi_{byk}| \otimes |y\rangle\langle y|$$

Diagonal terms ρ^D_{yk}

$$+ \sum_b |b\rangle\langle b\oplus 1| \otimes |x_{by}\rangle\langle x_{b\oplus 1,y}| \otimes |\psi_{byk}\rangle\langle\psi_{b+1\, yk}| \otimes |y\rangle\langle y|$$

cross terms ρ^C_{yk}

$$= \rho^D_{yk} + \rho^C_{yk}$$

$$\rightarrow \quad \sigma_{rk} = \sum_{bd\tau} O_{brd\tau}(Z^r\otimes I)\left(\rho^D_{yk} + \rho^C_{yk}\right)(Z^r\otimes I)O^\dagger_{brd\tau}$$

$$= \sum_{bd\tau} O_{brd\tau}\left(\rho^D_{yk} + (-1)^r \rho^C_{yk}\right)O^\dagger_{brd\tau}$$

$$= \sigma^D_{rk} + \sigma^C_{rk}$$

$$\left[\begin{array}{l} Z|b\rangle\langle b|Z = |b\rangle\langle b| \\ Z|b\rangle\langle b+1|Z = -|b\rangle\langle b+1| \end{array}\right]$$

$\rightarrow \quad \sigma^D_{rk} = \sum_{bdt} O_{brdt}\, S^D_{yk}\, O^\dagger_{brdt}$

$$\sigma^C_{rk} = \sum_{bdt} O_{brdt}\, (-1)^r\, S^C_{yk}\, O^\dagger_{brdt}$$

$\rightarrow$ σ_{0k}, σ_{1k}'s first qubit denotes the measurement statistics with provers $\mathbb{P}, \hat{\mathbb{P}}_1$ respectively.

$$\mathrm{Tr}_{>1}[\sigma_{0k}] = \sum_m D_{\mathbb{P},h_1}(m)\, |m\rangle\langle m|$$

$$\mathrm{Tr}_{>1}[\sigma_{1k}] = \sum_m D_{\mathbb{P},h_2}(m)\, |m\rangle\langle m|$$

$D_{\mathbb{P},h_1} \sim D_{\mathbb{P},h_2} \Longleftarrow \sigma_{0k}, \sigma_{1k}$ are computationally indistinguishable

$\rightarrow$ To prove: σ_{0k}, σ_{1k} are computationally indistinguishable

$\Rightarrow$ (1) $\sigma^D_{0k}, \sigma^D_{1k}$ are computationally indistinguishable
(2) $\sigma^C_{0k}, \sigma^C_{1k}$ are computationally indistinguishable.

$\rightarrow$ (1) $\sigma^D_{0k}, \sigma^D_{1k}$ are computationally indistinguishable

Proof: Assume not.
i.e, $\exists$ procedure $\mathcal{A}$ that distinguishes them
i.e., $\exists$ a CPTP map $\mathcal{S}$ which when passed through a state σ and then measuring (the first qubit) is able to find out if $\sigma = \sigma^D_{0k}$ or σ^D_{1k}.

$$\left| \mathrm{Tr}(|0\rangle\langle 0| \otimes I)\, \mathcal{S}(\sigma^D_{0k} - \sigma^D_{1k}) \right| \geq \lambda(n)$$

$\hookrightarrow$ not a negligible fxn.

(Idea: Use $\mathcal{A}$ to violate the hardcore bit property of $\mathcal{F}$).