Verifier on a Leash

Andrea Coladangelo

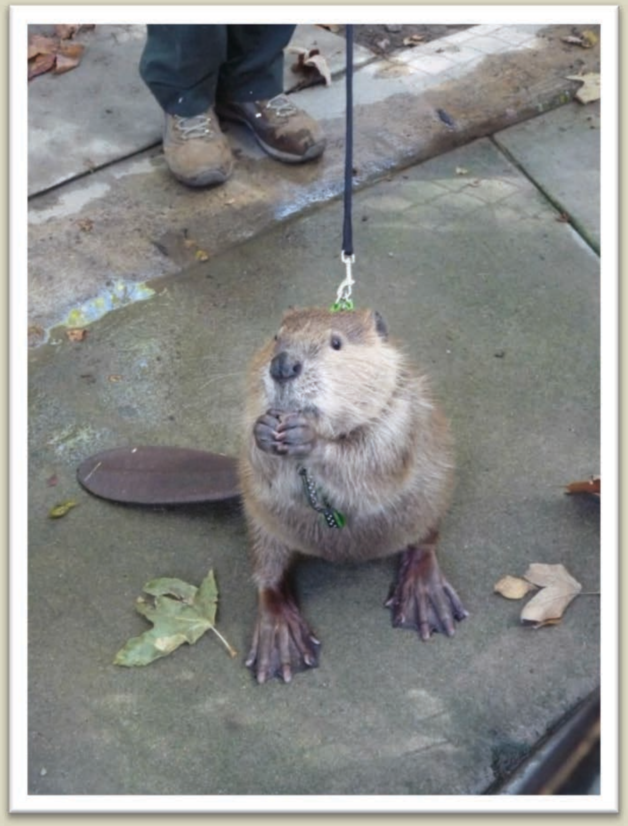
Based on joint work with Alex Grilo, Stacey Jeffery and Thomas Vidick

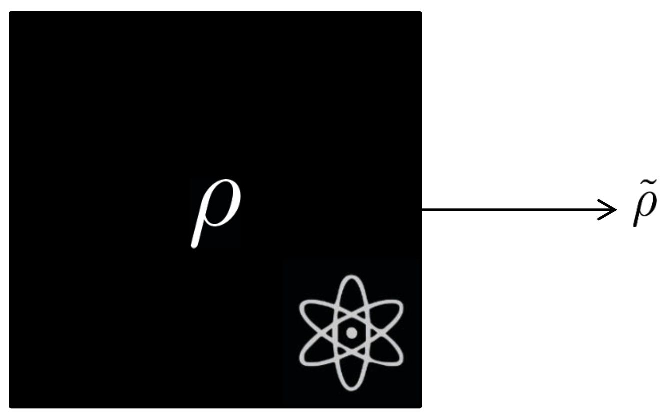
QuSoft
Research Center for Quantum Software

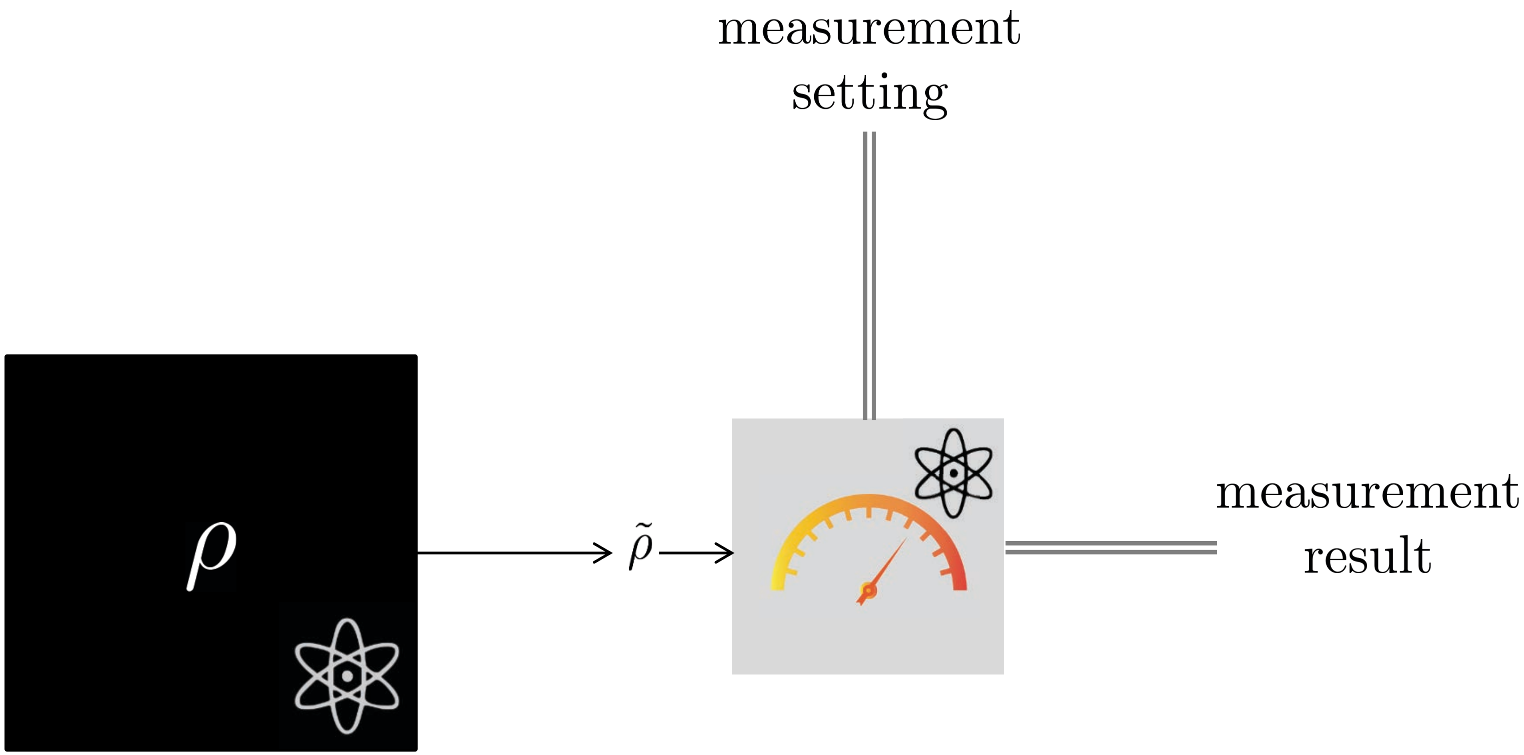
Caltech

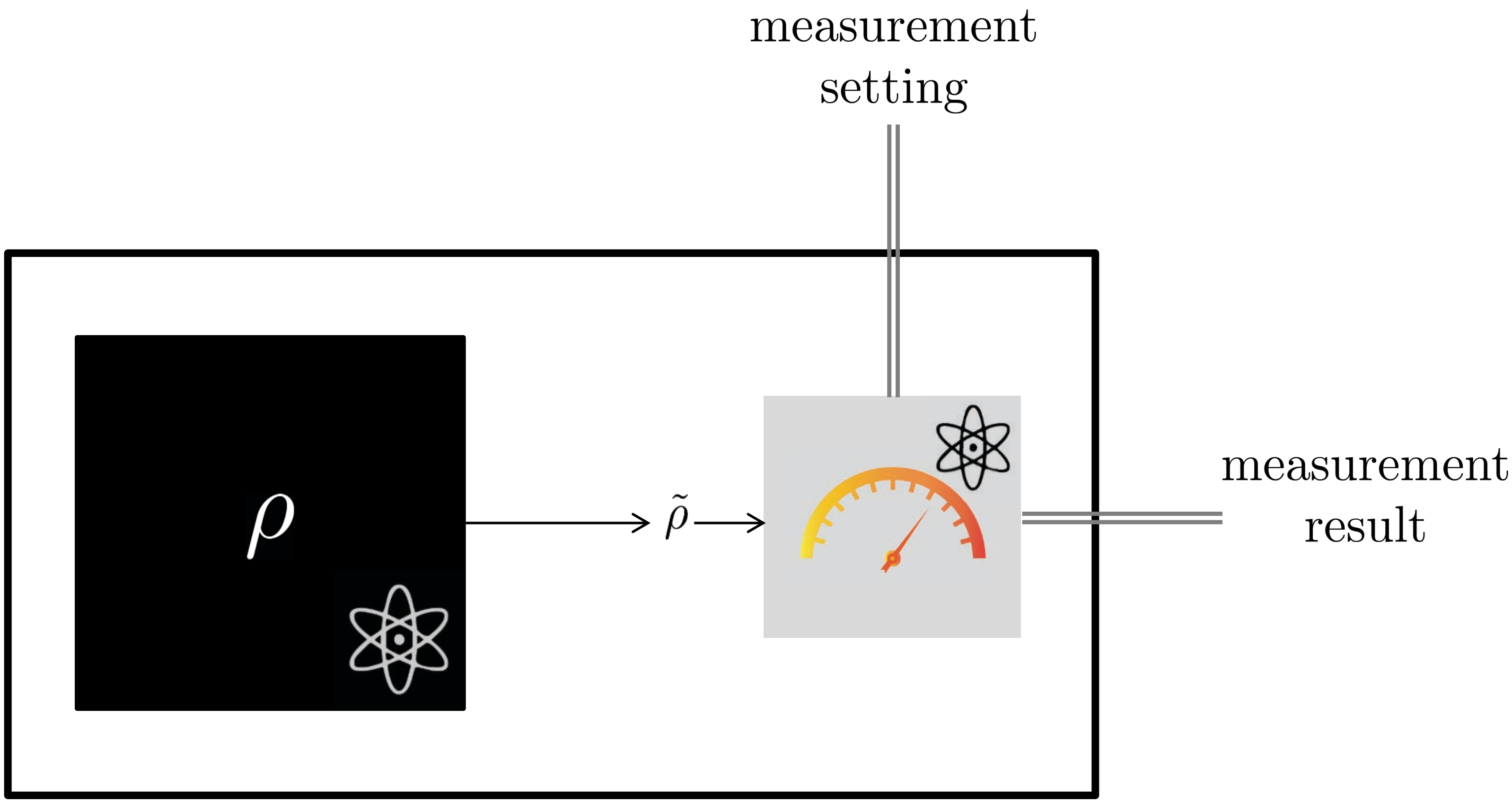
université
PARIS DIDEROT
PARIS 7

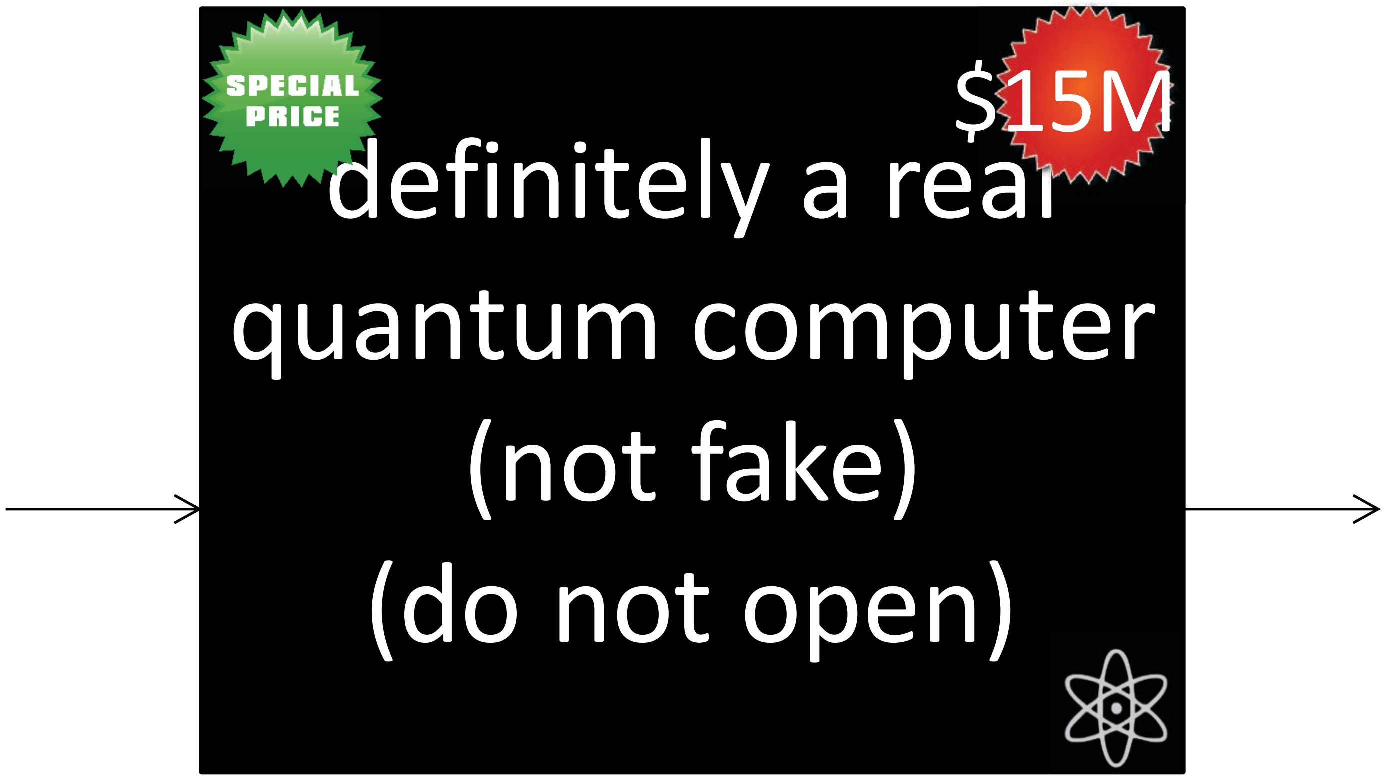
Testing a Quantum Device

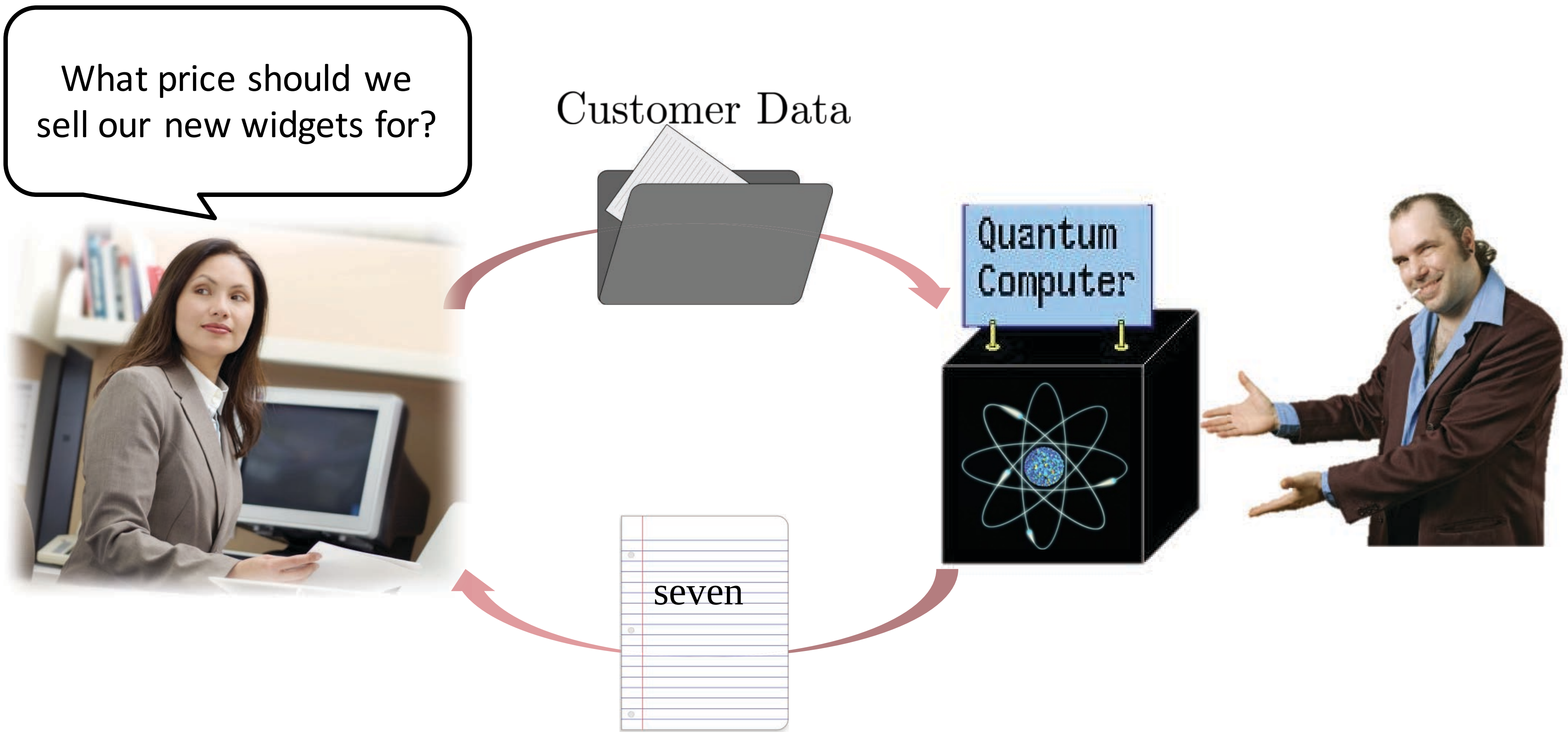



ρ
$\tilde{\rho}$

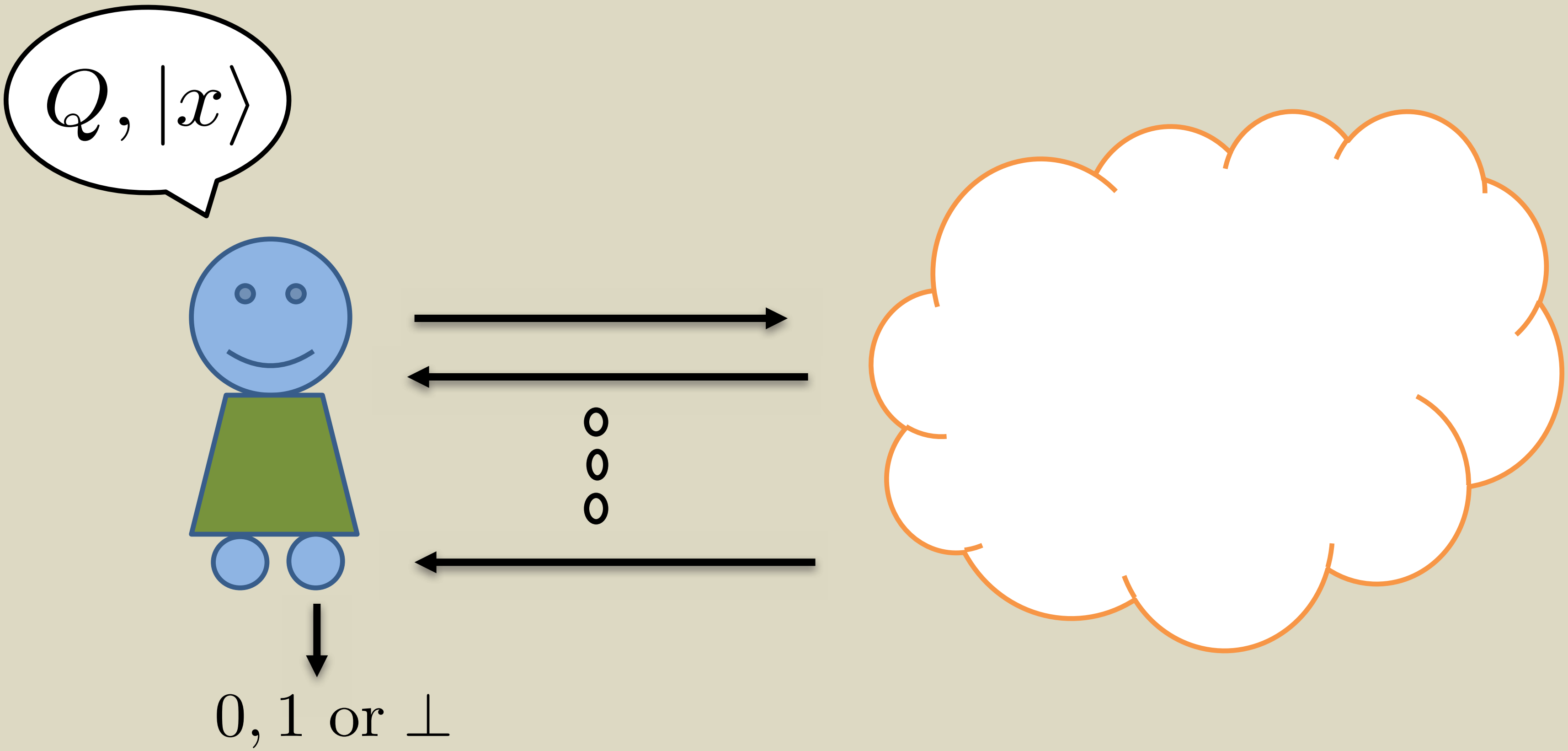

measurement
setting
ρ
$\tilde{\rho}$
measurement
result


measurement
setting
ρ
$\tilde{\rho}$
measurement
result


SPECIAL PRICE
$15M
definitely a real quantum computer
(not fake)
(do not open)


What price should we sell our new widgets for?
Customer Data
Quantum Computer
seven

Delegating a Quantum Computation



Desired properties

Desired properties

Verifiability:

Either the verifier outputs $\perp$,
OR she is outputting the correct outcome of the computation (with very high probability).

Desired properties

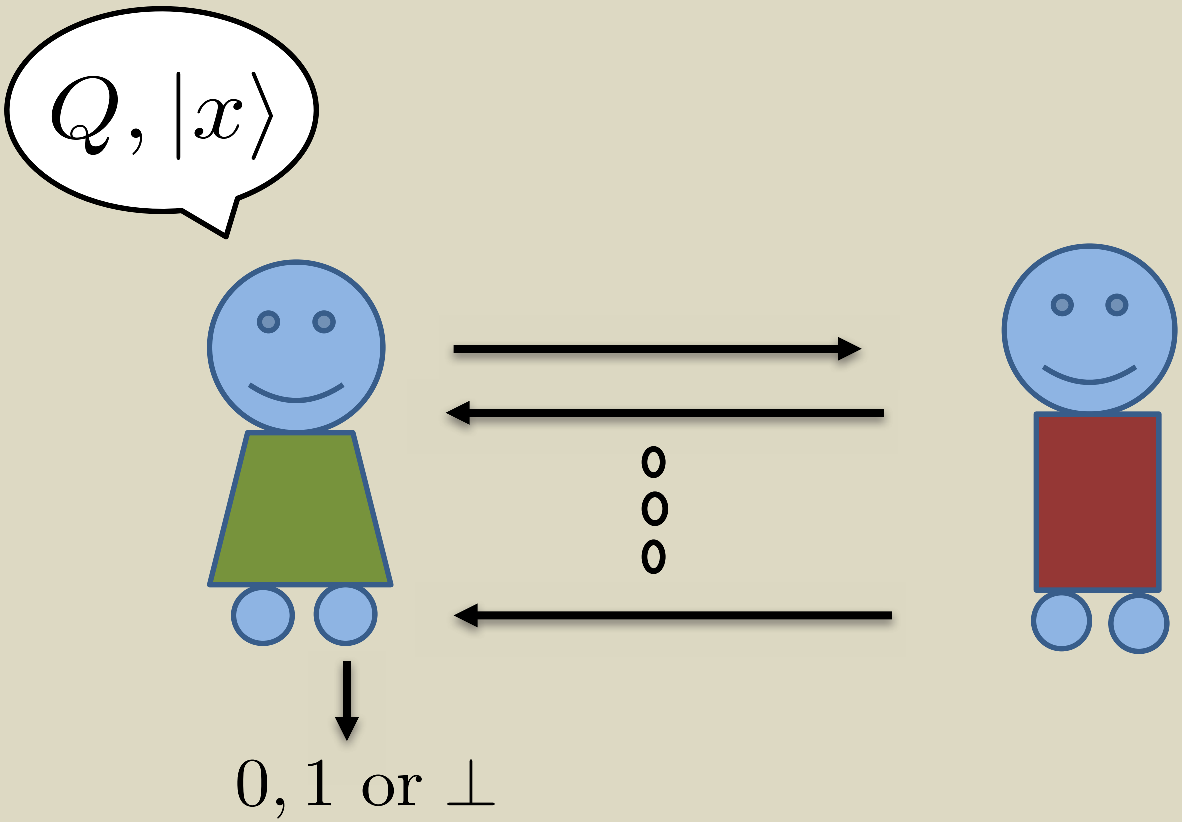
Verifiability:

Either the verifier outputs $\perp$,
OR she is outputting the correct outcome of the computation (with very high probability).

Blindness:

The final state of the server and his view of the transcript don't depend on the verifier's input to the protocol.

Single-Prover Delegation



Single-Prover delegation

Single-Prover delegation

- (Slightly) Quantum verifier,
- Single prover bound by quantum mechanics,
- Verifier interacts (quantumly) with provers

[Aharonov, Ben-Or, Eban 2010]

[Broadbent 2015]

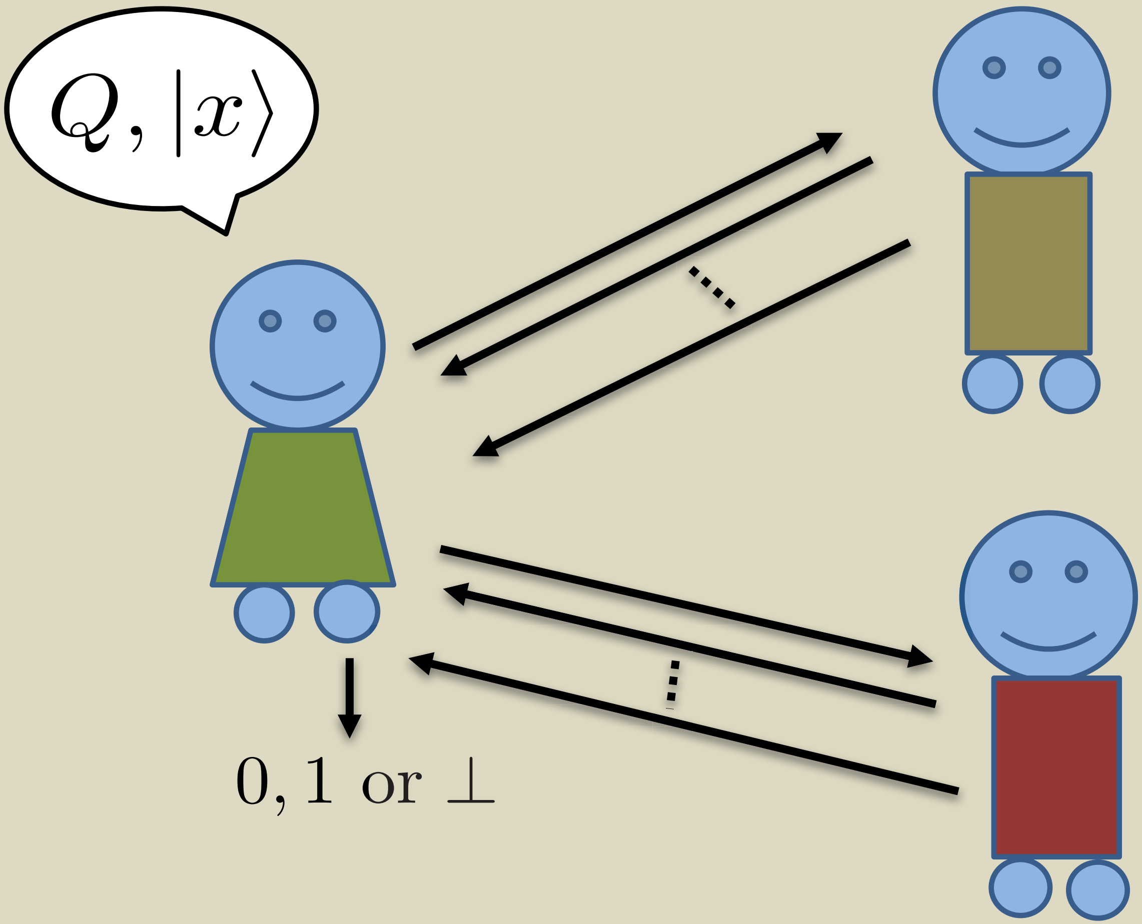
[Fitzsimons, Kashefi 2017]

[Morimae 2014]

[Morimae, Fitzsimons 2016]

Complexity of delegating m-gate circuit: $O(m)$

Two-Provers Delegation



Two-provers delegation

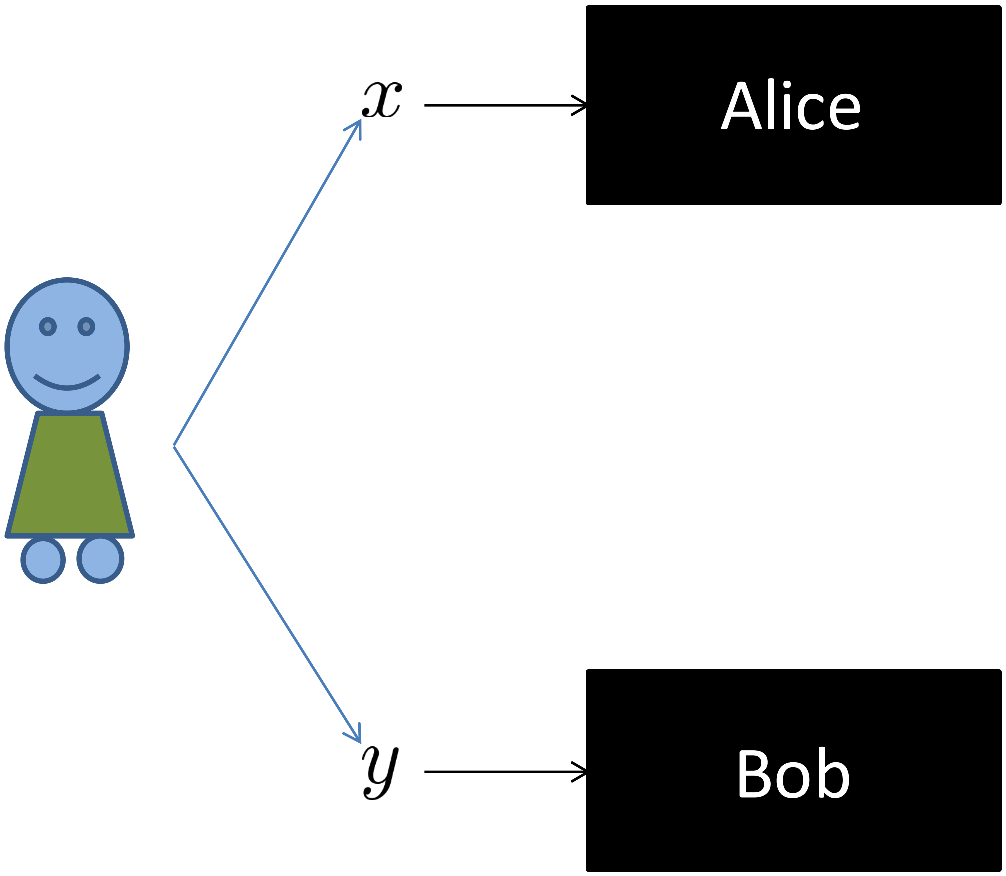
Two-provers delegation

- Classical verifier
- Two provers bound by quantum mechanics, and non-communicating.
- Verifier interacts (classically) with provers.

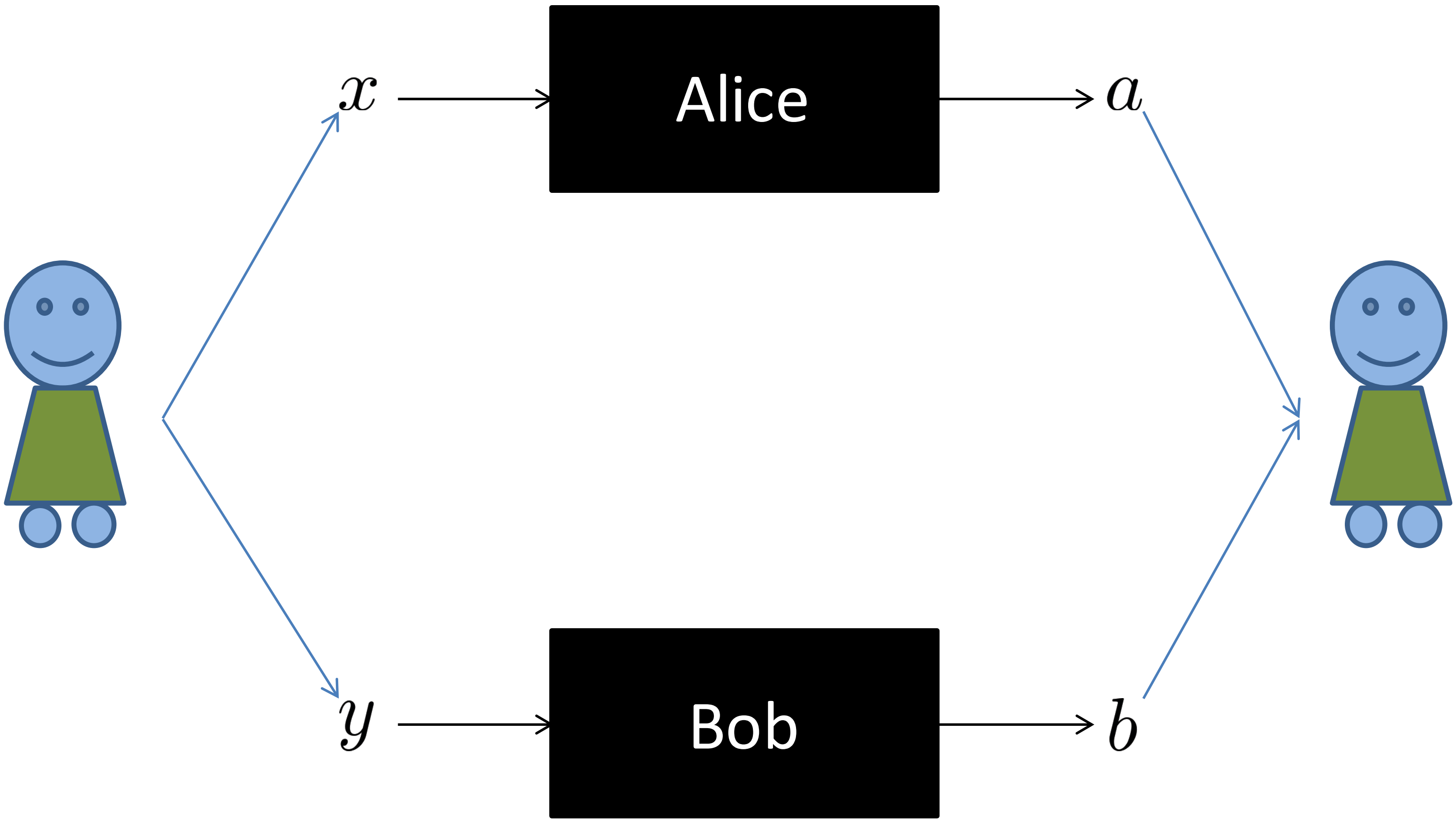
Bell Inequalities

CHSH Game

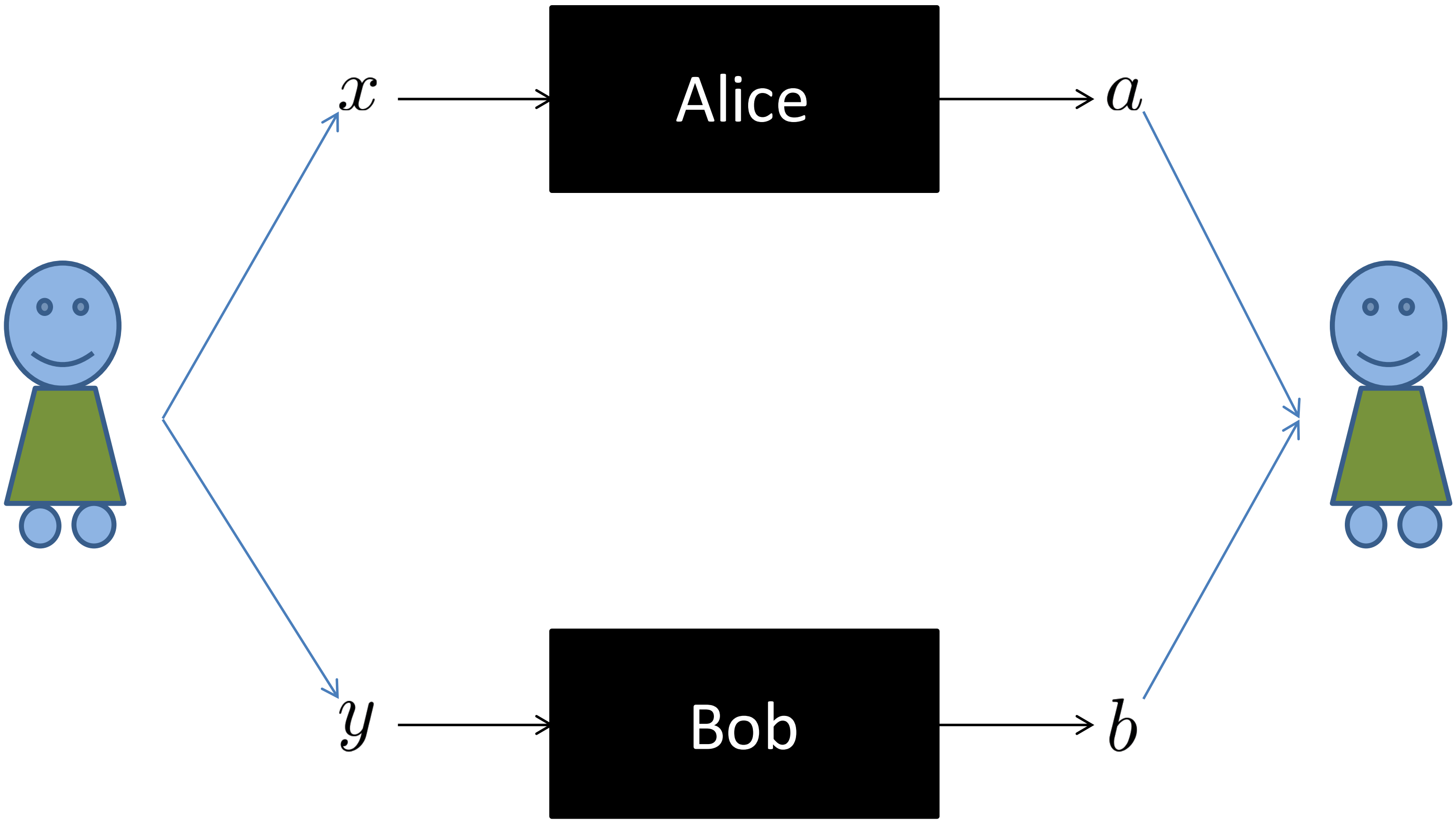
CHSH Game



CHSH Game

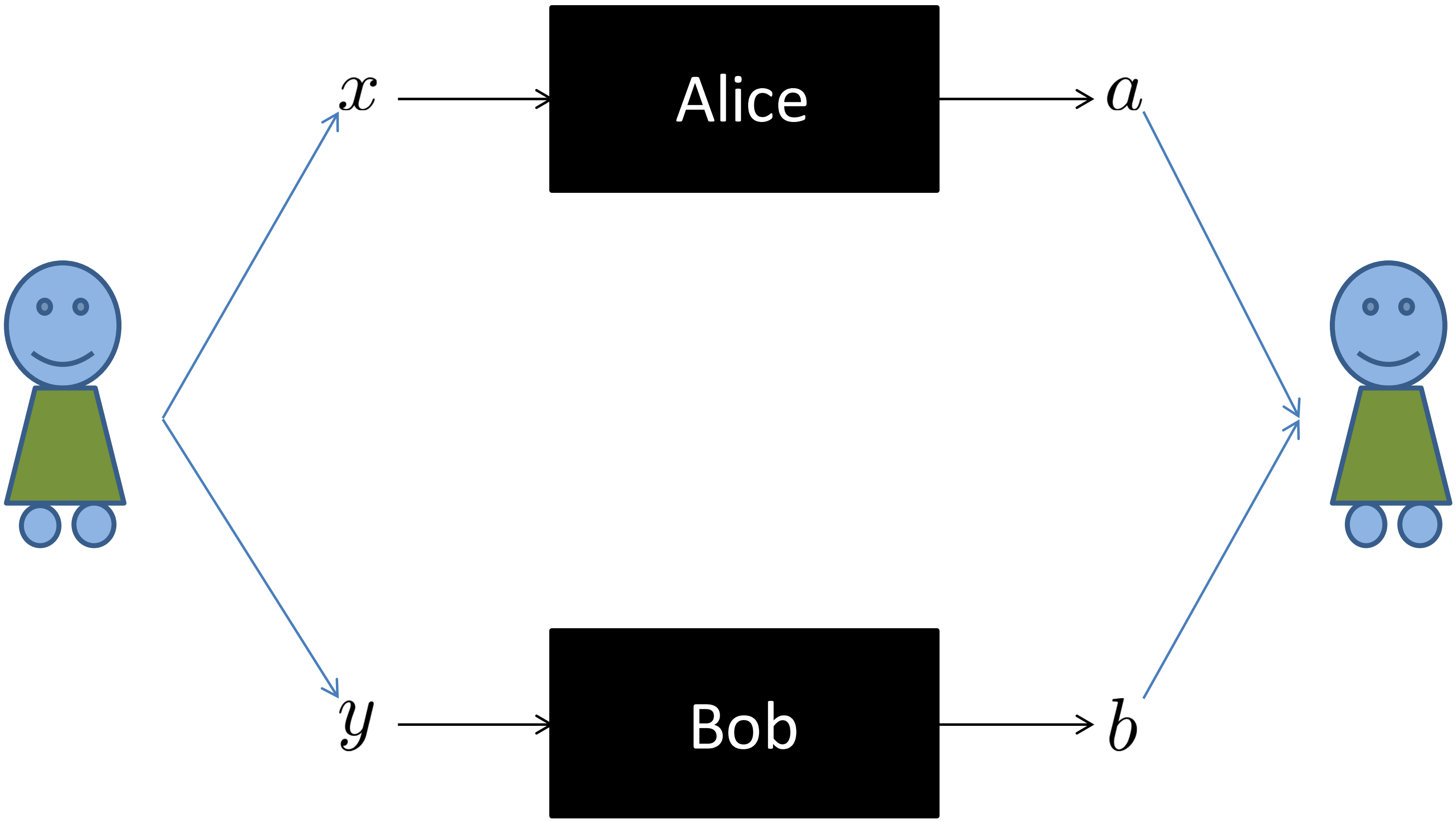


CHSH Game



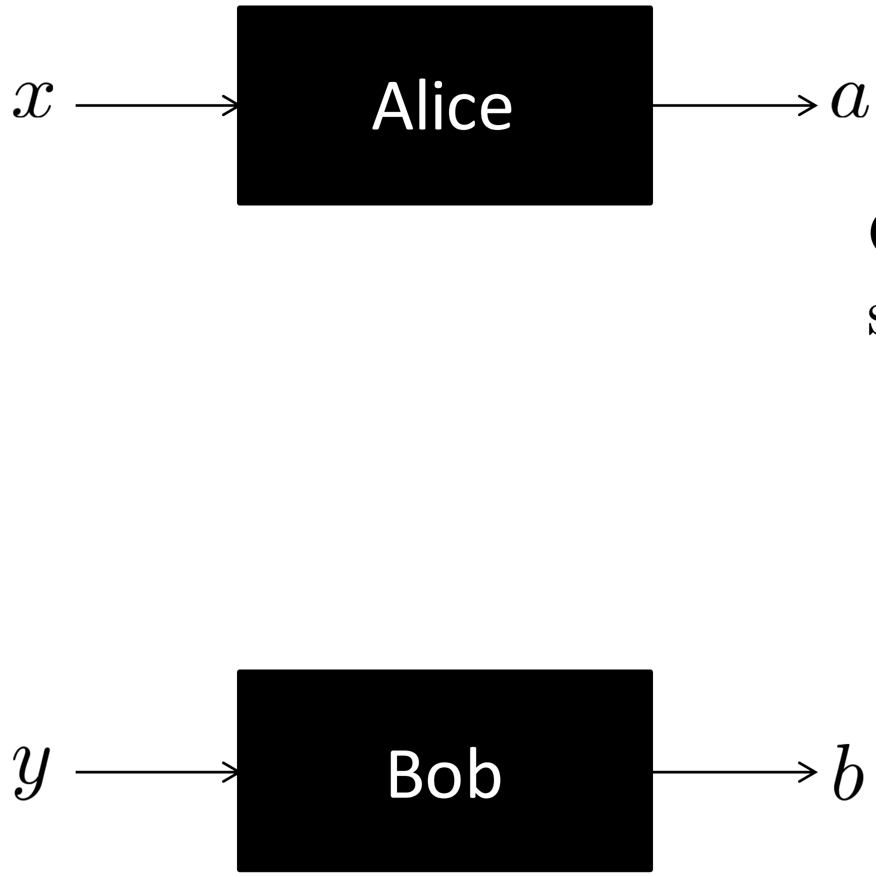
Alice and Bob win if $a \oplus b = xy$

CHSH Game



Alice and Bob win if $a \oplus b = xy$

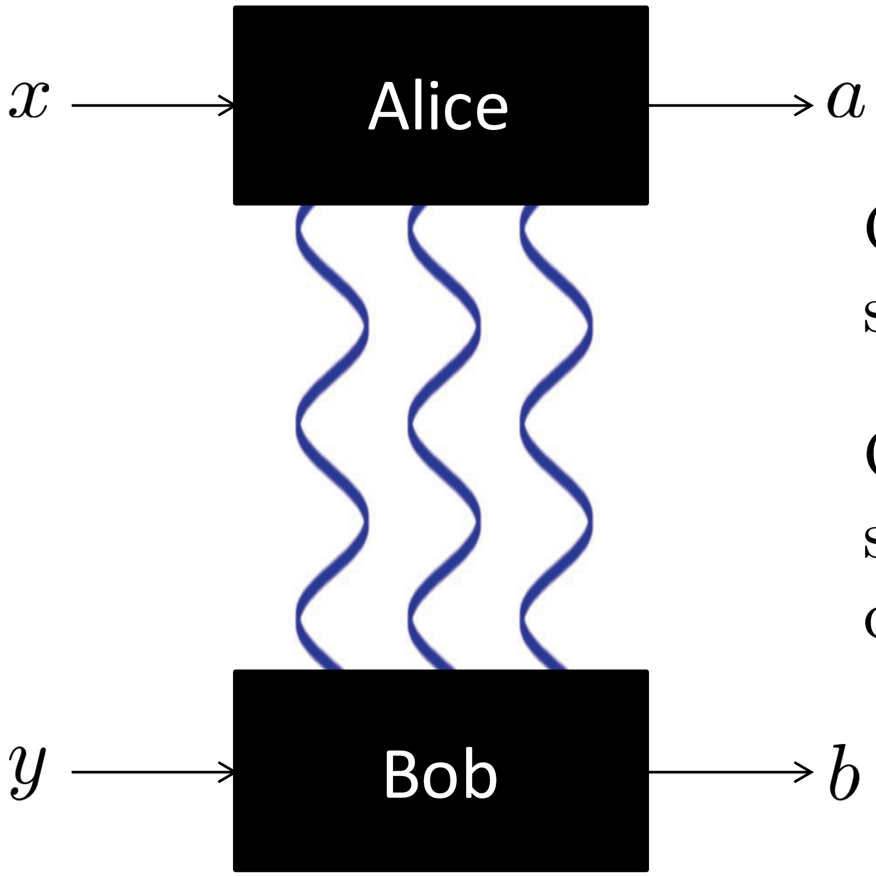
CHSH Game



Optimal classical success prob.: $\frac{3}{4}$

Alice and Bob win if $a \oplus b = xy$

CHSH Game



Optimal classical success prob.: $\frac{3}{4}$

Optimal quantum success prob.: $\cos^2 \frac{\pi}{8} \approx .85$

Alice and Bob win if $a \oplus b = xy$

CHSH Game

Optimal classical success prob.: $\frac{3}{4}$

Optimal quantum success prob.: $\cos^2 \frac{\pi}{8} \approx .85$

Alice and Bob win if $a \oplus b = xy$

CHSH Game

$$|EPR\rangle = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_B$$

Optimal classical success prob.: $\frac{3}{4}$

Optimal quantum success prob.: $\cos^2\frac{\pi}{8} \approx .85$

Alice and Bob win if $a \oplus b = xy$

CHSH Game

$$|EPR\rangle = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_B$$

$$A_0 = \sigma_Z, \quad A_1 = \sigma_X$$

Optimal classical success prob.: $\frac{3}{4}$

Optimal quantum success prob.: $\cos^2\frac{\pi}{8} \approx .85$

Alice and Bob win if $a \oplus b = xy$

CHSH Game

$$|EPR\rangle = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_B$$

$$A_0 = \sigma_Z, \quad A_1 = \sigma_X$$

$$B_0 = \frac{\sigma_Z + \sigma_X}{2}, \quad B_1 = \frac{\sigma_Z - \sigma_X}{2}$$

Optimal classical success prob.: $\frac{3}{4}$

Optimal quantum success prob.: $\cos^2 \frac{\pi}{8} \approx .85$

Alice and Bob win if $a \oplus b = xy$

CHSH Game

CHSH Game

If Alice and Bob play CHSH and win with probability opt, they must share an EPR pair.

CHSH Game

If Alice and Bob play CHSH and win with probability opt, they must share an EPR pair.

If Alice and Bob play n rounds of CHSH and win an $\text{opt} - \epsilon$ fraction of the games, their strategy must be within $\delta(\epsilon, n)$ of the n-fold tensor product of optimal single-round strategies.

[Reichardt, Unger, Vazirani 2012]

CHSH Game

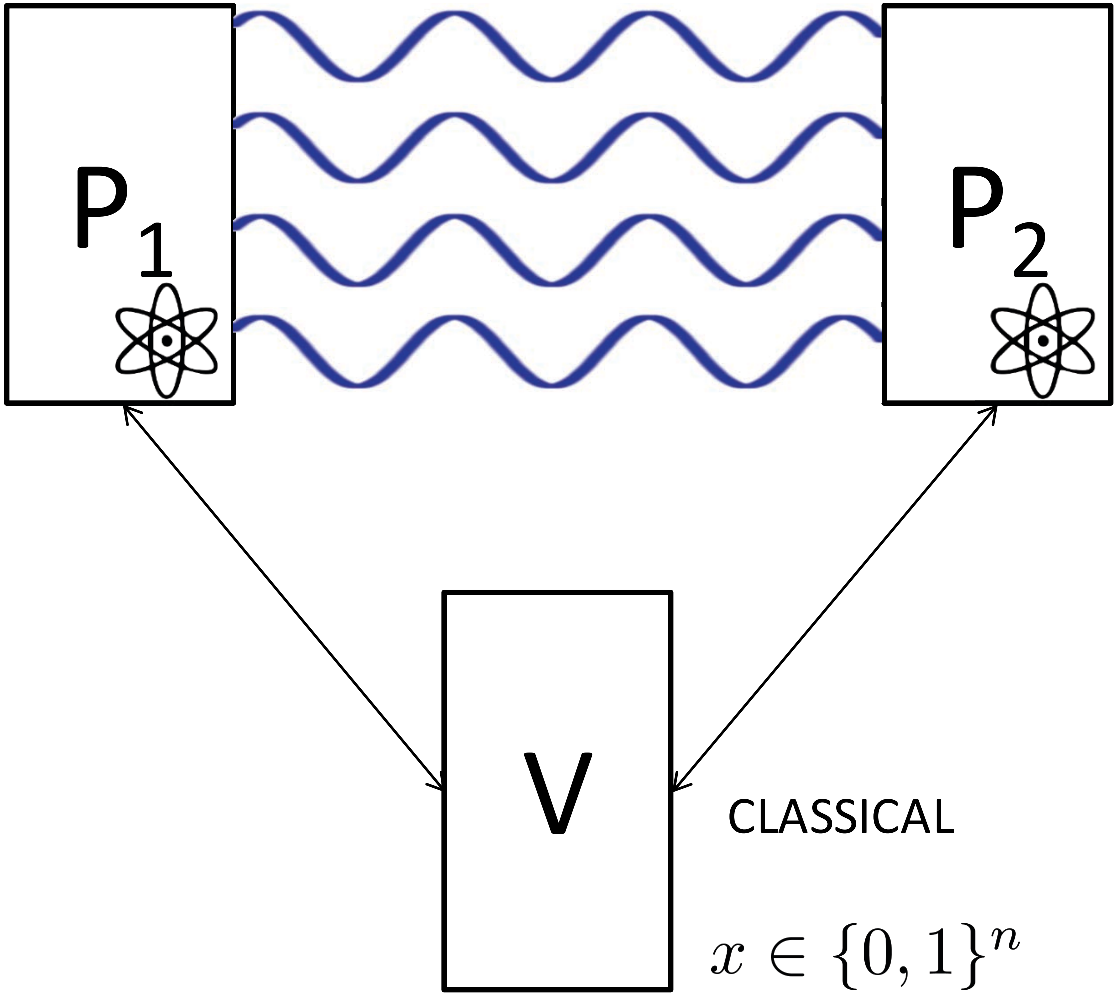
If Alice and Bob play CHSH and win with probability opt, they must share an EPR pair.

If Alice and Bob play n rounds of CHSH and win an $\text{opt} - \epsilon$ fraction of the games, their strategy must be within $\delta(\epsilon, n)$ of the n-fold tensor product of optimal single-round strategies.

This property is called RIGIDITY or SELF-TESTING

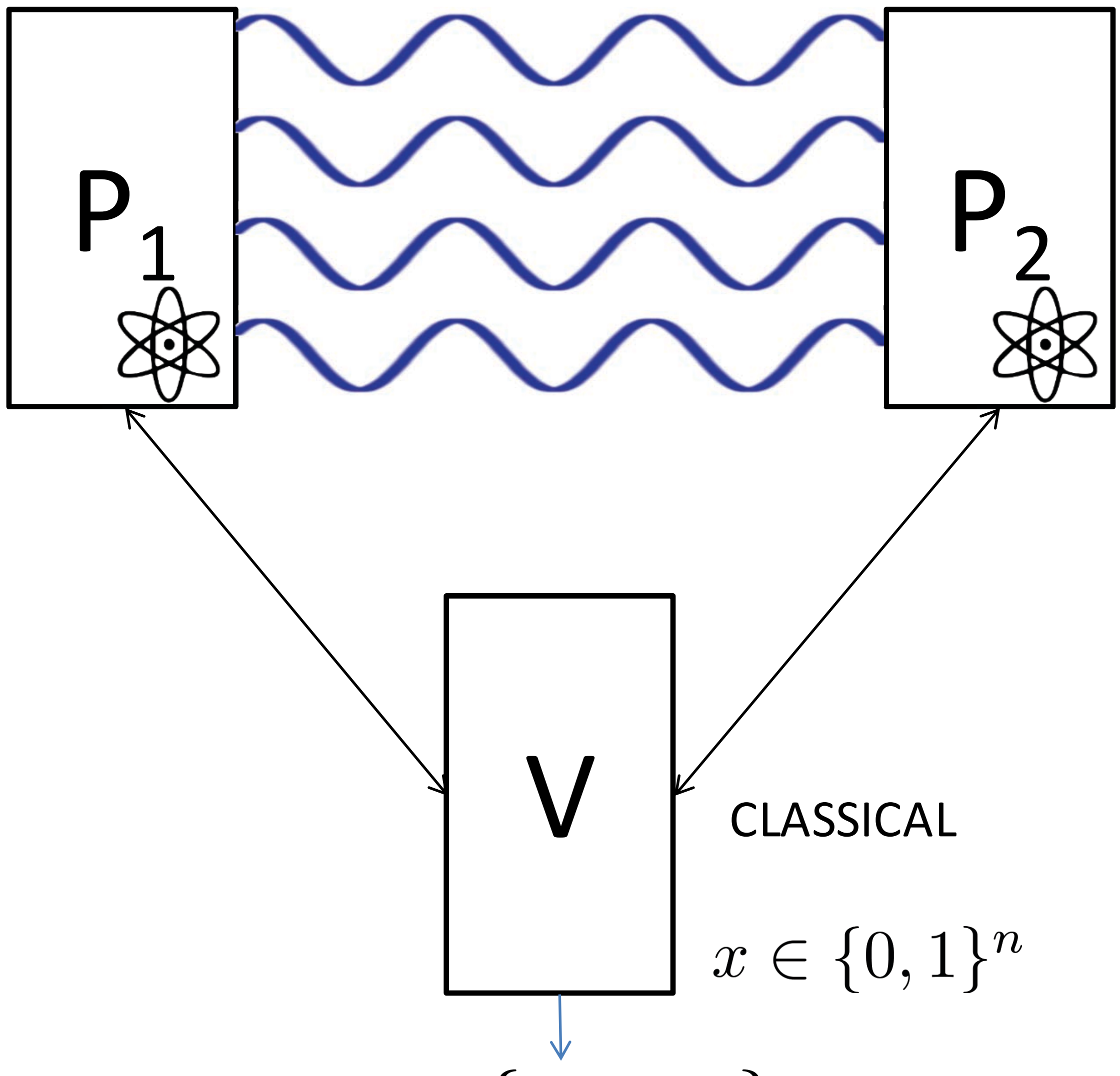
[Reichardt, Unger, Vazirani 2012]

RUV Protocol



[Reichardt, Unger, Vazirani 2012]

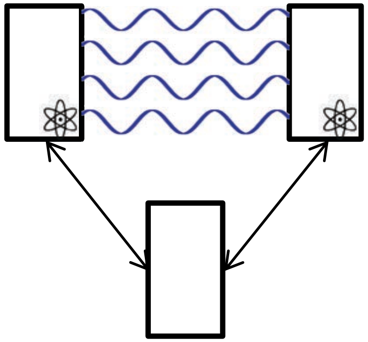
RUV Protocol



$$c \in \{0, 1, \perp\}$$

[Reichardt, Unger, Vazirani 2012]

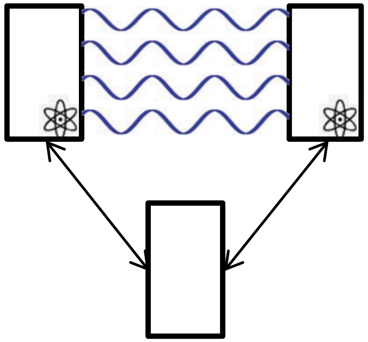
RUV Protocol



[Reichardt, Unger, Vazirani 2012]

RUV Protocol

- Key insight: alternate Rigidity test with actual computation.

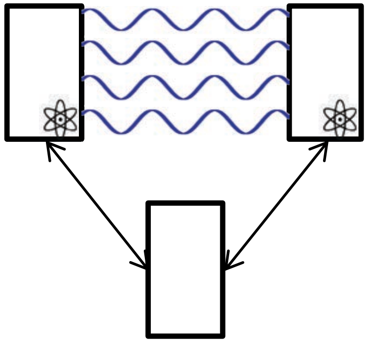


[Reichardt, Unger, Vazirani 2012]

RUV Protocol

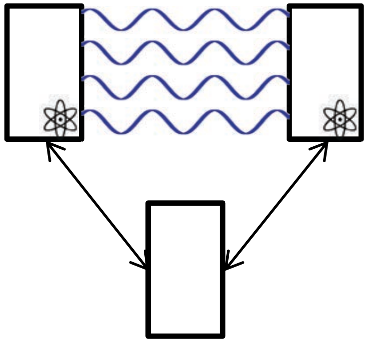
- Key insight: alternate Rigidity test with actual computation.

- Enforce that Prover 2 prepares certain resource states on Prover 1’s side.



[Reichardt, Unger, Vazirani 2012]

RUV Protocol



- Key insight: alternate Rigidity test with actual computation.
- Enforce that Prover 2 prepares certain resource states on Prover 1's side.
- Have Prover 1 use these resource states to perform computation by teleportation.

[Reichardt, Unger, Vazirani 2012]

Complexity of delegating m-gate circuit:

[Reichardt, Unger, Vazirani 2012]

Complexity of delegating m-gate circuit: $O(m^{8192})$

[Reichardt, Unger, Vazirani 2012]

Complexity of delegating m-gate circuit: $O(m^{8192})$

[Reichardt, Unger, Vazirani 2012]

[McKague 2013]

[Gheorghiu, Kashefi, Wallden 2015]

[Hajdušek, Perez-Delgado, Fitzsimons 2015]

[Fitzsimons, Hajdušek 2015]

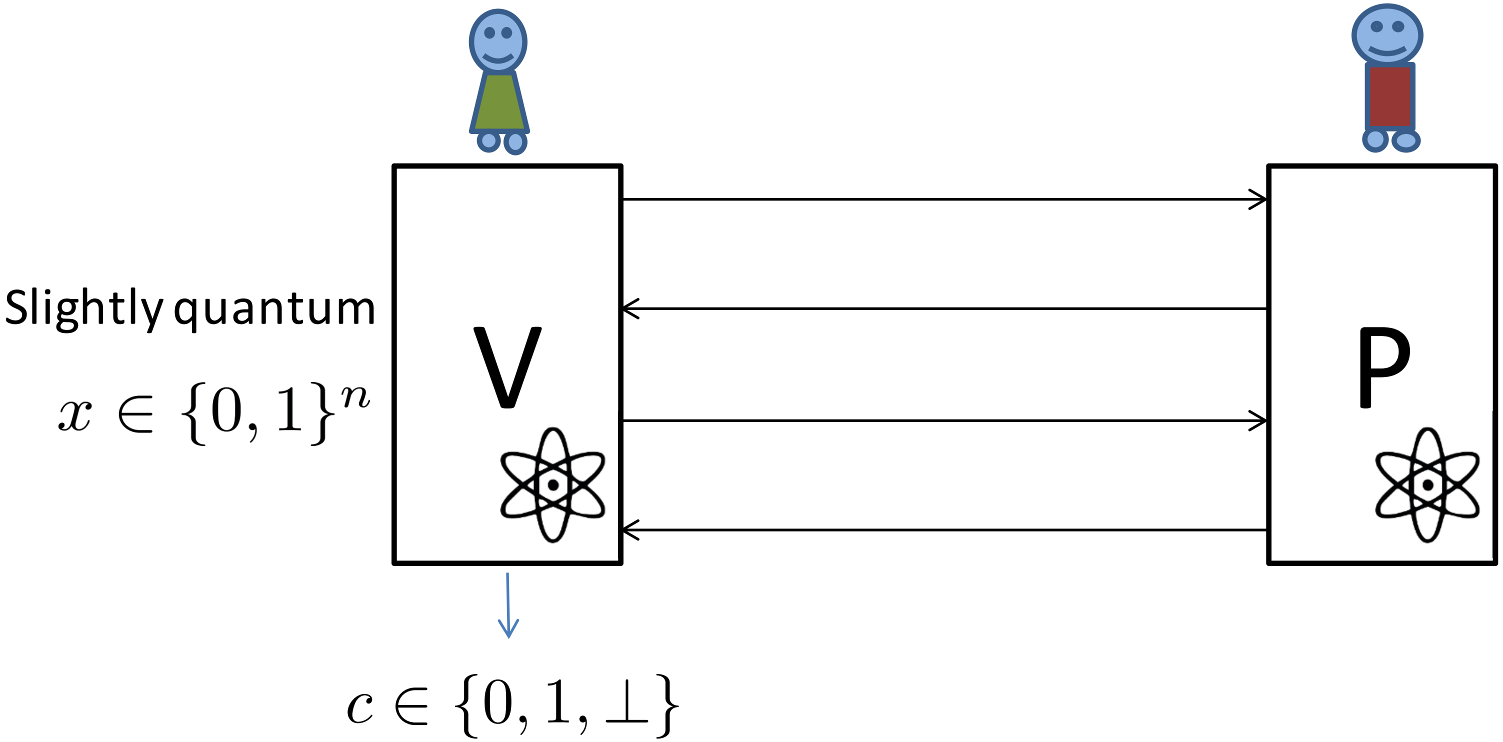
[Natarajan, Vidick 2016]

$\Omega(m^4)$

Our result in one sentence:

We develop new rigidity results, and use them to turn a single-prover delegation protocol into a two prover protocol with overall complexity scaling as $O(m \log m)$.

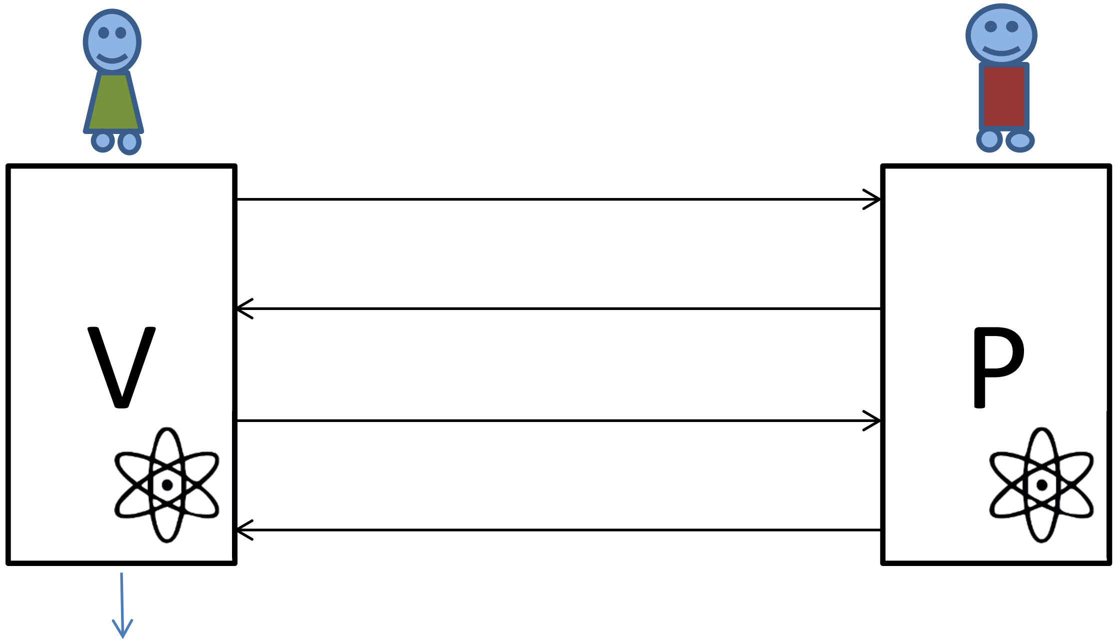
EPR Protocol [Broadbent 2016]



EPR Protocol [Broadbent 2016]

Slightly quantum

$x \in \{0,1\}^n$



$c \in \{0,1,\perp\}$

Complexity of delegating m-gate circuit: $O(m)$

EPR Protocol

EPR Protocol

$$\{H, CNOT, T\}$$

EPR Protocol

$\{H, CNOT, T\}$

$T\left|b\right\rangle = e^{ib\pi/4}\left|b\right\rangle$

EPR Protocol

$$\{H, CNOT, T\}$$

$$T\left|b\right\rangle = e^{ib\pi/4}\left|b\right\rangle$$

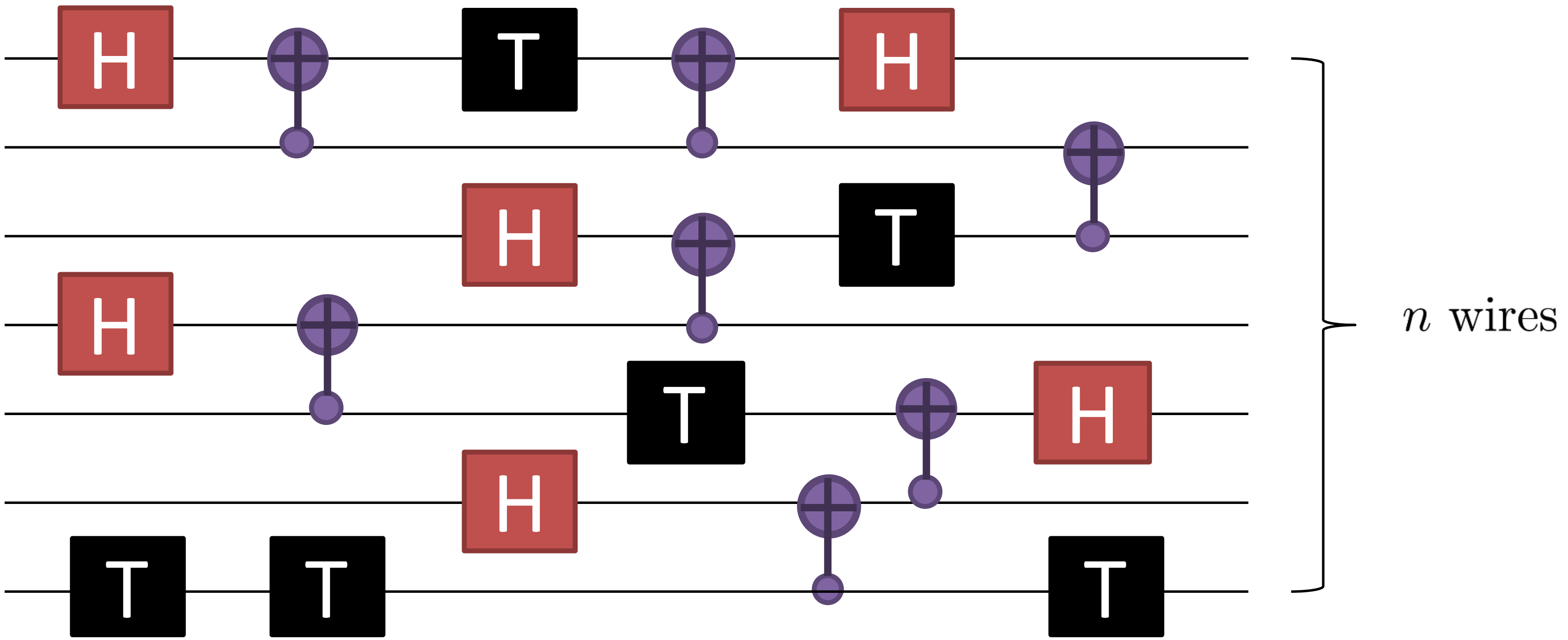
$$P\left|b\right\rangle = e^{ib\pi/2}\left|b\right\rangle$$

EPR Protocol

$$\{H, CNOT, T\}$$

$$T\,|b\rangle = e^{ib\pi/4}\,|b\rangle$$

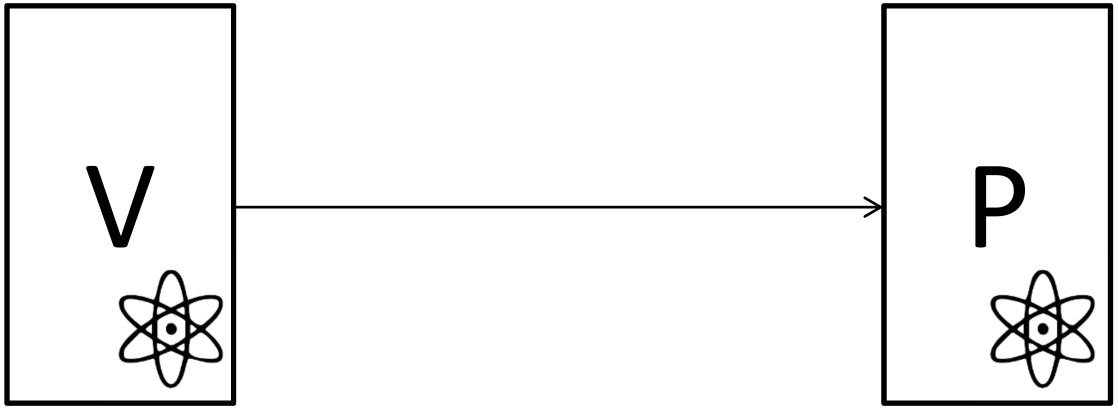
$$P\,|b\rangle = e^{ib\pi/2}\,|b\rangle$$



EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$

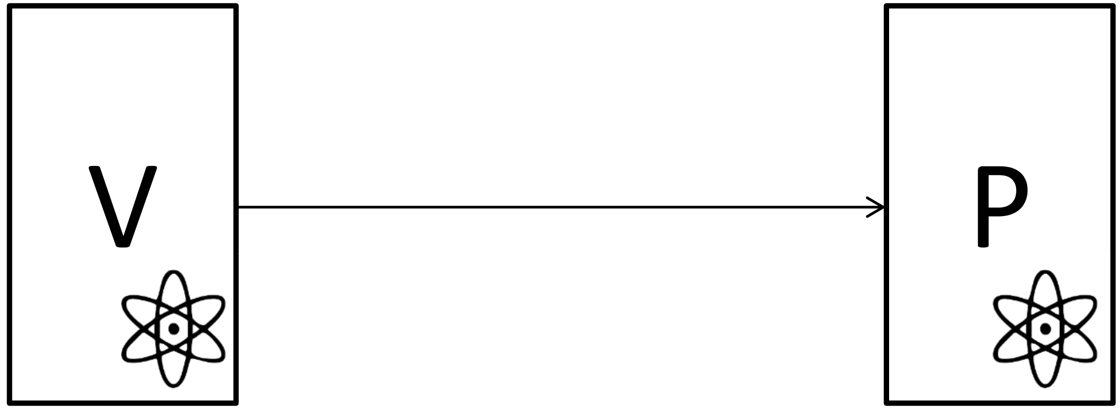


[Broadbent 2016]

EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$



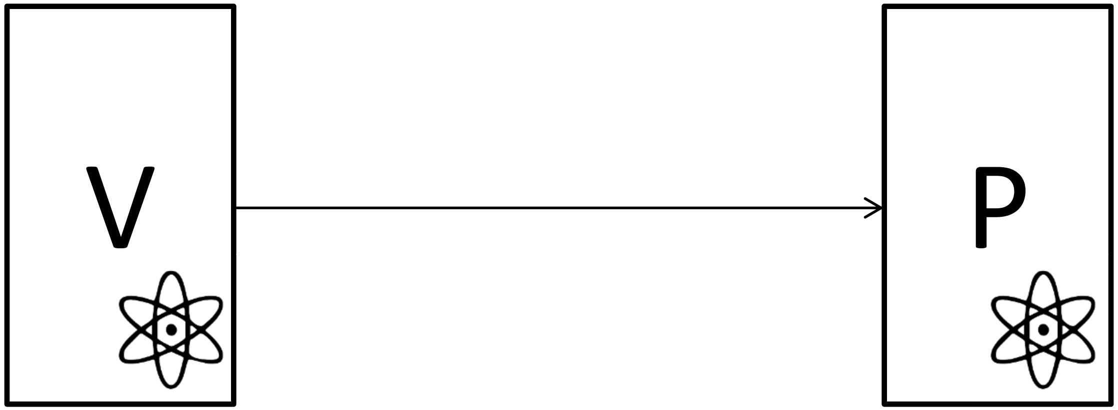
- V selects encrypting key at random: $a \in \{0,1\}^n$

[Broadbent 2016]

EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$



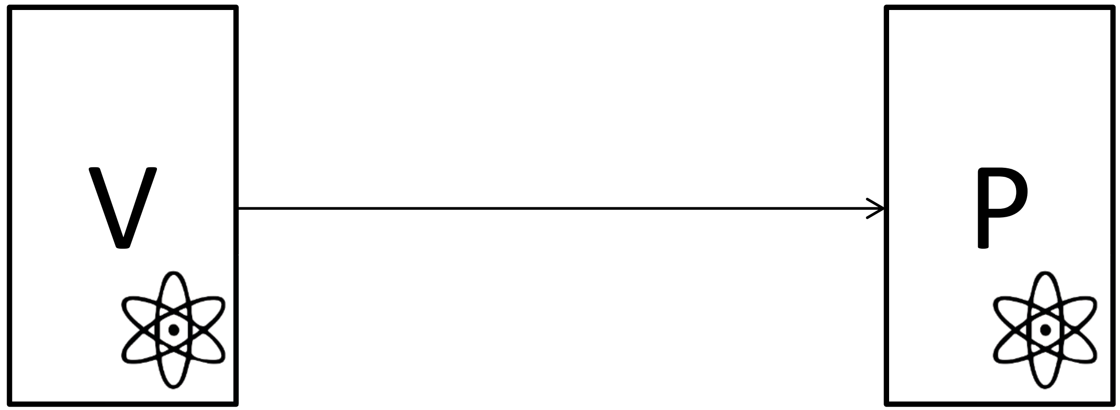
- V selects encrypting key at random: $a \in \{0,1\}^n$
- Sends encrypted input to P: $X^{a_1}\,|x_1\rangle \otimes \cdots \otimes X^{a_n}\,|x_n\rangle$

[Broadbent 2016]

EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$



- V selects encrypting key at random: $a \in \{0,1\}^n$

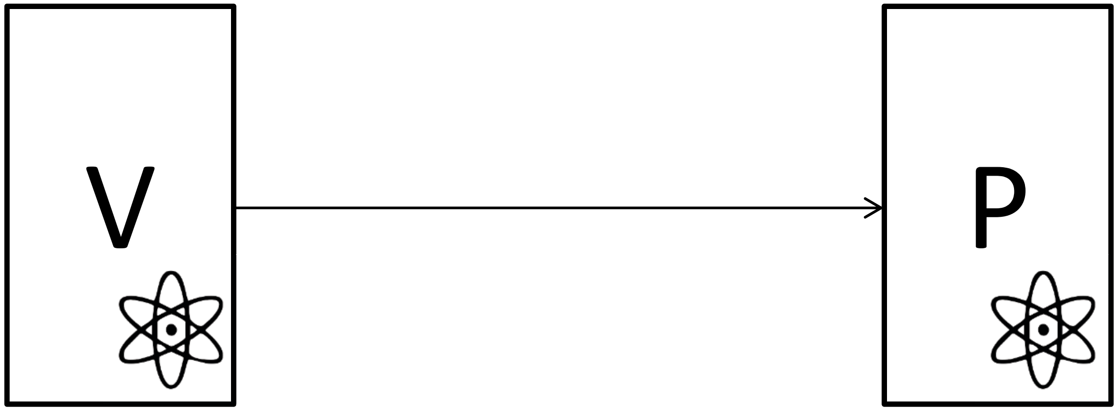
- Sends encrypted input to P: $X^{a_1} |x_1\rangle \otimes \cdots \otimes X^{a_n} |x_n\rangle$
    - Share n EPR pairs, V measures each half in comp. basis with outcomes $e_1, .., e_n$

[Broadbent 2016]

EPR Protocol

Slightly quantum

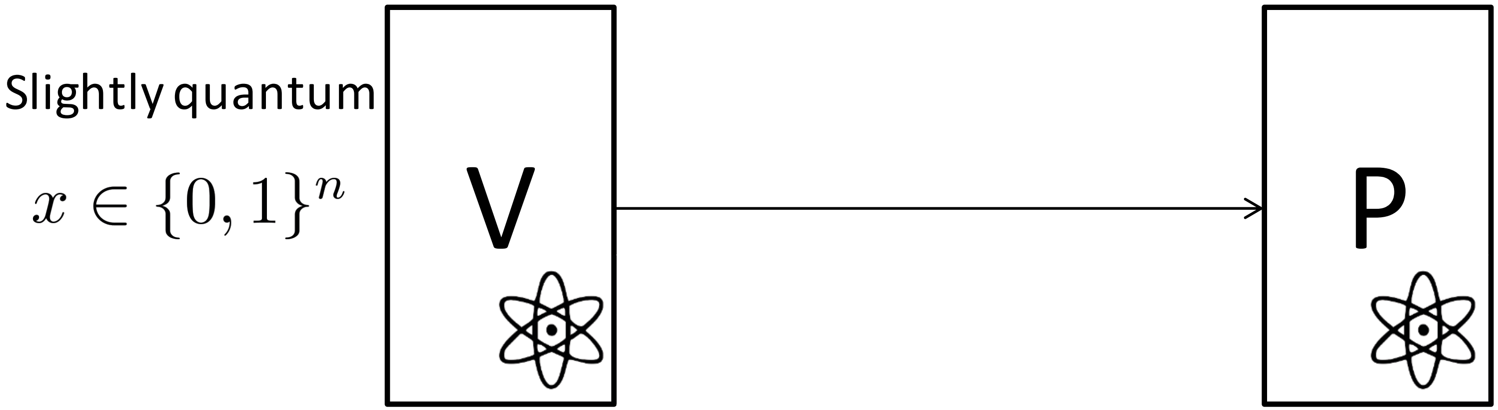
$x \in \{0,1\}^n$



- V selects encrypting key at random: $a \in \{0,1\}^n$
- Sends encrypted input to P: $X^{a_1}|x_1\rangle \otimes \cdots \otimes X^{a_n}|x_n\rangle$
  - Share n EPR pairs, V measures each half in comp. basis with outcomes $e_1, .., e_n$
  - Halves of P collapse to $|e_1, .., e_n\rangle$

[Broadbent 2016]

EPR Protocol

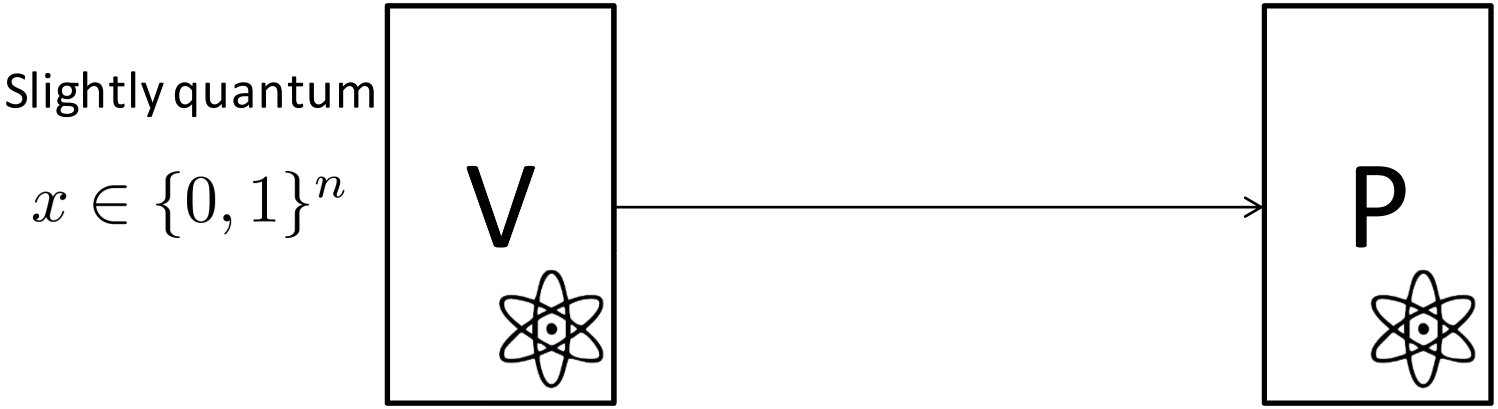


- V selects encrypting key at random: $a \in \{0,1\}^n$

- Sends encrypted input to P: $X^{a_1}|x_1\rangle \otimes \cdots \otimes X^{a_n}|x_n\rangle$
  - Share n EPR pairs, V measures each half in comp. basis with outcomes $e_1, .., e_n$
  - Halves of P collapse to $|e_1, .., e_n\rangle$
  - V sets the encrypting keys to $a_i := e_i \oplus x_i$

[Broadbent 2016]

EPR Protocol

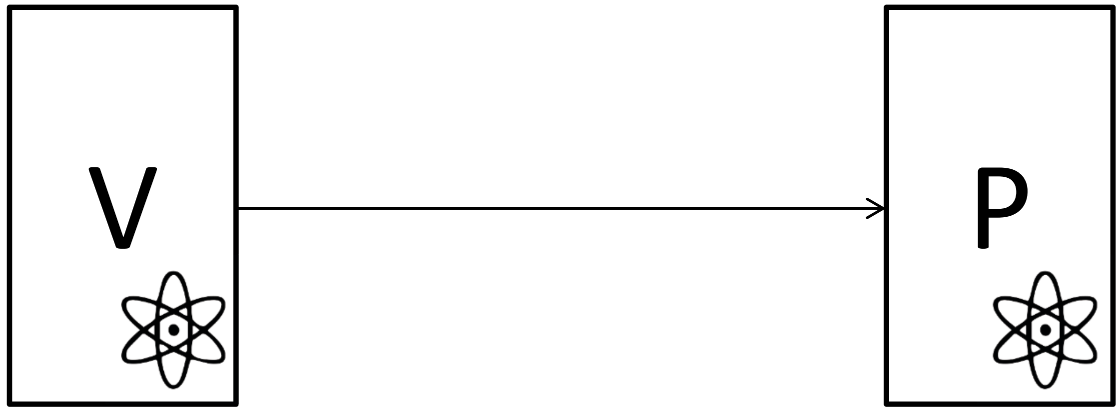


[Broadbent 2016]

EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$



- More generally, the state of a wire is:

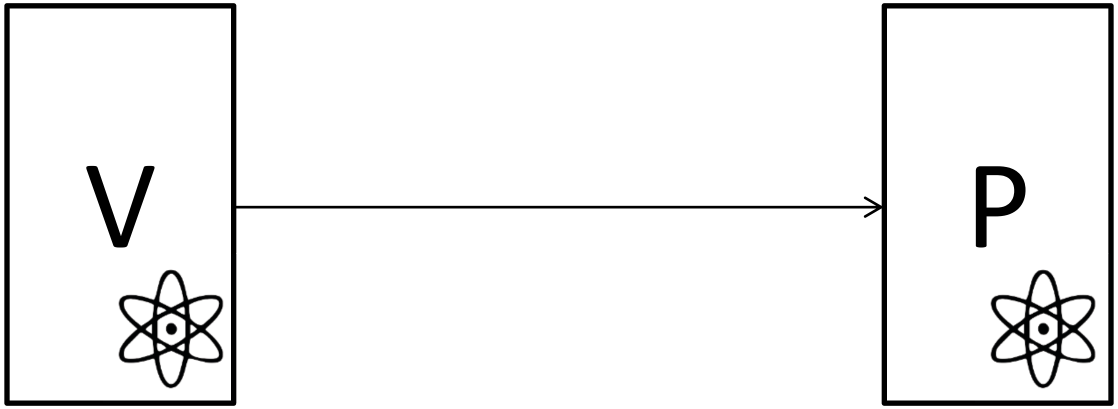
$$X^a Z^b \left|\psi\right\rangle, \quad a, b \in \{0,1\}$$

[Broadbent 2016]

EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$



- More generally, the state of a wire is:

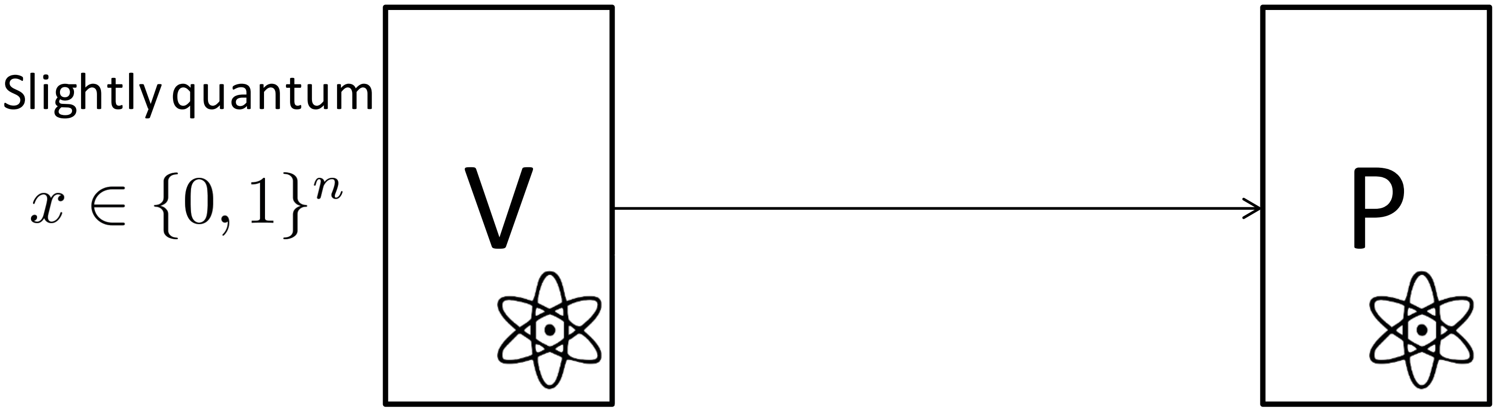
$$X^a Z^b \left|\psi\right\rangle, \quad a,b \in \{0,1\}$$

- For example, P applies Hadamard gate:

$$H X^a Z^b \left|\psi\right\rangle = X^b Z^a H \left|\psi\right\rangle$$

[Broadbent 2016]

EPR Protocol



- More generally, the state of a wire is:

$$X^a Z^b \left|\psi\right\rangle, \quad a, b \in \{0,1\}$$

- For example, P applies Hadamard gate:

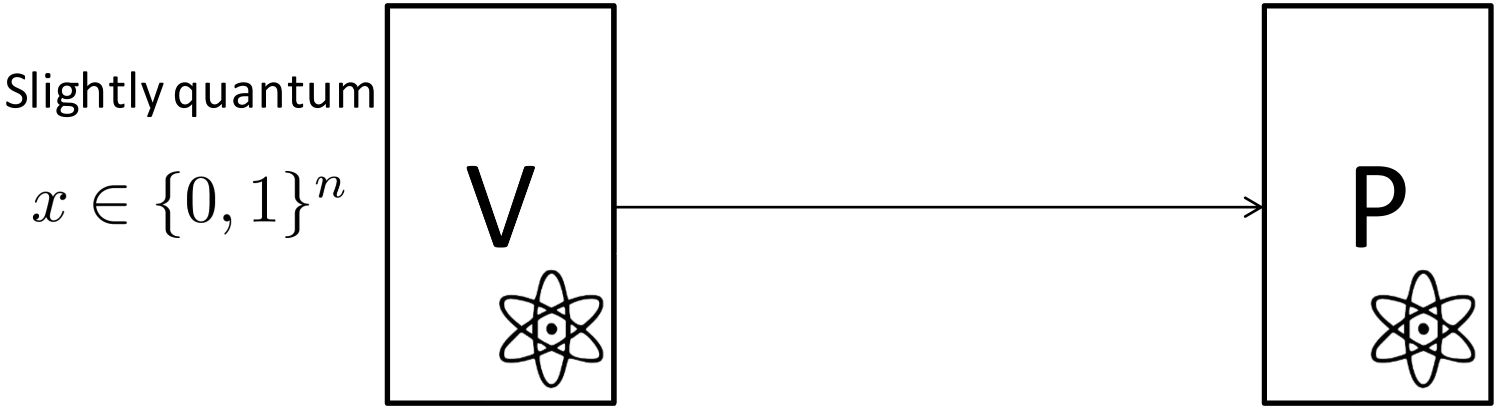
$$H X^a Z^b \left|\psi\right\rangle = X^b Z^a H \left|\psi\right\rangle$$

- V updates encrypting keys:

$$a' \leftarrow b, \quad b' \leftarrow a$$

[Broadbent 2016]

EPR Protocol

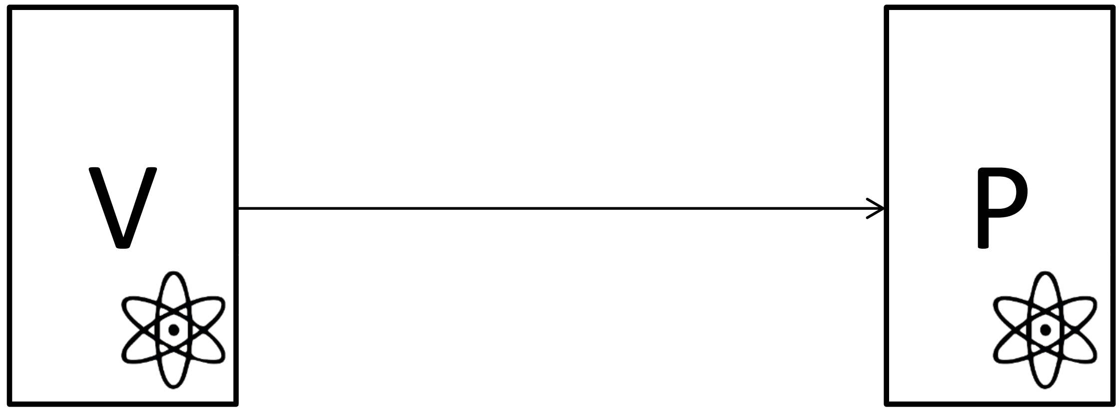


[Broadbent 2016]

EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$



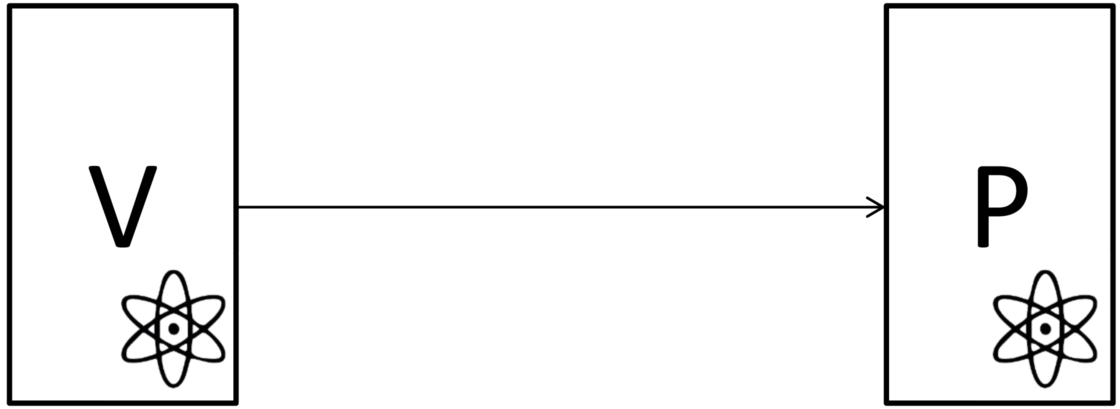
- Clifford gates (H, CNOT) are easy to implement!

[Broadbent 2016]

EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$

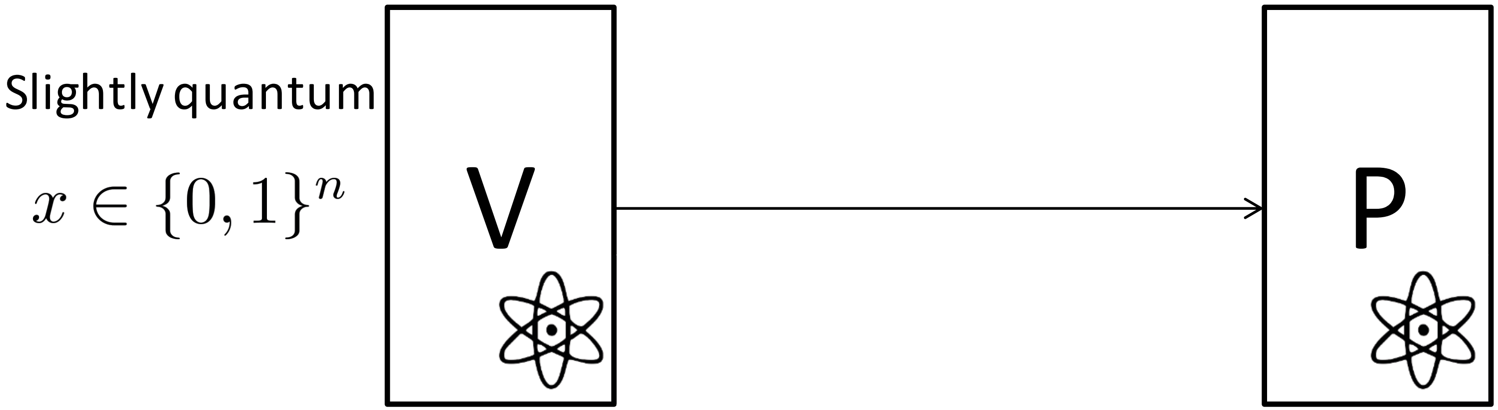


- Clifford gates (H, CNOT) are easy to implement!

- T-gates are more complicated to implement without revealing the encrypting keys:

[Broadbent 2016]

EPR Protocol



- Clifford gates (H, CNOT) are easy to implement!

- T-gates are more complicated to implement without revealing the encrypting keys:

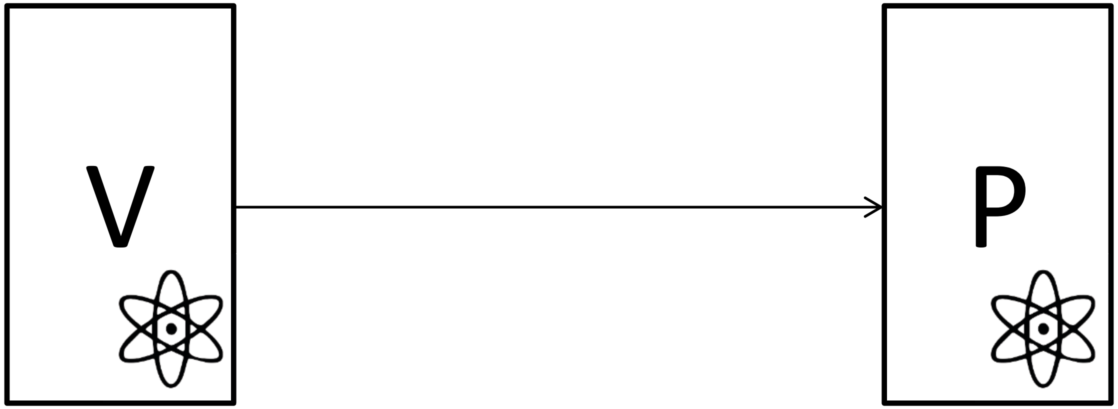
$$TX^aZ^b\left|\psi\right\rangle = X^aZ^{a\oplus b}\left(P^aT\left|\psi\right\rangle\right)$$

[Broadbent 2016]

EPR Protocol

Slightly quantum

$x \in \{0,1\}^n$



- Clifford gates (H, CNOT) are easy to implement!

- T-gates are more complicated to implement without revealing the encrypting keys:

$$T X^a Z^b |\psi\rangle = X^a Z^{a \oplus b} (P^a T |\psi\rangle)$$

[Broadbent 2016]

EPR Protocol: T-gadget

[Broadbent 2016]

EPR Protocol: T-gadget

FACT: There exists a sub-protocol that implements a T-gate on an encrypted input, without revealing the encrypting keys.

[Broadbent 2016]

EPR Protocol: T-gadget

FACT: There exists a sub-protocol that implements a T-gate on an encrypted input, without revealing the encrypting keys.

- We call this sub-protocol a T-gadget.
- The verifier can implement it by measuring products of single-qubit Clifford observables

[Broadbent 2016]

EPR Protocol: T-gadget

FACT: There exists a sub-protocol that implements a T-gate on an encrypted input, without revealing the encrypting keys.

- We call this sub-protocol a T-gadget.
- The verifier can implement it by measuring products of single-qubit Clifford observables

What about verifiability?

[Broadbent 2016]

EPR Protocol: T-gadget

FACT: There exists a sub-protocol that implements a T-gate on an encrypted input, without revealing the encrypting keys.

- We call this sub-protocol a T-gadget.
- The verifier can implement it by measuring products of single-qubit Clifford observables

What about verifiability?

Verifier randomly chooses between a computation run and test runs.

[Broadbent 2016]

EPR Protocol: T-gadget

FACT: There exists a sub-protocol that implements a T-gate on an encrypted input, without revealing the encrypting keys.

- We call this sub-protocol a T-gadget.
- The verifier can implement it by measuring products of single-qubit Clifford observables

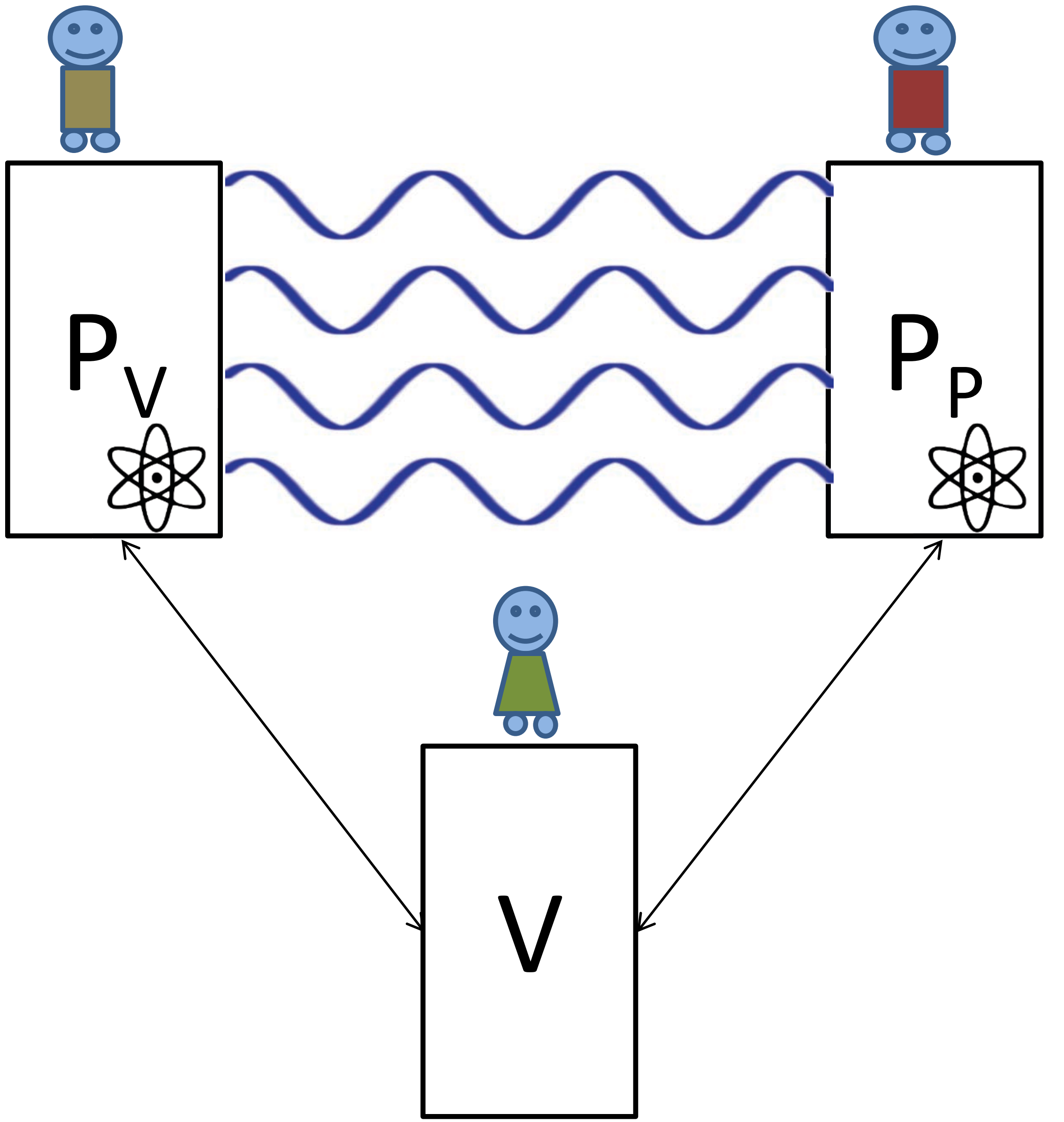
What about verifiability?

Verifier randomly chooses between a computation run and test runs.

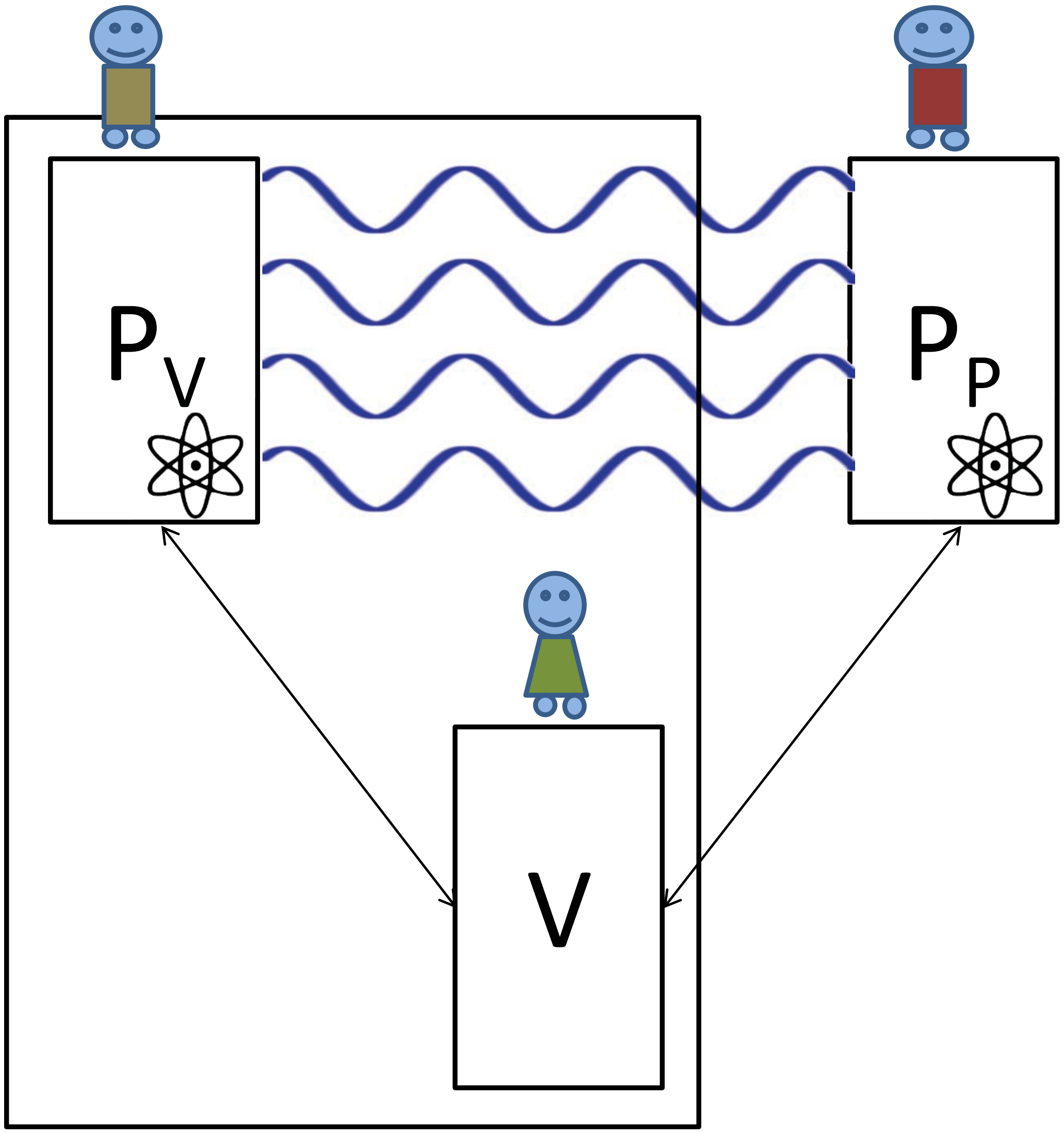
Test runs are indistinguishable from computation runs from the Prover's perspective!
But the verifier's input is fixed, and she expects deterministic replies.

[Broadbent 2016]

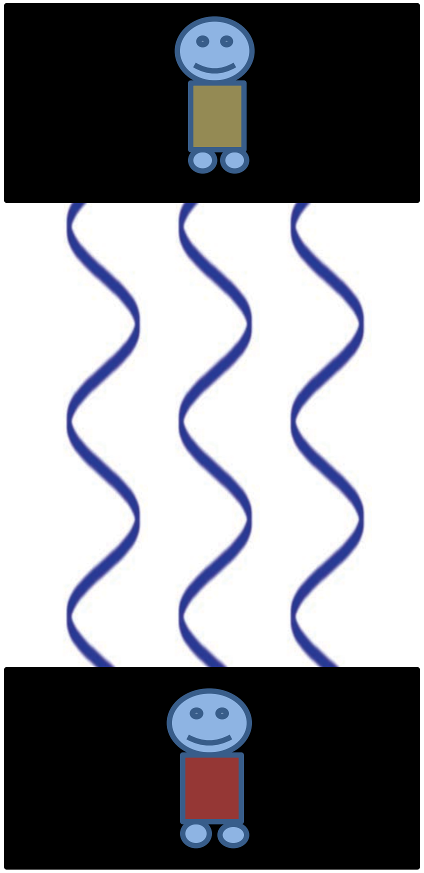
Putting the Verifier on a Leash



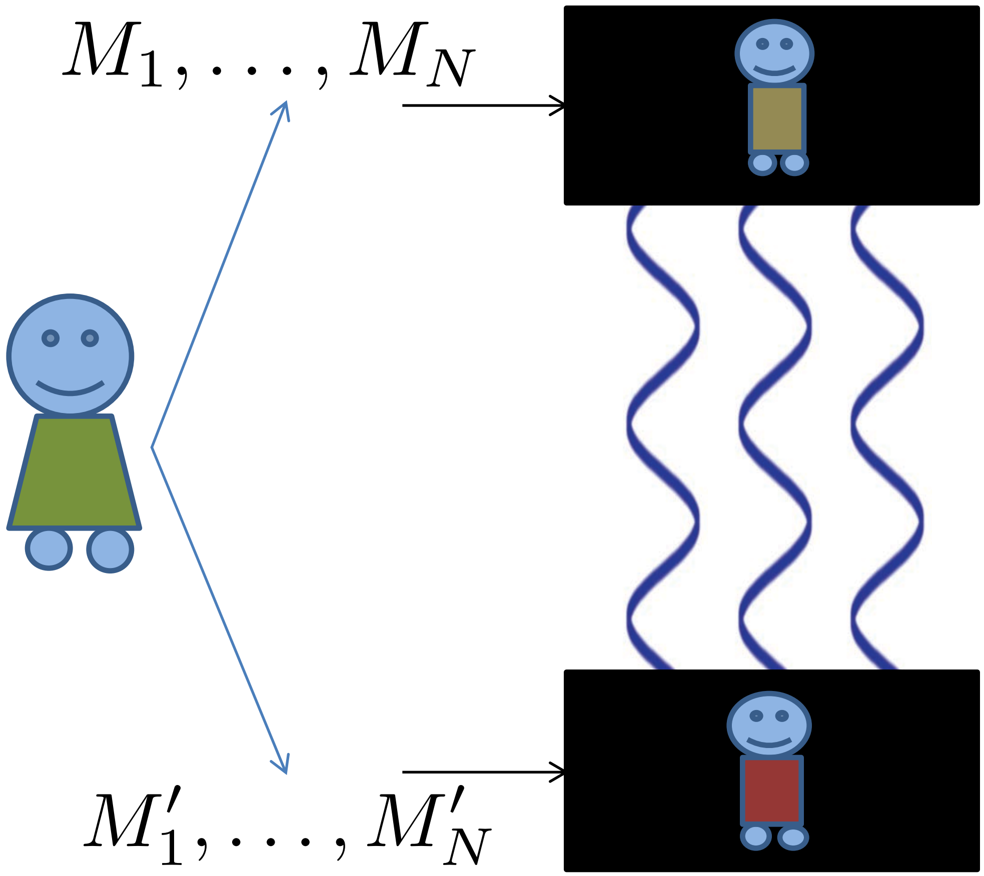
P_V
P_P
V


P_V
P_P
V

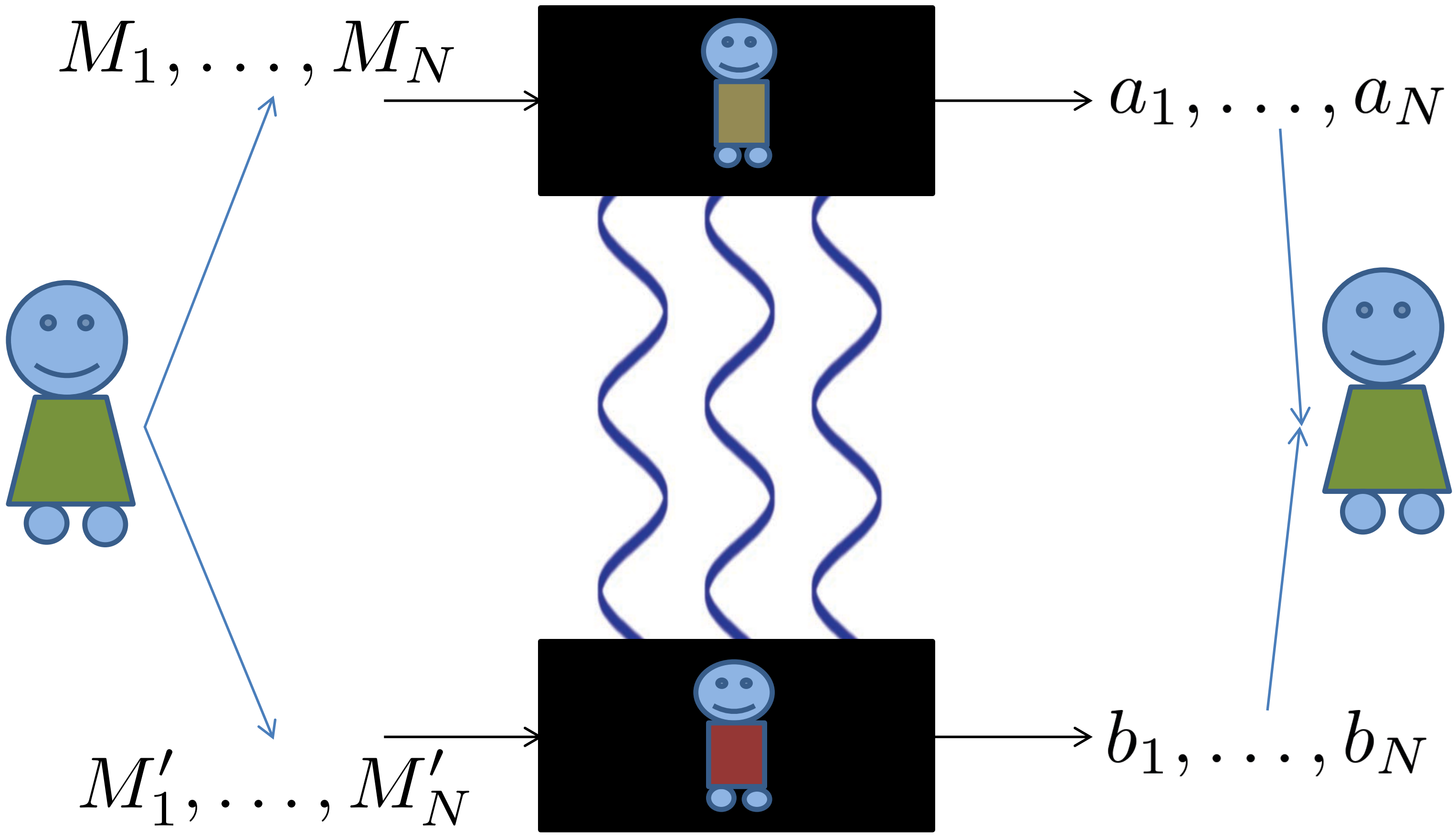
Rigidity Game



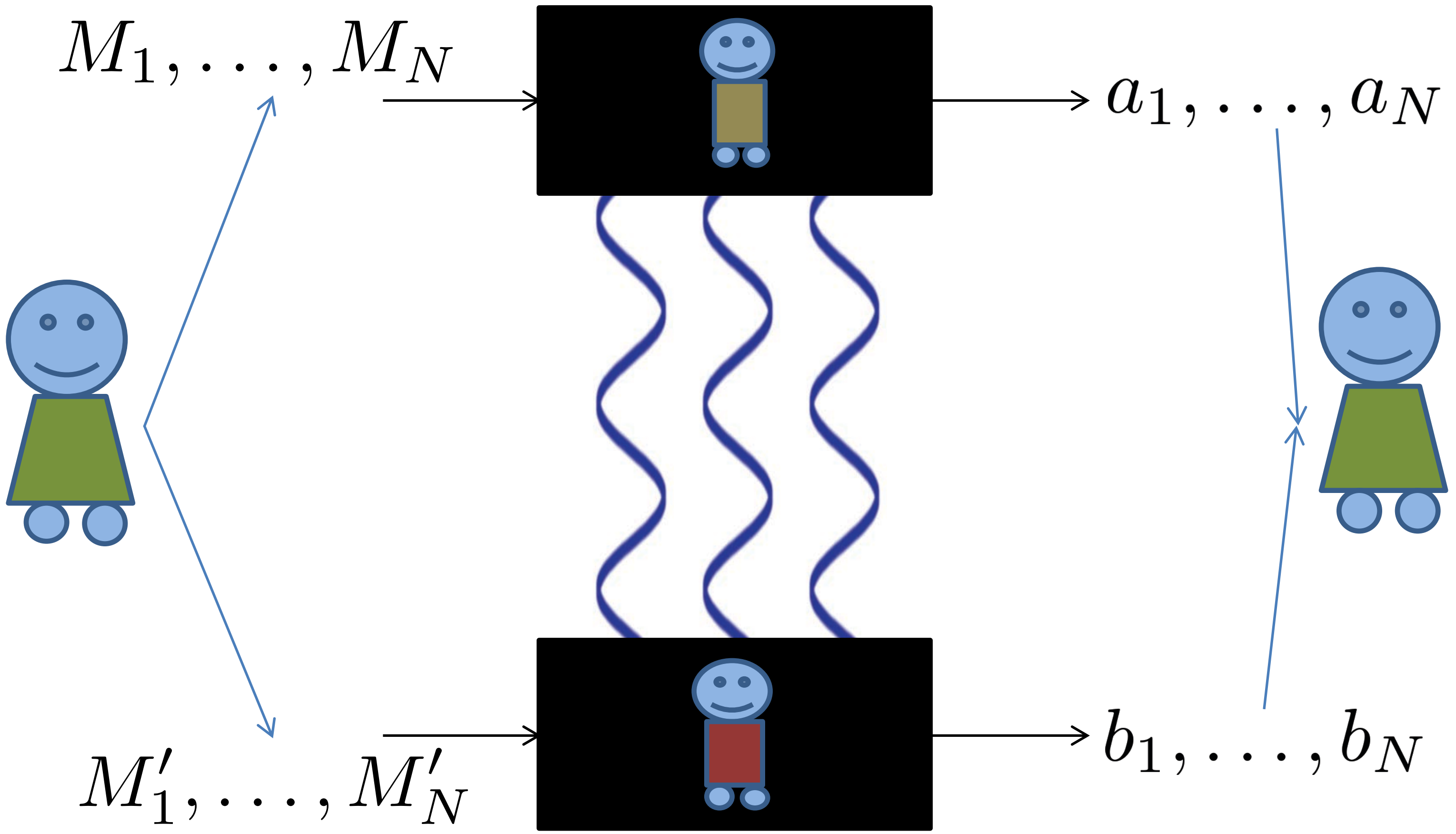
Rigidity Game



Rigidity Game

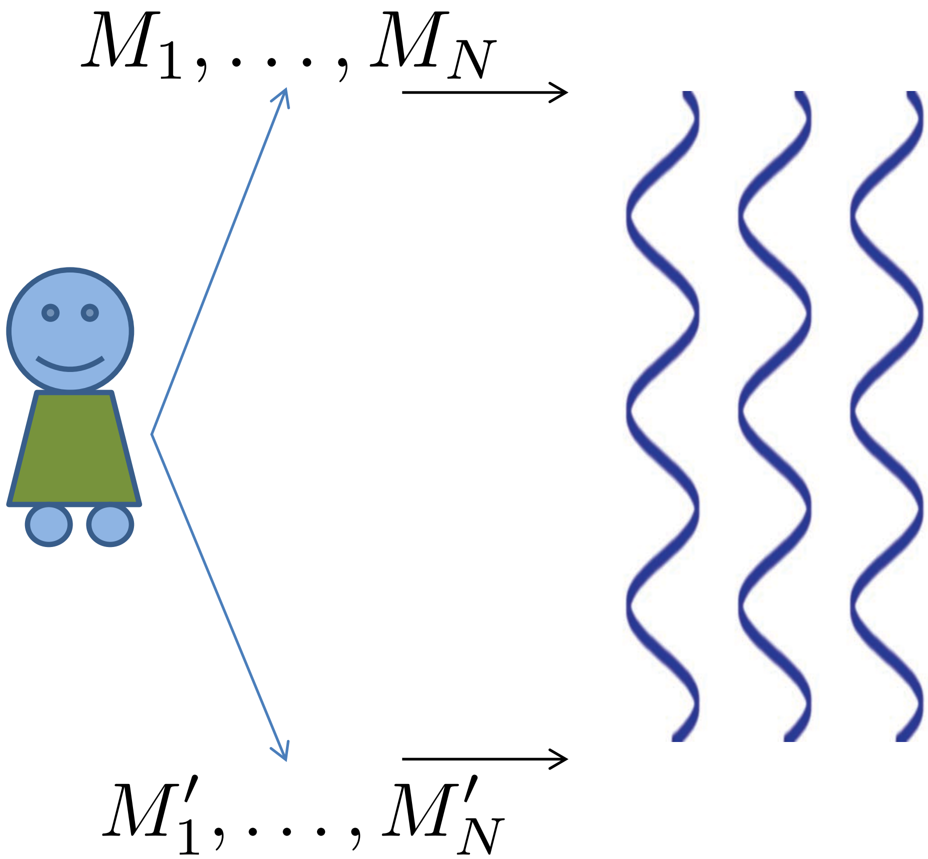


Rigidity Game

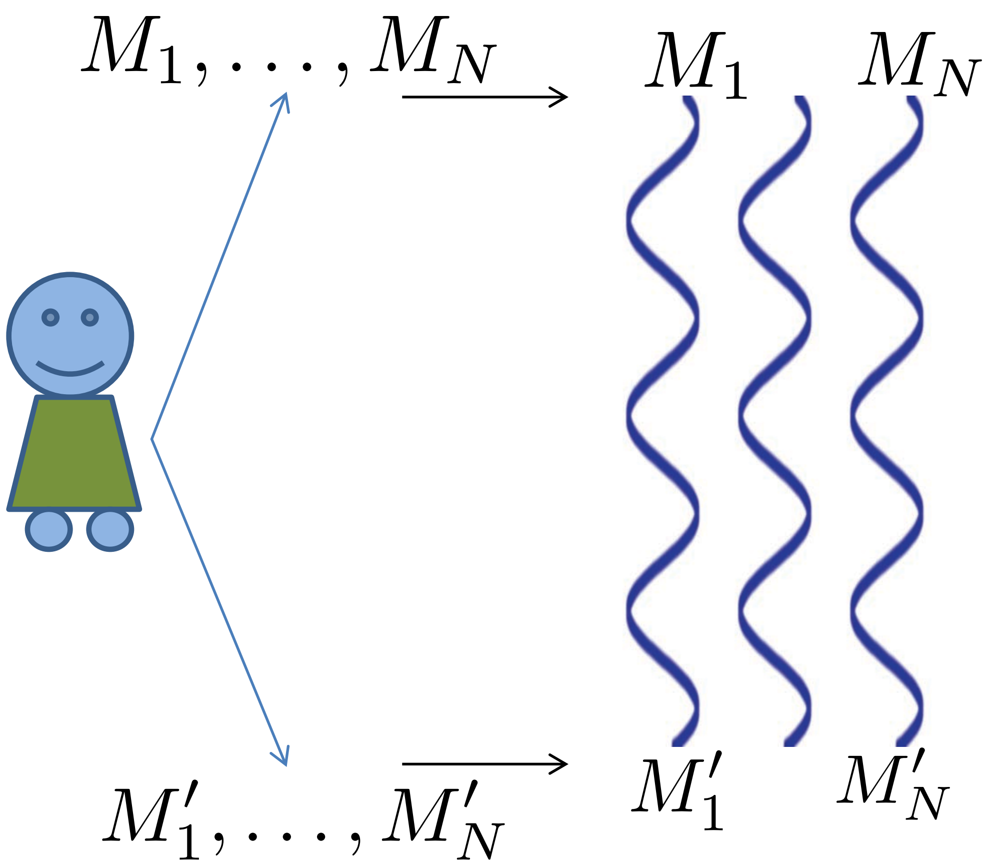


Provers win if $(\{M_i\}, \{M'_i\}, a, b) \in S_{\text{rigid}}$

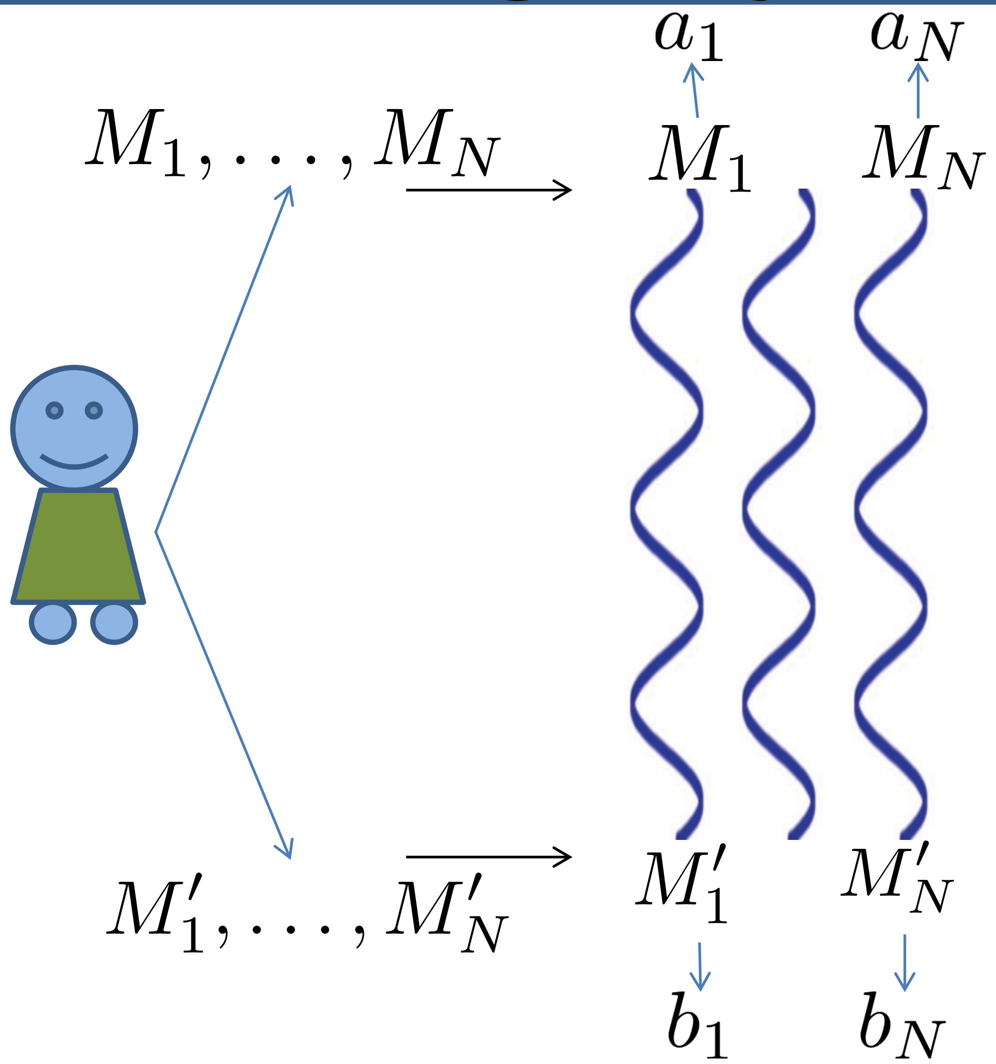
Rigidity Game



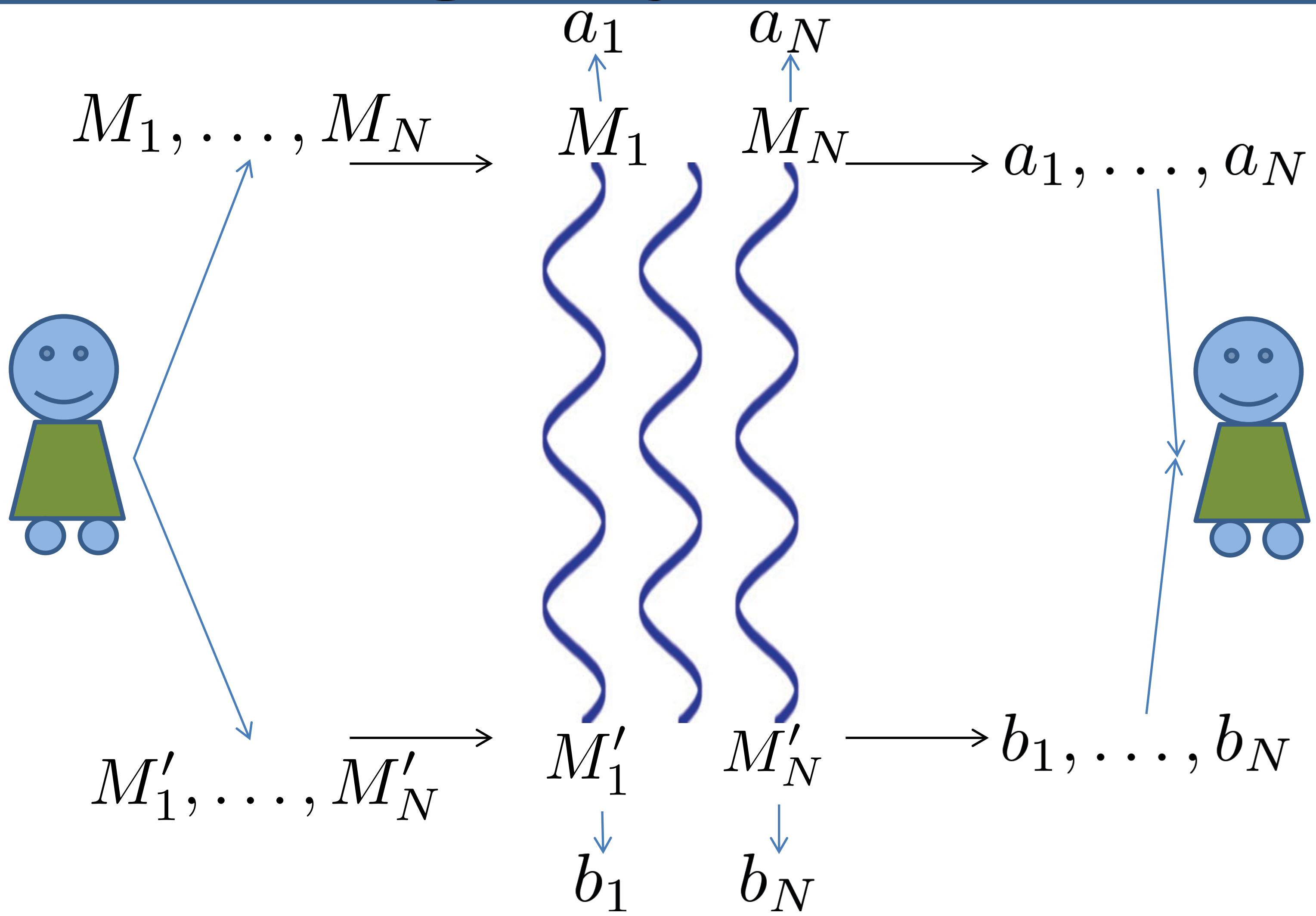
Rigidity Game



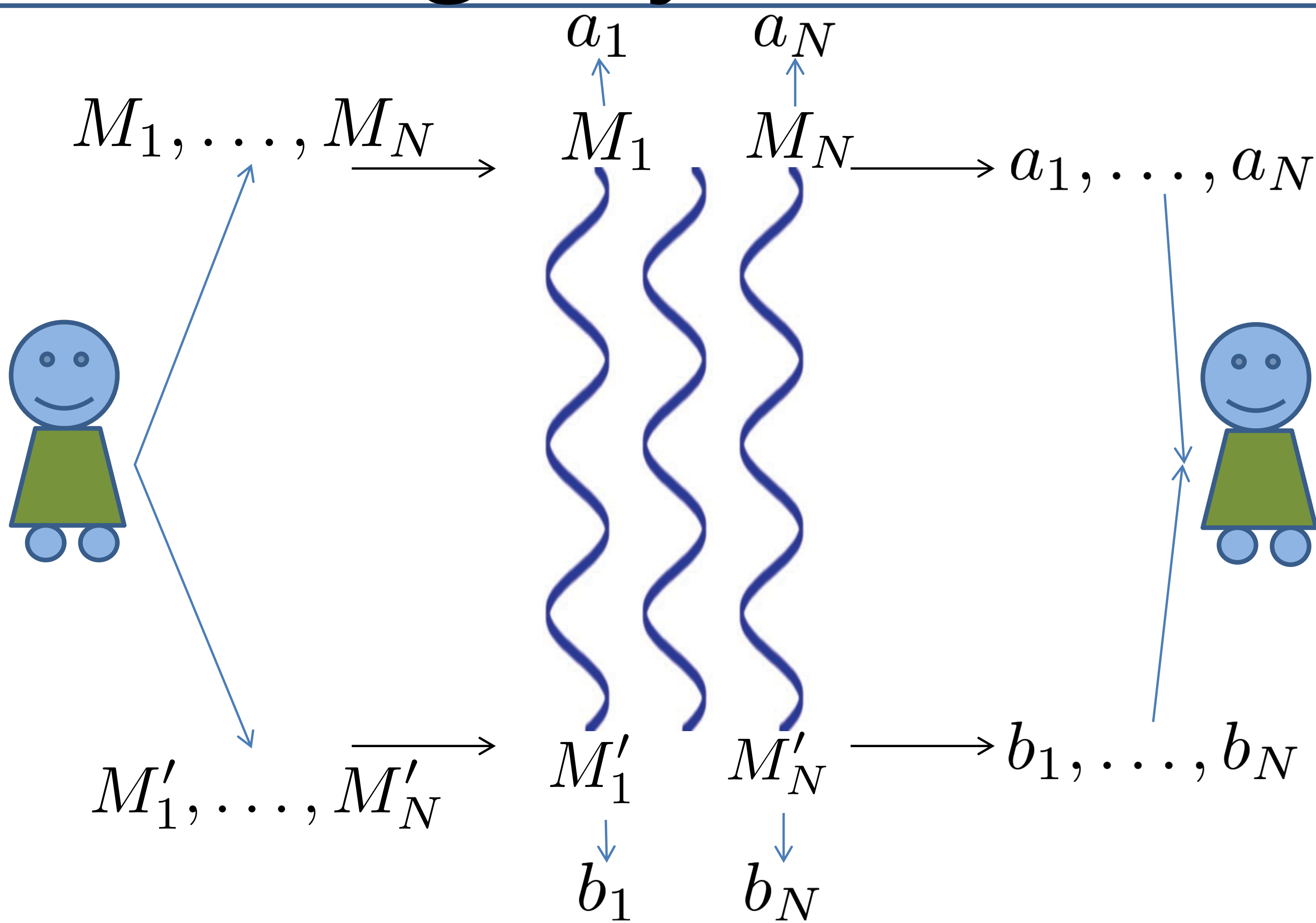
Rigidity Game



Rigidity Game



Rigidity Game



Completeness: Honest Alice and Bob win with probability 1.

Rigidity Game

Completeness: Honest Alice and Bob win with probability 1.

Soundness: If Alice and Bob win with probability $1-\epsilon$, their strategy must be within $O(\epsilon^c)$ of the honest strategy.

Rigidity Game

Completeness: Honest Alice and Bob win with probability 1.

Soundness: If Alice and Bob win with probability $1 - \epsilon$, their strategy must be within $O(\epsilon^c)$ of the honest strategy.

Features:

- Can test that provers measure any product of single-qubit Clifford observables.
- Robustness independent of number of EPR pairs tested.

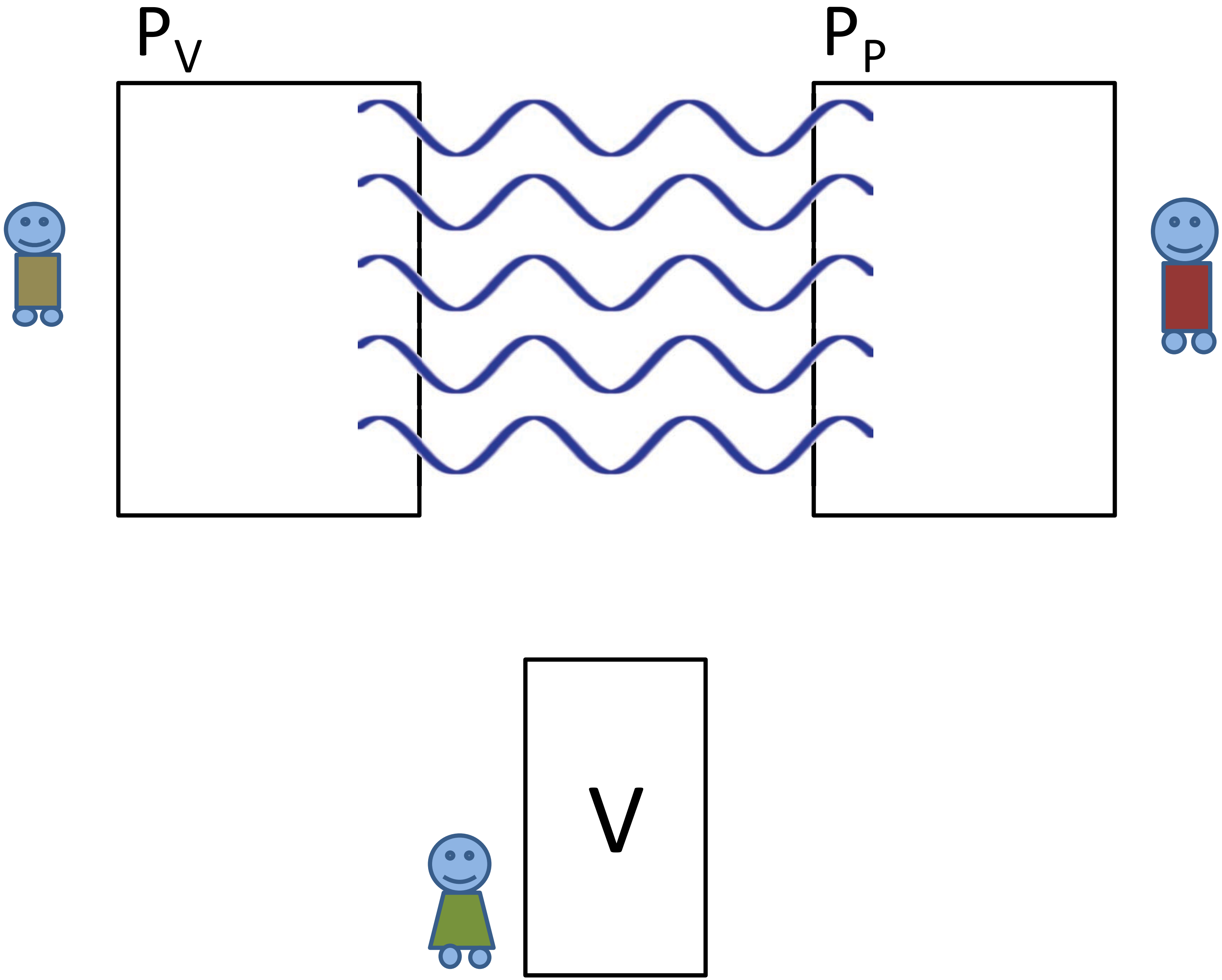
Rigidity Game

Completeness: Honest Alice and Bob win with probability 1.

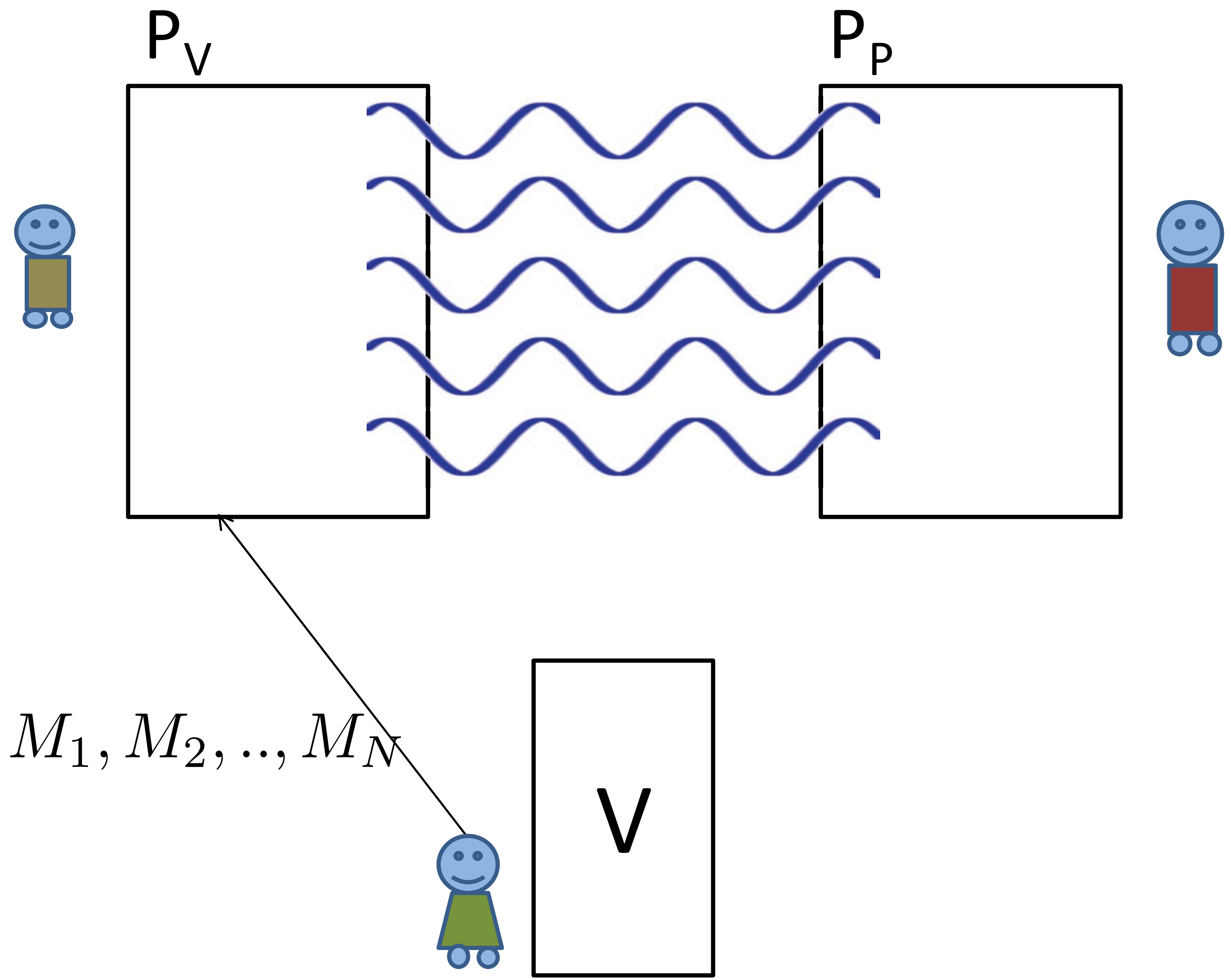
Soundness: If Alice and Bob win with probability $1 - \epsilon$, their strategy must be within $O(\epsilon^c)$ of the honest strategy.

Features:

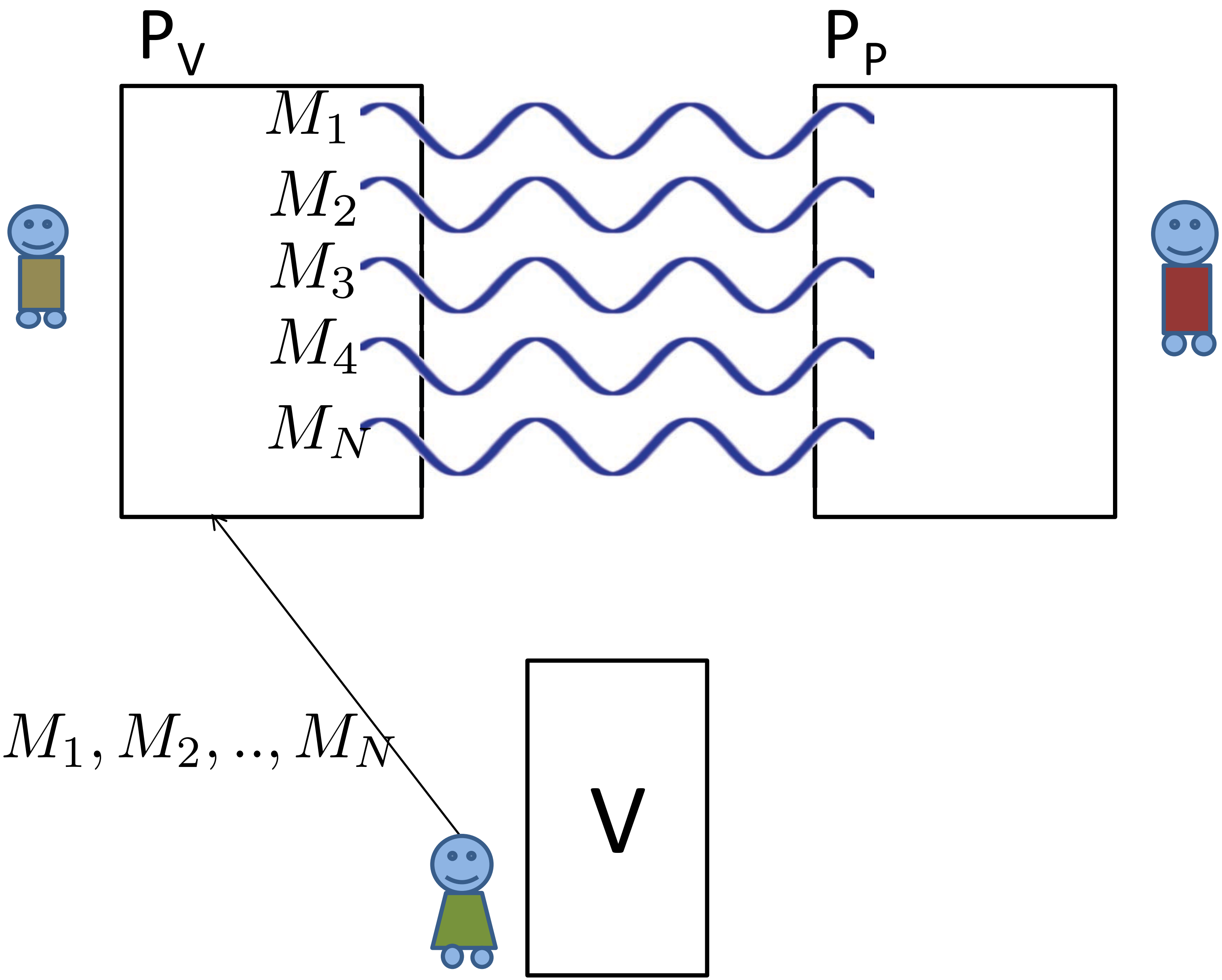
- Can test that provers measure any product of single-qubit Clifford observables.
- Robustness independent of number of EPR pairs tested. ([Natarajan, Vidick 2016] tests for Pauli X and Z measurements)



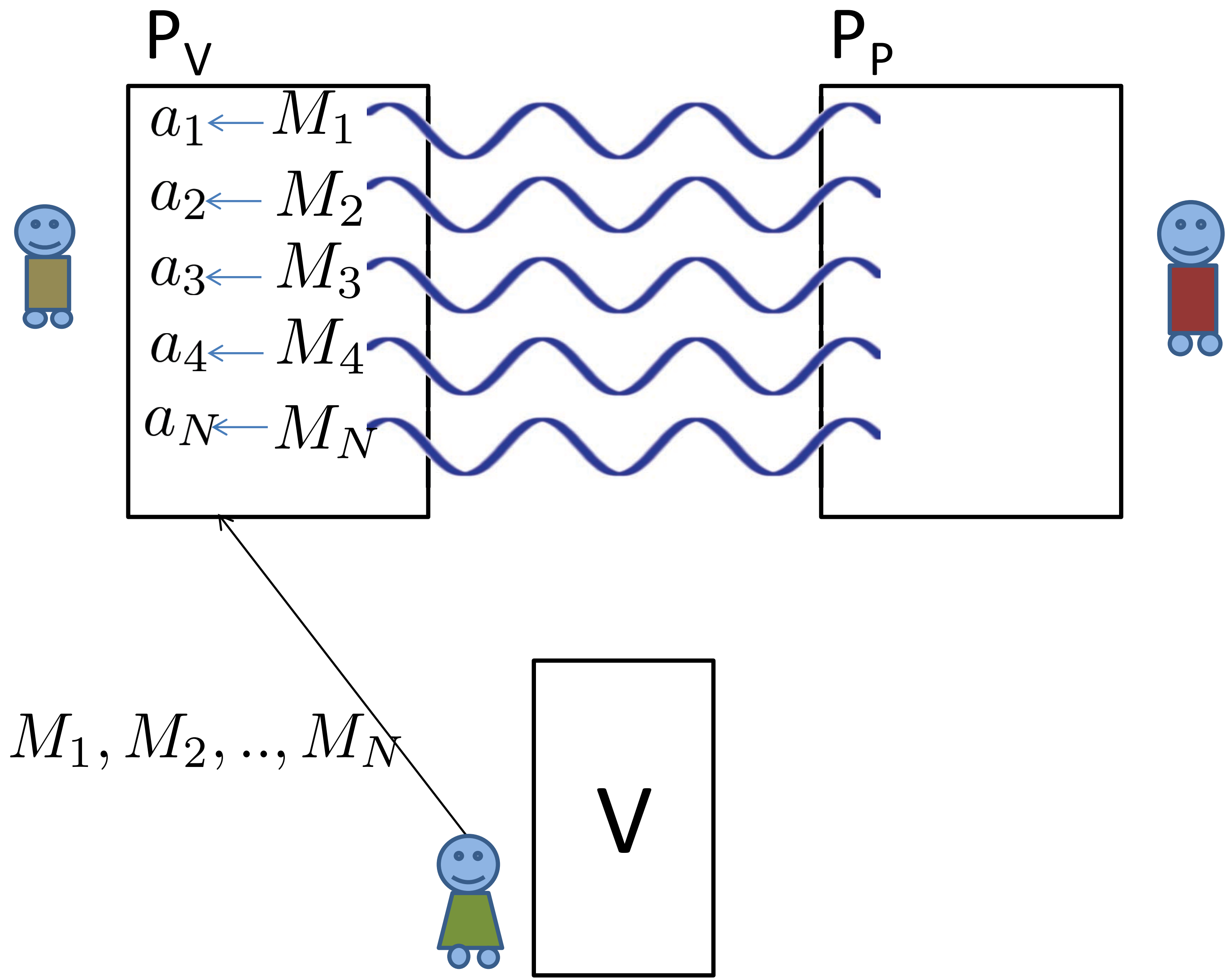
P_V
P_P
V



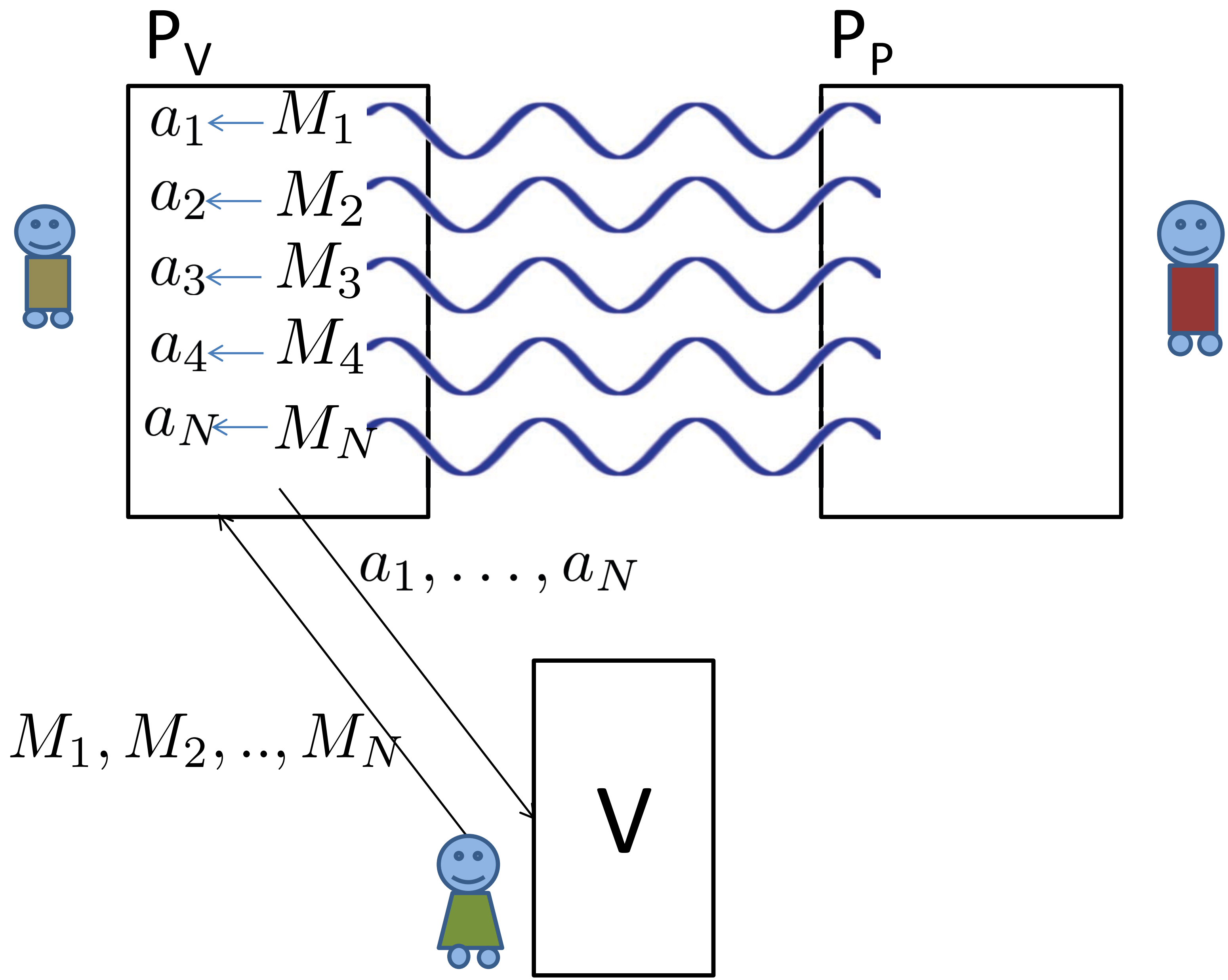
P_V
P_P
$M_1, M_2, .., M_N$
V



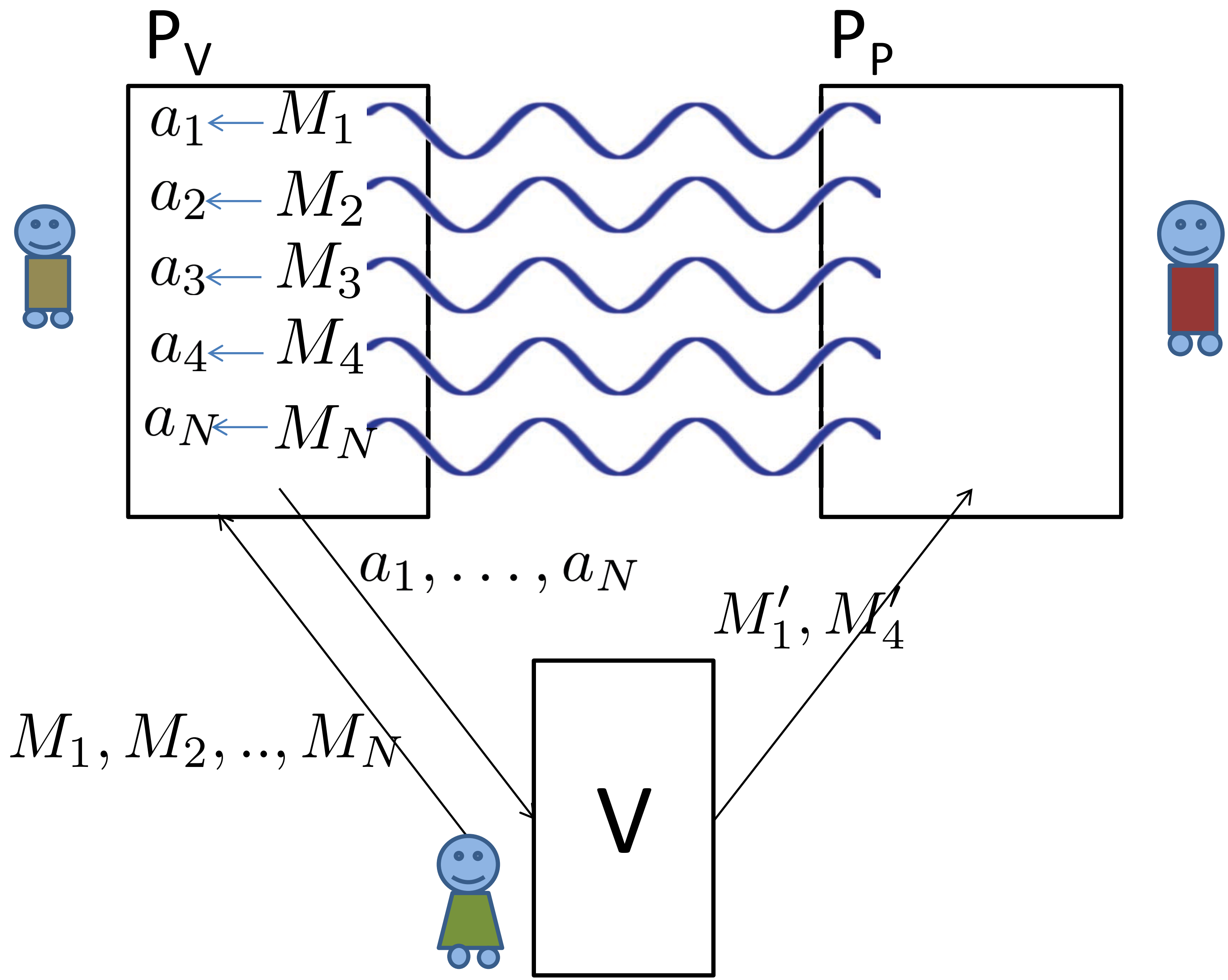
P_V
P_P
M_1
M_2
M_3
M_4
M_N
$M_1, M_2, .., M_N$
V



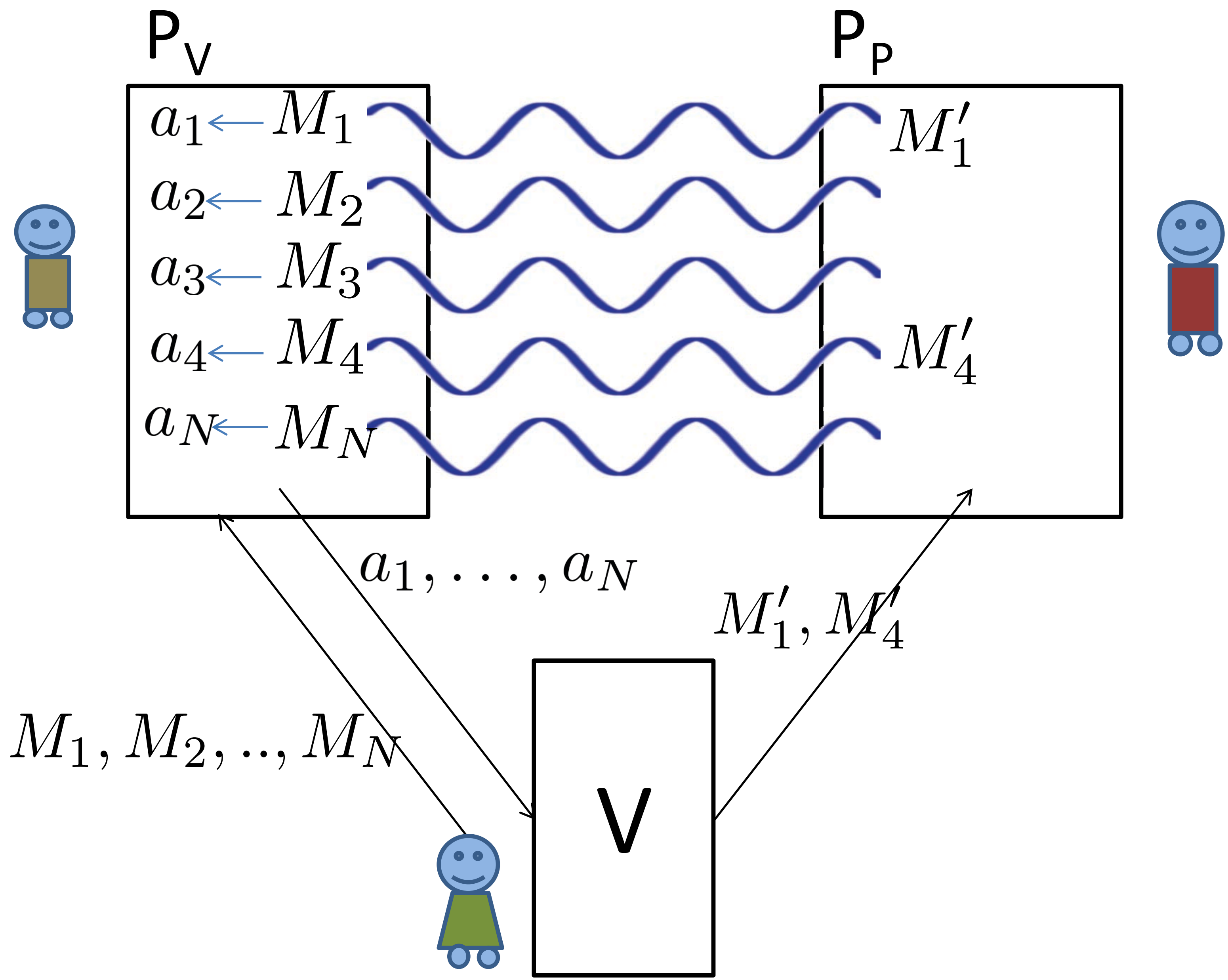
P_V
P_P
$a_1 \leftarrow M_1$
$a_2 \leftarrow M_2$
$a_3 \leftarrow M_3$
$a_4 \leftarrow M_4$
$a_N \leftarrow M_N$
$M_1, M_2, .., M_N$
V



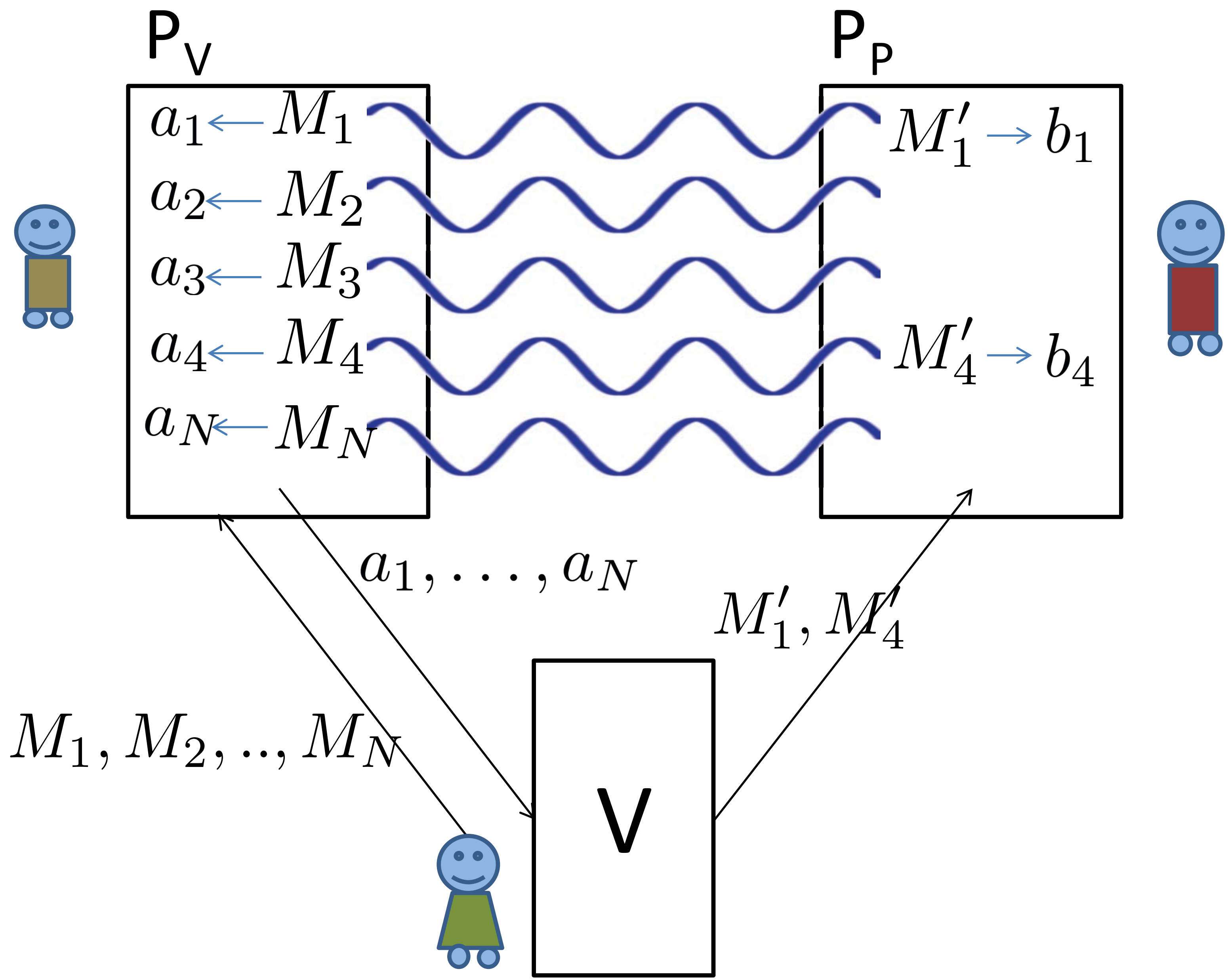
P_V
P_P
a_1 M_1
a_2 M_2
a_3 M_3
a_4 M_4
a_N M_N
$a_1, \ldots, a_N$
$M_1, M_2, .., M_N$
V



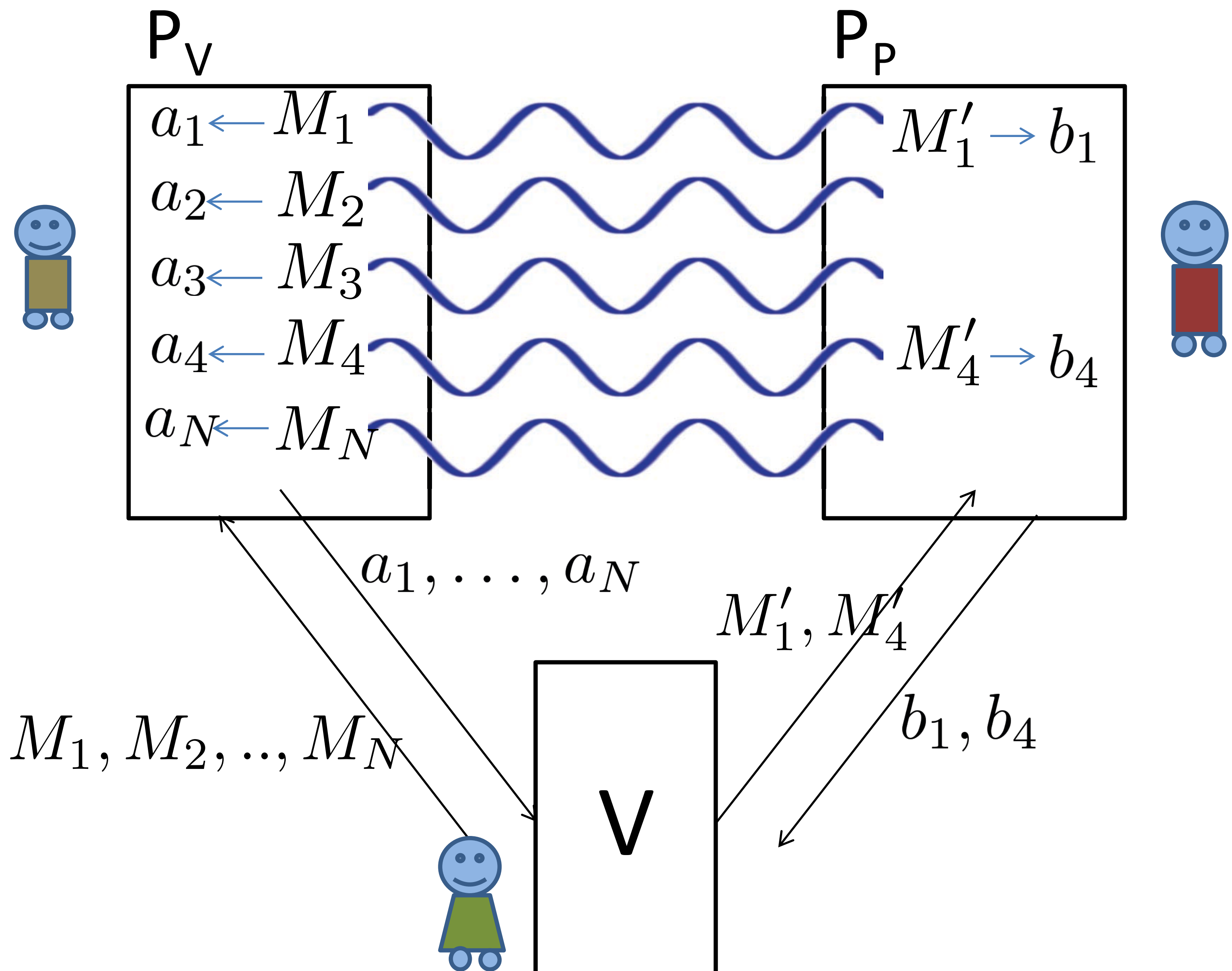
P_V
P_P
a_1 M_1
a_2 M_2
a_3 M_3
a_4 M_4
a_N M_N
$a_1, \ldots, a_N$
M'_1, M'_4
$M_1, M_2, .., M_N$
V



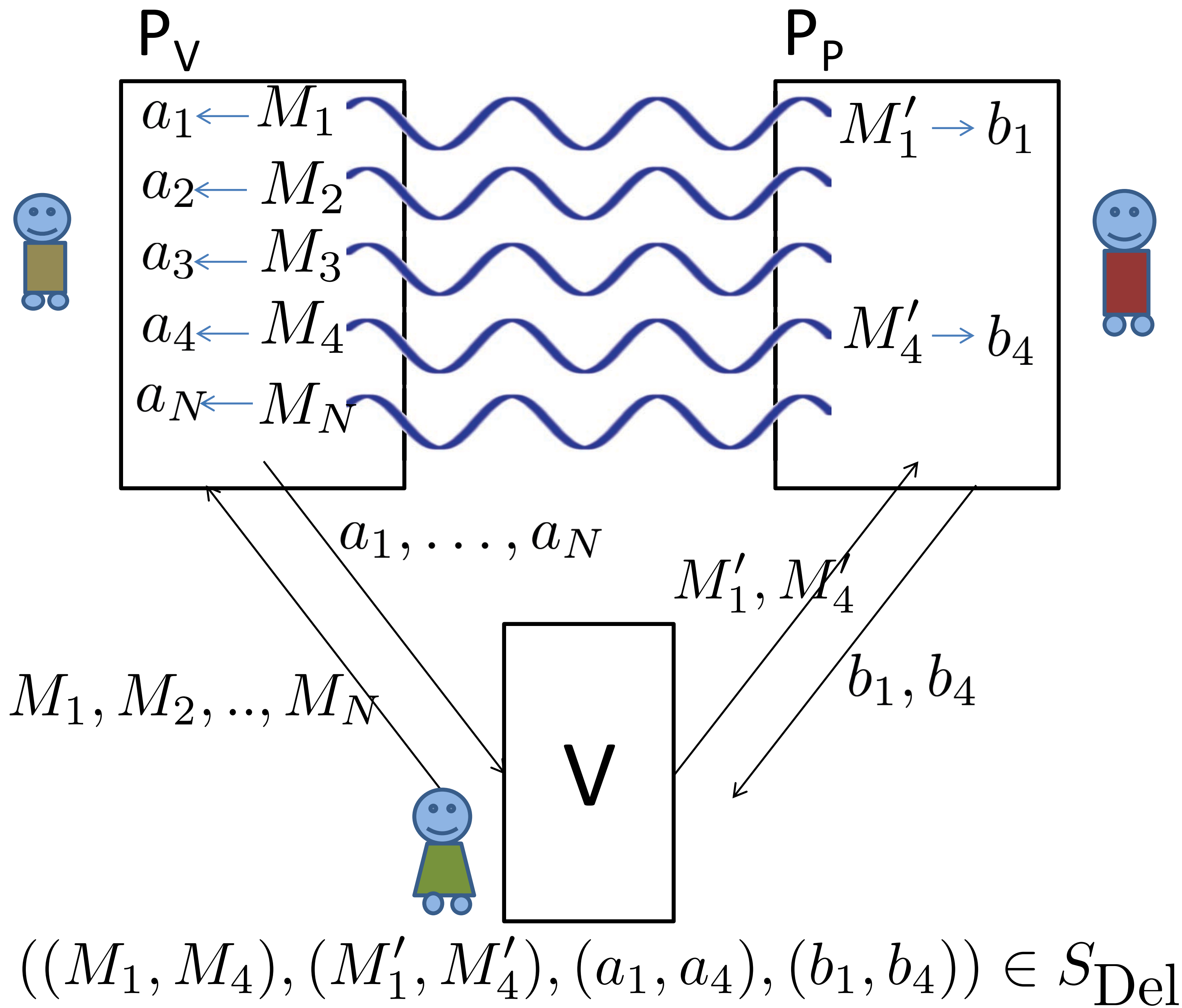
P_V
P_P
$a_1 \leftarrow M_1$
$a_2 \leftarrow M_2$
$a_3 \leftarrow M_3$
$a_4 \leftarrow M_4$
$a_N \leftarrow M_N$
M'_1
M'_4
$a_1, \ldots, a_N$
M'_1, M'_4
$M_1, M_2, .., M_N$
V



P_V
P_P
$a_1 \leftarrow M_1$
$a_2 \leftarrow M_2$
$a_3 \leftarrow M_3$
$a_4 \leftarrow M_4$
$a_N \leftarrow M_N$
$M'_1 \rightarrow b_1$
$M'_4 \rightarrow b_4$
$a_1, \ldots, a_N$
M'_1, M'_4
$M_1, M_2, .., M_N$
V



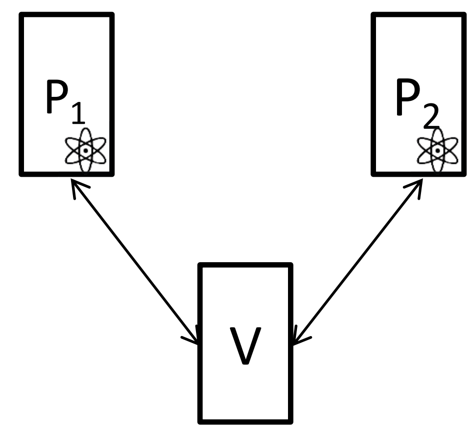
P_V
P_P
$a_1 \leftarrow M_1$
$a_2 \leftarrow M_2$
$a_3 \leftarrow M_3$
$a_4 \leftarrow M_4$
$a_N \leftarrow M_N$
$M_1' \rightarrow b_1$
$M_4' \rightarrow b_4$
$a_1, \ldots, a_N$
M_1', M_4'
b_1, b_4
$M_1, M_2, .., M_N$
V



P_V
P_P
$a_1 \leftarrow M_1$
$a_2 \leftarrow M_2$
$a_3 \leftarrow M_3$
$a_4 \leftarrow M_4$
$a_N \leftarrow M_N$
$M'_1 \rightarrow b_1$
$M'_4 \rightarrow b_4$
$a_1, \ldots, a_N$
M'_1, M'_4
b_1, b_4
$M_1, M_2, .., M_N$
V
$((M_1, M_4), (M'_1, M'_4), (a_1, a_4), (b_1, b_4)) \in S_{\mathrm{Del}}$

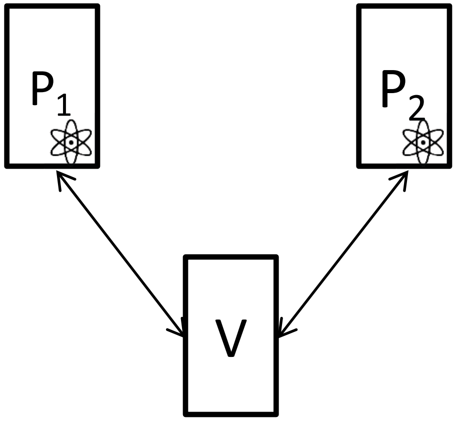
Verifier on a Leash Protocol

- Classical verifier, two quantum provers
- Total complexity: $O(m \log m)$
- Round complexity: $O(T\text{-depth})$



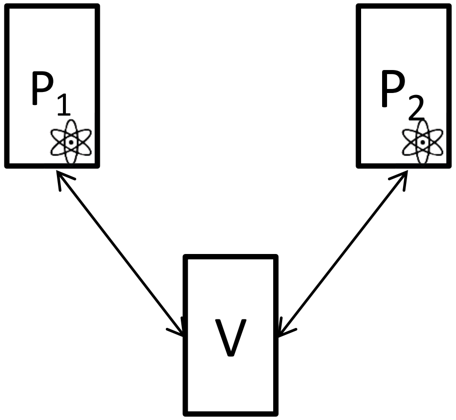
Verifier on a Leash Protocol

- Classical verifier, two quantum provers
- Total complexity: $O(m \log m)$
- Round complexity: $O(T\text{-depth})$
- Encrypted input



Dog-Walker Protocol

- Classical verifier, two quantum provers
- Total complexity: $O(m \log m)$
- Round complexity: $O(1)$
- Input is known to P_V

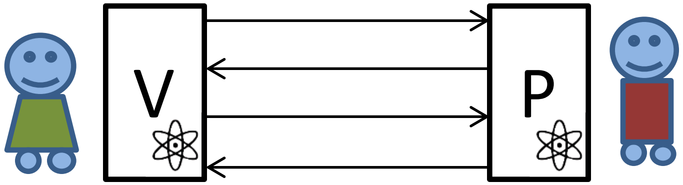


Summary

Summary

Previously:

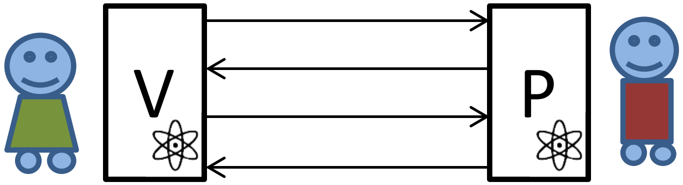
- $O(m)$ protocol for slightly-quantum verifier to delegate m-gate circuit to quantum prover



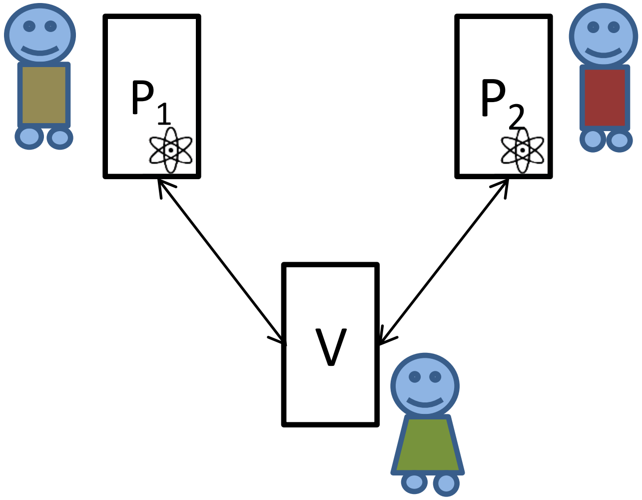
Summary

Previously:

- $O(m)$ protocol for slightly-quantum verifier to delegate m-gate circuit to quantum prover



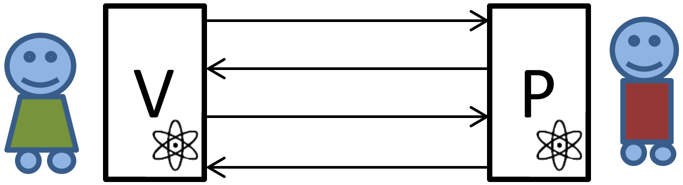
- from $O(m^4)$ to $O(m^{8192})$ protocols for classical verifier to delegate m-gate circuit to two quantum provers



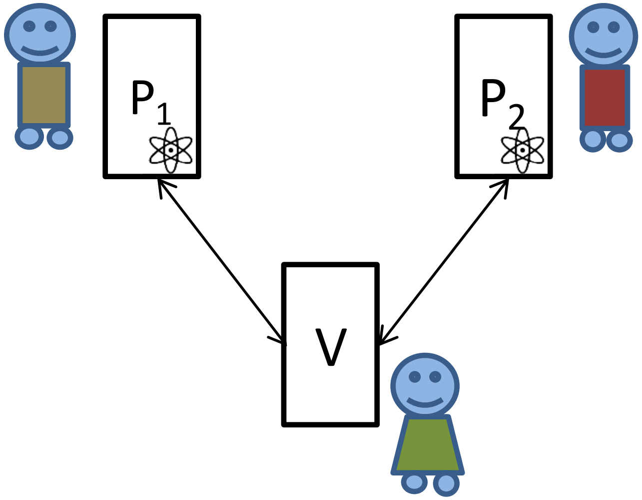
Summary

Previously:

- $O(m)$ protocol for slightly-quantum verifier to delegate m-gate circuit to quantum prover



- from $O(m^4)$ to $O(m^{8192})$ protocols for classical verifier to delegate m-gate circuit to two quantum provers

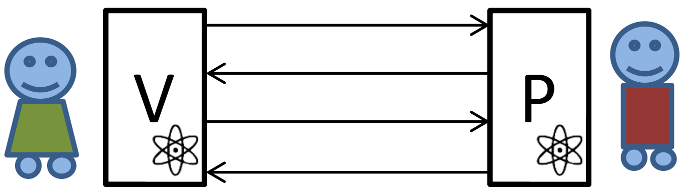


New:

Summary

Previously:

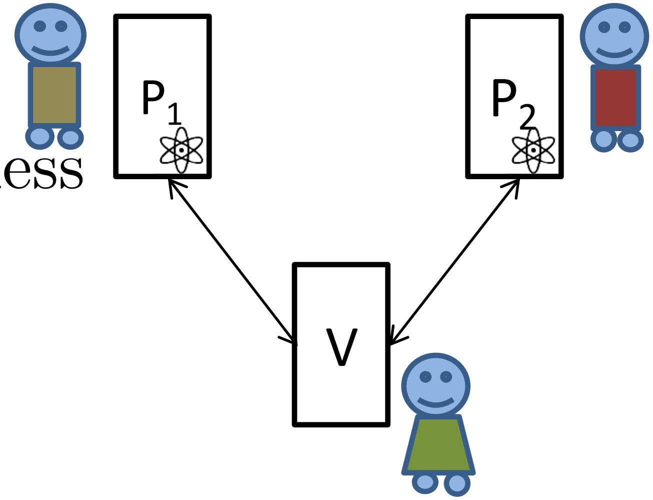
- $O(m)$ protocol for slightly-quantum verifier to delegate m-gate circuit to quantum prover



- from $O(m^4)$ to $O(m^{8192})$ protocols for classical verifier to delegate m-gate circuit to two quantum provers

New:

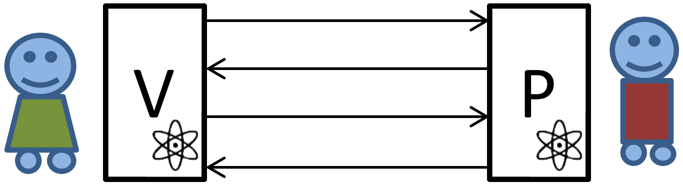
- new rigidity theorems with robustness independent of number of EPR pairs tested.



Summary

Previously:

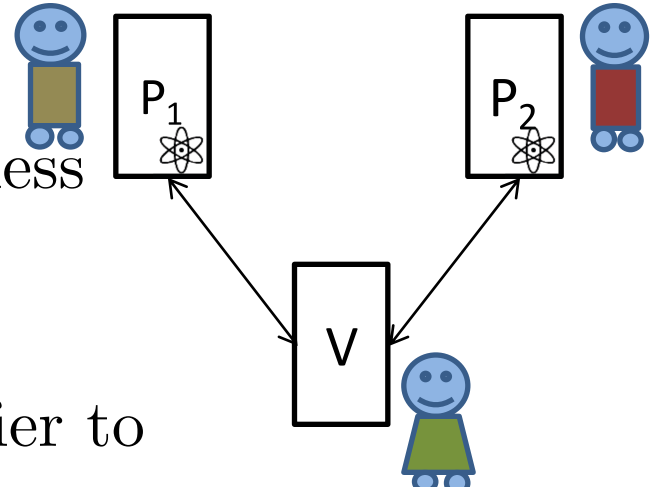
- $O(m)$ protocol for slightly-quantum verifier to delegate m-gate circuit to quantum prover



- from $O(m^4)$ to $O(m^{8192})$ protocols for classical verifier to delegate m-gate circuit to two quantum provers

New:

- new rigidity theorems with robustness independent of number of EPR pairs tested.
- $O(m \log m)$ protocols for classical verifier to delegate m-gate circuit to two quantum provers.



Open Questions

- Avoiding the non-communication assumption (while keeping the client classical)?

Open Questions

- Avoiding the non-communication assumption (while keeping the client classical)?

  - Single-Round Protocols: [Grilo 2017]

Open Questions

- Avoiding the non-communication assumption (while keeping the client classical)?

  - Single-Round Protocols: [Grilo 2017]

  - Single-server Protocols (with classical client): [Mahadev 2017]

Open Questions

- Avoiding the non-communication assumption (while keeping the client classical)?

  - Single-Round Protocols: [Grilo 2017]

  - Single-server Protocols (with classical client): [Mahadev 2017]

- Noise tolerance?

Open Questions

- Avoiding the non-communication assumption (while keeping the client classical)?

  - Single-Round Protocols: [Grilo 2017]

  - Single-server Protocols (with classical client): [Mahadev 2017]

- Noise tolerance?
  - [Arnon-Friedman, Yuen 2017]