Position-Based Cryptography

connecting space, time, and information

Speaker: Zikuan Huang

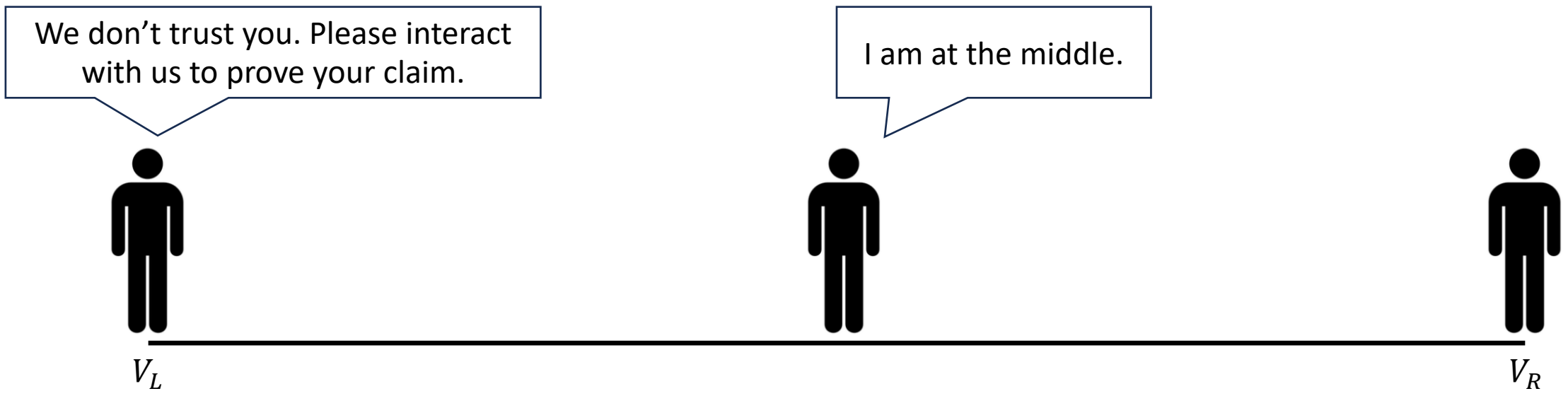
Before we start

- I am a PhD student supervised by Prof. Tom Gur.
- I do quantum cryptography & quantum complexity.
- Interrupt me if you have any question.

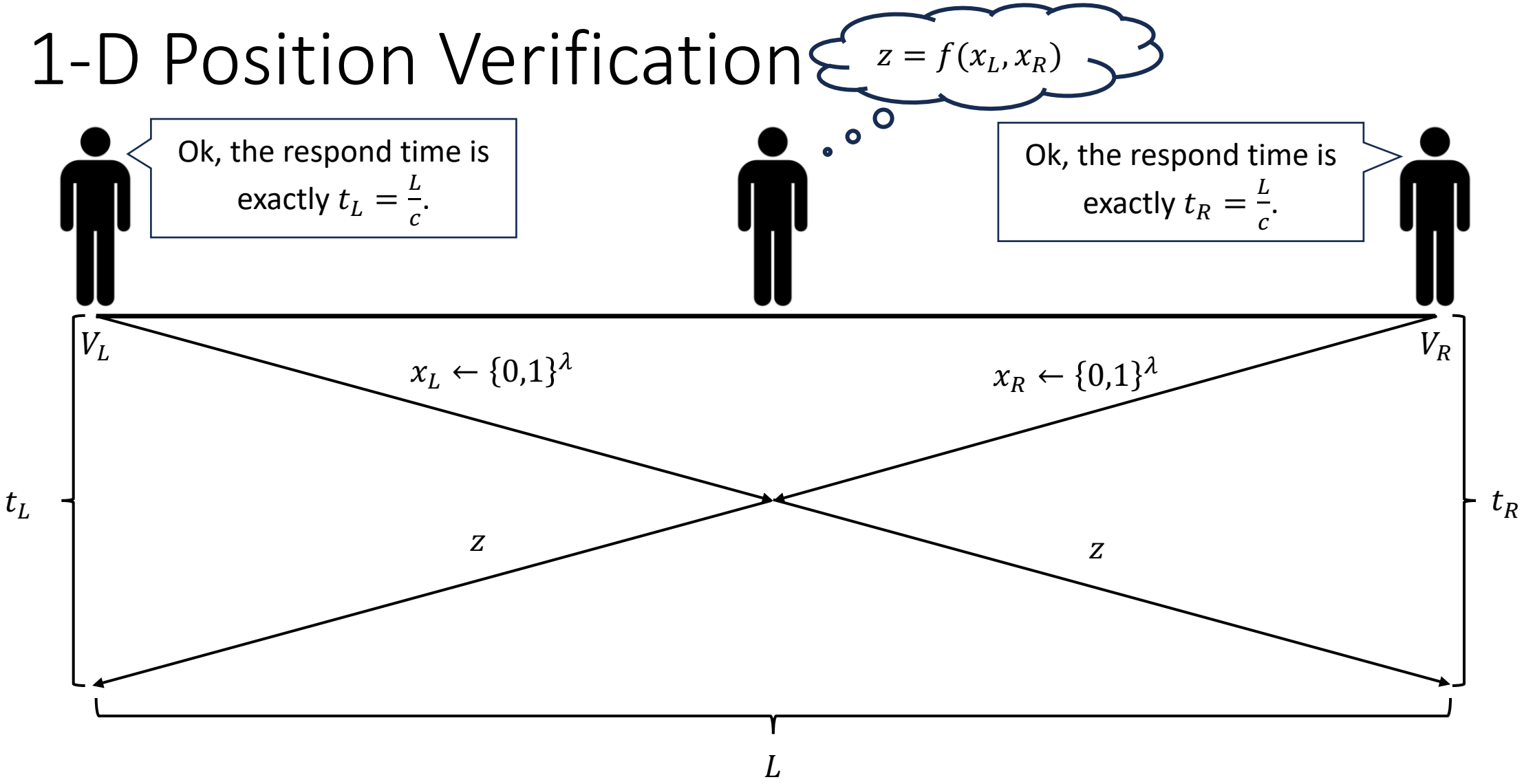
Position Based Cryptography

- In Cryptography, we verify the attribute of a party in different ways.
  - Witness: NP proof system.
  - Ownership of secret keys: PKE, SKE.
  - Ownership of Signing tokens: Signatures.
  - Position? If the “party” is at some place.

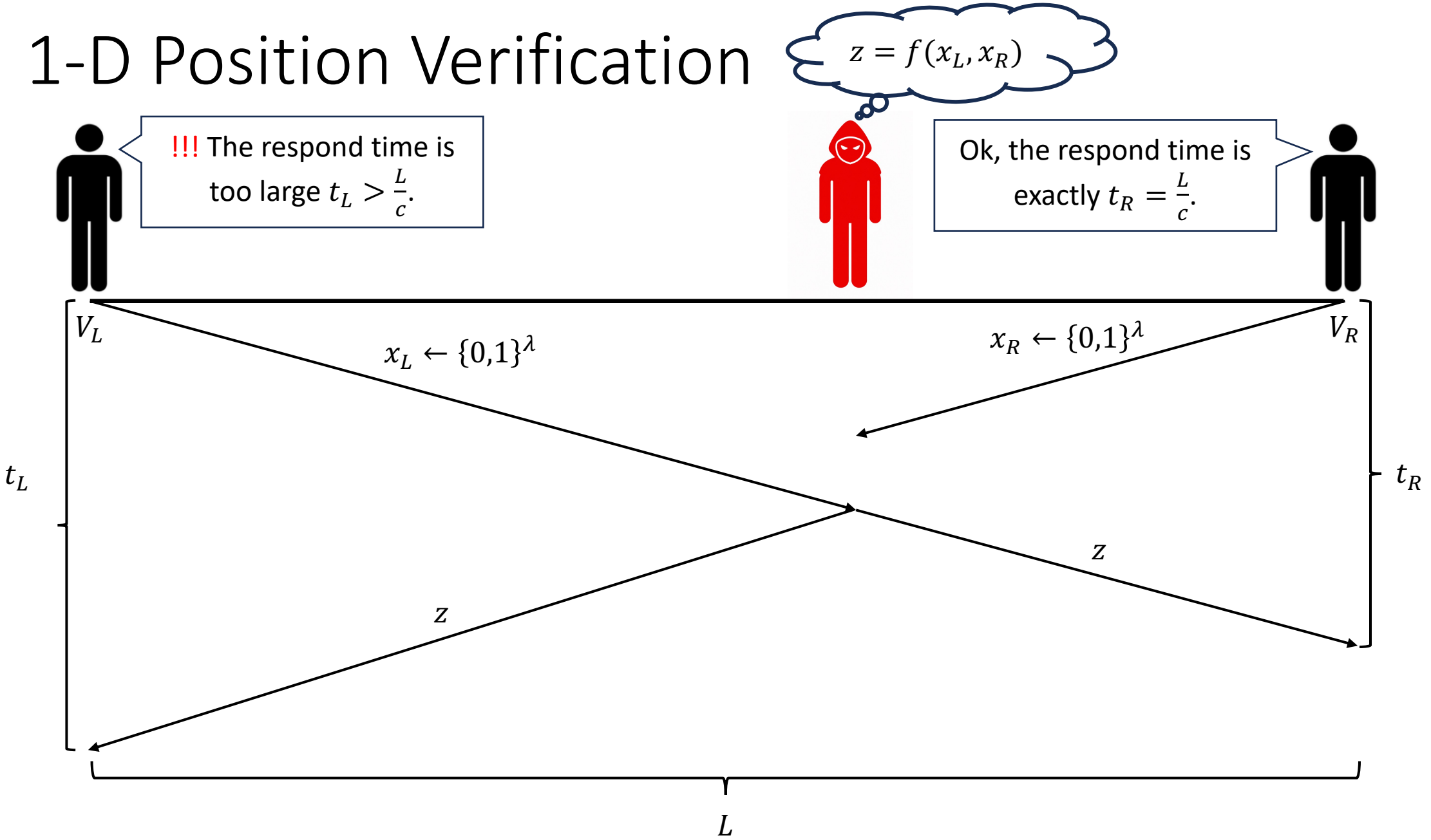
1-D Position Verification [CGMO09]



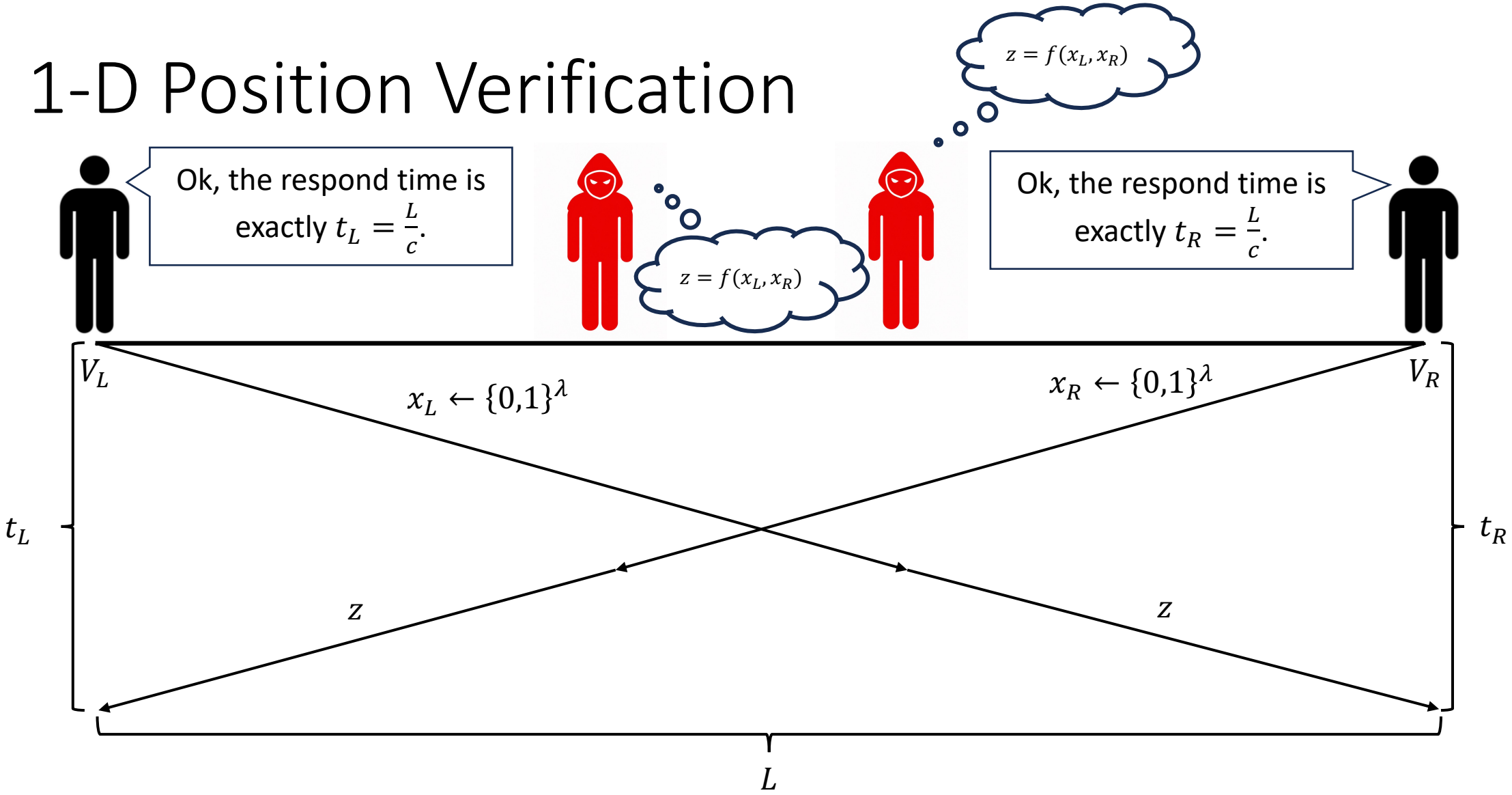
1-D Position Verification



1-D Position Verification

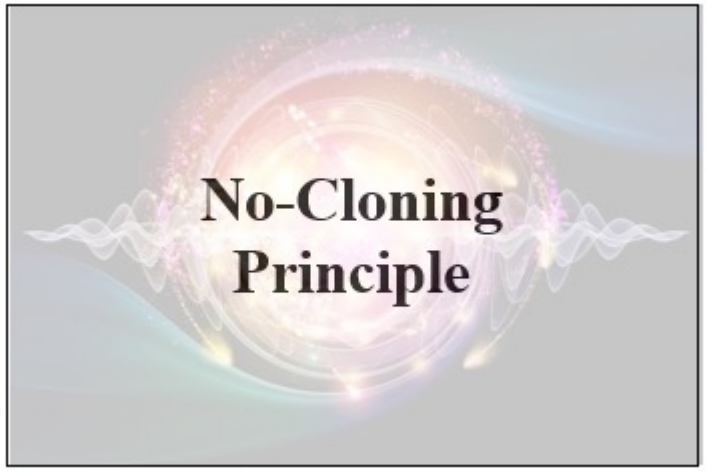


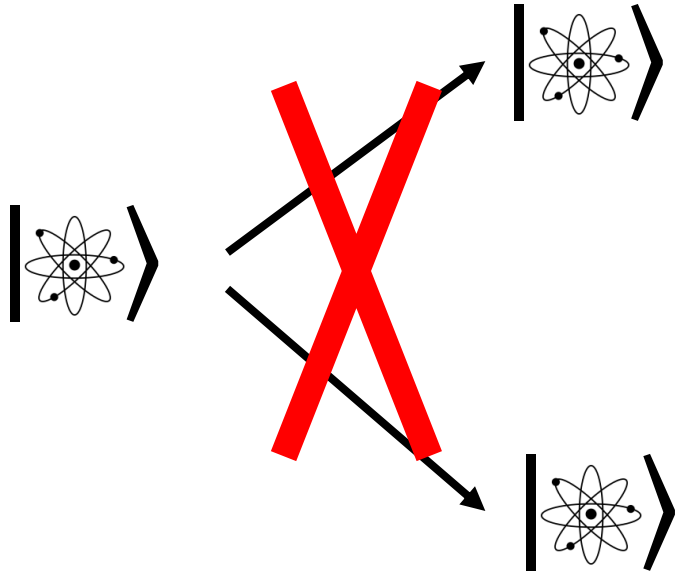
1-D Position Verification



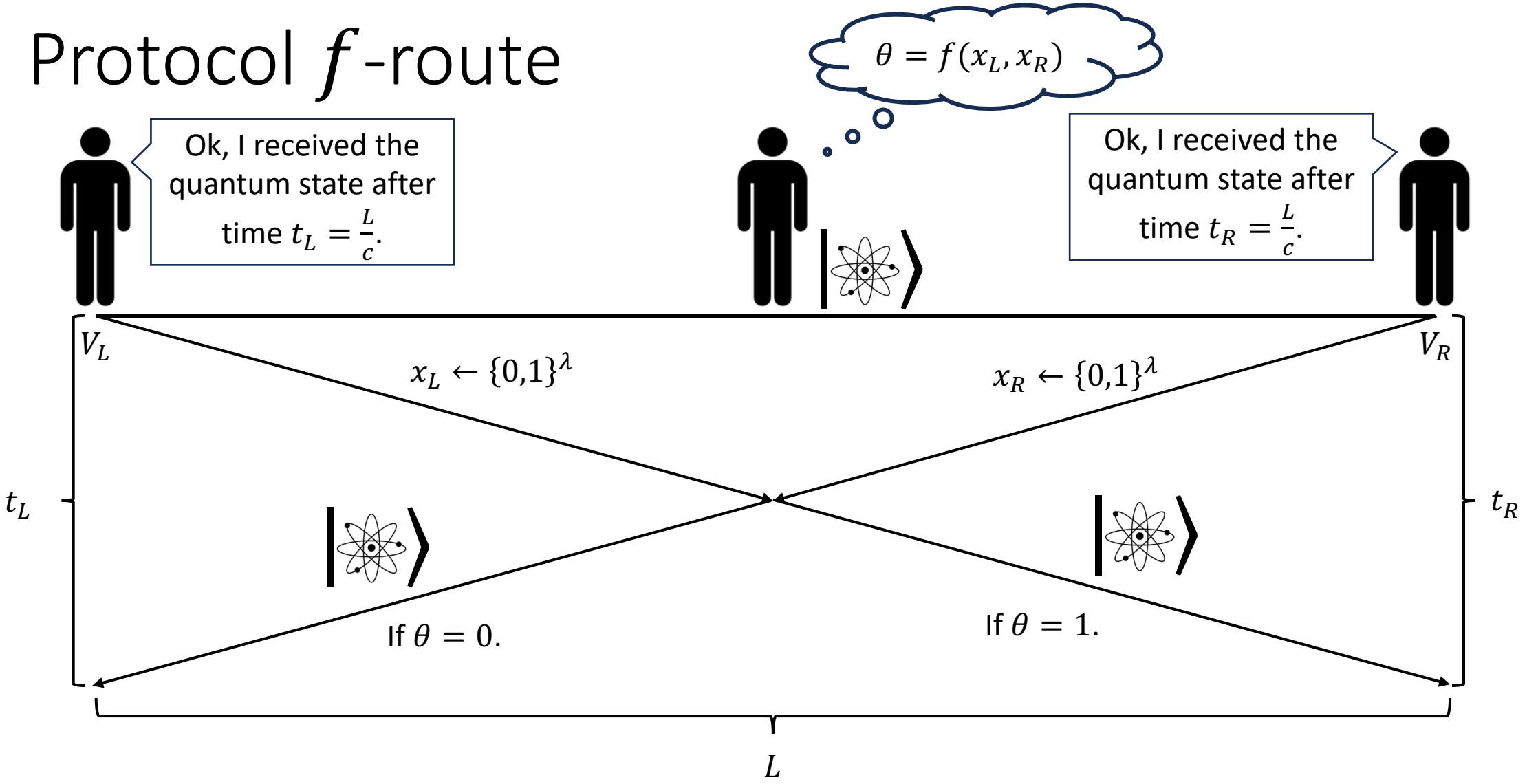
$z = f(x_L, x_R)$ is a classical task!

What is unclonable cryptography?

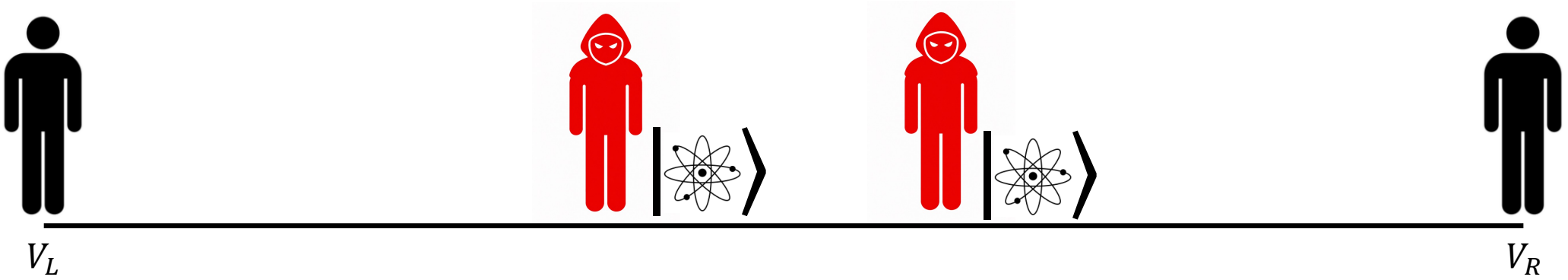




Protocol f-route



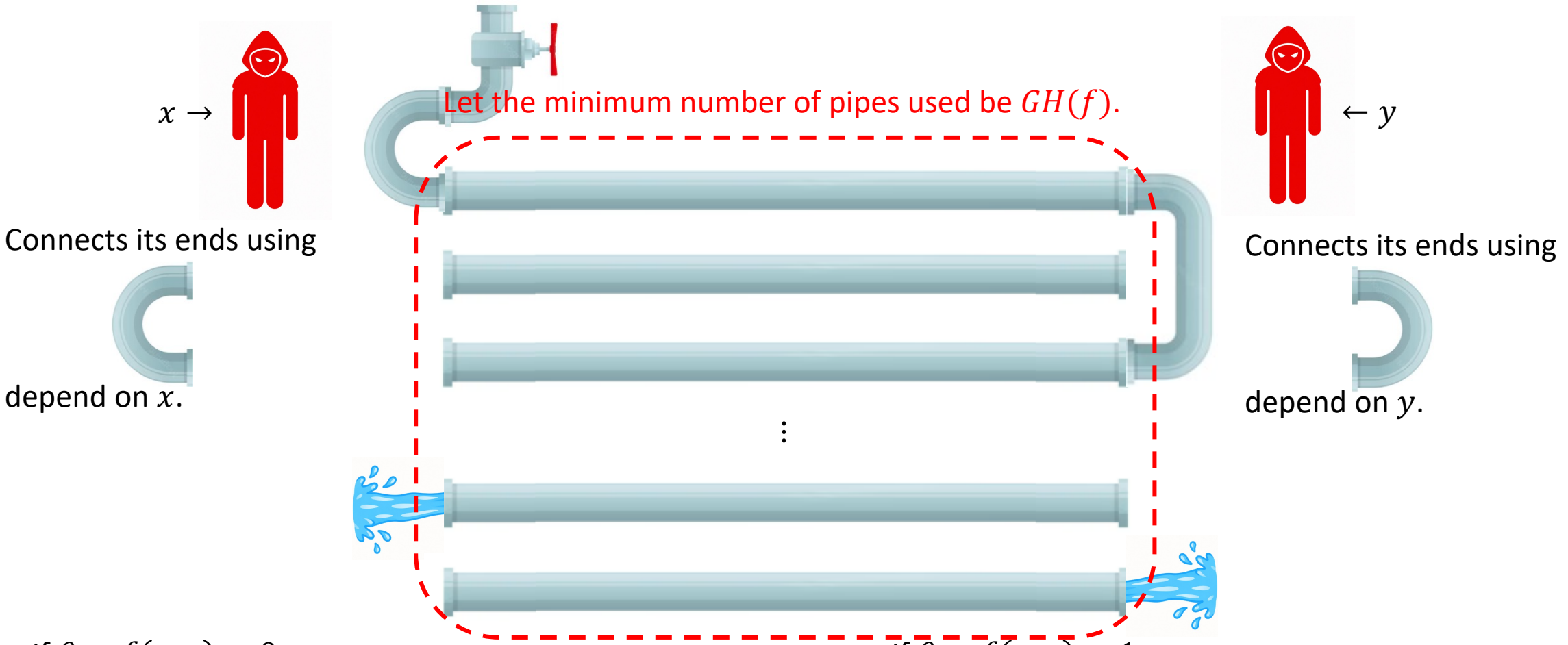
Protocol f-route



Cannot clone the state in general.

Are we done? No!
We need to choose f.

The Garden-Hose Complexity[BFSS13] for f



If $\theta = f(x, y) = 0$.
Water comes out from the left end of some pipe.

If $\theta = f(x, y) = 1$.
Water comes out from the right end of some pipe.

The Garden-Hose Complexity for AND is 2.

$0,1 = x \rightarrow$



$\leftarrow y = 0,1$

The Garden-Hose Complexity for AND is 2.

$0 = x \rightarrow$



$\leftarrow y = 0,1$

The Garden-Hose Complexity for AND is 2.

$1 = x \rightarrow$



$\leftarrow y = 0$

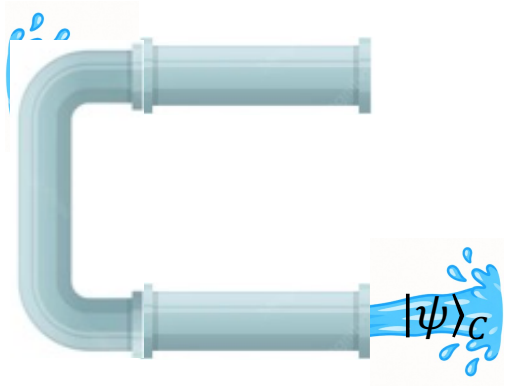
The Garden-Hose Complexity for AND is 2.

$1 = x \rightarrow$



$\leftarrow y = 1$

Quantum Teleportation & Pipes



$\approx$

Measure AC under Bell basis to obtain m.

$|\psi\rangle_C$

$\frac{1}{\sqrt{2}}|00\rangle_{AB} + \frac{1}{\sqrt{2}}|11\rangle_{AB}$

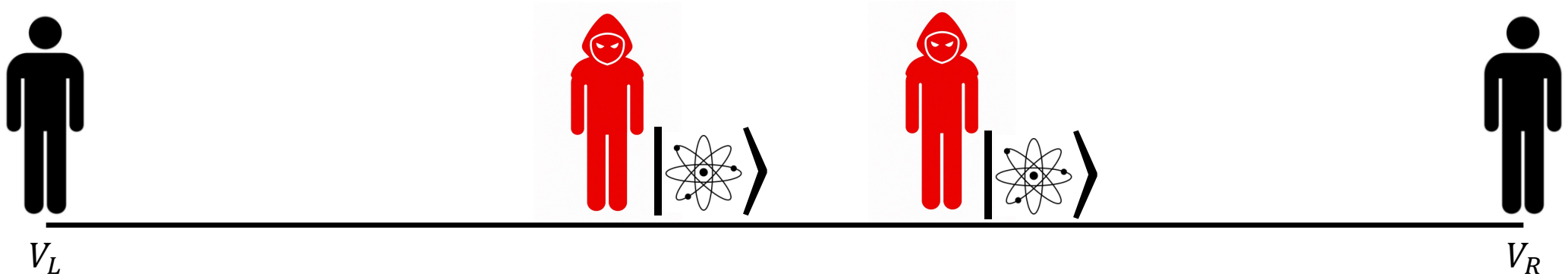
A

B

Use m to decode its state. It will get $|\psi\rangle$.

Send m.

Protocol f-route



Theorem[BFSS13]: there exists an attack on f-route where the adversary shares $GH(f)$ bits of entanglement.

Theorem[BFSS13]: for any $f \in L$, $GH(f) = \text{poly}$.

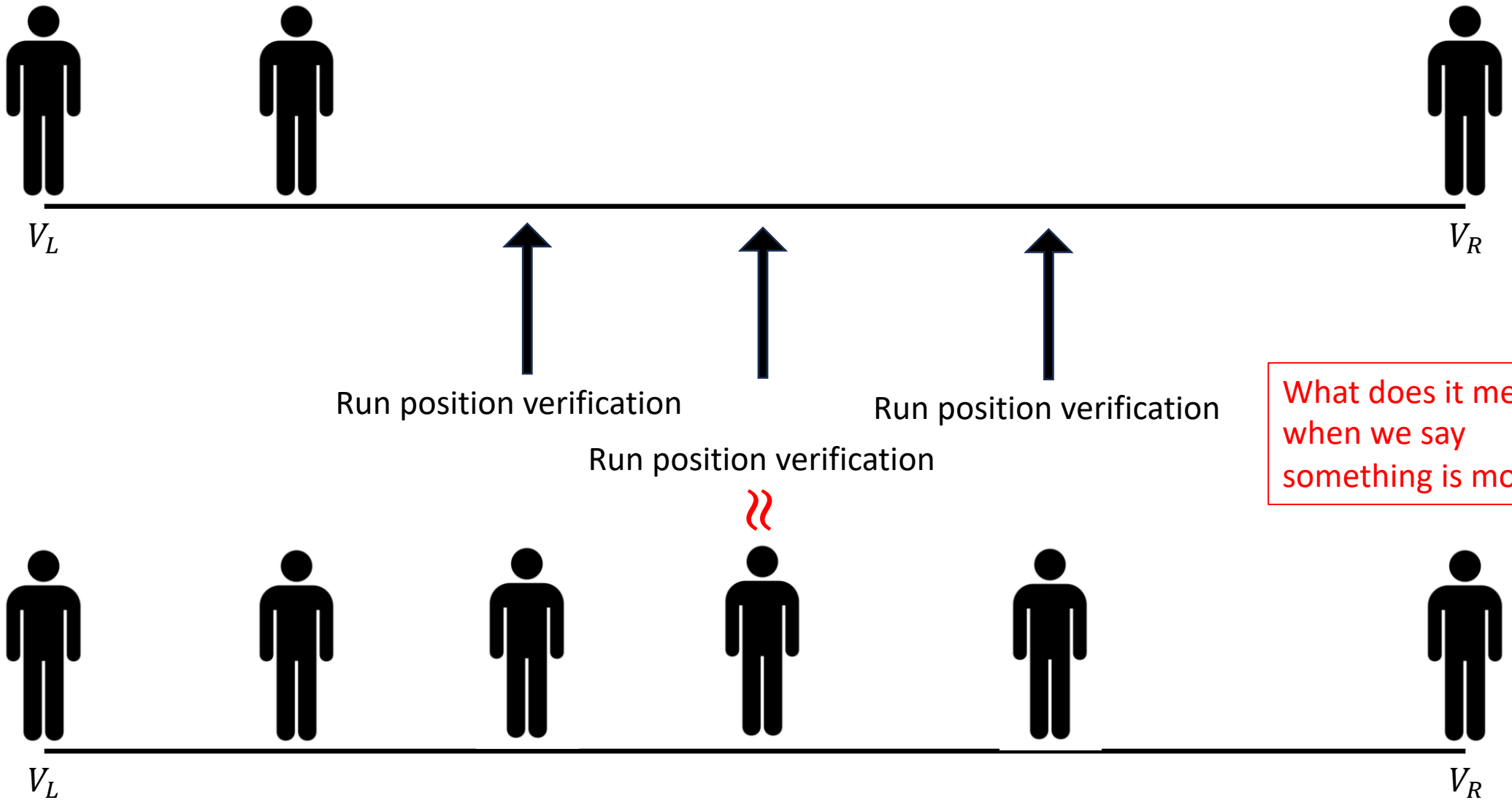
Theorem[BFSS13]: Showing the completeness & security of f-route for any f implies $L \neq P$.

Plaintext position verification against unbounded entanglement adversary remains open. But we are able to prove security when f is a random oracle.

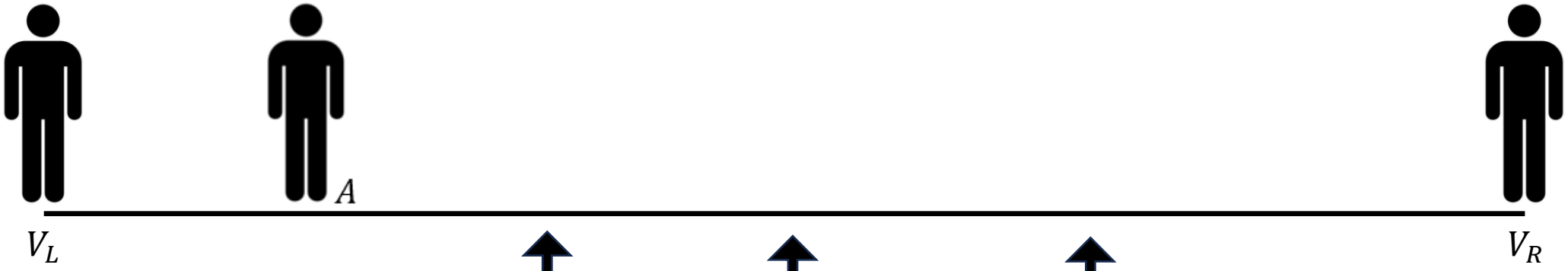
Trajectory Verification[BHOY26]



Trajectory Verification[BHOY26] (first attempt)



Trajectory Verification[BHOY26]



AB is initialized to a fully entangled state.

B is "entangled with this area"

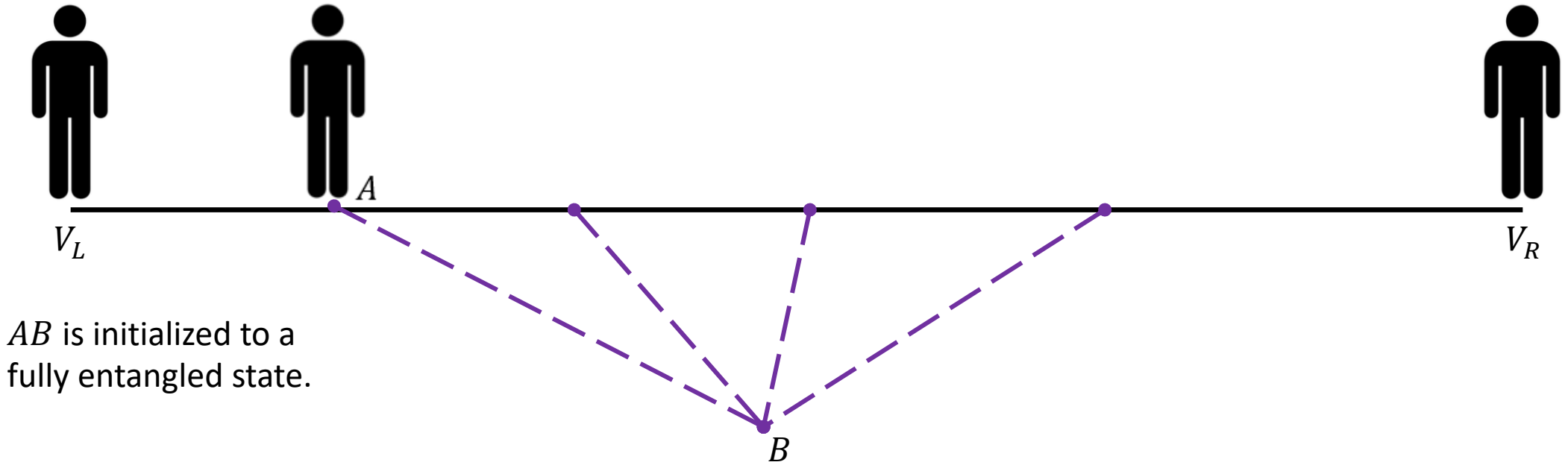
B is "entangled with this area"

B is "entangled with this area"

We say a B is entangled with an area if the joint state of all quantum register in that area is entangled with B.

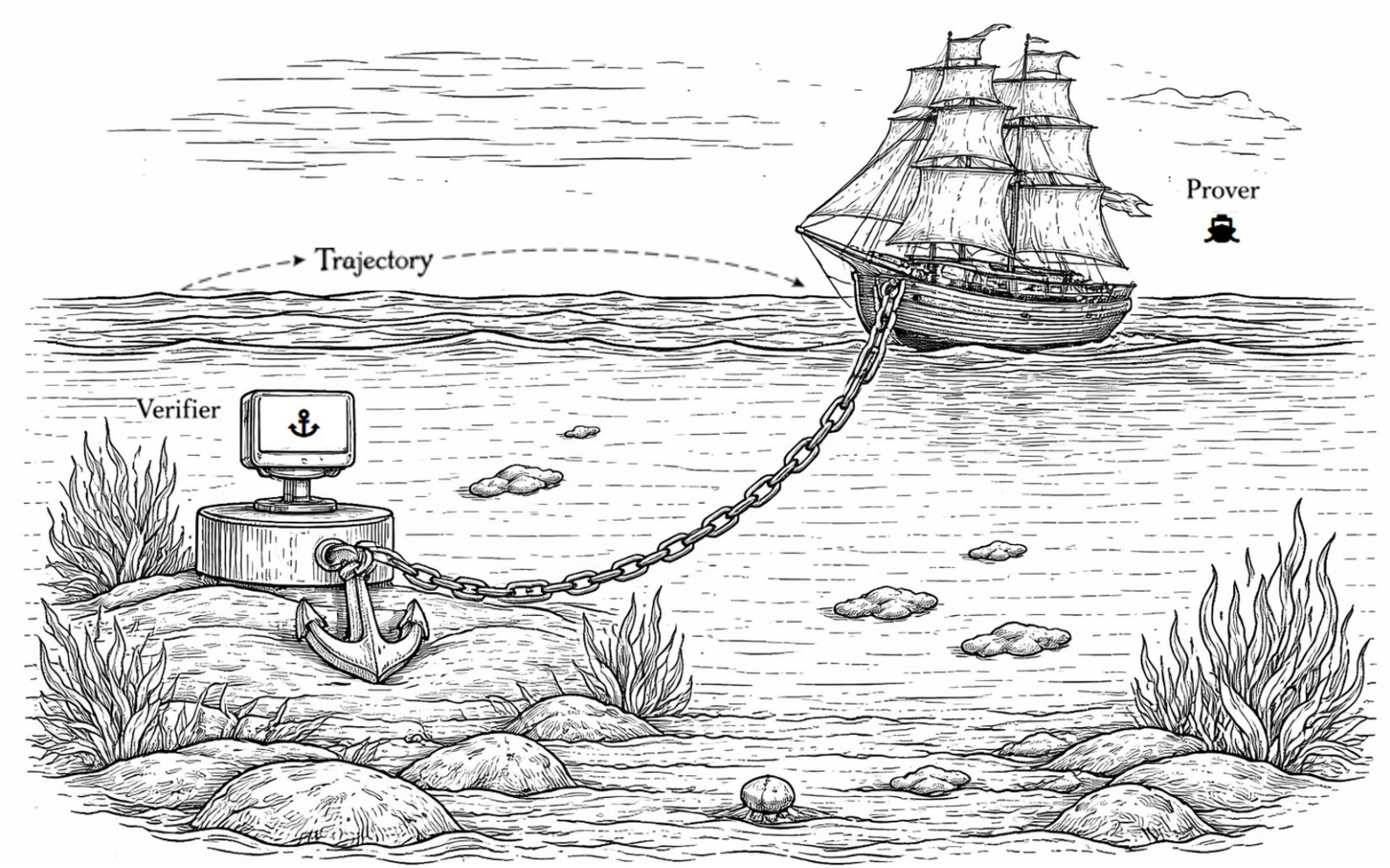
Monogamy of Entanglement

- A qubit can only be fully entangled with one qubit. That is, if A and B are fully entangled then B cannot entangled with C.



AB is initialized to a fully entangled state.

Quantum Anchor [BHOY26]



Generated by GPT.

Non-destructive entanglement localization scheme.

- Let D be an area in our universe and let t be a time step. A fully entangled state $|\psi\rangle_{AB}$ is generated with n bit entanglement. An interactive protocol between a prover and a verifier is a localization scheme if:
- An honest prover holding A inside D can pass the protocol and the state after the test is negligibly close to $|\psi\rangle_{AB}$.
- For any prover (possibly malicious) that passes the protocol with inverse polynomial probability. There exists a channel on the joint register of D and a channel on B such that apply them at time t will make the joint state on AB a n bit EPR pair.

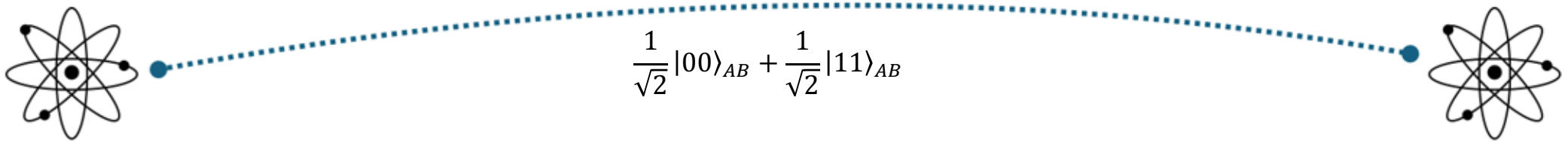
Difficulties

- Previous schemes for entanglement testing always destroys the state.
- We need to take space into account. [Turns out to be highly non-trivial. Not covered today.]

Destructive Entanglement Testing

Probably malicious

Always honest



$\frac{1}{\sqrt{2}}|00\rangle_{AB} + \frac{1}{\sqrt{2}}|11\rangle_{AB}$

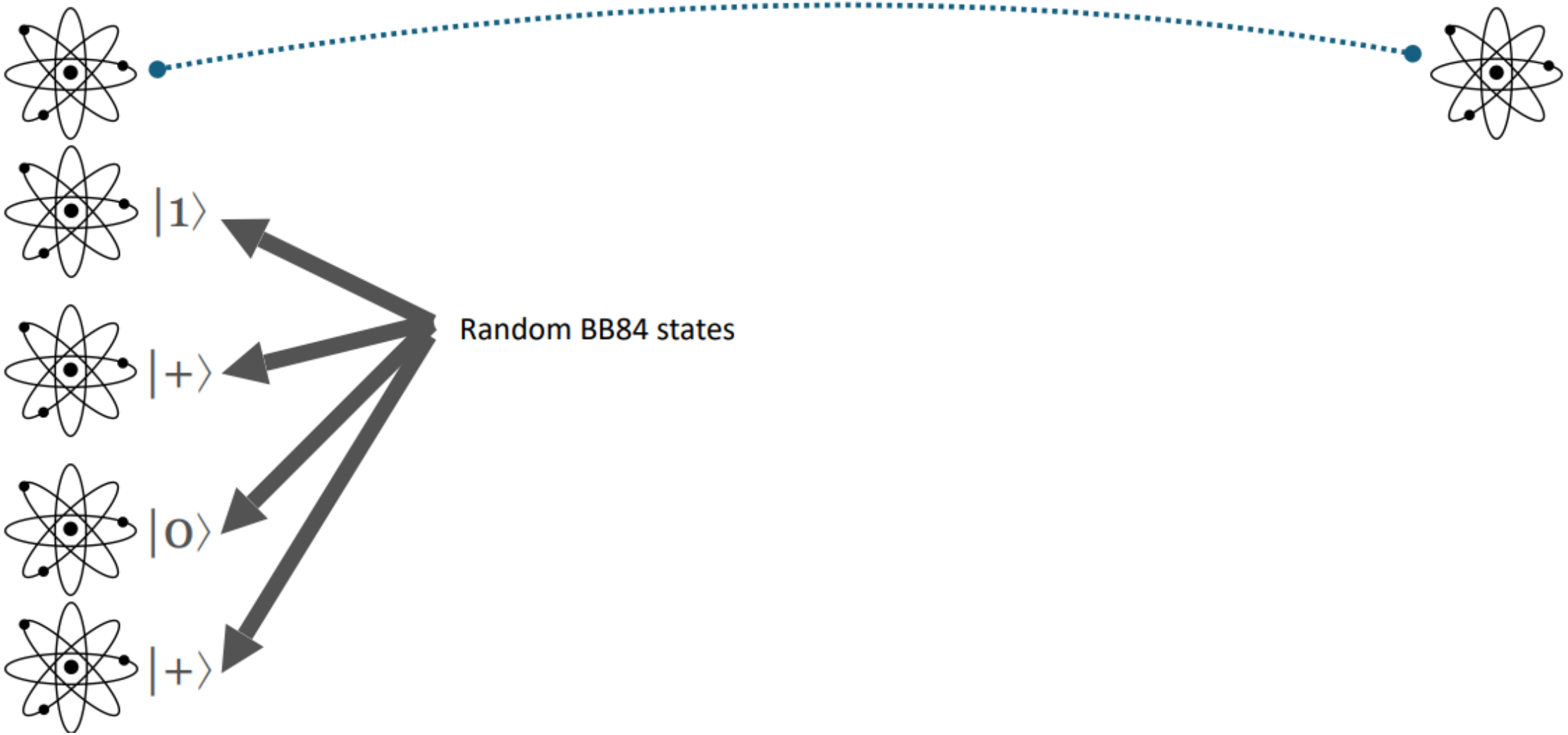
Measure under θ-basis
Obtain b_L.

$\theta \leftarrow \{\text{Standard}, \text{Hadamard}\}$

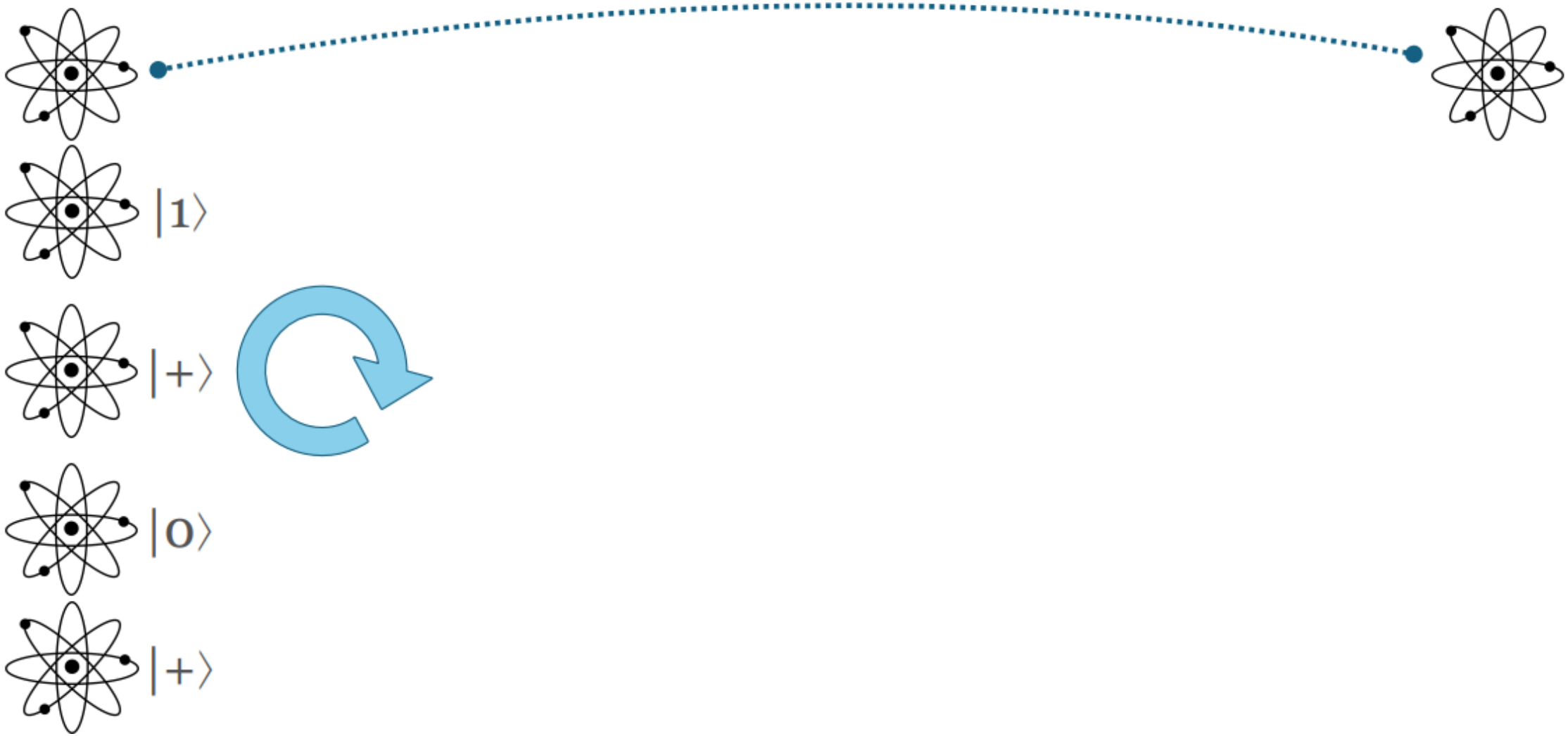
Measure under θ-basis
Obtain b_R.

If they share a EPR pair then $b_L = b_r$.
If they are not entangled then no strategy can achieve $\Pr[b_L = b_r] \geq \cos(\frac{\pi}{8})$.

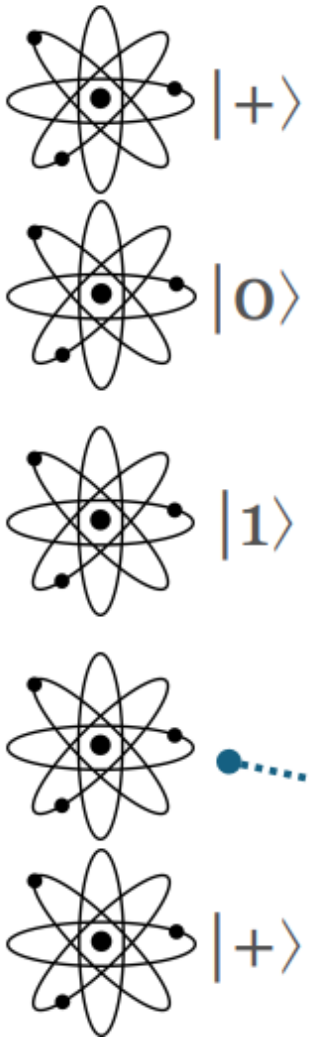
Adding Decoy Qubits



Adding Decoy Qubits



Adding Decoy Qubits



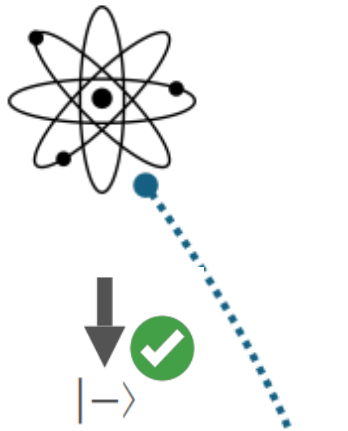
"I got |+⟩."

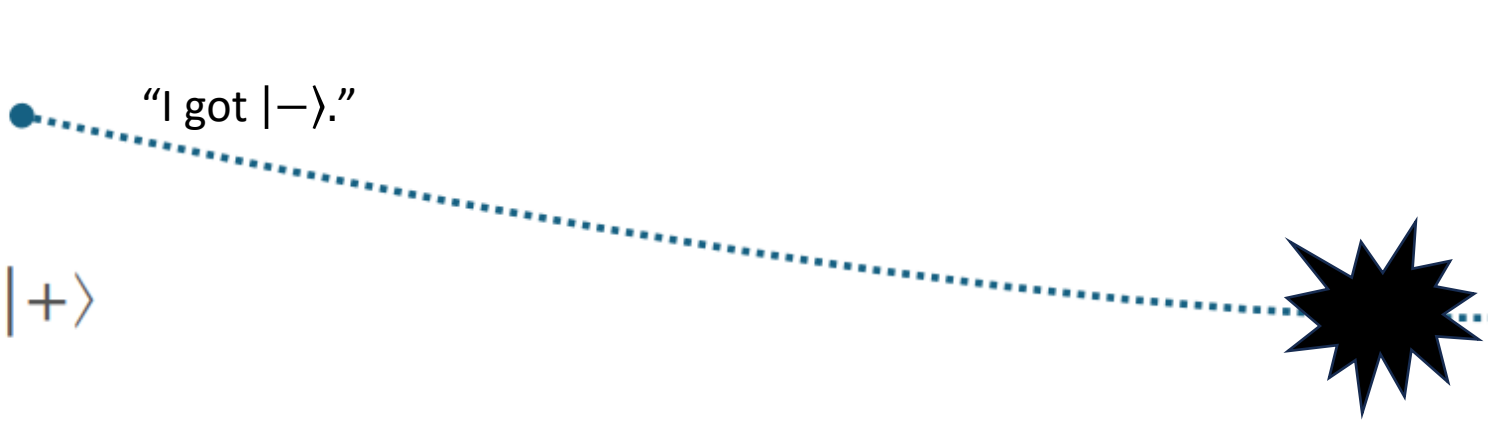
"I got |−⟩."

Measure qubit 3 in the standard basis.

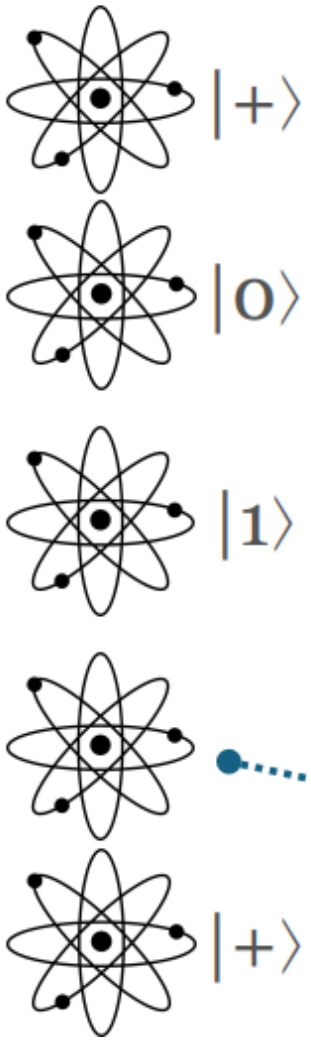
Measure qubit 1 in the Hadamard basis.

Measure qubit 4 in the Hadamard basis.





Adding Decoy Qubits



Measure qubit 3 in the standard basis.

Measure qubit 1 in the Hadamard basis.

Measure qubit 4 in the Hadamard basis.

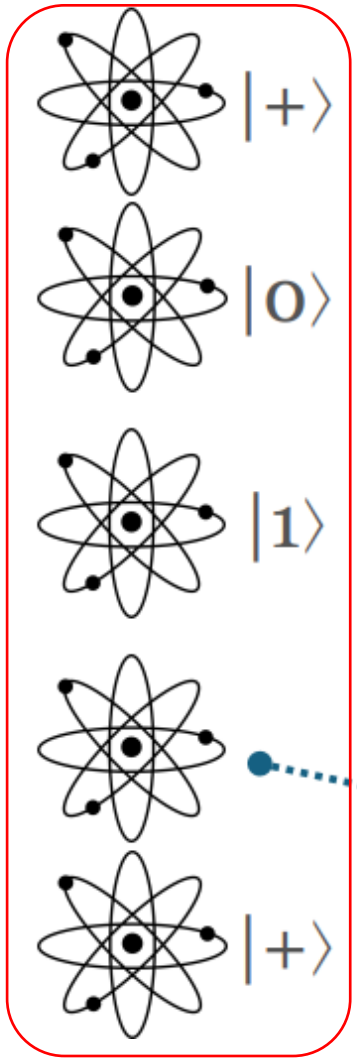
Non-destructive test.

Destructive test.

Indistinguishable on the side of the prover!

If the prover is able to pass random non-destructive test, I will believe that it can pass the destructive test.

Adding Decoy Qubits



Final trick:
Scramble information using random basis-change unitary.
So that it can stand multiple challenges.
!!!We need oracle in this step.



Final Construction

- Let $L(t)$ be the claim trajectory of the prover.
- For $i = 0,1,2,\cdots,m$, run an entanglement localization on region $[L(\frac{ti}{m}) - \epsilon, L(\frac{ti}{m}) + \epsilon]$ at time $\frac{ti}{m}$.
- This shows that the “entanglement” moves along the path.

Connect space, time, and information

- We also obtain state localization and functionality localization:
  - State localization is a scheme which the verifier, after its acceptance on the proof, can assure that an unclonable state is somewhere in the region.
  - Functionality localization is a scheme where the verifier, after its acceptance on the proof, can make sure that:
    - 1, Using the joint state on the register in the region, one can compute a function f.
    - 2, No one outside (even multiple parties) the region can compute f.

Thanks!