How to Track Qubits Through Space and Time

Stronger guarantees for position-based cryptography, and how to achieve them

Leo Orshansky (Columbia University)

Zikuan Huang

Shanghai Qizhi Institute

James Bartusek

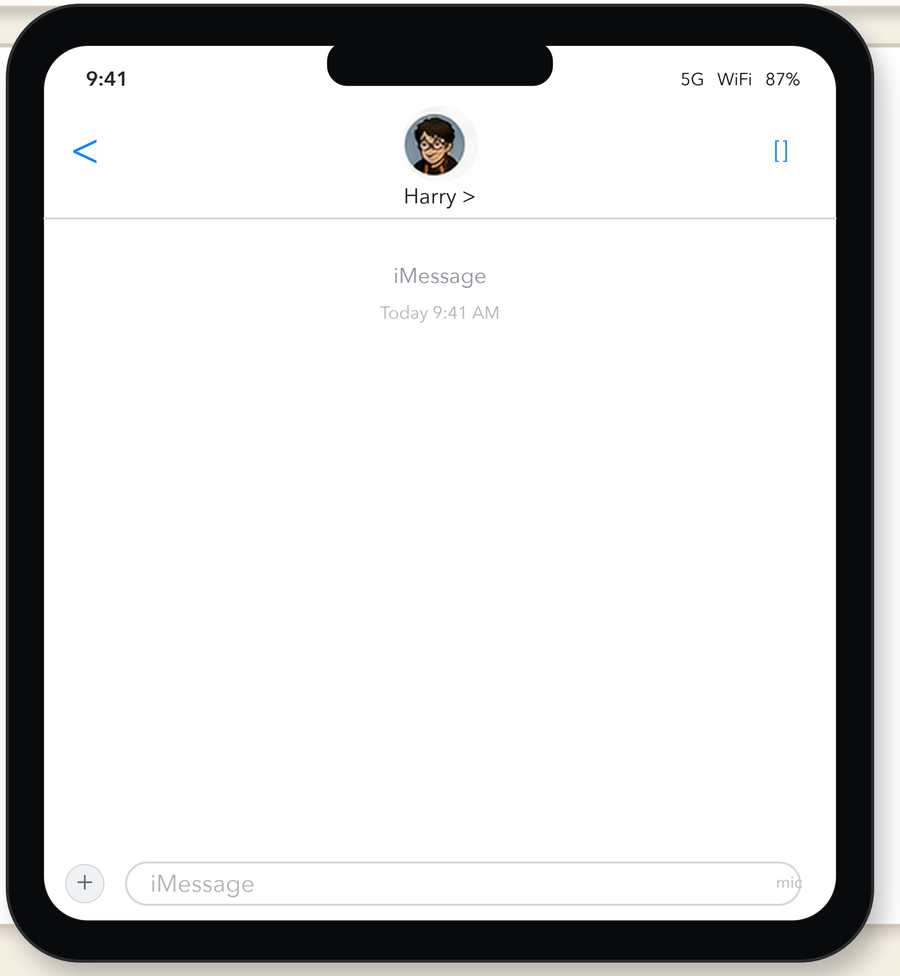
Columbia University

Henry Yuen

Columbia University

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.



Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 1

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 2

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 2

Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 2

Scenario: A Friend Needs Help

When position-based cryptography comes in handy.

Can we authenticate a message by its positional origin?

Scenario 2

Scenario: A Friend Needs Help

When position-based cryptography comes in handy.

Scenario 2

Can we authenticate a message by its positional origin?

[BCF+14]: Yes, with Quantum Position Verification (QPV).

Scenario: A Friend Needs Help

When position-based cryptography comes in handy.

Scenario 2

Can we authenticate a message by its positional origin?

[BCF+14]: Yes, with Quantum Position Verification (QPV).

Scenario: A Friend Needs Help

When position-based cryptography comes in handy.

Scenario 2

Can we authenticate a message by its positional origin?

[BCF+14]: Yes, with Quantum Position Verification (QPV).

Scenario: A Friend Needs Help

When position-based cryptography comes in handy.

Scenario 2

Can we authenticate a message by its positional origin?

[BCF+14]: Yes, with Quantum Position Verification (QPV).

Scenario: A Friend Needs Help

When position-based cryptography comes in handy.

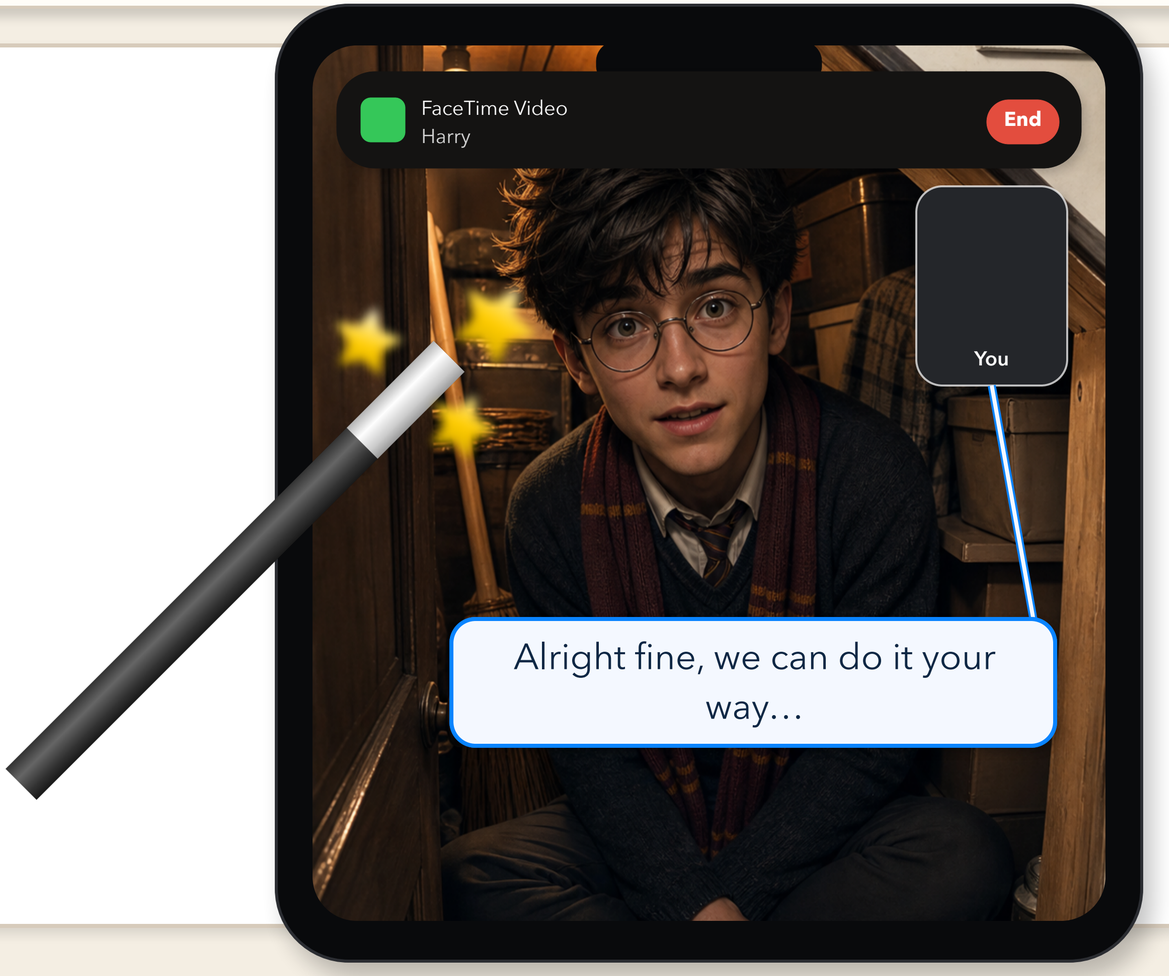
Scenario 2

Can we authenticate a message by its positional origin?

[BCF+14]: Yes, with Quantum Position Verification (QPV).

Scenario: A Friend Needs Help

When position-based cryptography comes in handy.



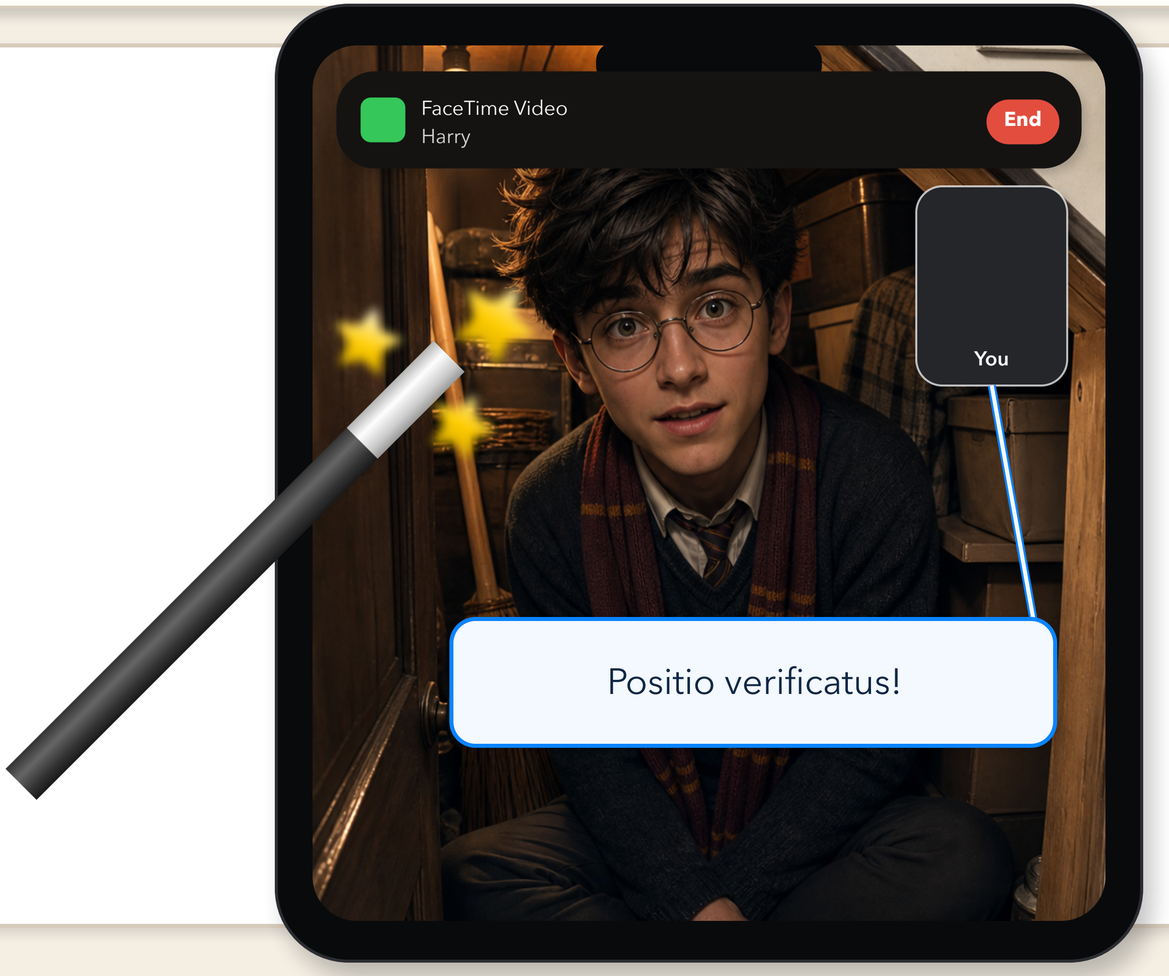
Can we authenticate a message by its positional origin?

[BCF+14]: Yes, with Quantum Position Verification (QPV).

Scenario 2

Scenario: A Friend Needs Help

When position-based cryptography comes in handy.



Scenario 2

Can we authenticate a message by its positional origin?

[BCF+14]: Yes, with Quantum Position Verification (QPV).

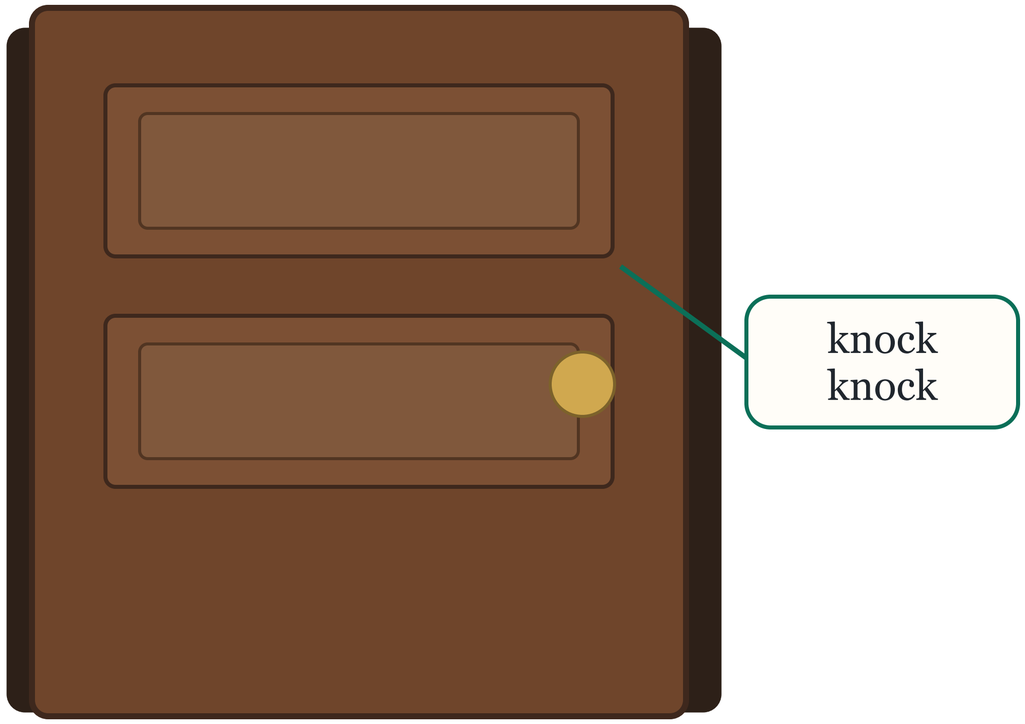
Scenario: A Friend Needs Help

> When position-based cryptography comes in handy.

Scenario 2

Scenario 2: Realistic Clones

What cryptographic credential can distinguish us from *any* other entity?



Scenario 2: Realistic Clones

> What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

> What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

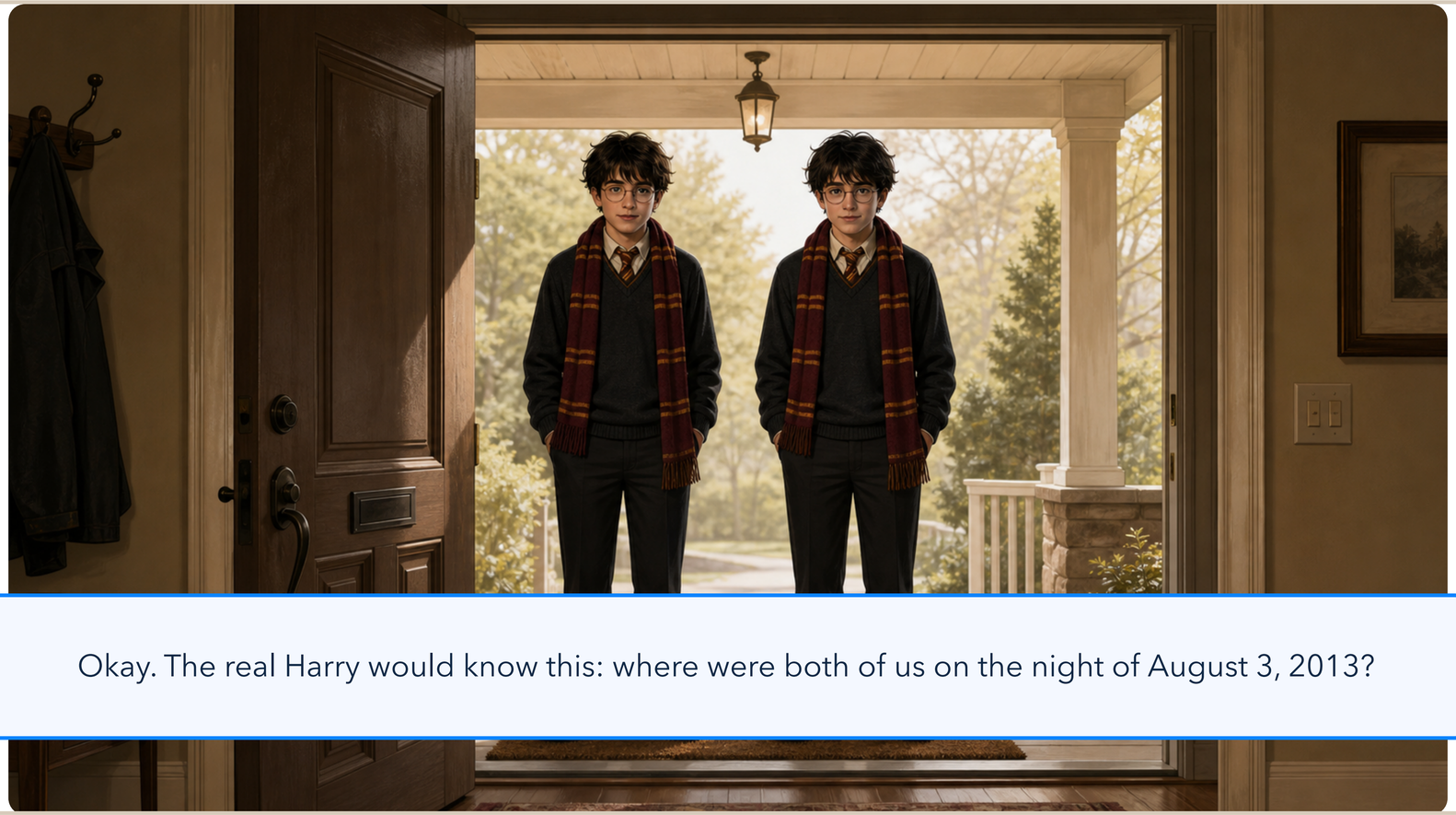
> What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

> What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

What cryptographic credential can distinguish us from *any* other entity?



Scenario 2: Realistic Clones

> What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

> What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

> What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

> What cryptographic credential can distinguish us from *any* other entity?

Scenario 2: Realistic Clones

What cryptographic credential can distinguish us from *any* other entity?

Claim: **Existing position-based crypto is *insufficient* to solve both scenarios 1 and 2**

Claim: **Existing position-based crypto is *insufficient* to solve both scenarios 1 and 2**

This Work: **Strengthening Position-Based Guarantees**

Claim: **Existing position-based crypto is *insufficient* to solve both scenarios 1 and 2**

This Work: Strengthening Position-Based Guarantees

Talk Outline:

1. **Background — position-based cryptography**
2. **Introduce quantum localization schemes**
3. **Construct entanglement localization and trajectory verification**
4. **Bonus: functionality localization, with applications to PBA**

Position as a Credential

> Shifting identity from *what you know* to *where you are*

Position as a Credential

> Shifting identity from *what you know* to *where you are*

What you know:

- Bank account password

- Decryption/Signing private keys (PKI)

Position as a Credential

Shifting identity from *what you know* to *where you are*

What you know:

- Bank account password
- Decryption/Signing private keys (PKI)

Where you are:

- Have access to a secure facility (e.g. bank vault, military base)
- Located within a particular jurisdiction

Could be more robust!

Position as a Credential

> Shifting identity from *what you know* to *where you are*

What you know:

- Bank account password
- Decryption/Signing private keys (PKI)

Where you are:

- Have access to a secure facility (e.g. bank vault, military base)
- Located within a particular jurisdiction

Enables a new kind of cryptography: position-based cryptography

Position-Based Cryptography

Position-Based Authentication

Position-Based Key Exchange

Position-Based Cryptography

Position-Based Authentication

Prover's goal: Send a message m to the verifiers, authenticated with his location.

E.g. m = "Cashapp me $500"

Verifier's goal: Accept m *only* if the sender was at some location L.

E.g. L = "cupboard under the stairs"

Position-Based Key Exchange

Position-Based Cryptography

Position-Based Authentication

Prover's goal: Send a message m to the verifiers, authenticated with his location.

E.g. m = "Cashapp me $500"

Verifier's goal: Accept m *only* if the sender was at some location L.

E.g. L = "cupboard under the stairs"

Position-Based Key Exchange

Prover's goal: establish a shared key with the verifiers.

Verifier's goal: *only* someone at location L can learn the key.

Application: sending a message which can only be read at a specific location.

Position-Based Cryptography

Position-Based Authentication

Position-Based Key Exchange

Position-Based Cryptography

Position-Based Authentication

Position-Based Key Exchange

Position Verification

Prover's goal: convince verifier he is at location L

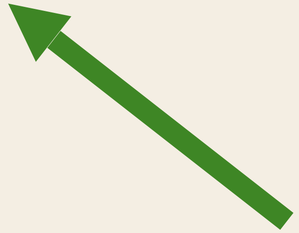
Verifier's goal: Accept *only* if the prover is at location L

Position-Based Cryptography

Position-Based Authentication

Position-Based Key Exchange

[BCFGGOS'10, U'14]: PV -> PBA

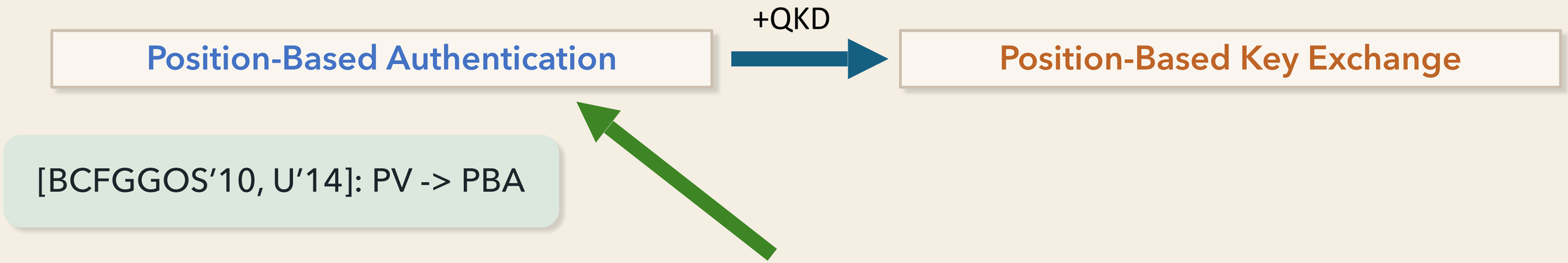


Position Verification

Prover's goal: convince verifier he is at location L

Verifier's goal: Accept *only* if the prover is at location L

Position-Based Cryptography



Position Verification

Prover's goal: convince verifier he is at location L

Verifier's goal: Accept *only* if the prover is at location L

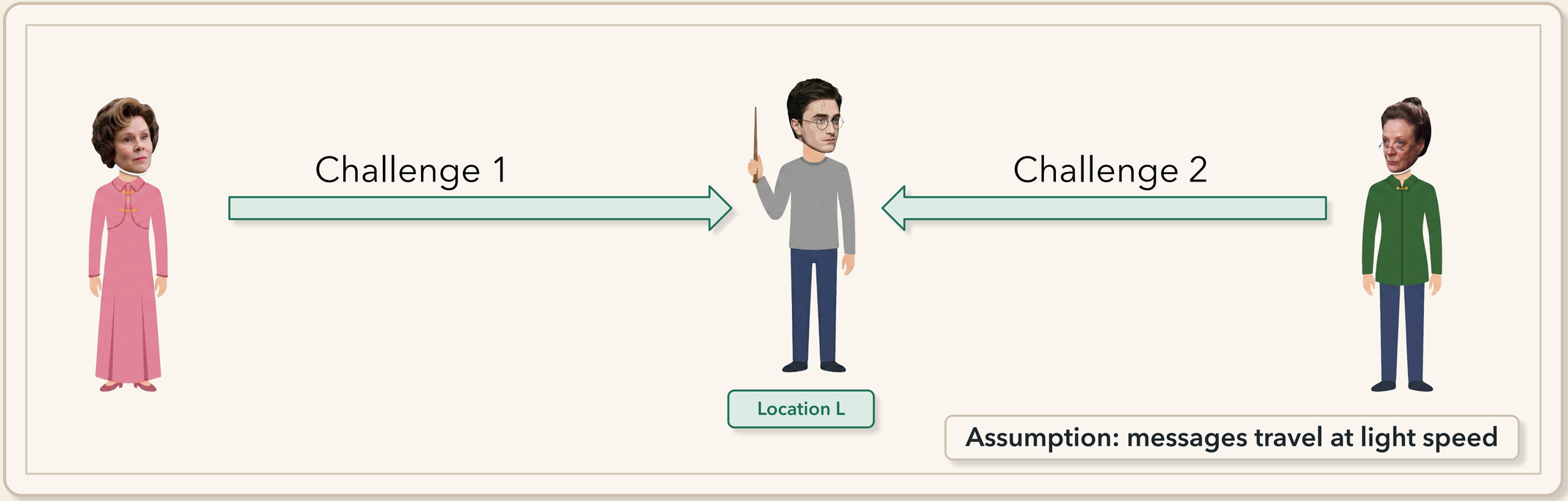
Position Verification

The core building block of position-based cryptography.

Location L

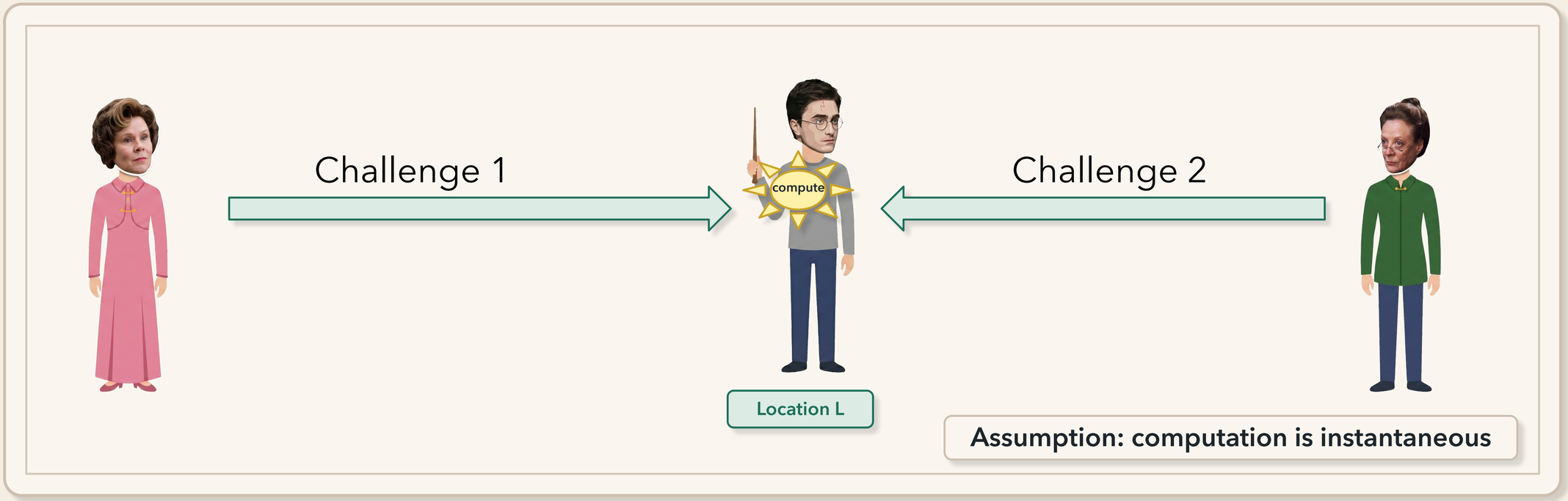
Position Verification

The core building block of position-based cryptography.



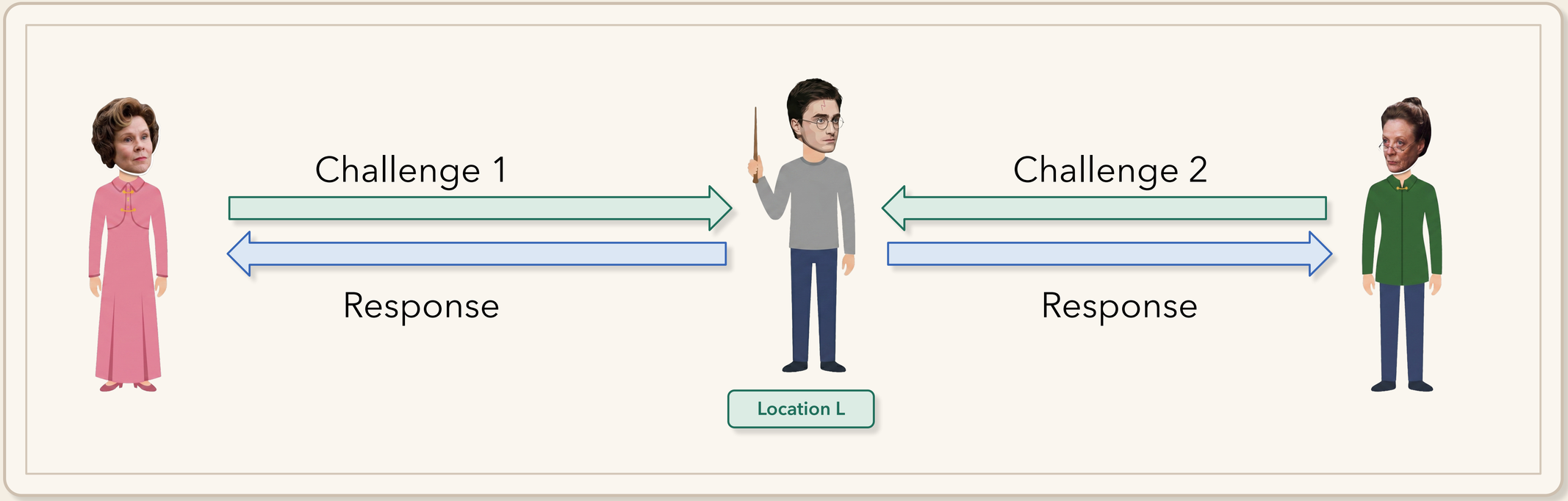
Position Verification

The core building block of position-based cryptography.



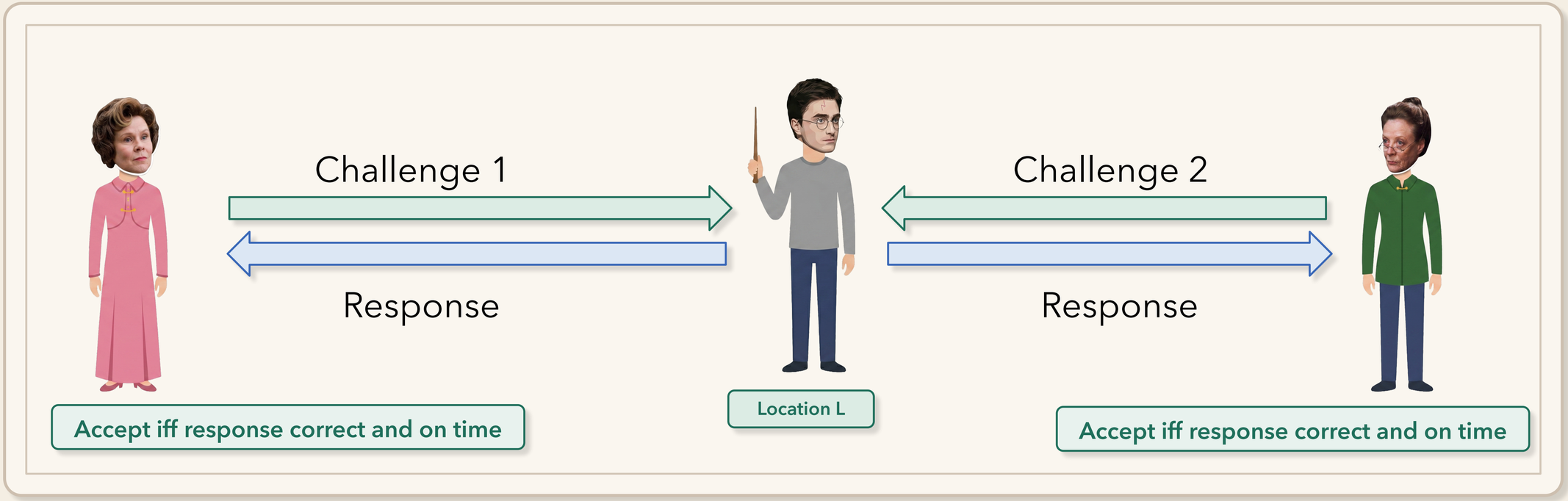
Position Verification

> The core building block of position-based cryptography.



Position Verification

The core building block of position-based cryptography.



Position Verification

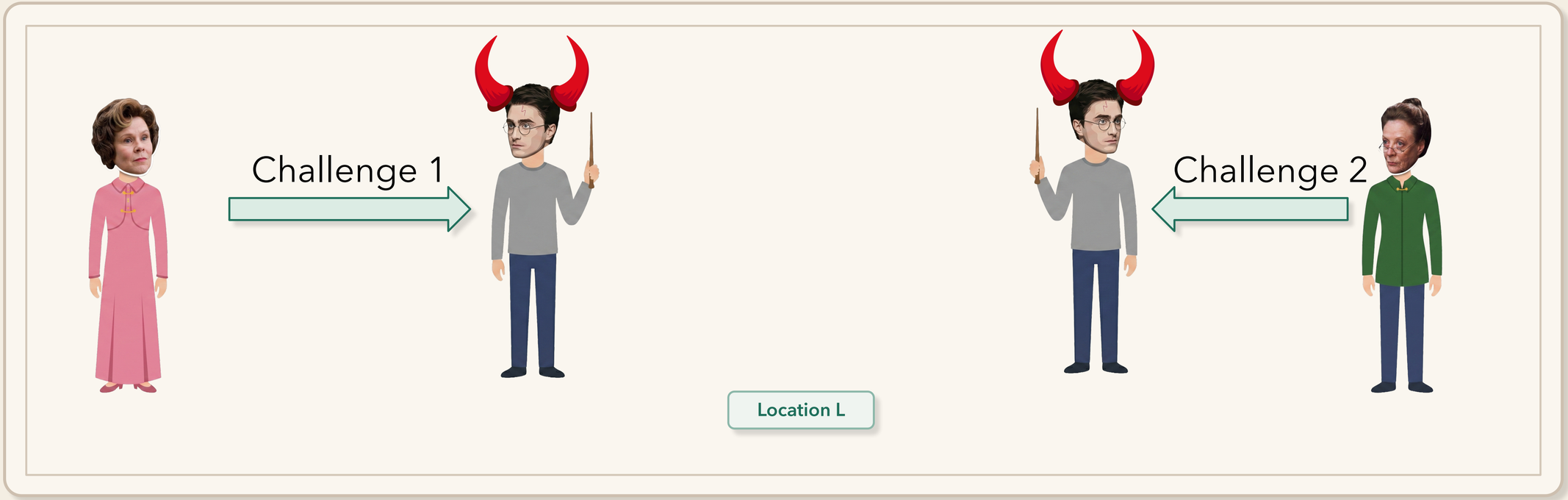
The core building block of position-based cryptography.

What if there are two colluding spoofers?

Location L

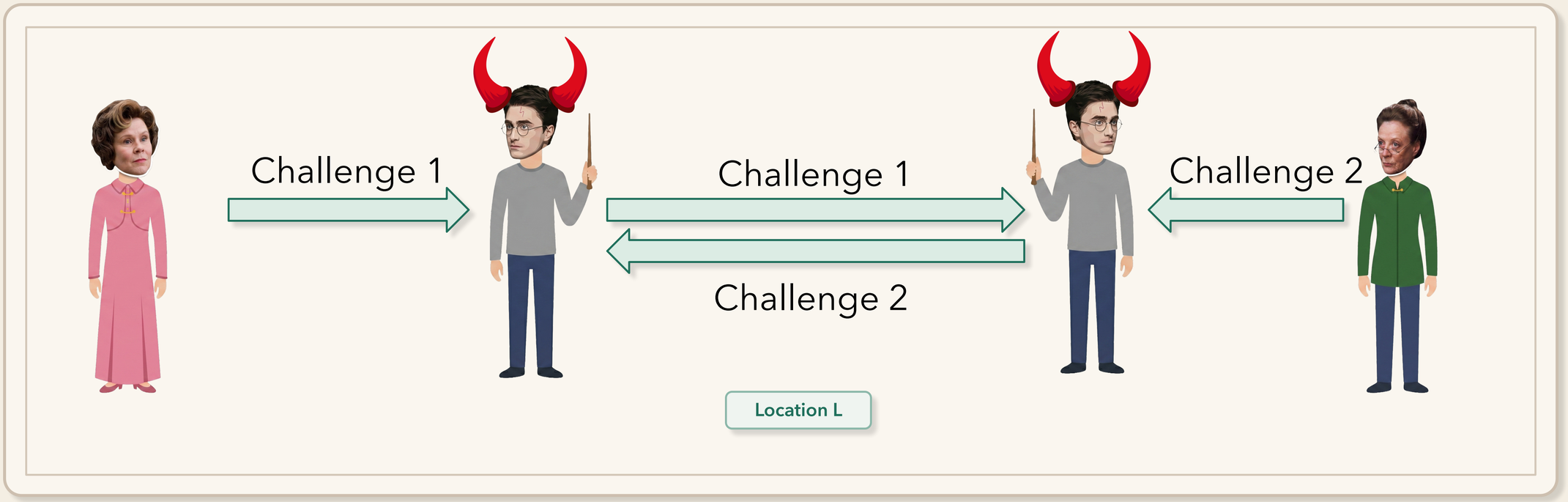
Position Verification

> The core building block of position-based cryptography.



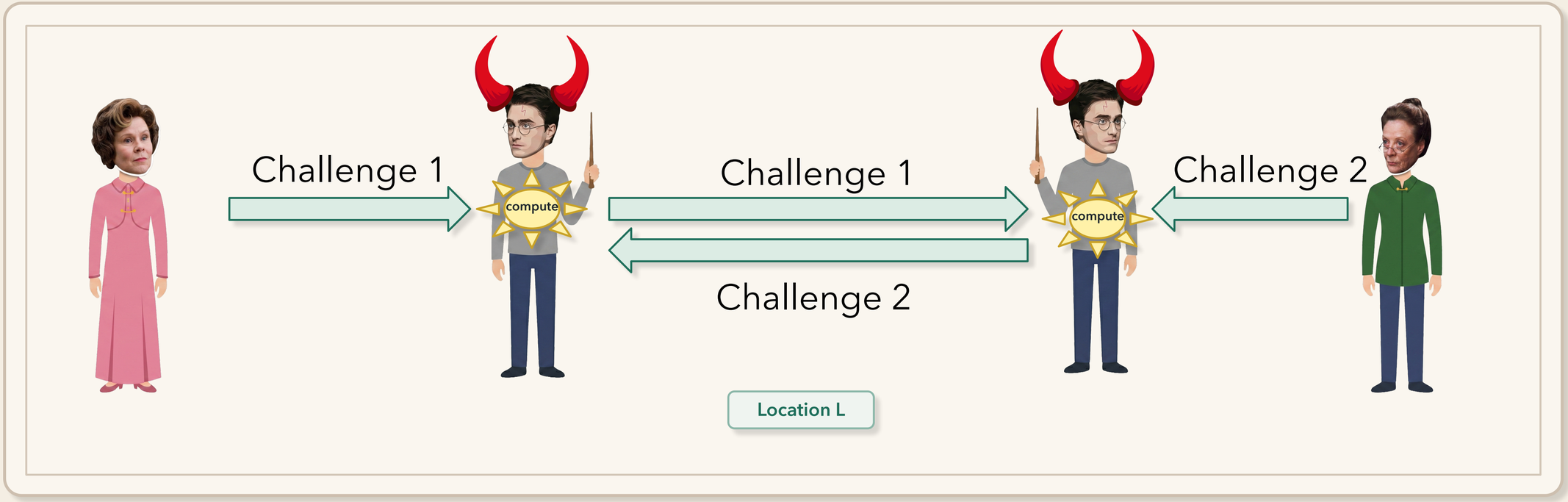
Position Verification

> The core building block of position-based cryptography.



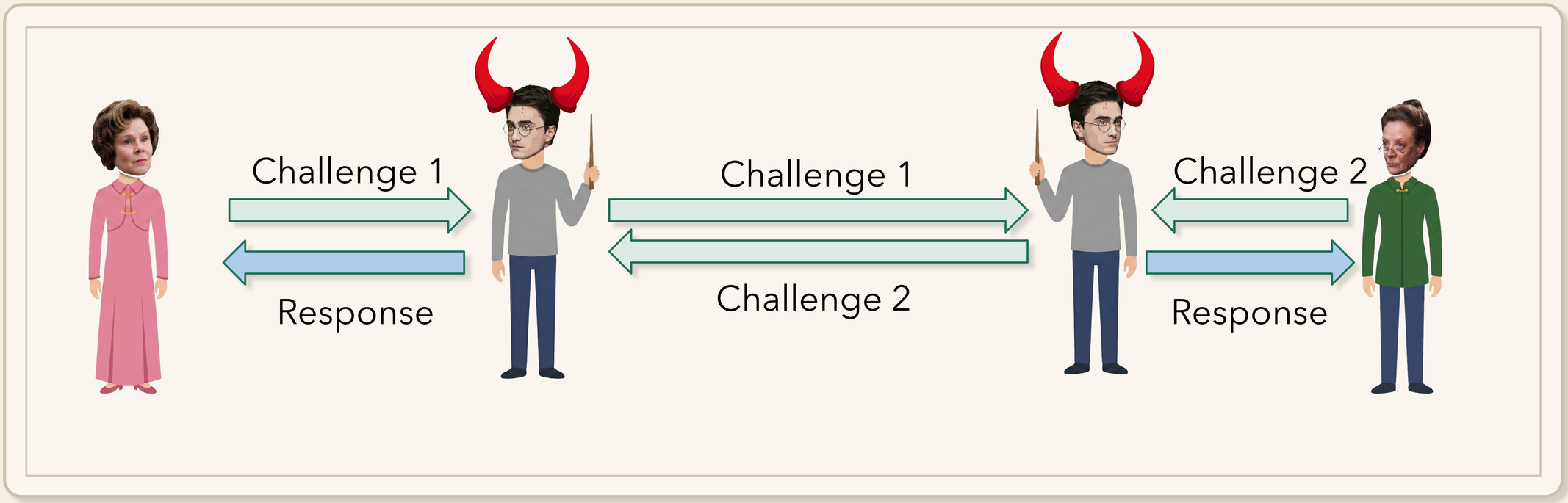
Position Verification

> The core building block of position-based cryptography.



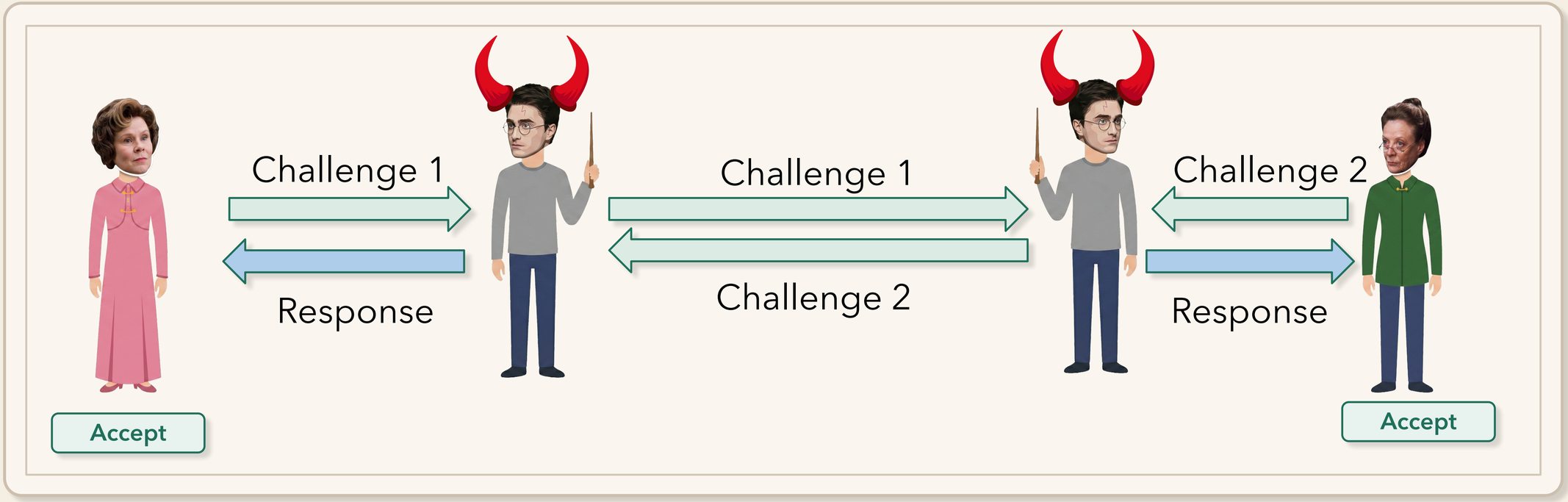
Position Verification

> The core building block of position-based cryptography.



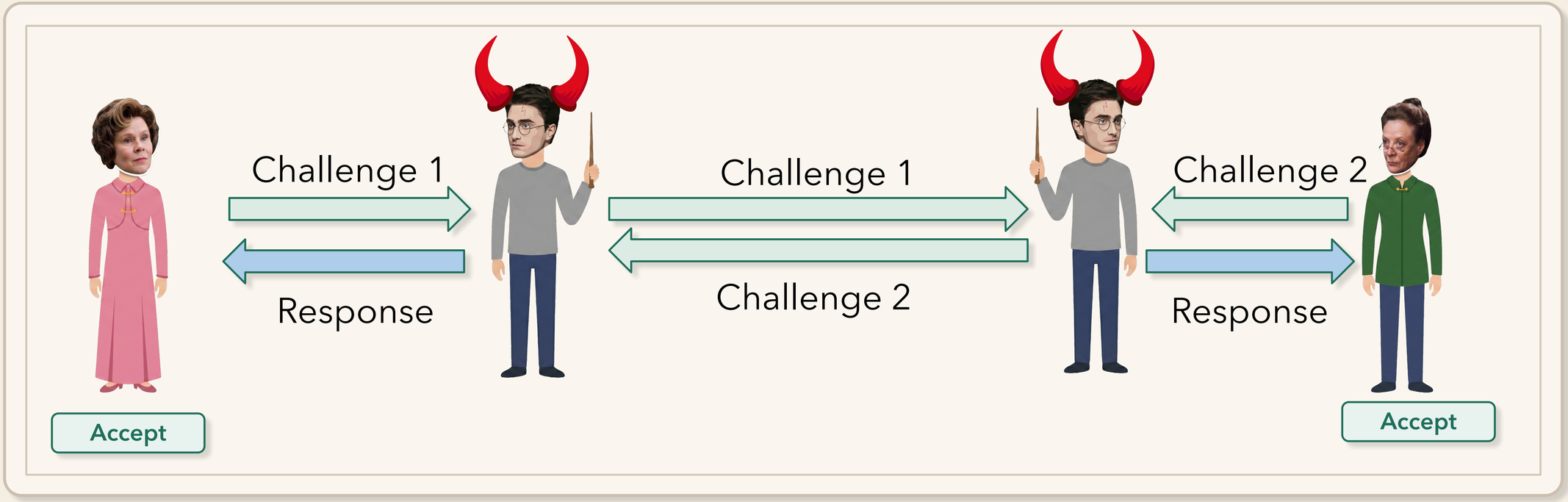
Position Verification

> The core building block of position-based cryptography.



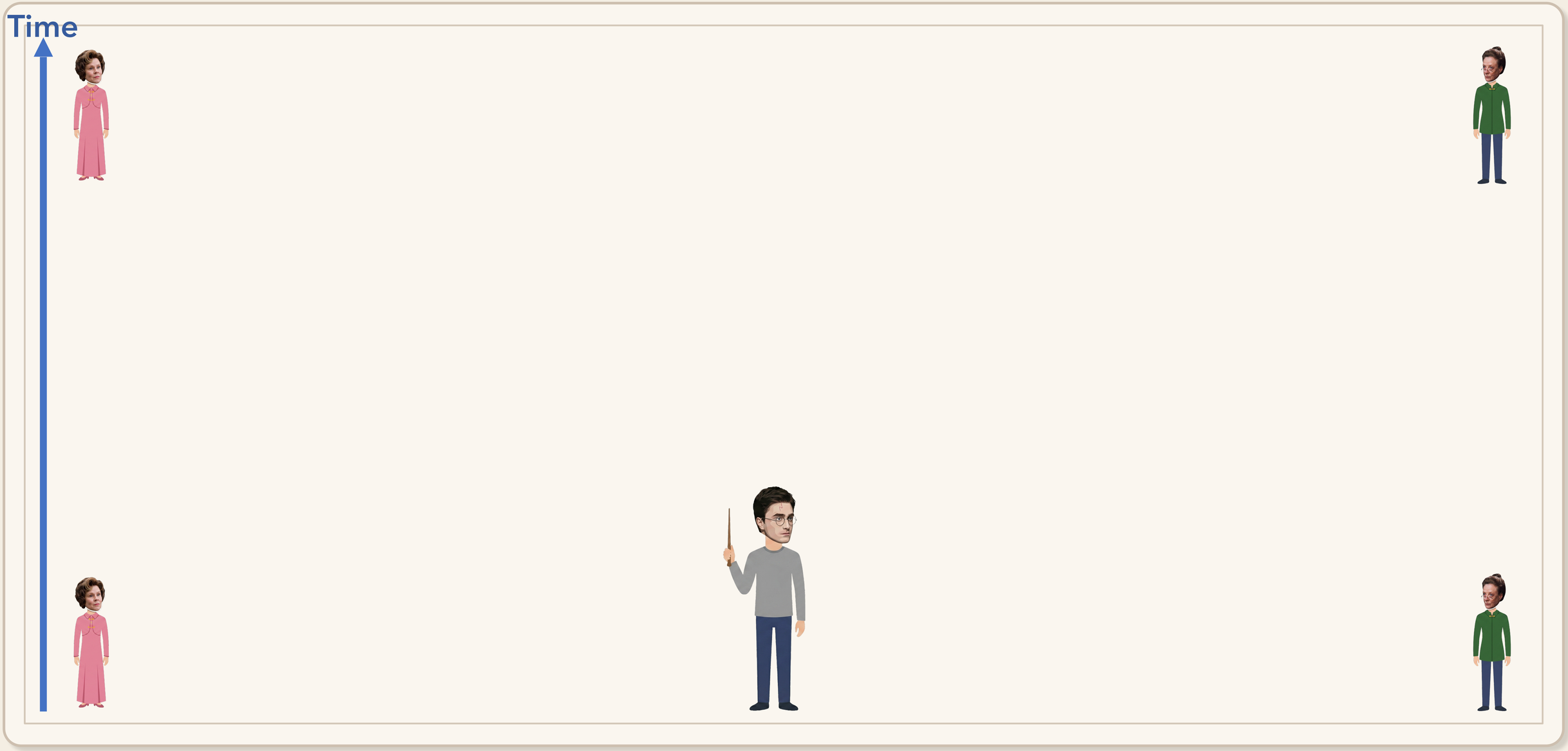
Position Verification

> The core building block of position-based cryptography.

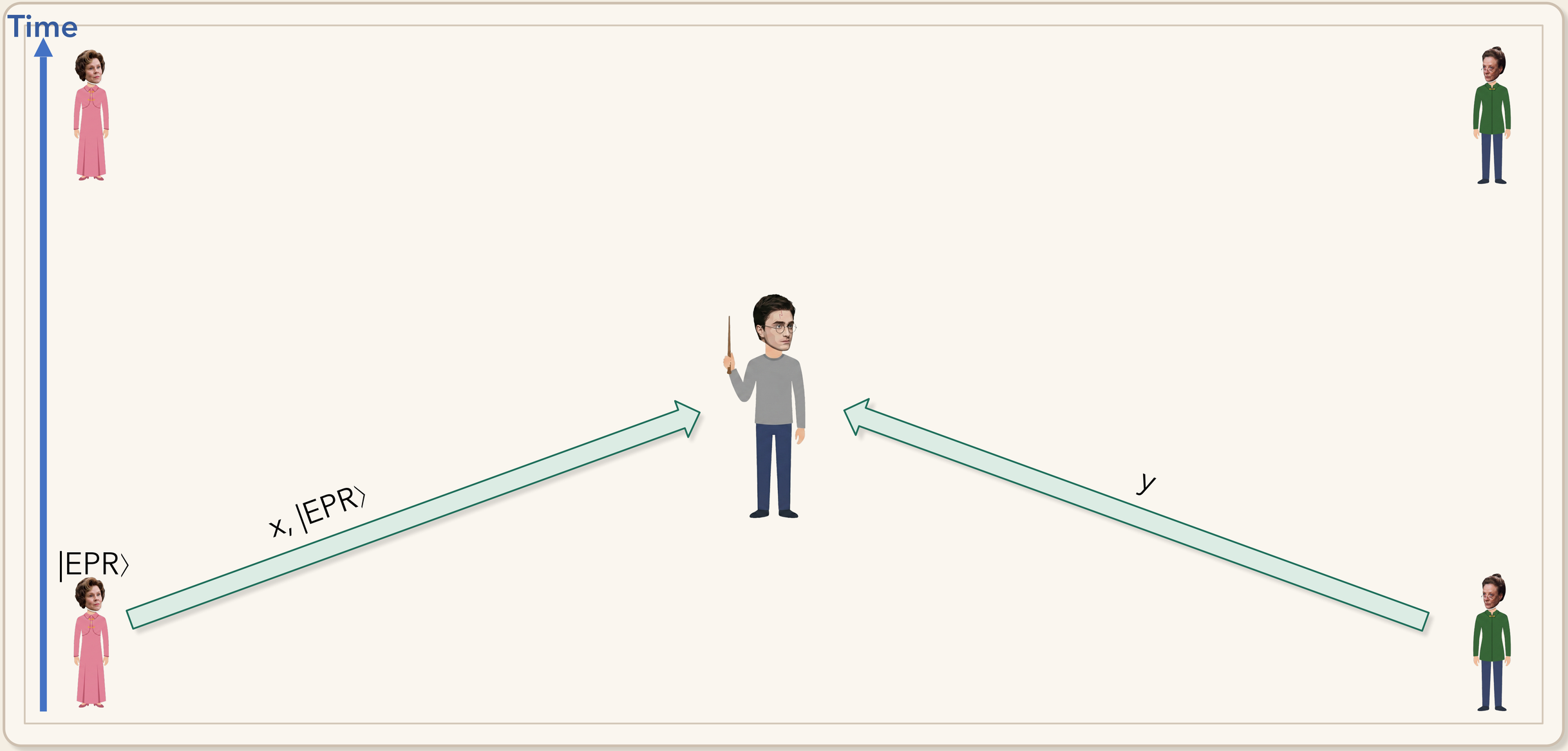


Classically, secure schemes don't exist ([CGMO'09]).
But what about quantum schemes?

A Quantum Position Verification Scheme

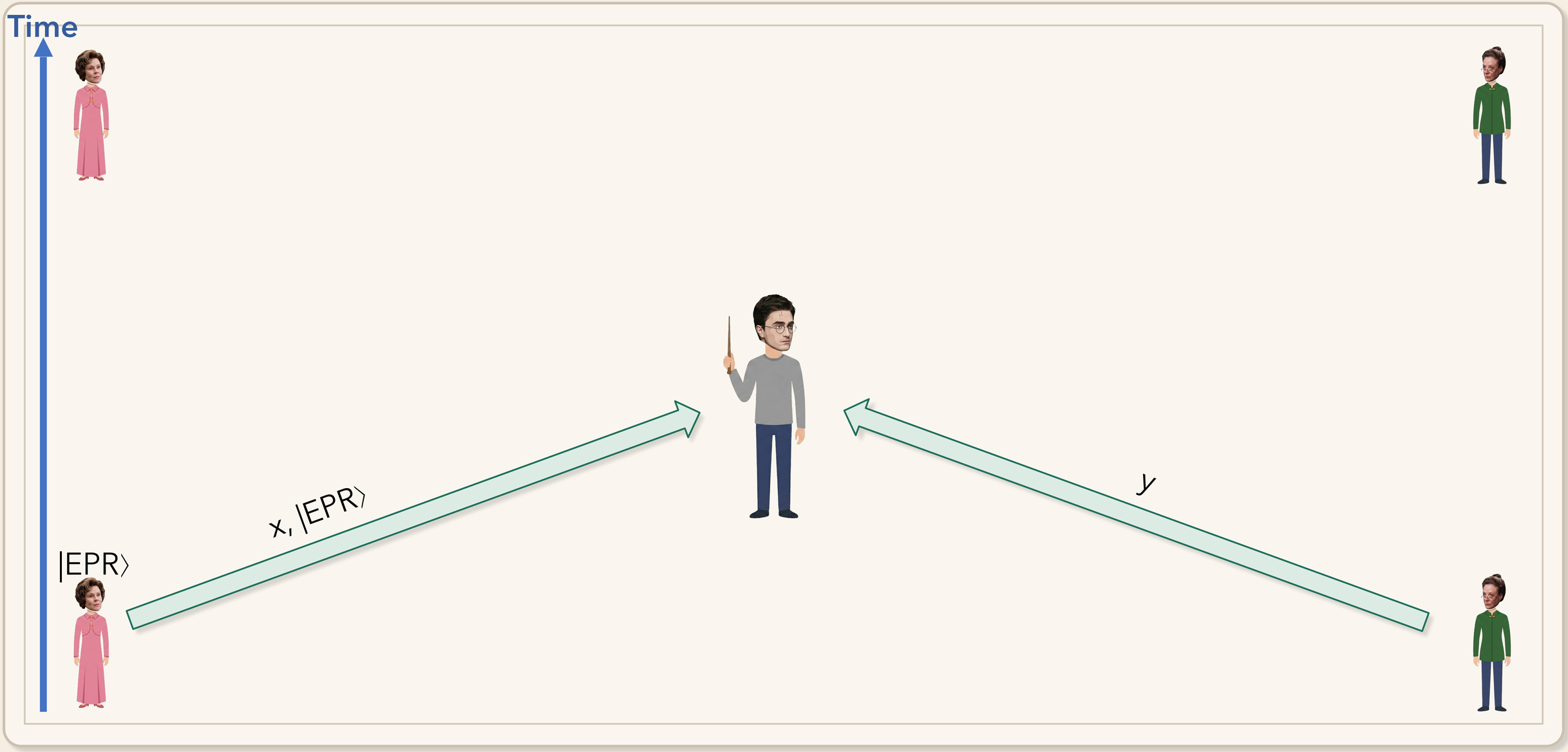


A Quantum Position Verification Scheme



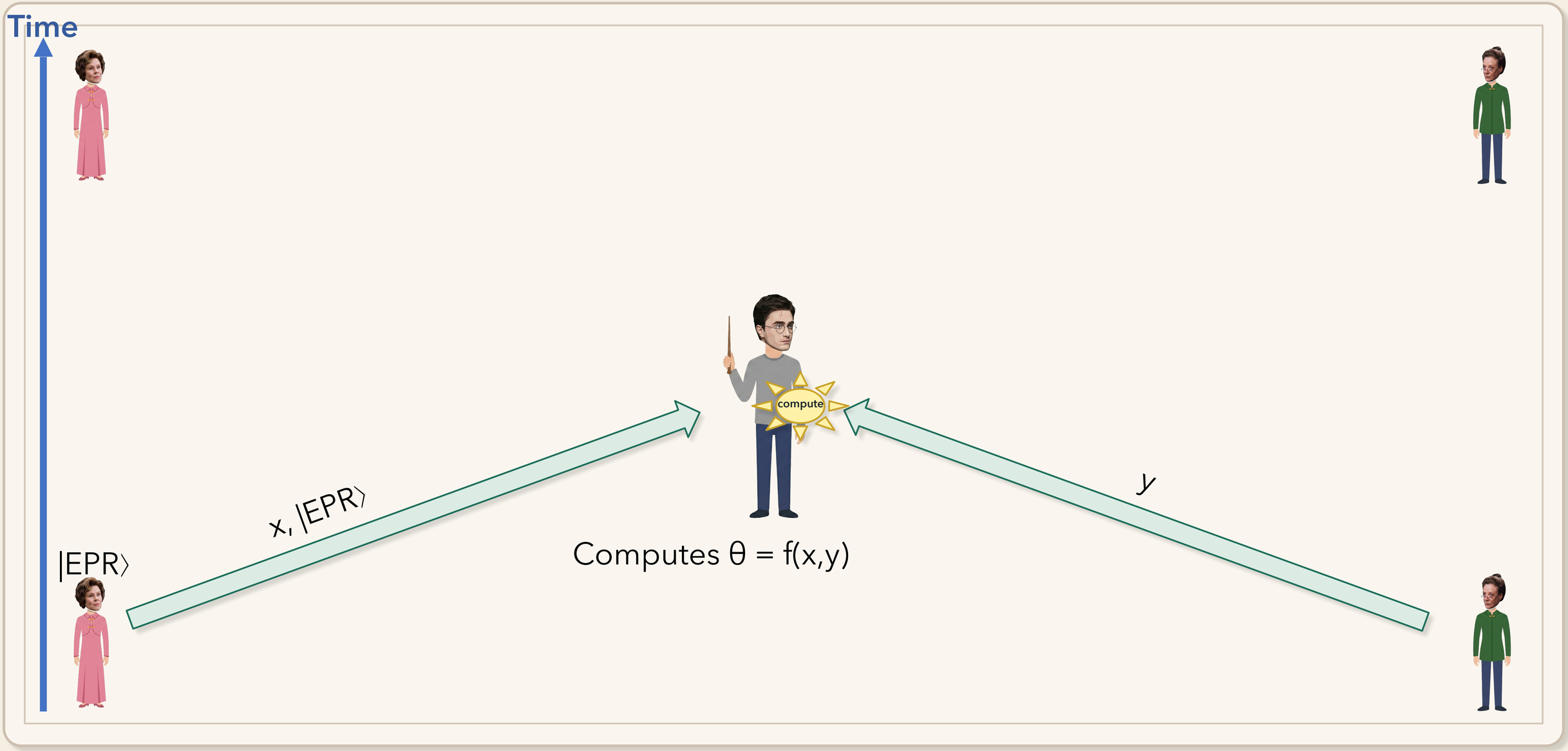
A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"



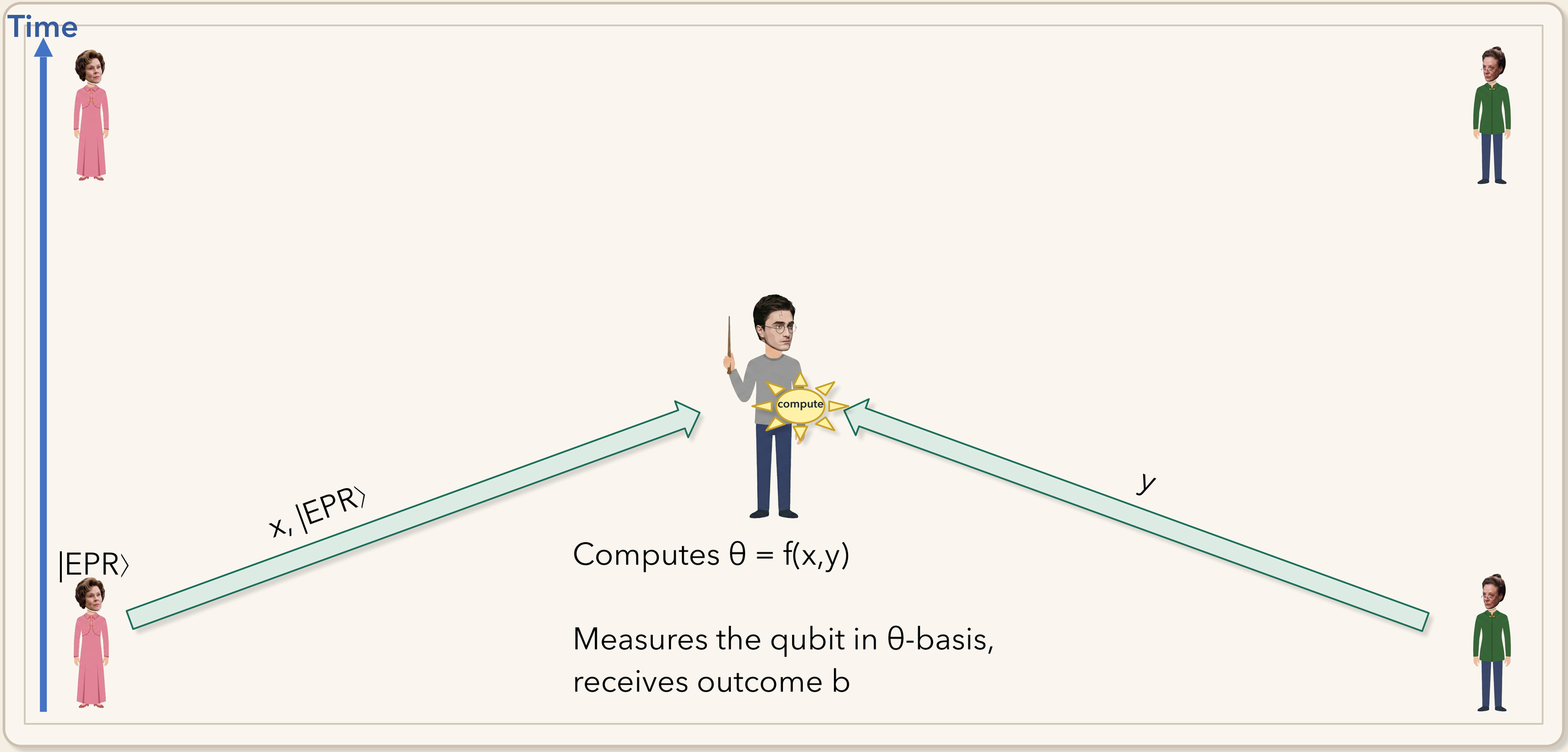
A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"

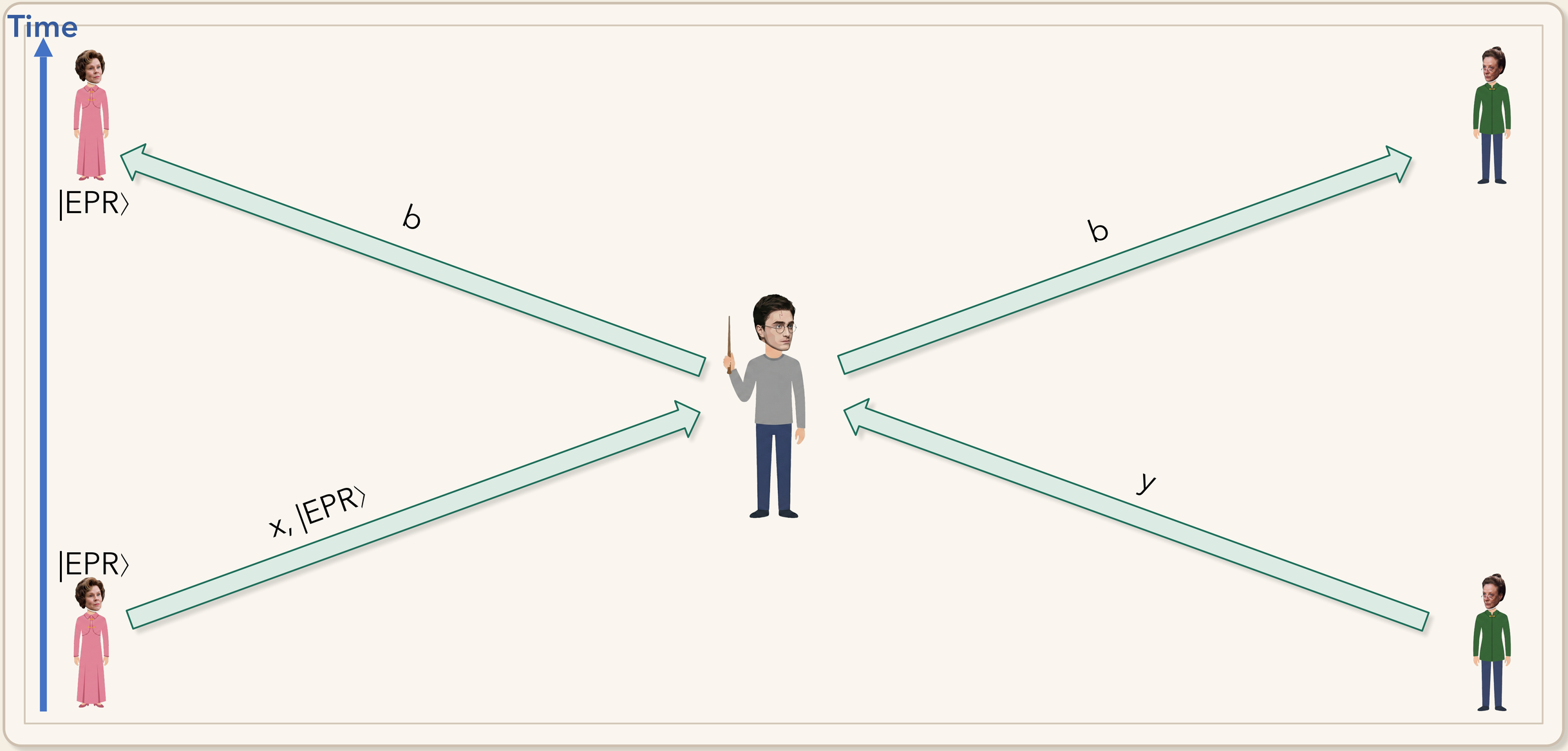


A Quantum Position Verification Scheme

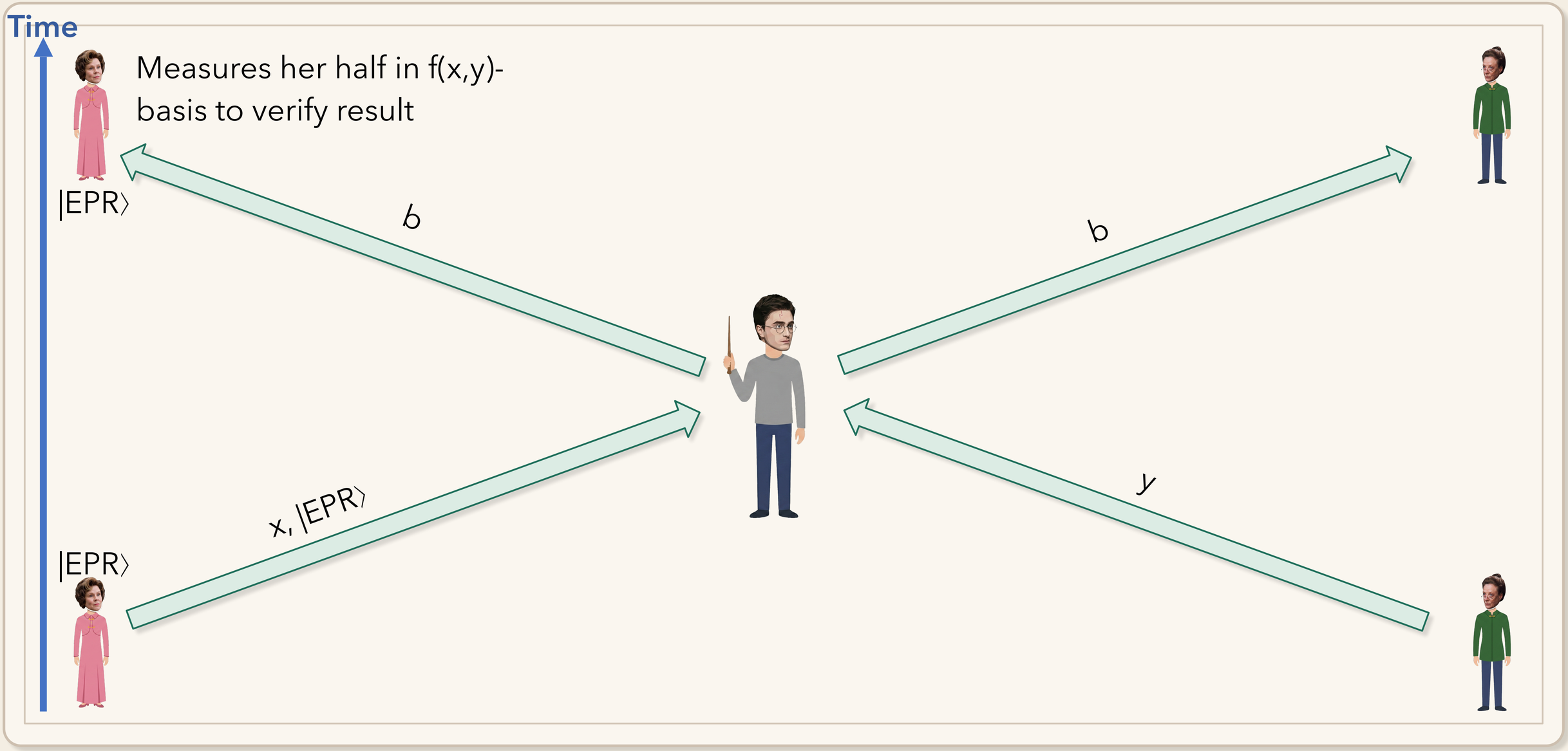
"Purified f-measure/f-BB84"



A Quantum Position Verification Scheme

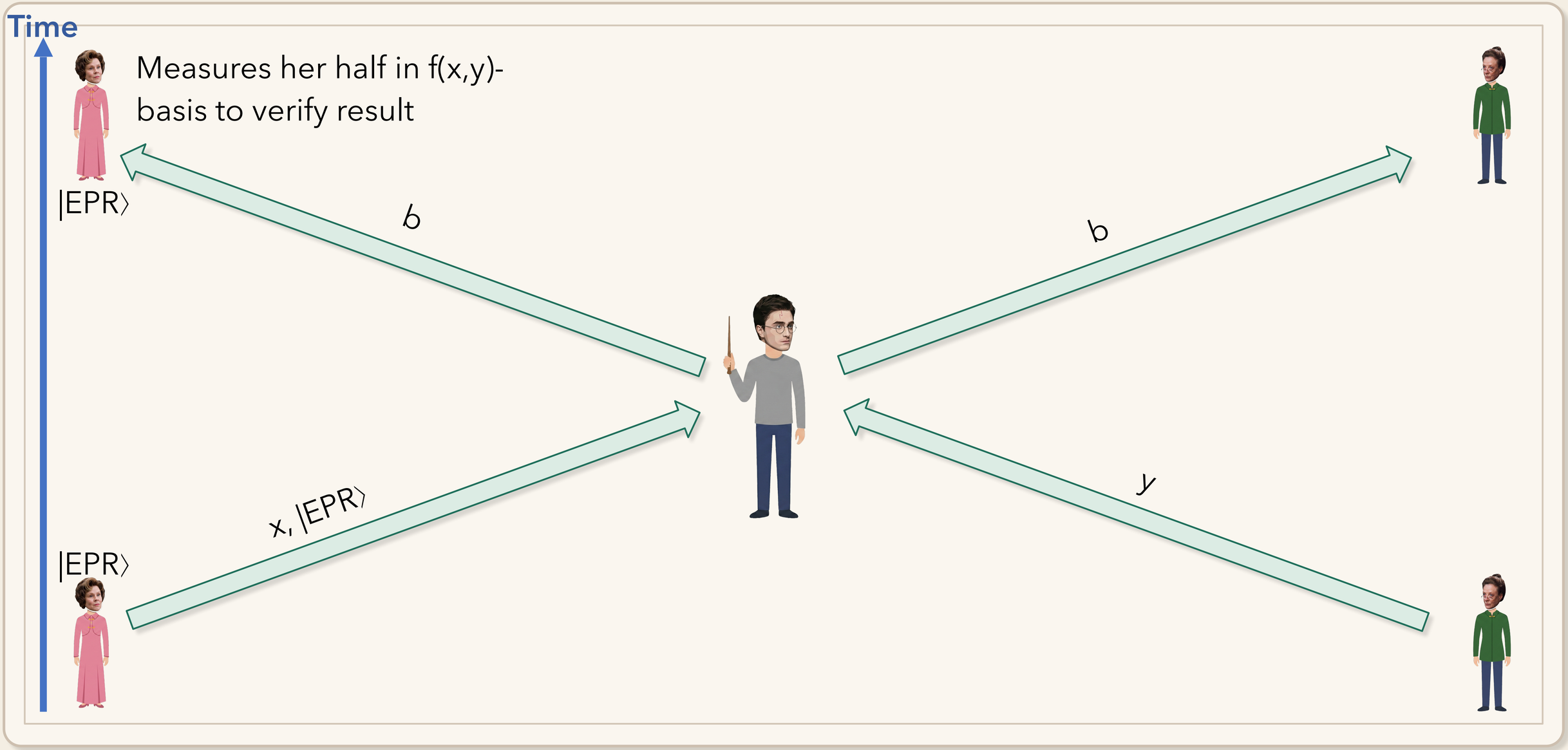


A Quantum Position Verification Scheme

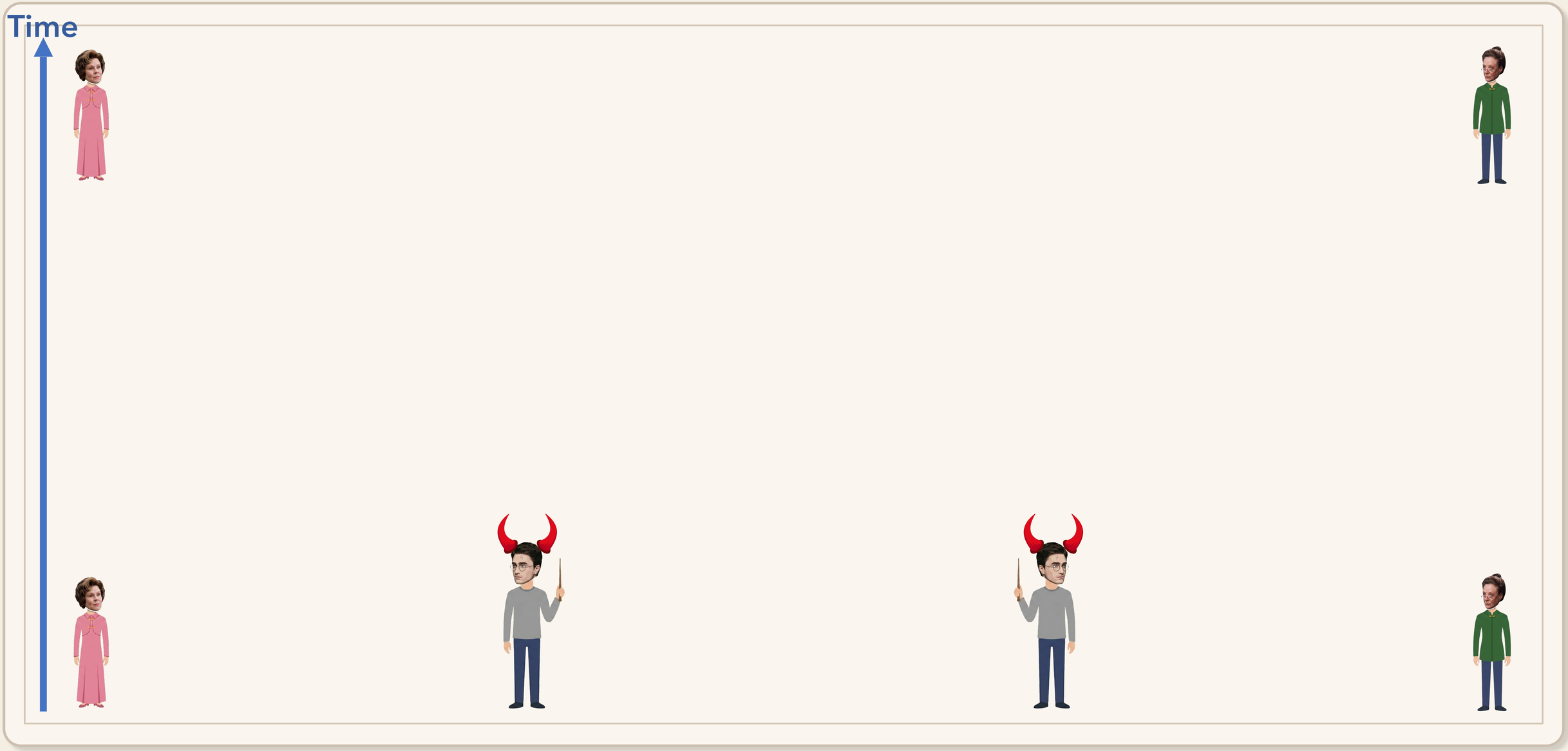


A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"

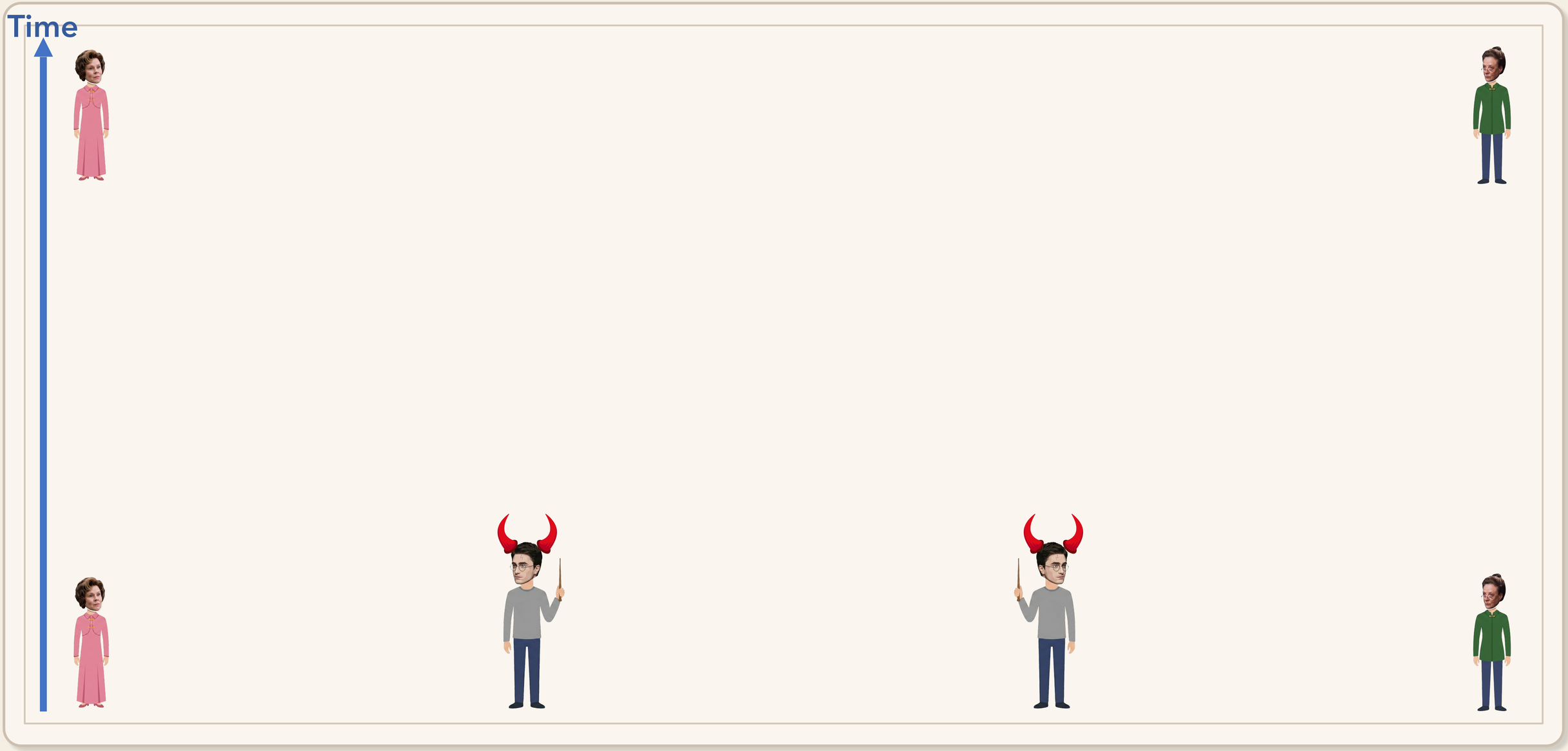


A Quantum Position Verification Scheme

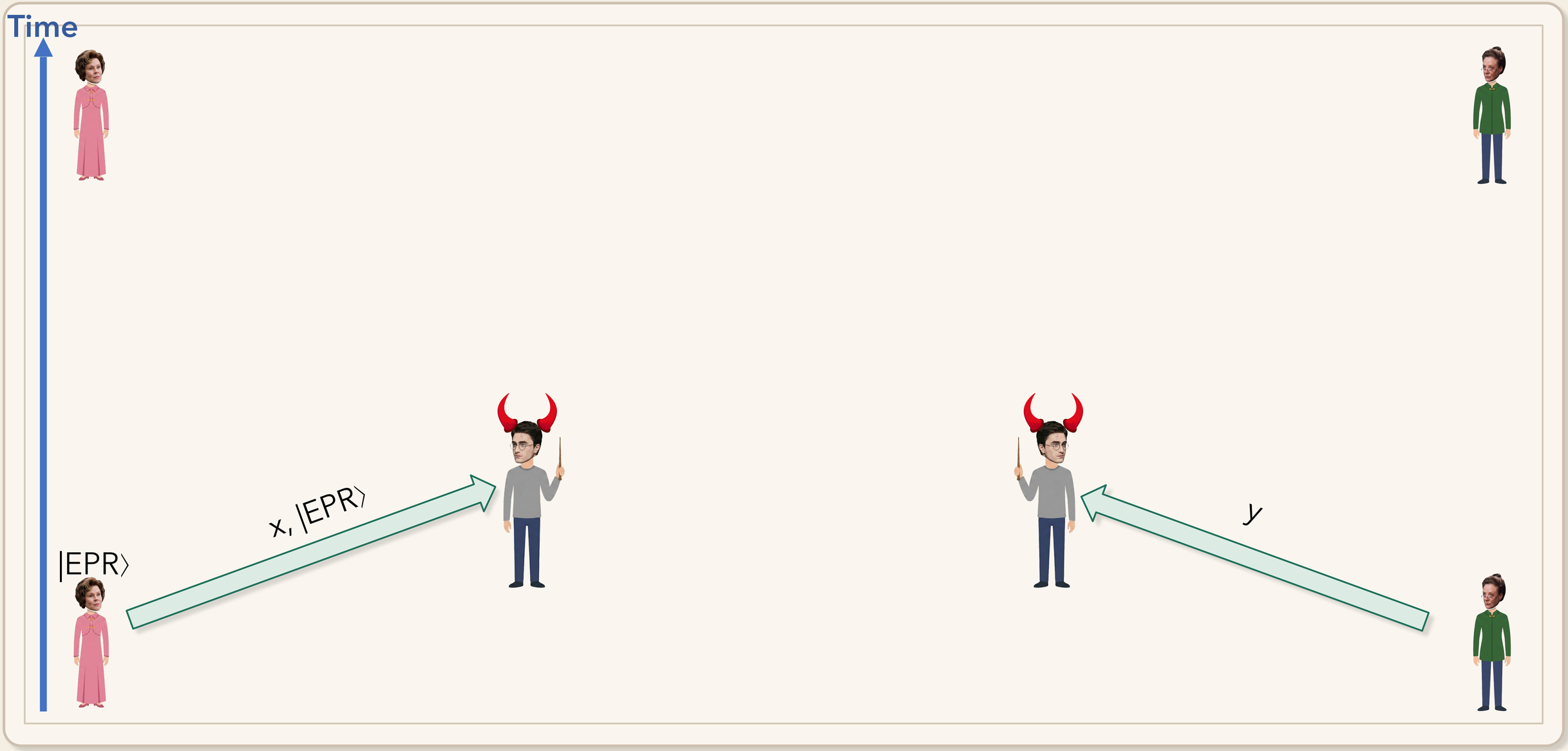


A Quantum Position Verification Scheme

“Purified f-measure/f-BB84”

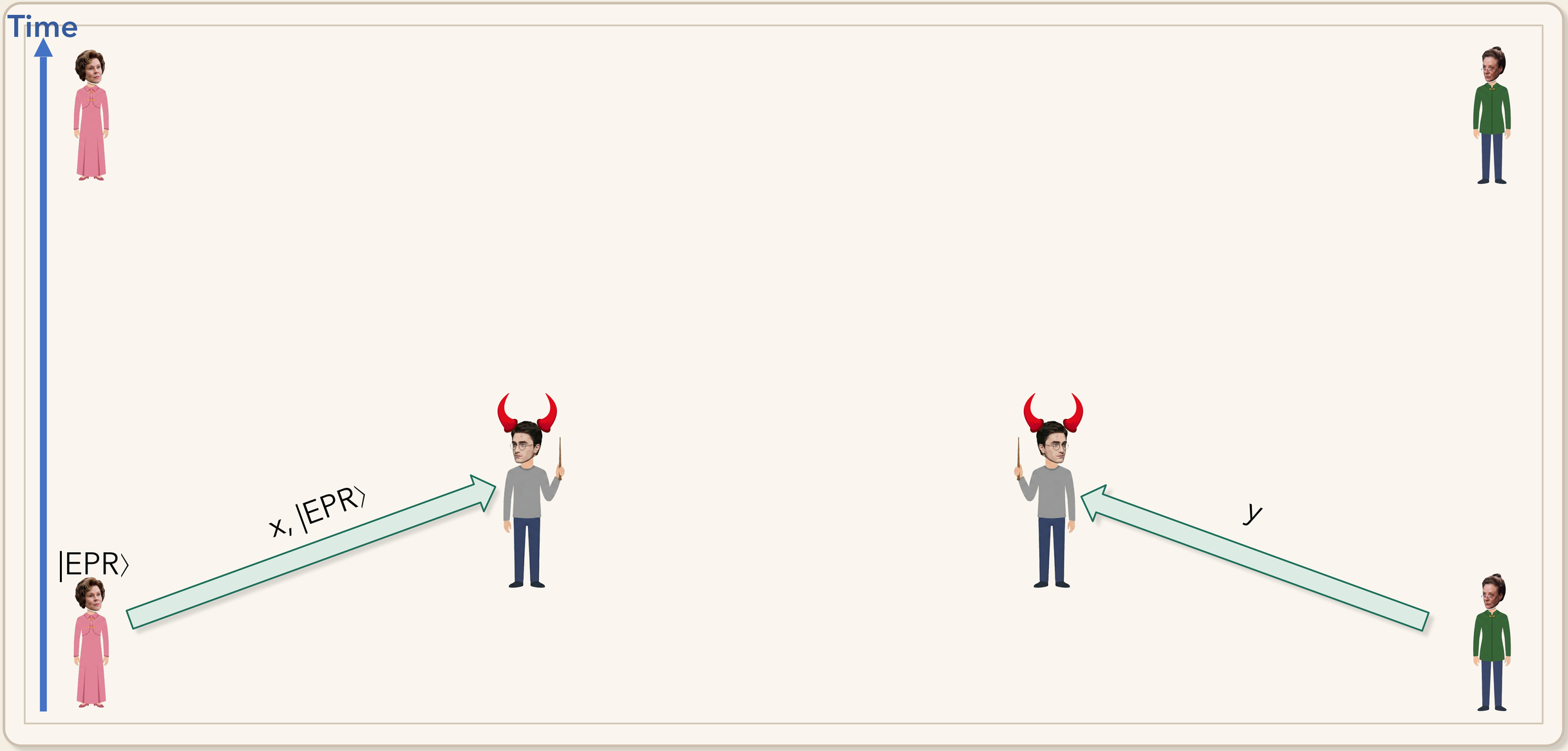


A Quantum Position Verification Scheme

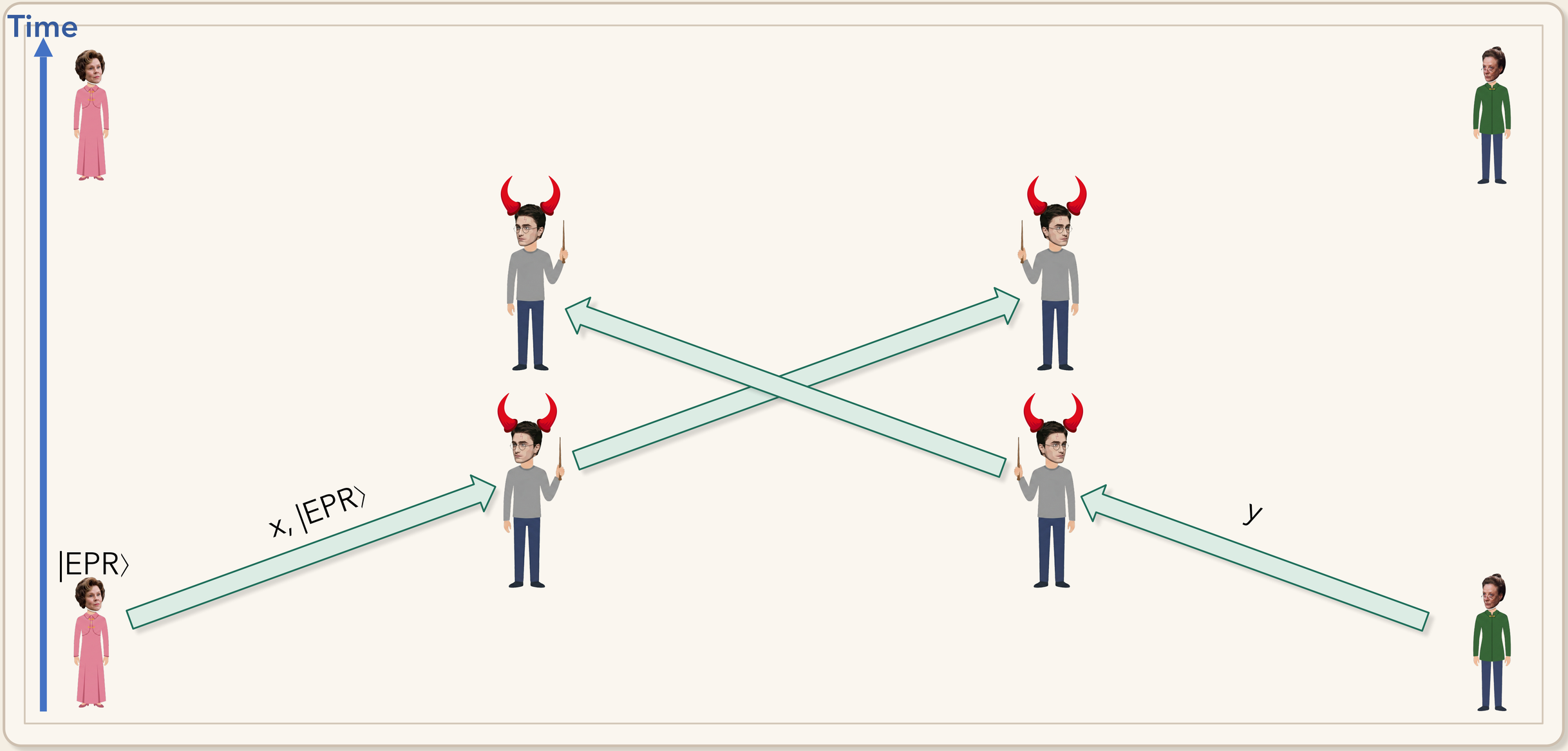


A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"

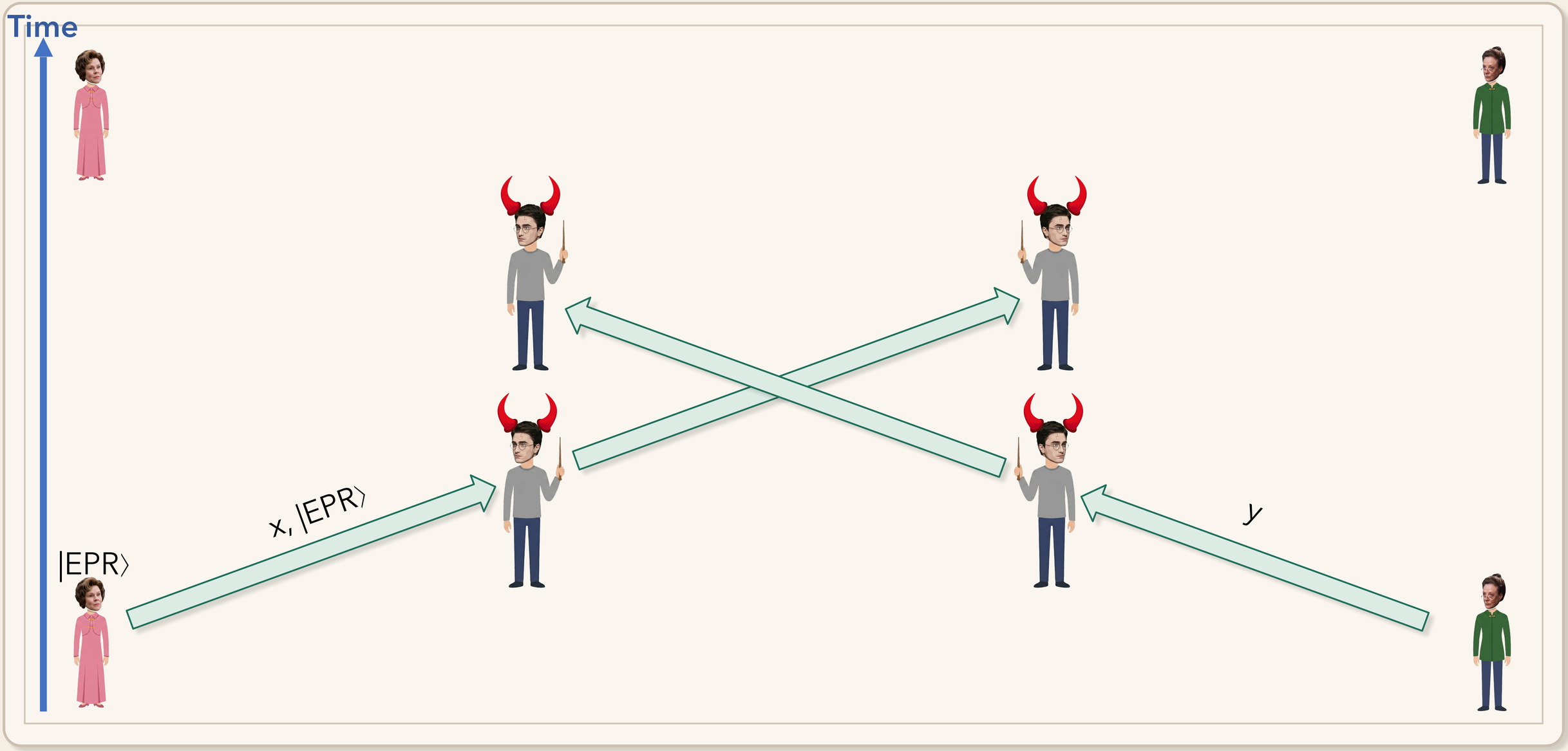


A Quantum Position Verification Scheme

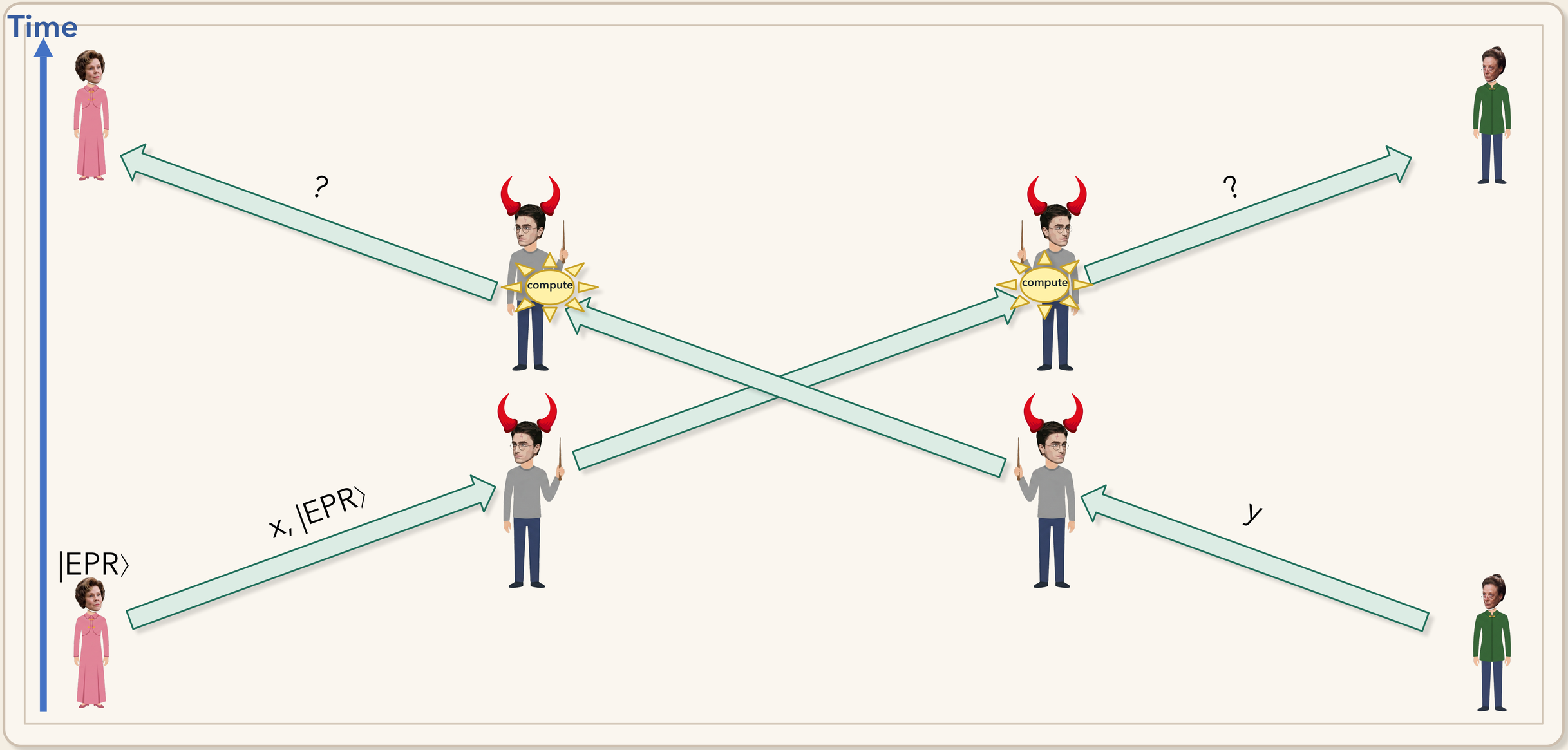


A Quantum Position Verification Scheme

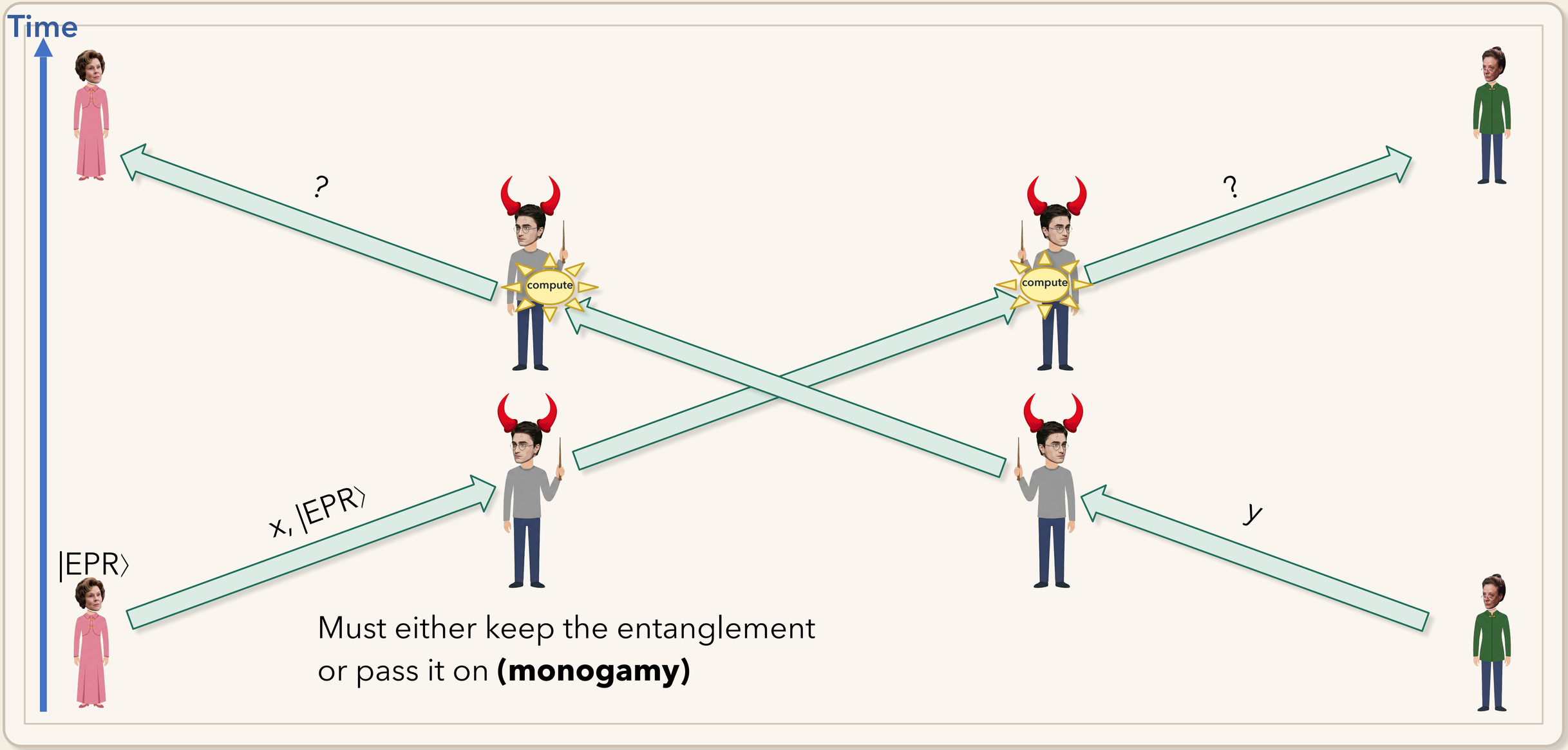
"Purified f-measure/f-BB84"



A Quantum Position Verification Scheme

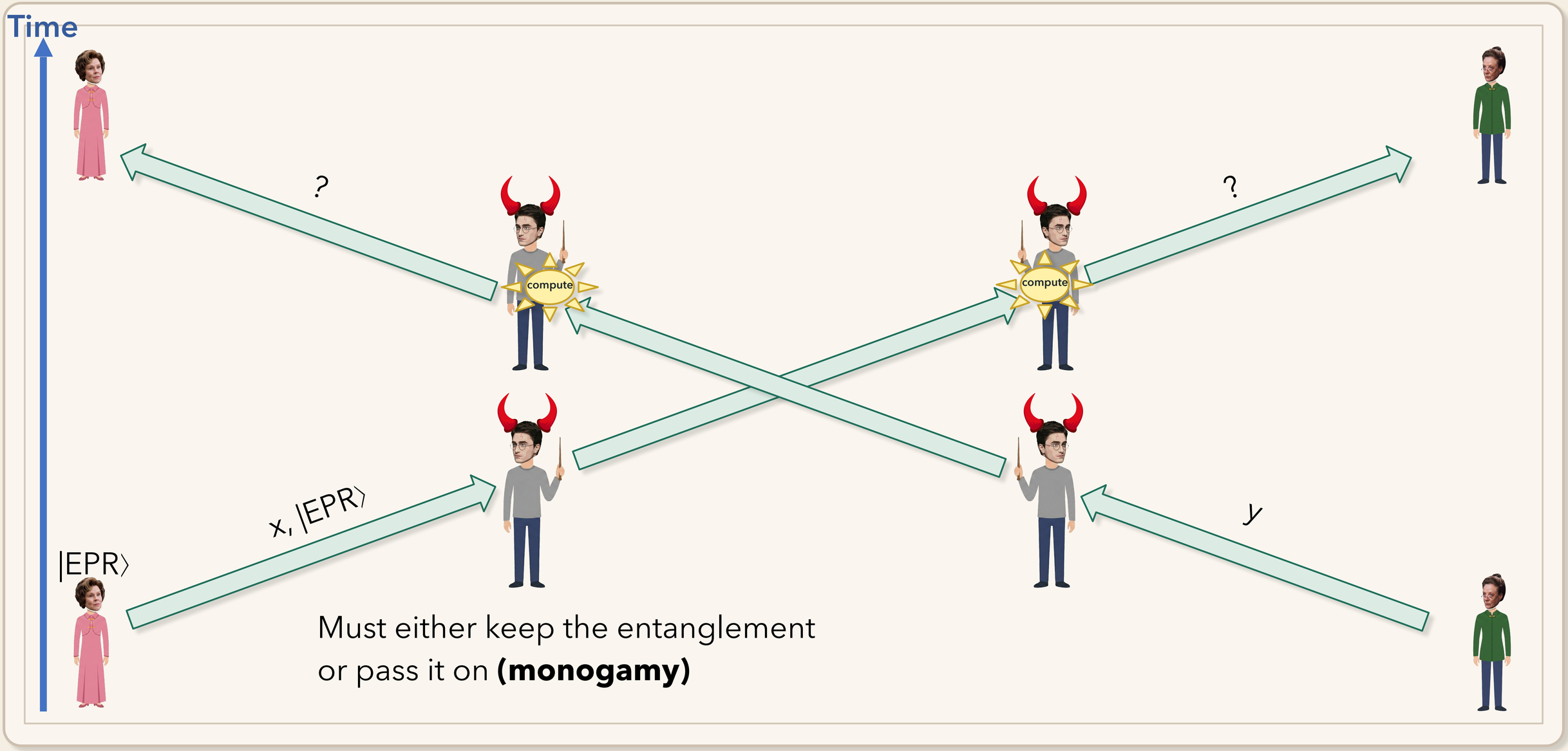


A Quantum Position Verification Scheme

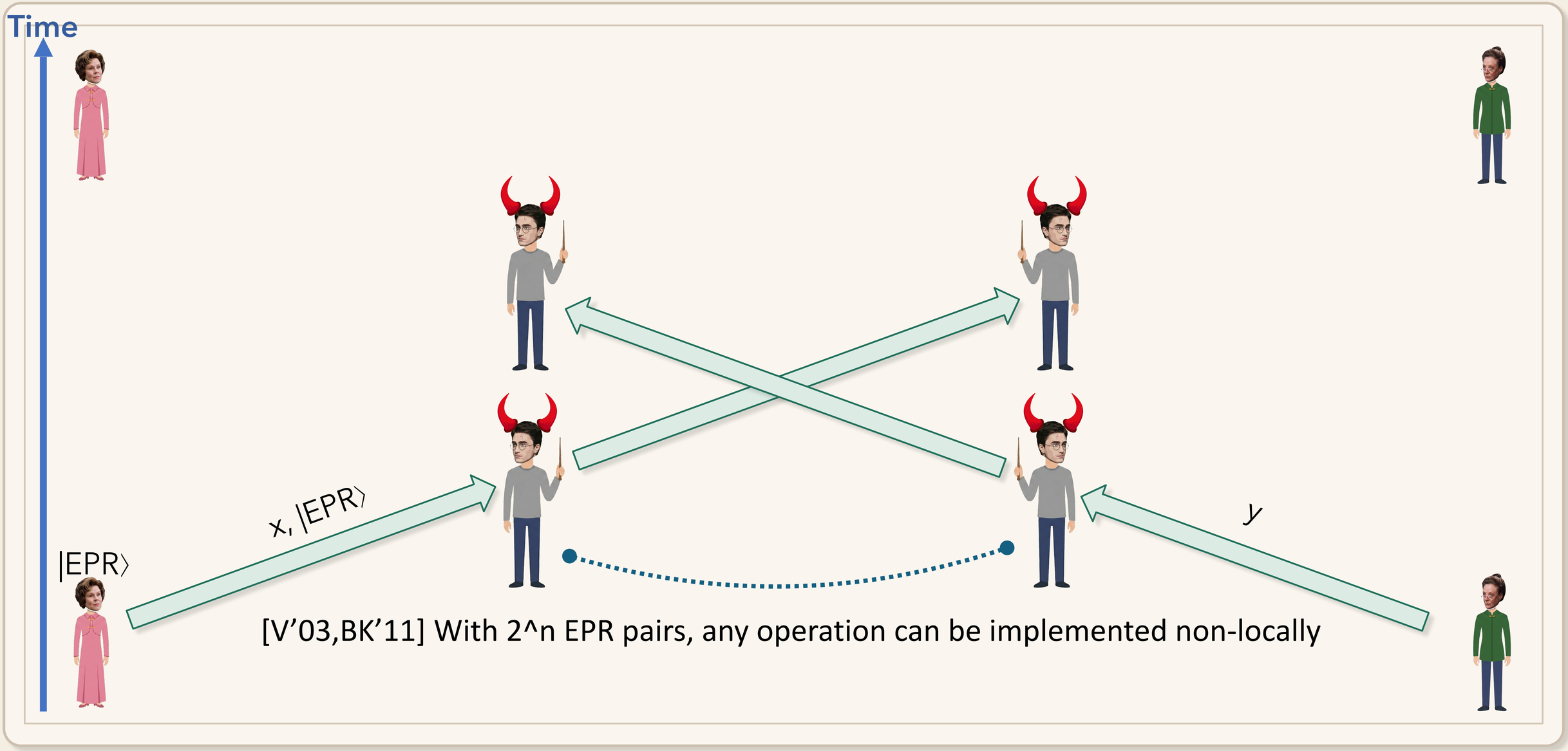


A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"

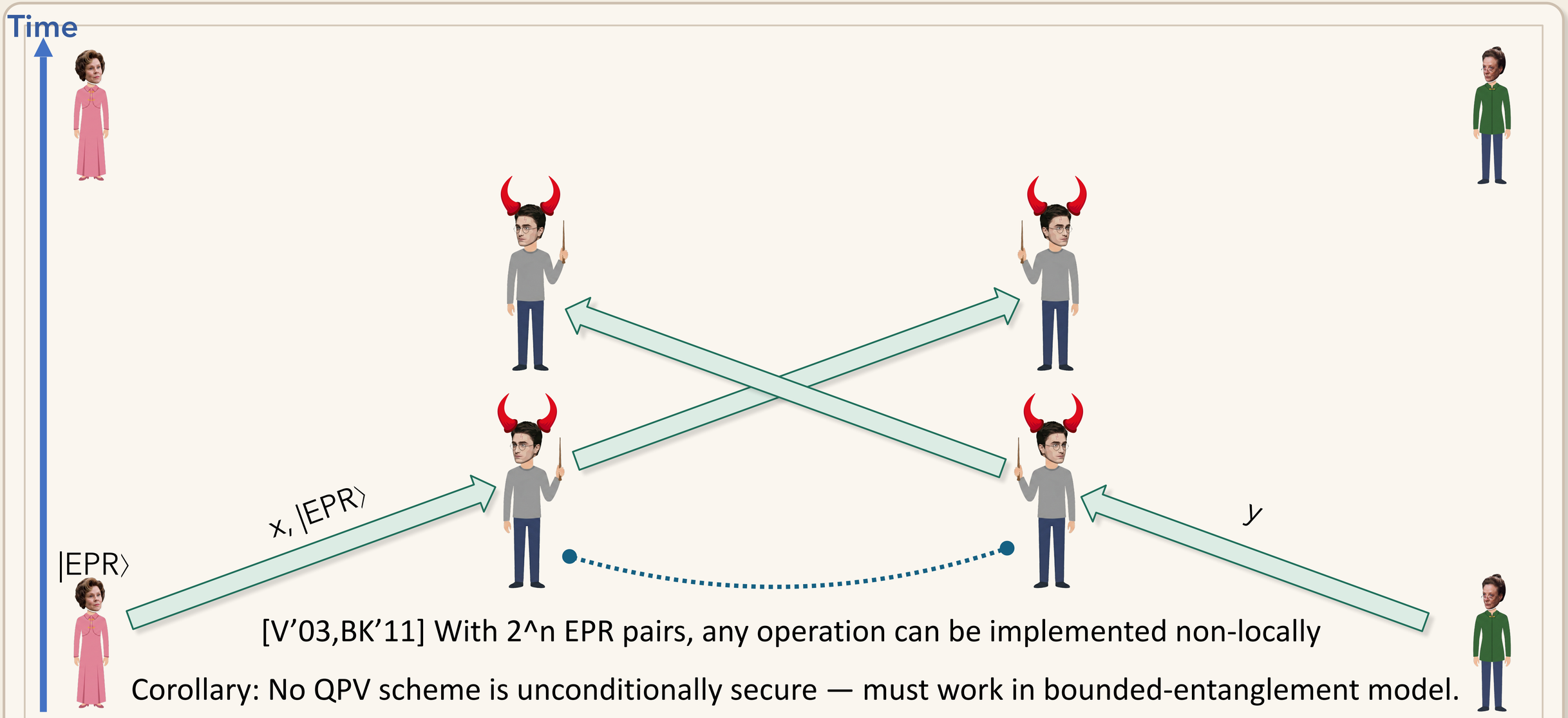


A Quantum Position Verification Scheme



[V'03,BK'11] With 2^n EPR pairs, any operation can be implemented non-locally

A Quantum Position Verification Scheme

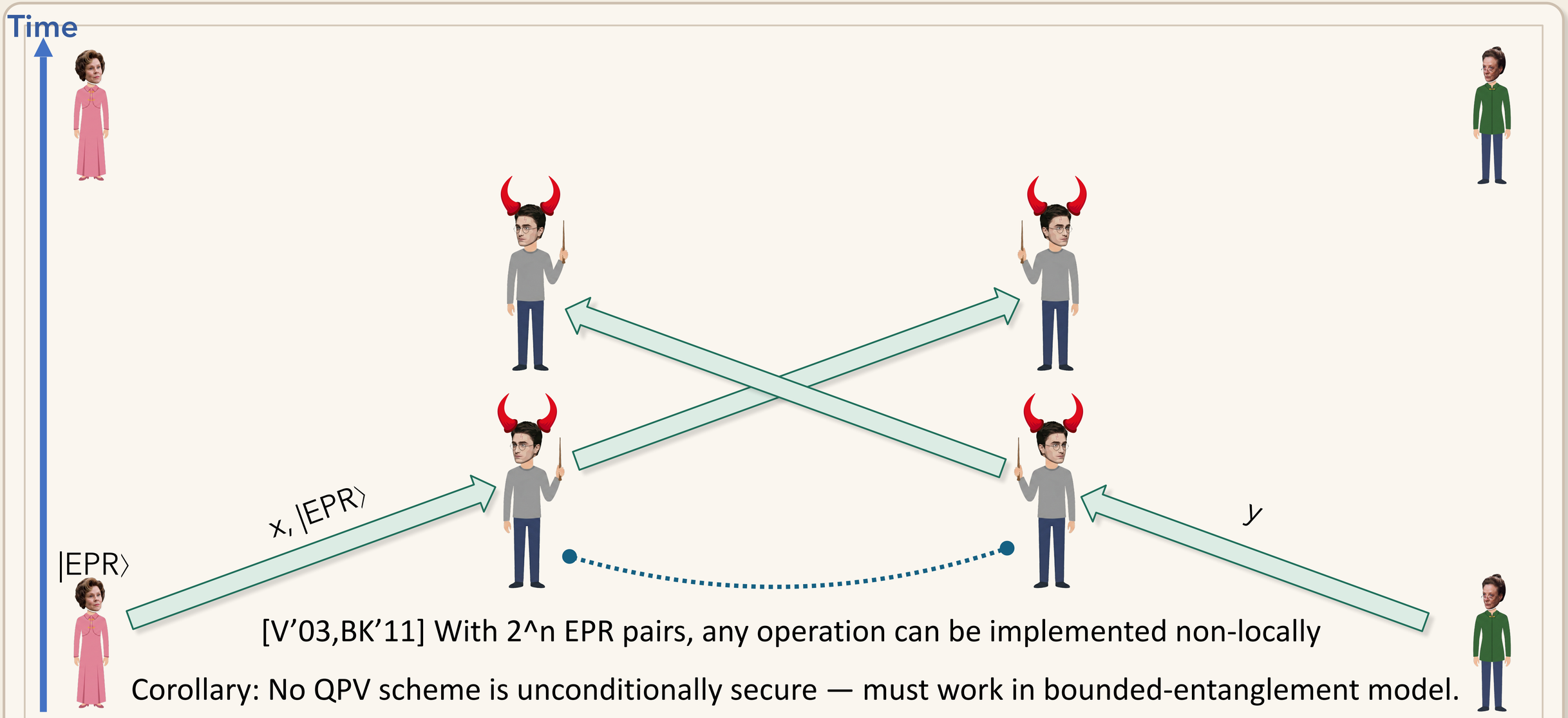


[V'03,BK'11] With 2^n EPR pairs, any operation can be implemented non-locally

Corollary: No QPV scheme is unconditionally secure — must work in bounded-entanglement model.

A Quantum Position Verification Scheme

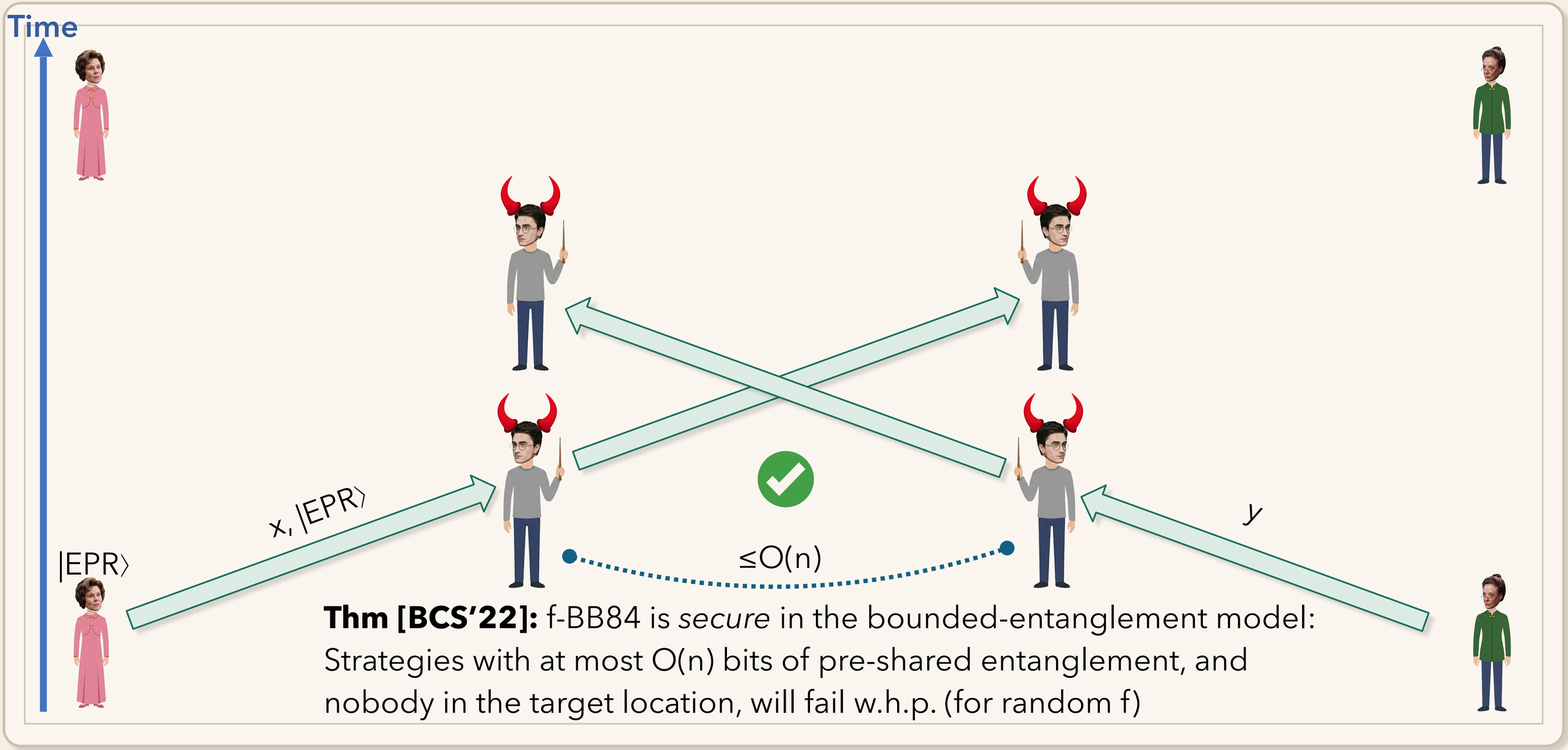
"Purified f-measure/f-BB84"



[V'03,BK'11] With 2^n EPR pairs, any operation can be implemented non-locally

Corollary: No QPV scheme is unconditionally secure — must work in bounded-entanglement model.

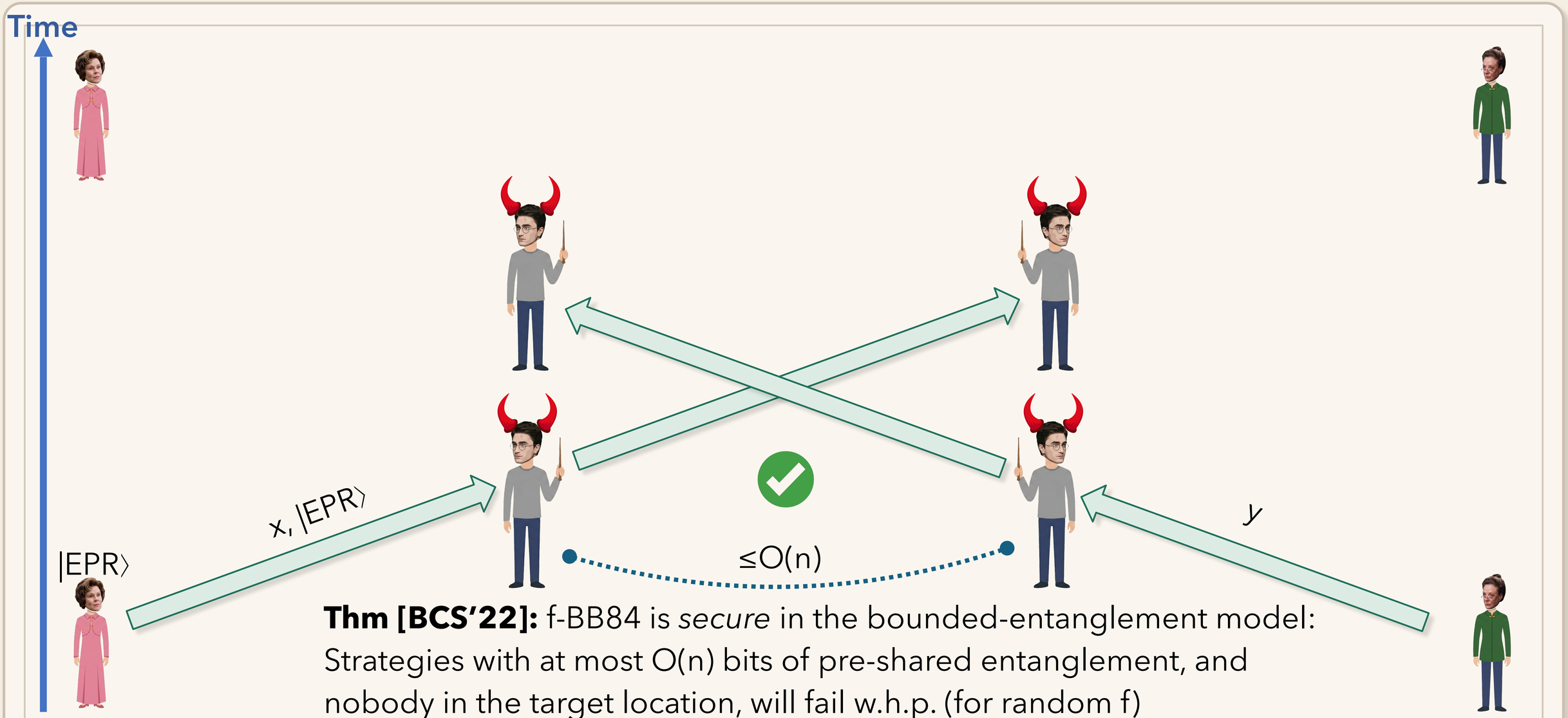
A Quantum Position Verification Scheme



Thm [BCS'22]: f-BB84 is *secure* in the bounded-entanglement model: Strategies with at most O(n) bits of pre-shared entanglement, and nobody in the target location, will fail w.h.p. (for random f)

A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"



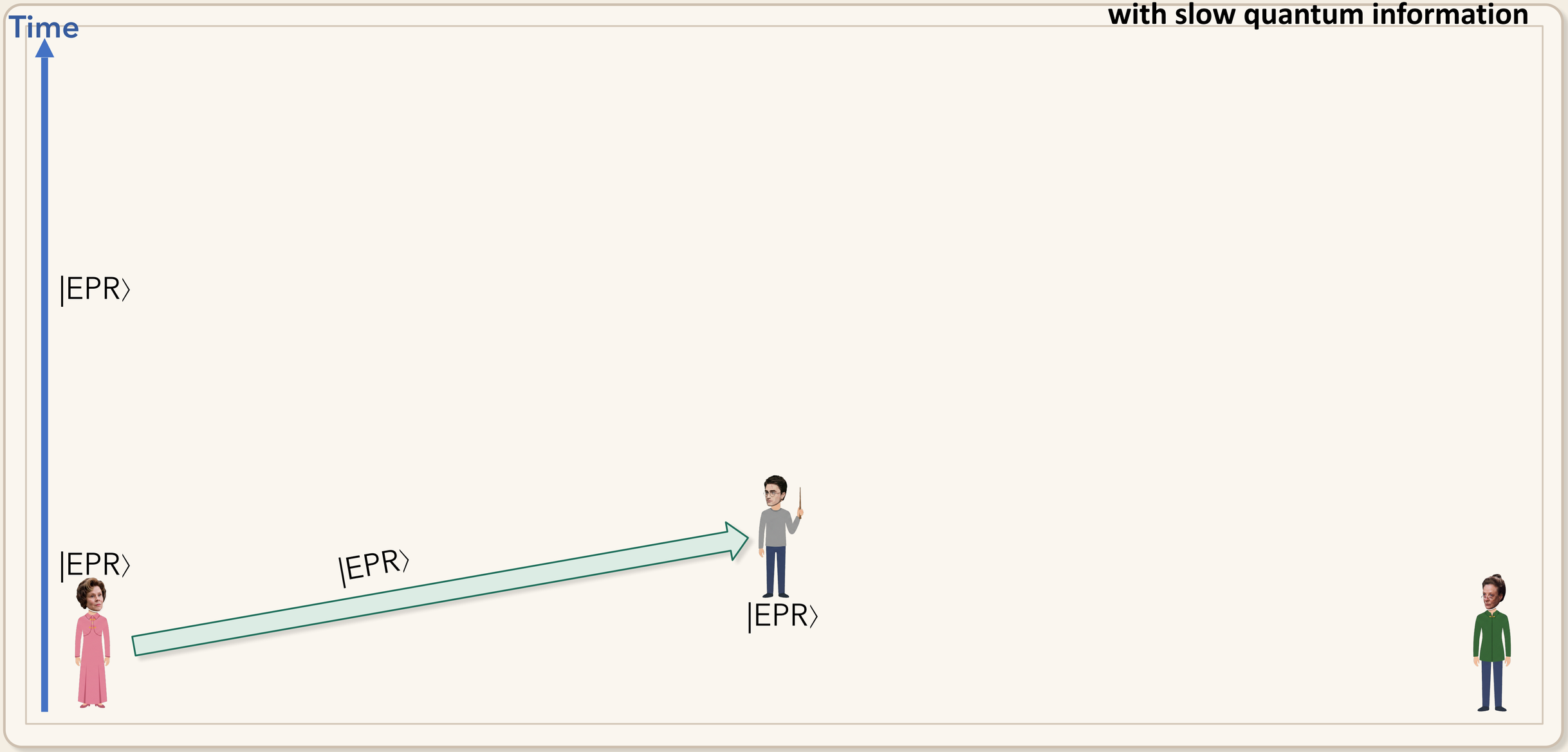
Thm [BCS'22]: f-BB84 is *secure* in the bounded-entanglement model: Strategies with at most O(n) bits of pre-shared entanglement, and nobody in the target location, will fail w.h.p. (for random f)

A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"
with slow quantum information

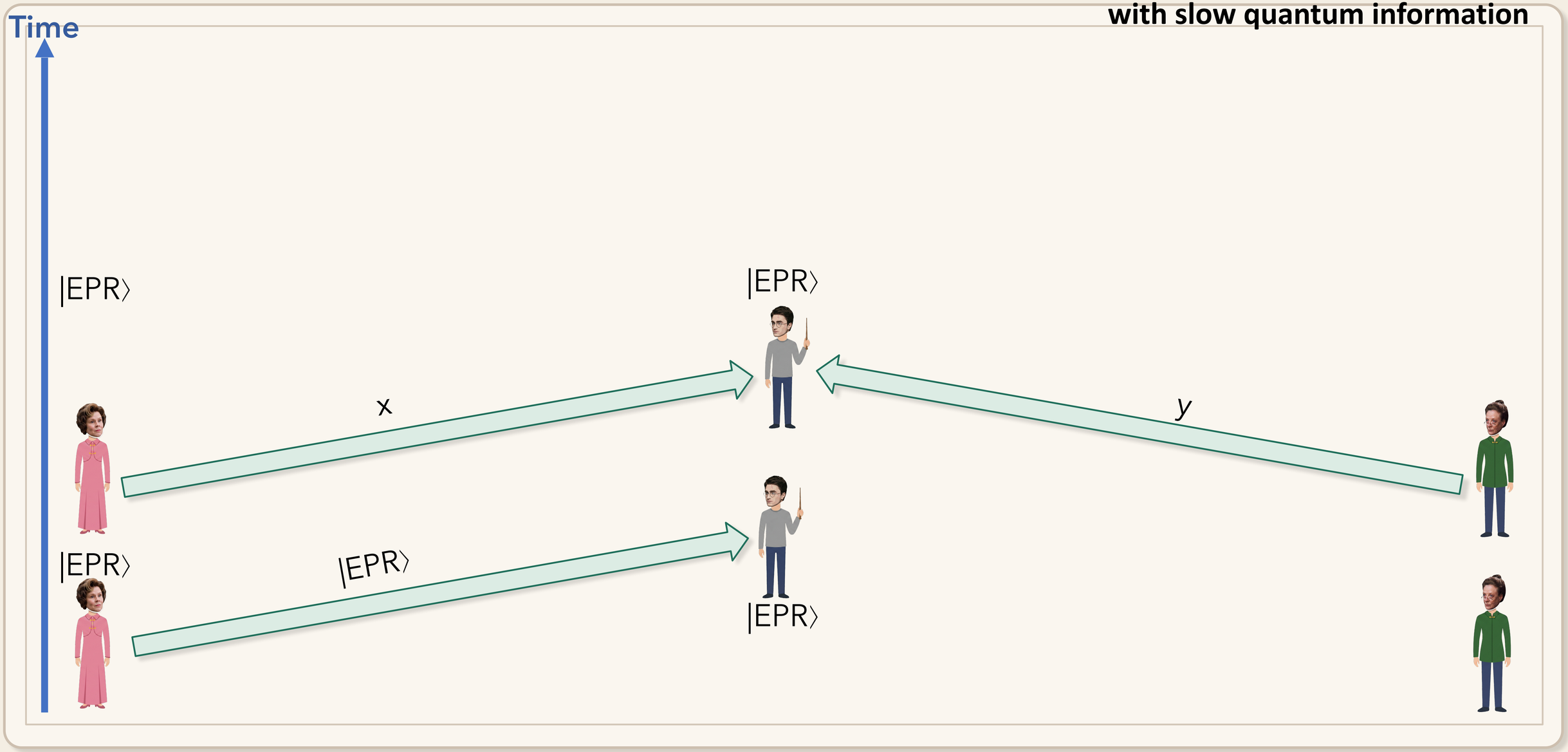
A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"
with slow quantum information



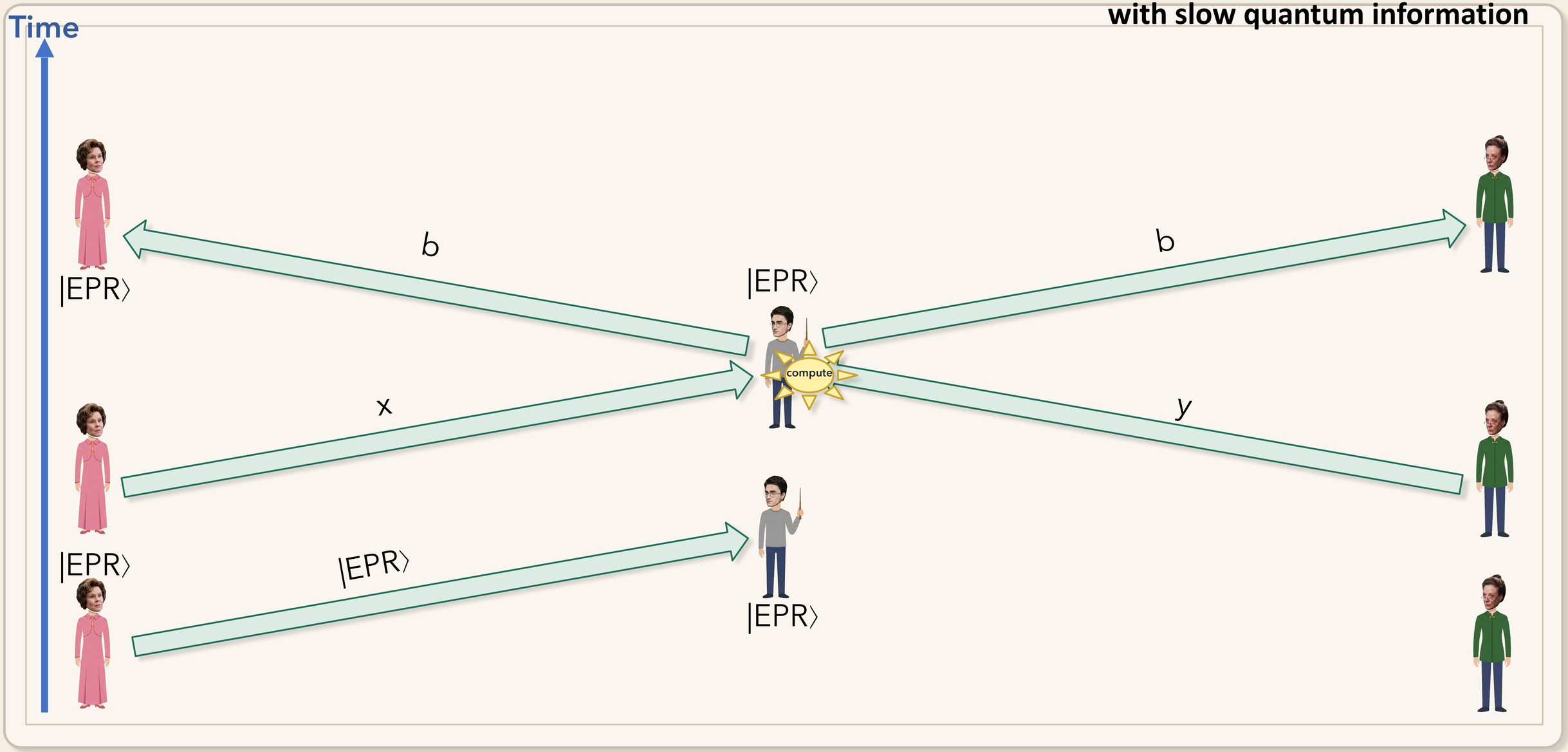
A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"
with slow quantum information



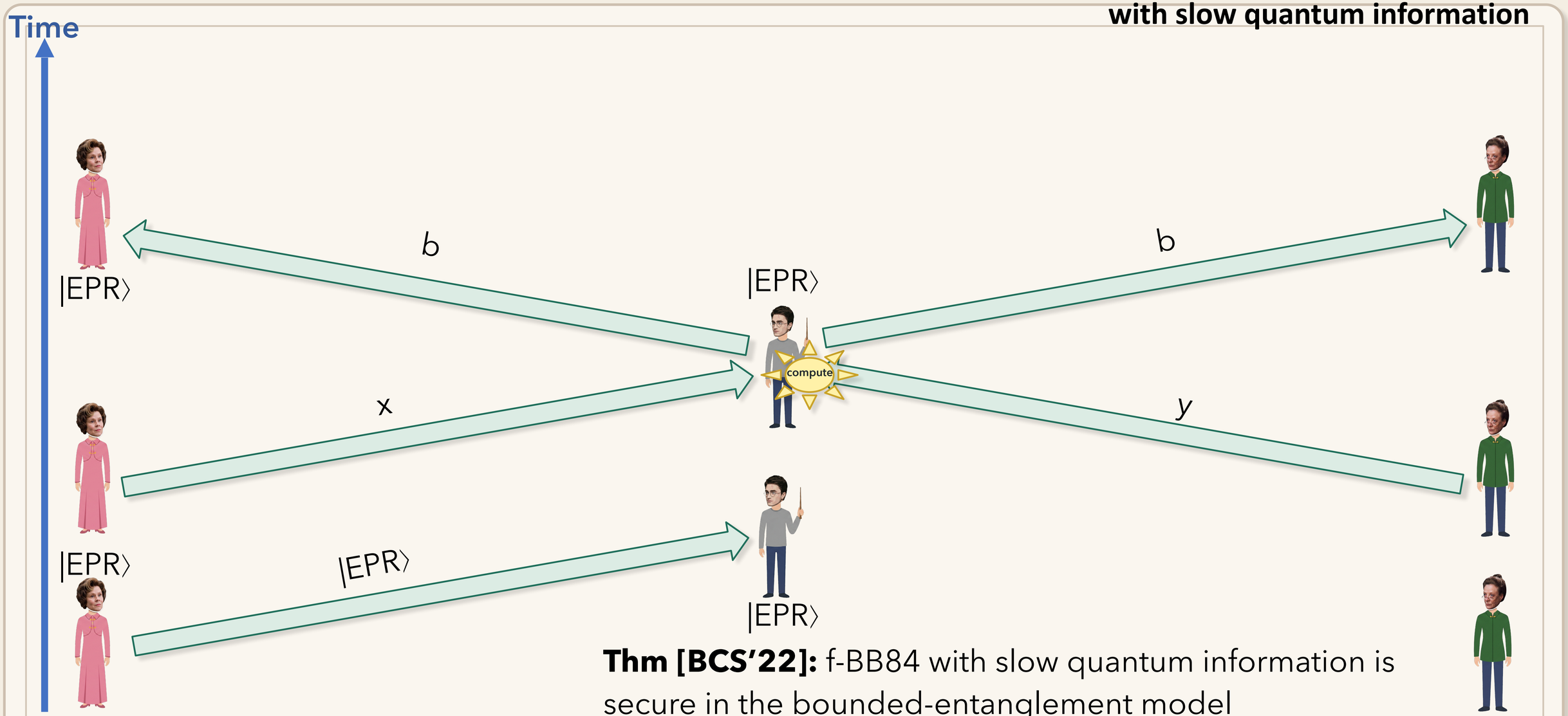
A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"
with slow quantum information



A Quantum Position Verification Scheme

"Purified f-measure/f-BB84"
with slow quantum information



Thm [BCS'22]: f-BB84 with slow quantum information is secure in the bounded-entanglement model

Visualizing PV in Spacetime

Thm [BCS'22]: f-BB84 is secure in the BEM

Visualizing PV in Spacetime

Thm [BCS'22]: f-BB84 is secure in the BEM

Secure: "Strategies with nobody in the middle should fail with high probability."
=> If protocol succeeds, *something* happened at the middle

Visualizing PV in Spacetime

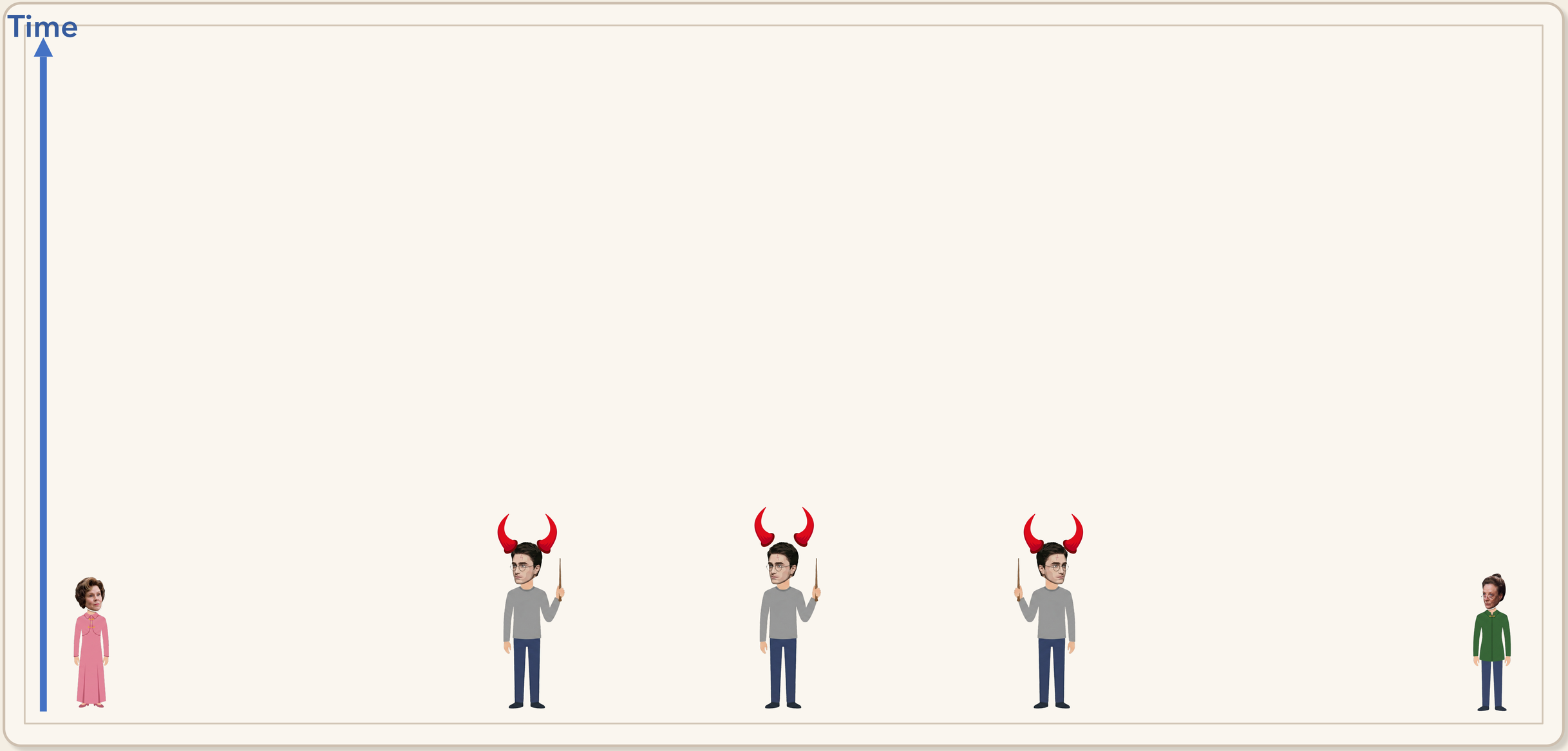
Thm [BCS'22]: f-BB84 is secure in the BEM

Secure: "Strategies with nobody in the middle should fail with high probability."
=> If protocol succeeds, *something* happened at the middle

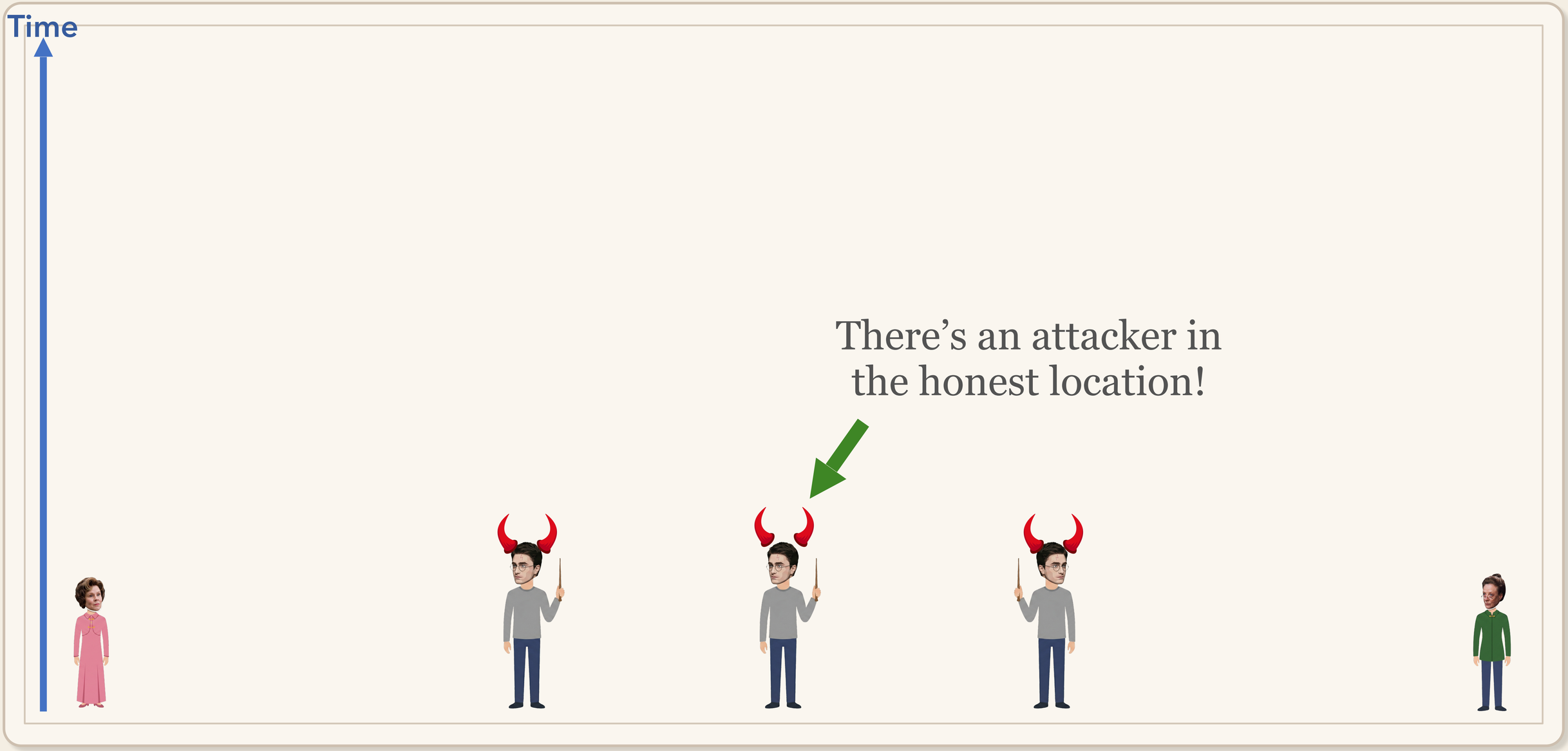
But we'd like to know *more* about what's happening at the middle.

Can we say, e.g., that the qubit must be measured in the middle?

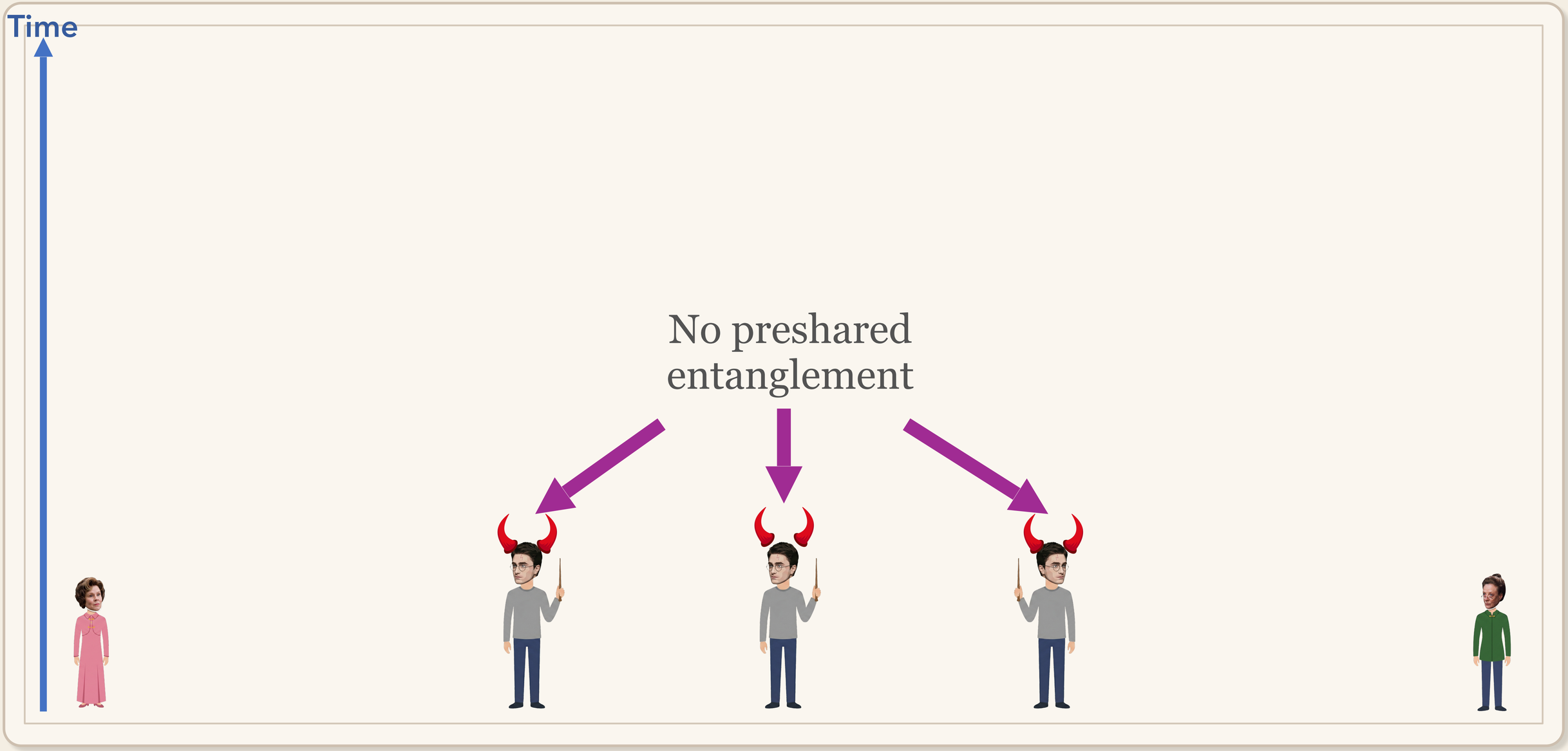
Non-Localizability of f-BB84



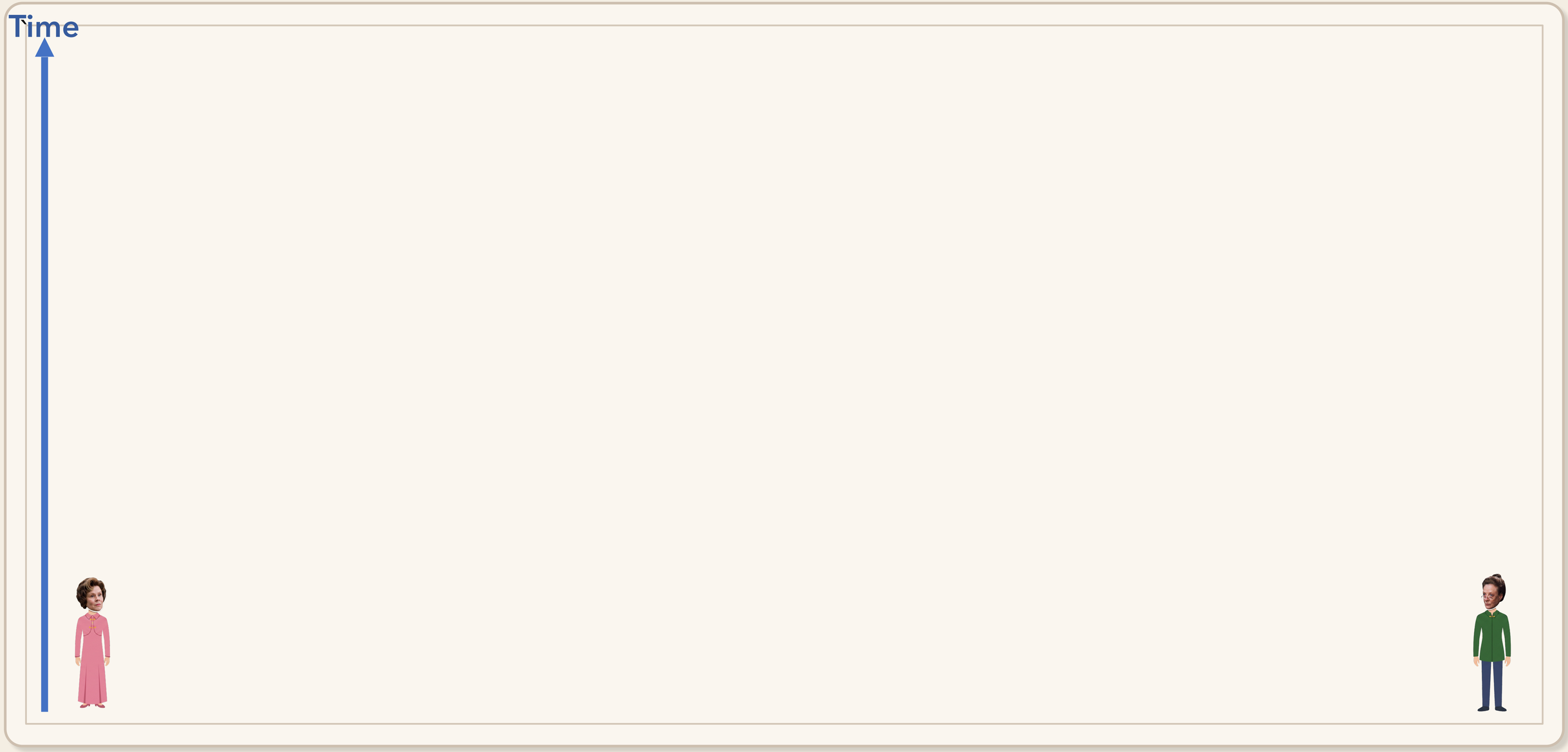
Non-Localizability of f-BB84



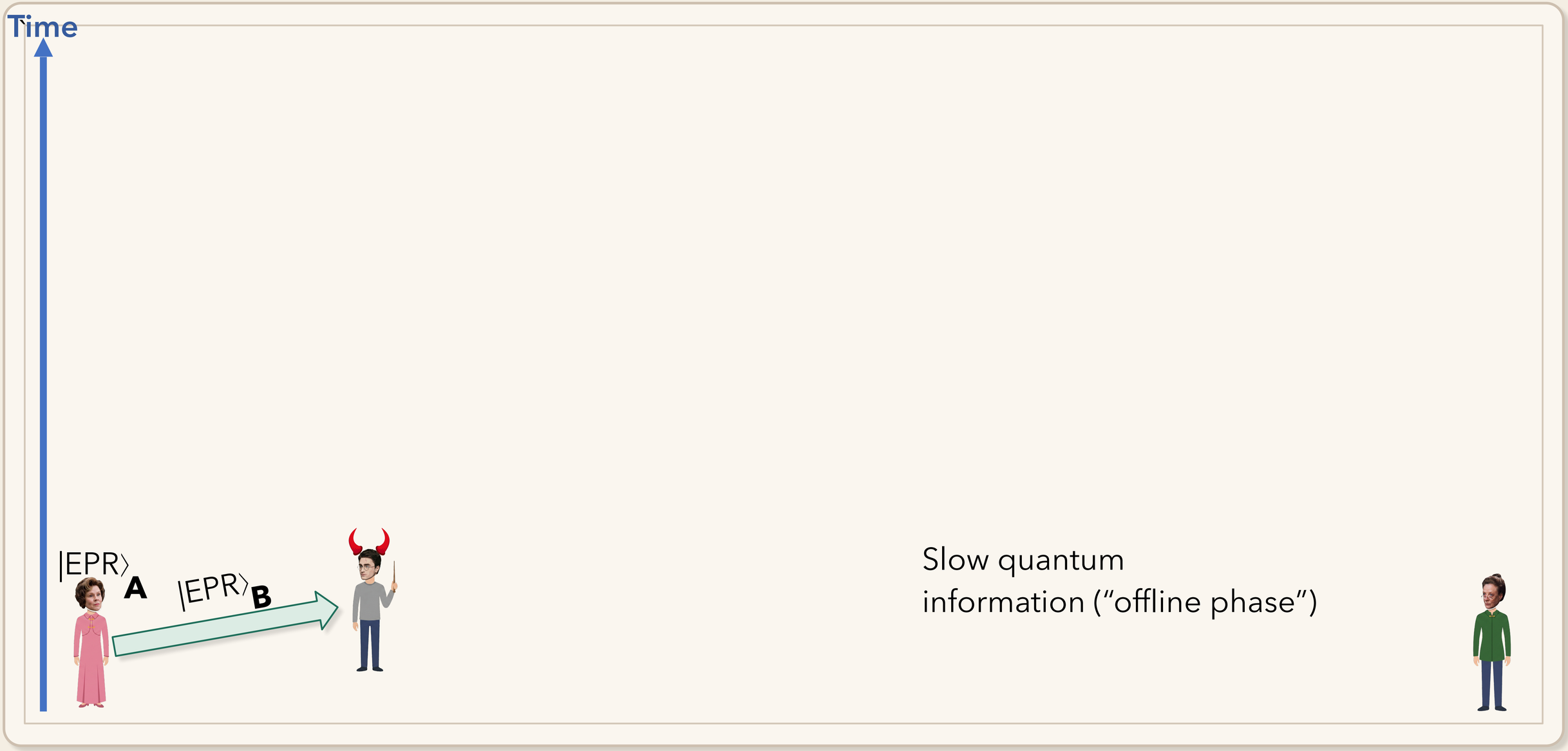
Non-Localizability of f-BB84



Non-Localizability of f-BB84

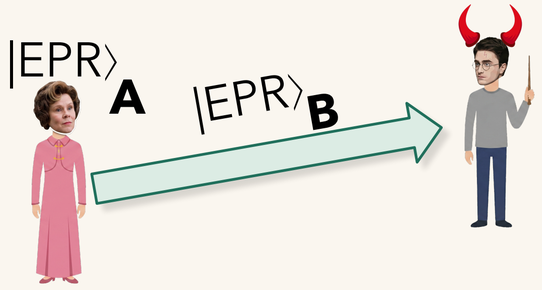


Non-Localizability of f-BB84



Non-Localizability of f-BB84

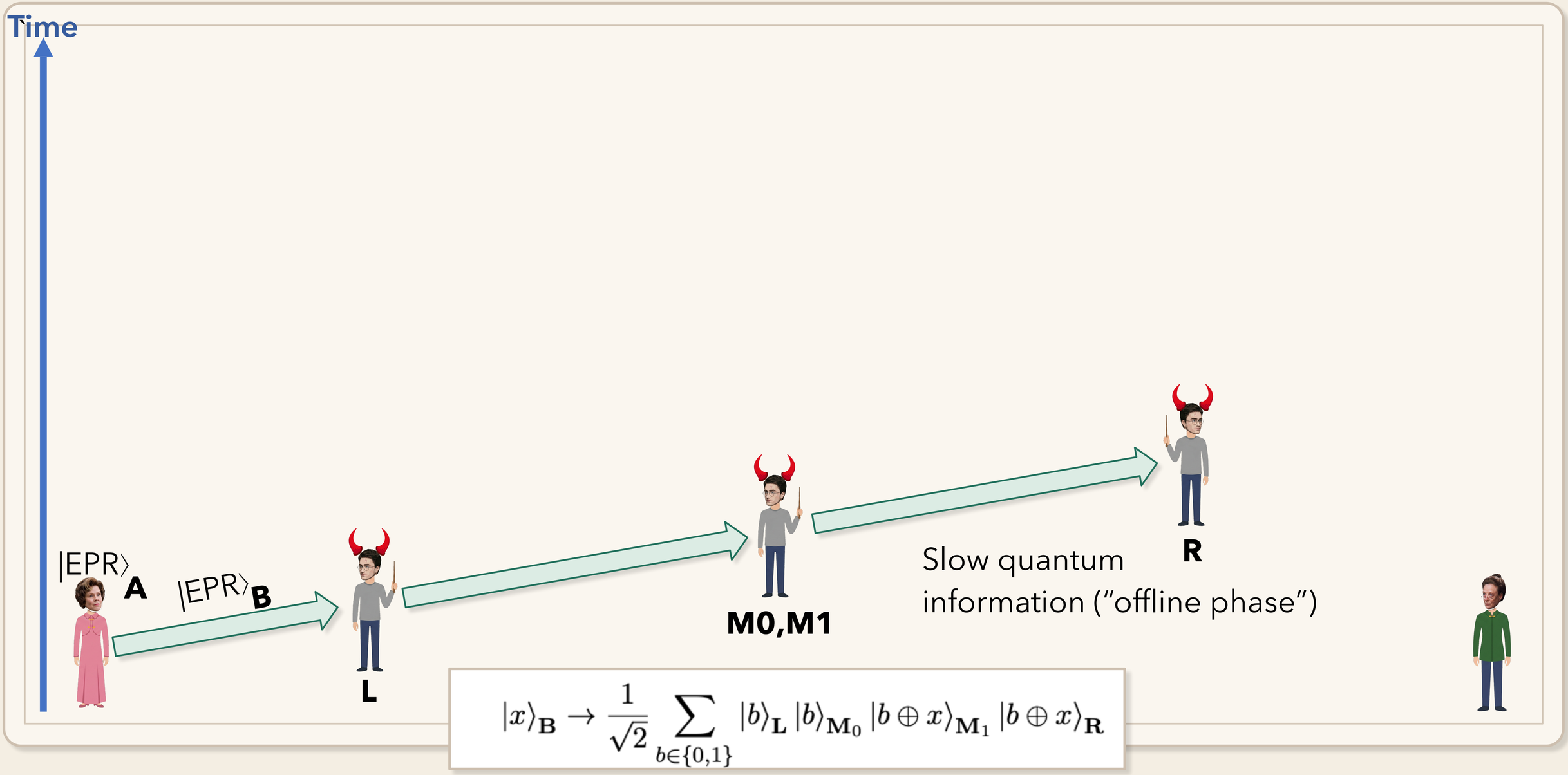
Time



Slow quantum
information (“offline phase”)

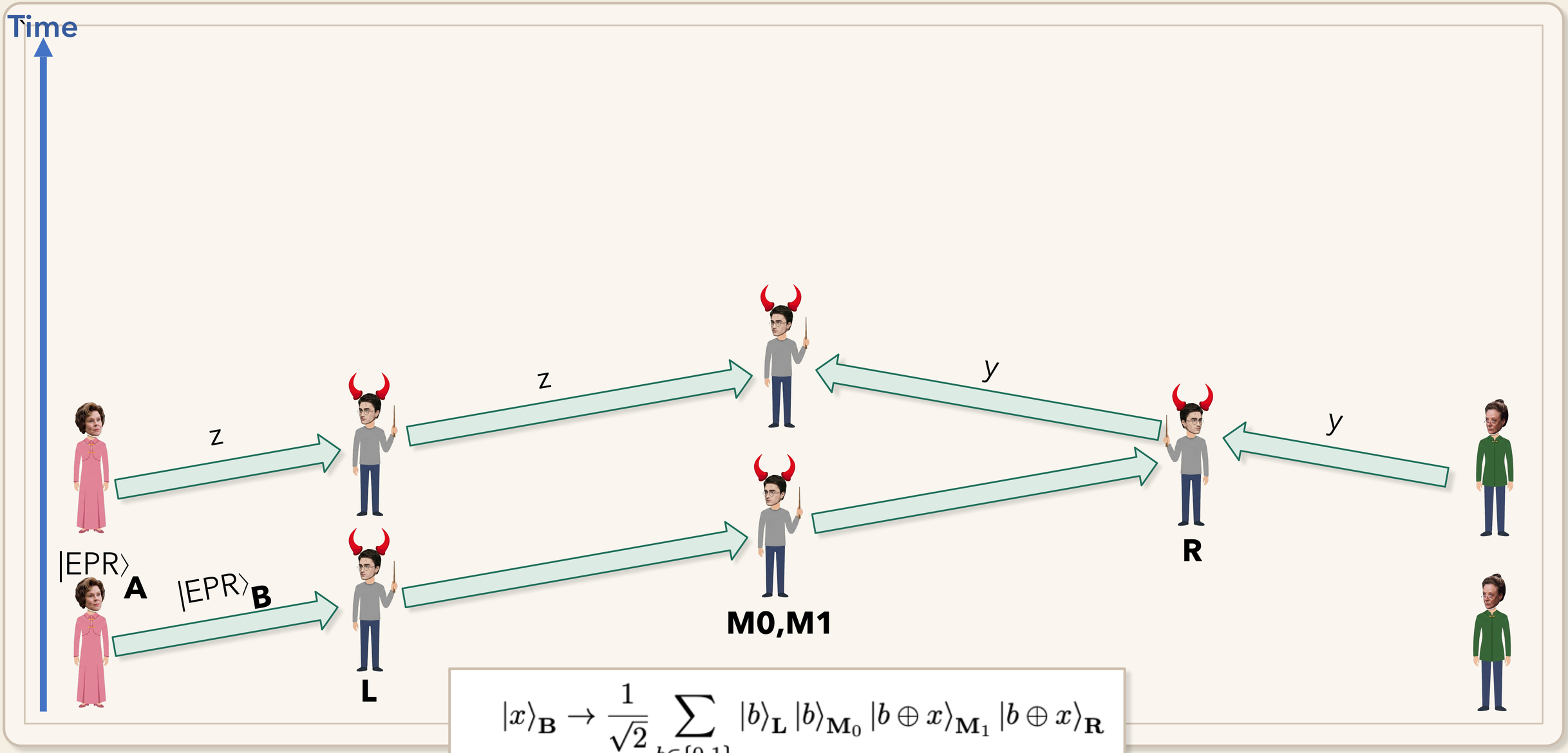
$$|x\rangle_{\mathbf{B}} \to \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} |b\rangle_{\mathbf{L}} |b\rangle_{\mathbf{M}_0} |b\oplus x\rangle_{\mathbf{M}_1} |b\oplus x\rangle_{\mathbf{R}}$$

Non-Localizability of f-BB84



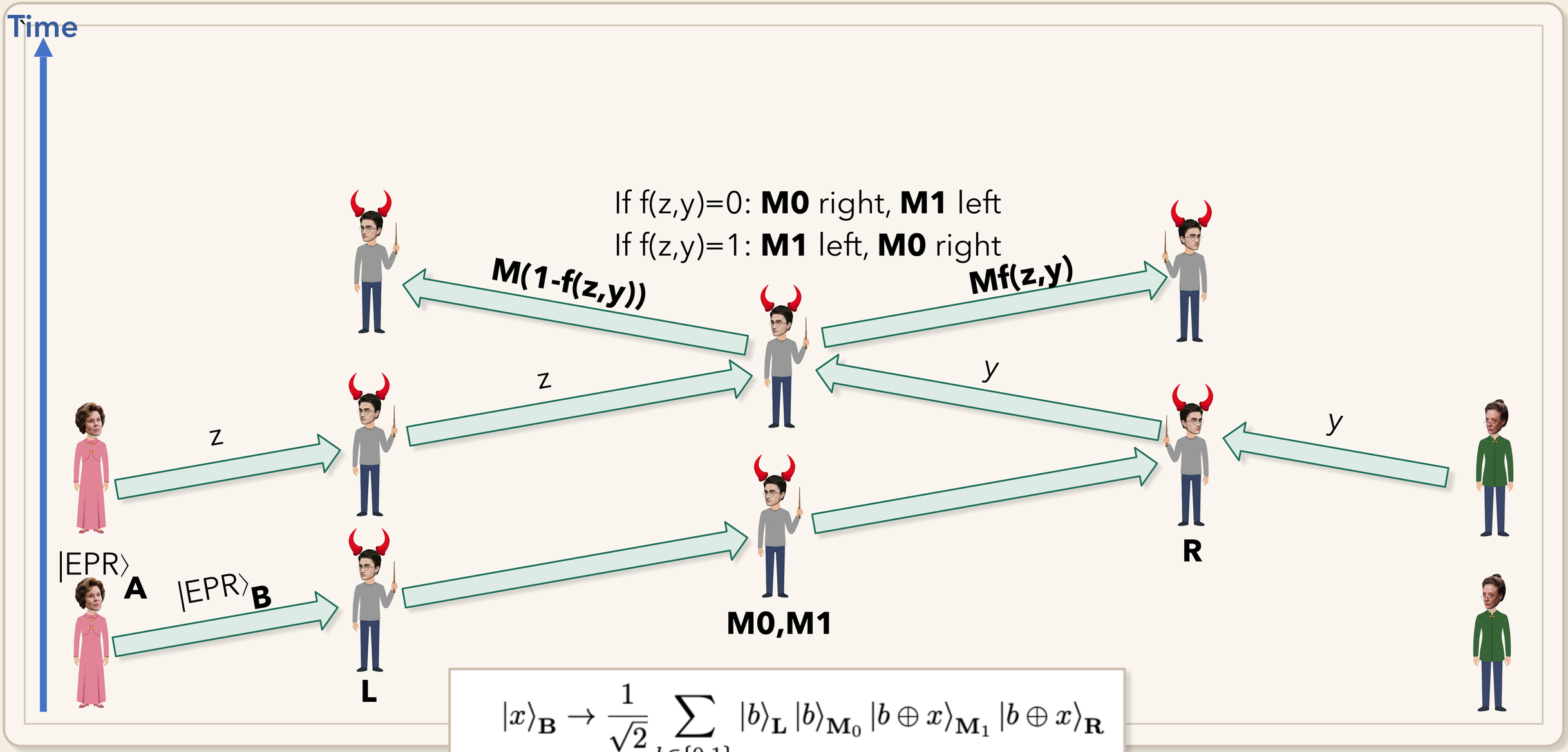
$$|x\rangle_{\mathbf{B}} \to \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} |b\rangle_{\mathbf{L}} |b\rangle_{\mathbf{M}_0} |b\oplus x\rangle_{\mathbf{M}_1} |b\oplus x\rangle_{\mathbf{R}}$$

Non-Localizability of f-BB84

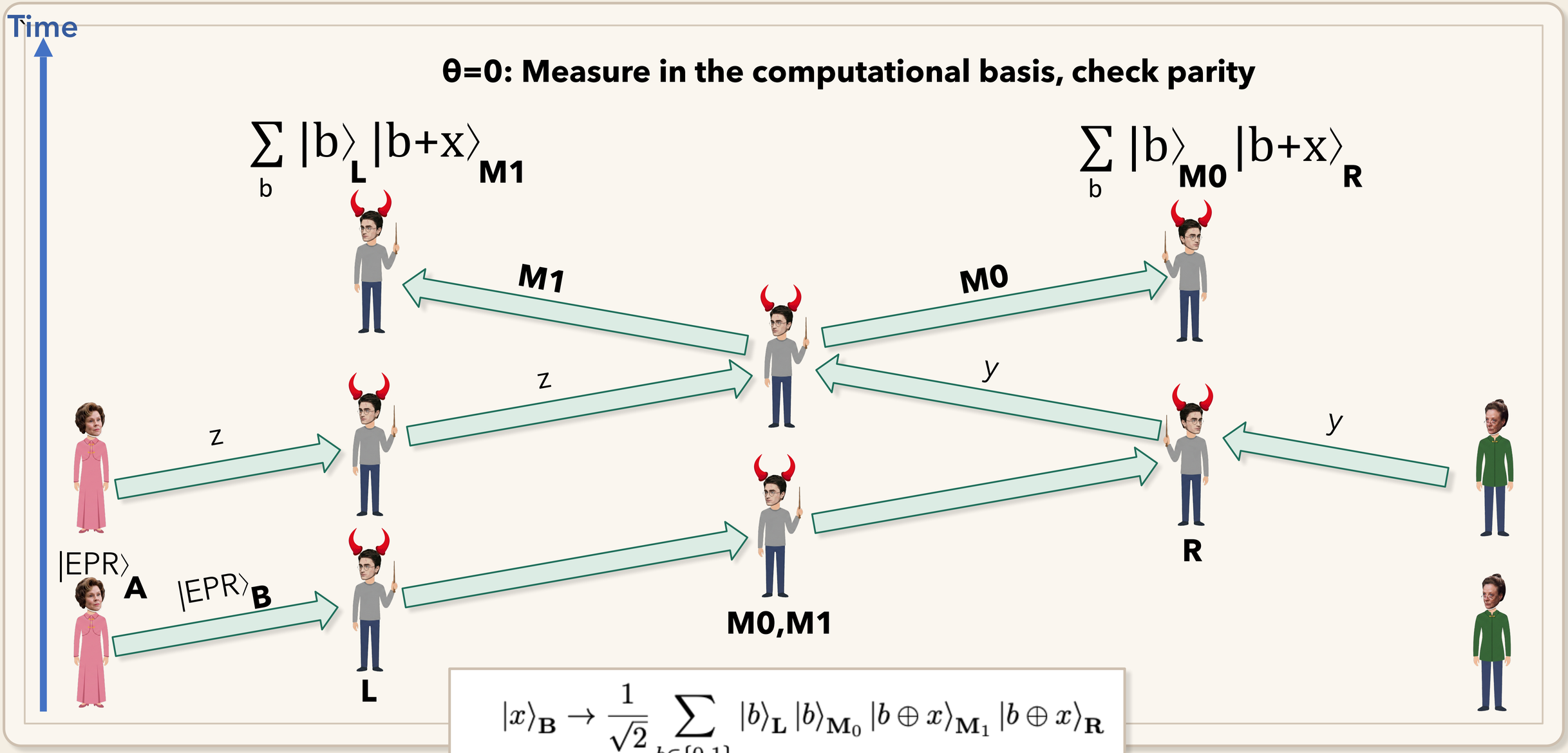


$$|x\rangle_{\mathbf{B}} \to \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} |b\rangle_{\mathbf{L}} |b\rangle_{\mathbf{M}_0} |b\oplus x\rangle_{\mathbf{M}_1} |b\oplus x\rangle_{\mathbf{R}}$$

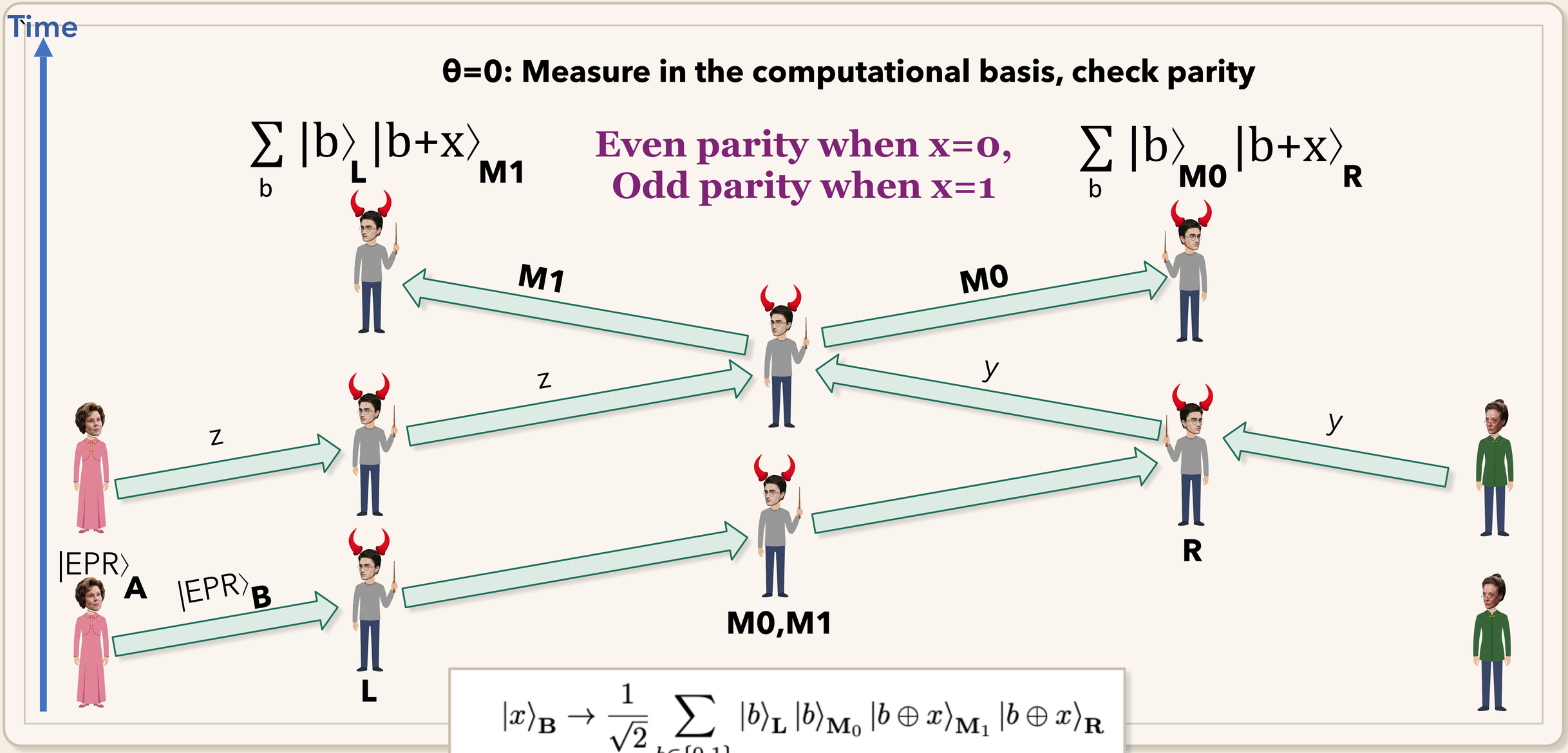
Non-Localizability of f-BB84



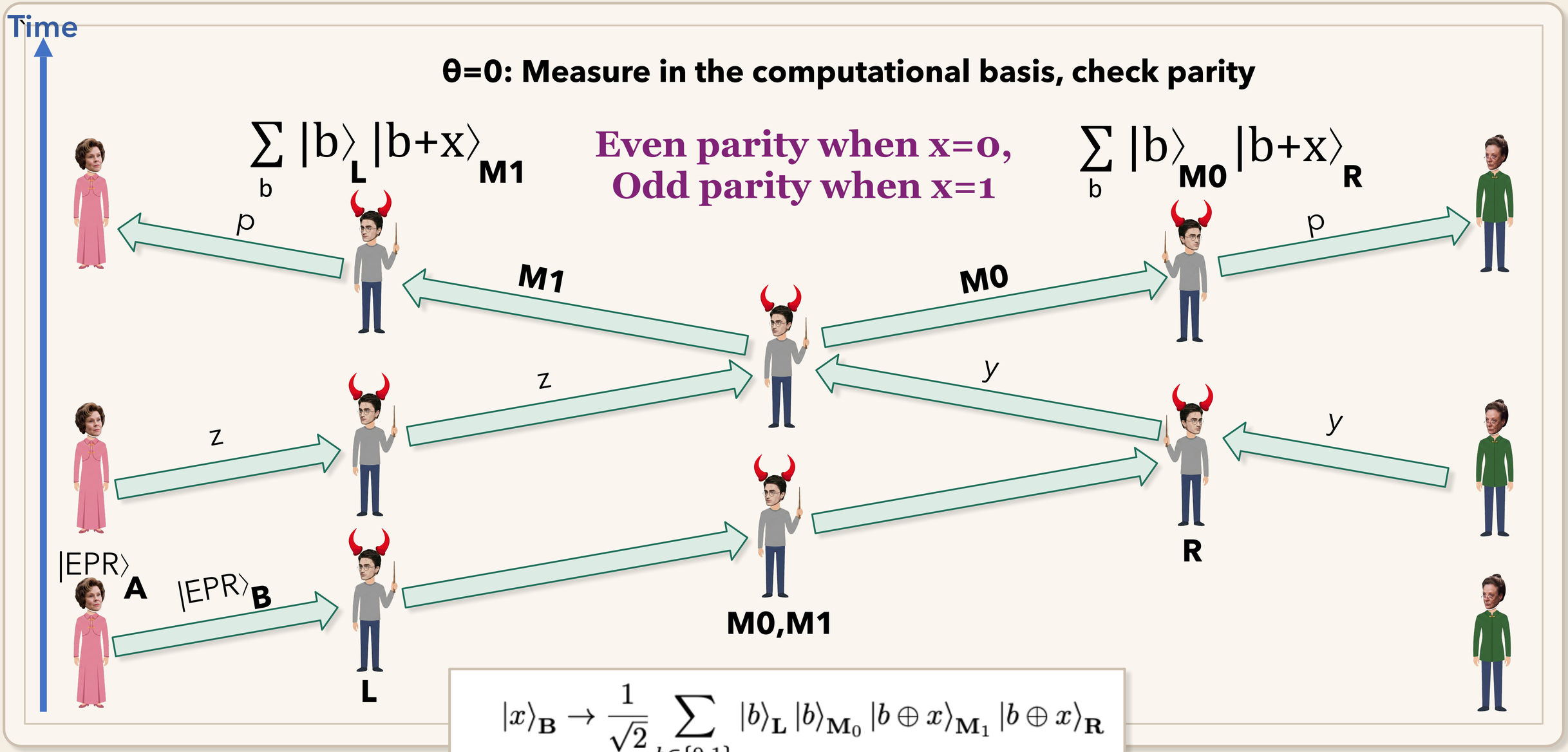
Non-Localizability of f-BB84



Non-Localizability of f-BB84

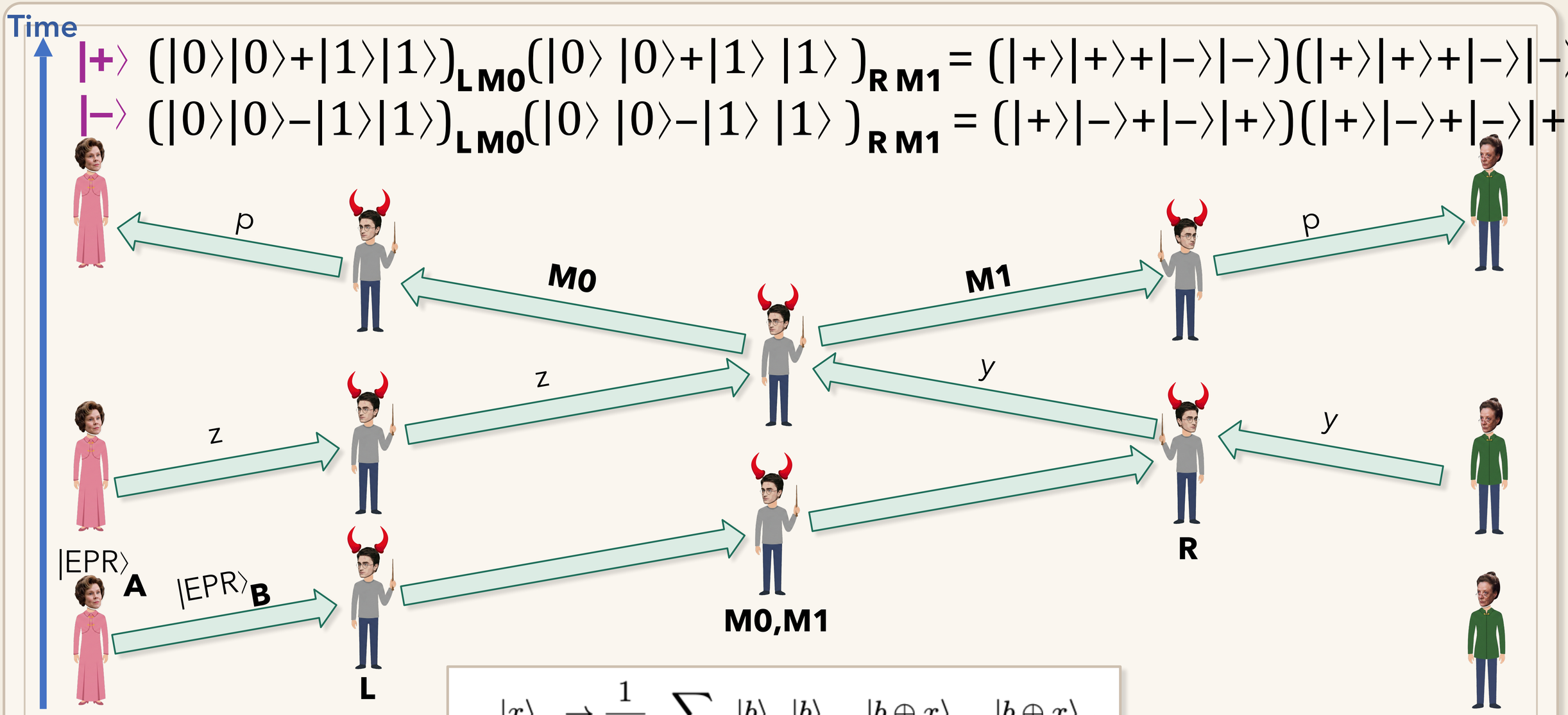


Non-Localizability of f-BB84



Non-Localizability of f-BB84

θ=1: Measure in the Hadamard basis, check parity



Non-Localizability of f-BB84

θ=1: Measure in the Hadamard basis, check parity

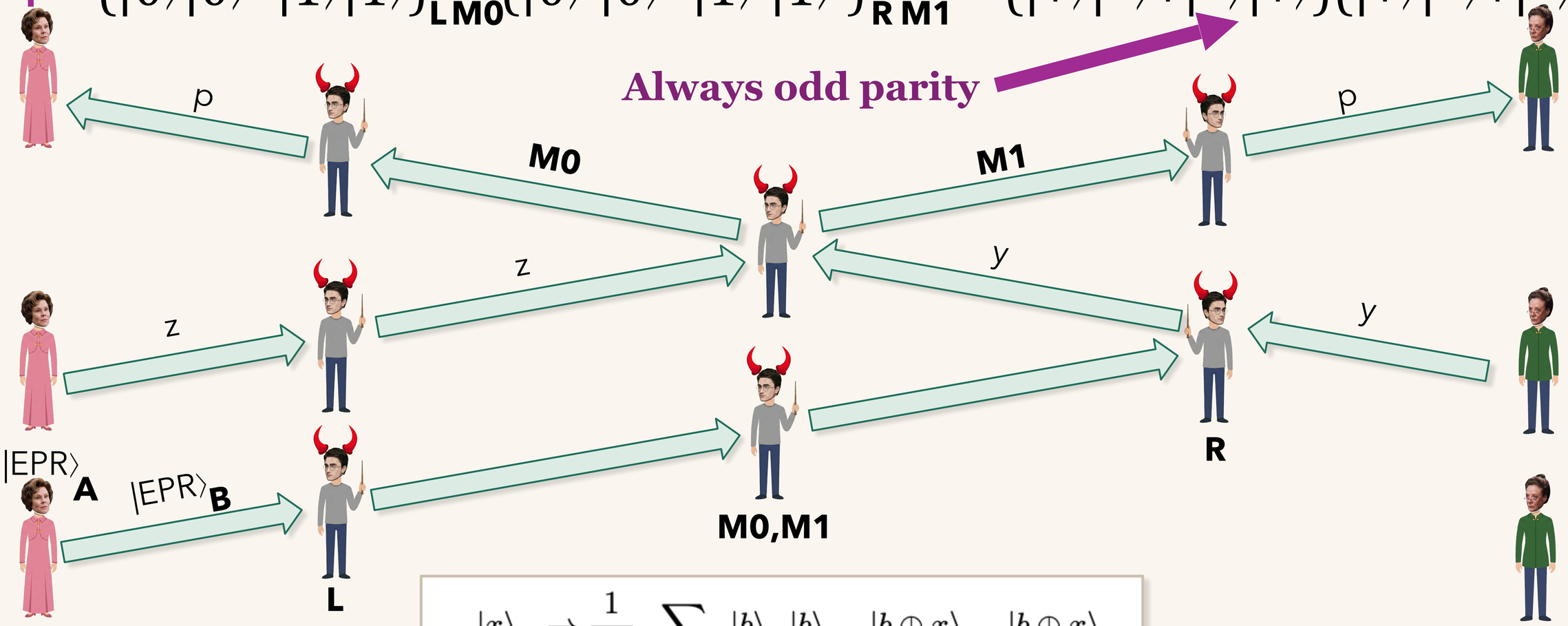
Always even parity

Time

$|+\rangle\ (|0\rangle|0\rangle+|1\rangle|1\rangle)_{\mathbf{L\,M0}}(|0\rangle\ |0\rangle+|1\rangle\ |1\rangle\ )_{\mathbf{R\,M1}} = (|+\rangle|+\rangle+|-\rangle|-\rangle)(|+\rangle|+\rangle+|-\rangle|-\rangle)$

$|-\rangle\ (|0\rangle|0\rangle-|1\rangle|1\rangle)_{\mathbf{L\,M0}}(|0\rangle\ |0\rangle-|1\rangle\ |1\rangle\ )_{\mathbf{R\,M1}} = (|+\rangle|-\rangle+|-\rangle|+\rangle)(|+\rangle|-\rangle+|-\rangle|+\rangle)$

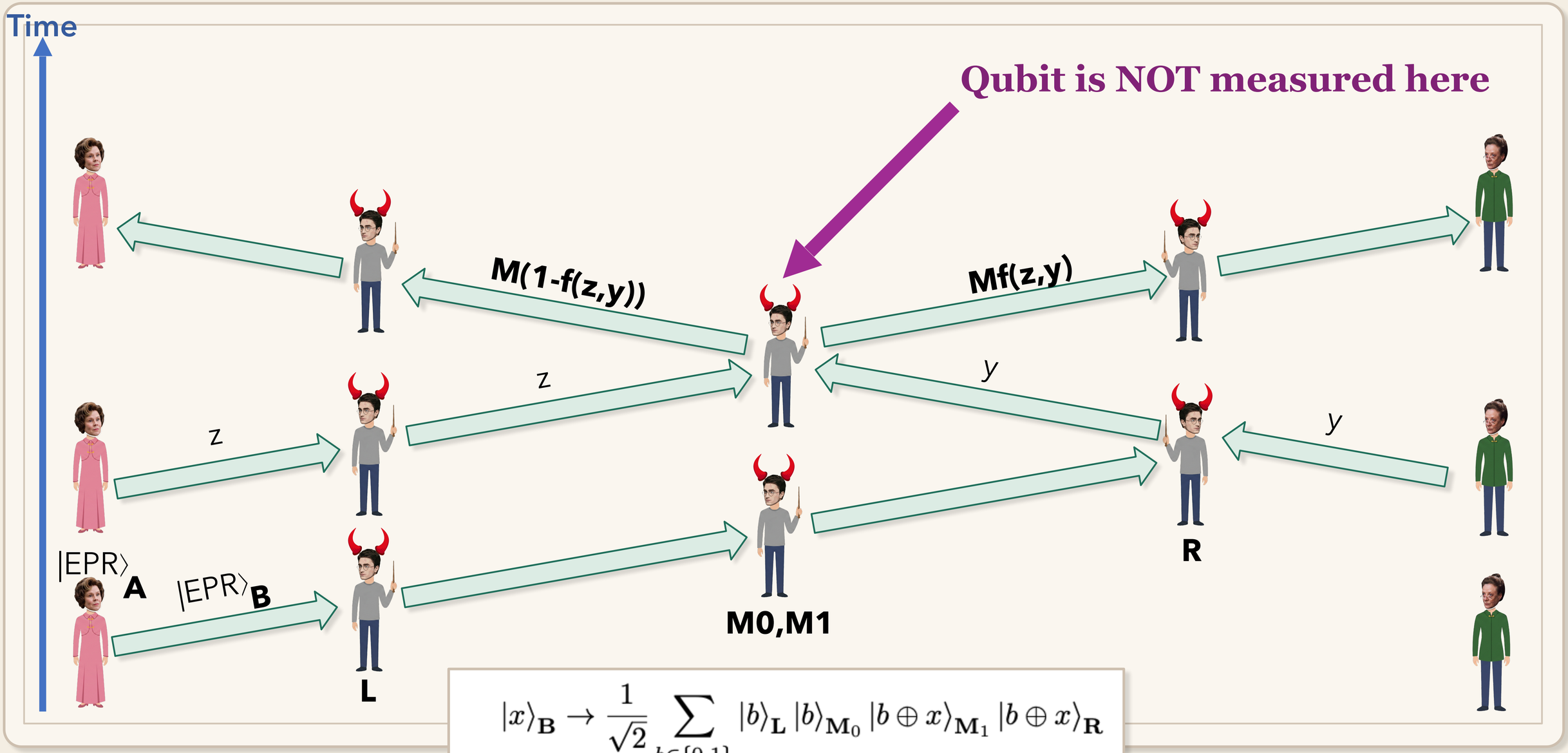
Always odd parity



$$|x\rangle_{\mathbf{B}} \rightarrow \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} |b\rangle_{\mathbf{L}}\,|b\rangle_{\mathbf{M}_0}\,|b\oplus x\rangle_{\mathbf{M}_1}\,|b\oplus x\rangle_{\mathbf{R}}$$

Non-Localizability of f-BB84

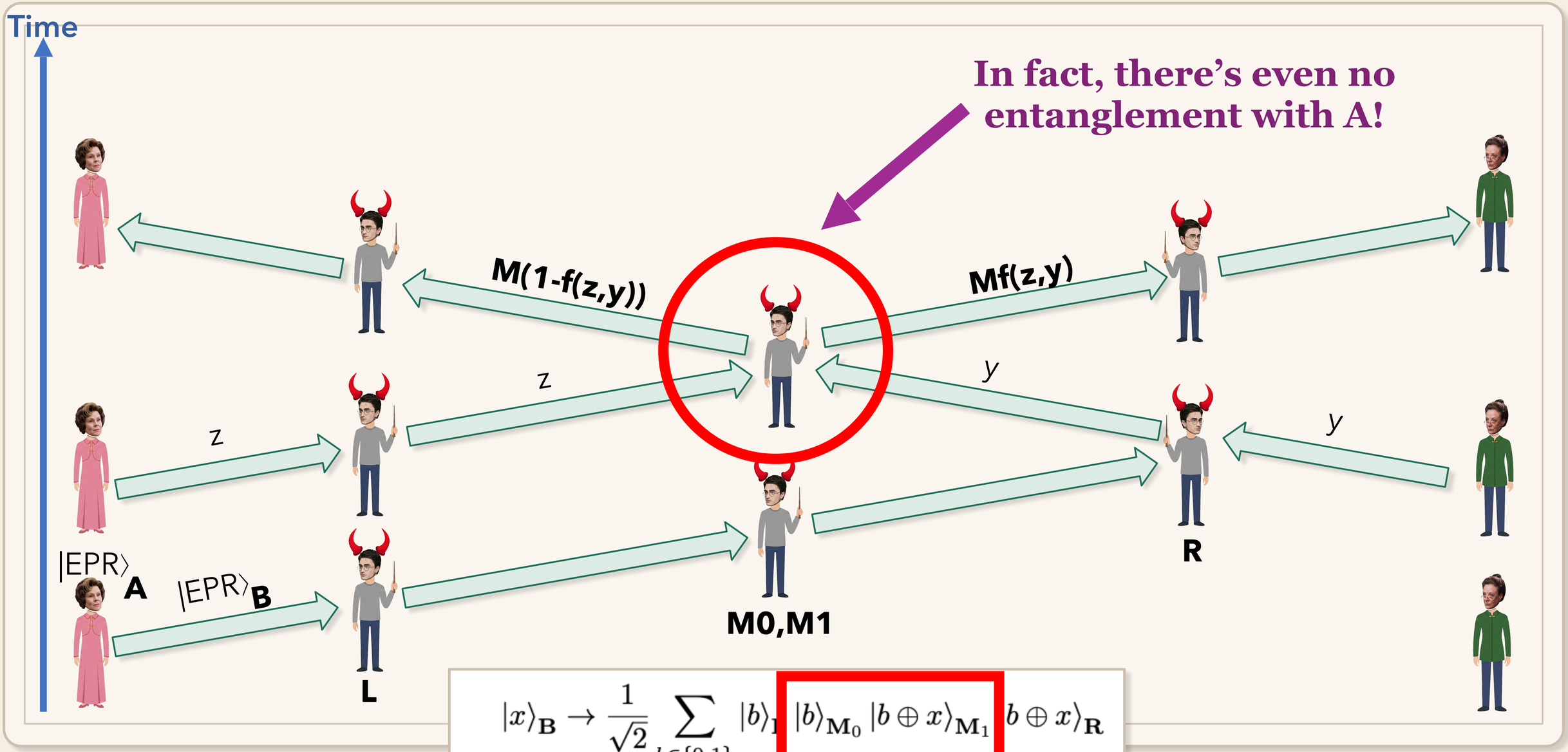
θ=1: Measure in the Hadamard basis, check parity



$$|x\rangle_{\mathbf{B}} \to \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} |b\rangle_{\mathbf{L}} |b\rangle_{\mathbf{M}_0} |b\oplus x\rangle_{\mathbf{M}_1} |b\oplus x\rangle_{\mathbf{R}}$$

Non-Localizability of f-BB84

θ=1: Measure in the Hadamard basis, check parity



Security Guarantees for Position-Based Crypto

Security Guarantees for Position-Based Crypto

Previously: “There’s at least *some* entity at the target location.”

Security Guarantees for Position-Based Crypto

Previously: “There’s at least *some* entity at the target location.”

Goal: “A specific entity (namely, *the one I’m interacting with)* is at the target location.”

Security Guarantees for Position-Based Crypto

Previously: “There’s at least *some* entity at the target location.”

Goal: “A specific entity (namely, *the one I’m interacting with)* is at the target location.”

Let’s try to formalize this…

Security Guarantees for Position-Based Crypto

Previously: “There’s at least *some* entity at the target location.”

Goal: “A specific entity (namely, *the one I’m interacting with)* is at the target location.”

Let’s try to formalize this…

What does it mean for an entity to ***be*** at a specific location?

Security Guarantees for Position-Based Crypto

Previously: "There's at least *some* entity at the target location."

Goal: "A specific entity (namely, *the one I'm interacting with)* is at the target location."

Let's try to formalize this…

What does it mean for an entity to ***be*** at a specific location?

What does it even mean to *exist?*

Security Guarantees for Position-Based Crypto

Previously: “There’s at least *some* entity at the target location.”

Goal: “A specific entity (namely, *the one I’m interacting with)* is at the target location.”

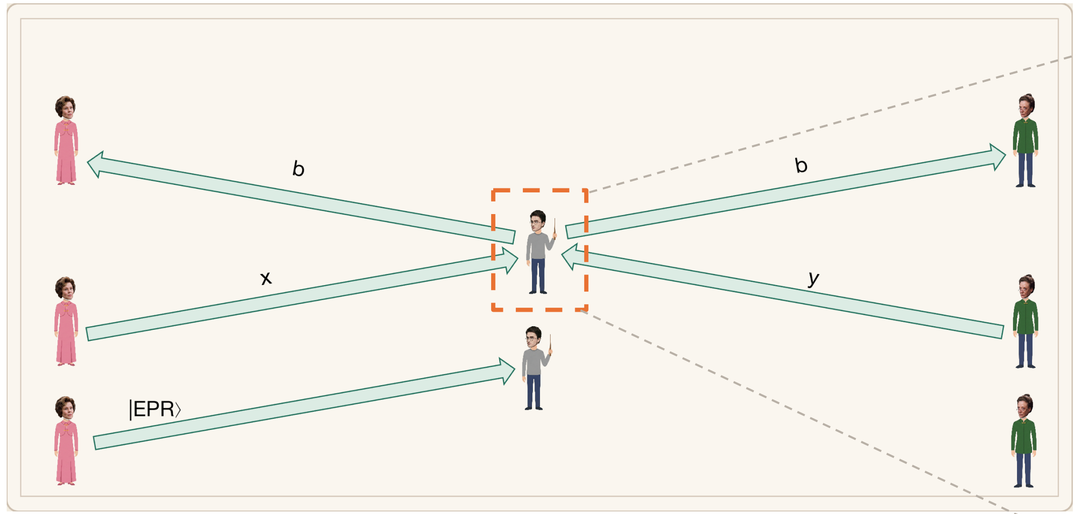
Let’s try to formalize this…

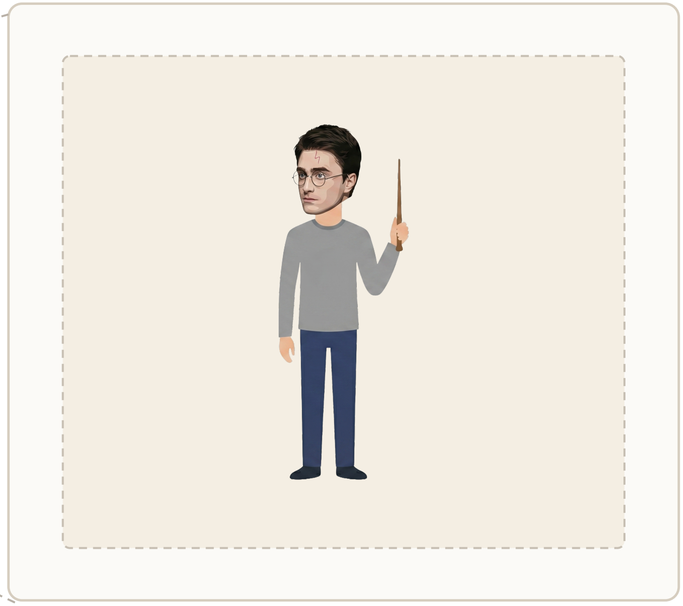
What does it mean for an entity to ***be*** at a specific location?

~~What does it even mean to *exist?*~~

Finding an Entity Somewhere

> “Zooming in” on a region of space to see what it contains





Given all of the quantum registers in [ ], can we reconstruct  ?

Finding a Unique Quantum State

But again, even if we find something,
how do we *identify* it?

Finding a Unique Quantum State

But again, even if we find something,
how do we *identify* it?

Physical Uniqueness —

For any pair of *disjoint* spatial regions A and B, and any time t, a physically unique object can be "found" within region A at time t only if it *cannot* be "found" within region B at time t.

Finding a Unique Quantum State

But again, even if we find something,
how do we *identify* it?

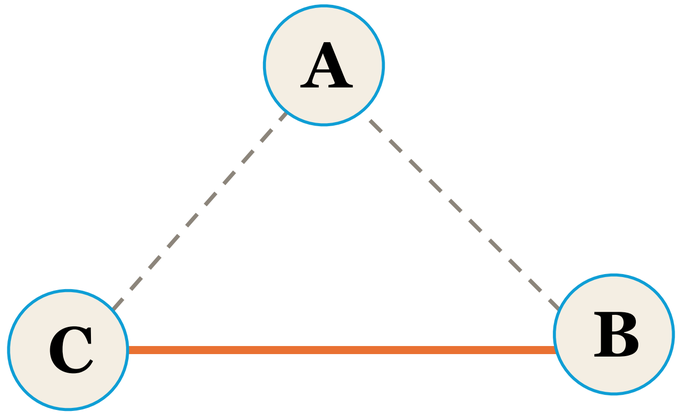
Physical Uniqueness —

For any pair of *disjoint* spatial regions A and B, and any time t, a physically unique object can be "found" within region A at time t only if it *cannot* be "found" within region B at time t.

Note: unique => unclonable,
but not vice versa! e.g. BB84 states

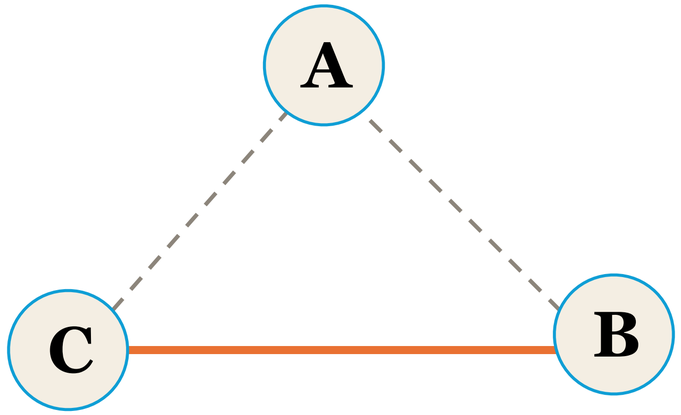
Physically Unique Resource — Entanglement!

Monogamy-of-entanglement is precisely a physical uniqueness property



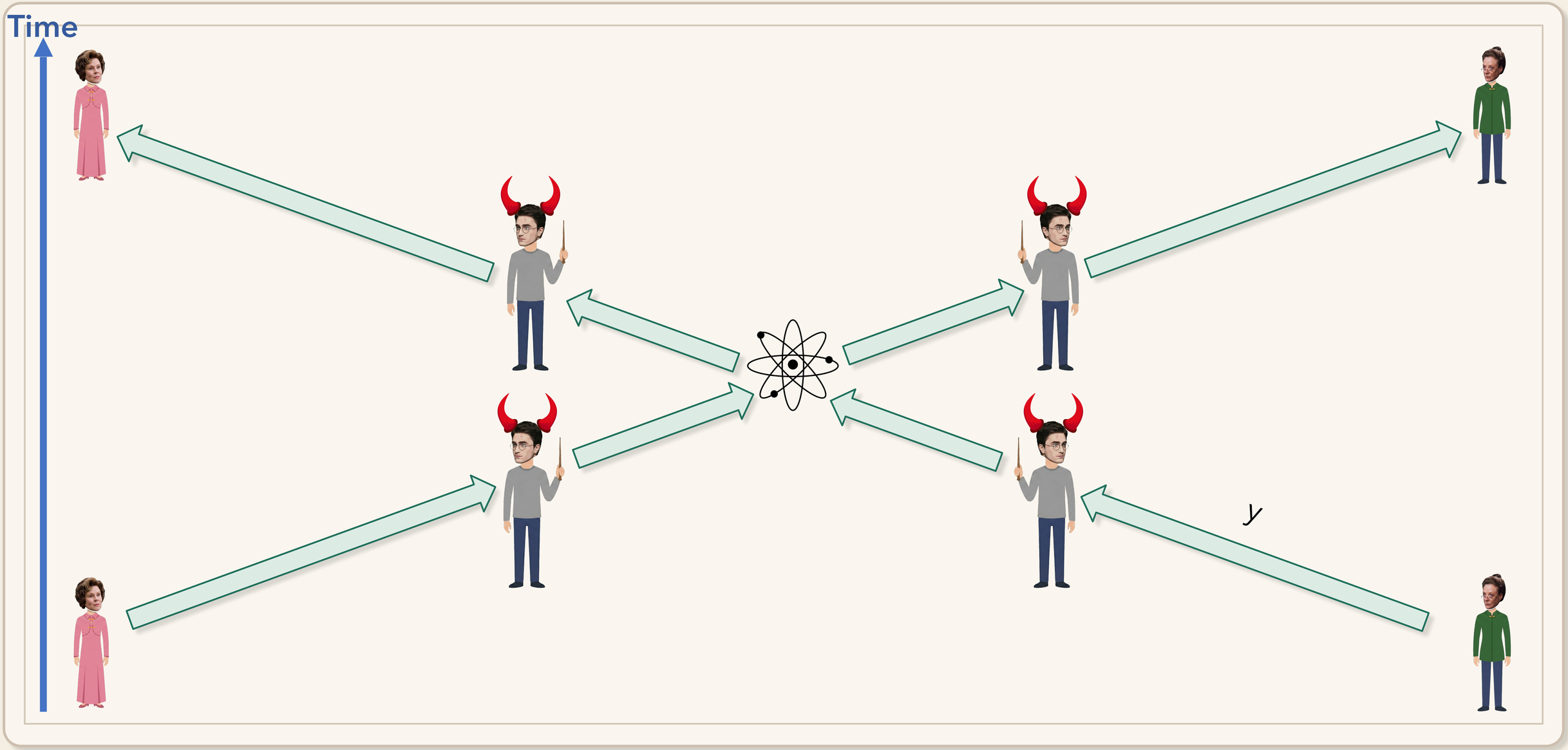
Physically Unique Resource — Entanglement!

Monogamy-of-entanglement is precisely a physical uniqueness property

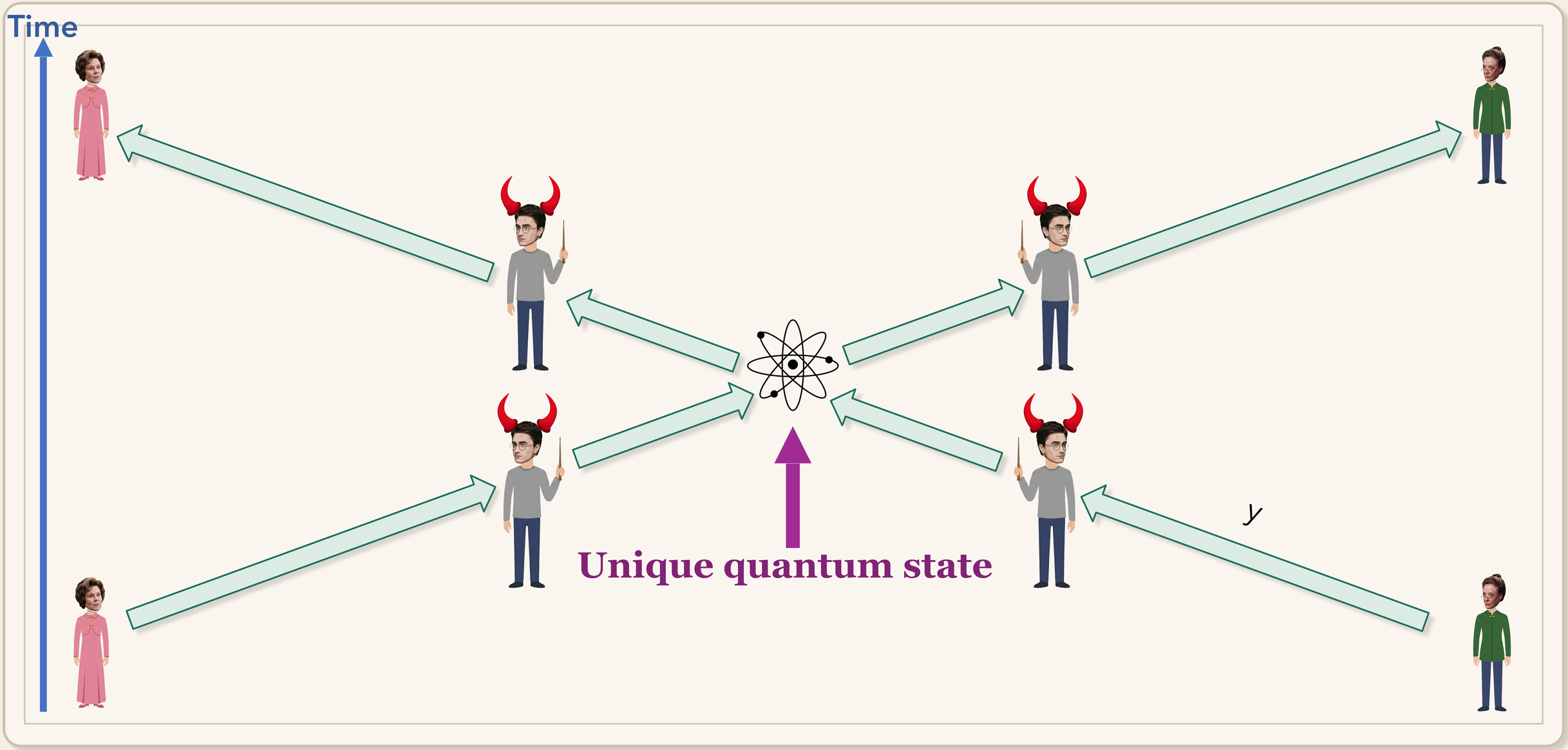


Uniqueness: If an EPR half can be found in one region, then it cannot be found in any disjoint region

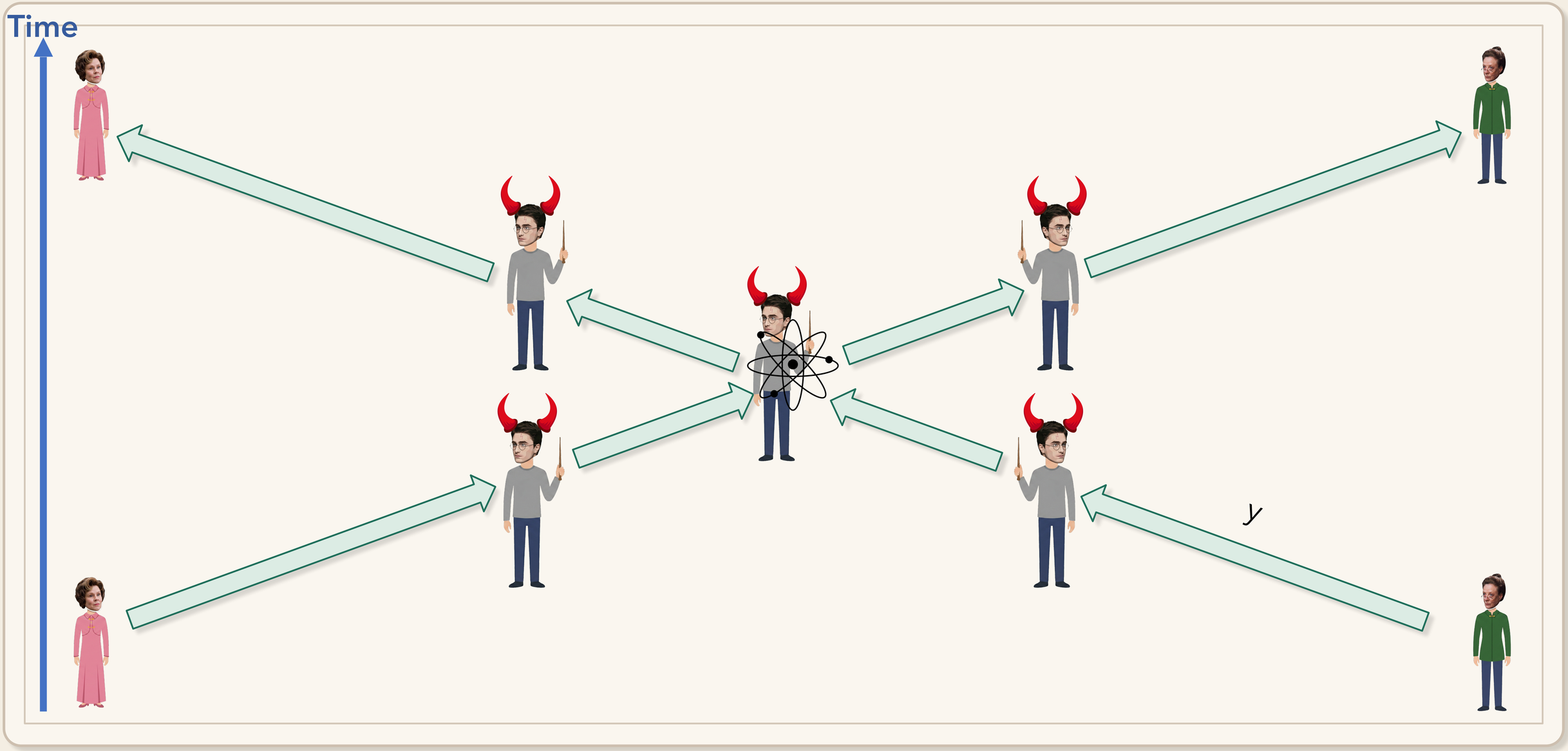
Visualizing PV in Spacetime



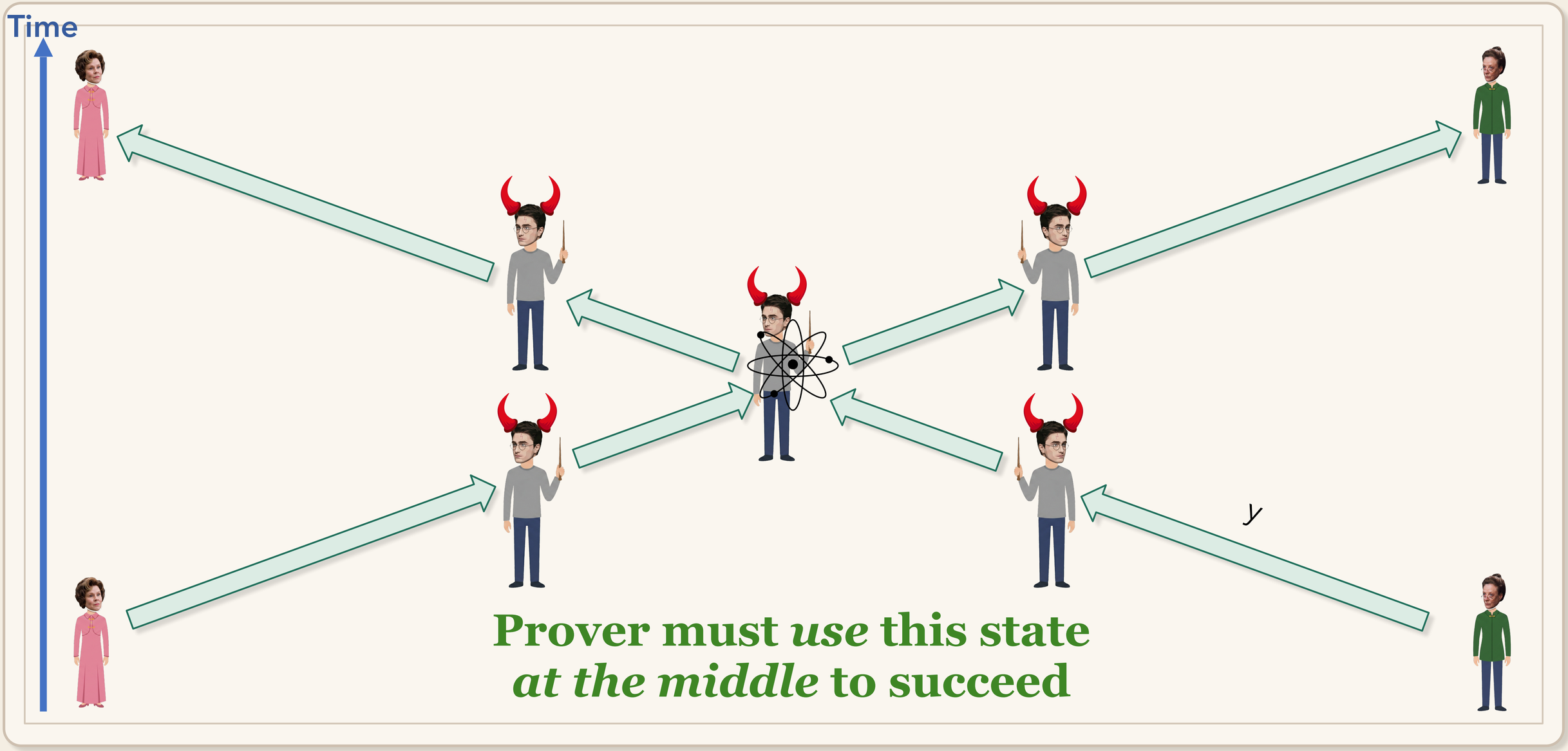
Visualizing PV in Spacetime



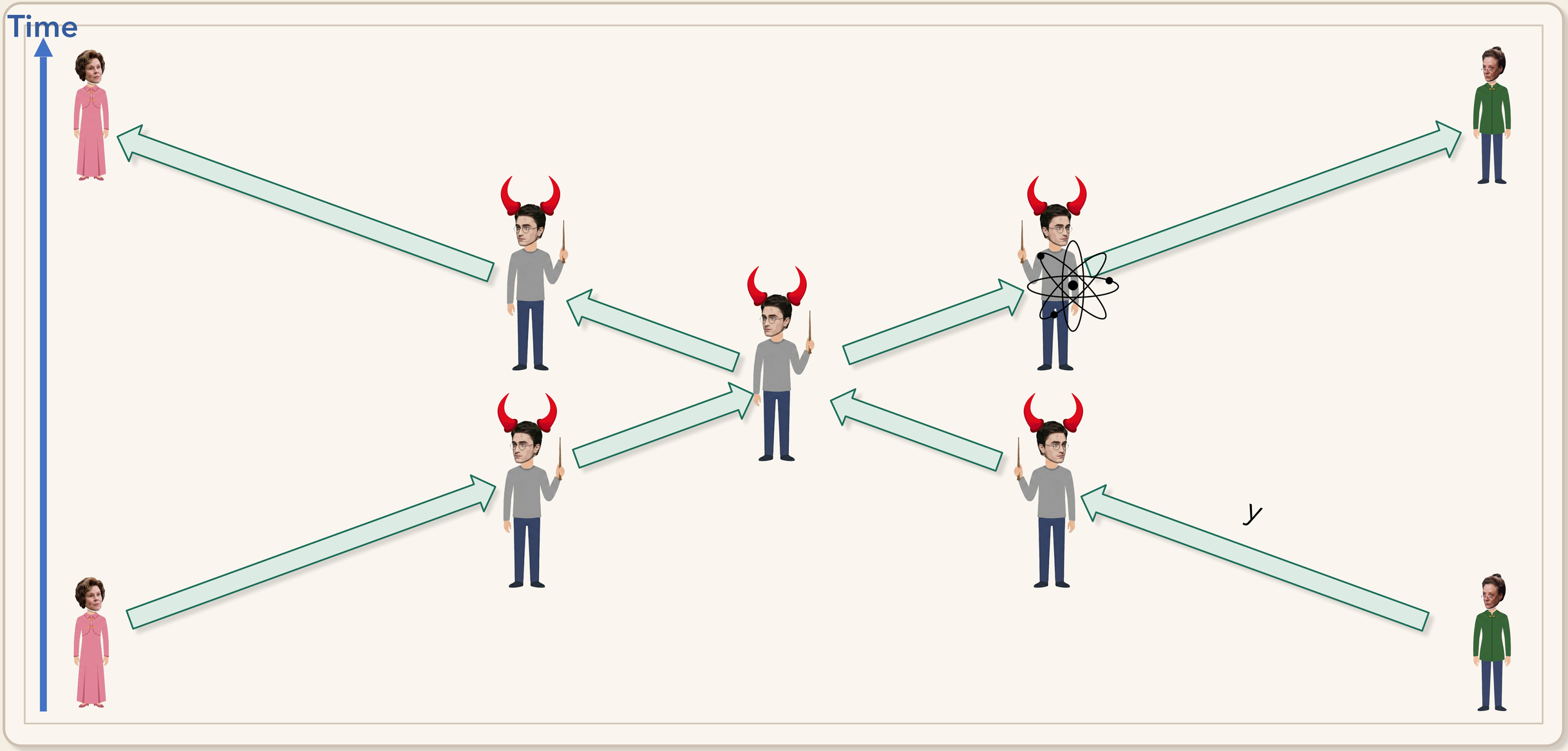
Visualizing PV in Spacetime



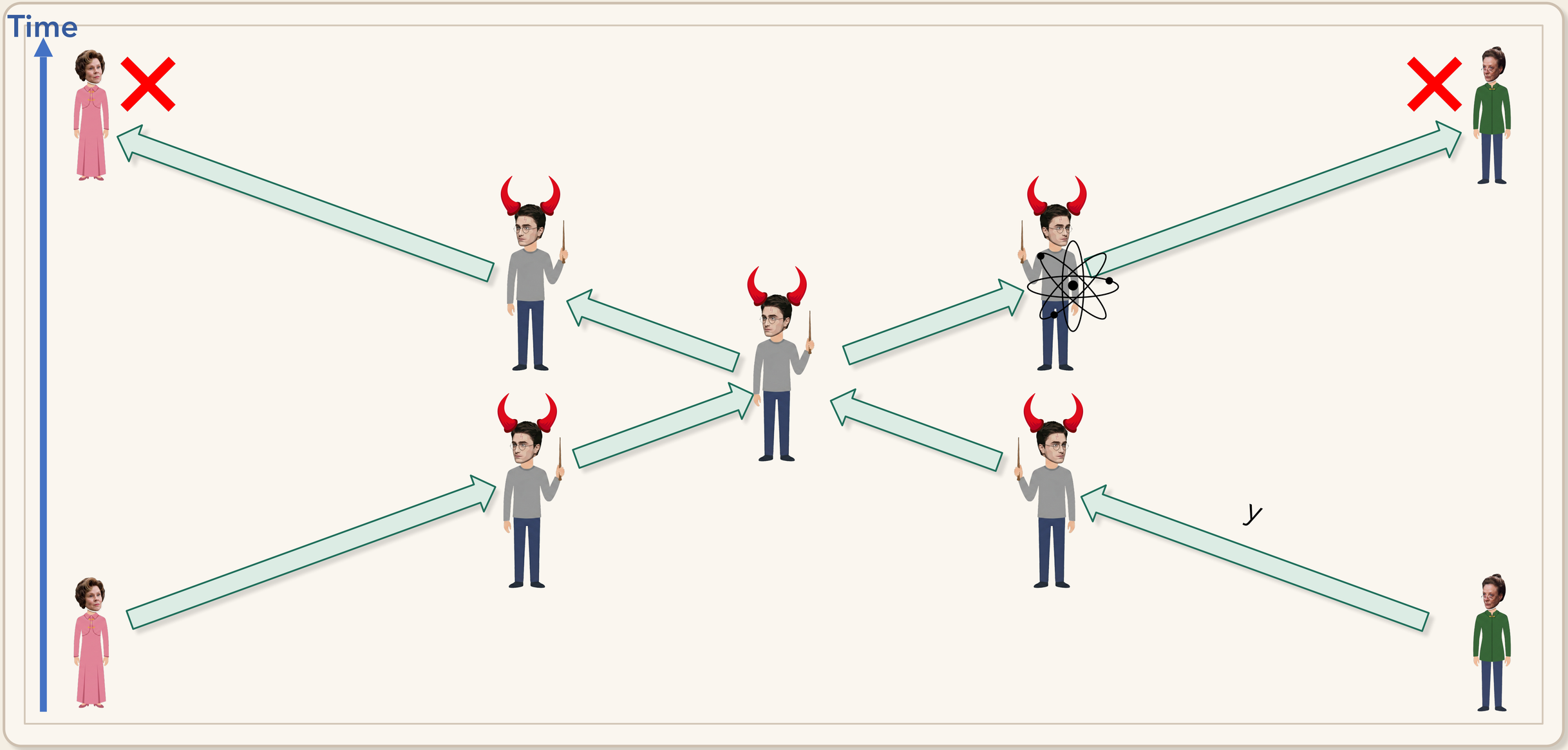
Visualizing PV in Spacetime



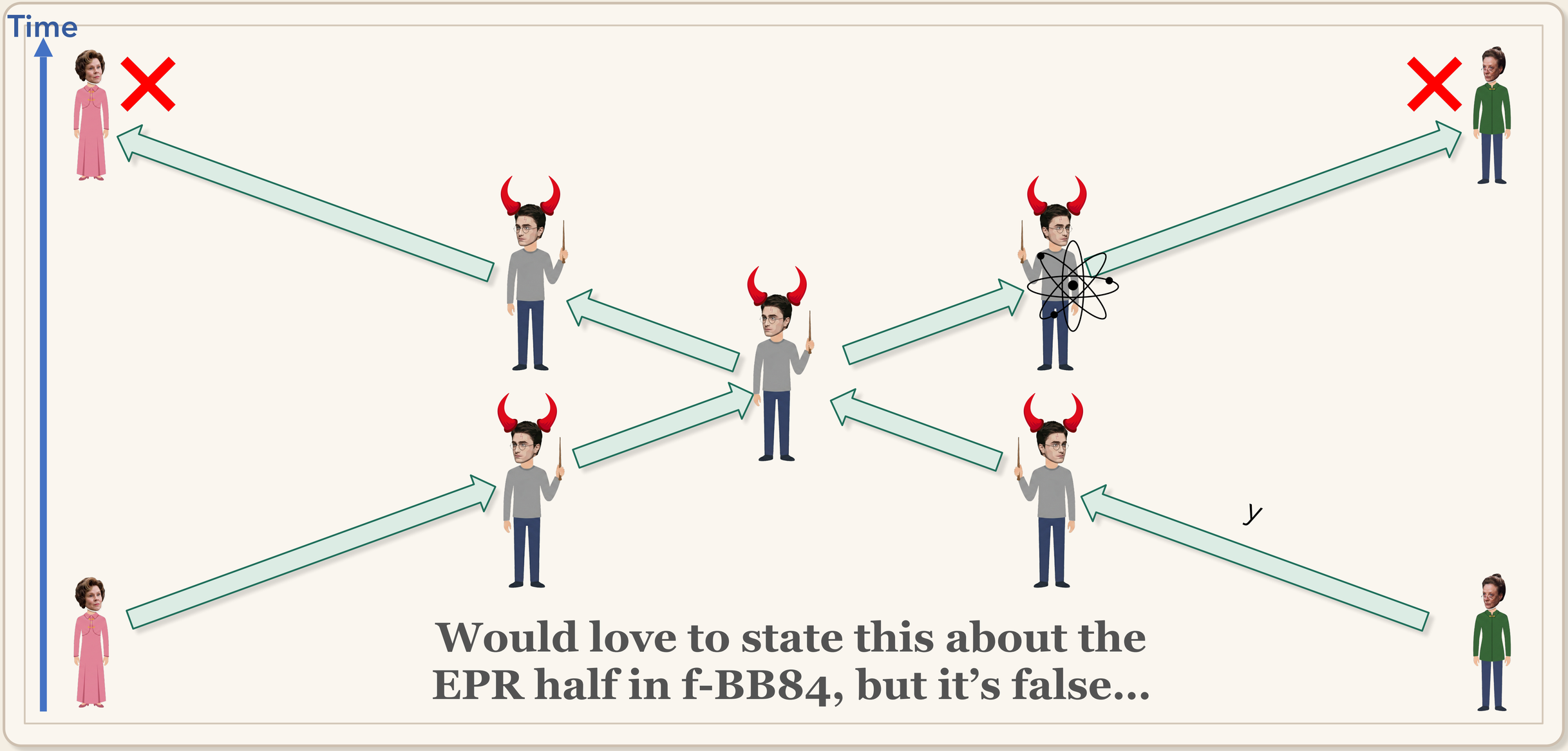
Visualizing PV in Spacetime



Visualizing PV in Spacetime



Visualizing PV in Spacetime



Would love to state this about the EPR half in f-BB84, but it's false…

Finding a Quantum State at a Location

Given a “snapshot” of a spatial region, can we **extract** some quantum state from it?

Finding a Quantum State at a Location

Given a “snapshot” of a spatial region, can we **extract** some quantum state from it?

Def (informal):

Take a spatial region R (at some fixed time) and a quantum state $|\psi\rangle$. We say that $|\psi\rangle$ can be found within R if there exists some physical operation

$$E(R) \rightarrow |\psi\rangle$$

Finding a Quantum State at a Location

Given a “snapshot” of a spatial region, can we **extract** some quantum state from it?

Def (informal):

Take a spatial region R (at some fixed time) and a quantum state $|\psi\rangle$. We say that $|\psi\rangle$ can be found within R if there exists some physical operation

$$E(R) \rightarrow |\psi\rangle$$

CPTP “Extractor”

Finding a Quantum State at a Location

Given a “snapshot” of a spatial region, can we **extract** some quantum state from it?

Def (informal):

Take a spatial region R (at some fixed time) and a quantum state $|\psi\rangle$. We say that $|\psi\rangle$ can be found within R if there exists some physical operation

$$E(R) \rightarrow |\psi\rangle$$

Finding a Quantum State at a Location

Given a "snapshot" of a spatial region, can we **extract** some quantum state from it?

Def (informal):

Take a spatial region R (at some fixed time) and a quantum state $|\psi\rangle$. We say that $|\psi\rangle$ can be found within R if there exists some physical operation

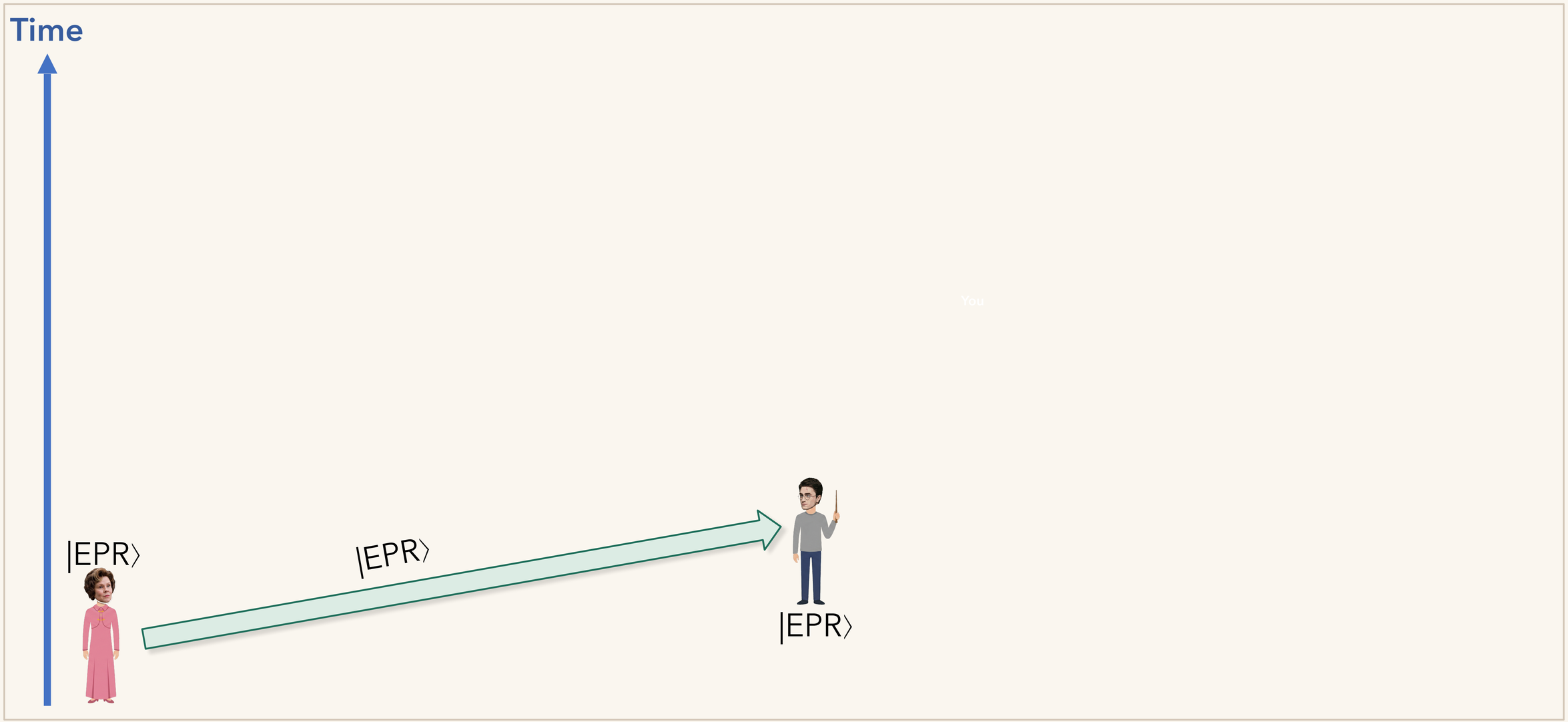
$$E(R) \to |\psi\rangle$$

CPTP "Extractor"

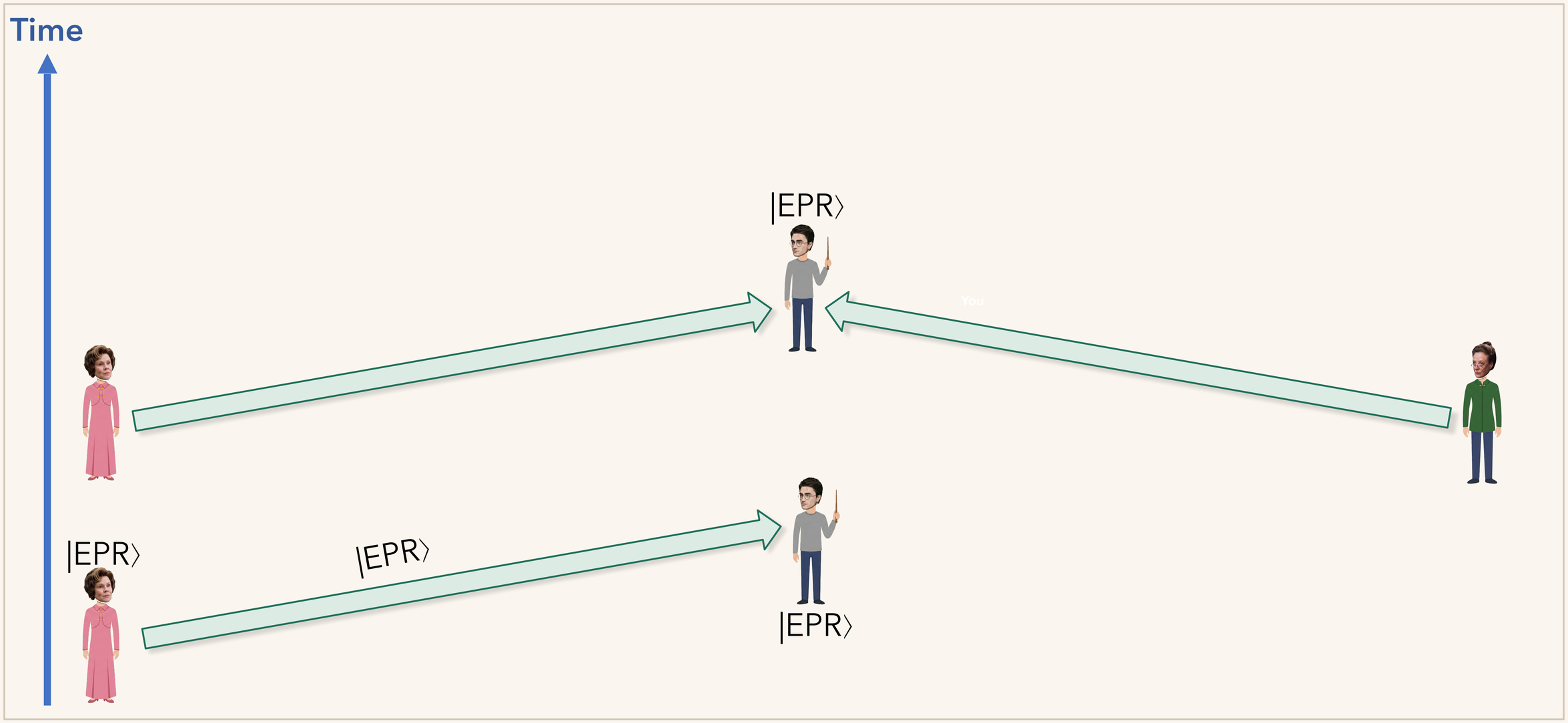
The state on "all registers of R" at the given point in time.

Really, w.h.p. output $|\phi\rangle$ having high fidelity with $|\psi\rangle$

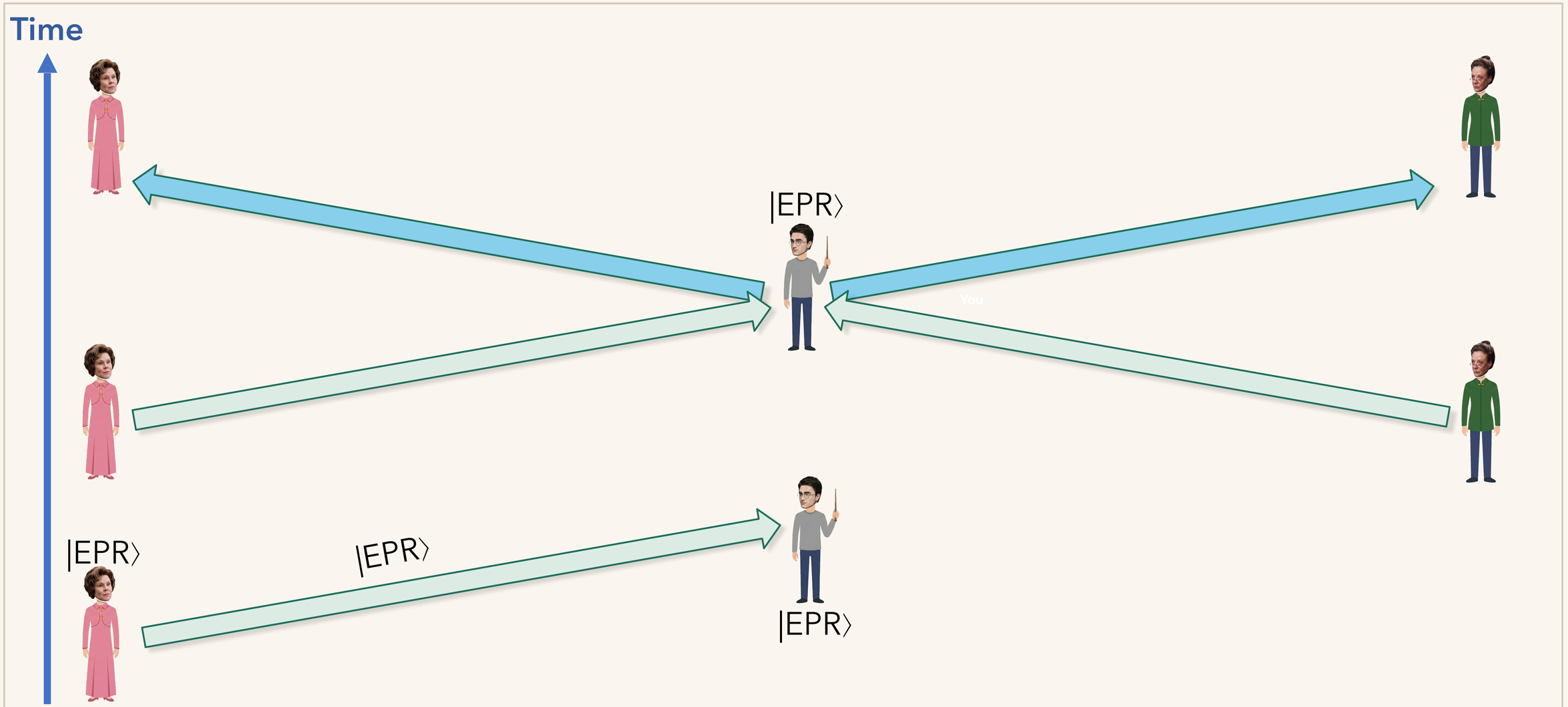
Task: Entanglement Localization



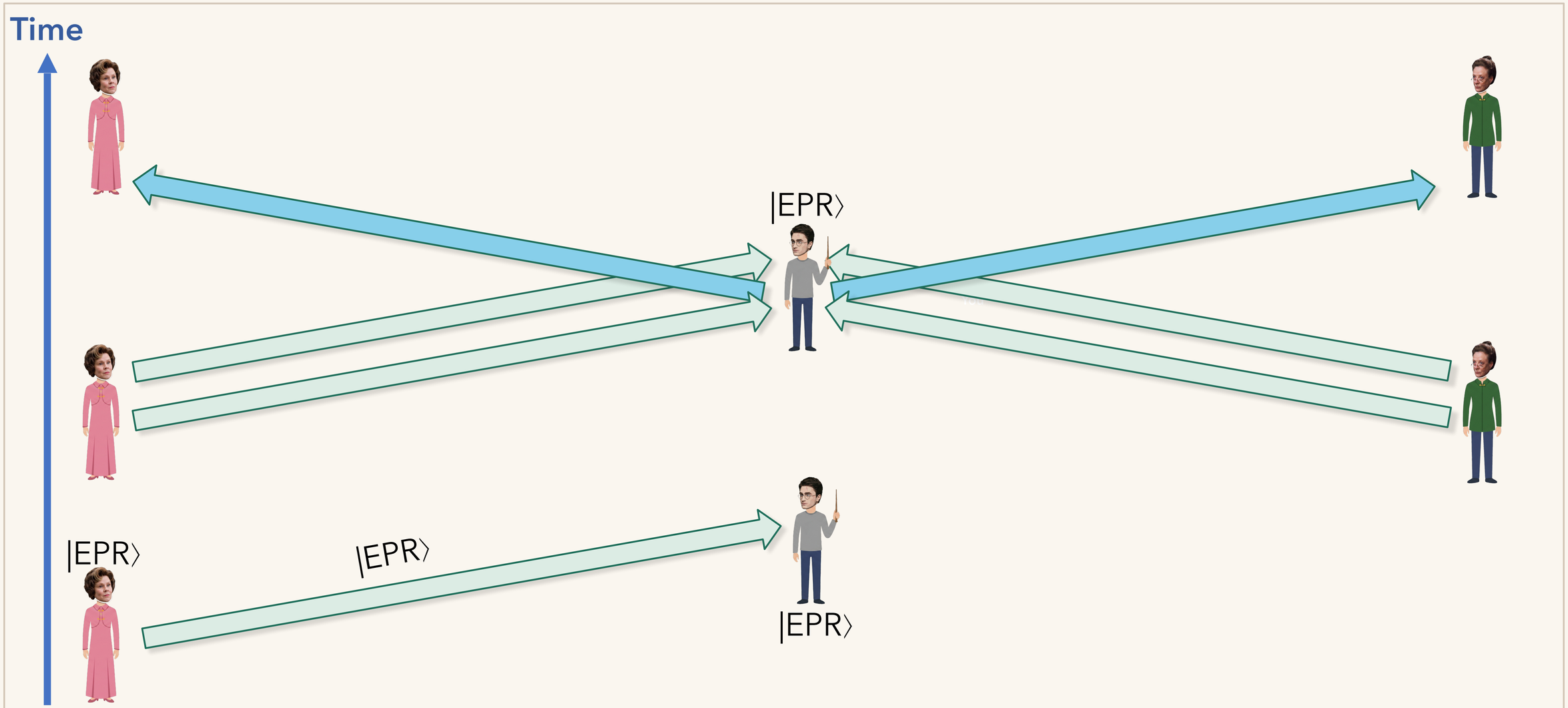
Task: Entanglement Localization



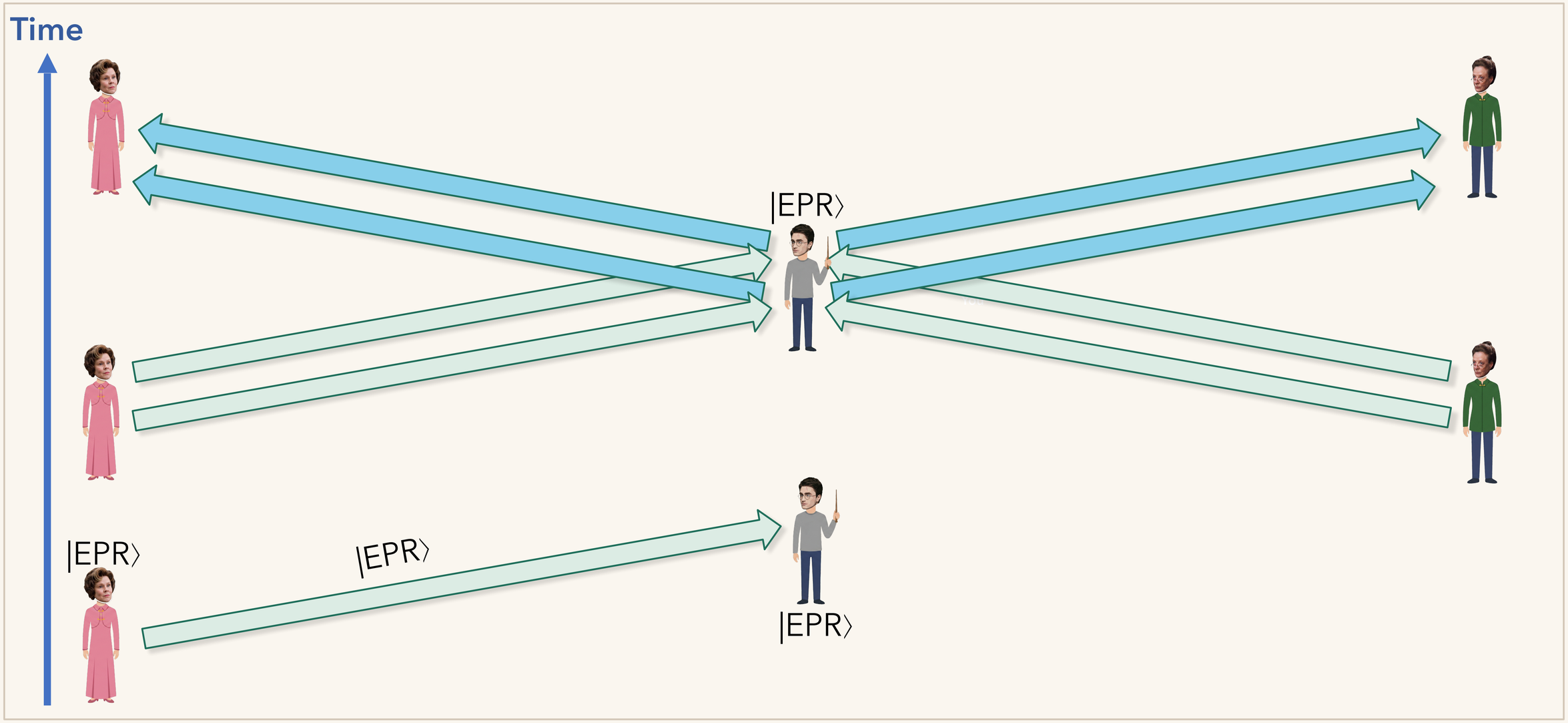
Task: Entanglement Localization



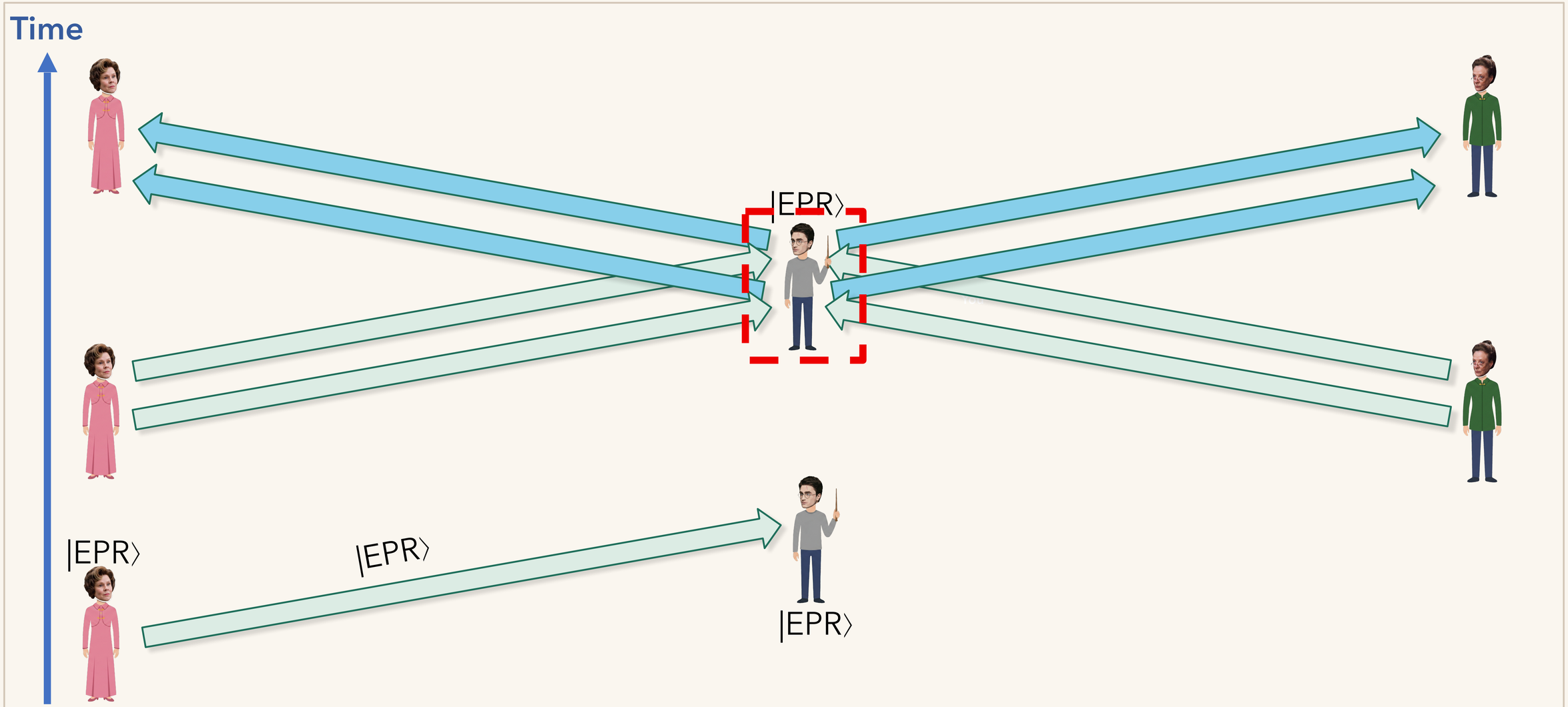
Task: Entanglement Localization



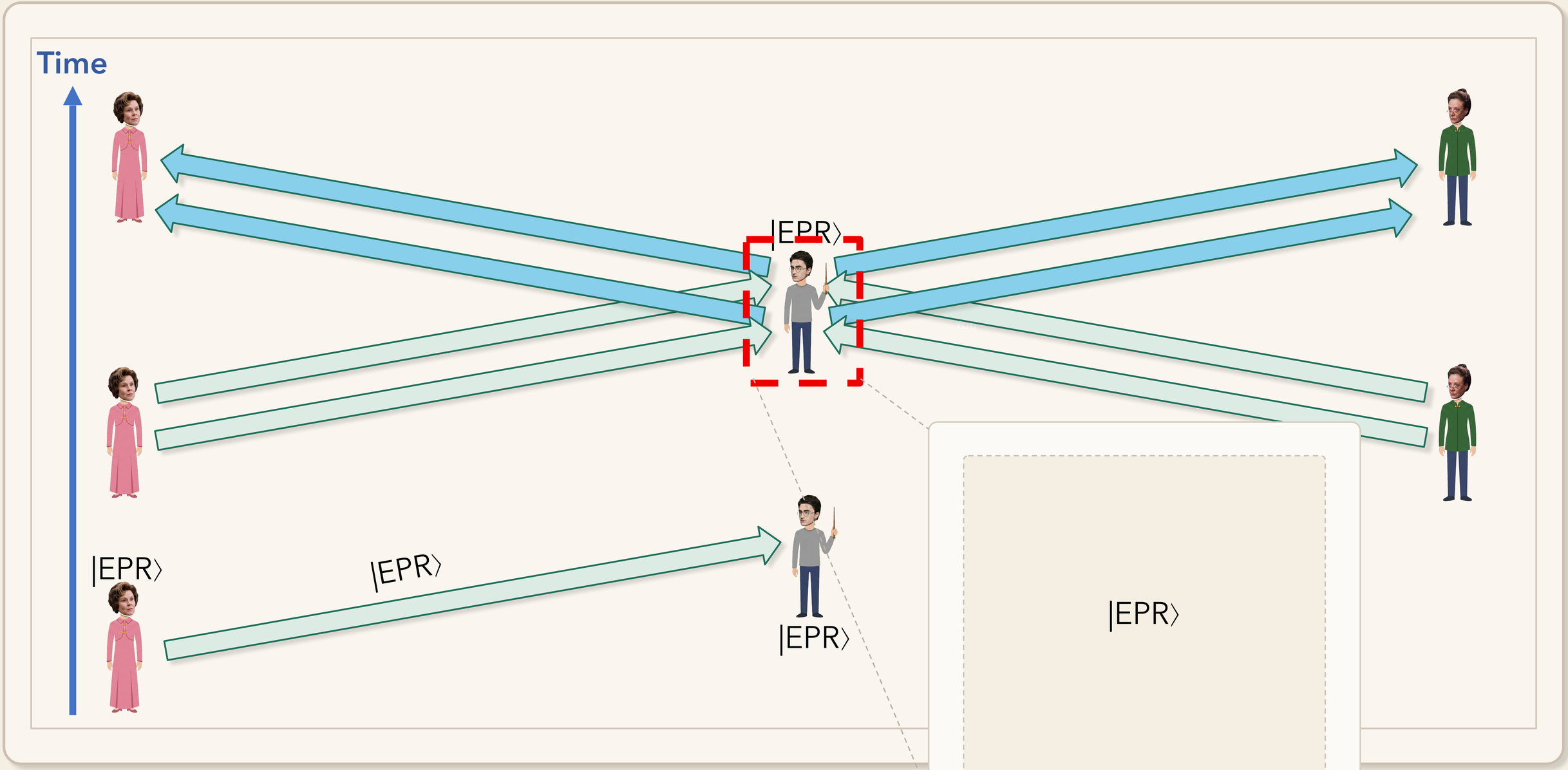
Task: Entanglement Localization



Task: Entanglement Localization

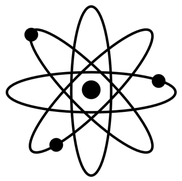


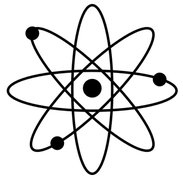
Task: Entanglement Localization



Task: Entanglement Localization

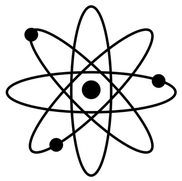
EPR Extraction:

 : “I am an EPR half”

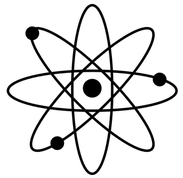


Task: Entanglement Localization

EPR Extraction:

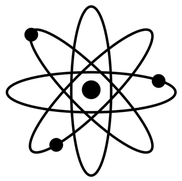
 : “I am an EPR half”

“Prove it”

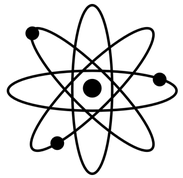


Task: Entanglement Localization

EPR Extraction:

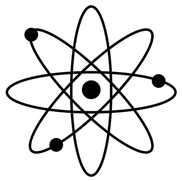


“Measure in the standard basis”

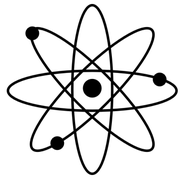


Task: Entanglement Localization

EPR Extraction:

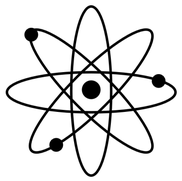
 : “I got $|0\rangle$”

“Measure in the standard basis”

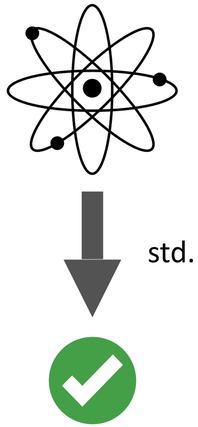


Task: Entanglement Localization

EPR Extraction:

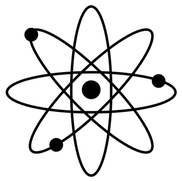

: “I got $|0\rangle$”

“Measure in the standard basis”

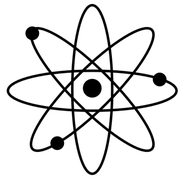


Task: Entanglement Localization

EPR Extraction:

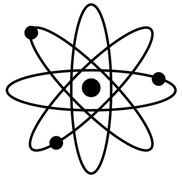


OR



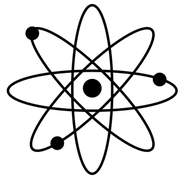
Task: Entanglement Localization

EPR Extraction:



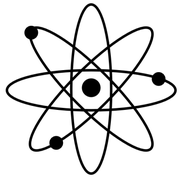
OR

“Measure in the Hadamard basis”



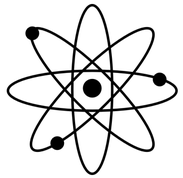
Task: Entanglement Localization

EPR Extraction:

 : “I got $|+\rangle$”

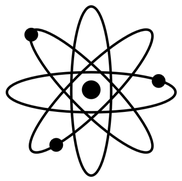
OR

“Measure in the Hadamard basis”



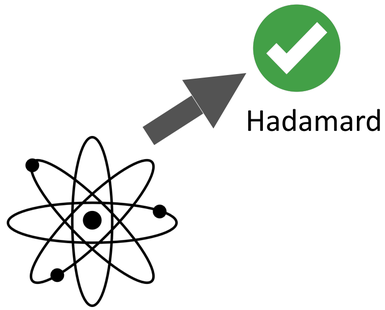
Task: Entanglement Localization

EPR Extraction:


: “I got $|+\rangle$”

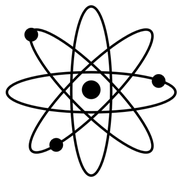
OR

“Measure in the Hadamard basis”



Task: Entanglement Localization

EPR Extraction:

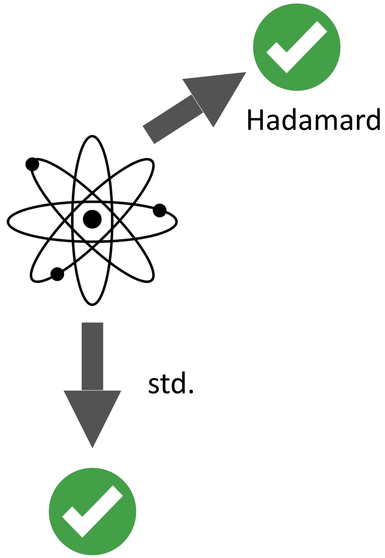


: “I got $|+\rangle$”

w.p. 1/2 **“Measure in the standard basis”**

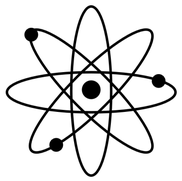
OR

w.p. 1/2 **“Measure in the Hadamard basis”**



Task: Entanglement Localization

EPR Extraction:

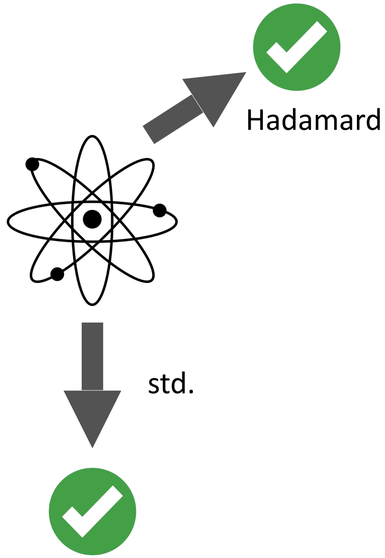


Assume
$\Pr[\text{win}] = 1 - \varepsilon$

w.p. 1/2 **“Measure in the standard basis”**

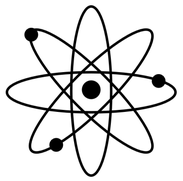
OR

w.p. 1/2 **“Measure in the Hadamard basis”**



Task: Entanglement Localization

EPR Extraction:



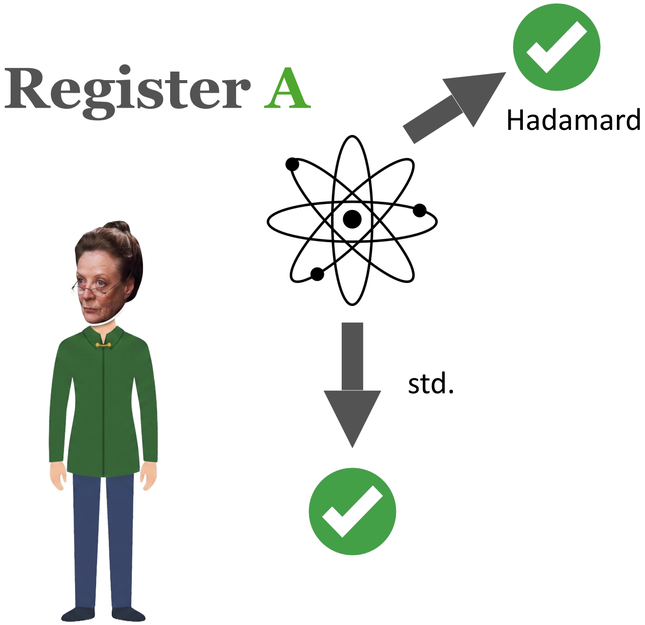
Register **B**

Assume
$\Pr[\text{win}] = 1 - \varepsilon$

w.p. 1/2 **“Measure in the standard basis”**

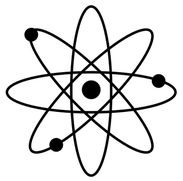
OR

w.p. 1/2 **“Measure in the Hadamard basis”**



Task: Entanglement Localization

EPR Extraction:



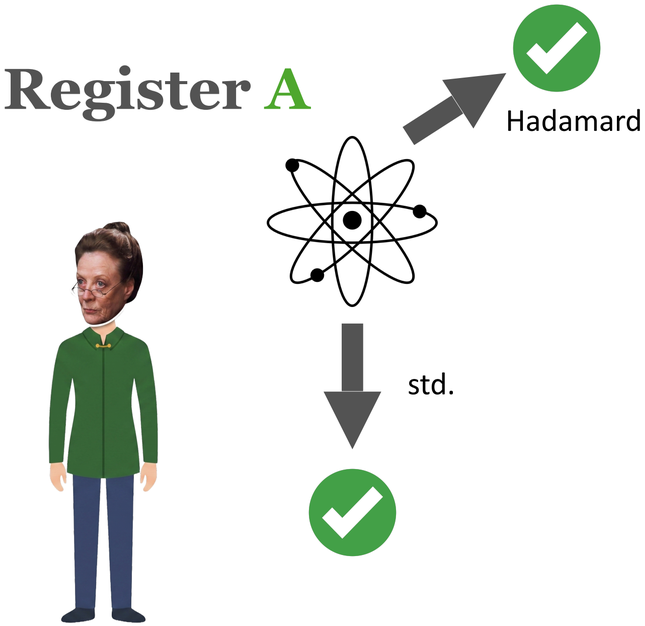
Register B

Assume
Pr[win] = 1 - ε

w.p. 1/2 **“Measure in the standard basis”**

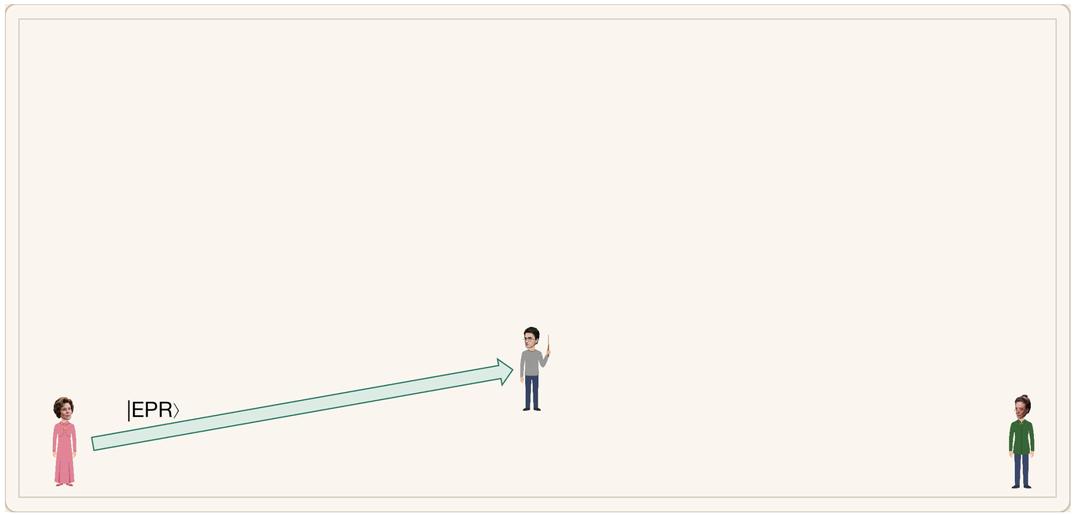
OR

w.p. 1/2 **“Measure in the Hadamard basis”**



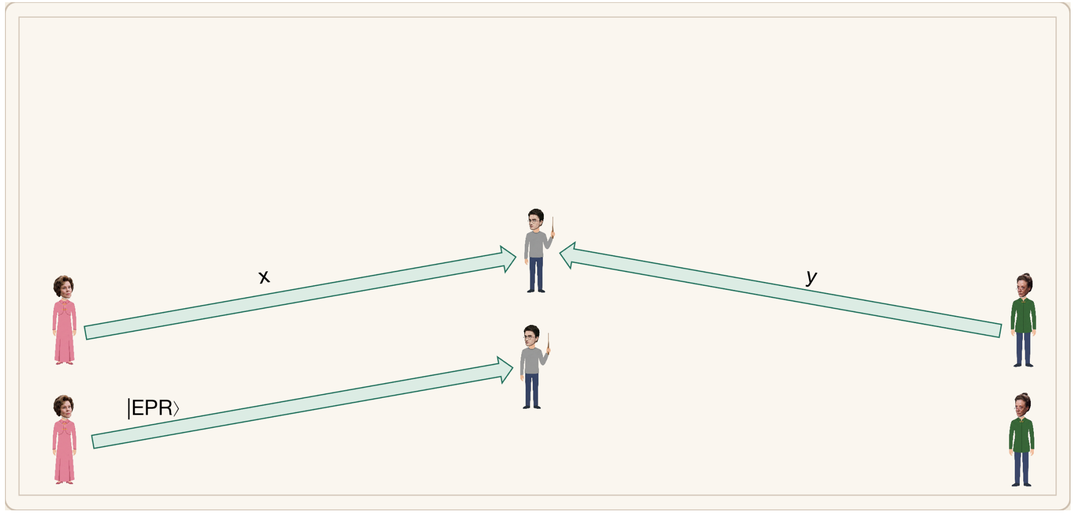
[VZ’21]: There exists an isometry E(B) -> CX such that the state on AC is ε-close to |EPR⟩

Task: Entanglement Localization



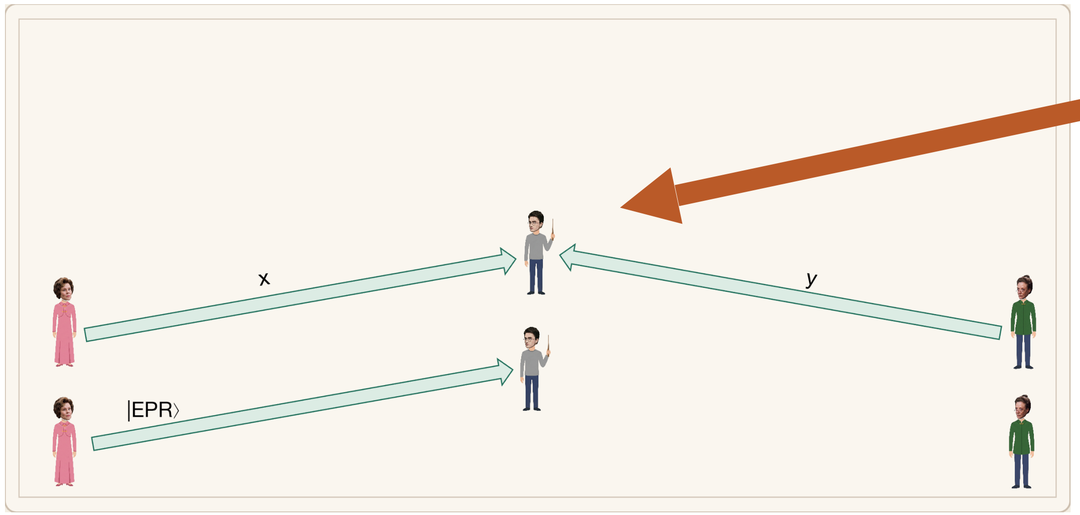
Doesn’t f-BB84 already include this measurement game?

Task: Entanglement Localization



Doesn’t f-BB84 already include this measurement game?

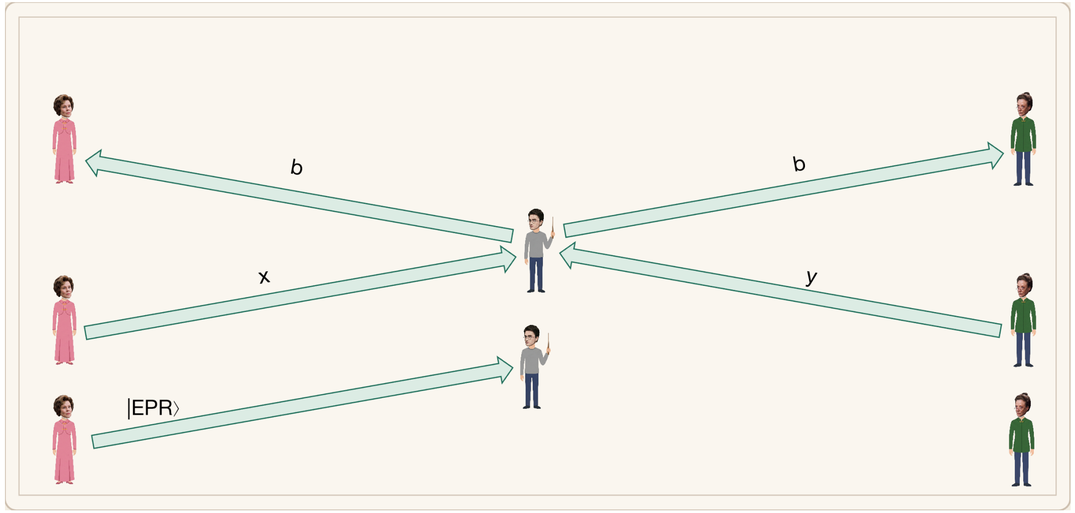
Task: Entanglement Localization



Can be either standard or Hadamard

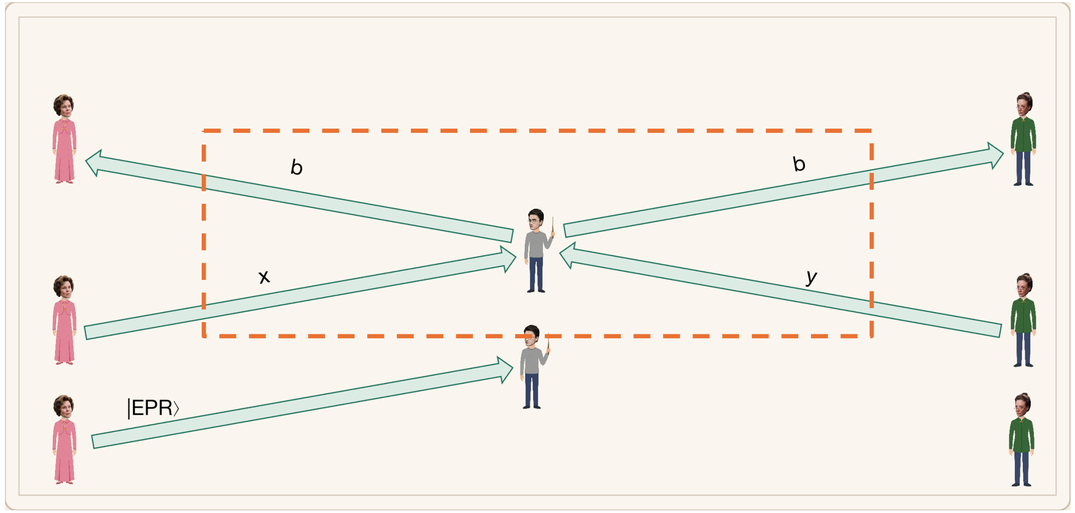
Doesn’t f-BB84 already include this measurement game?

Task: Entanglement Localization



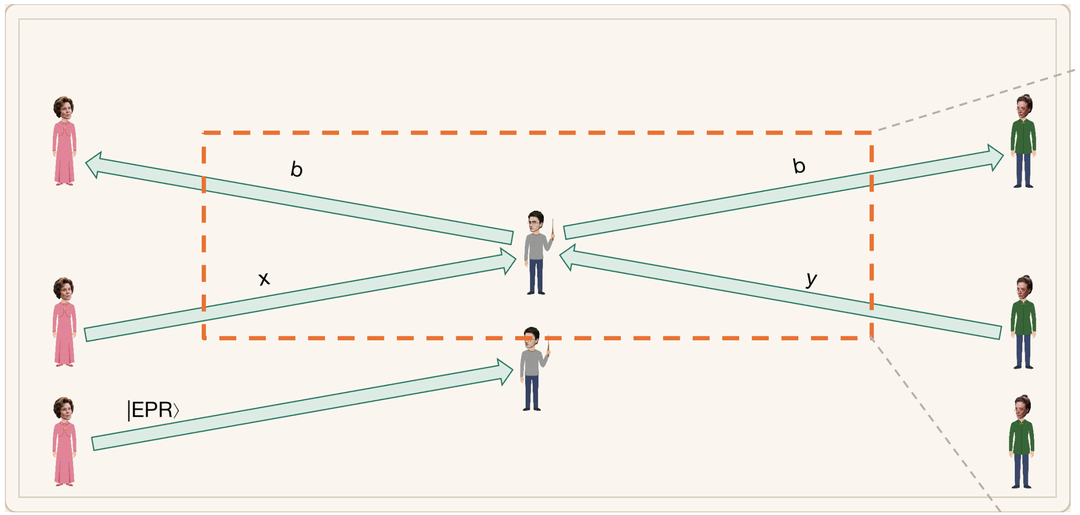
Doesn’t f-BB84 already include this measurement game?

Task: Entanglement Localization

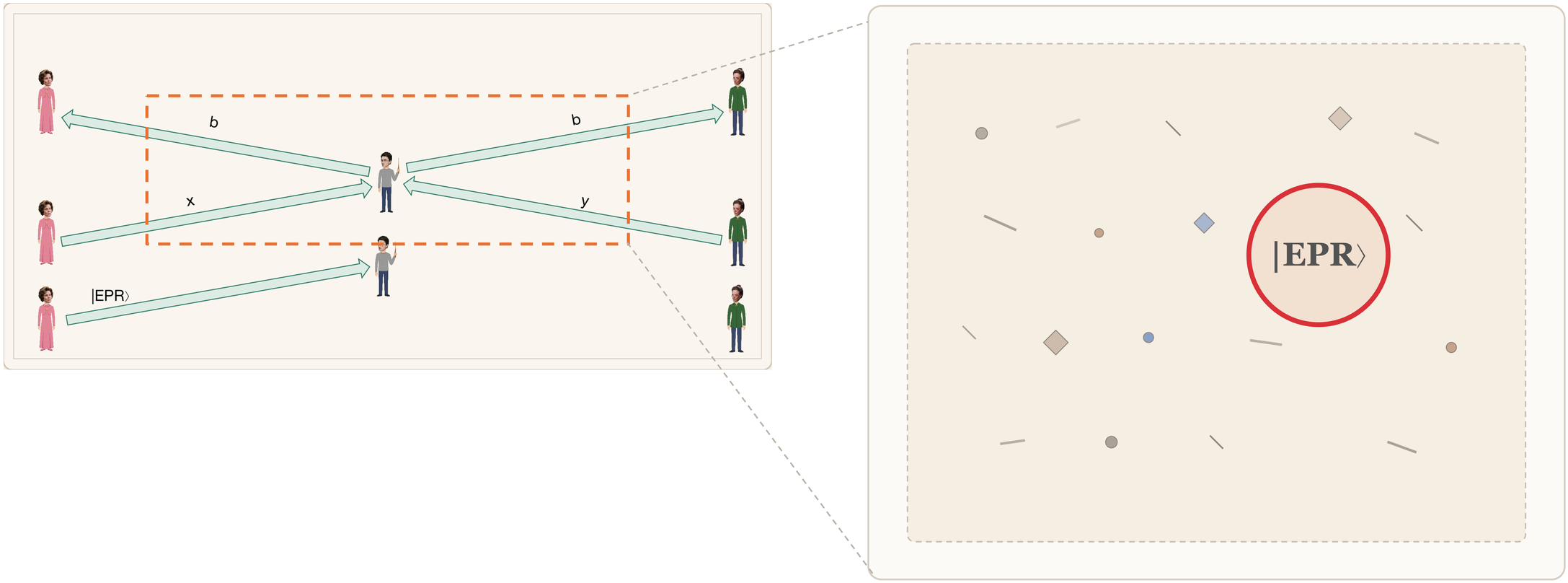


This box passes the [VZ'21] game with high probability, therefore ∃ isometry => ≈|EPR⟩

Task: Entanglement Localization

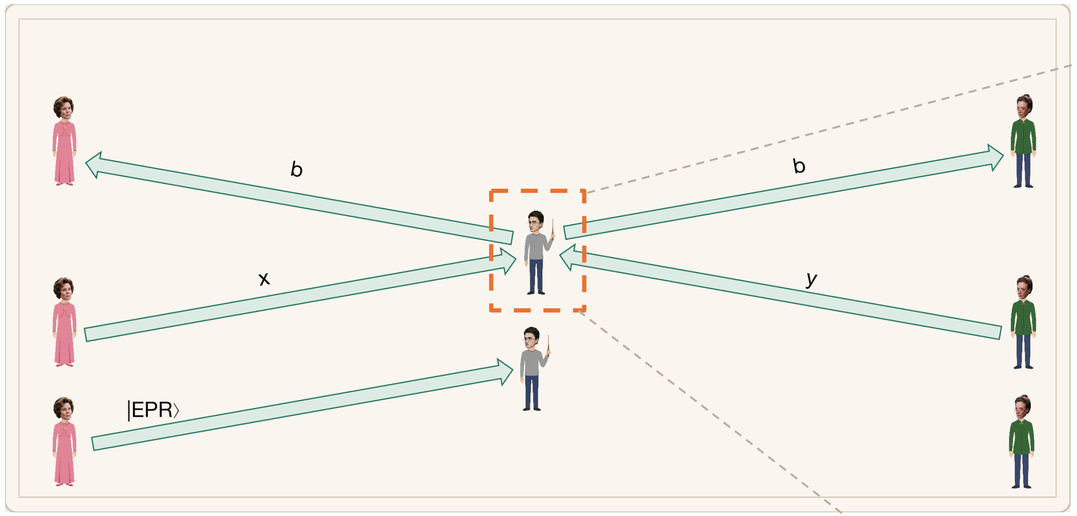


Task: Entanglement Localization



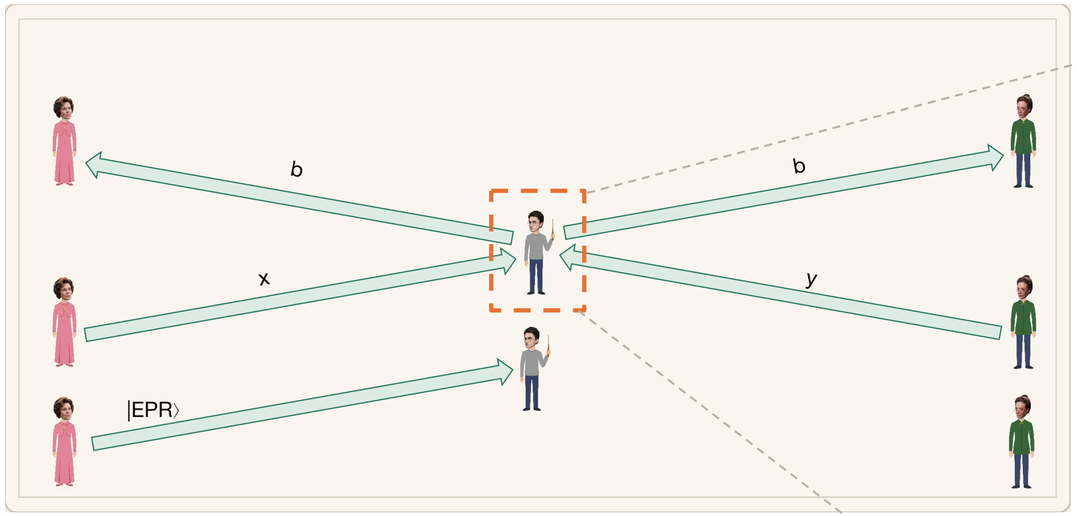
Sure, but… that box is huge. Want a claim only about the middle!

Task: Entanglement Localization



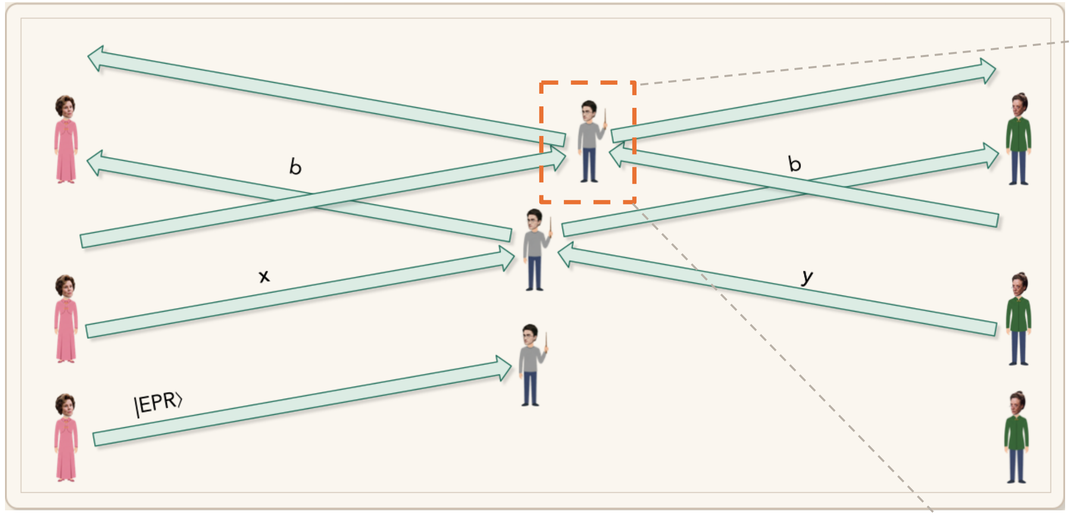
?

Task: Entanglement Localization



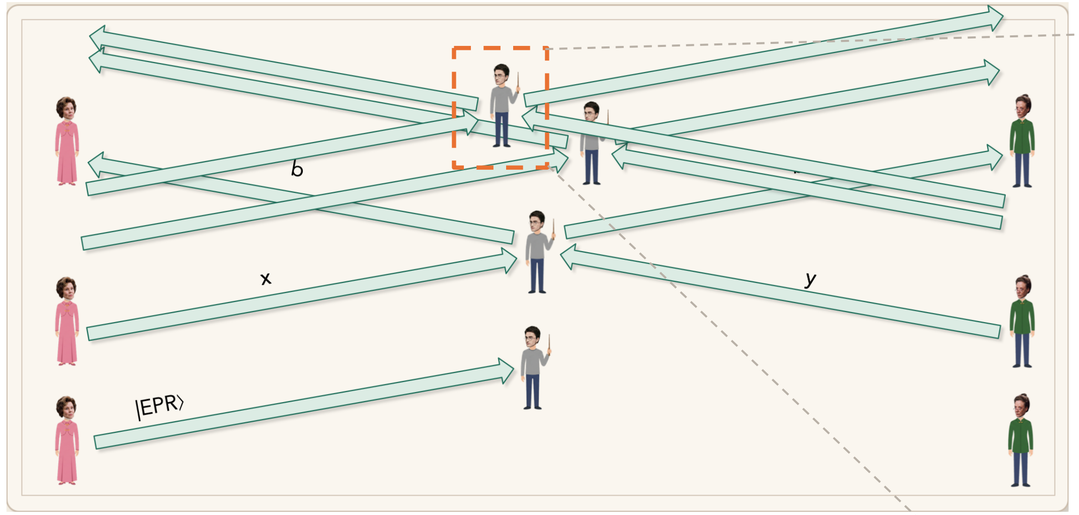
Also, what if this didn't destroy the EPR pair…

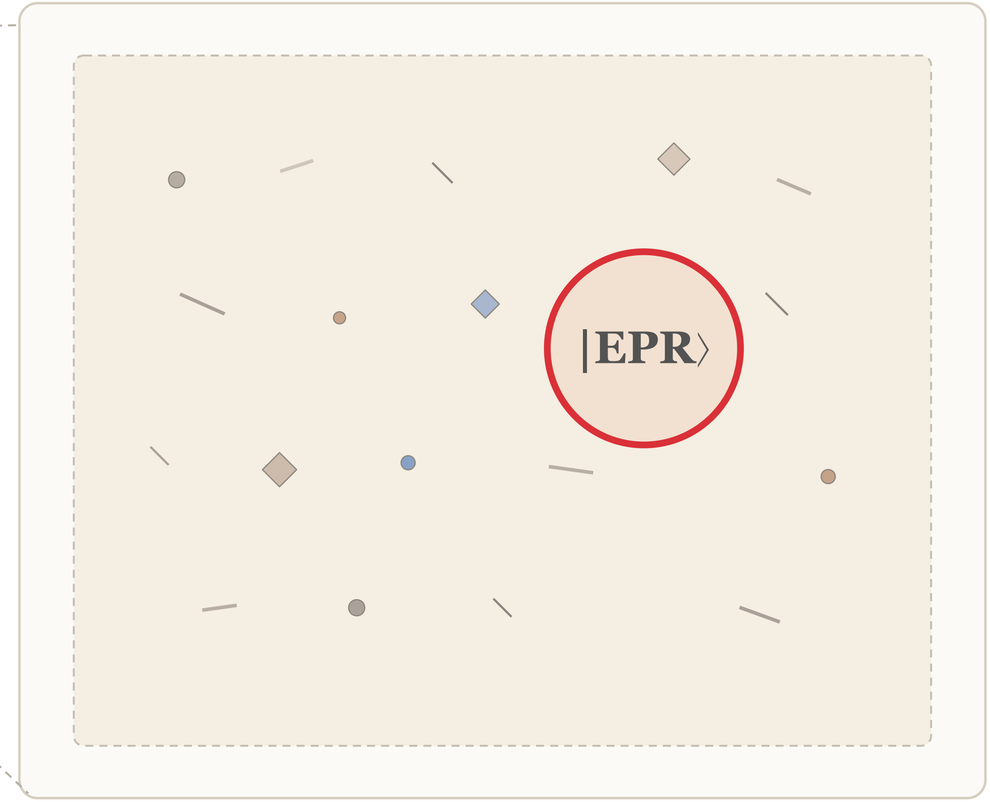
Task: Entanglement Localization



Also, what if this didn't destroy the EPR pair…

Task: Entanglement Localization





Also, what if this didn't destroy the EPR pair…

Task: Entanglement Localization

Task: Entanglement Localization

Main Questions:

Task: Entanglement Localization

Main Questions:

- *Can we localize entanglement to a small region?*

Task: Entanglement Localization

Main Questions:

- *Can we localize entanglement to a small region?*
- *Can we do so non-destructively?*

Task: Entanglement Localization

Main Questions:

- *Can we localize entanglement to a small region?*
- *Can we do so non-destructively?*

This work:

Task: Entanglement Localization

Main Questions:

- *Can we localize entanglement to a small region?*
- *Can we do so non-destructively?*

This work:

1. **Not without new protocols:** f-BB84 admits distributed and *non-localizable* prover strategies.

Task: Entanglement Localization

Main Questions:

- *Can we localize entanglement to a small region?*
- *Can we do so non-destructively?*

This work:

1. **Not without new protocols:** f-BB84 admits distributed and *non-localizable* prover strategies.

Task: Entanglement Localization

Main Questions:

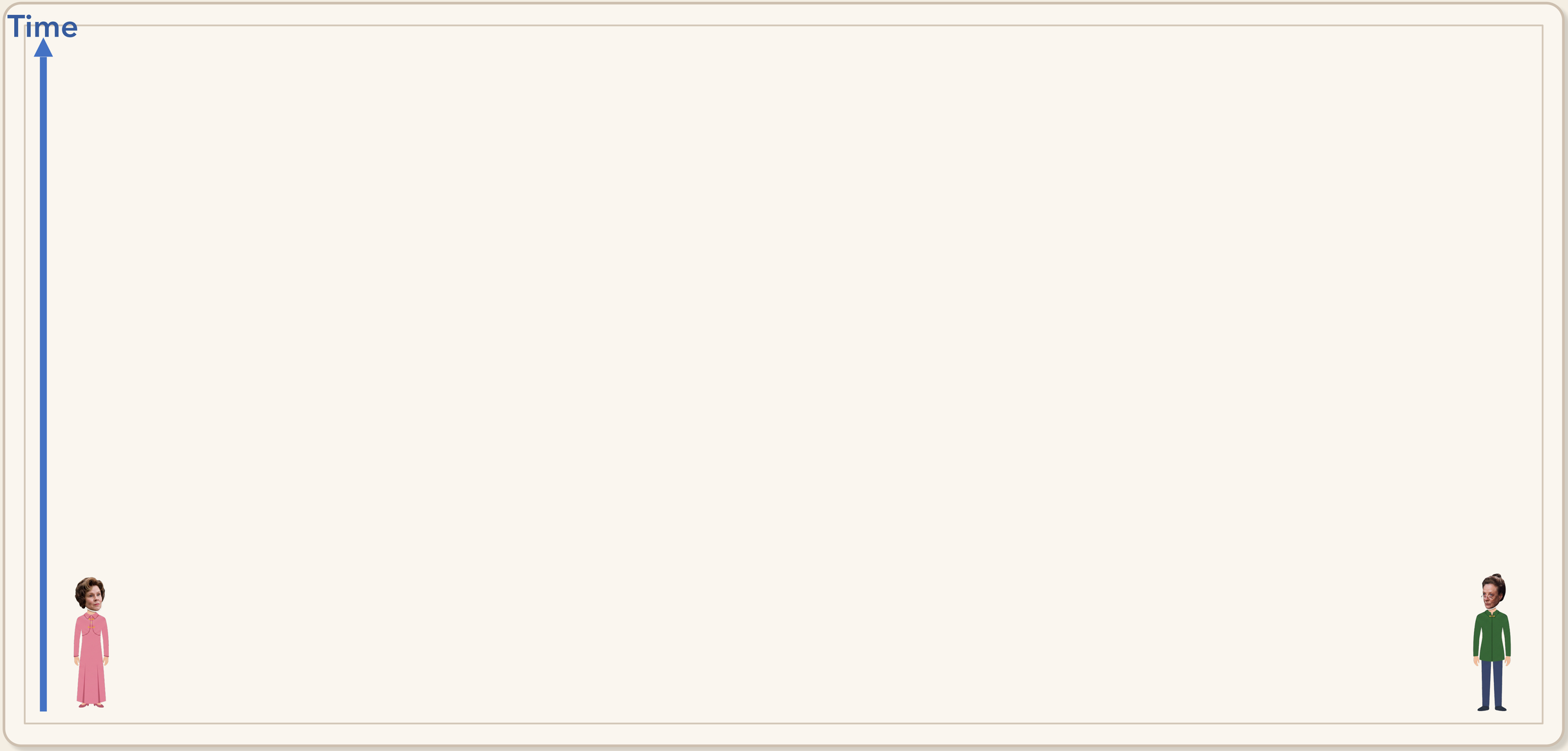
- *Can we localize entanglement to a small region?*
- *Can we do so non-destructively?*

This work:

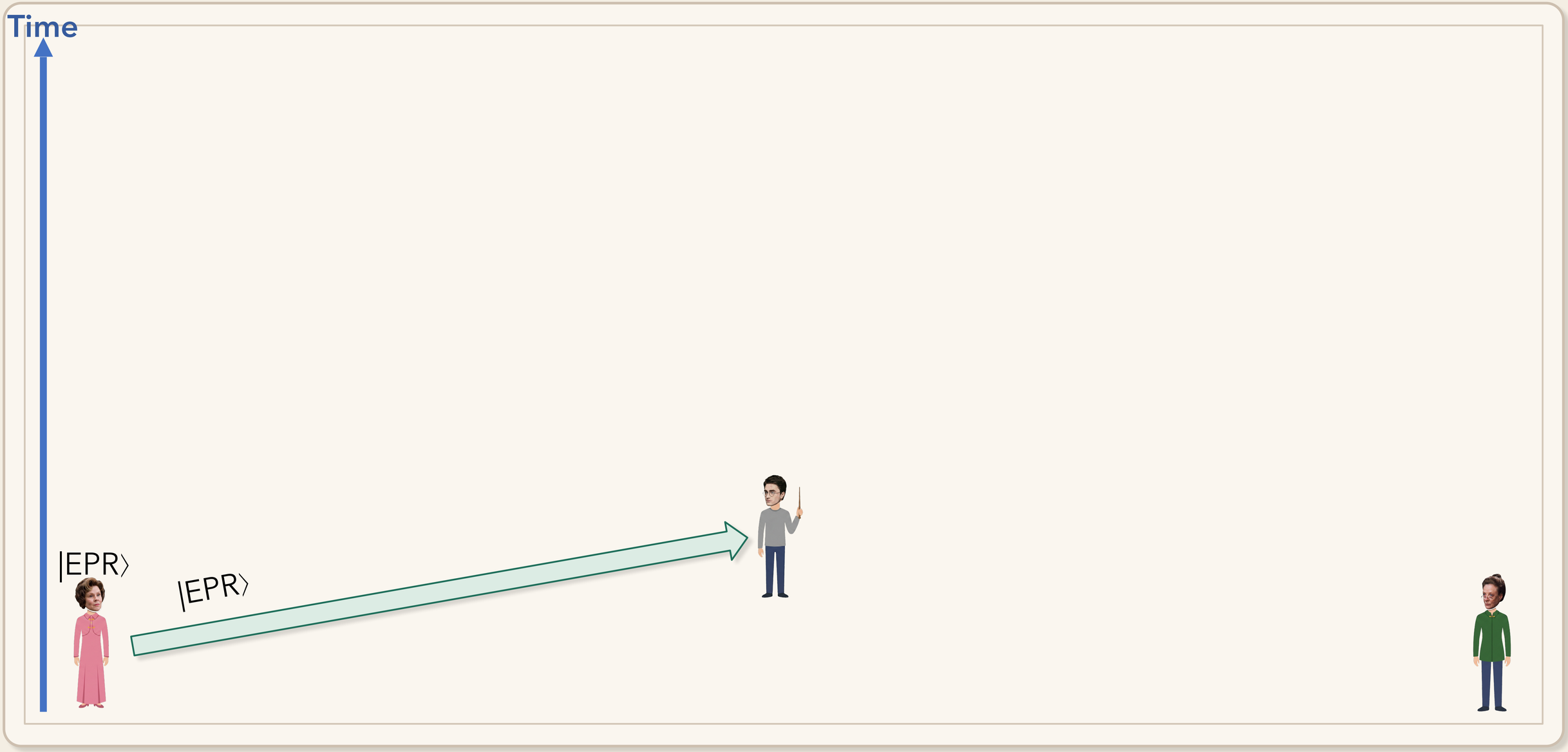
1. **Not without new protocols:** f-BB84 admits distributed and *non-localizable* prover strategies.

2. **With oracles, it's possible:** We construct non-destructive entanglement protocols in the *classical oracle model*. The state is extracted from an arbitrarily small region around the target.

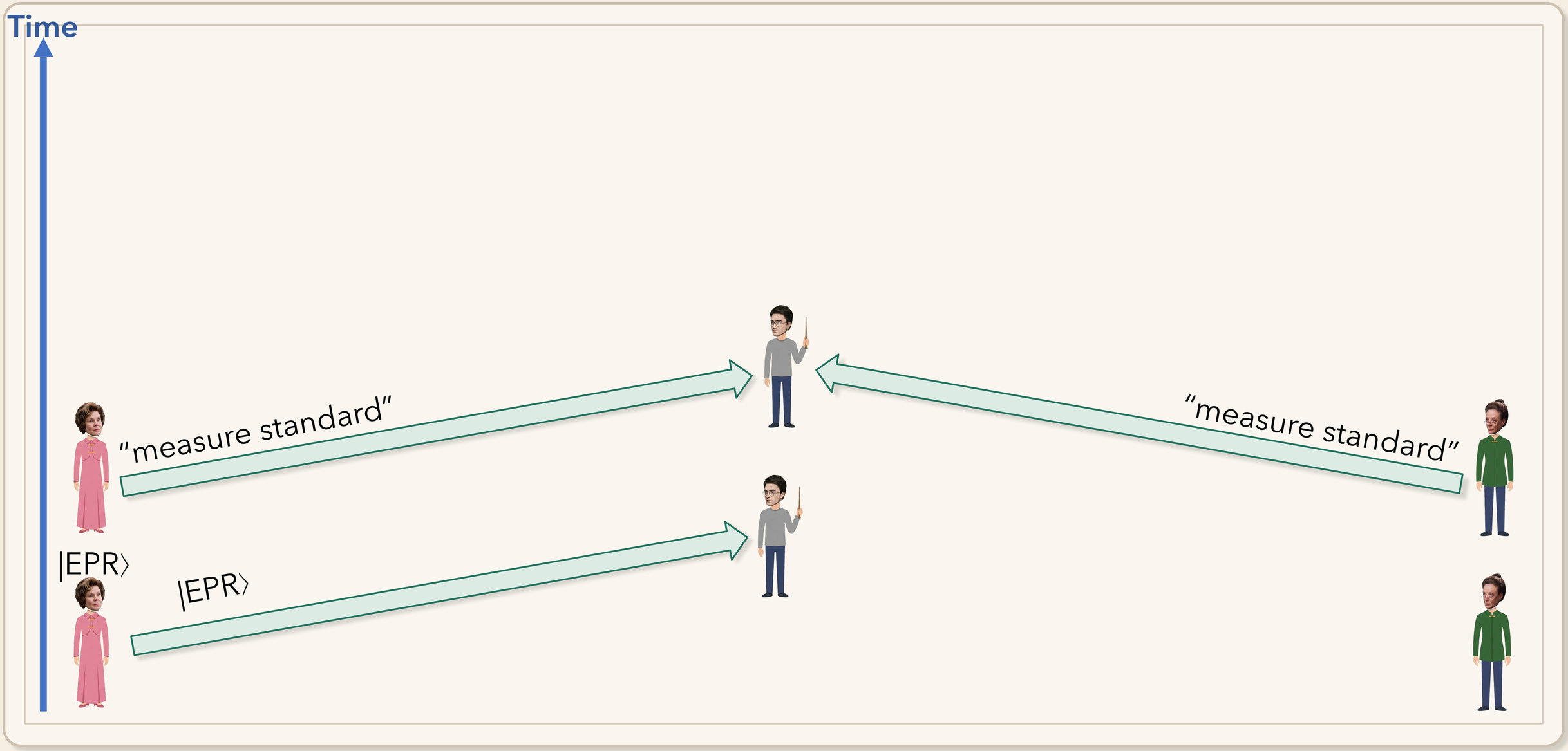
Precise Localization via Non-Destructive Tests



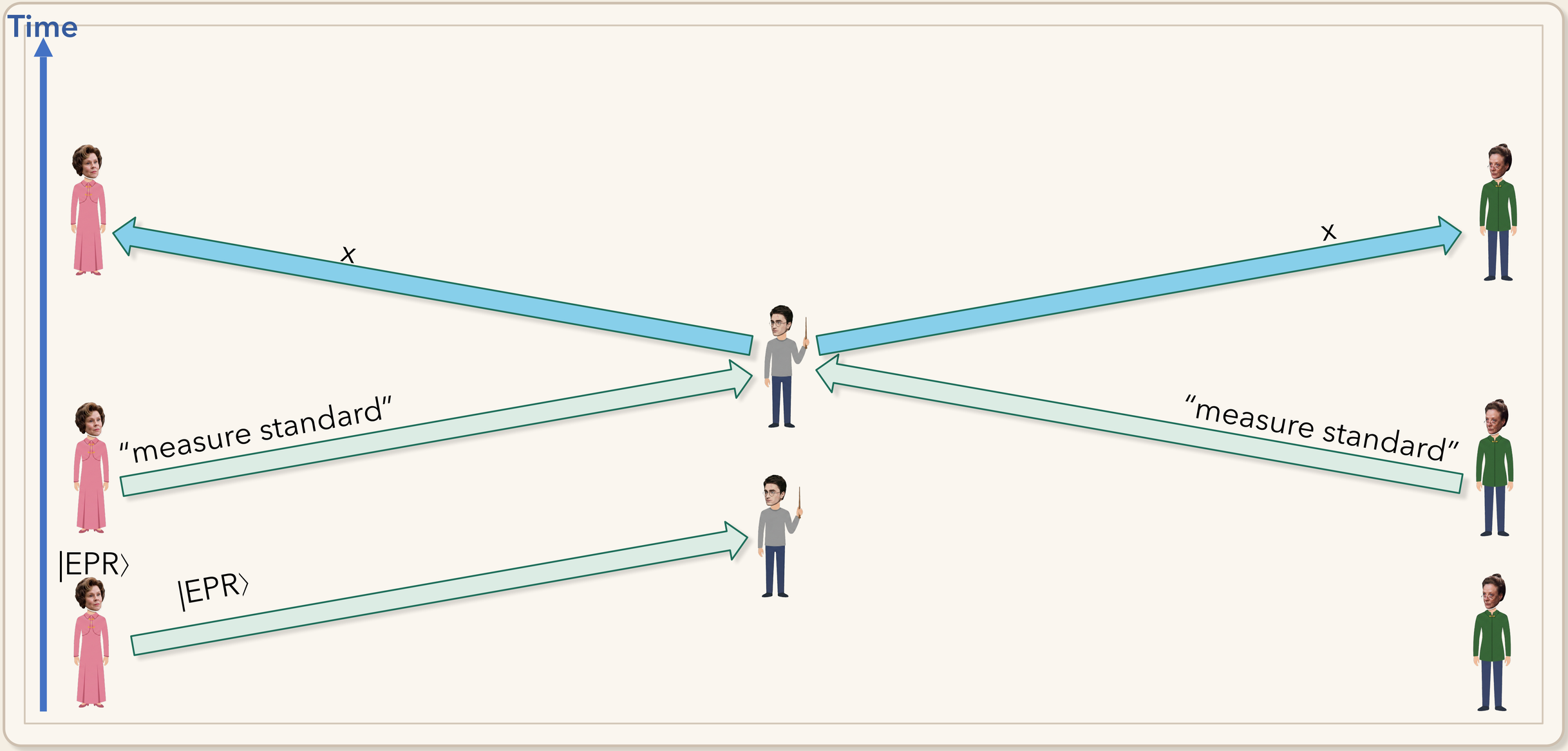
Precise Localization via Non-Destructive Tests



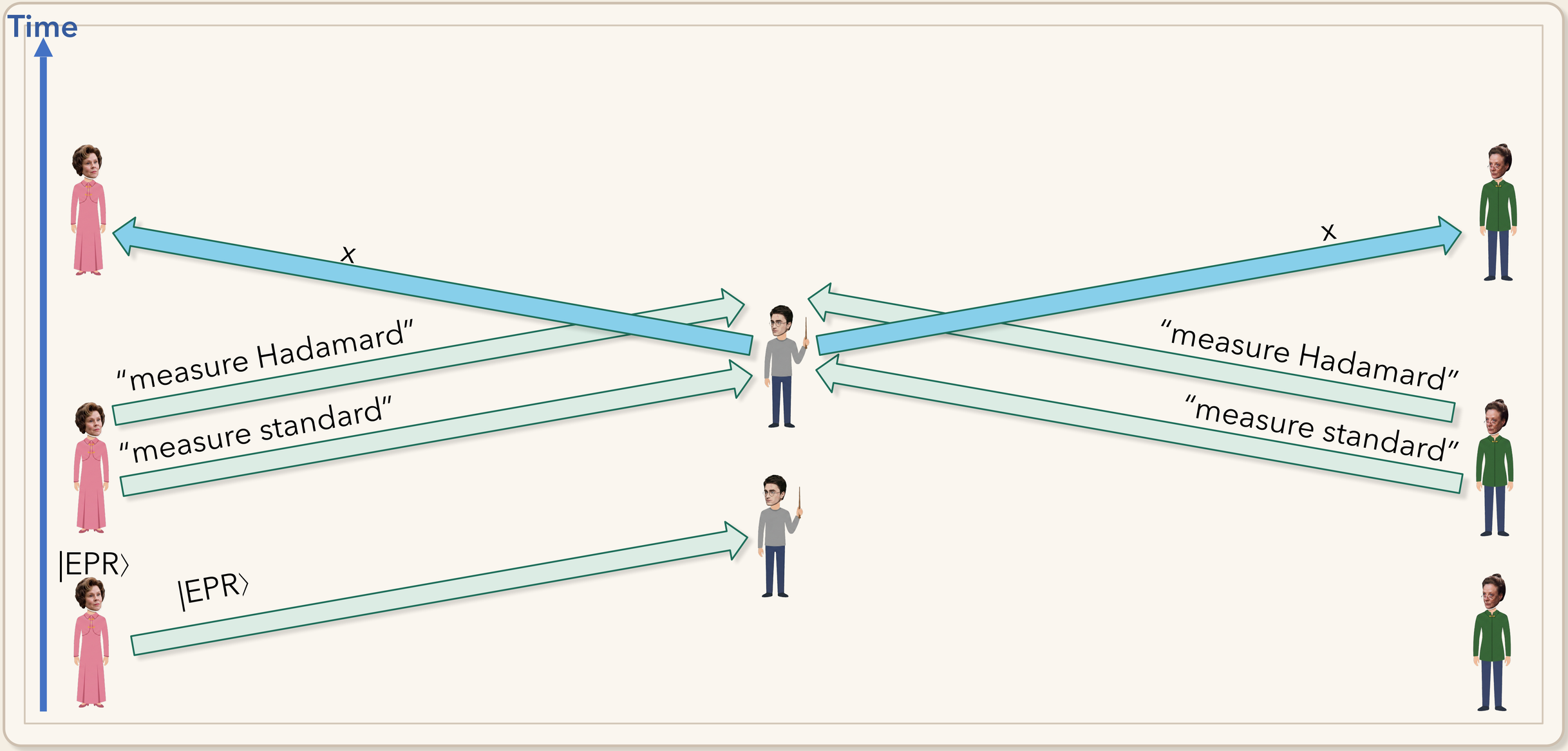
Precise Localization via Non-Destructive Tests



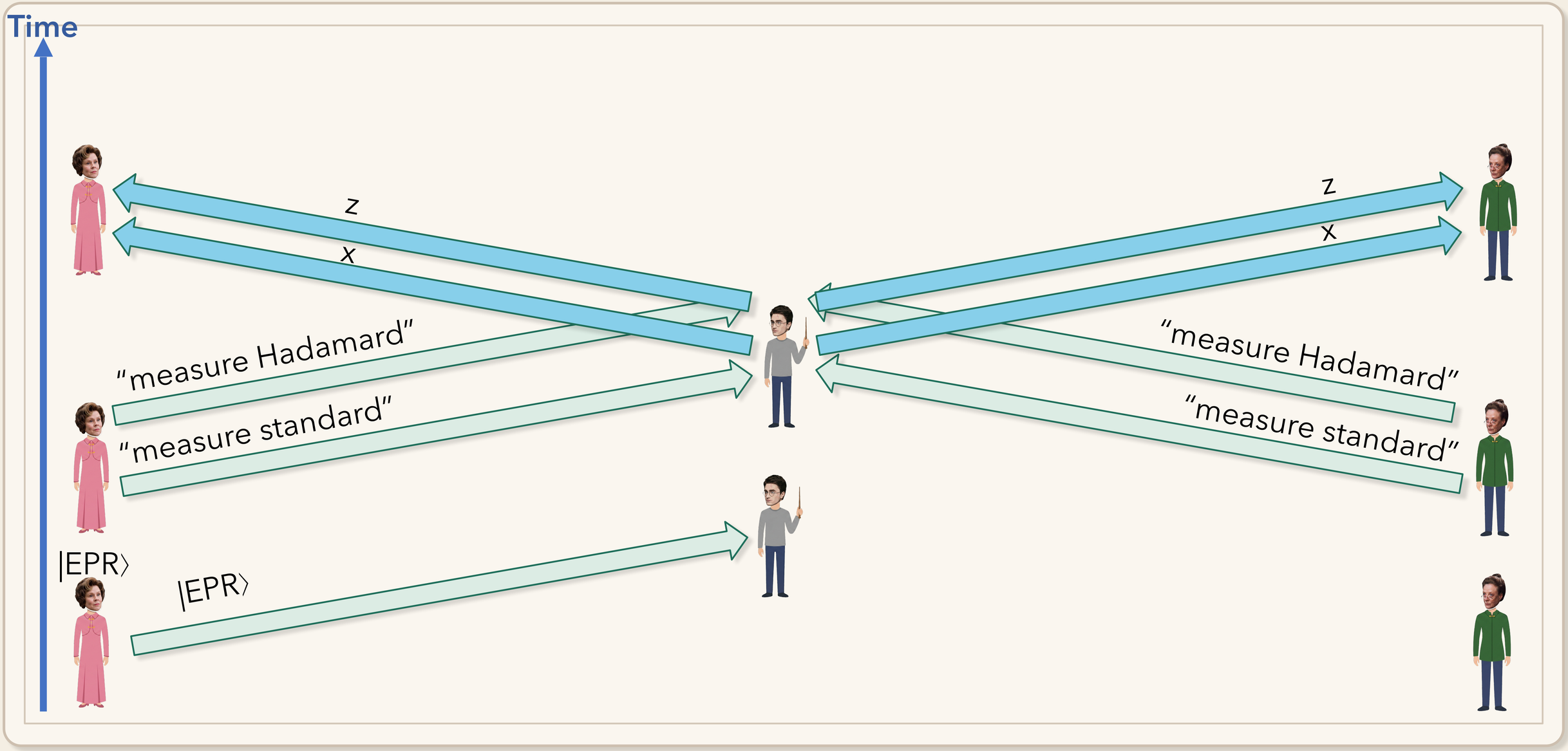
Precise Localization via Non-Destructive Tests



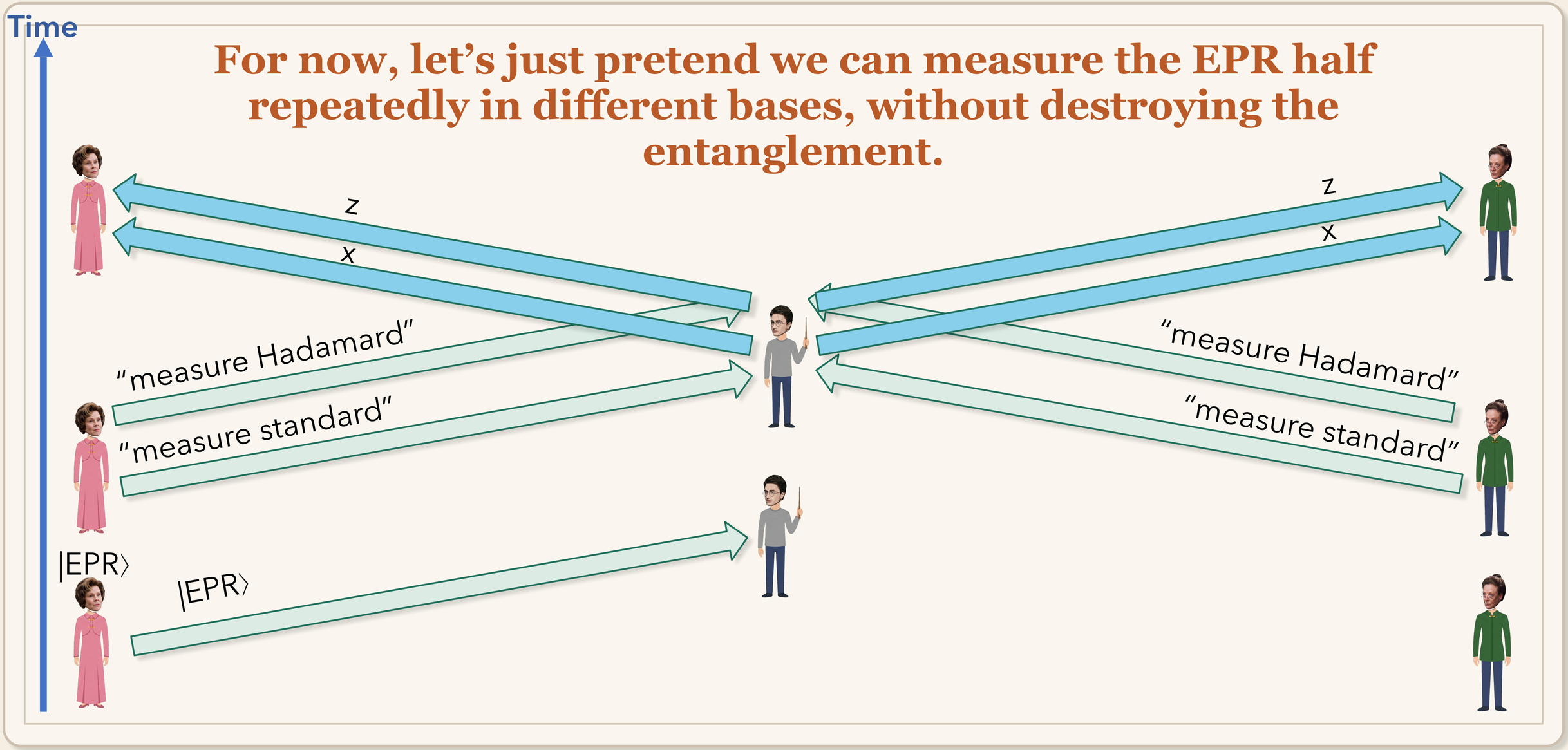
Precise Localization via Non-Destructive Tests



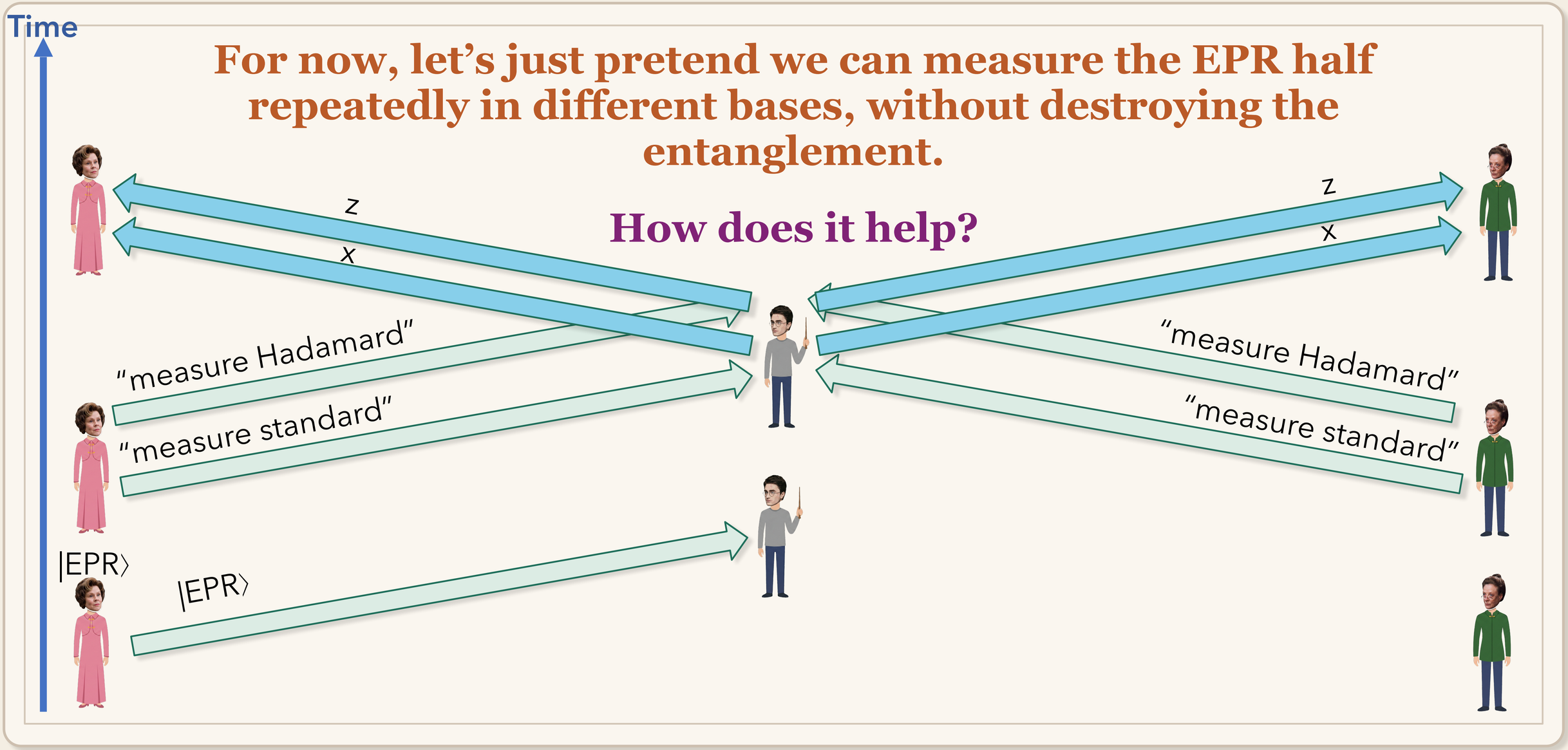
Precise Localization via Non-Destructive Tests



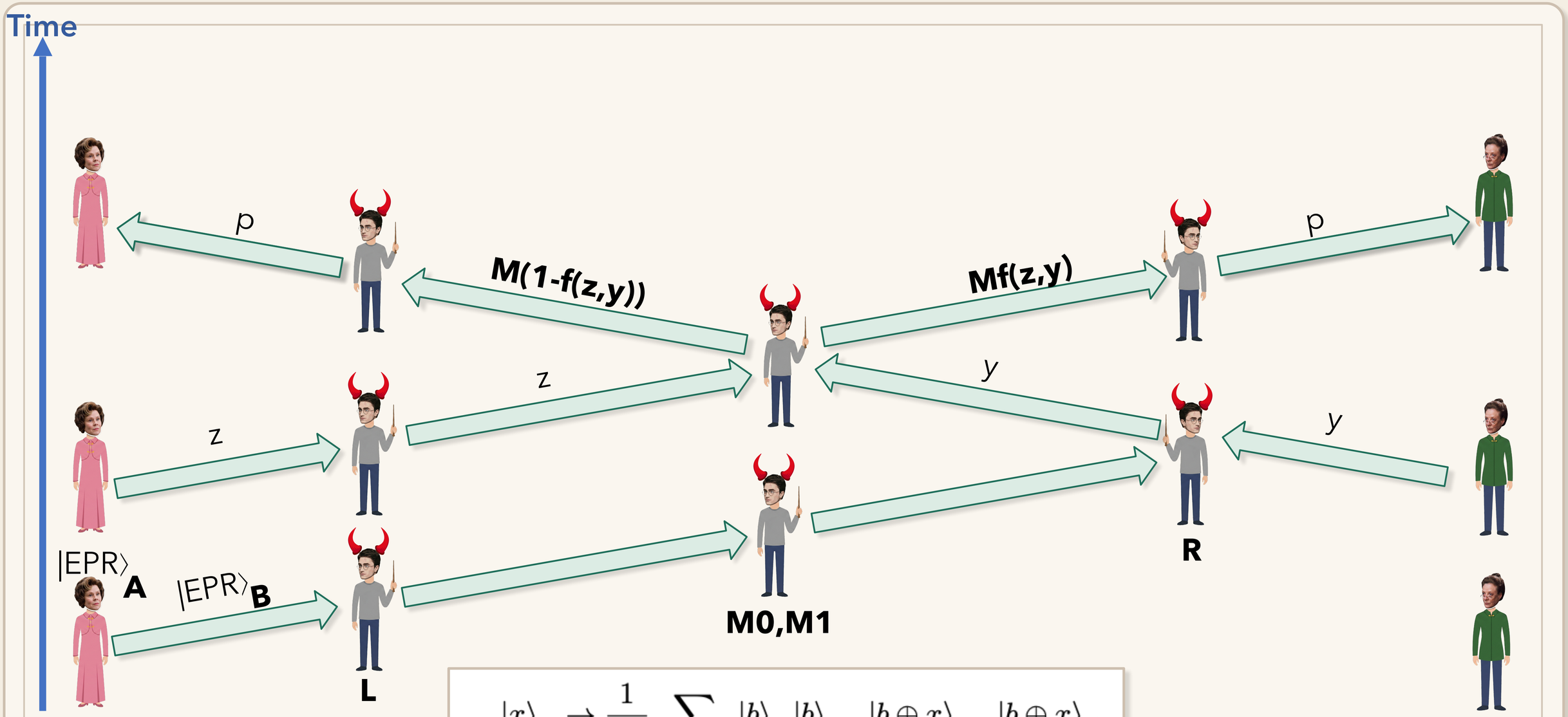
Precise Localization via Non-Destructive Tests



Precise Localization via Non-Destructive Tests

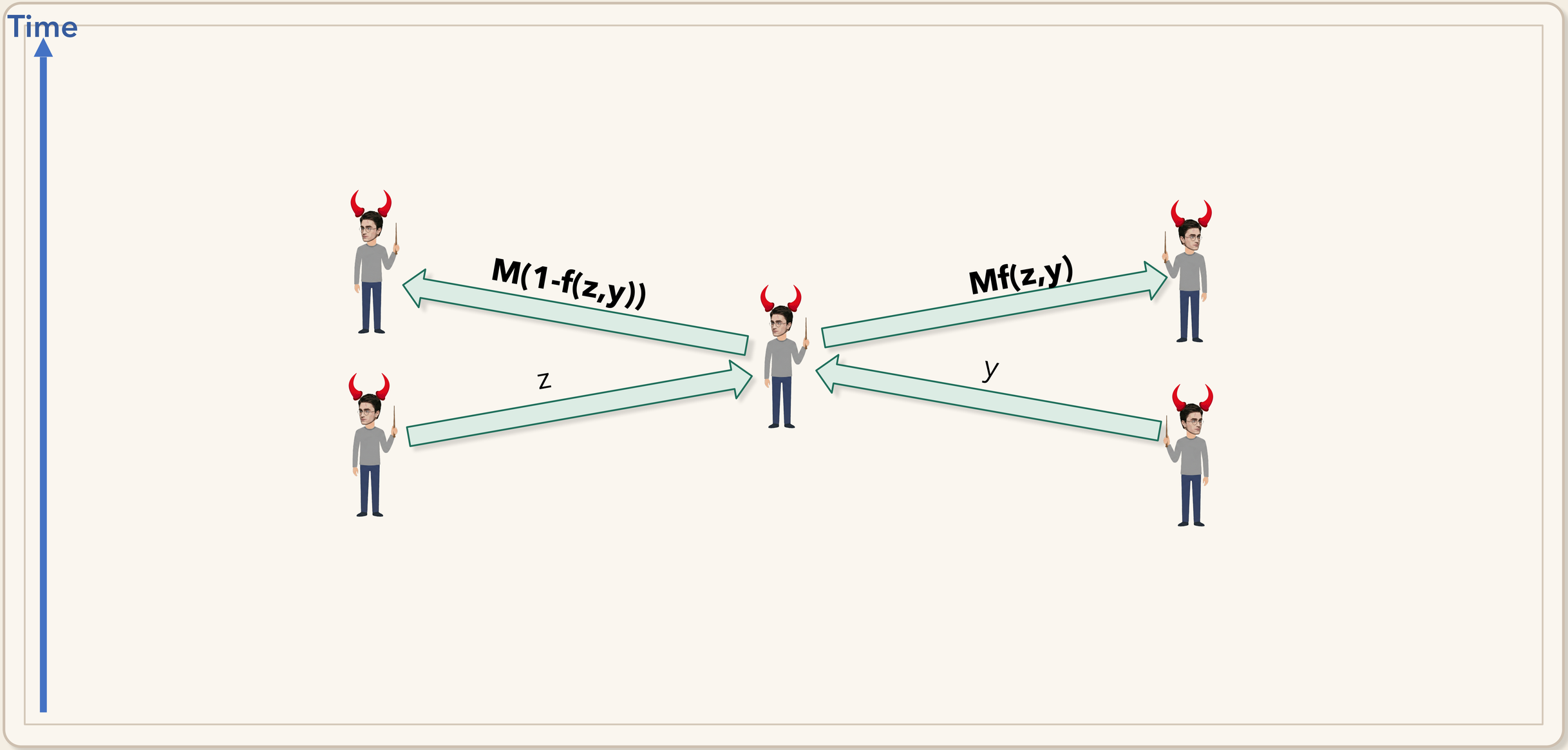


(FLASHBACK) Non-Localizability of f-BB84



$$|x\rangle_{\mathbf{B}} \to \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} |b\rangle_{\mathbf{L}} |b\rangle_{\mathbf{M}_0} |b\oplus x\rangle_{\mathbf{M}_1} |b\oplus x\rangle_{\mathbf{R}}$$

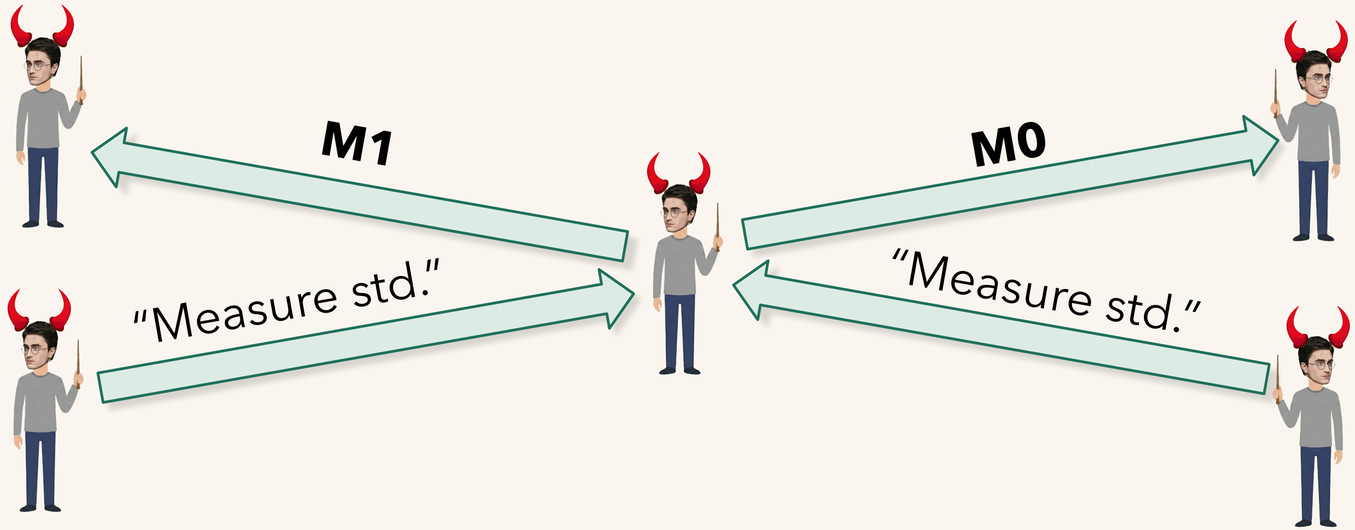
(FLASHBACK) Non-Localizability of f-BB84



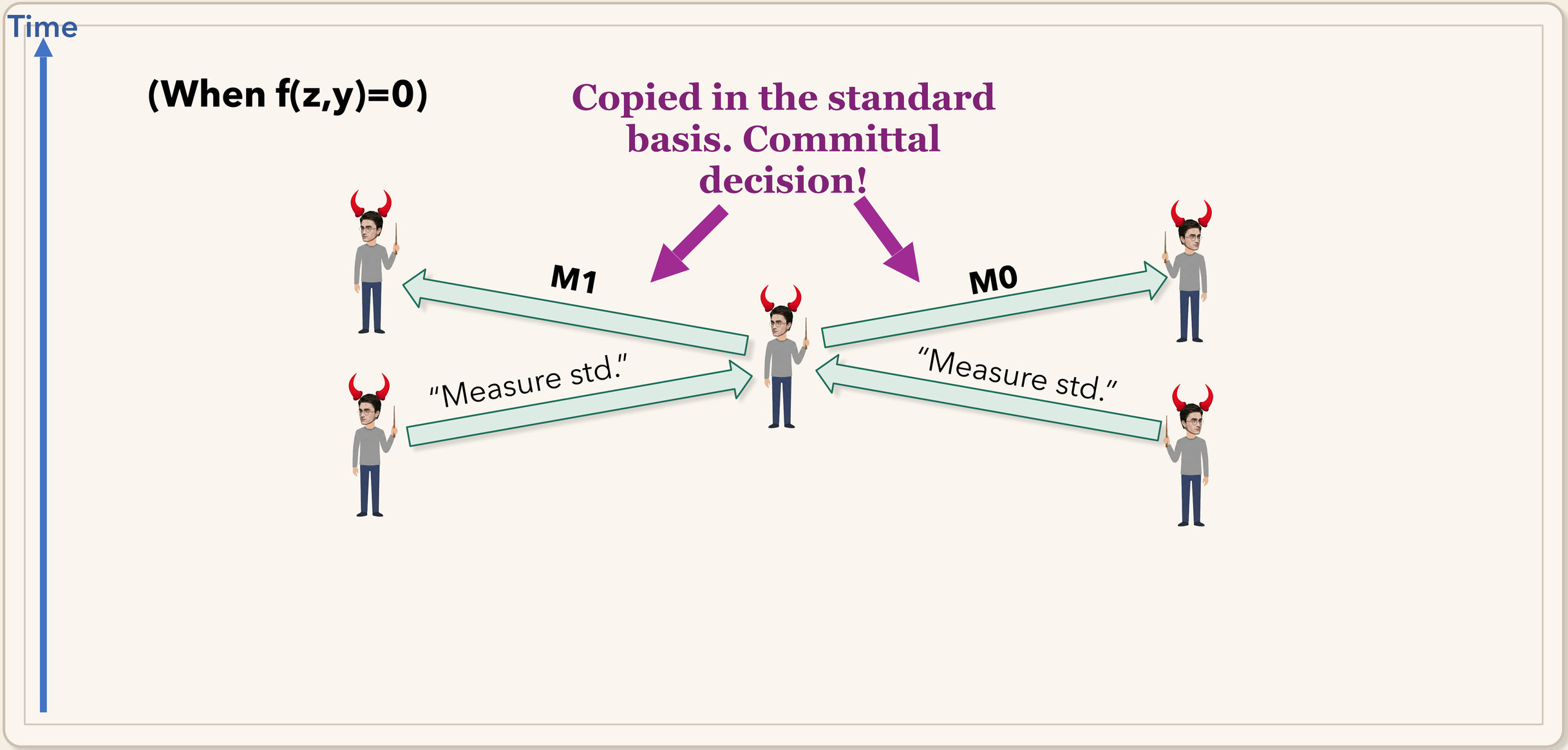
(FLASHBACK) Non-Localizability of f-BB84

Time

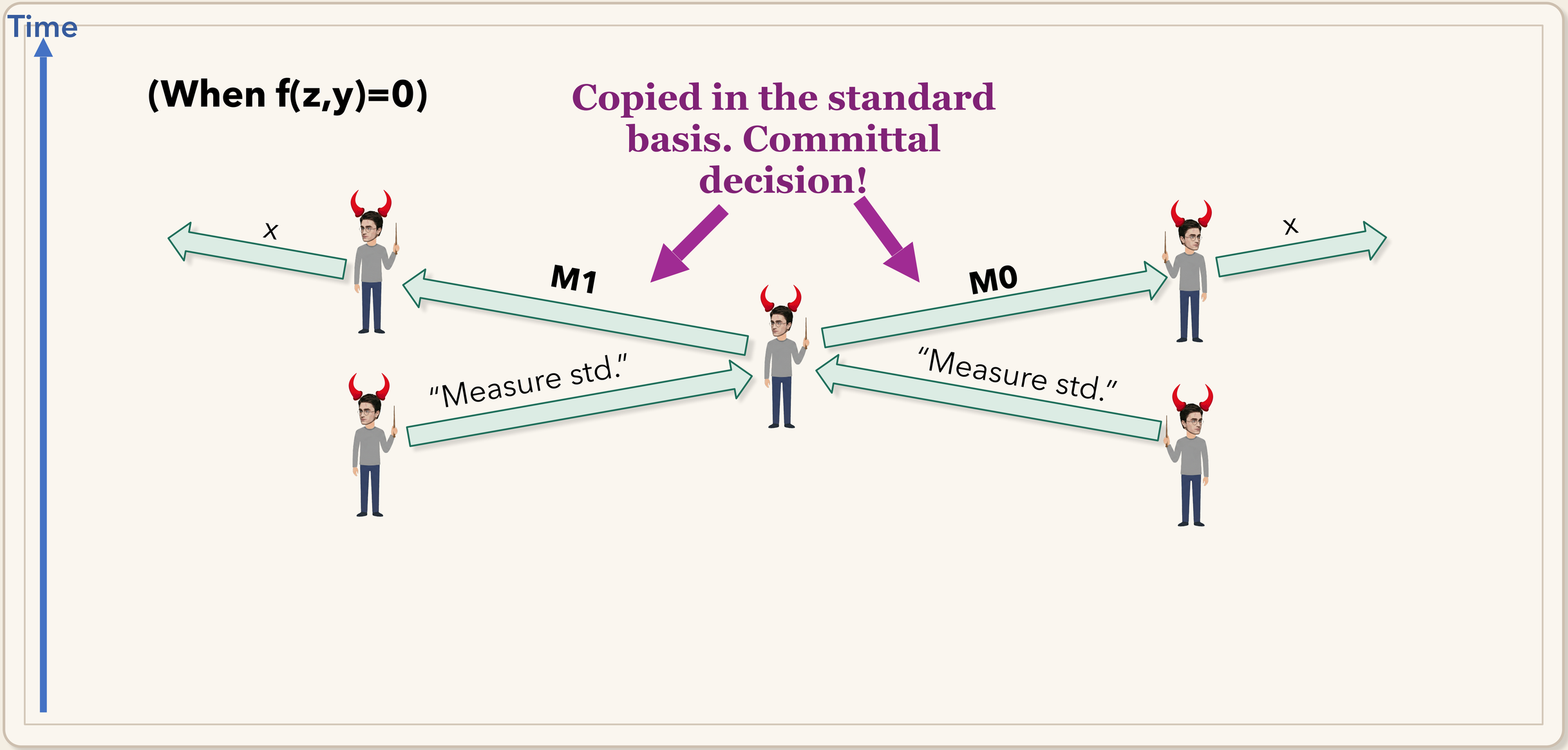
(When f(z,y)=0)



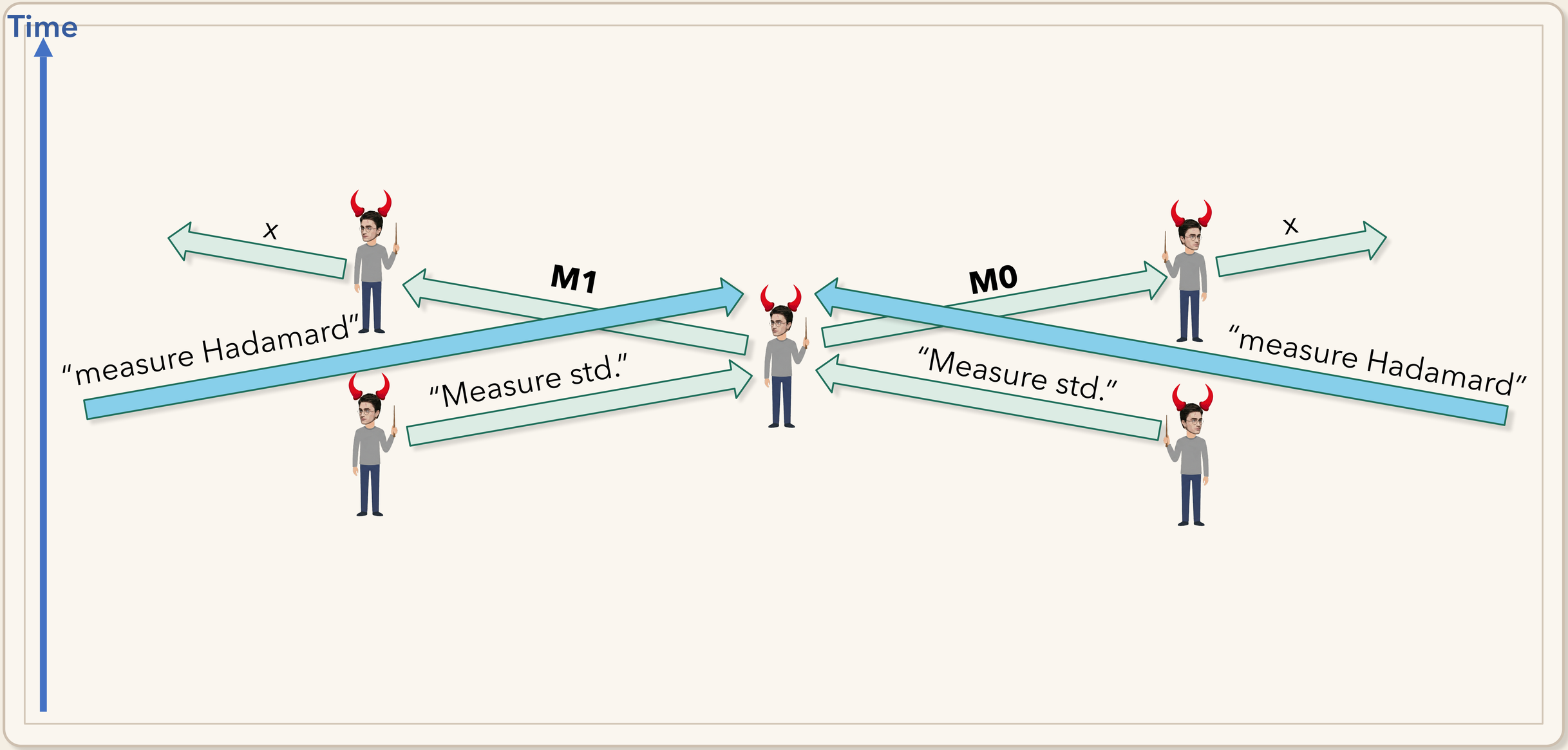
(FLASHBACK) Non-Localizability of f-BB84



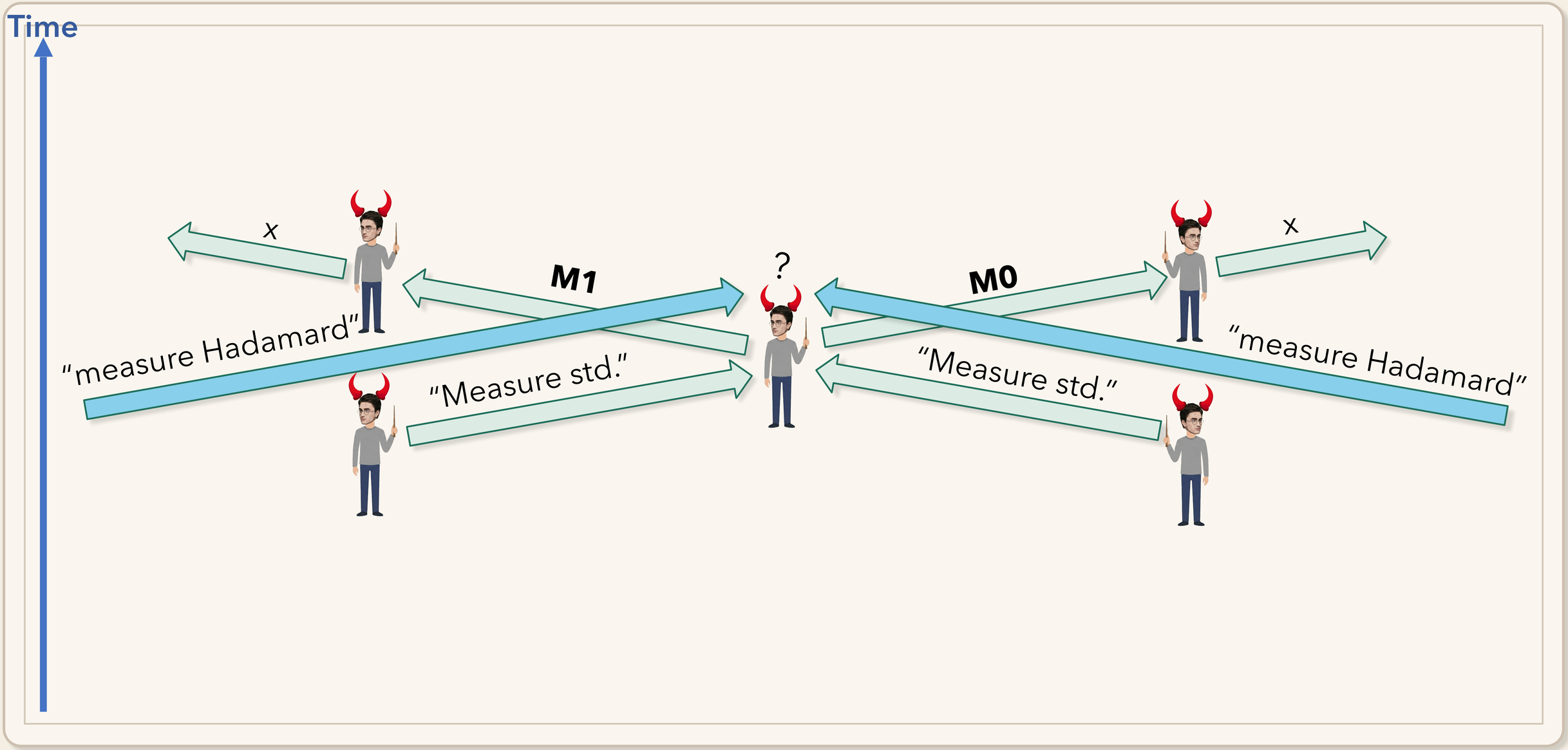
(FLASHBACK) Non-Localizability of f-BB84



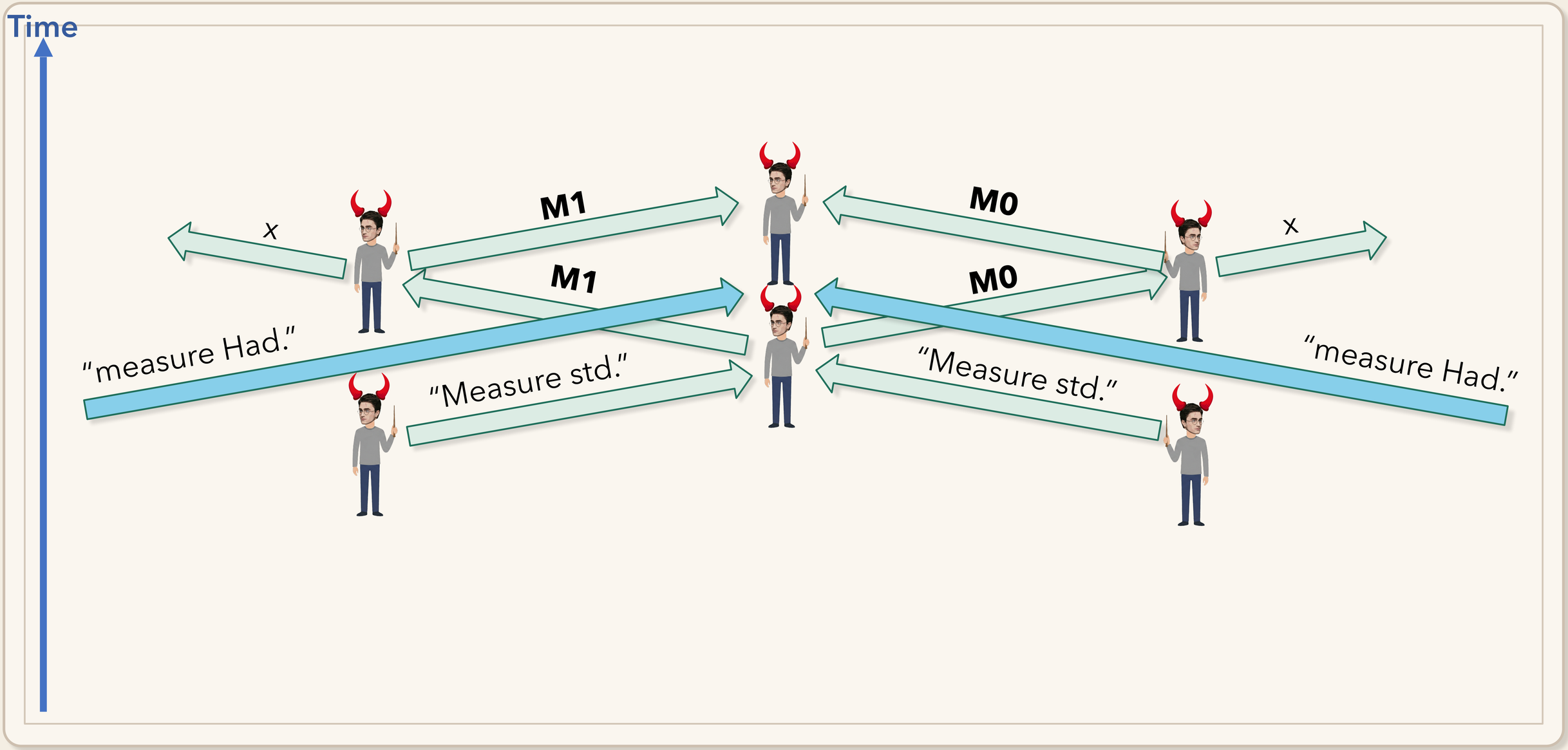
(FLASHBACK) Non-Localizability of f-BB84



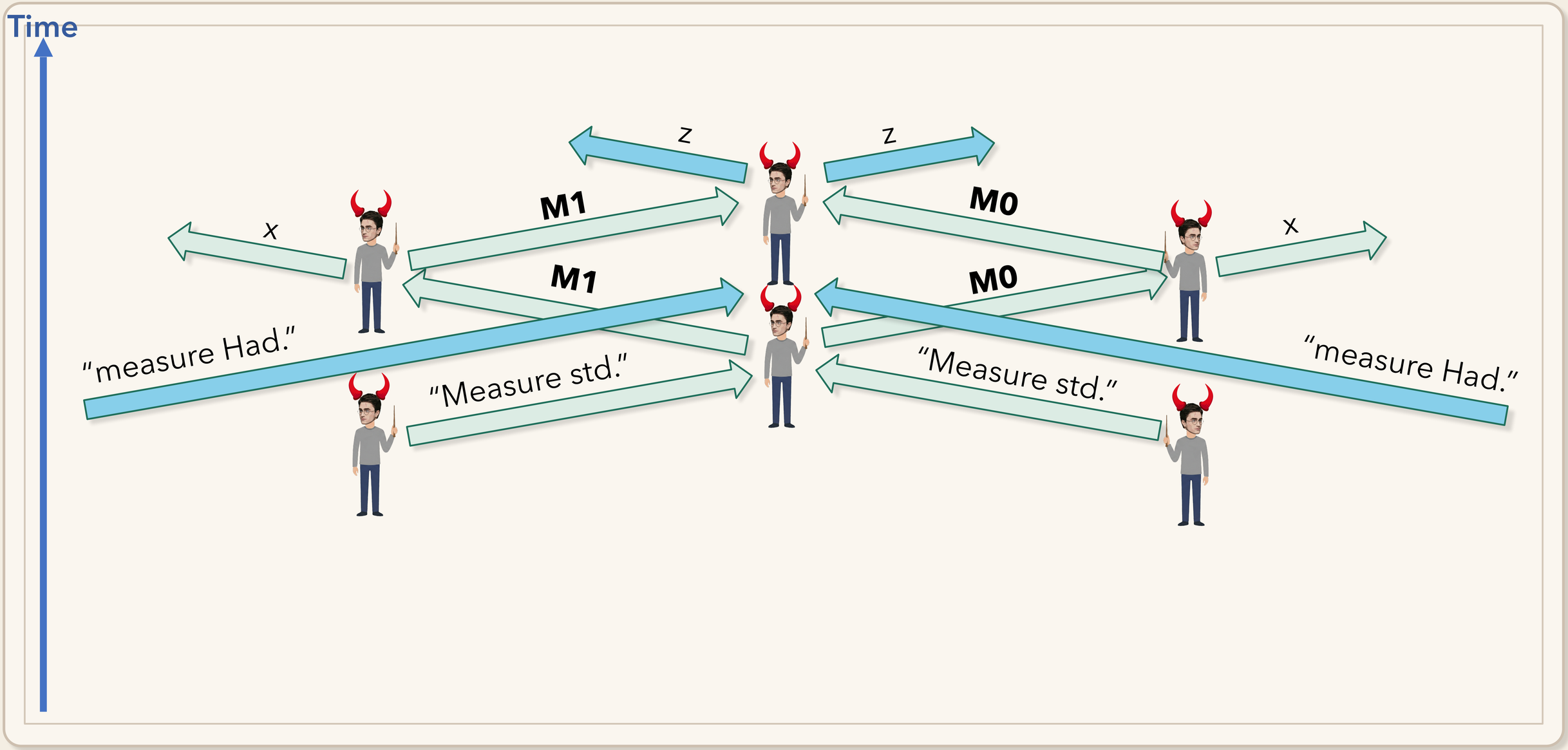
(FLASHBACK) Non-Localizability of f-BB84



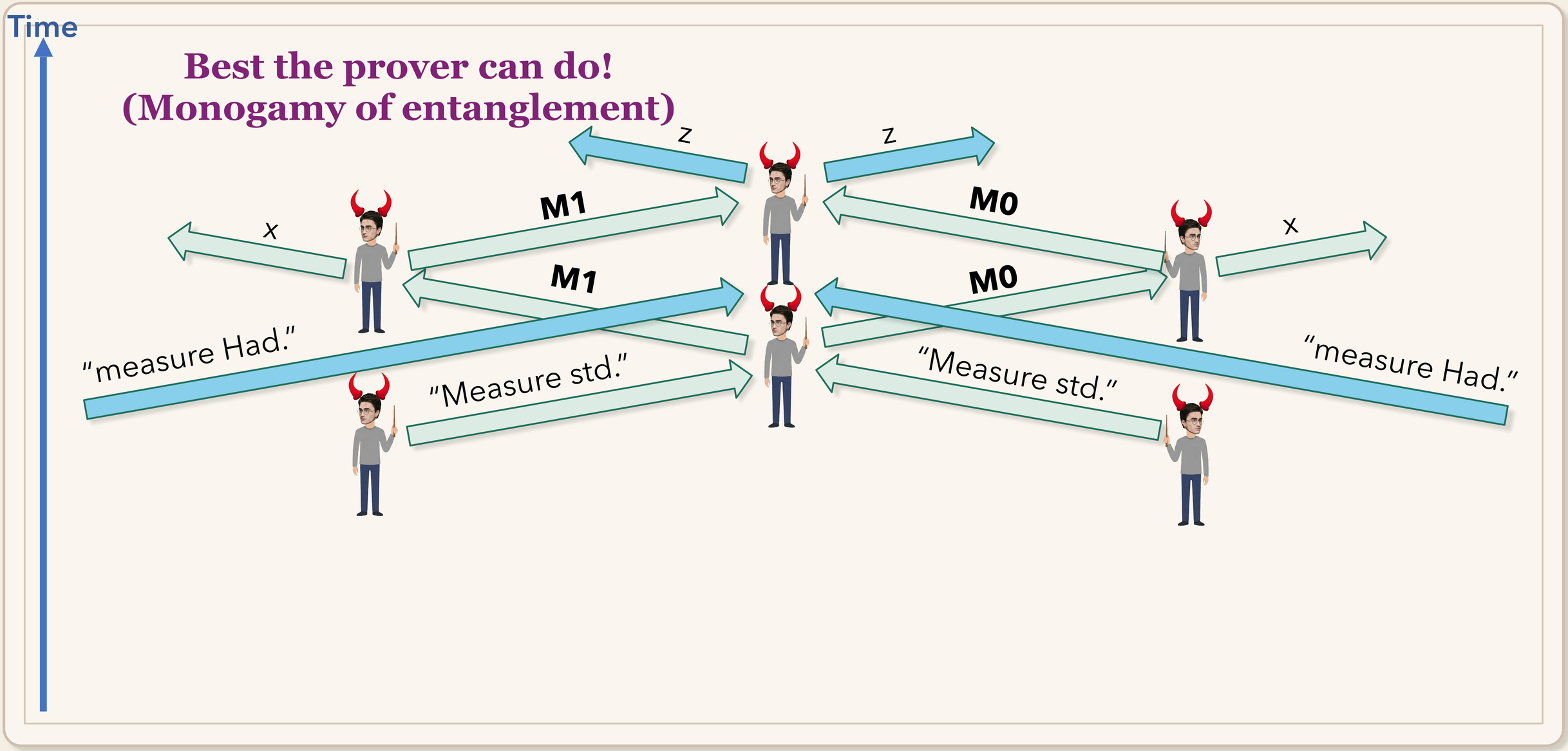
(FLASHBACK) Non-Localizability of f-BB84



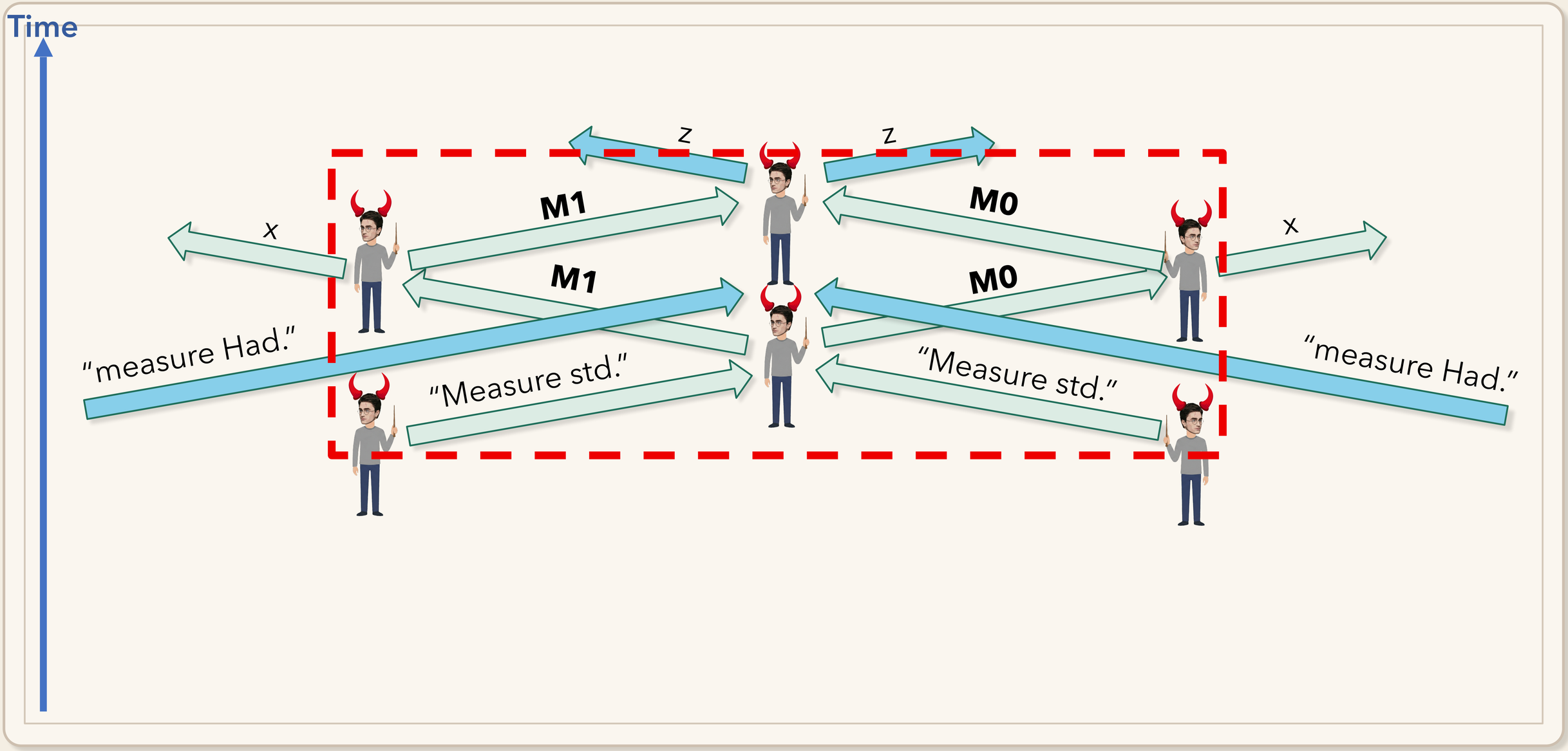
(FLASHBACK) Non-Localizability of f-BB84



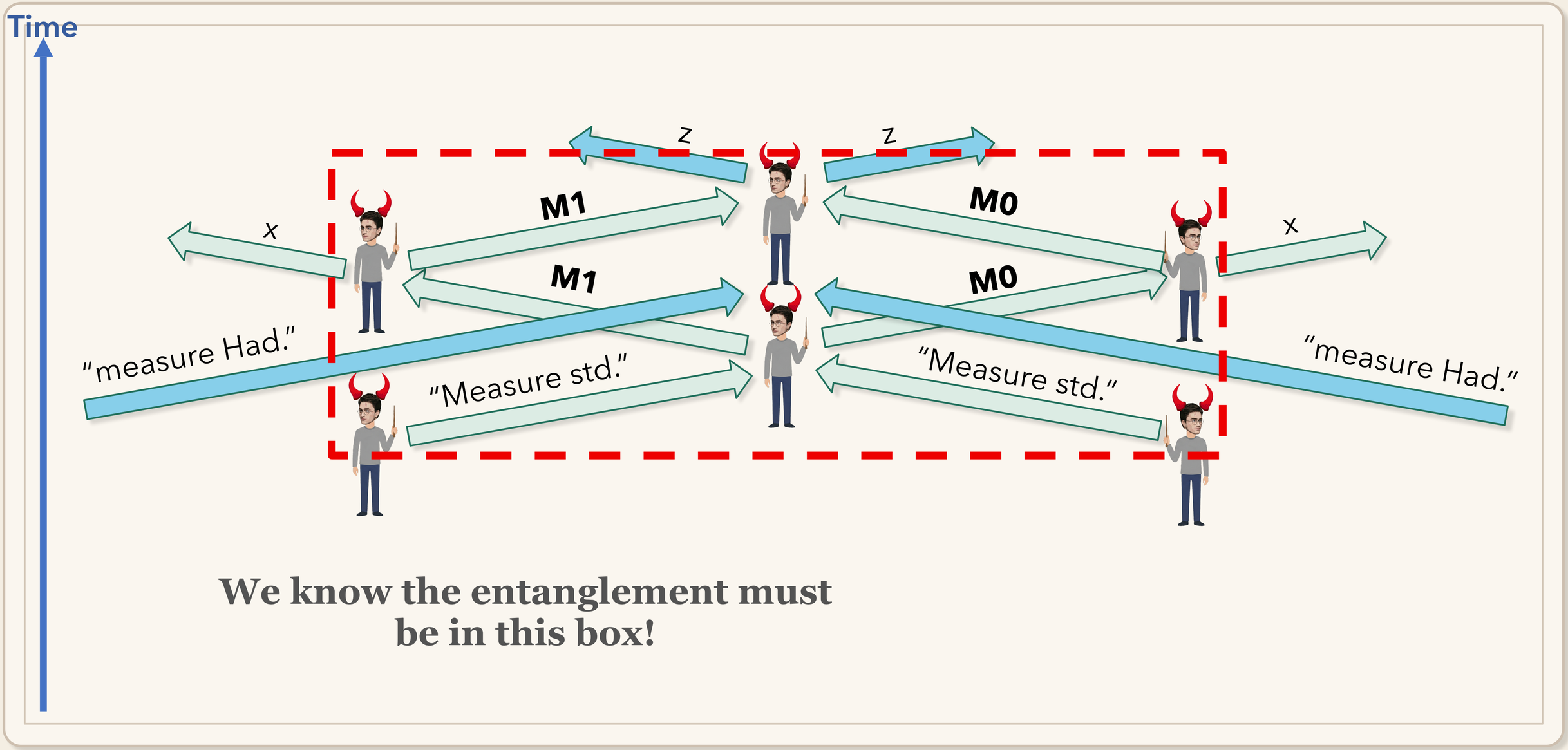
(FLASHBACK) Non-Localizability of f-BB84



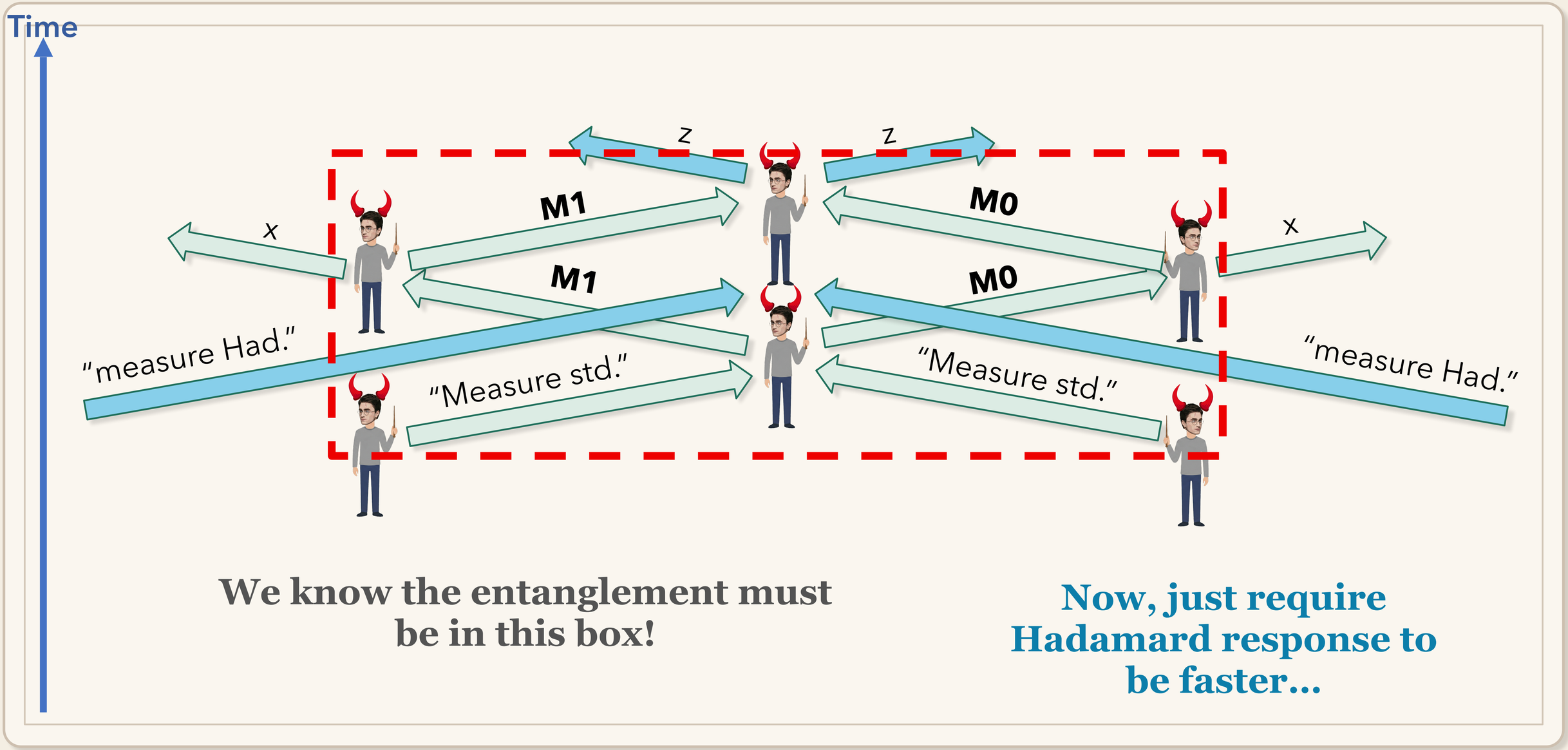
(FLASHBACK) Non-Localizability of f-BB84



(FLASHBACK) Non-Localizability of f-BB84



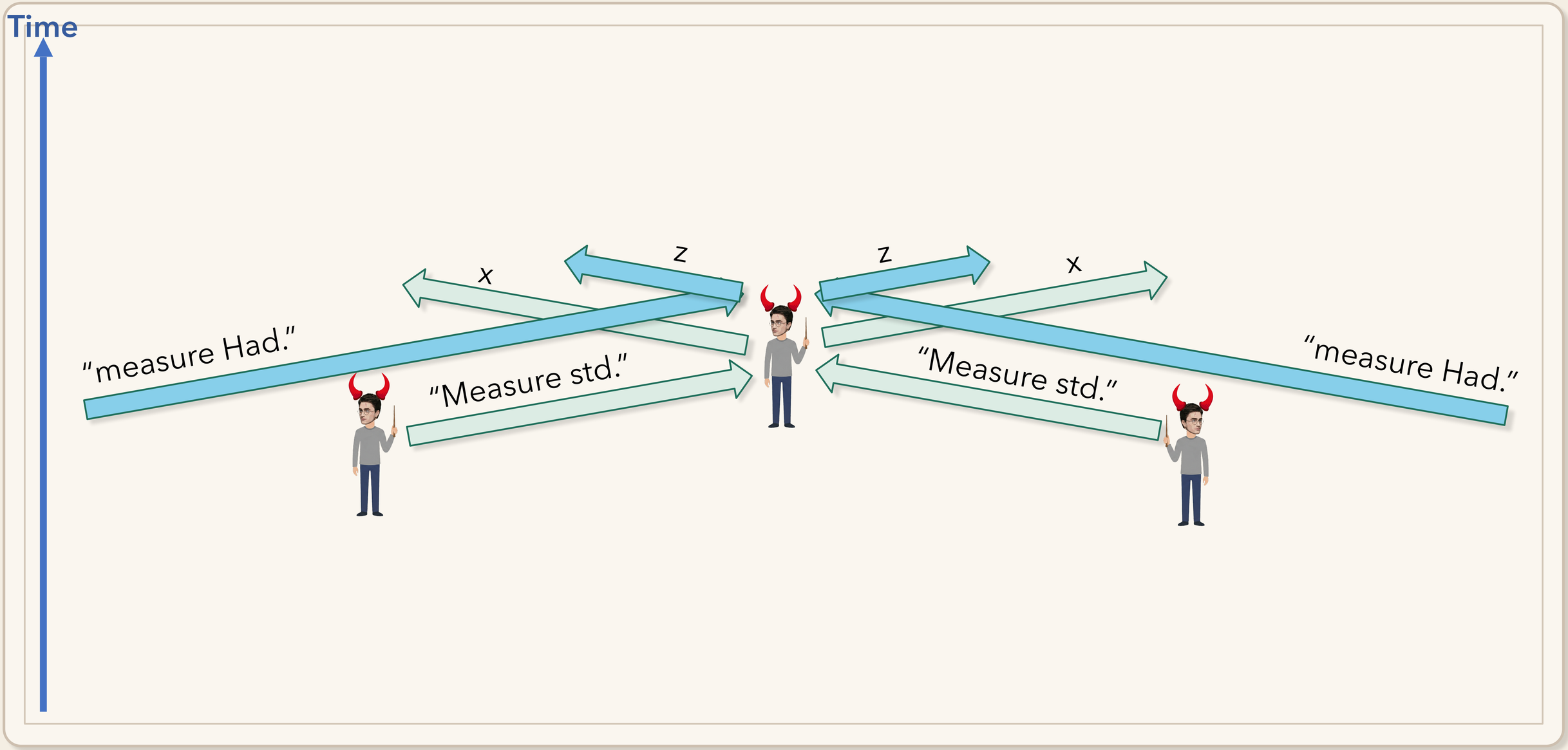
(FLASHBACK) Non-Localizability of f-BB84



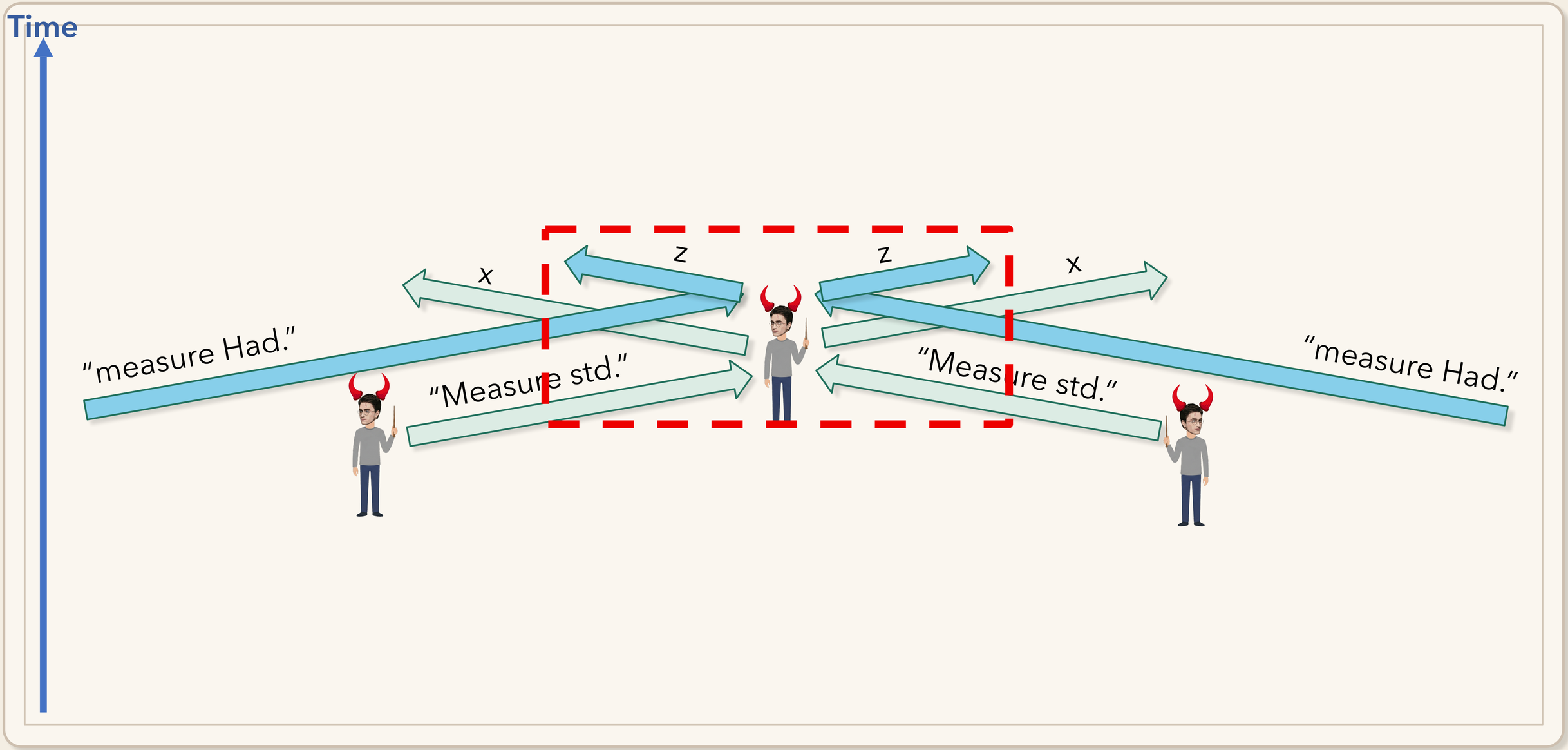
We know the entanglement must be in this box!

Now, just require Hadamard response to be faster…

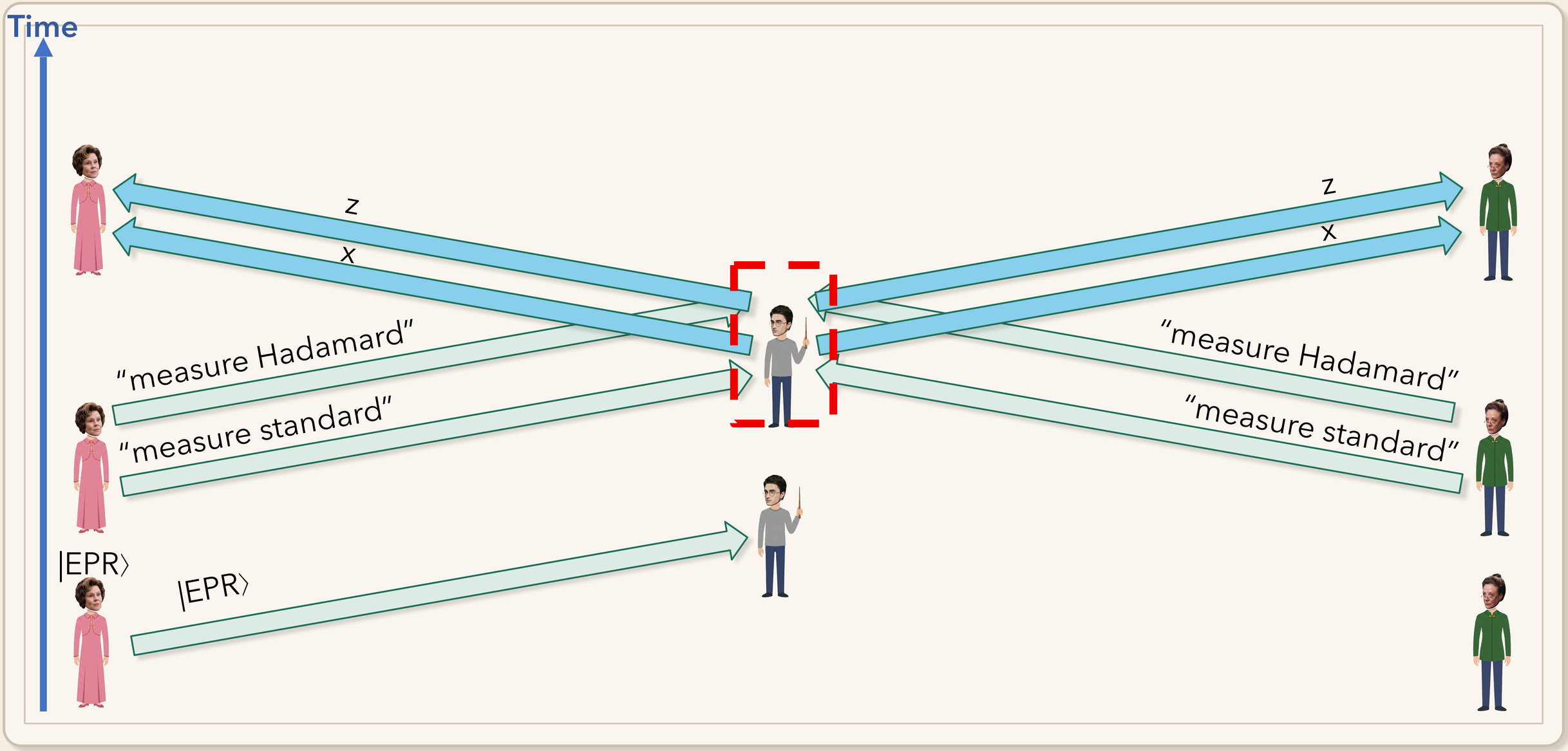
(FLASHBACK) Non-Localizability of f-BB84



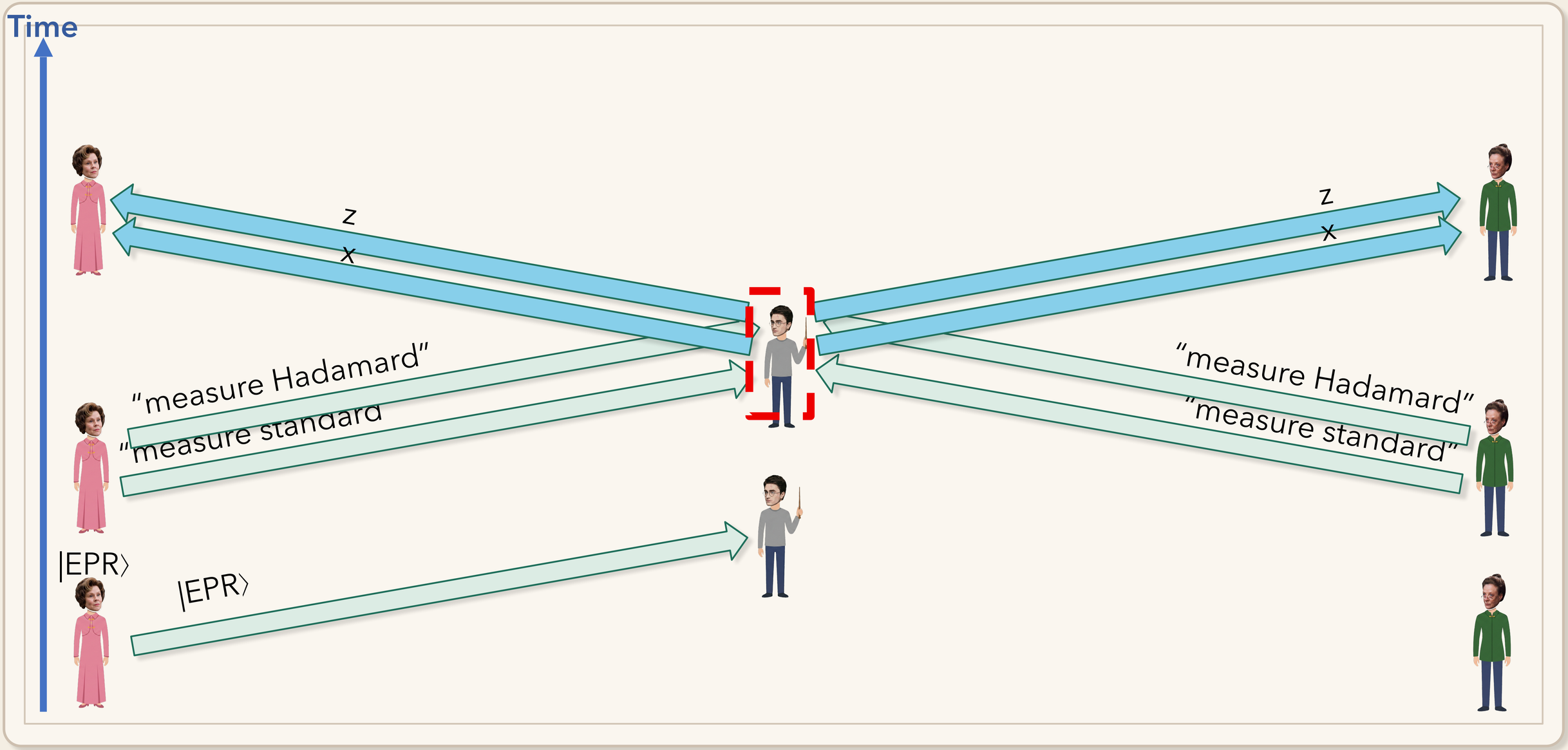
(FLASHBACK) Non-Localizability of f-BB84



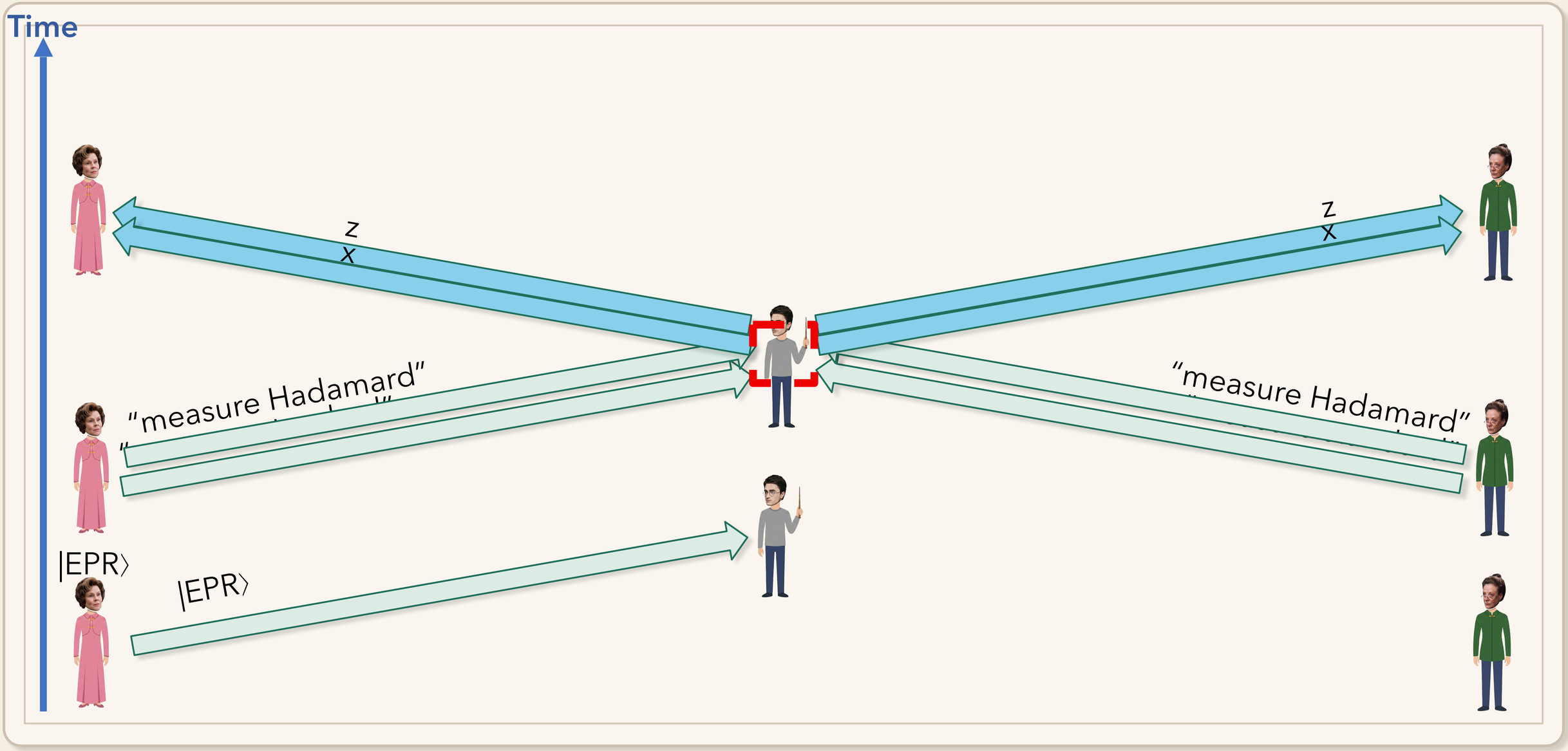
Precise Localization via Non-Destructive Tests



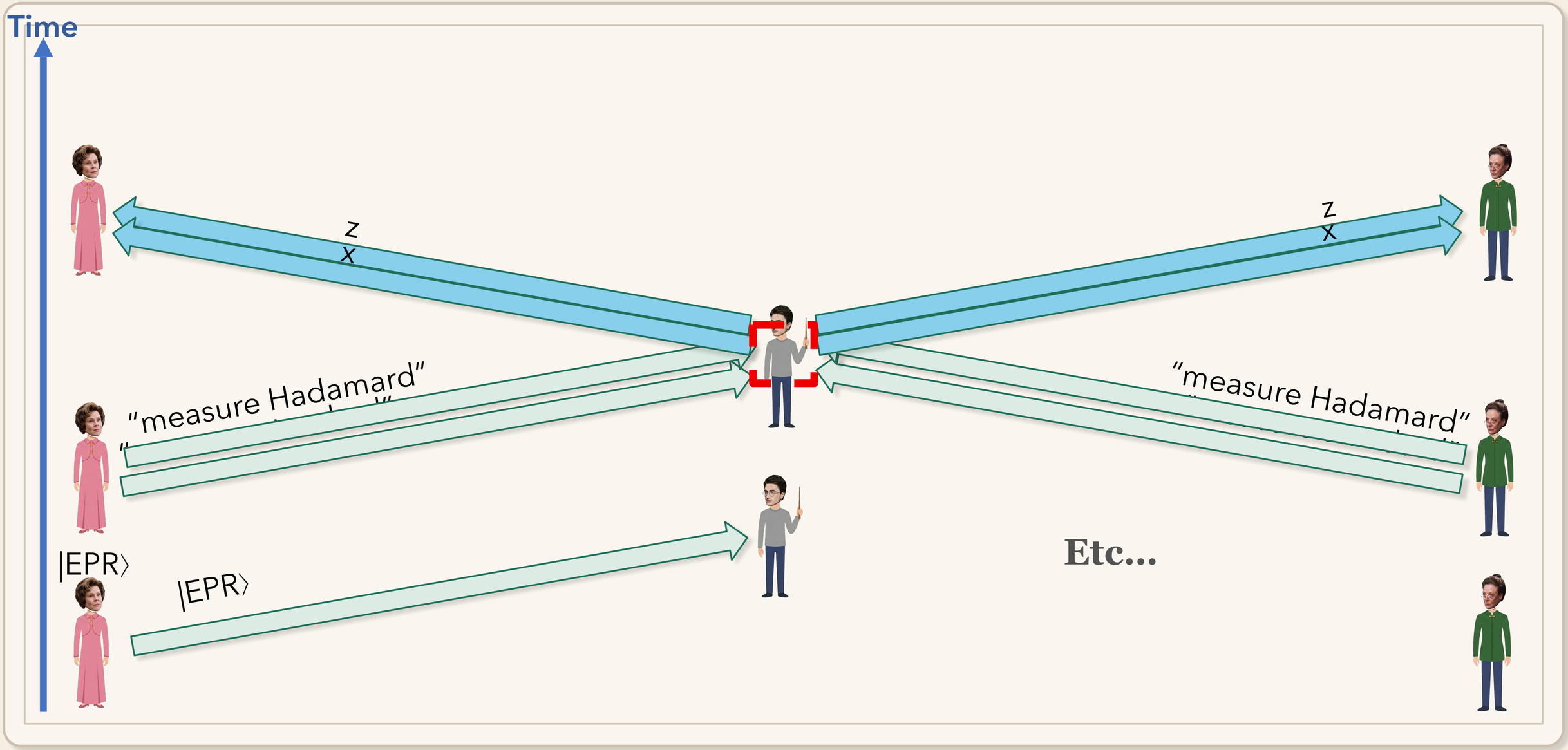
Precise Localization via Non-Destructive Tests



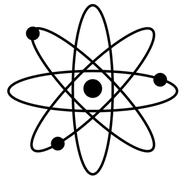
Precise Localization via Non-Destructive Tests



Precise Localization via Non-Destructive Tests



Non-Destructive Entanglement Testing

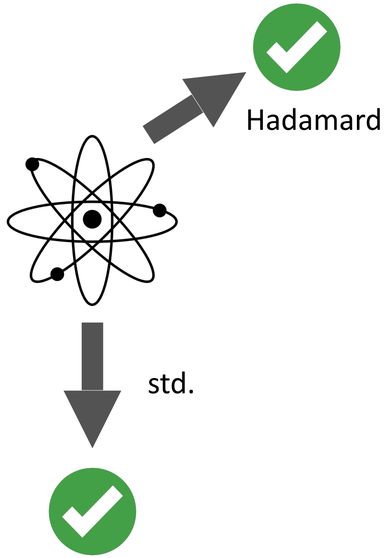


: “I got $|+\rangle$/I got $|0\rangle$”

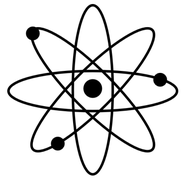
w.p. 1/2 **“Measure in the standard basis”**

OR

w.p. 1/2 **“Measure in the Hadamard basis”**



Non-Destructive Entanglement Testing

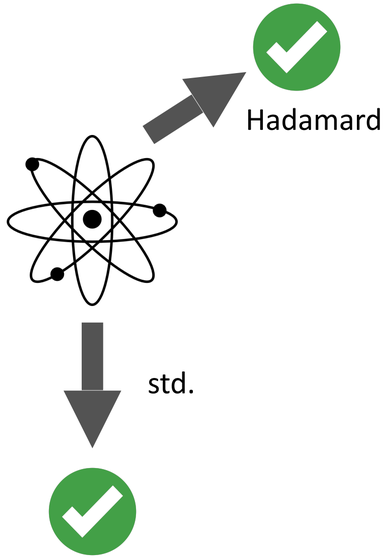


: “I got |+⟩/I got |0⟩”

w.p. 1/2 **“Measure in the standard basis”**

OR

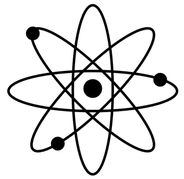
w.p. 1/2 **“Measure in the Hadamard basis”**



This is destructive! But need it be?

Non-Destructive Entanglement Testing

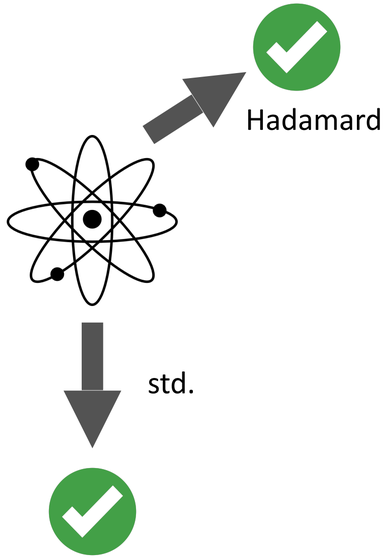
Adding Decoy Qubits


: “I got |+⟩/I got |0⟩”

w.p. 1/2 **“Measure in the standard basis”**

OR

w.p. 1/2 **“Measure in the Hadamard basis”**

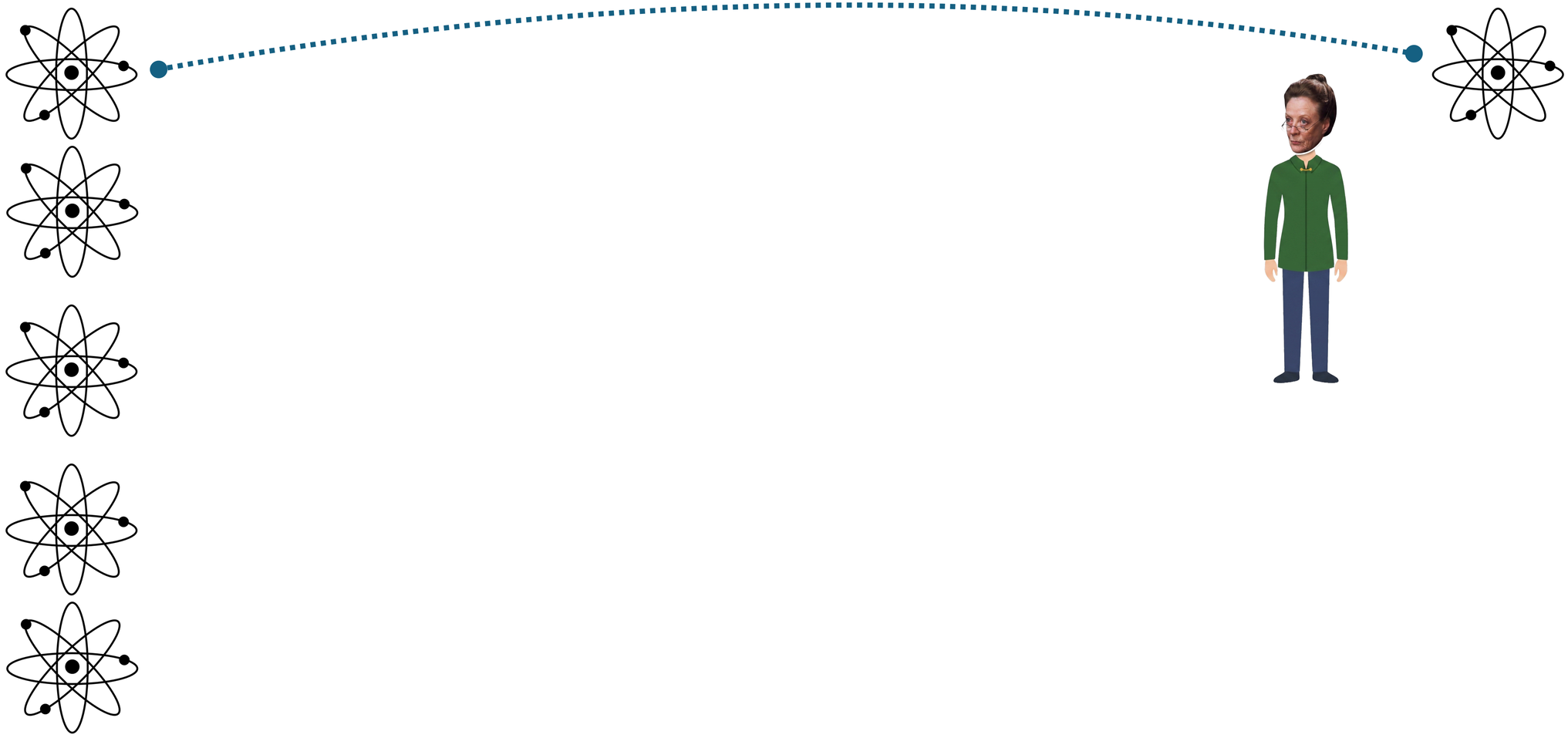


Non-Destructive Entanglement Testing

Adding Decoy Qubits

Non-Destructive Entanglement Testing

Adding Decoy Qubits

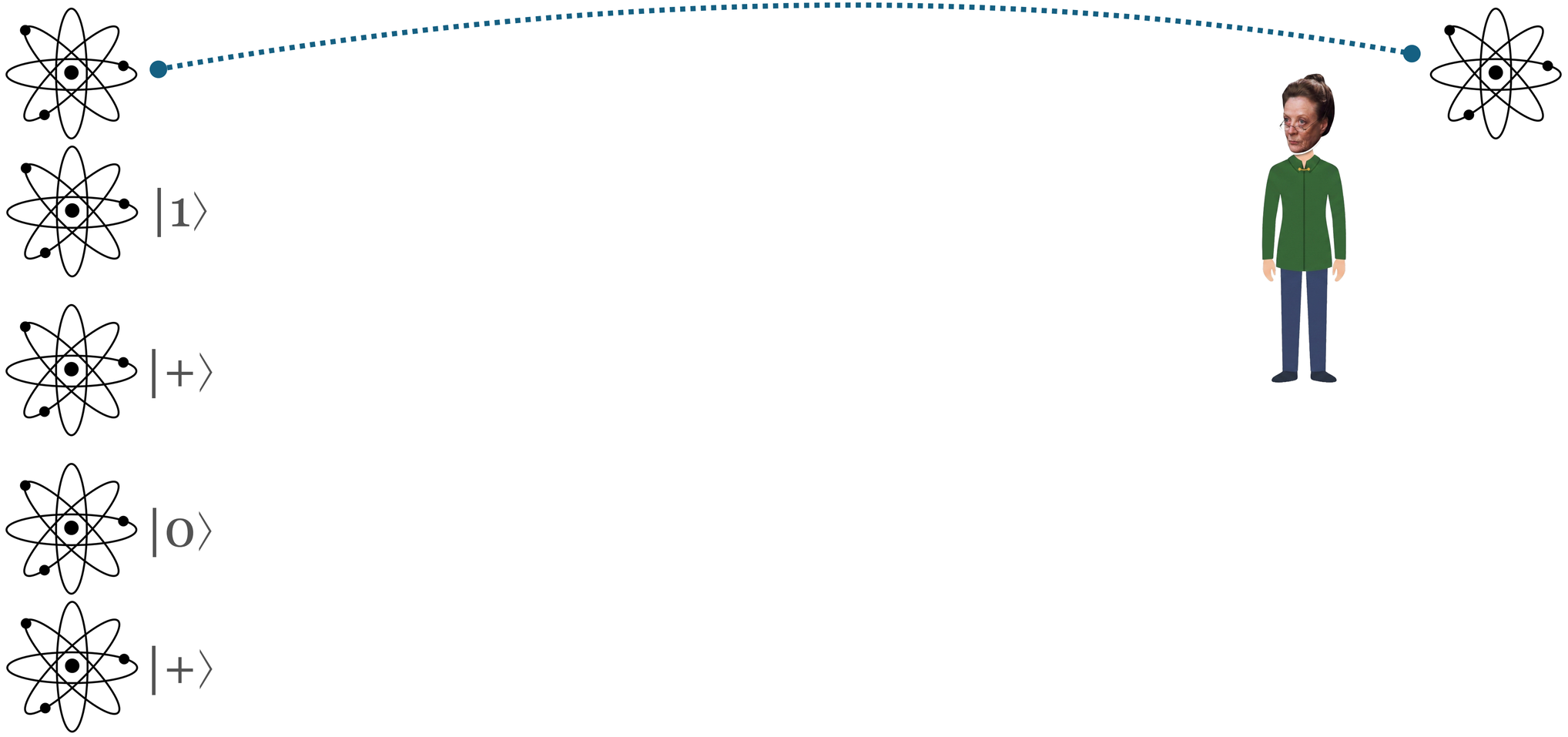


Non-Destructive Entanglement Testing

Adding Decoy Qubits

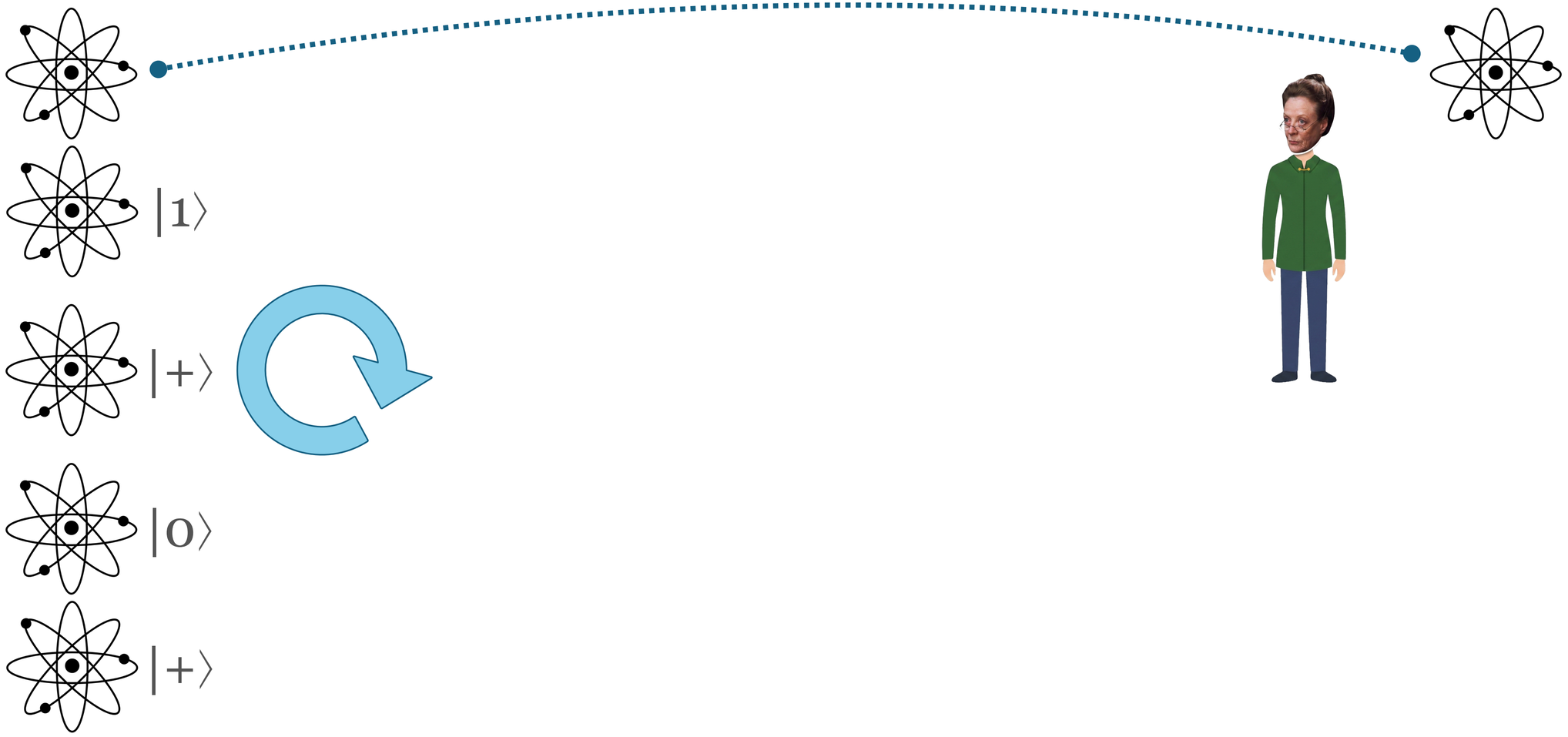
Non-Destructive Entanglement Testing

Adding Decoy Qubits



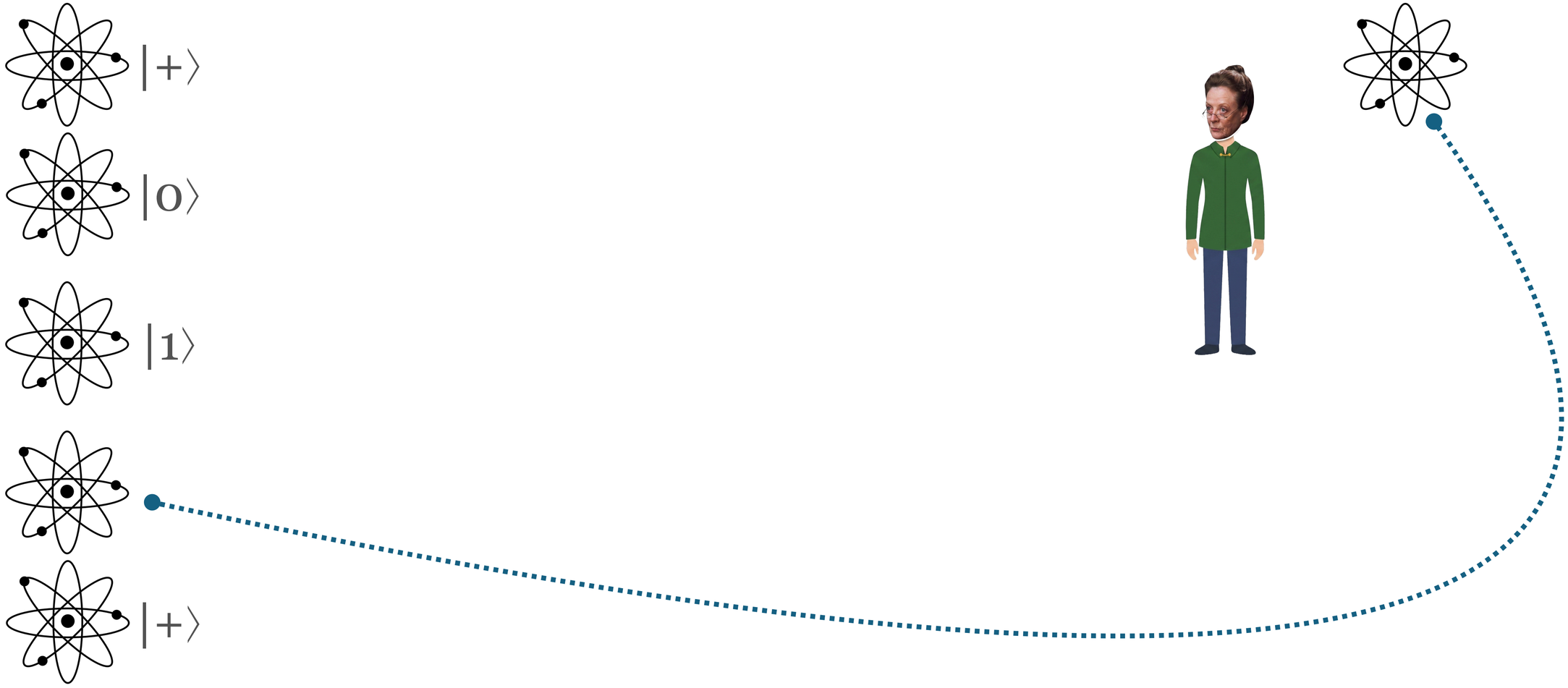
Non-Destructive Entanglement Testing

Adding Decoy Qubits



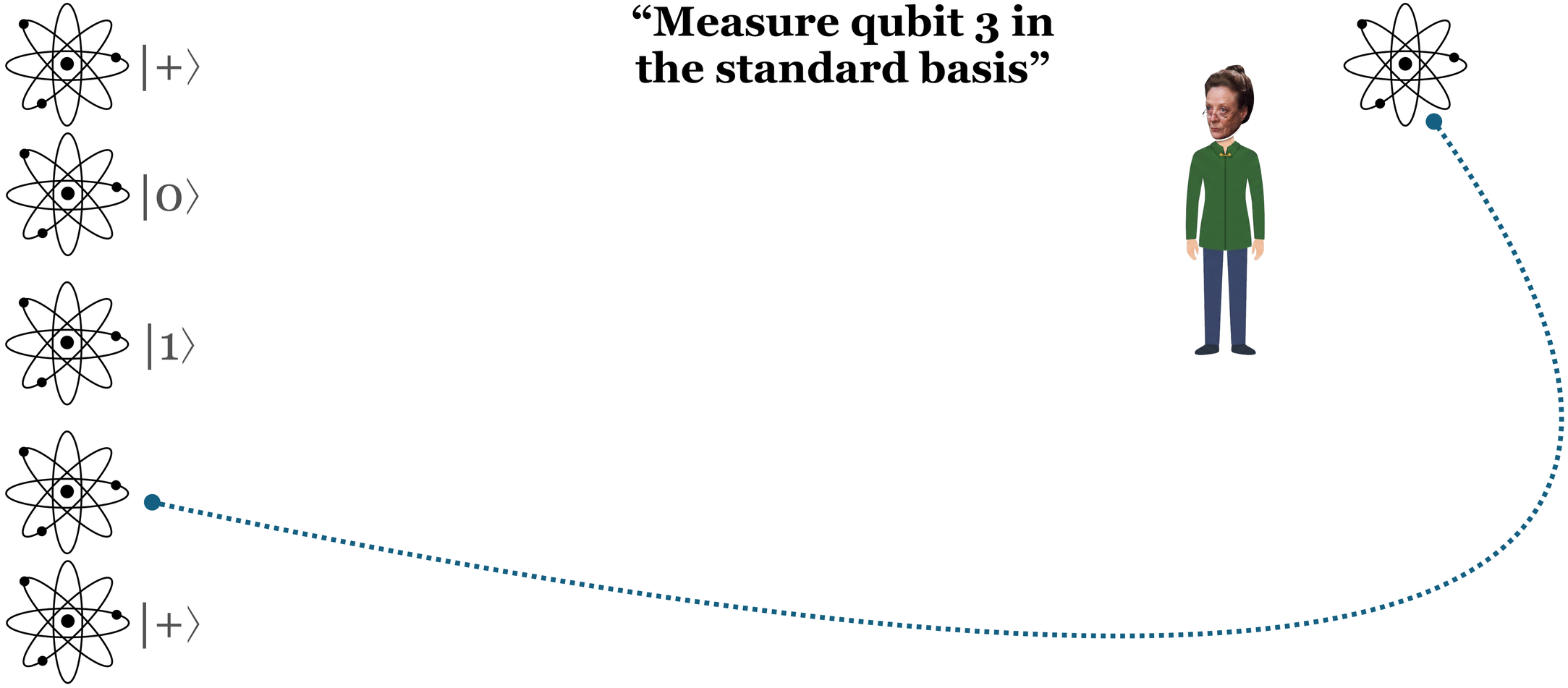
Non-Destructive Entanglement Testing

Adding Decoy Qubits



Non-Destructive Entanglement Testing

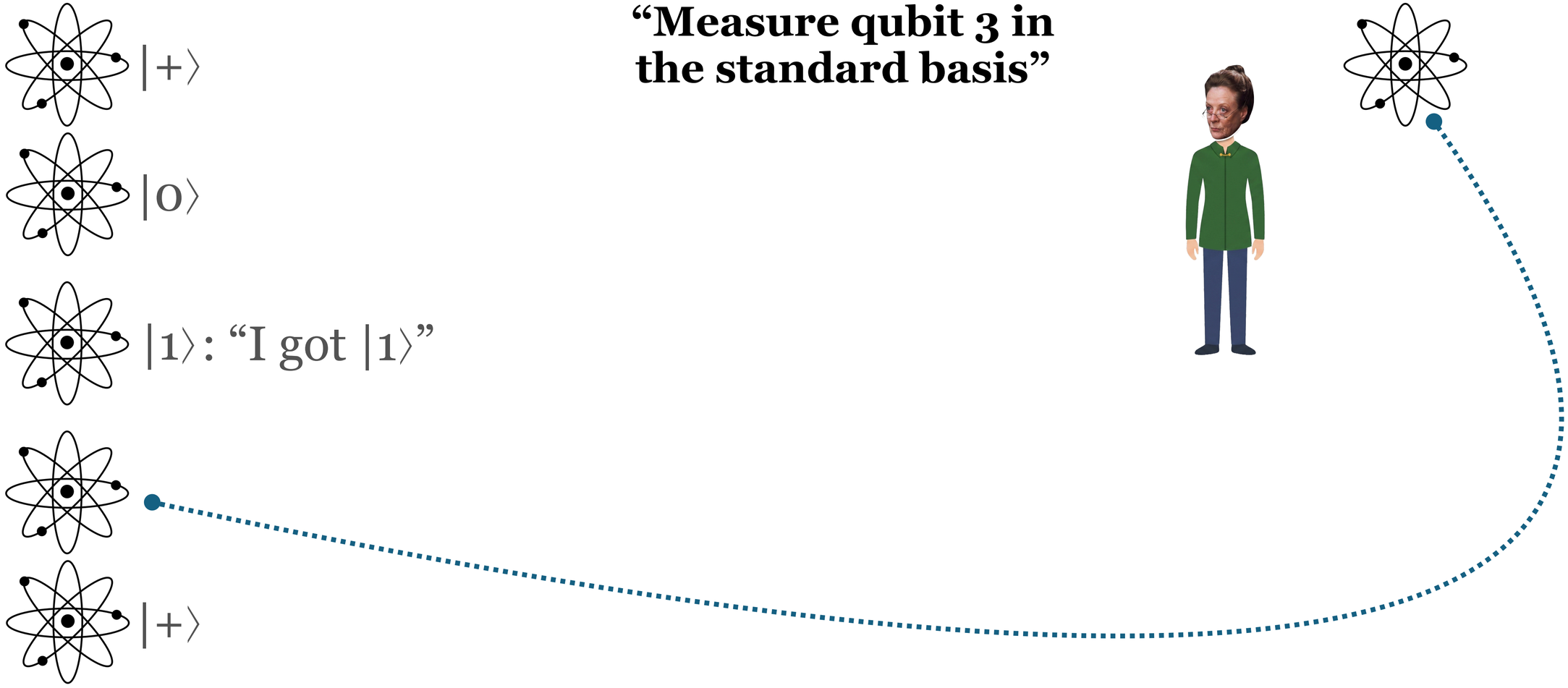
Adding Decoy Qubits



“Measure qubit 3 in the standard basis”

Non-Destructive Entanglement Testing

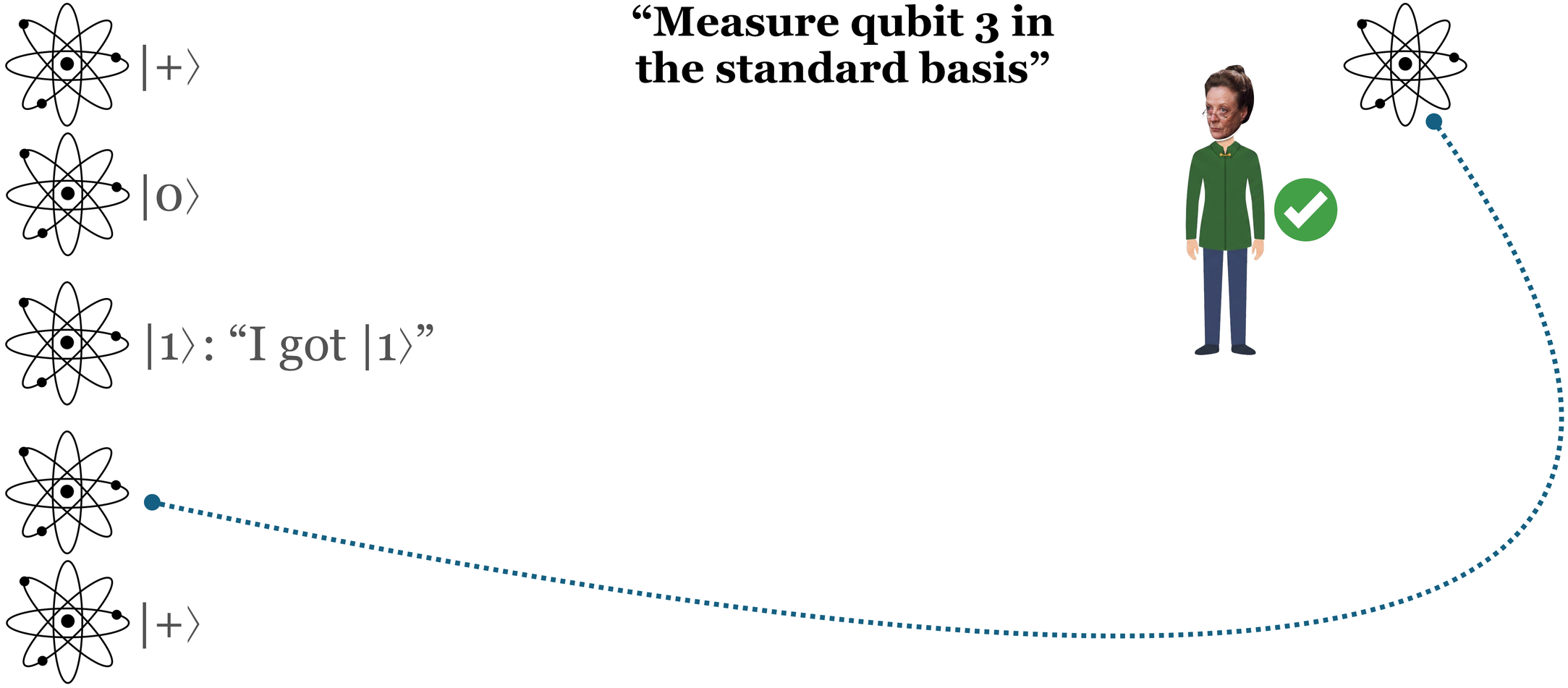
Adding Decoy Qubits



“Measure qubit 3 in the standard basis”

Non-Destructive Entanglement Testing

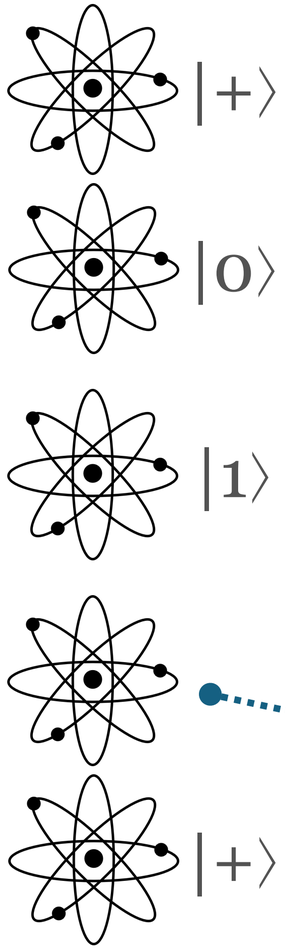
Adding Decoy Qubits



“Measure qubit 3 in the standard basis”

Non-Destructive Entanglement Testing

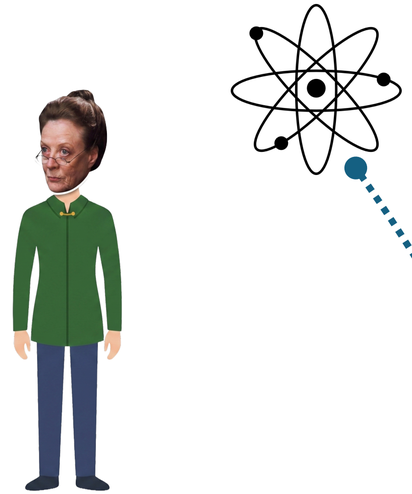
Adding Decoy Qubits



“Measure qubit 3 in the standard basis”

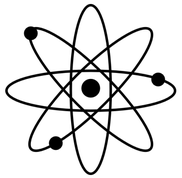
OR

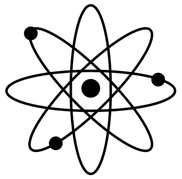
“Measure qubit 1 in the Hadamard basis”

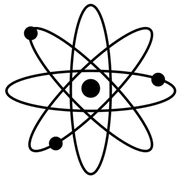


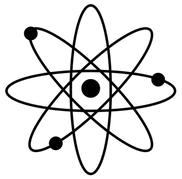
Non-Destructive Entanglement Testing

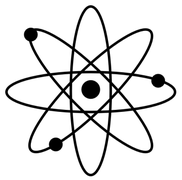
Adding Decoy Qubits


$|+\rangle$: “I got $|+\rangle$”


$|0\rangle$


$|1\rangle$

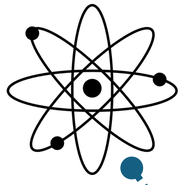



$|+\rangle$

“Measure qubit 3 in the standard basis”

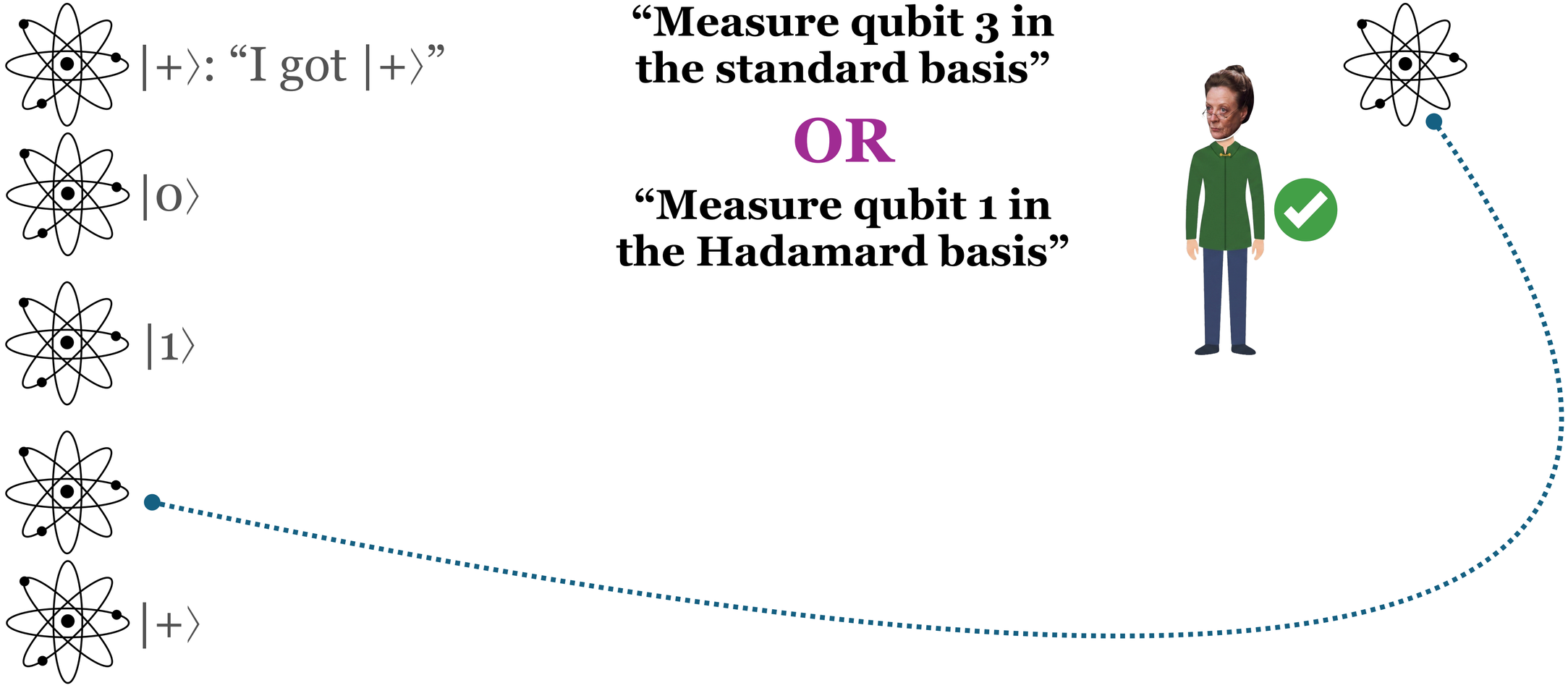
OR

“Measure qubit 1 in the Hadamard basis”



Non-Destructive Entanglement Testing

Adding Decoy Qubits



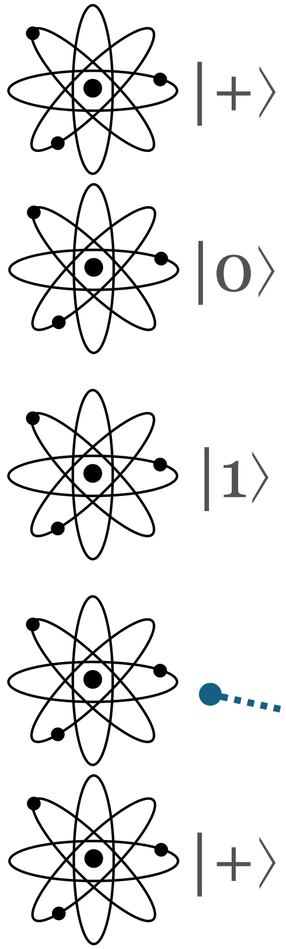
“Measure qubit 3 in the standard basis”

OR

“Measure qubit 1 in the Hadamard basis”

Non-Destructive Entanglement Testing

Adding Decoy Qubits



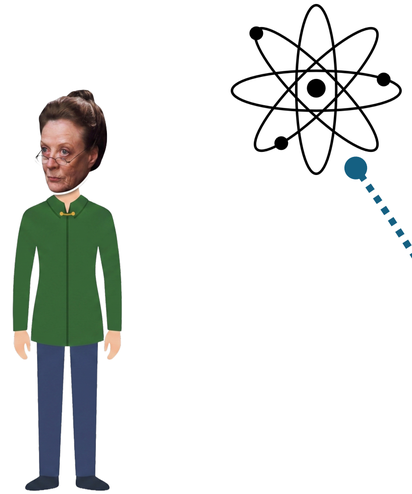
“Measure qubit 3 in the standard basis”

OR

“Measure qubit 1 in the Hadamard basis”

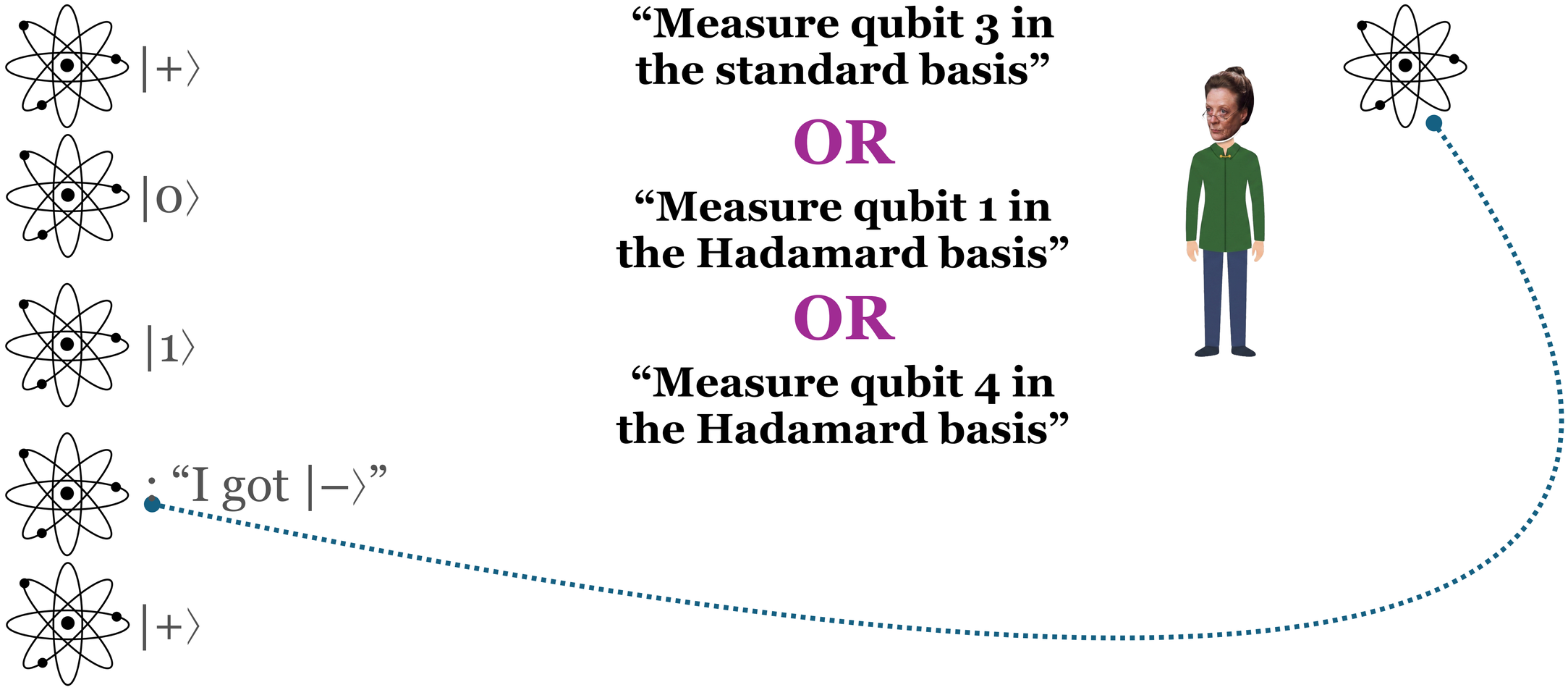
OR

“Measure qubit 4 in the Hadamard basis”



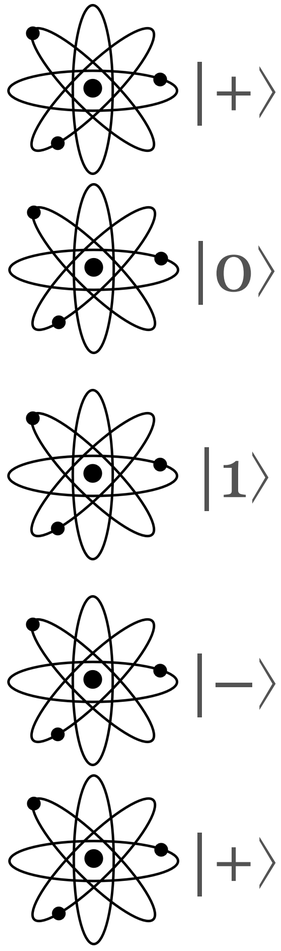
Non-Destructive Entanglement Testing

Adding Decoy Qubits



Non-Destructive Entanglement Testing

Adding Decoy Qubits



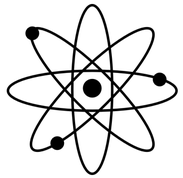
“Measure qubit 3 in the standard basis”

OR

“Measure qubit 1 in the Hadamard basis”

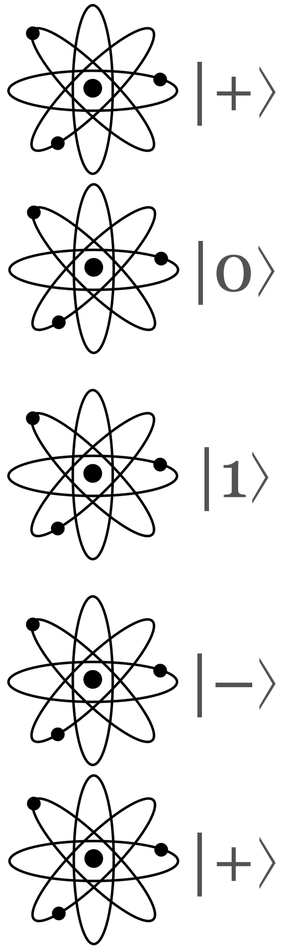
OR

“Measure qubit 4 in the Hadamard basis”



Non-Destructive Entanglement Testing

Adding Decoy Qubits



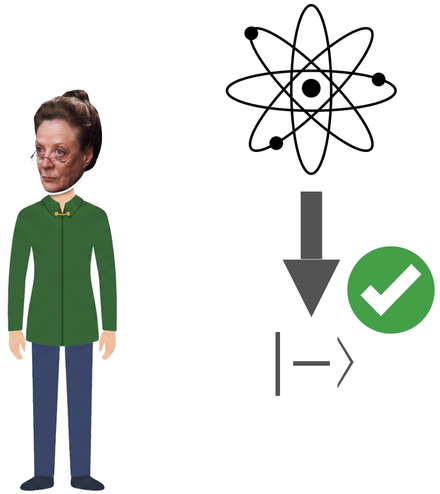
“Measure qubit 3 in the standard basis”

OR

“Measure qubit 1 in the Hadamard basis”

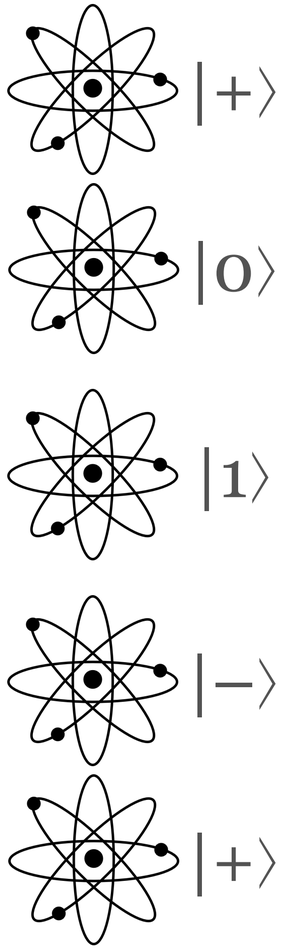
OR

“Measure qubit 4 in the Hadamard basis”



Non-Destructive Entanglement Testing

Adding Decoy Qubits



Non-destructive

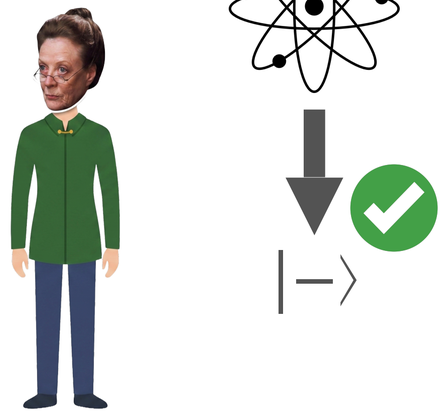
“Measure qubit 3 in the standard basis”

OR

“Measure qubit 1 in the Hadamard basis”

OR

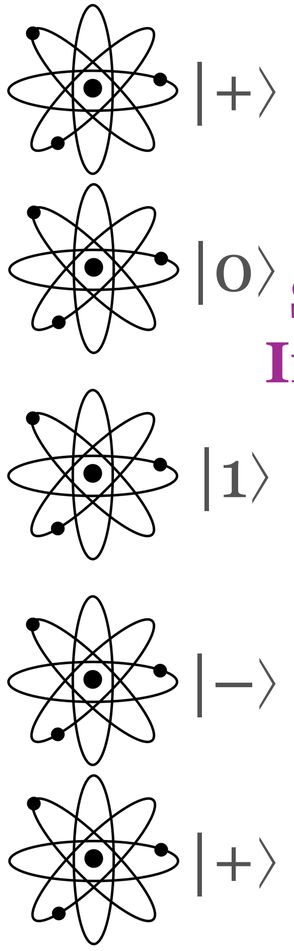
“Measure qubit 4 in the Hadamard basis”



Destructive!

Non-Destructive Entanglement Testing

Adding Decoy Qubits



Statistically Indistinguishable

“Measure qubit 3 in the standard basis”

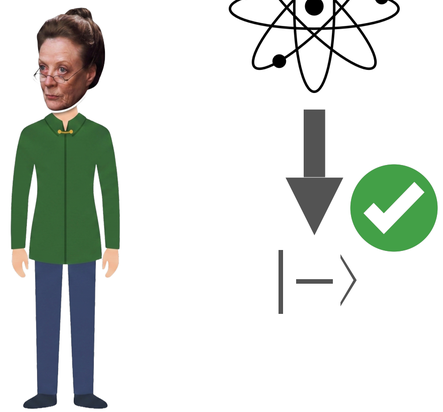
OR

“Measure qubit 1 in the Hadamard basis”

OR

“Measure qubit 4 in the Hadamard basis”

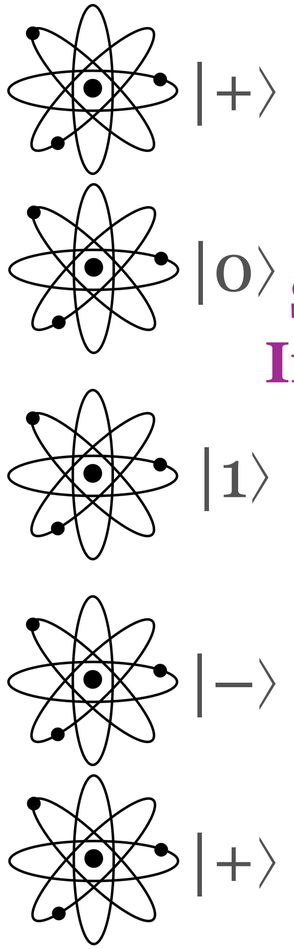
Non-destructive



Destructive!

Non-Destructive Entanglement Testing

Adding Decoy Qubits



Statistically Indistinguishable

"Measure qubit 3 in the standard basis"

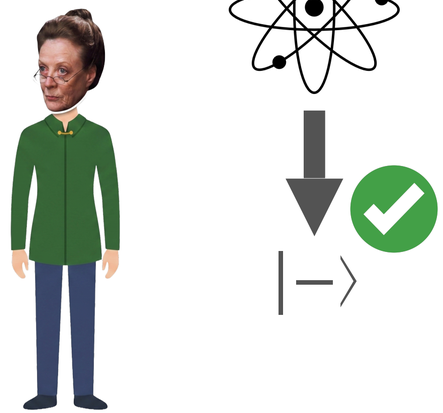
OR

"Measure qubit 1 in the Hadamard basis"

OR

"Measure qubit 4 in the Hadamard basis"

Non-destructive

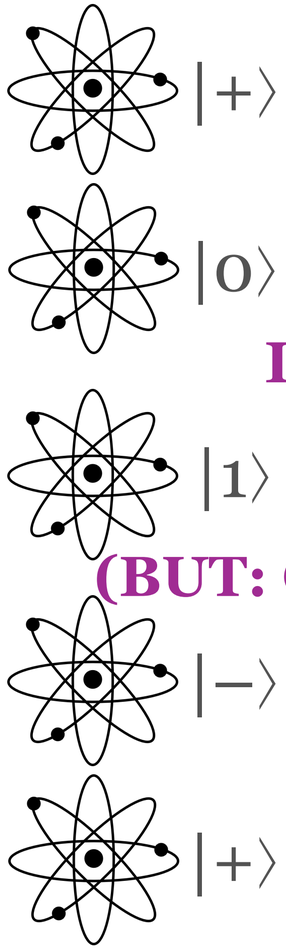


Destructive!

Moral: Real experiment performs *non-destructive* test, then analysis argues that it *could* have been the destructive test, thus certifying entanglement

Non-Destructive Entanglement Testing

Adding Decoy Qubits



Statistically Indistinguishable

(BUT: Only single-use)

Non-destructive

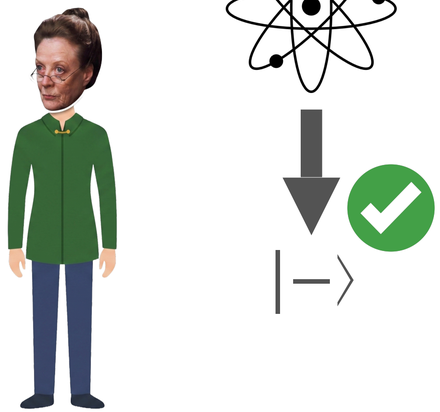
"Measure qubit 3 in the standard basis"

OR

"Measure qubit 1 in the Hadamard basis"

OR

"Measure qubit 4 in the Hadamard basis"

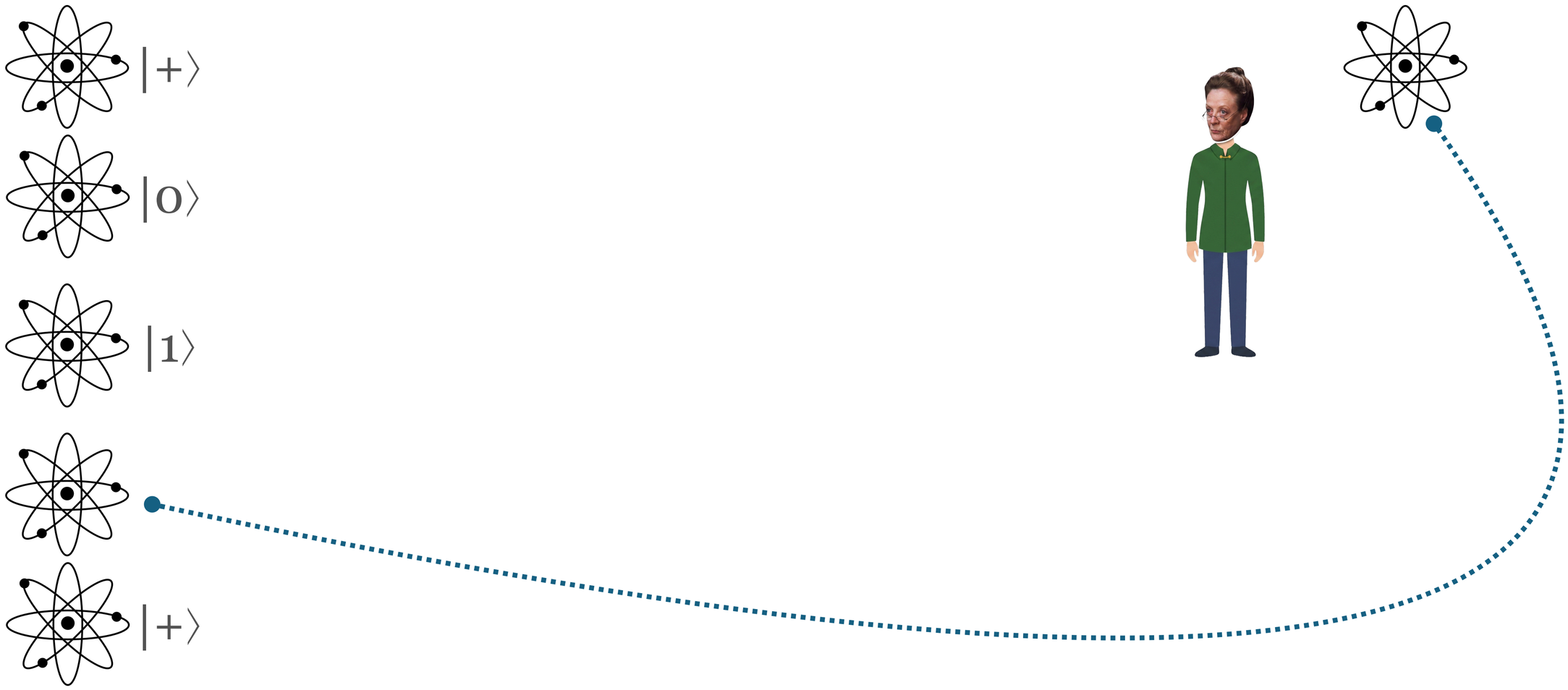


Destructive!

Moral: Real experiment performs *non-destructive* test, then analysis argues that it *could* have been the destructive test, thus certifying entanglement

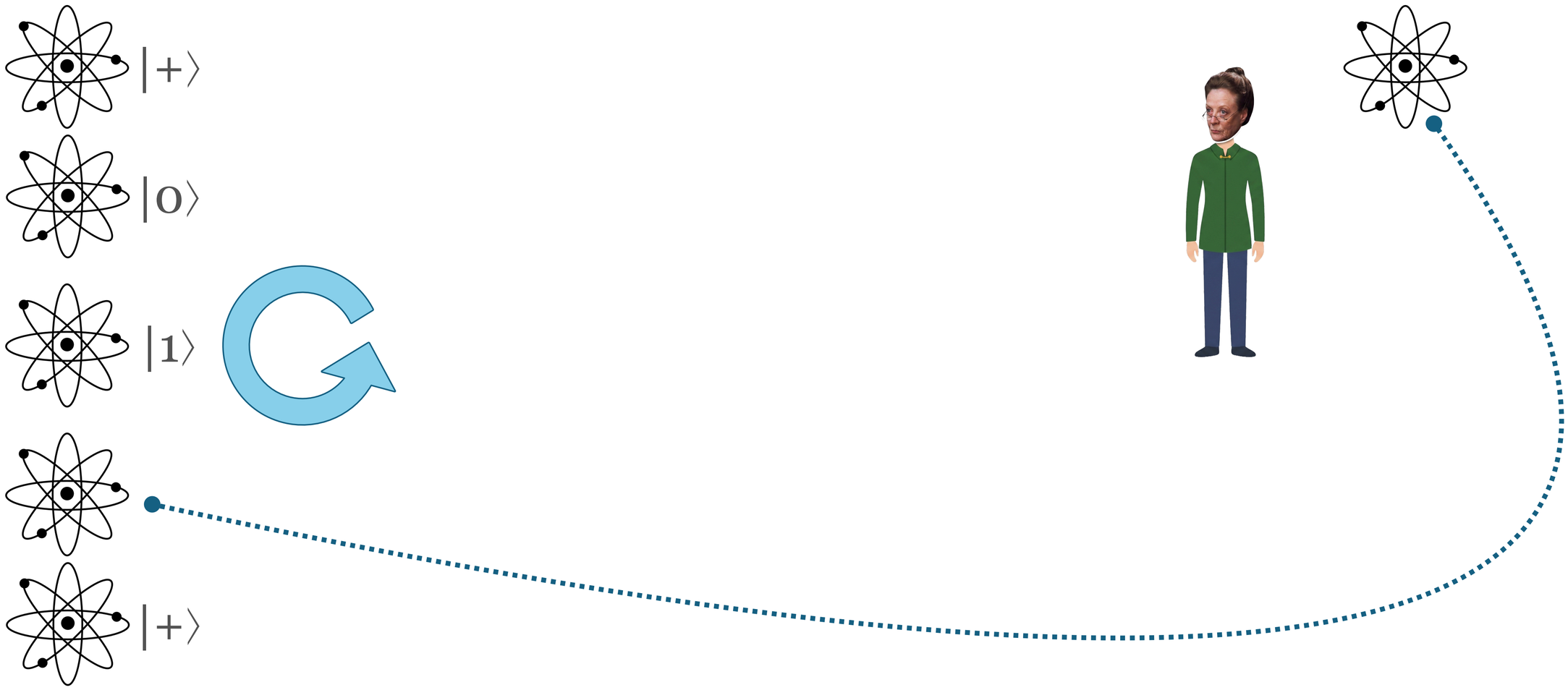
Non-Destructive Entanglement Testing

Hiding Entanglement



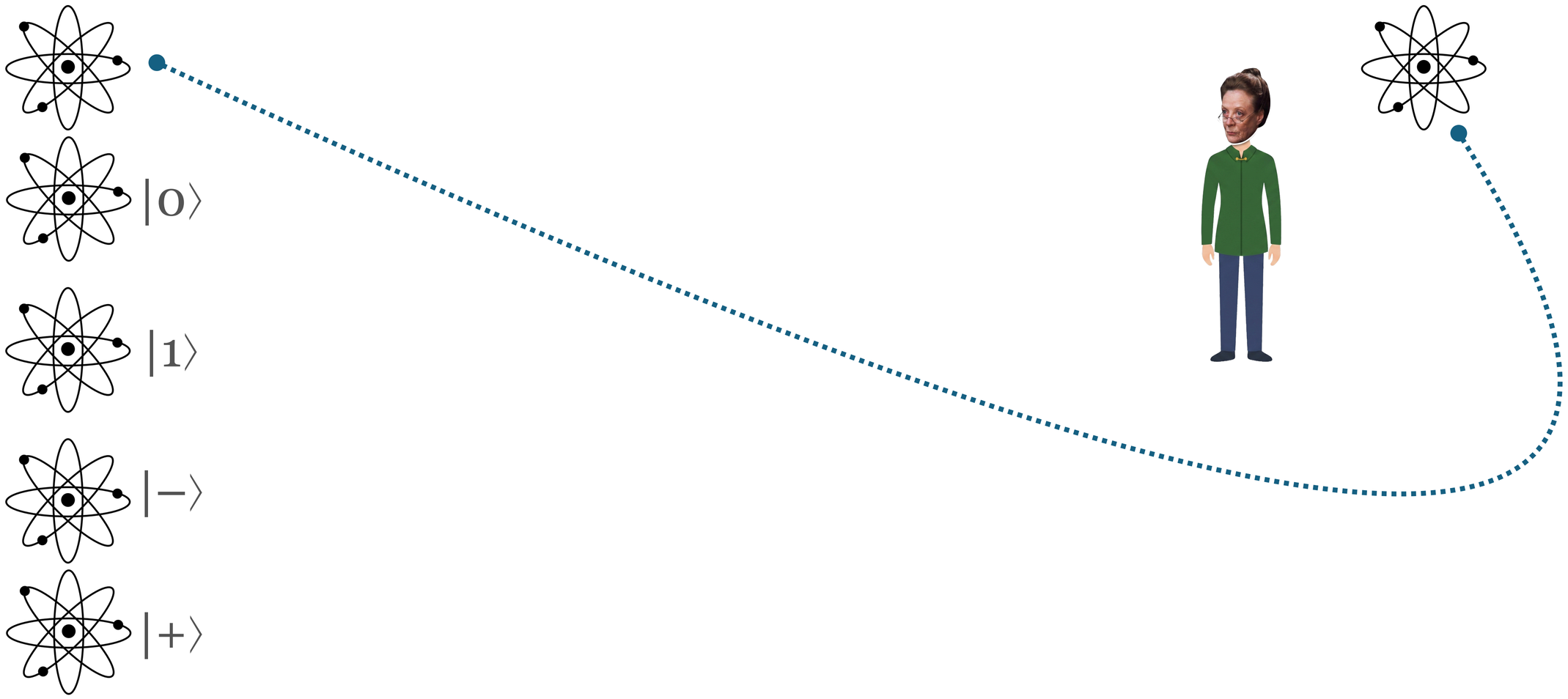
Non-Destructive Entanglement Testing

Hiding Entanglement

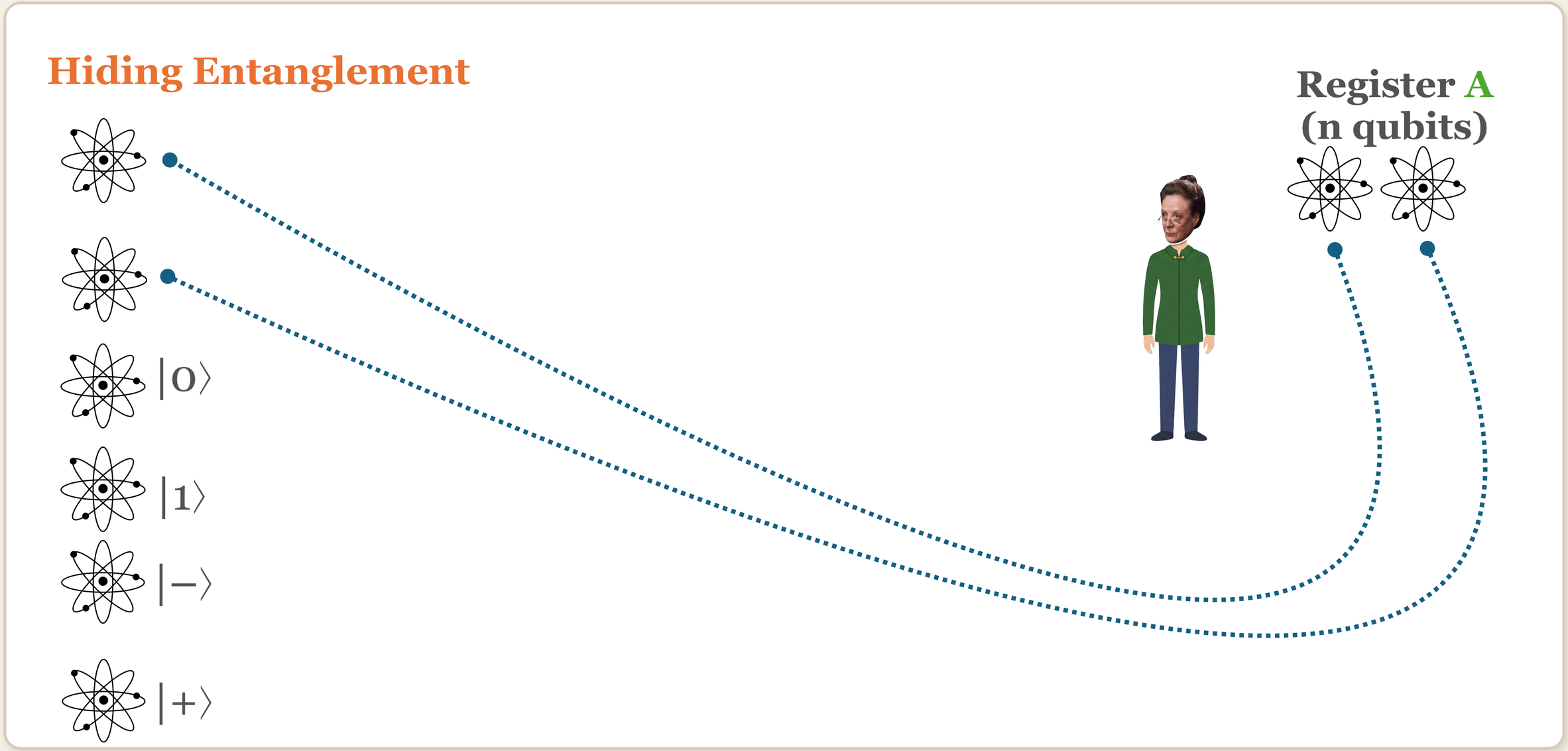


Non-Destructive Entanglement Testing

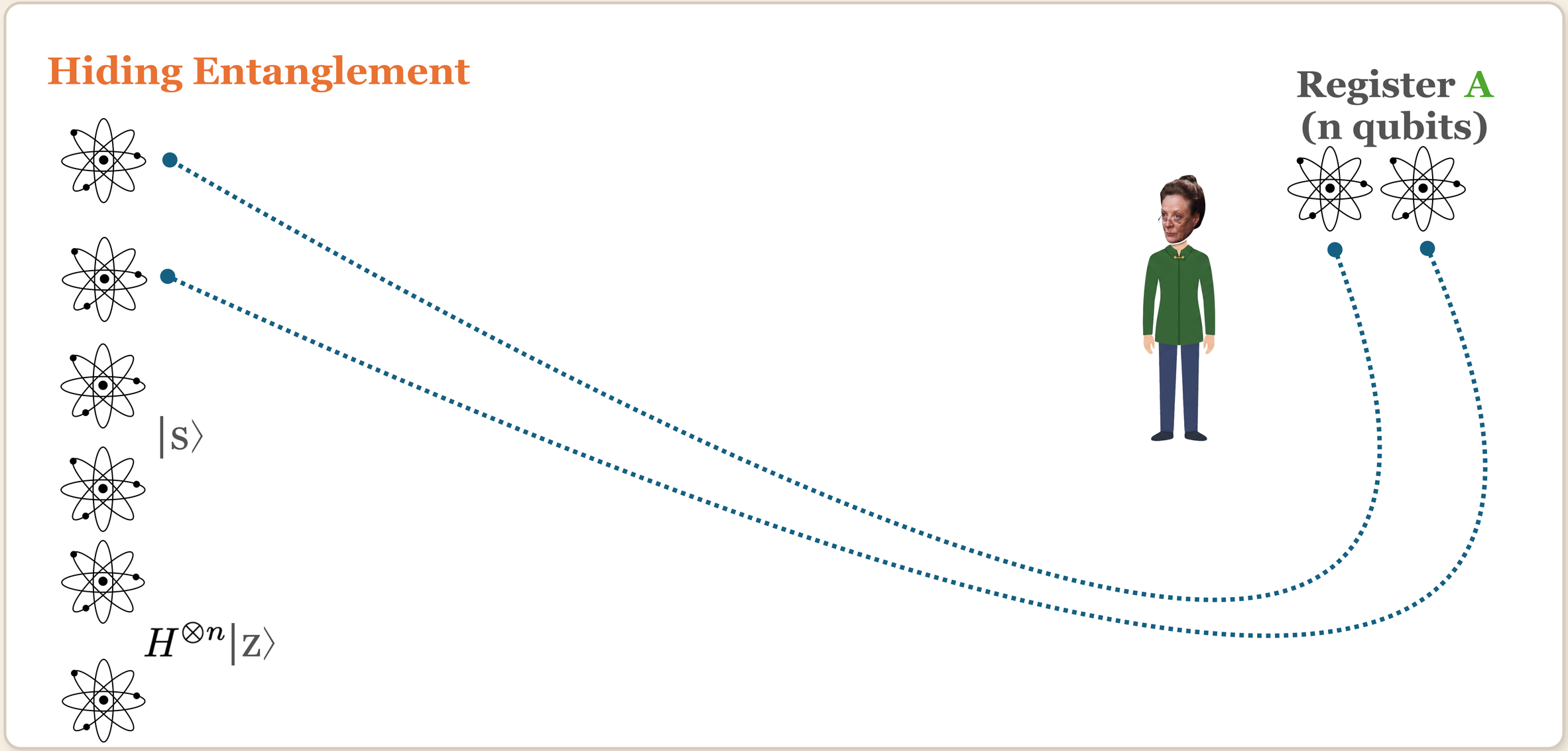
Hiding Entanglement



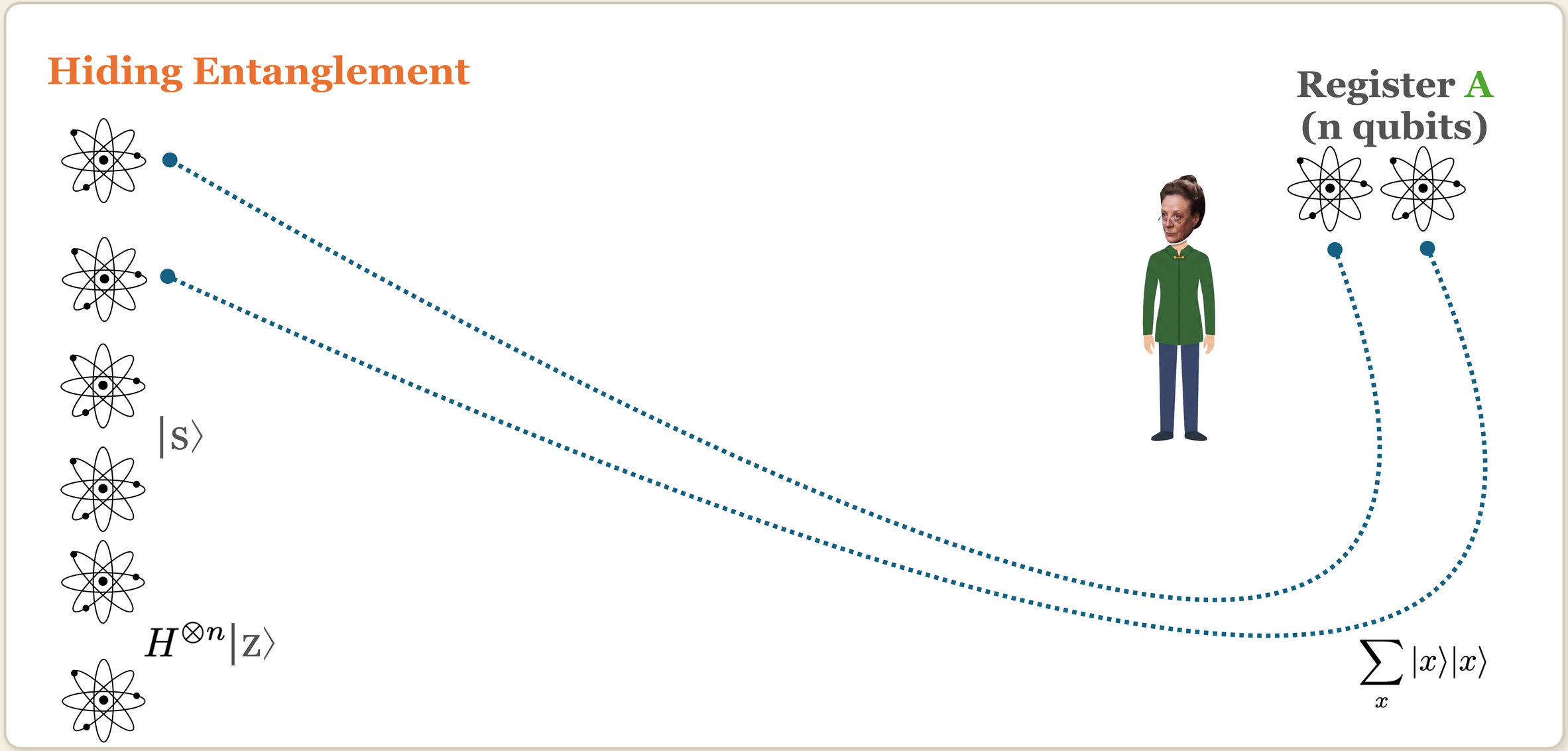
Non-Destructive Entanglement Testing



Non-Destructive Entanglement Testing

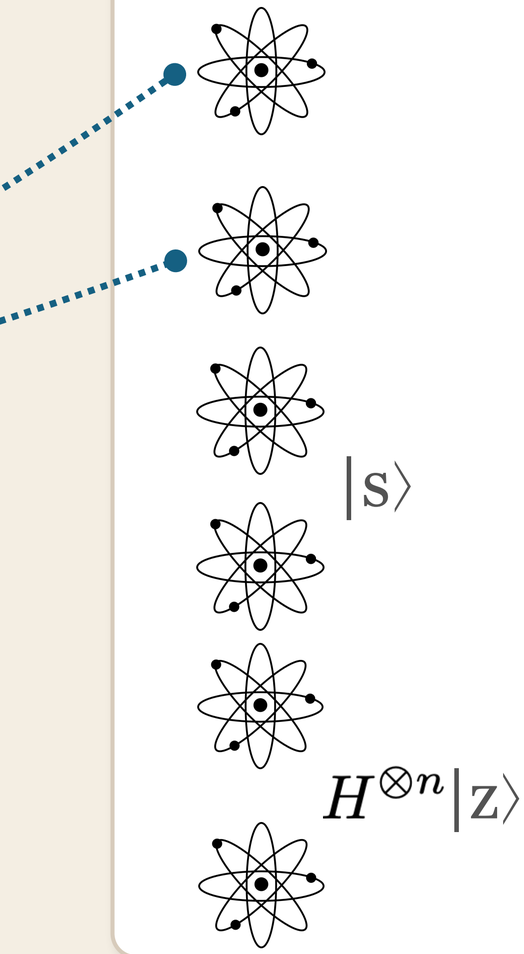


Non-Destructive Entanglement Testing

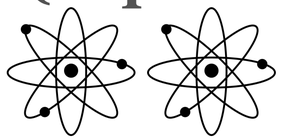


Non-Destructive Entanglement Testing

Hiding Entanglement



Register **A** (n qubits)

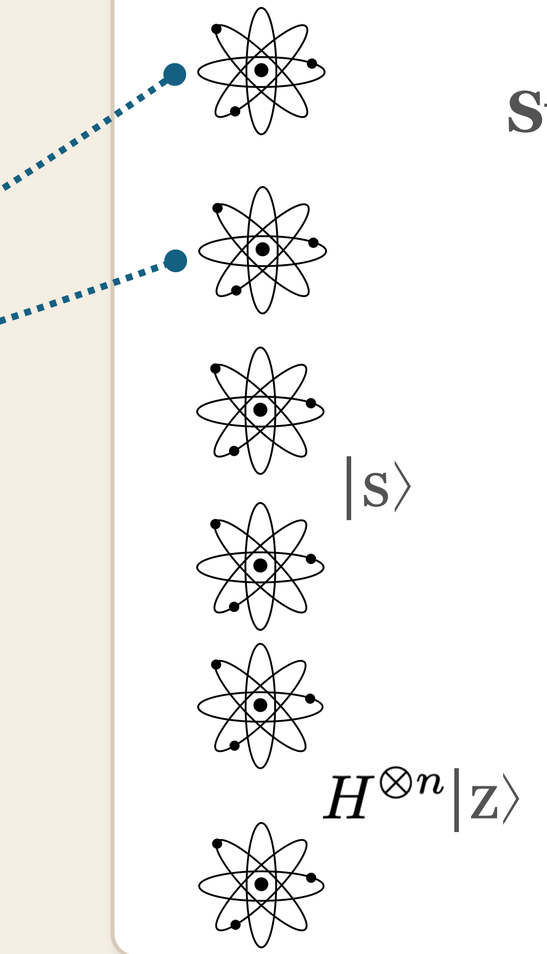


$$\sum_x |x\rangle|x\rangle$$

Register **B** (3n qubits)

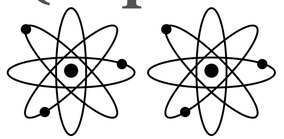
Non-Destructive Entanglement Testing

Hiding Entanglement



State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

Register A (n qubits)



$\sum_x |x\rangle|x\rangle$

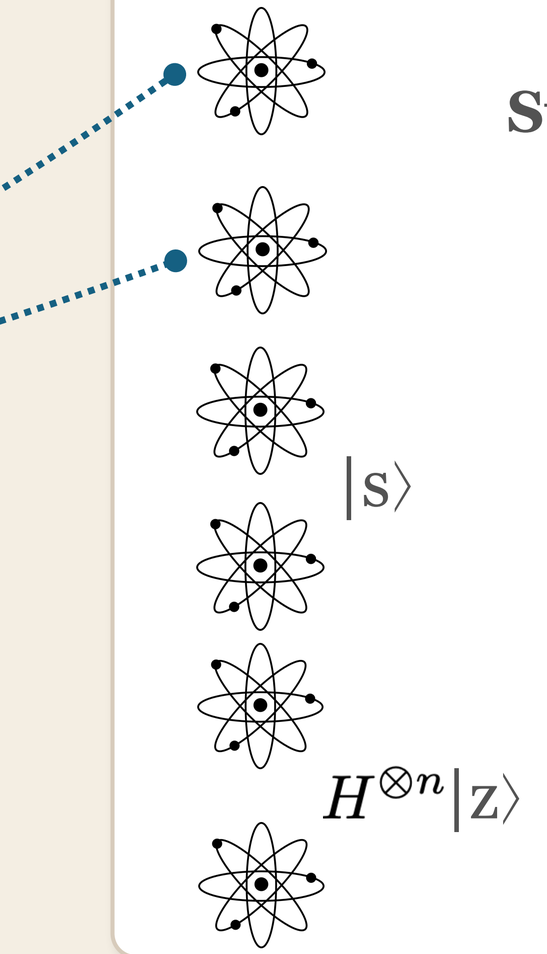
Register B (3n qubits)

Non-Destructive Entanglement Testing

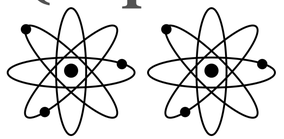
Hiding Entanglement

Randomly sample a change-of-basis matrix $U_{\text{shift}} \in \mathbb{F}_2^{3n \times 3n}$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle} |a\rangle\right) \otimes |s\rangle$



Register **A** (n qubits)



$\sum_x |x\rangle|x\rangle$

Register **B** (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n \times 3n}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle} |a\rangle\right) \otimes |s\rangle$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Register A (n qubits)

$$\sum_x |x\rangle|x\rangle$$

$|s\rangle$

$H^{\otimes n}|z\rangle$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement

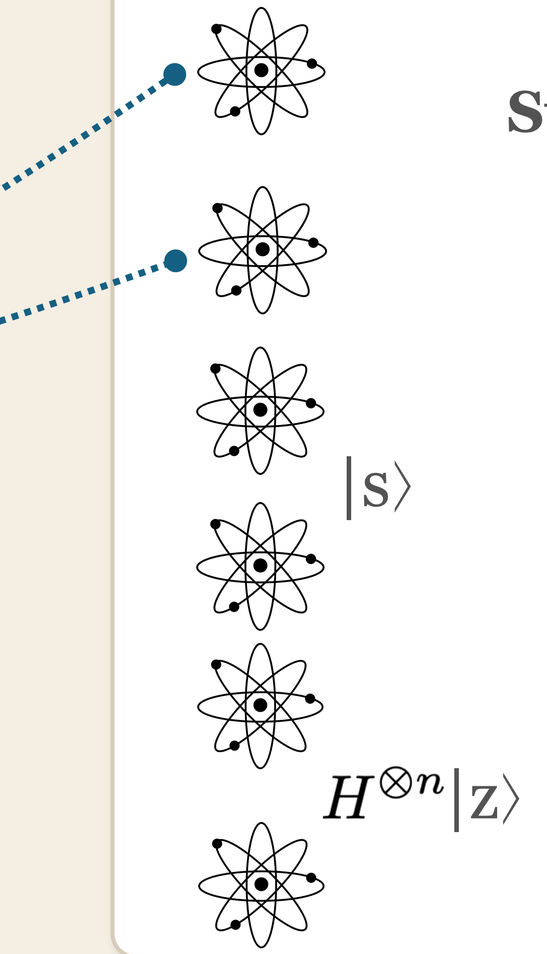
Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n \times 3n}$$

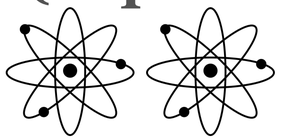
$$T = \overbrace{\underbrace{S}_{}\quad \underbrace{S^{\perp} \cap T}_{}}^{T} \quad \underbrace{T^{\perp}}_{}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z \rangle} |a\rangle\right) \otimes |s\rangle$



Register A (n qubits)

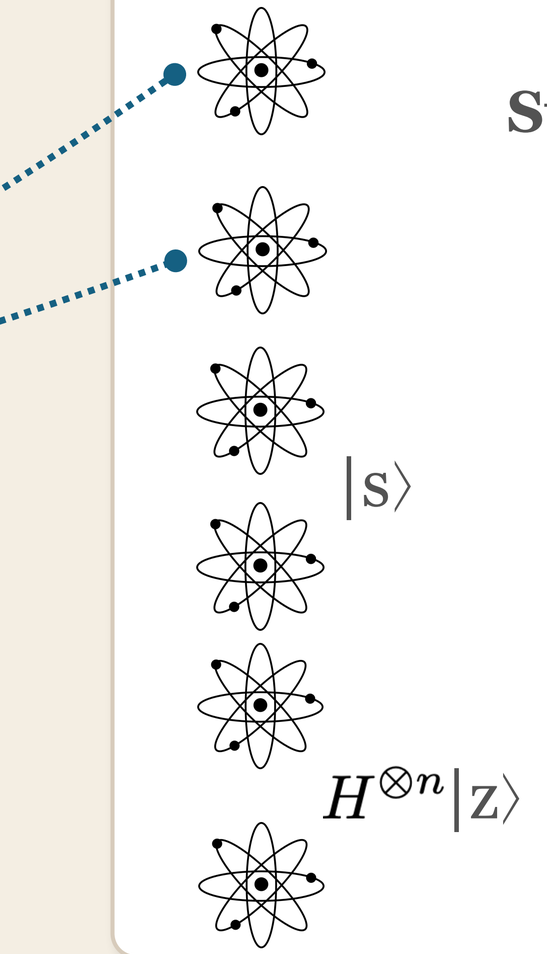


$$\sum_x |x\rangle|x\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n \times 3n}$$

$$\overbrace{\begin{matrix} \underbrace{}_{S} & \underbrace{}_{S^\perp \cap T} & \underbrace{}_{T^\perp} \end{matrix}}^{T}$$

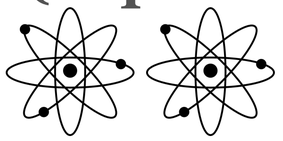
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle} |a\rangle\right) \otimes |s\rangle$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}} x\rangle$$

$$\sum_{x \in \mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a \in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle_{\mathbf{B}}$$

Register A (n qubits)

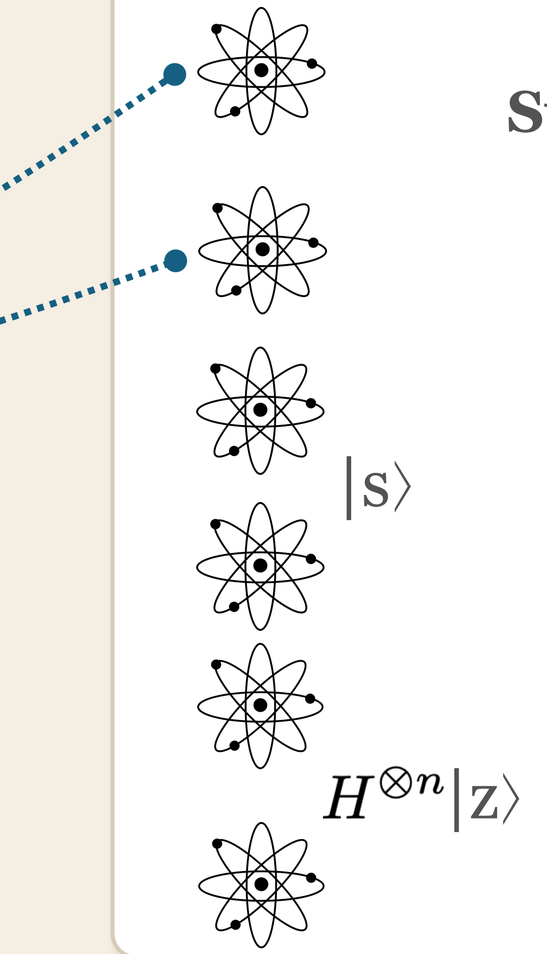


$$\sum_x |x\rangle|x\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



$|s\rangle$

$H^{\otimes n}|z\rangle$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n\times 3n}$$

$$\overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}}^{T}$$

$$\overbrace{\phantom{\begin{pmatrix} 1 & 0 \end{pmatrix}}}^{S}\ \overbrace{\phantom{\begin{pmatrix} 0 & 0 \end{pmatrix}}}^{S^\perp\cap T}\ \overbrace{\phantom{\begin{pmatrix} 0 & 0 \end{pmatrix}}}^{T^\perp}$$

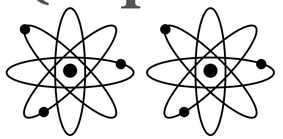
State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle_{\mathbf{B}}$$

S=span(first n columns of U_{shift})

Register A (n qubits)

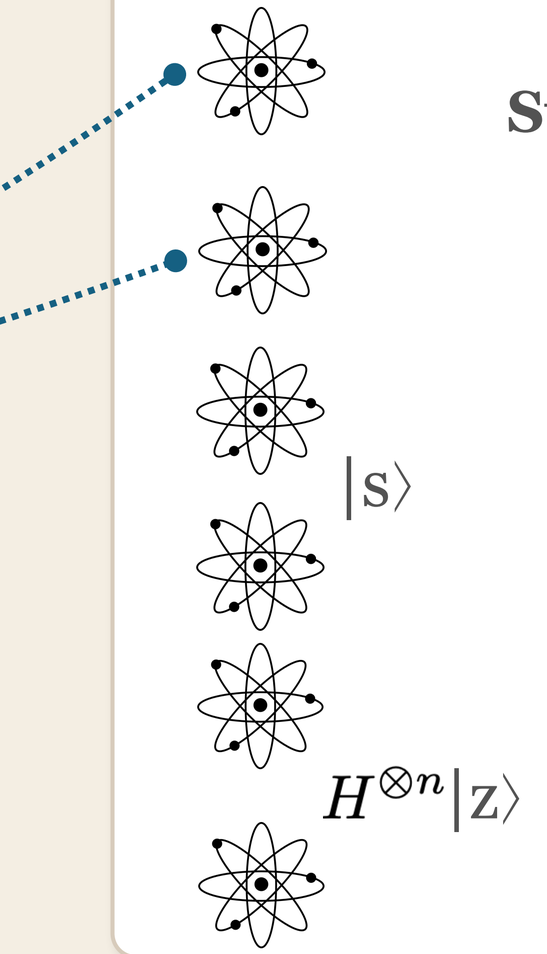


$$\sum_x |x\rangle|x\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



$|\mathrm{S}\rangle$

$H^{\otimes n}|\mathrm{Z}\rangle$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n\times 3n}$$

$$\overbrace{\begin{matrix}\underbrace{}_{S} & \underbrace{}_{S^\perp\cap T} & \underbrace{}_{T^\perp}\end{matrix}}^{T}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$$

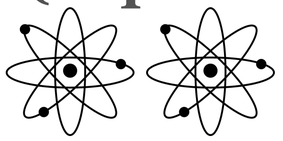
$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle_{\mathbf{B}}$$

S=span(first n columns of U_{shift})

$$v = U_{\text{shift}}(s \times 0^{2n})$$

$$u = U_{\text{shift}}^{-T}(0^{2n} \times z)$$

Register A (n qubits)

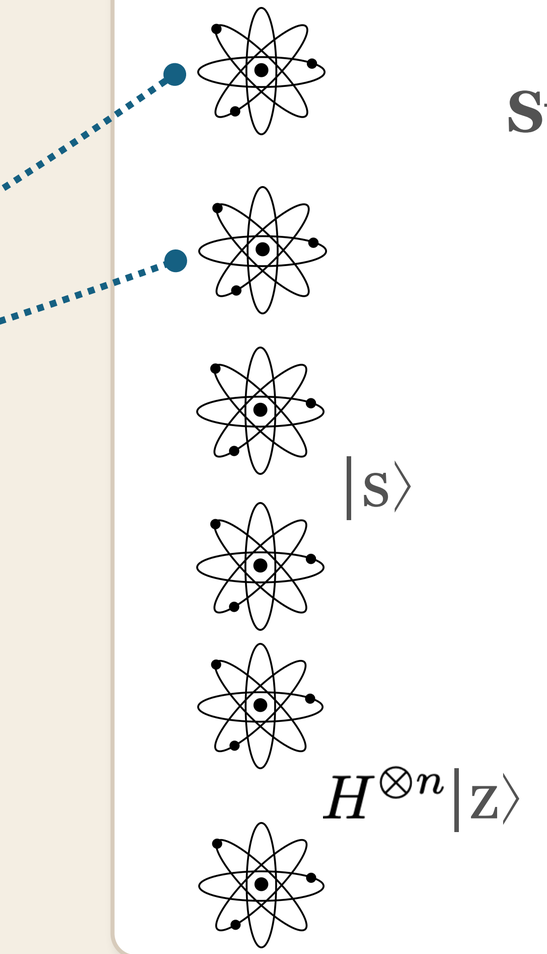


$$\sum_x |x\rangle|x\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



$|s\rangle$

$H^{\otimes n}|z\rangle$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n \times 3n}$$

$$T = \overbrace{S}^{S} \quad \overbrace{S^{\perp} \cap T}^{S^{\perp} \cap T} \quad \overbrace{T^{\perp}}^{T^{\perp}}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle} |a\rangle\right) \otimes |s\rangle$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}} x\rangle$$

$$\sum_{x \in \mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a \in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle_{\mathbf{B}}$$

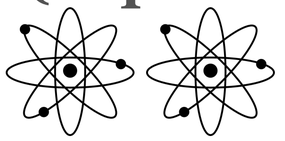
Without knowing U_{shift}, u, v, entanglement is "hidden"

S=span(first n columns of U_{shift})

$$v = U_{\text{shift}}(s \times 0^{2n})$$

$$u = U_{\text{shift}}^{-T}(0^{2n} \times z)$$

Register A (n qubits)

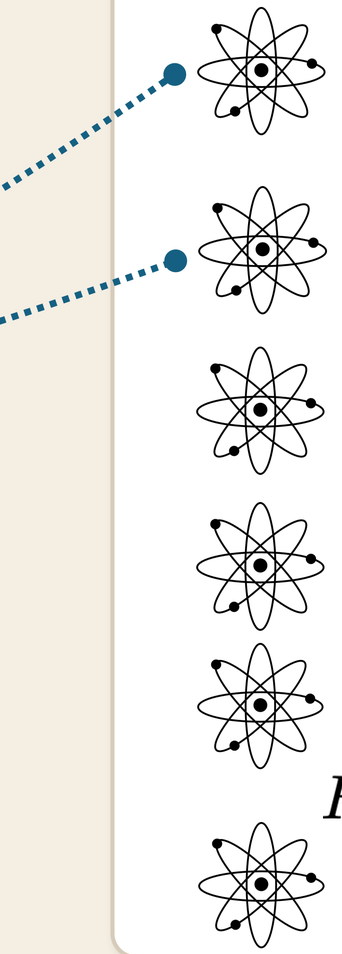


$$\sum_x |x\rangle|x\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



$|s\rangle$

$H^{\otimes n}|z\rangle$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n \times 3n}$$

$$\begin{array}{c} \overbrace{}^{T} \\ \begin{array}{cccccc} \underbrace{}_{S} & & \underbrace{}_{S^\perp \cap T} & & \underbrace{}_{T^\perp} & \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{array} \end{array}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle_{\mathbf{B}}$$

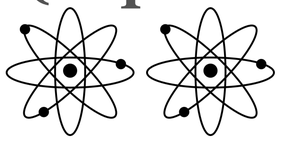
New test: "is register B in the coset T+v" Non-destructive!

S=span(first n columns of U_{shift})

$$v = U_{\text{shift}}(s \times 0^{2n})$$

$$u = U_{\text{shift}}^{-T}(0^{2n} \times z)$$

Register A (n qubits)

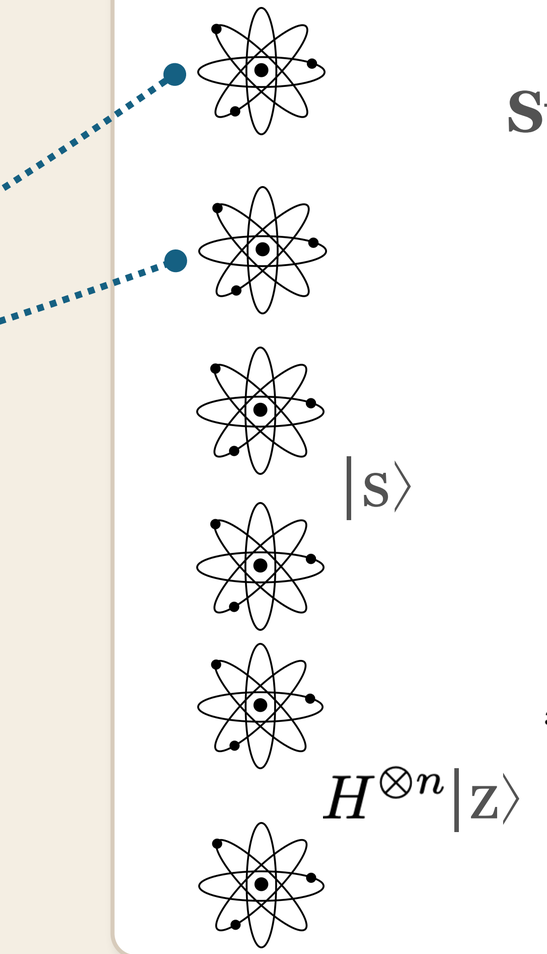


$$\sum_x |x\rangle|x\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



$|s\rangle$

$H^{\otimes n}|z\rangle$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n\times 3n}$$

$$\overbrace{\begin{matrix}\underbrace{}_{S} & \underbrace{}_{S^\perp\cap T} & \underbrace{}_{T^\perp}\end{matrix}}^{T}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle_{\mathbf{B}}$$

$H^{\otimes n}$

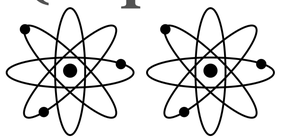
$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in T^\perp} (-1)^{\langle a,v\rangle} |a + U_{\text{shift}}^{-T}(0^n \times x \times 0^n) + u\rangle_{\mathbf{B}}$$

T=span(first 2n columns of U_{shift})

$$v = U_{\text{shift}}(s \times 0^{2n})$$

$$u = U_{\text{shift}}^{-T}(0^{2n} \times z)$$

Register A (n qubits)

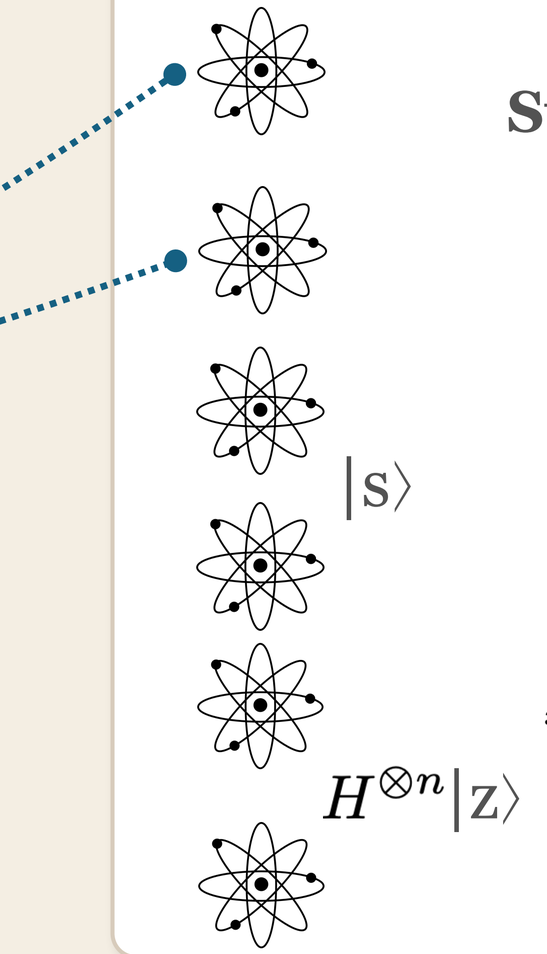


$$\sum_x |x\rangle|x\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



$|\mathrm{S}\rangle$

$H^{\otimes n}|\mathrm{Z}\rangle$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n\times 3n}$$

$$\overbrace{\begin{matrix}\overbrace{}^{S} & \overbrace{}^{S^\perp\cap T} & \overbrace{}^{T^\perp}\end{matrix}}^{T}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle_{\mathbf{B}}$$

$$H^{\otimes n}$$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in T^\perp} (-1)^{\langle a,v\rangle} |a + U_{\text{shift}}^{-T}(0^n \times x \times 0^n) + u\rangle_{\mathbf{B}}$$

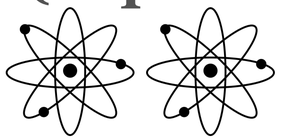
Now: "is register B in the coset T^⊥ +u"

T=span(first 2n columns of U_{shift})

$$v = U_{\text{shift}}(s \times 0^{2n})$$

$$u = U_{\text{shift}}^{-T}(0^{2n} \times z)$$

Register A (n qubits)

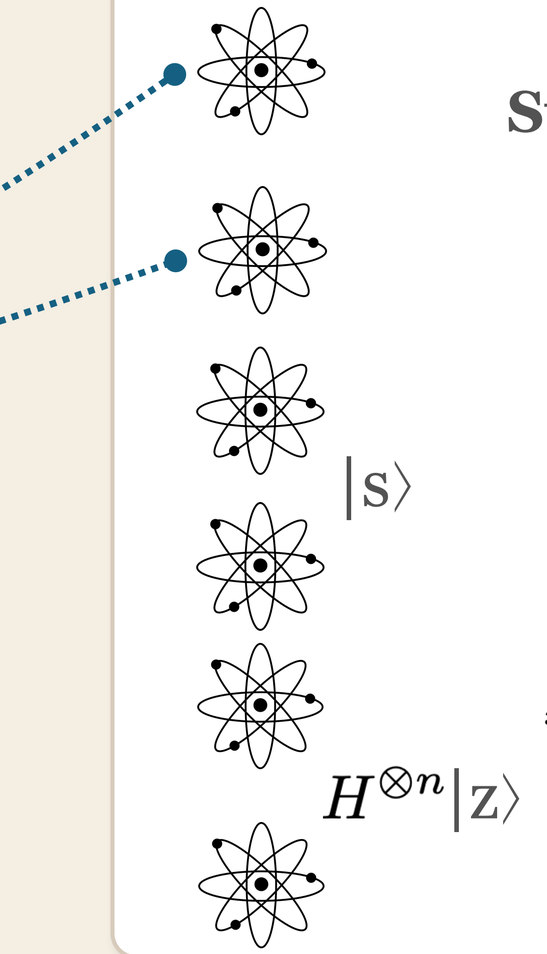


$$\sum_x |x\rangle|x\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



$|\mathrm{S}\rangle$

$H^{\otimes n}|\mathrm{Z}\rangle$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{3n\times 3n}$$

$$\overbrace{\begin{matrix}\underbrace{}_{S} & \underbrace{}_{S^\perp\cap T} & \underbrace{}_{T^\perp}\end{matrix}}^{T}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle_{\mathbf{B}}$$

$H^{\otimes n}$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in T^\perp} (-1)^{\langle a,v\rangle} |a + U_{\text{shift}}^{-T}(0^n \times x \times 0^n) + u\rangle_{\mathbf{B}}$$

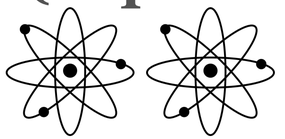
Now: "is register B in the coset T^⊥ +u"

T=span(first 2n columns of U_{shift})

$$v = U_{\text{shift}}(s \times 0^{2n})$$

$$u = U_{\text{shift}}^{-T}(0^{2n} \times z)$$

Register A (n qubits)



$$\sum_x |x\rangle|x\rangle$$

(Cf.) Coset state:

$$\sum_{a\in A} (-1)^{\langle a,z\rangle} |a + s\rangle$$

Register B (3n qubits)

Non-Destructive Entanglement Testing

Crash Course: Coset States

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^{\theta}|w\rangle$$

$$w|_{\theta_i=1} := z$$

$$w|_{\theta_i=0} := s$$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$BB84^{\otimes n} := H^\theta |w\rangle$

$w|_{\theta_i=1} := z$

$w|_{\theta_i=0} := s$

Want "Public verification oracle"

$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$BB84^{\otimes n} := H^\theta |w\rangle$

$w|_{\theta_i=1} := z$

$w|_{\theta_i=0} := s$

Want "Public verification oracle"

$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$ ✗

Susceptible to qubit-by-qubit attack!

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta |w\rangle$$

$$w|_{\theta_i=1} := z$$

$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$

$$\mathcal{O}_{s,z,\theta}$$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

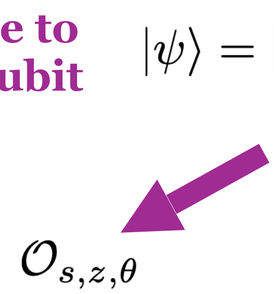
$$BB84^{\otimes n} := H^\theta |w\rangle$$

$$w|_{\theta_i=1} := z$$

$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$



Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$

$$X \otimes I \otimes \cdots \otimes I$$

$$\mathcal{O}_{s,z,\theta}$$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta |w\rangle$$

$$w|_{\theta_i=1} := z$$

$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$

$$X \otimes I \otimes \cdots \otimes I$$

$$I \otimes X \otimes \cdots \otimes I$$

$$\mathcal{O}_{s,z,\theta}$$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta |w\rangle$$

$$w|_{\theta_i=1} := z$$

$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$

$$X \otimes I \otimes \cdots \otimes I$$

$$I \otimes X \otimes \cdots \otimes I$$

$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n \times 2n}$$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta |w\rangle$$

$$w|_{\theta_i=1} := z$$

$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$

$$X \otimes I \otimes \cdots \otimes I$$

$$I \otimes X \otimes \cdots \otimes I$$

$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n \times 2n}$$

$$\mathcal{U}_{\text{shift}} |x\rangle := |U_{\text{shift}} x\rangle$$

$$|A_{s,z}\rangle := \sum_{a \in A} (-1)^{\langle a,z \rangle} |a + s\rangle$$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta |w\rangle$$
$$w|_{\theta_i=1} := z$$
$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$
$$X \otimes I \otimes \cdots \otimes I$$
$$I \otimes X \otimes \cdots \otimes I$$
$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n \times 2n}$$

$$\mathcal{U}_{\text{shift}} |x\rangle := |U_{\text{shift}} x\rangle$$

$$|A_{s,z}\rangle := \sum_{a \in A} (-1)^{\langle a,z \rangle} |a+s\rangle$$

$$H^{\otimes n}$$

$$|A^\perp_{z,s}\rangle := \sum_{a \in A^\perp} (-1)^{\langle a,s \rangle} |a+z\rangle$$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta |w\rangle$$
$$w|_{\theta_i=1} := z$$
$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$
$$X \otimes I \otimes \cdots \otimes I$$
$$I \otimes X \otimes \cdots \otimes I$$
$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n \times 2n}$$

$$\mathcal{U}_{\text{shift}} |x\rangle := |U_{\text{shift}} x\rangle$$

$$|A_{s,z}\rangle := \sum_{a \in A} (-1)^{\langle a,z \rangle} |a+s\rangle$$

$$H^{\otimes n}$$

$$|A^\perp_{z,s}\rangle := \sum_{a \in A^\perp} (-1)^{\langle a,s \rangle} |a+z\rangle$$

A=span(first n columns of U_{shift})

$A^\perp$=span(last n columns of U_{shift})

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta |w\rangle$$
$$w|_{\theta_i=1} := z$$
$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$
$$X \otimes I \otimes \cdots \otimes I$$
$$I \otimes X \otimes \cdots \otimes I$$
$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n \times 2n}$$

$$\mathcal{U}_{\text{shift}} |x\rangle := |U_{\text{shift}} x\rangle$$

$$|A_{s,z}\rangle := \sum_{a \in A} (-1)^{\langle a,z \rangle} |a+s\rangle$$

$$H^{\otimes n}$$

$$|A^\perp_{z,s}\rangle := \sum_{a \in A^\perp} (-1)^{\langle a,s \rangle} |a+z\rangle$$

Public verification oracles

$$\mathcal{O}_{s,z,A} := |A_{s,z}\rangle\langle A_{s,z}|$$
$$\mathcal{O}_{z,s,A^\perp} := |A^\perp_{z,s}\rangle\langle A^\perp_{z,s}|$$

Get public-key quantum money!

A=span(first n columns of U_{shift})

$A^\perp$=span(last n columns of U_{shift})

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta|w\rangle$$
$$w|_{\theta_i=1} := z$$
$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta|w\rangle\langle w|H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$
$$X \otimes I \otimes \cdots \otimes I$$
$$I \otimes X \otimes \cdots \otimes I$$
$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n\times 2n}$$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$$

$$|A_{s,z}\rangle := \sum_{a\in A}(-1)^{\langle a,z\rangle}|a+s\rangle$$

$$\xrightarrow{H^{\otimes n}}$$

$$|A^\perp_{z,s}\rangle := \sum_{a\in A^\perp}(-1)^{\langle a,s\rangle}|a+z\rangle$$

A=span(first n columns of U_{shift})

$A^\perp$=span(last n columns of U_{shift})

Public verification oracles

$$\mathcal{O}_{s,z,A} := |A_{s,z}\rangle\langle A_{s,z}|$$
$$\mathcal{O}_{z,s,A^\perp} := |A^\perp_{z,s}\rangle\langle A^\perp_{z,s}|$$

Get public-key quantum money!

Coset MoE property [CV'22]:

$|A_{s,z}\rangle$

$\mathcal{O}_{s,z,A}$

$\mathcal{O}_{z,s,A^\perp}$

Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta|w\rangle$$
$$w|_{\theta_i=1} := z$$
$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta|w\rangle\langle w|H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$
$$X \otimes I \otimes \cdots \otimes I$$
$$I \otimes X \otimes \cdots \otimes I$$
$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n\times 2n}$$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$$

$$|A_{s,z}\rangle := \sum_{a\in A}(-1)^{\langle a,z\rangle}|a+s\rangle$$

$$\downarrow H^{\otimes n} \quad \uparrow H^{\otimes n}$$

$$|A^\perp_{z,s}\rangle := \sum_{a\in A^\perp}(-1)^{\langle a,s\rangle}|a+z\rangle$$

A=span(first n columns of U_{shift})

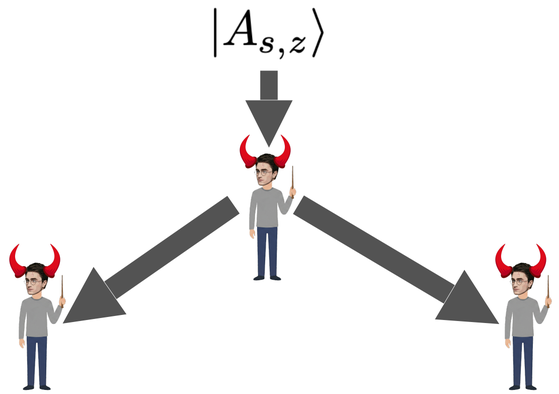
$A^\perp$=span(last n columns of U_{shift})

Public verification oracles

$$\mathcal{O}_{s,z,A} := |A_{s,z}\rangle\langle A_{s,z}|$$
$$\mathcal{O}_{z,s,A^\perp} := |A^\perp_{z,s}\rangle\langle A^\perp_{z,s}|$$

Get public-key quantum money!

Coset MoE property [CV'22]:



Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta |w\rangle$$
$$w|_{\theta_i=1} := z$$
$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta |w\rangle\langle w| H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$

$$X \otimes I \otimes \cdots \otimes I$$

$$I \otimes X \otimes \cdots \otimes I$$

$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n \times 2n}$$

$$\mathcal{U}_{\text{shift}} |x\rangle := |U_{\text{shift}} x\rangle$$

$$|A_{s,z}\rangle := \sum_{a \in A} (-1)^{\langle a,z \rangle} |a+s\rangle$$

$$H^{\otimes n}$$

$$|A^\perp_{z,s}\rangle := \sum_{a \in A^\perp} (-1)^{\langle a,s \rangle} |a+z\rangle$$

Public verification oracles

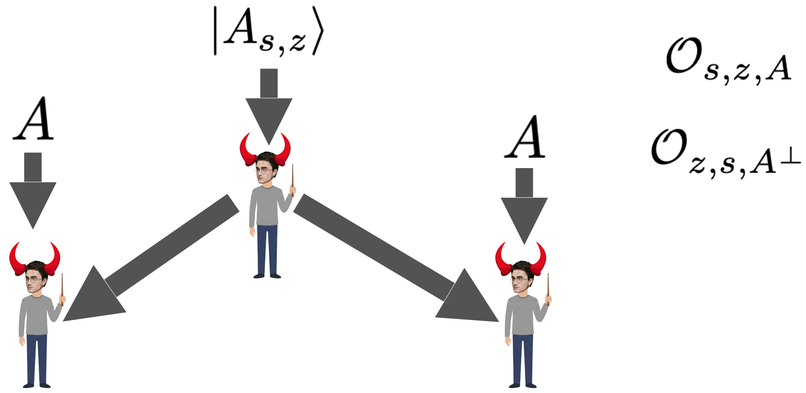
$$\mathcal{O}_{s,z,A} := |A_{s,z}\rangle\langle A_{s,z}|$$
$$\mathcal{O}_{z,s,A^\perp} := |A^\perp_{z,s}\rangle\langle A^\perp_{z,s}|$$

Get public-key quantum money!

A=span(first n columns of U_{shift})

$A^\perp$=span(last n columns of U_{shift})

Coset MoE property [CV'22]:



Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta|w\rangle$$
$$w|_{\theta_i=1} := z$$
$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta|w\rangle\langle w|H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$
$$X \otimes I \otimes \cdots \otimes I$$
$$I \otimes X \otimes \cdots \otimes I$$
$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n\times 2n}$$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$$

$$|A_{s,z}\rangle := \sum_{a\in A}(-1)^{\langle a,z\rangle}|a+s\rangle$$

$$H^{\otimes n}$$

$$|A^\perp_{z,s}\rangle := \sum_{a\in A^\perp}(-1)^{\langle a,s\rangle}|a+z\rangle$$

Public verification oracles

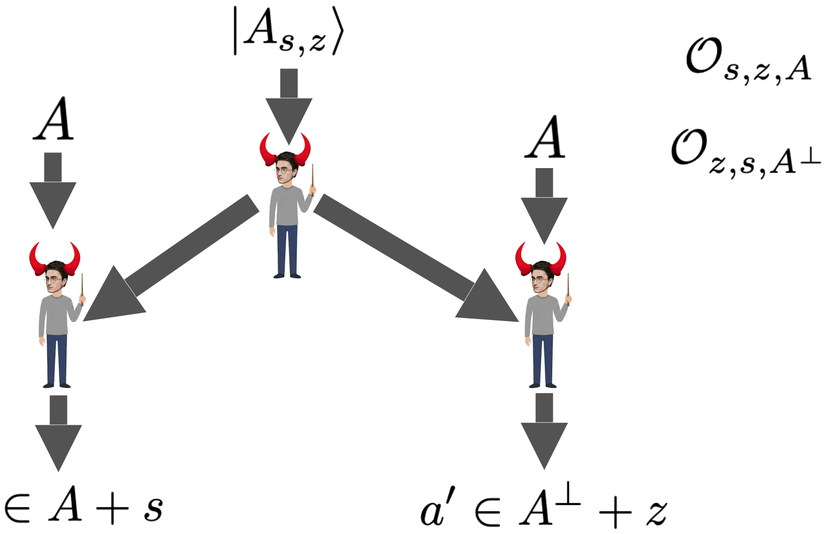
$$\mathcal{O}_{s,z,A} := |A_{s,z}\rangle\langle A_{s,z}|$$
$$\mathcal{O}_{z,s,A^\perp} := |A^\perp_{z,s}\rangle\langle A^\perp_{z,s}|$$

Get public-key quantum money!

A=span(first n columns of U_{shift})

$A^\perp$=span(last n columns of U_{shift})

Coset MoE property [CV'22]:



Non-Destructive Entanglement Testing

Crash Course: Coset States

Starting point: BB84 states

$$BB84^{\otimes n} := H^\theta|w\rangle$$
$$w|_{\theta_i=1} := z$$
$$w|_{\theta_i=0} := s$$

Want "Public verification oracle"

$$\mathcal{O}_{s,z,\theta} := H^\theta|w\rangle\langle w|H^\theta$$

Susceptible to qubit-by-qubit attack!

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$
$$X \otimes I \otimes \cdots \otimes I$$
$$I \otimes X \otimes \cdots \otimes I$$
$$\mathcal{O}_{s,z,\theta}$$

Randomly sample a change-of-basis matrix

$$U_{\text{shift}} \in \mathbb{F}_2^{2n\times 2n}$$

$$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$$

$$|A_{s,z}\rangle := \sum_{a\in A}(-1)^{\langle a,z\rangle}|a+s\rangle$$

$$H^{\otimes n}$$

$$|A^\perp_{z,s}\rangle := \sum_{a\in A^\perp}(-1)^{\langle a,s\rangle}|a+z\rangle$$

Public verification oracles

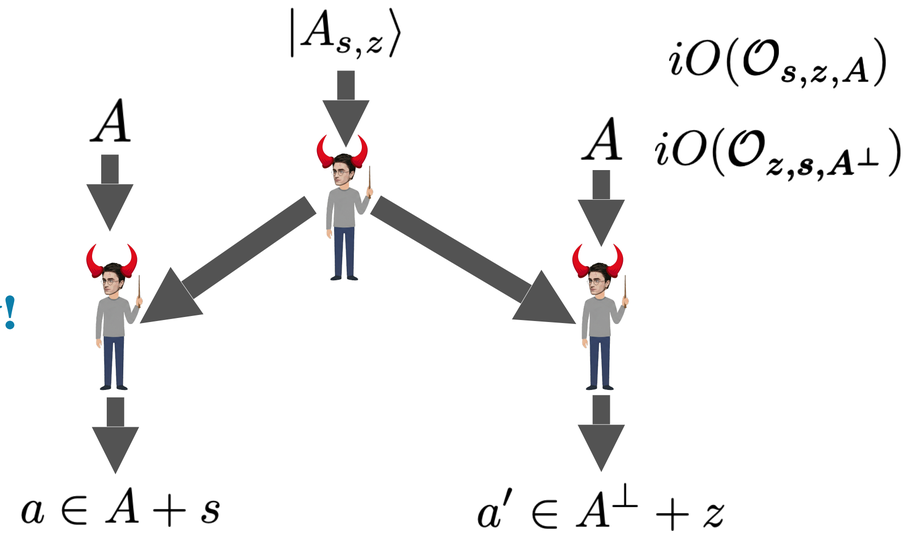
$$\mathcal{O}_{s,z,A} := |A_{s,z}\rangle\langle A_{s,z}|$$
$$\mathcal{O}_{z,s,A^\perp} := |A^\perp_{z,s}\rangle\langle A^\perp_{z,s}|$$

Get public-key quantum money!

A=span(first n columns of U_{shift})

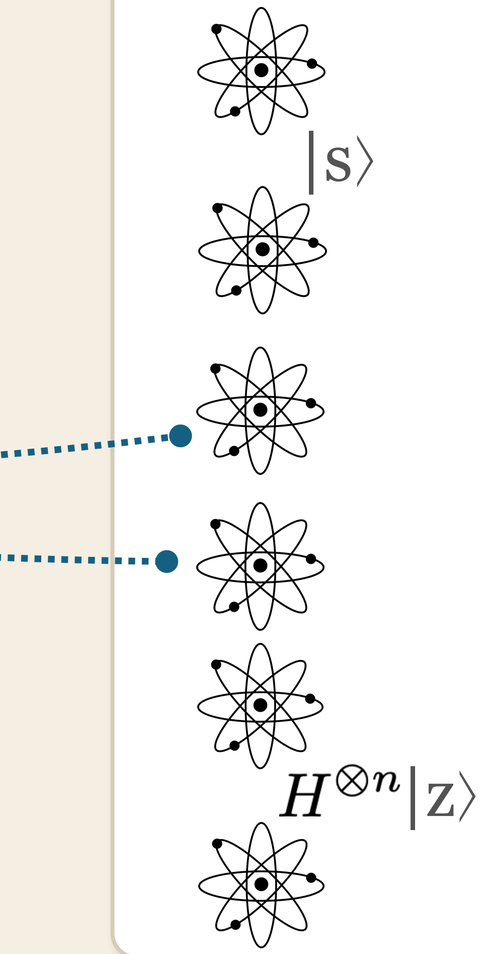
$A^\perp$=span(last n columns of U_{shift})

Coset MoE property [CV'22]:



Non-Destructive Entanglement Testing

Hiding Entanglement

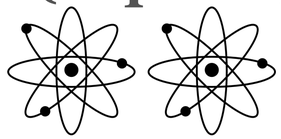


State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle \text{⚓} \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle \text{☠}$$

Register ⚓ (n qubits)



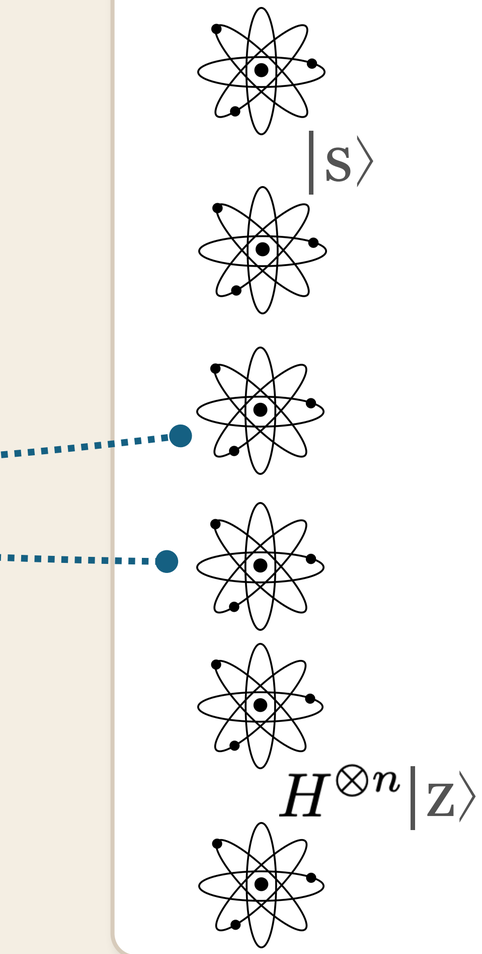
$\sum_x |x\rangle|x\rangle$

1. Verifier generates ⚓☠, sends ☠ to prover
2. Verifier gives out oracles $\mathcal{O}^{b_0}_{S,v}$ and $\mathcal{O}^{b_1}_{T^\perp,u}$, which hide secret random strings b0 and b1
3. Prover must find b0 and b1 by querying the oracles on the ☠ register
4. We've now non-destructively "taken standard and Hadamard measurements" of the entangled qubits

Register ☠ (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement

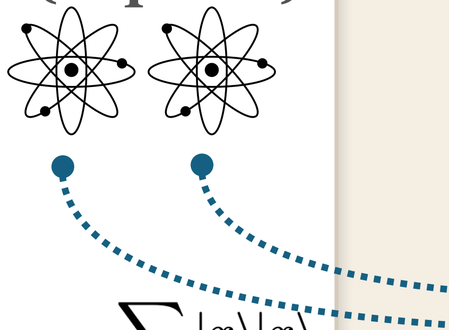


State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle$$

Register ⚓ (n qubits)



$$\sum_x |x\rangle|x\rangle$$

1. Verifier generates ⚓🏴‍☠️, sends 🏴‍☠️ to prover
2. Verifier gives out oracles $\mathcal{O}^{b_0}_{S,v}$ and $\mathcal{O}^{b_1}_{T^\perp,u}$, which hide secret random strings b0 and b1
3. Prover must find b0 and b1 by querying the oracles on the 🏴‍☠️ register
4. We've now non-destructively "taken standard and Hadamard measurements" of the entangled qubits

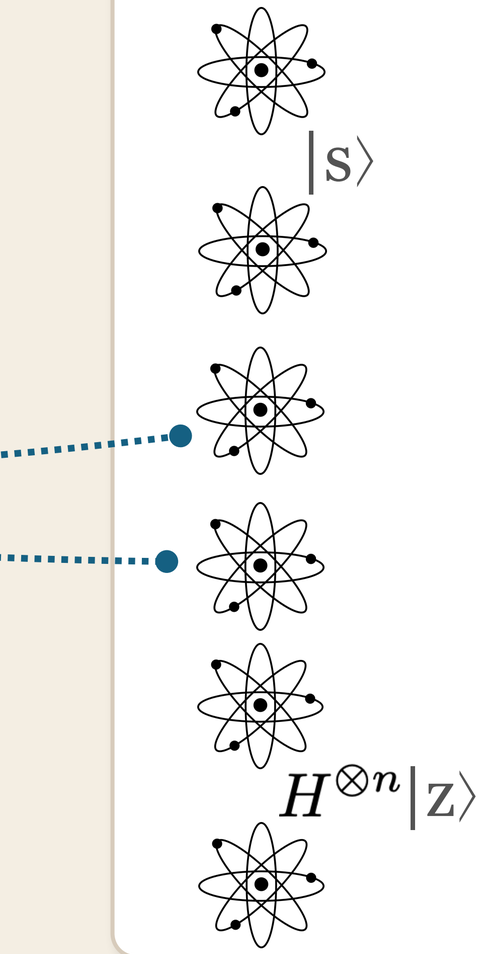
$$\mathcal{O}^{b_0}_{S,v}(a) = \begin{cases} b_0, & \text{if } a \in S + v, \\ \perp, & \text{otherwise} \end{cases}$$

$$\mathcal{O}^{b_1}_{T^\perp,u}(a) = \begin{cases} b_1, & \text{if } a \in T^\perp + u, \\ \perp, & \text{otherwise} \end{cases}$$

Register 🏴‍☠️ (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement



State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$

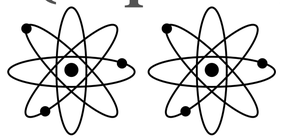
$$\sum_{x\in\mathbb{F}_2^n} |x\rangle \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle$$

$H^{\otimes n}$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle_{\mathbf{A}} \sum_{a\in T^\perp} (-1)^{\langle a,v\rangle} |a + U_{\text{shift}}^{-T}(0^n \times x \times 0^n) + u\rangle_{\mathbf{B}}$$

T=span(last n columns of U_{shift})

Register ⚓ (n qubits)



$$\sum_x |x\rangle|x\rangle$$

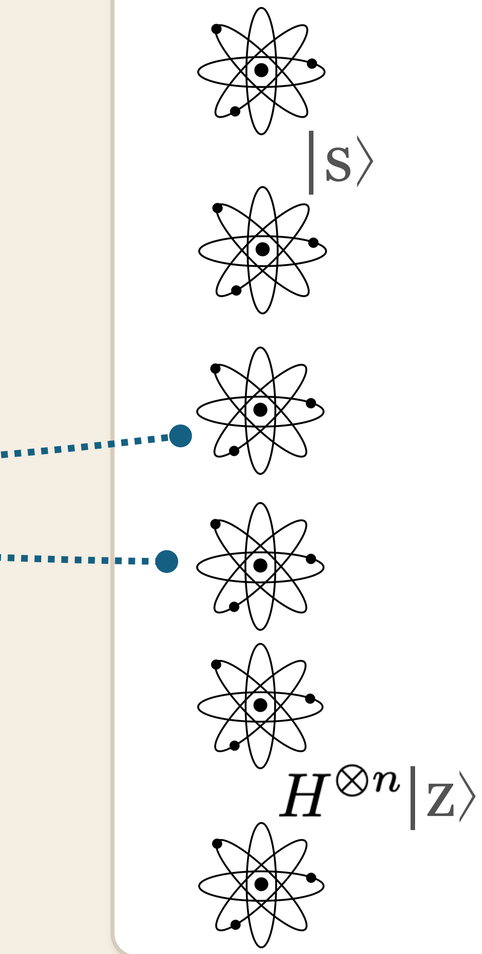
$$\mathcal{O}_{S,v}^{b_0}(a) = \begin{cases} b_0, & \text{if } a \in S + v, \\ \perp, & \text{otherwise} \end{cases}$$

$$\mathcal{O}_{T^\perp,u}^{b_1}(a) = \begin{cases} b_1, & \text{if } a \in T^\perp + u, \\ \perp, & \text{otherwise} \end{cases}$$

Register 🏴‍☠️ (3n qubits)

Non-Destructive Entanglement Testing

Hiding Entanglement

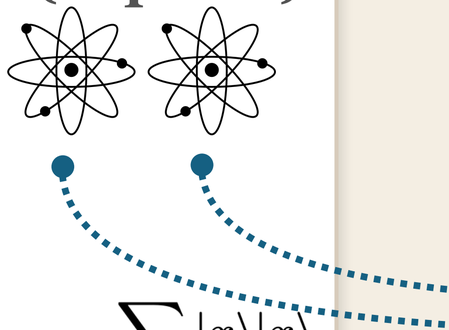


State: $\left(\sum_x |x\rangle\right) \otimes \left(\sum_a (-1)^{\langle a,z\rangle}|a\rangle\right) \otimes |s\rangle$

$\mathcal{U}_{\text{shift}}|x\rangle := |U_{\text{shift}}x\rangle$

$$\sum_{x\in\mathbb{F}_2^n} |x\rangle \sum_{a\in S} (-1)^{\langle a,u\rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle$$

Register ⚓ (n qubits)



$$\sum_x |x\rangle|x\rangle$$

1. Verifier generates ⚓🏴‍☠️, sends 🏴‍☠️ to prover
2. Verifier gives out oracles $\mathcal{O}^{b_0}_{S,v}$ and $\mathcal{O}^{b_1}_{T^\perp,u}$, which hide secret random strings b0 and b1
3. Prover must find b0 and b1 by querying the oracles on the 🏴‍☠️ register
4. We've now non-destructively "taken standard and Hadamard measurements" of the entangled qubits

$$\mathcal{O}^{b_0}_{S,v}(a) = \begin{cases} b_0, & \text{if } a \in S + v, \\ \perp, & \text{otherwise} \end{cases}$$

$$\mathcal{O}^{b_1}_{T^\perp,u}(a) = \begin{cases} b_1, & \text{if } a \in T^\perp + u, \\ \perp, & \text{otherwise} \end{cases}$$

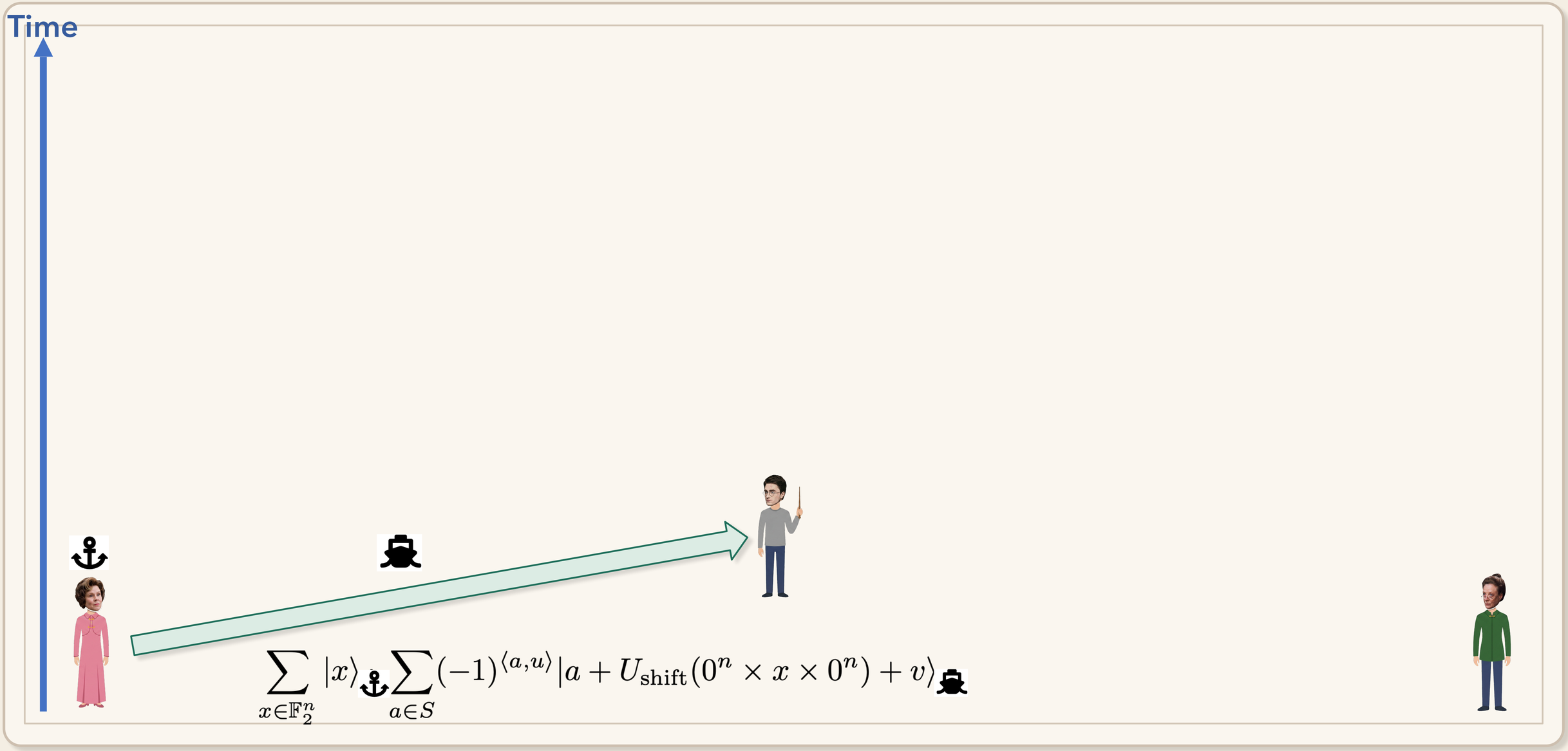
Register 🏴‍☠️ (3n qubits)

Protocol: Trajectory Verification

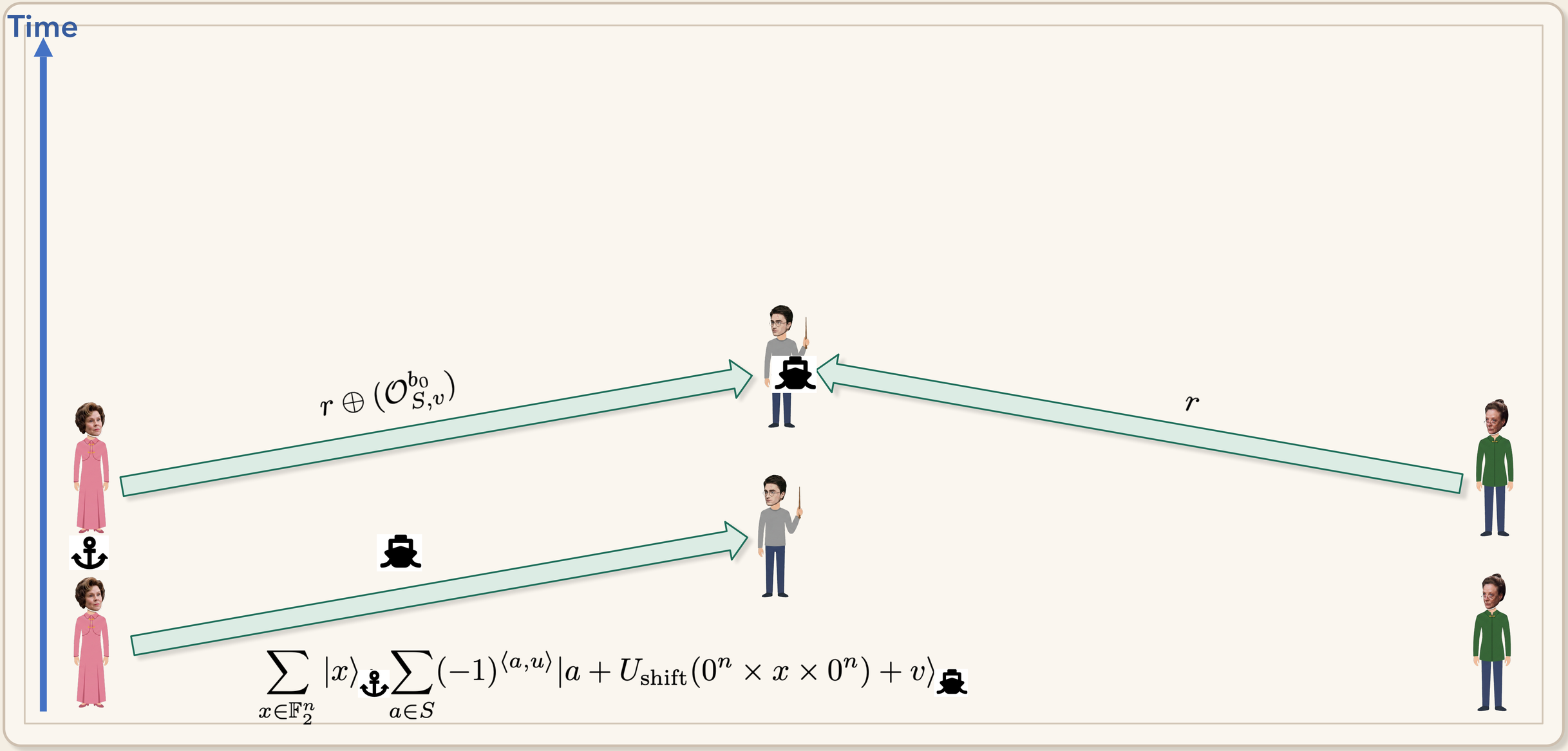
Time

$$\sum_{x \in \mathbb{F}_2^n} |x\rangle \sum_{a \in S} (-1)^{\langle a,u \rangle} |a + U_{\text{shift}}(0^n \times x \times 0^n) + v\rangle$$

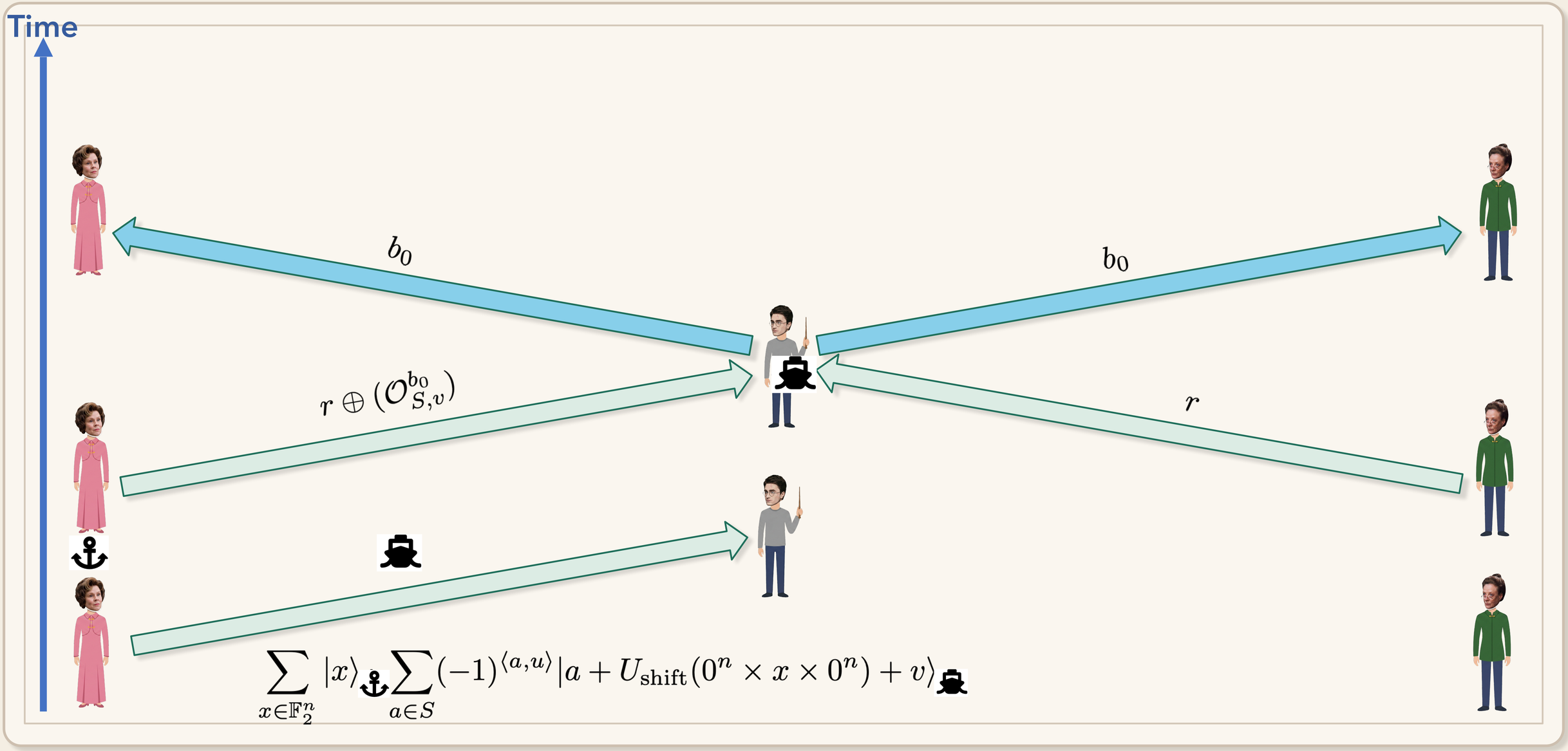
Protocol: Trajectory Verification



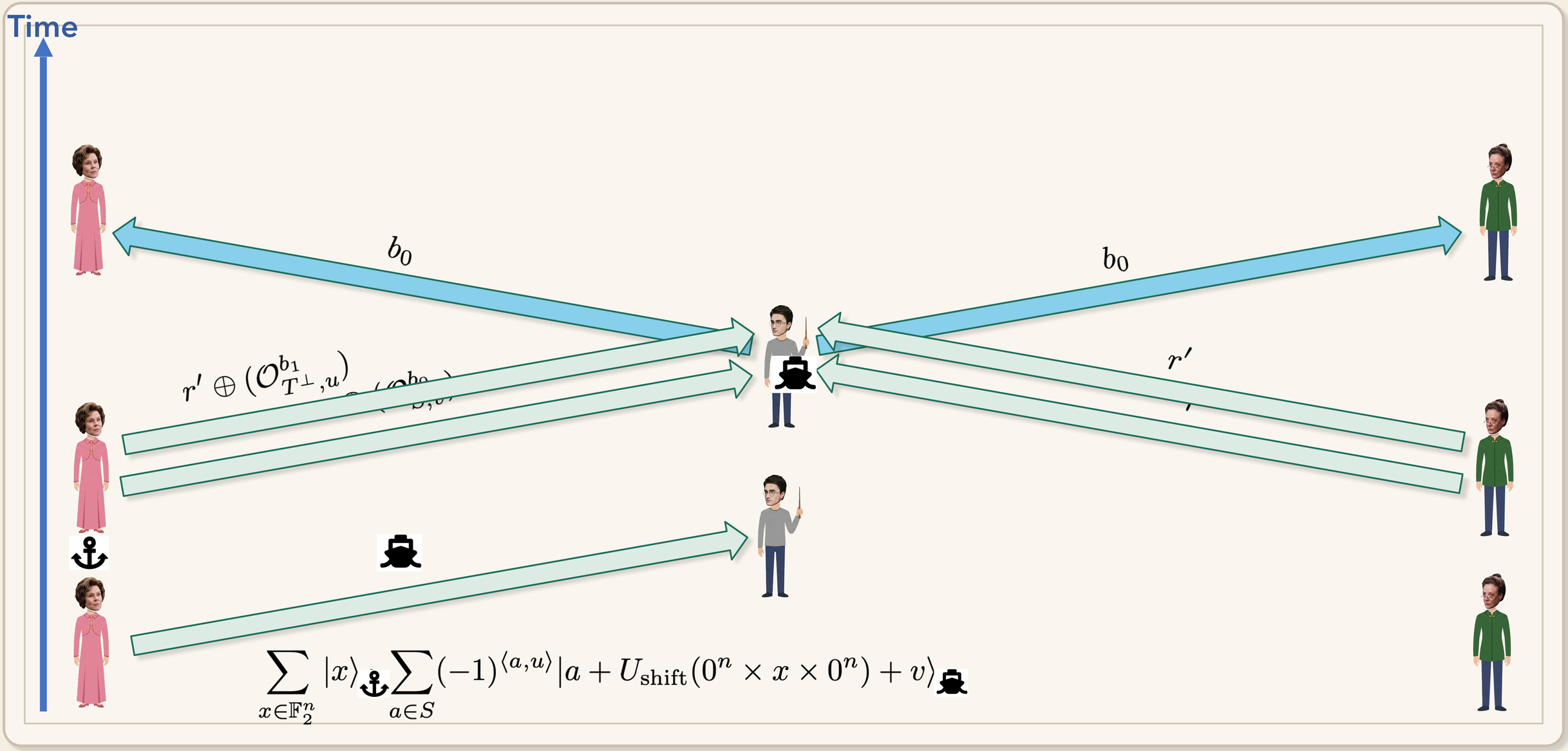
Protocol: Trajectory Verification



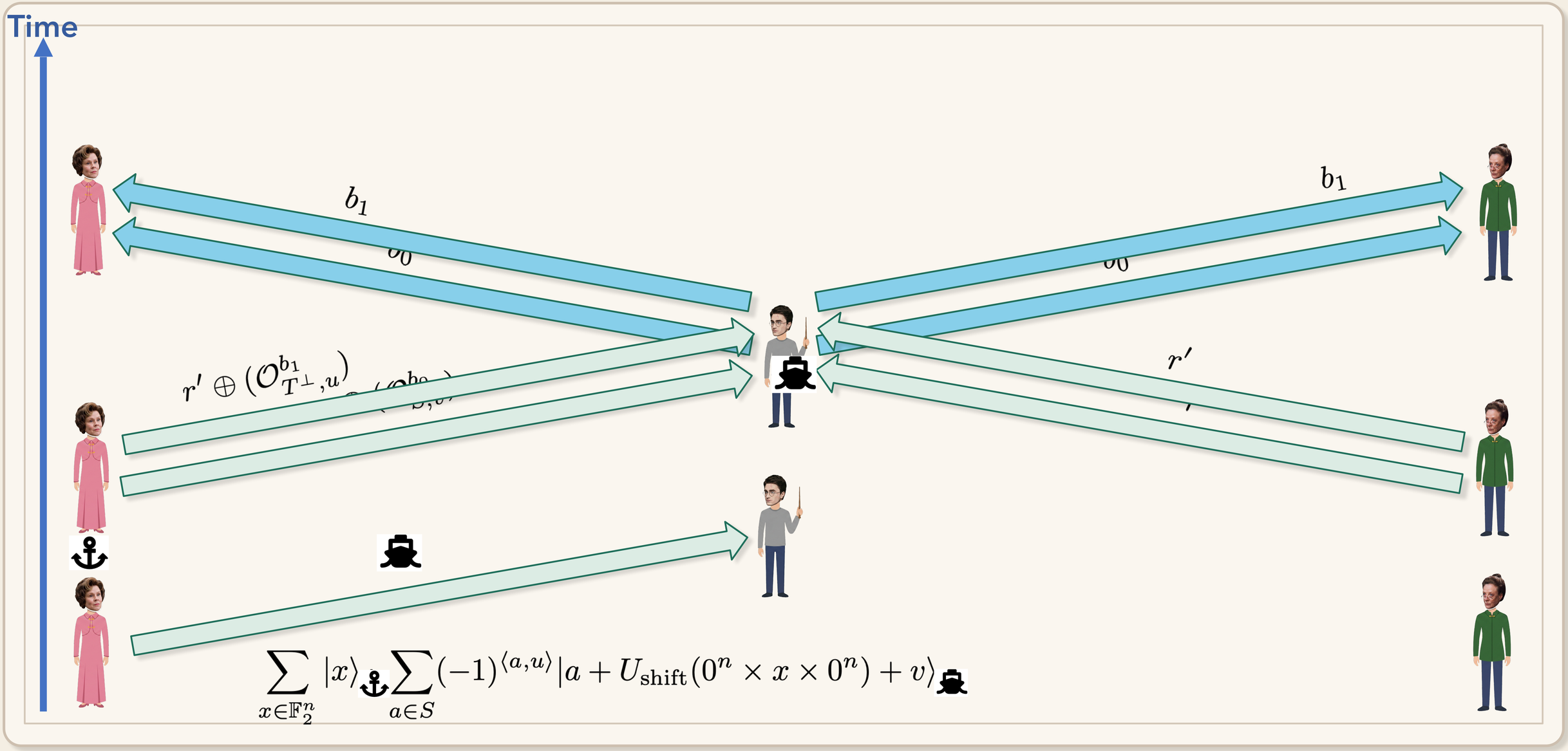
Protocol: Trajectory Verification



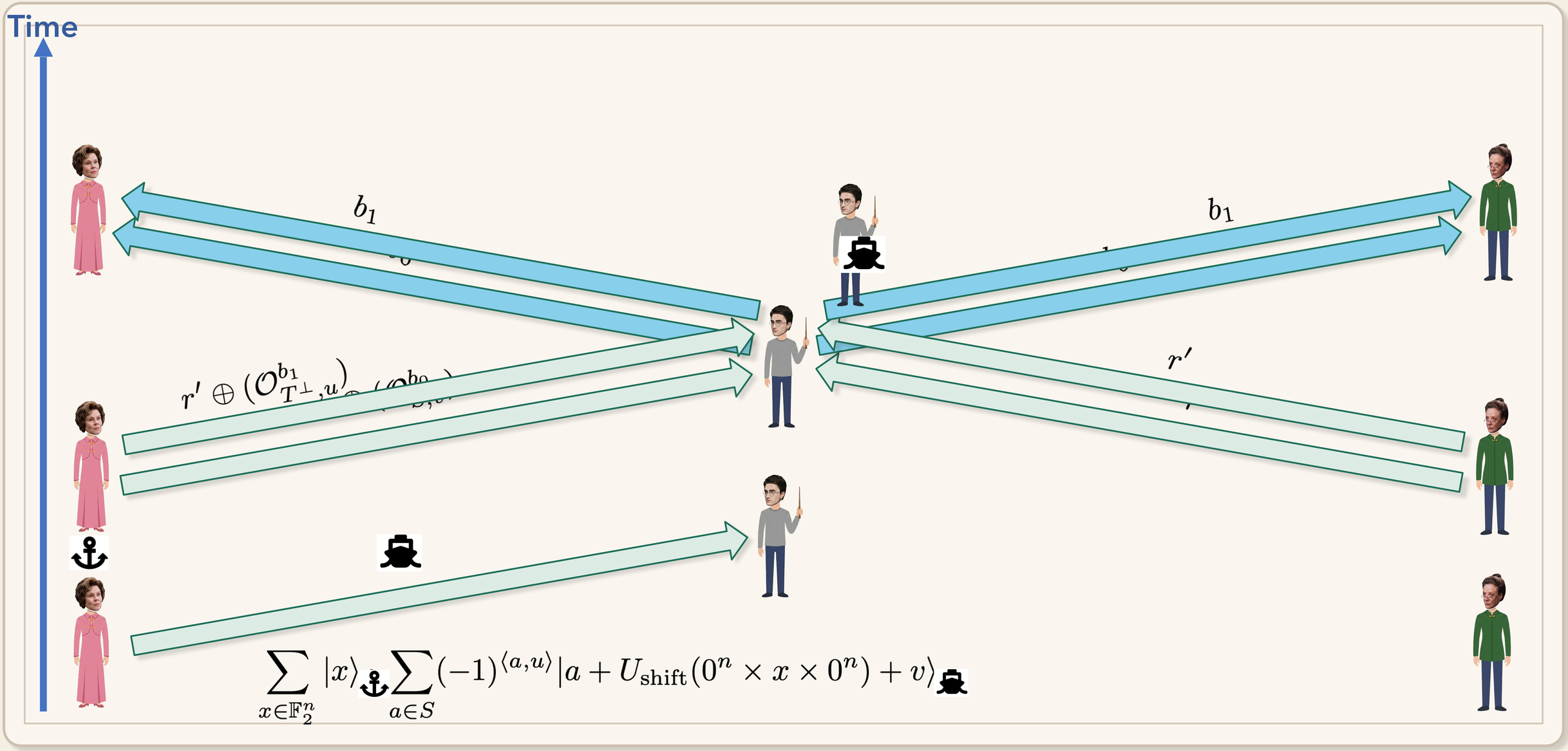
Protocol: Trajectory Verification



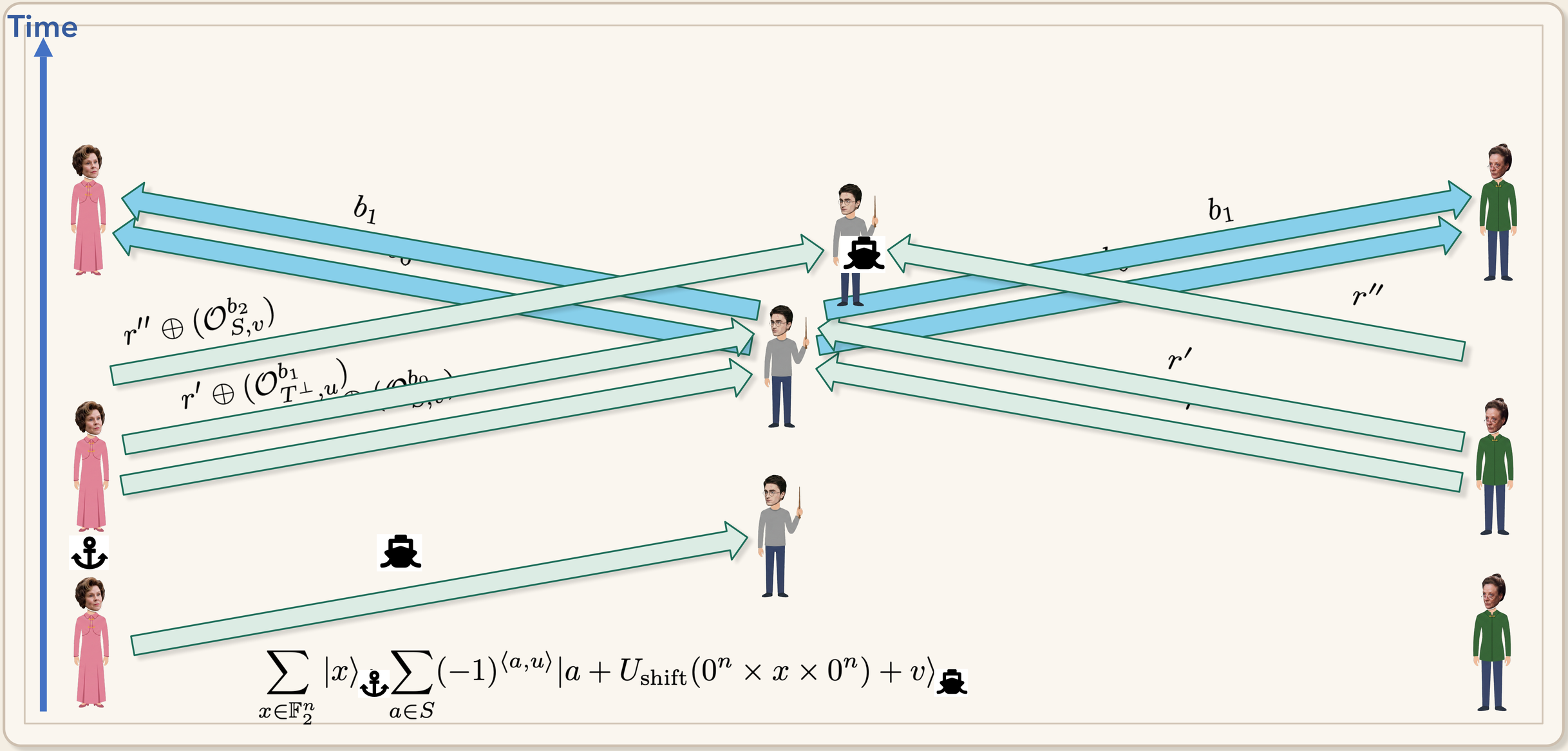
Protocol: Trajectory Verification



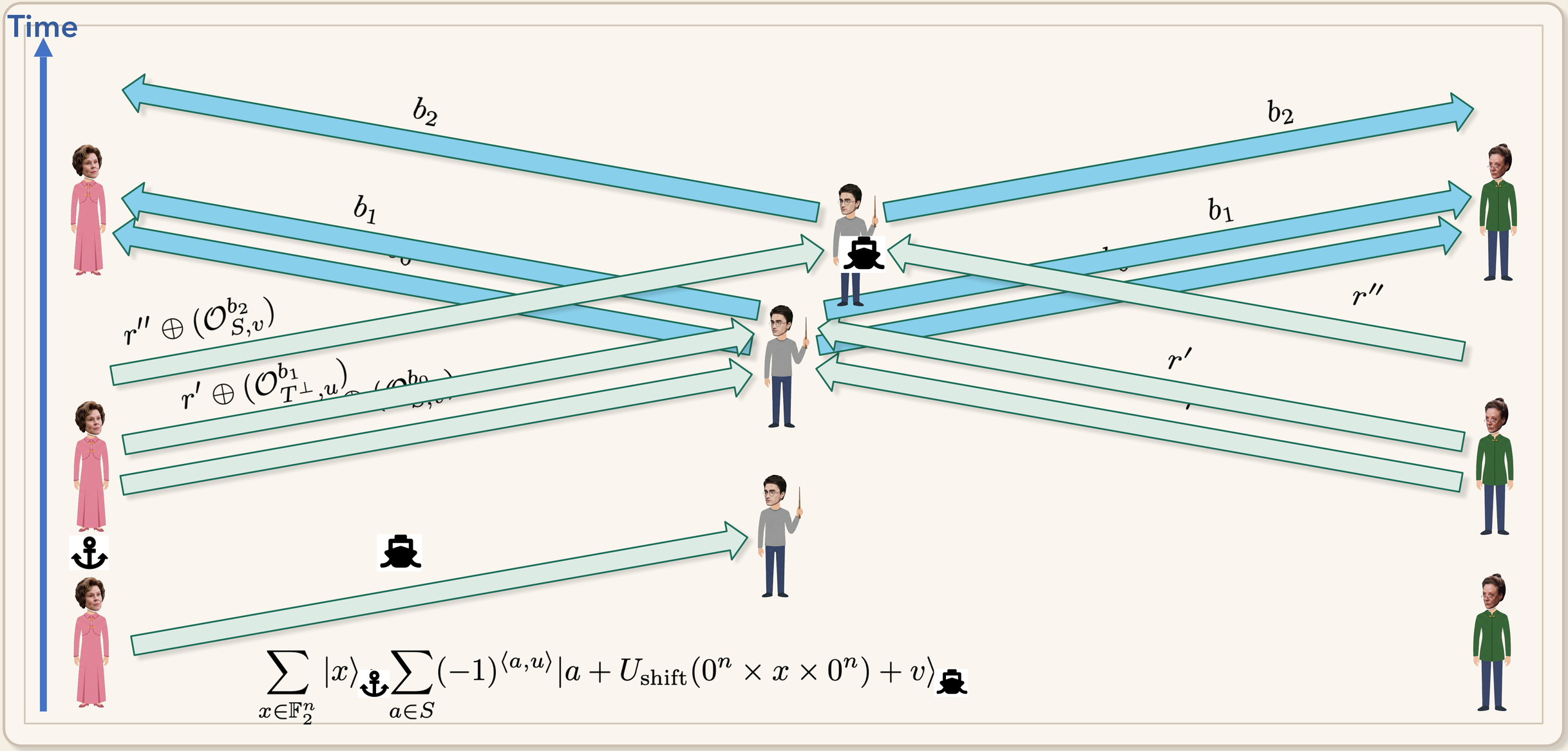
Protocol: Trajectory Verification



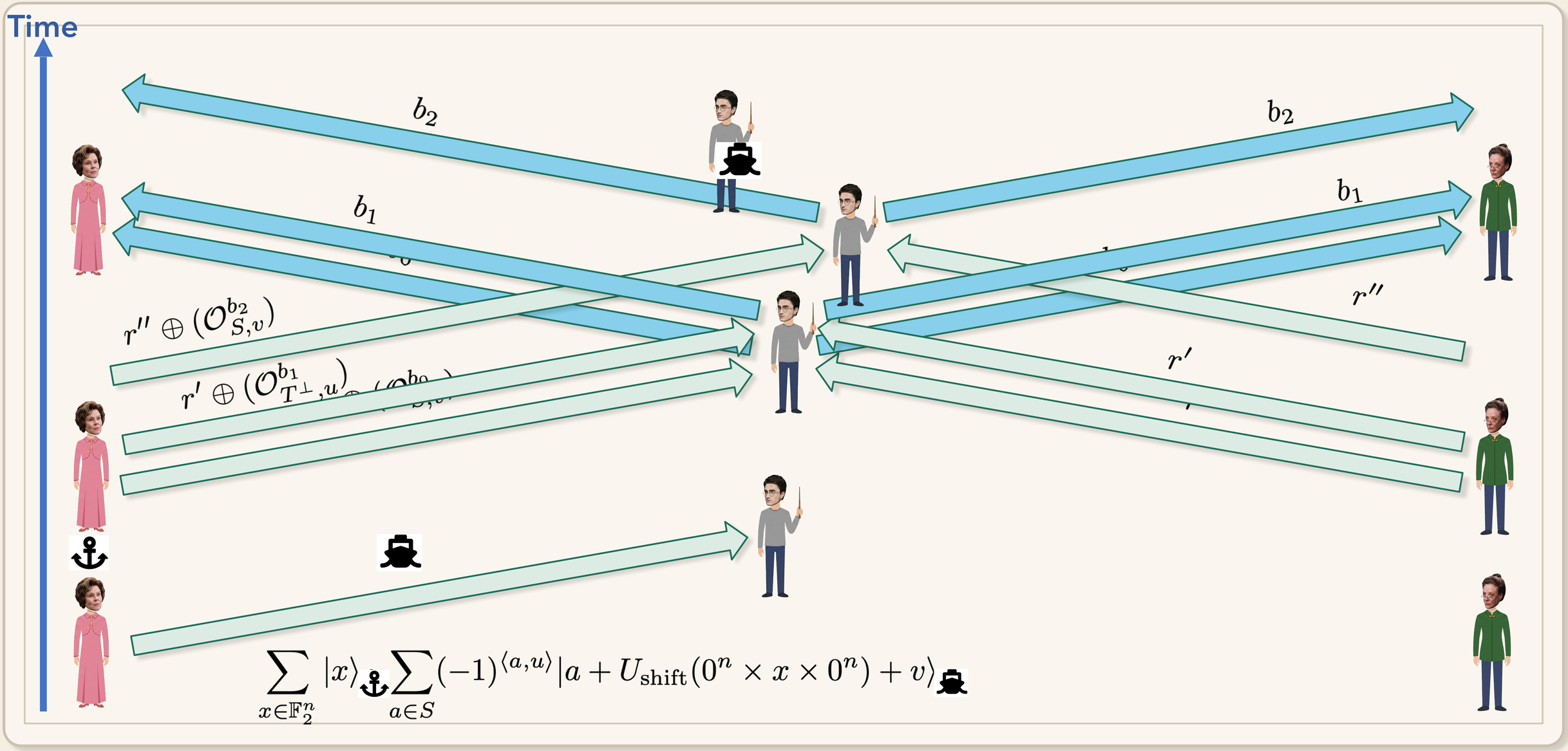
Protocol: Trajectory Verification



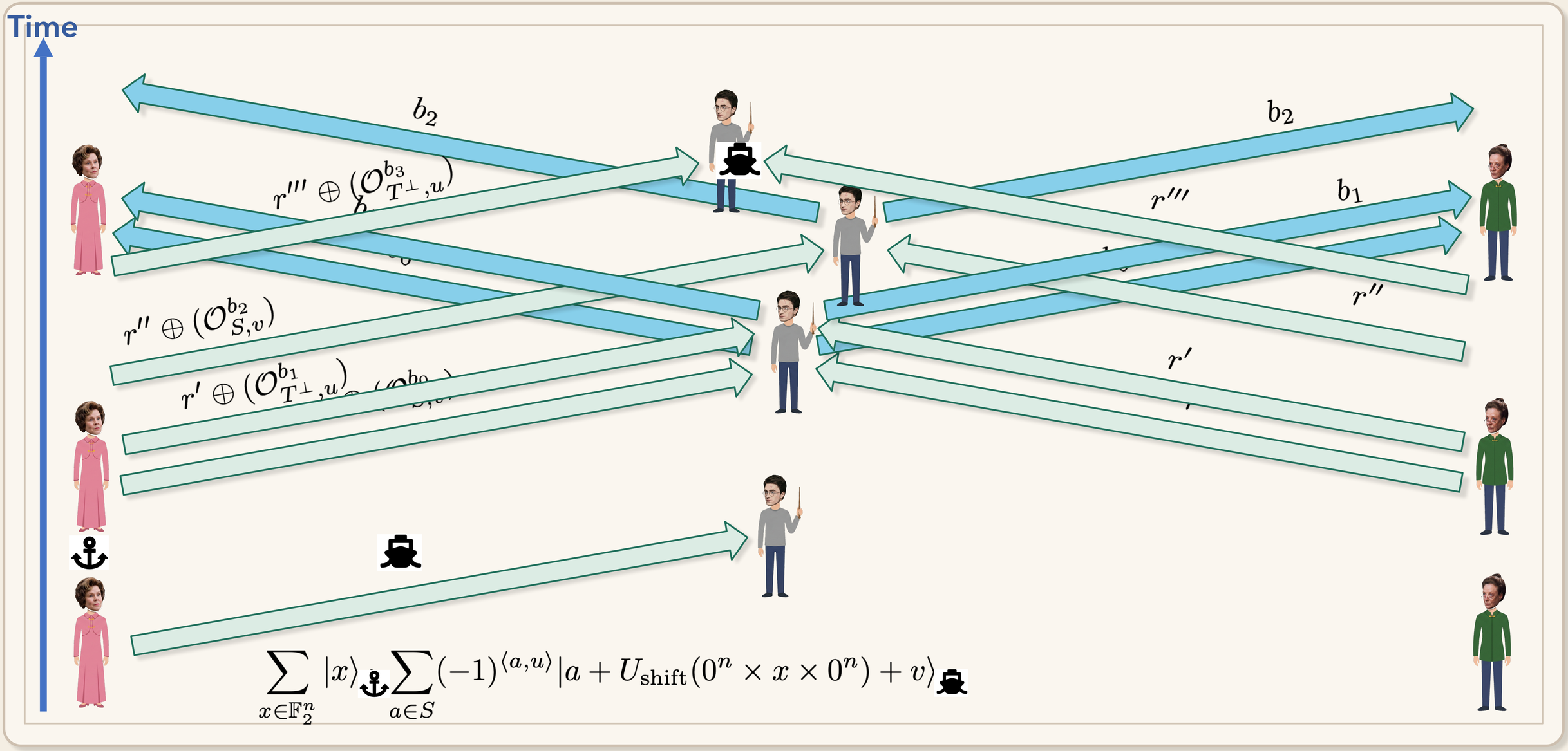
Protocol: Trajectory Verification



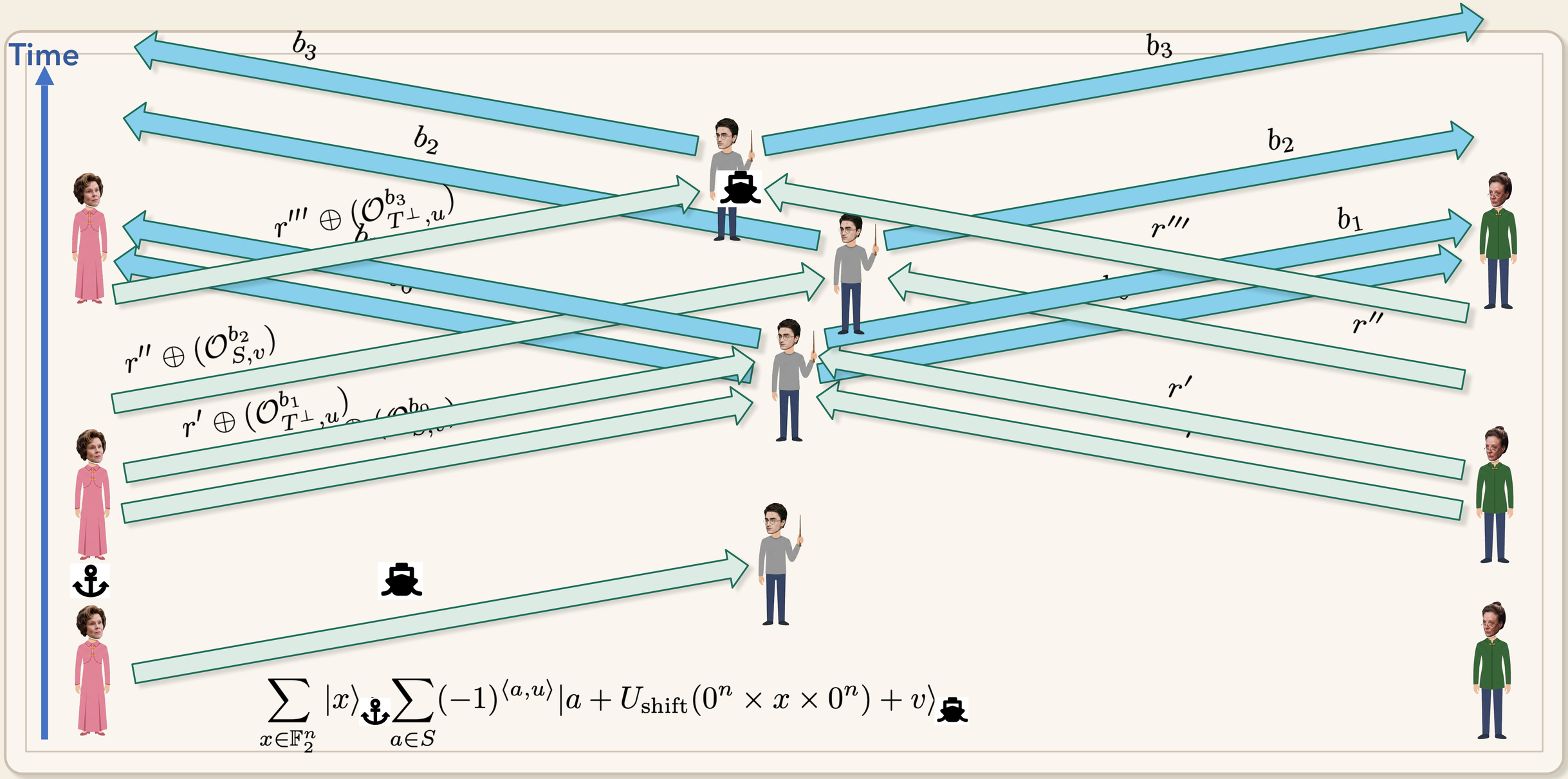
Protocol: Trajectory Verification



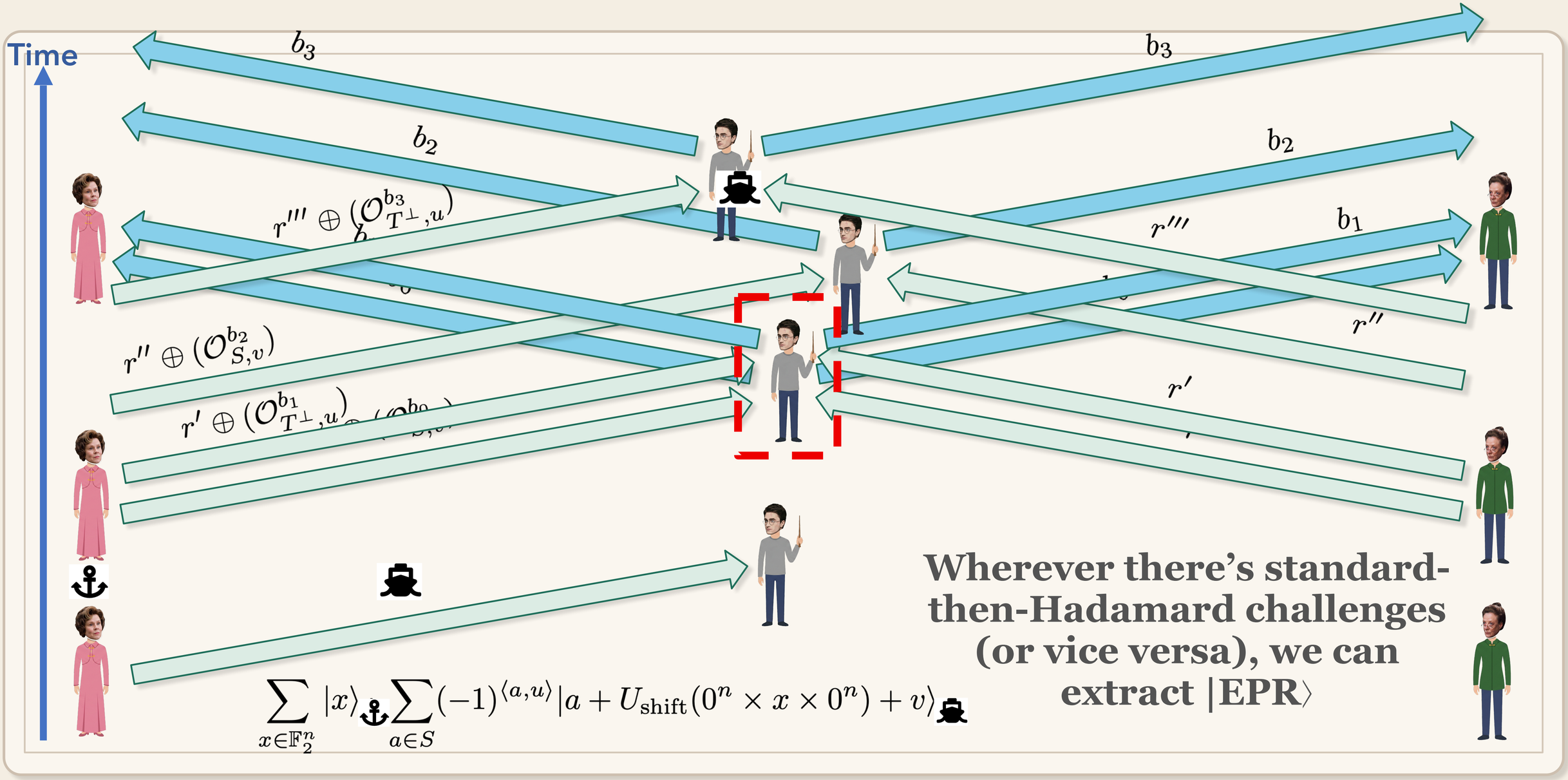
Protocol: Trajectory Verification



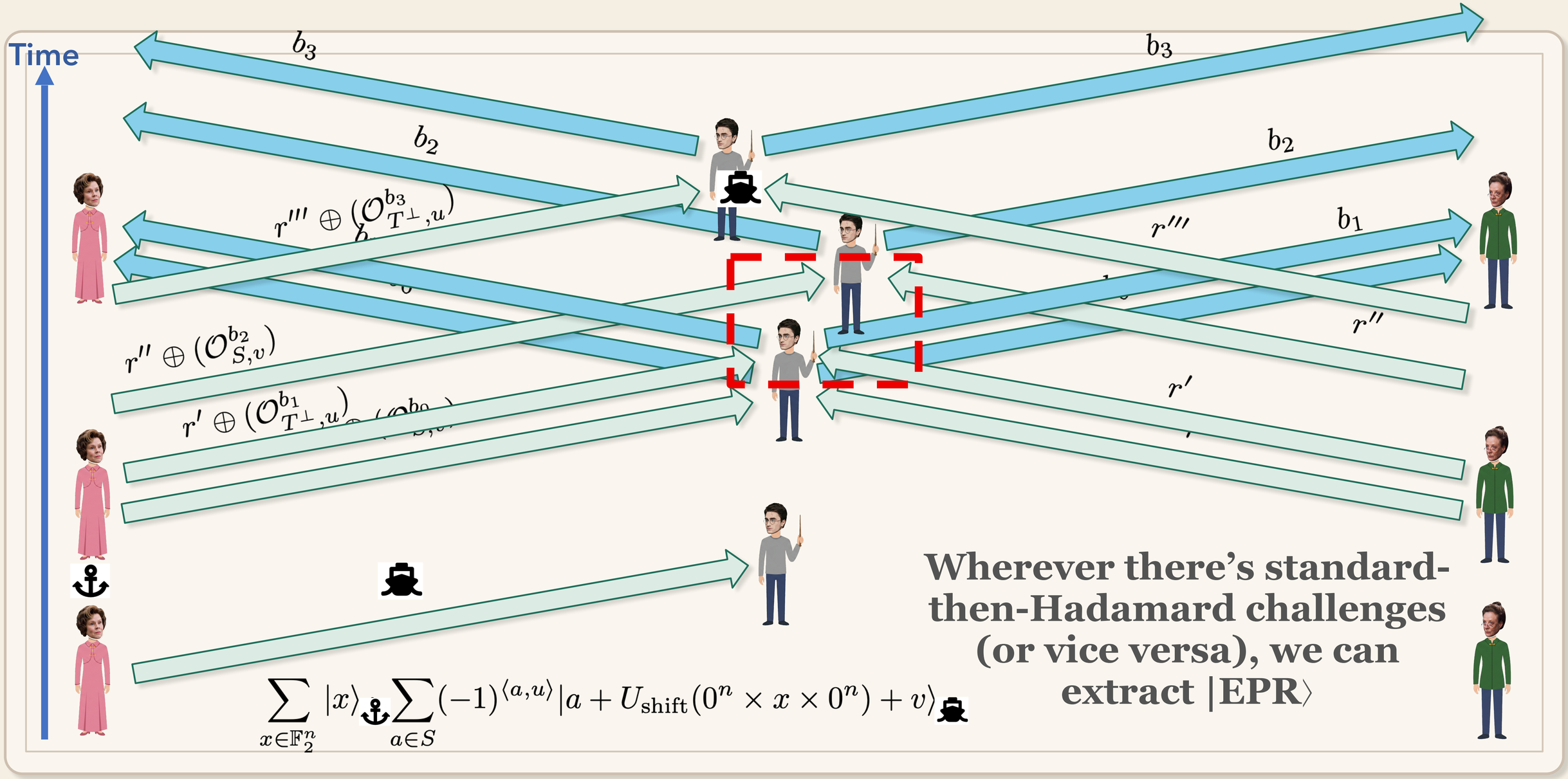
Protocol: Trajectory Verification



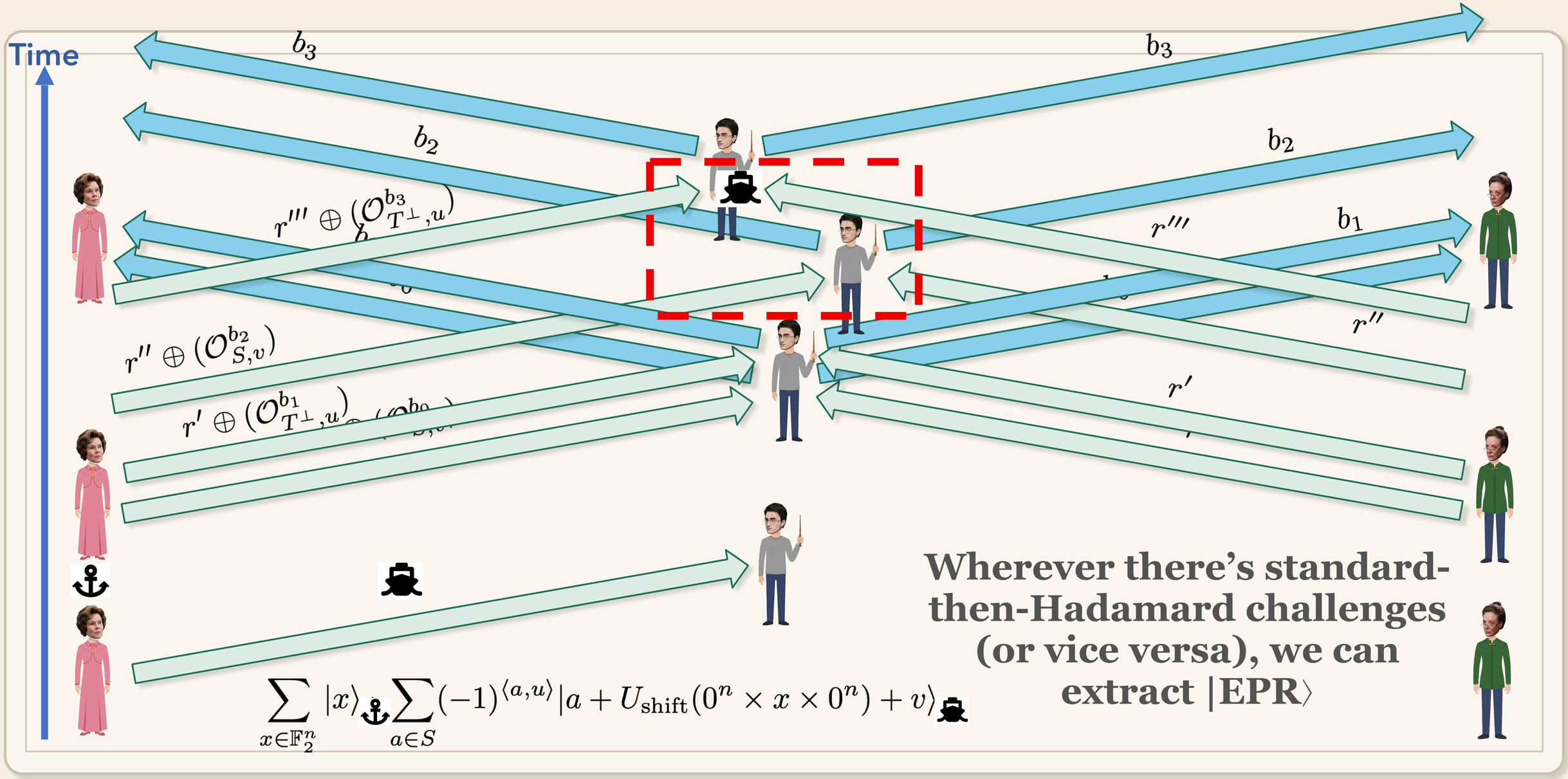
Protocol: Trajectory Verification



Protocol: Trajectory Verification

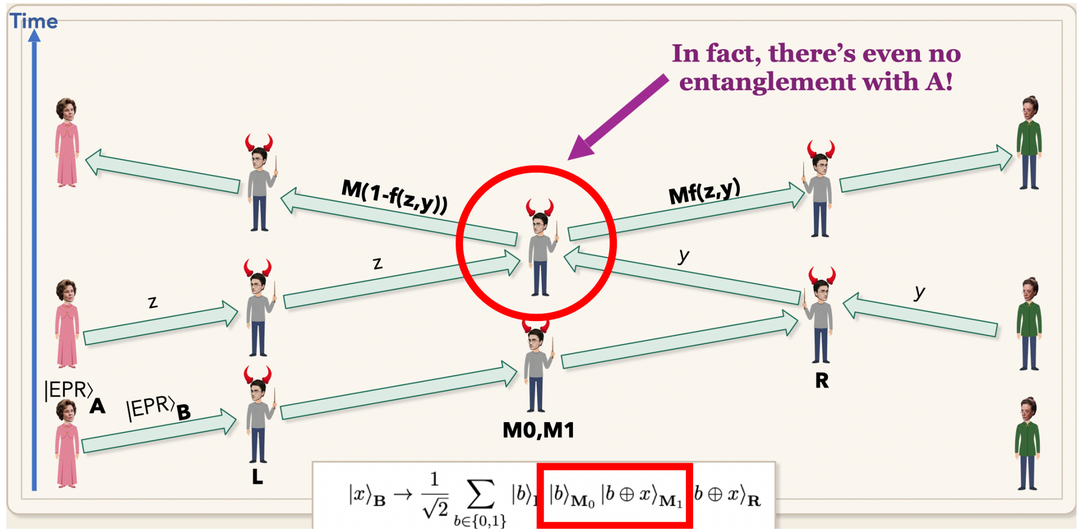


Protocol: Trajectory Verification



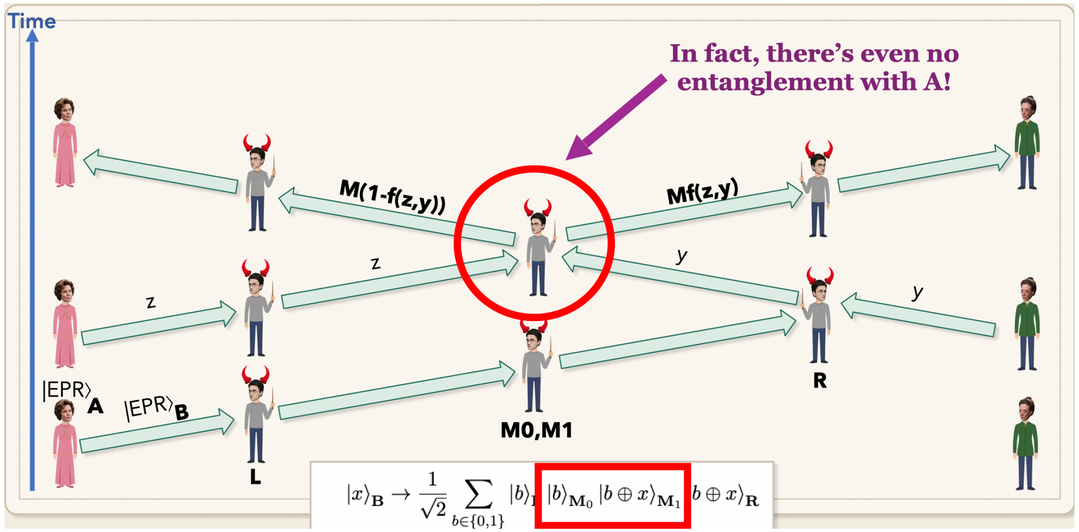
Towards a Stronger Position-Based Authentication

Towards a Stronger Position-Based Authentication



When position-based authentication is built from f-BB84, there is a non-local strategy which succeeds.

Towards a Stronger Position-Based Authentication



When position-based authentication is built from f-BB84, there is a non-local strategy which succeeds.

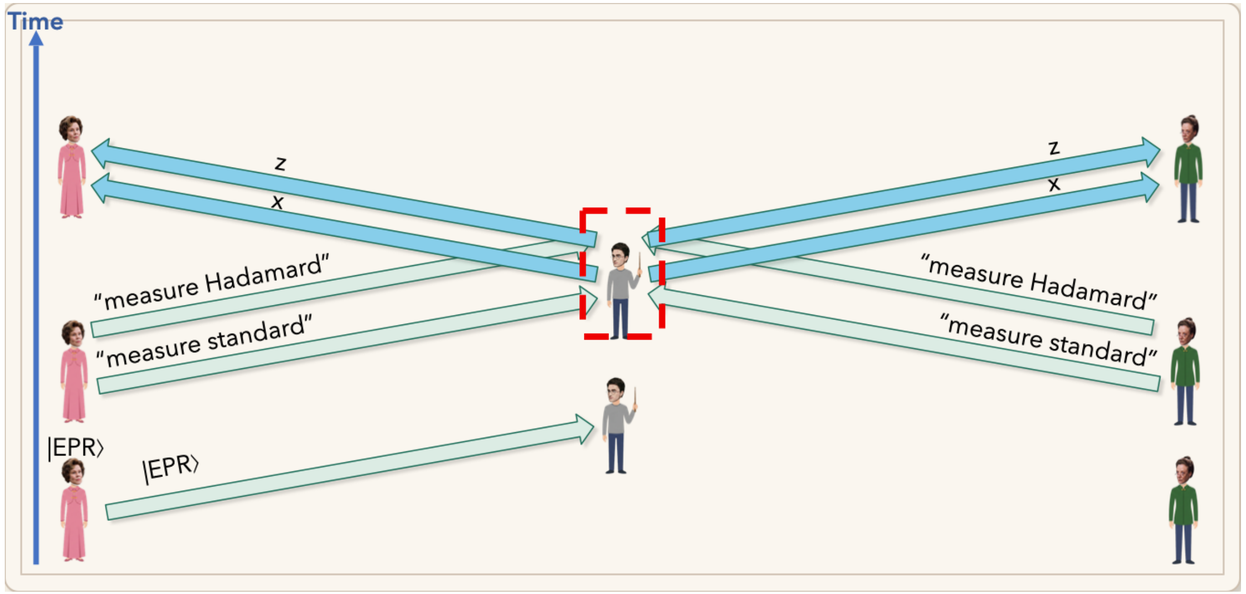
Can this be patched with localization?

Towards a Stronger Position-Based Authentication

Functionality Localization

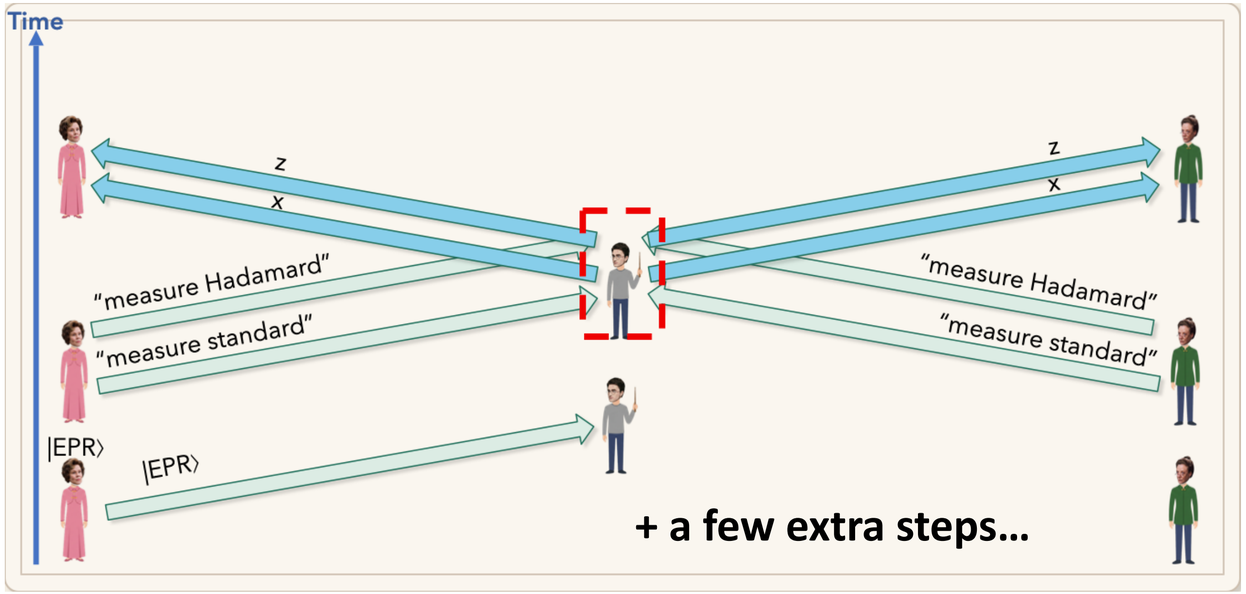
Towards a Stronger Position-Based Authentication

Functionality Localization



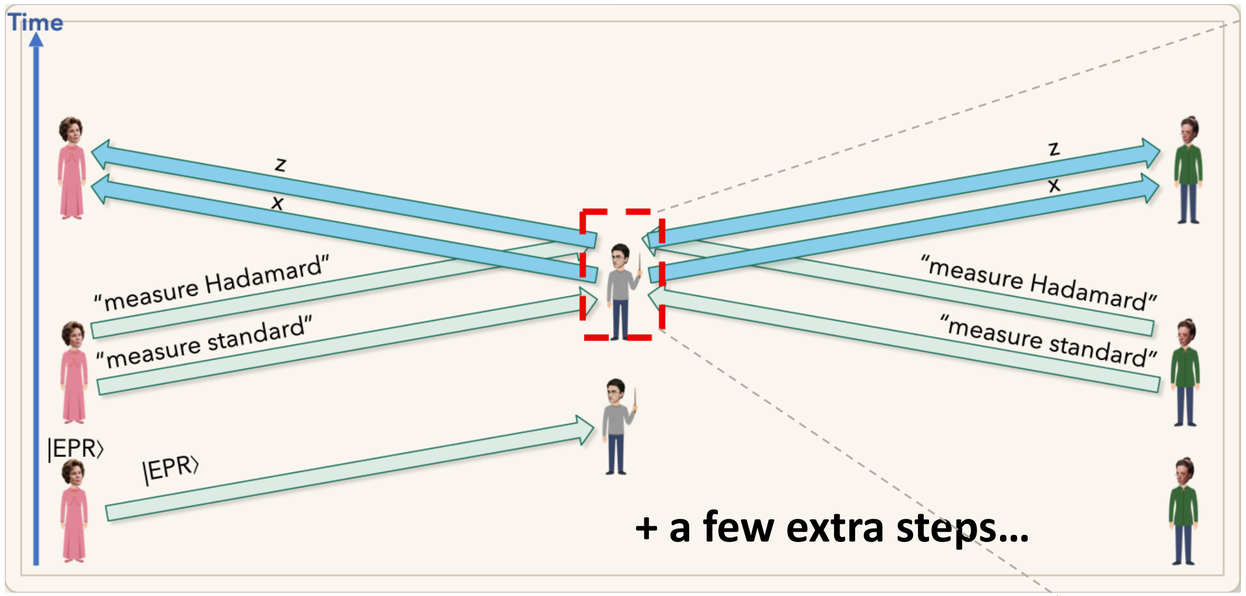
Towards a Stronger Position-Based Authentication

Functionality Localization



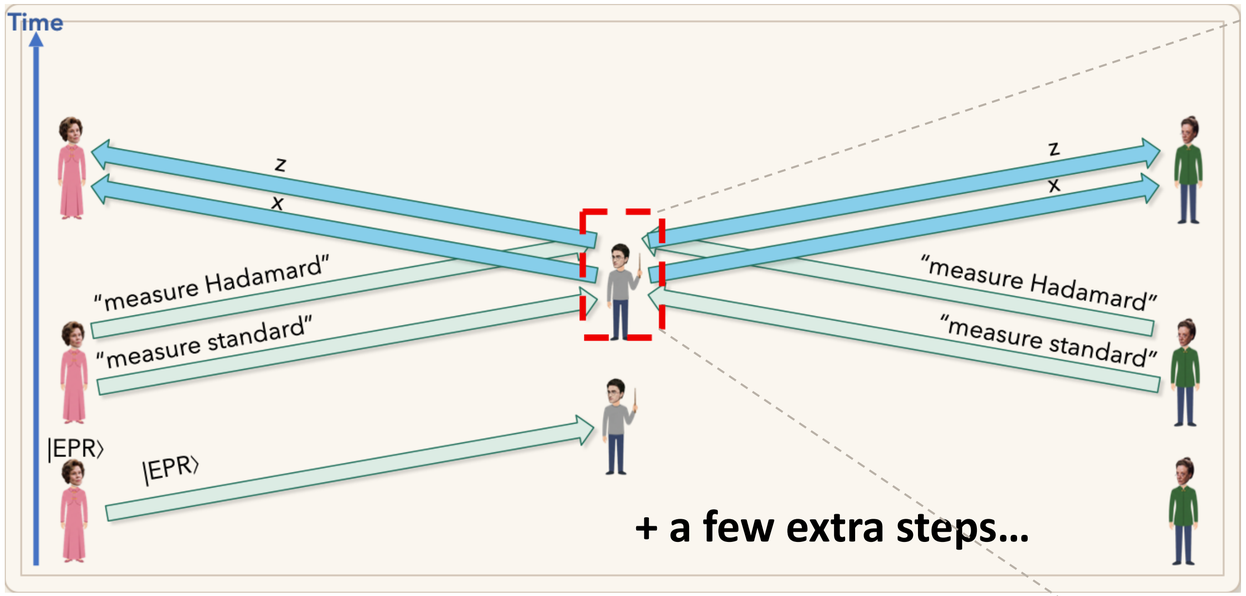
Towards a Stronger Position-Based Authentication

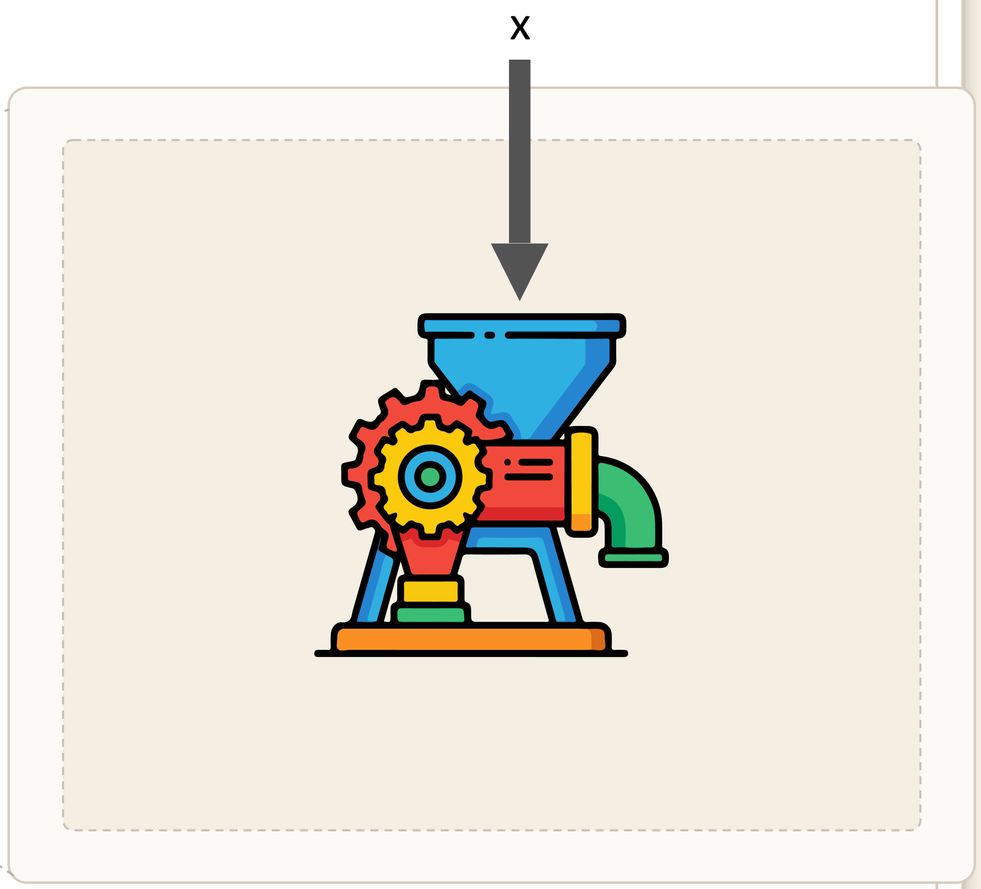
Functionality Localization



Towards a Stronger Position-Based Authentication

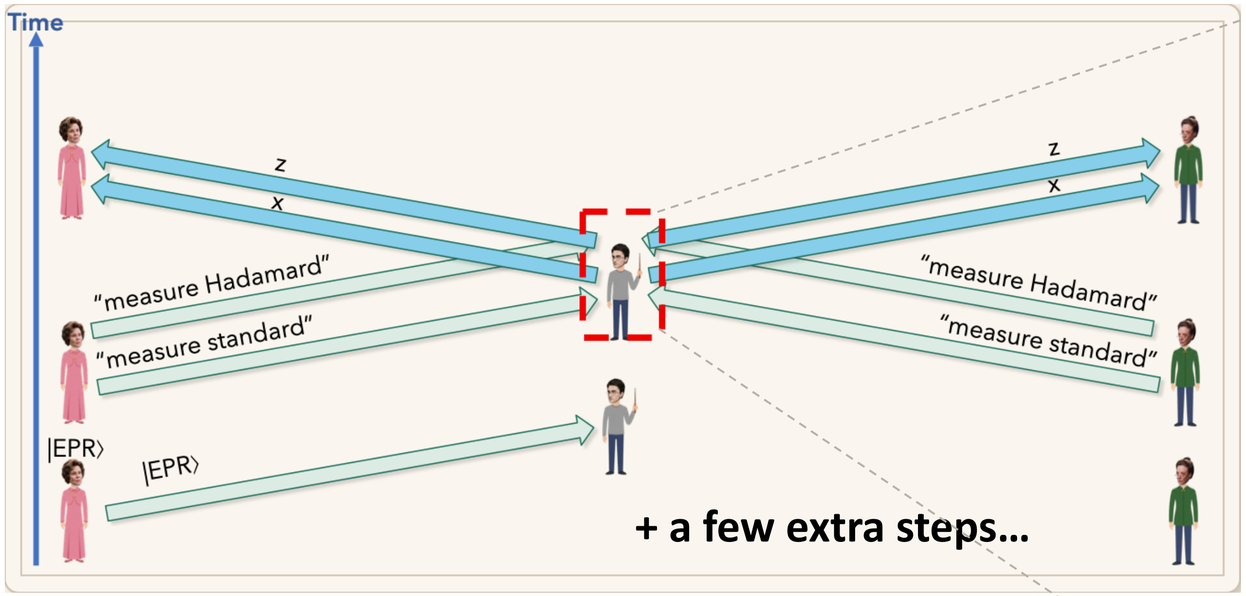
Functionality Localization

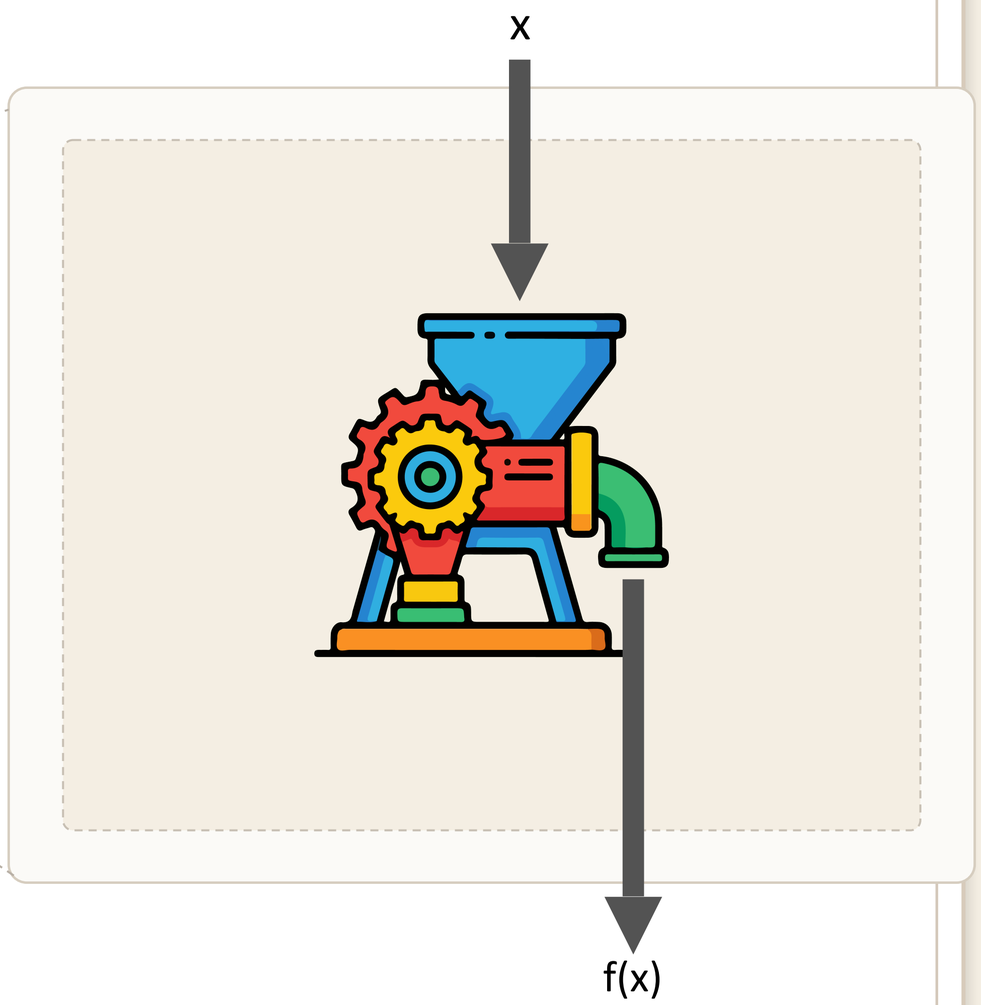




Towards a Stronger Position-Based Authentication

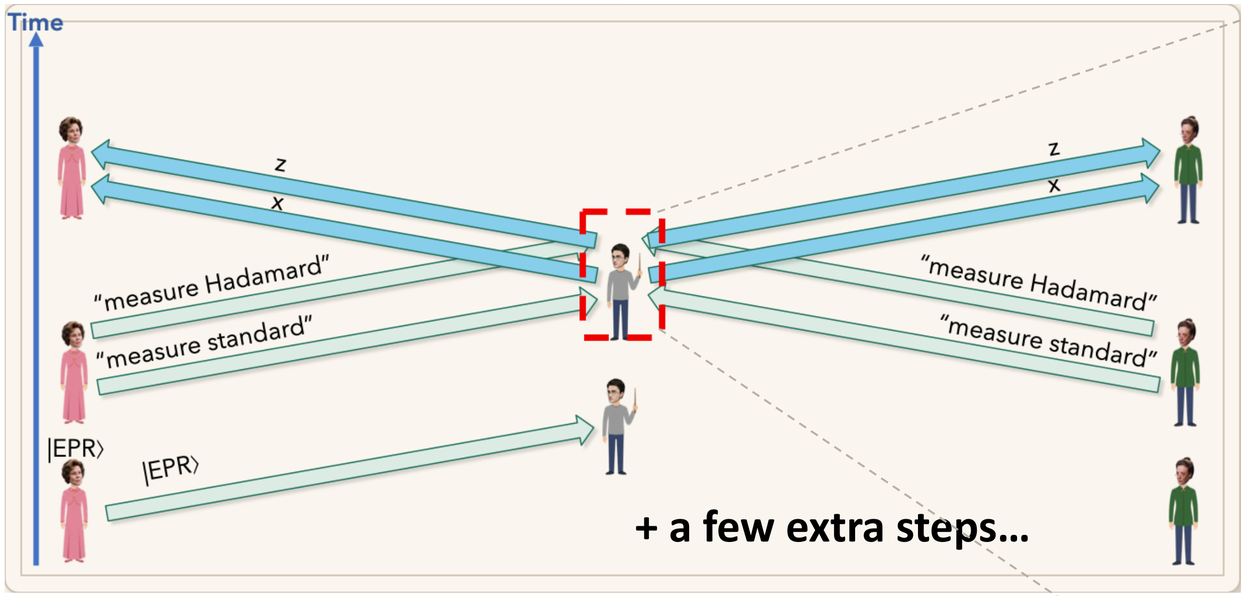
Functionality Localization

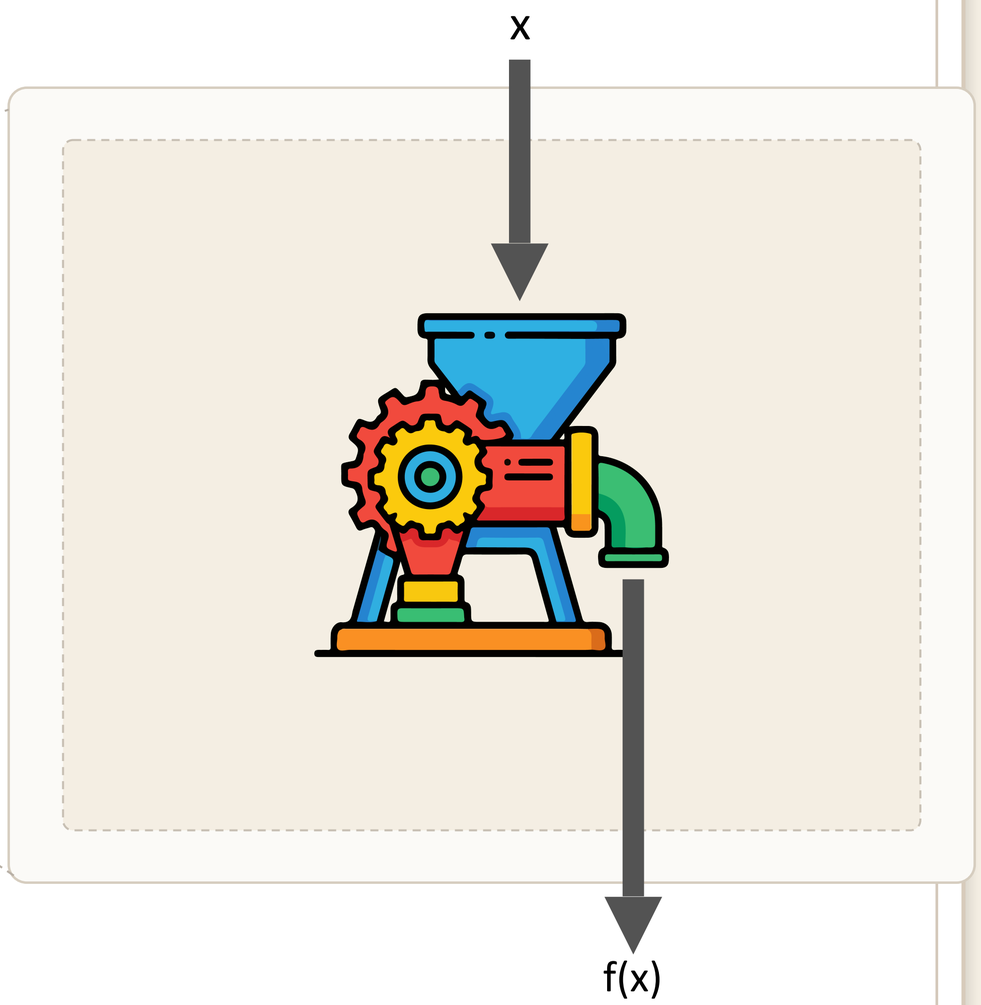




Towards a Stronger Position-Based Authentication

Functionality Localization

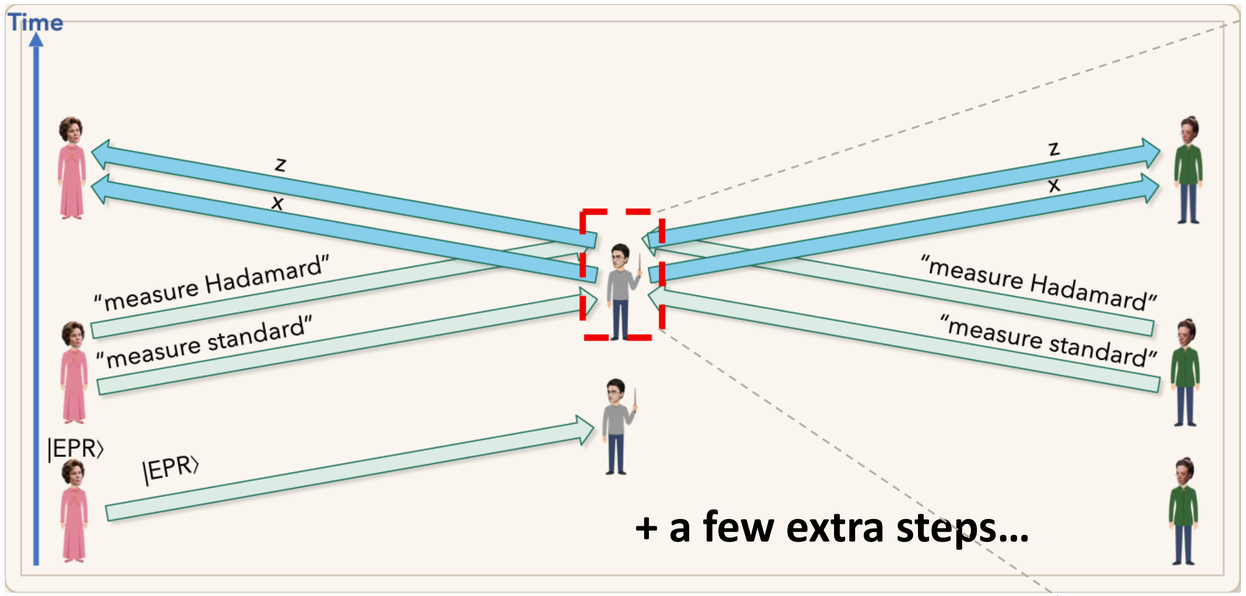


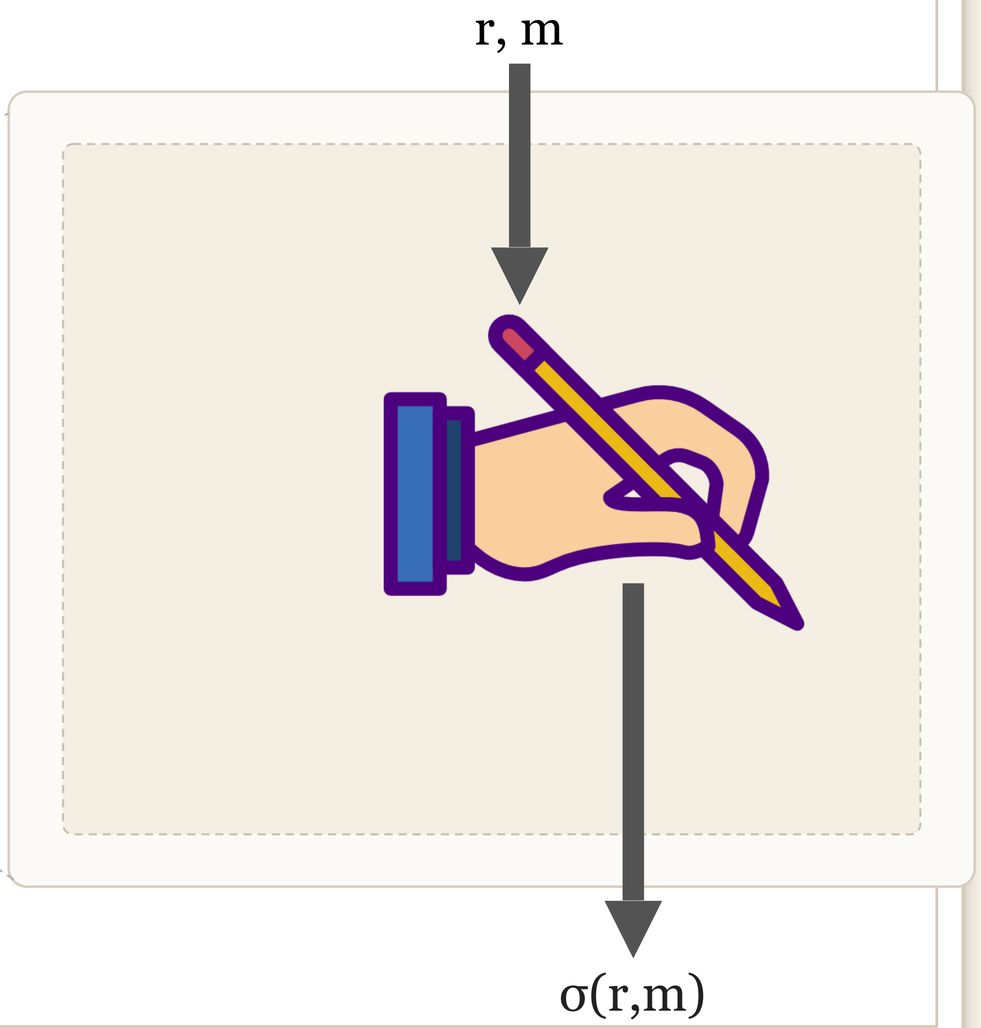


Can localize a function-like state.
If it's copy protected, we localize the *whole functionality*…

Towards a Stronger Position-Based Authentication

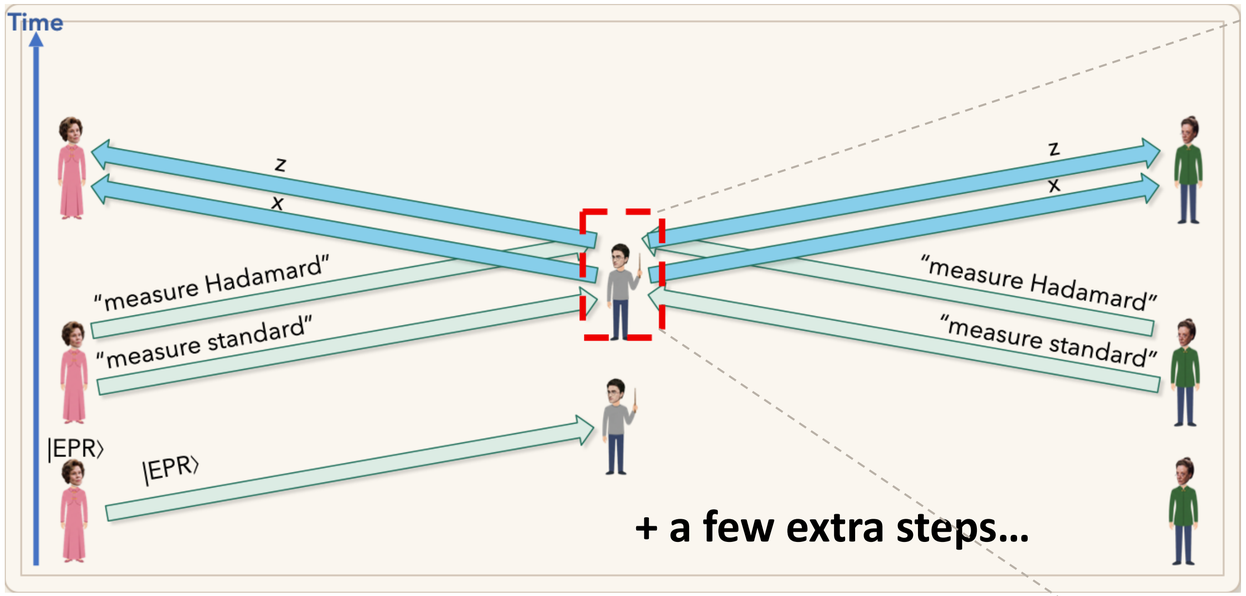
Functionality Localization



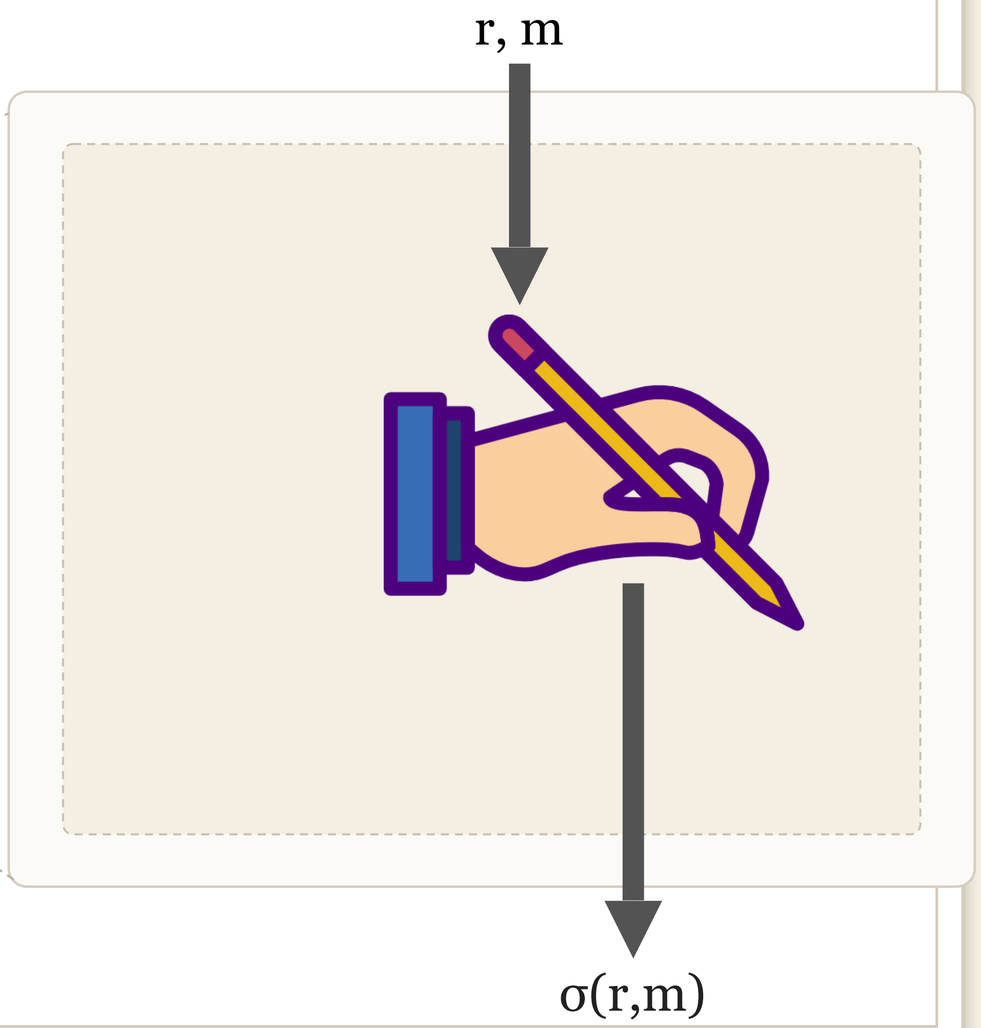


Towards a Stronger Position-Based Authentication

Functionality Localization

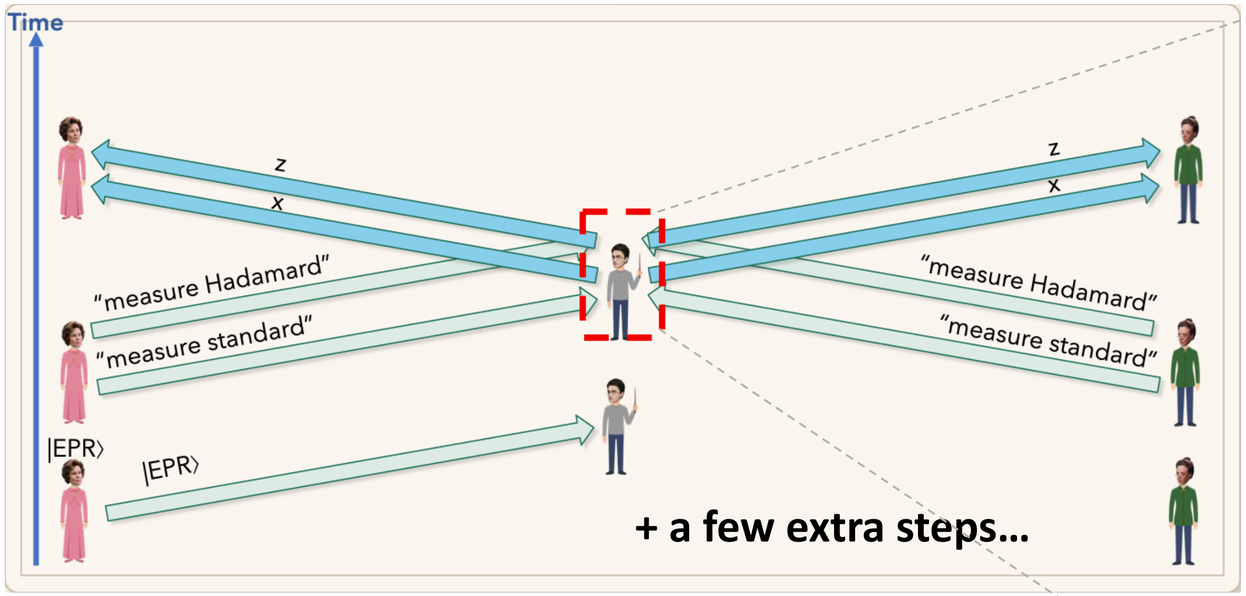


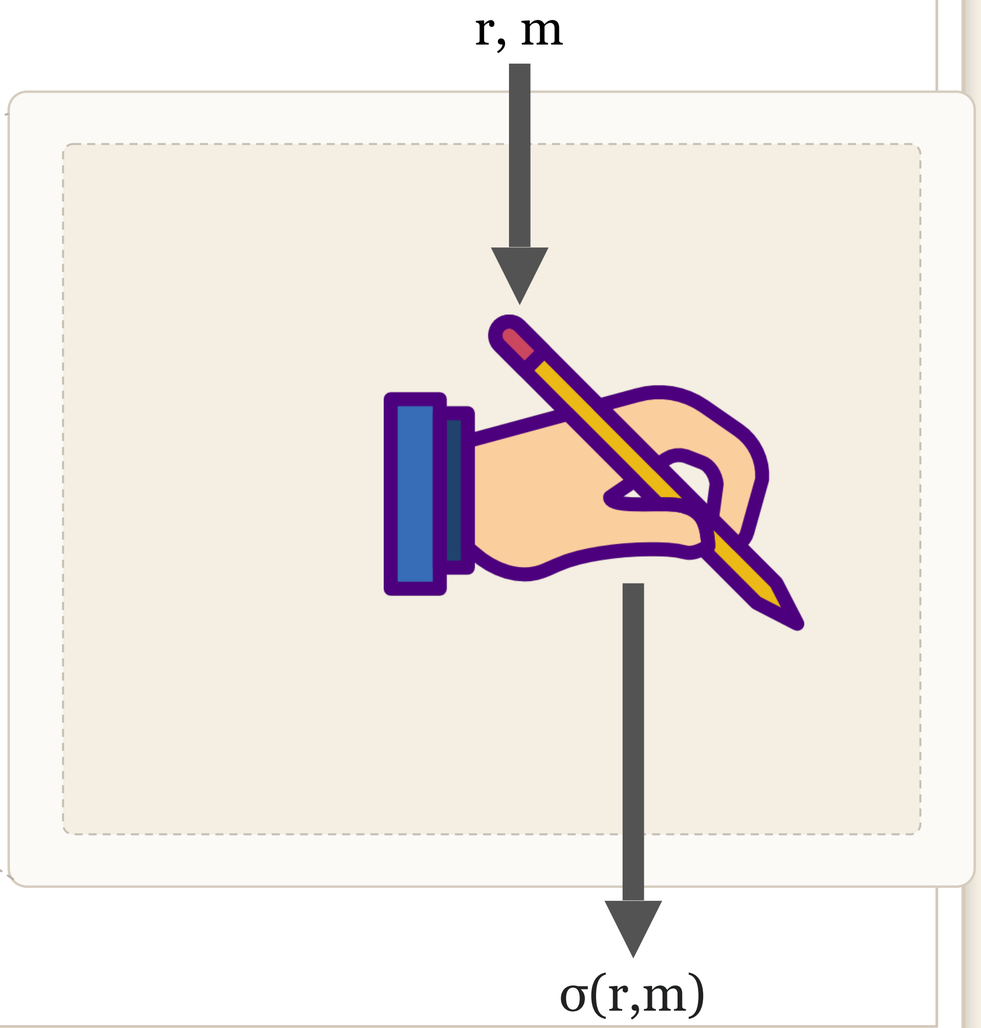
1. **Copy-protect a digital signature functionality into an unclonable state $|\Psi\rangle$**



Towards a Stronger Position-Based Authentication

Functionality Localization

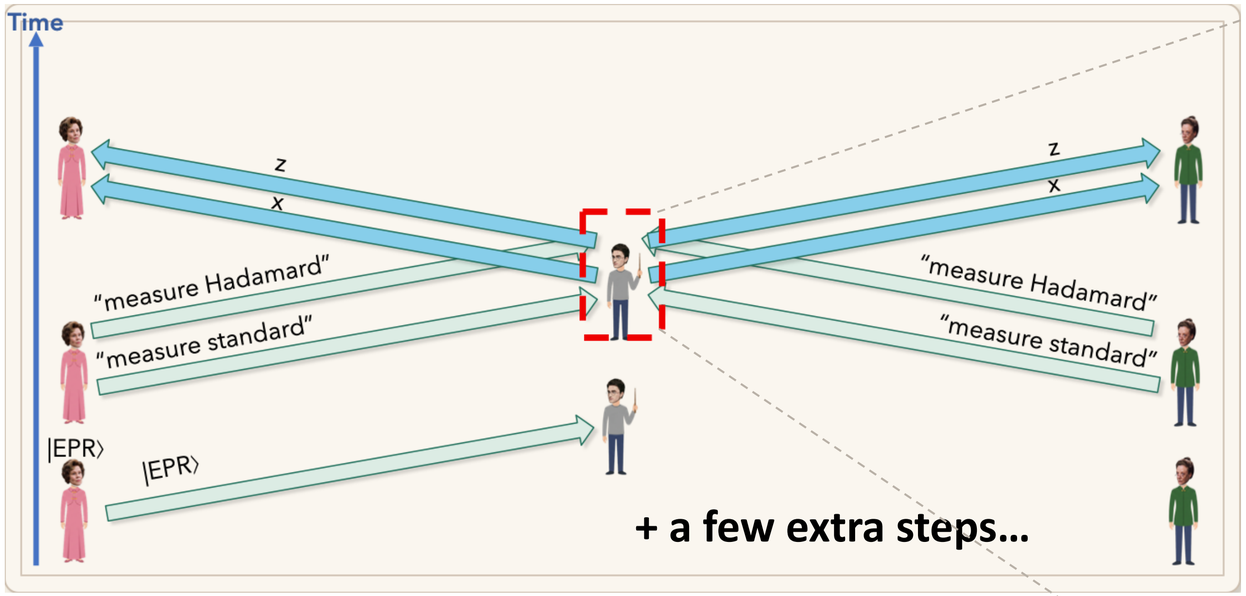


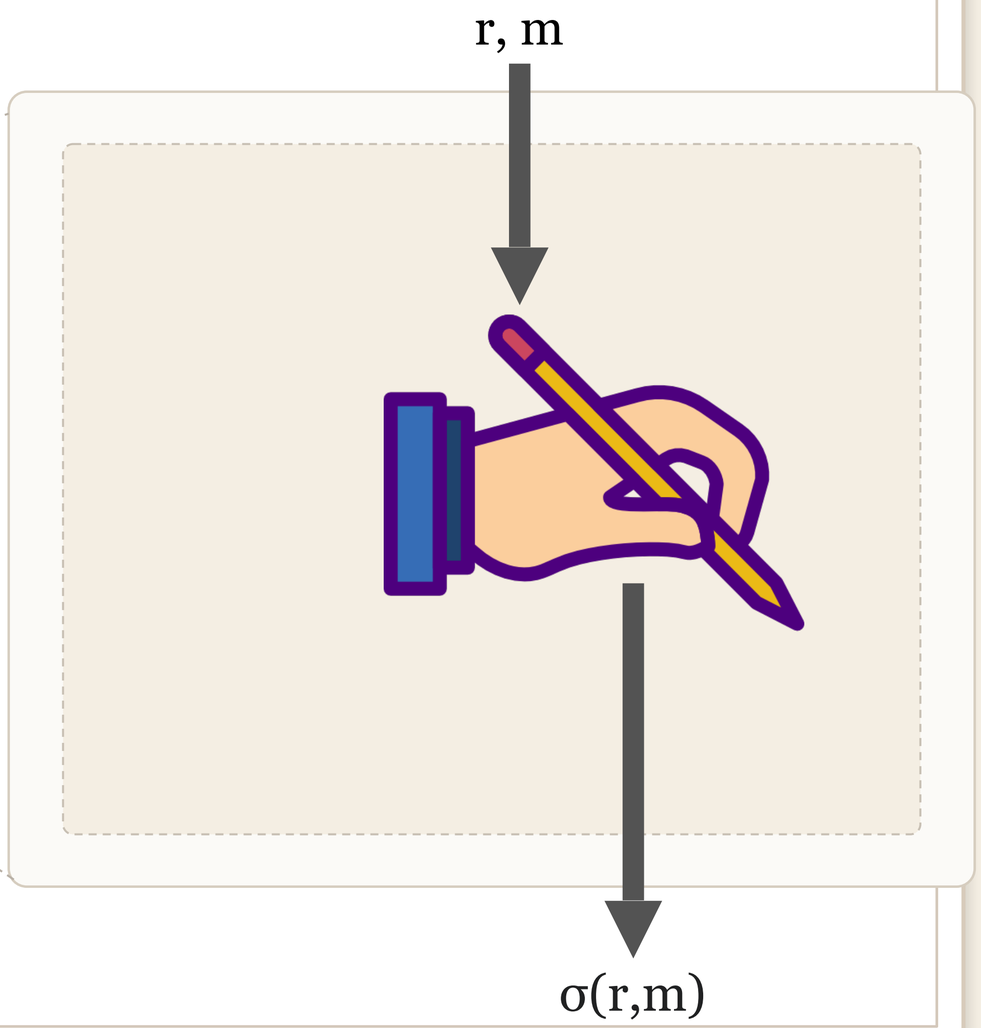


1. **Copy-protect a digital signature functionality into an unclonable state $|\Psi\rangle$**
2. **Request a signature on r,m where r is a random challenge**

Towards a Stronger Position-Based Authentication

Functionality Localization

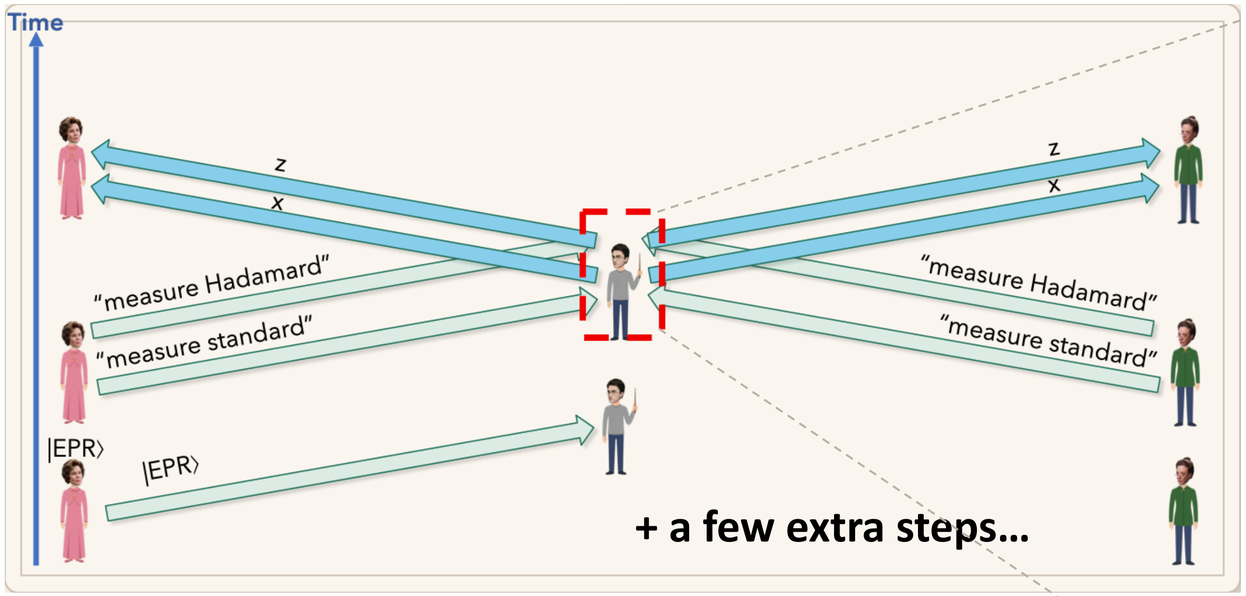




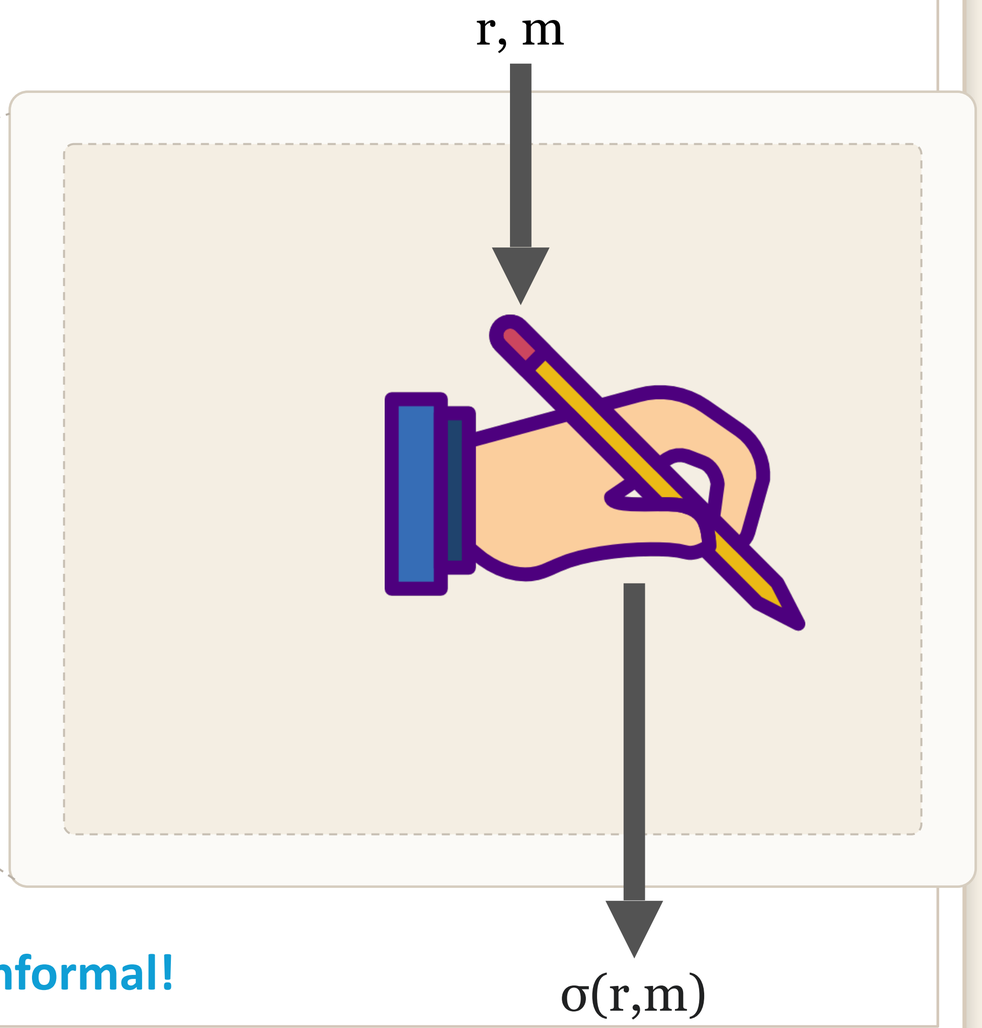
1. **Copy-protect a digital signature functionality into an unclonable state $|\Psi\rangle$**
2. **Request a signature on r,m where r is a random challenge**
3. **At the same time, localize $|\Psi\rangle$**

Towards a Stronger Position-Based Authentication

Functionality Localization



1. **Copy-protect a digital signature functionality into an unclonable state $|\Psi\rangle$**
2. **Request a signature on r,m where r is a random challenge**
3. **At the same time, localize $|\Psi\rangle$**



Informal!

Open Questions

Open Questions

Open Questions

1. **Removing Oracles:** Though even position verification (weaker than localization) is not known in the plain model, can we get anything nontrivial just from iO + OWF, perhaps in the bounded-entanglement model?

Open Questions

1. **Removing Oracles:** Though even position verification (weaker than localization) is not known in the plain model, can we get anything nontrivial just from iO + OWF, perhaps in the bounded-entanglement model?

Open Questions

1. **Removing Oracles:** Though even position verification (weaker than localization) is not known in the plain model, can we get anything nontrivial just from iO + OWF, perhaps in the bounded-entanglement model?

2. **Privacy:** Previously, zero-knowledge position verification was considered ([GGGM**O**Y'26]). What about zero-knowledge trajectory verification?

Open Questions

1. **Removing Oracles:** Though even position verification (weaker than localization) is not known in the plain model, can we get anything nontrivial just from iO + OWF, perhaps in the bounded-entanglement model?

2. **Privacy:** Previously, zero-knowledge position verification was considered ([GGGM**O**Y'26]). What about zero-knowledge trajectory verification?

Open Questions

1. **Removing Oracles:** Though even position verification (weaker than localization) is not known in the plain model, can we get anything nontrivial just from iO + OWF, perhaps in the bounded-entanglement model?

2. **Privacy:** Previously, zero-knowledge position verification was considered ([GGGM**O**Y'26]). What about zero-knowledge trajectory verification?

3. **Classical Communication:** [LLQ'21] showed a quantum position verification protocol which only requires classical communication. Are there localization protocols with this property?

Open Questions

1. **Removing Oracles:** Though even position verification (weaker than localization) is not known in the plain model, can we get anything nontrivial just from iO + OWF, perhaps in the bounded-entanglement model?

2. **Privacy:** Previously, zero-knowledge position verification was considered ([GGGM**O**Y'26]). What about zero-knowledge trajectory verification?

3. **Classical Communication:** [LLQ'21] showed a quantum position verification protocol which only requires classical communication. Are there localization protocols with this property?

Open Questions

1. **Removing Oracles:** Though even position verification (weaker than localization) is not known in the plain model, can we get anything nontrivial just from iO + OWF, perhaps in the bounded-entanglement model?

2. **Privacy:** Previously, zero-knowledge position verification was considered ([GGGM**O**Y'26]). What about zero-knowledge trajectory verification?

3. **Classical Communication:** [LLQ'21] showed a quantum position verification protocol which only requires classical communication. Are there localization protocols with this property?

And more (read our paper! There are lots of pretty pictures 😊)

Thank you!