QCRYPT 2023

Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers

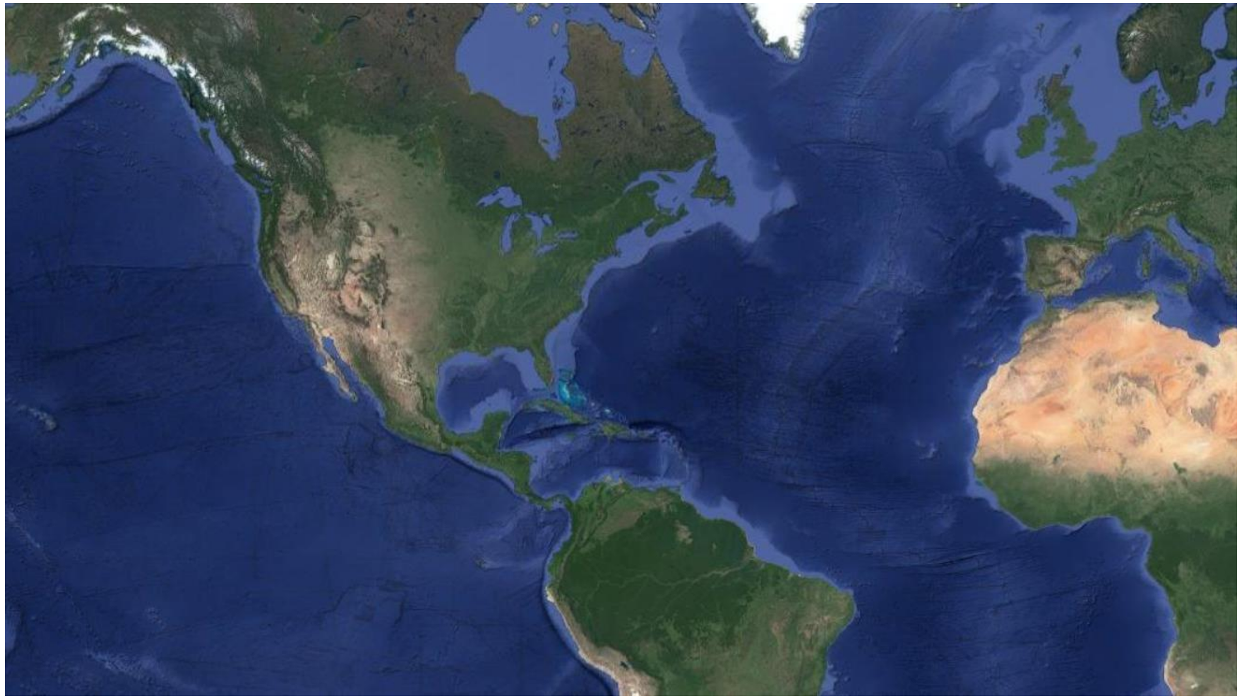
Llorenç Escolà Farràs, and Florian Speelman

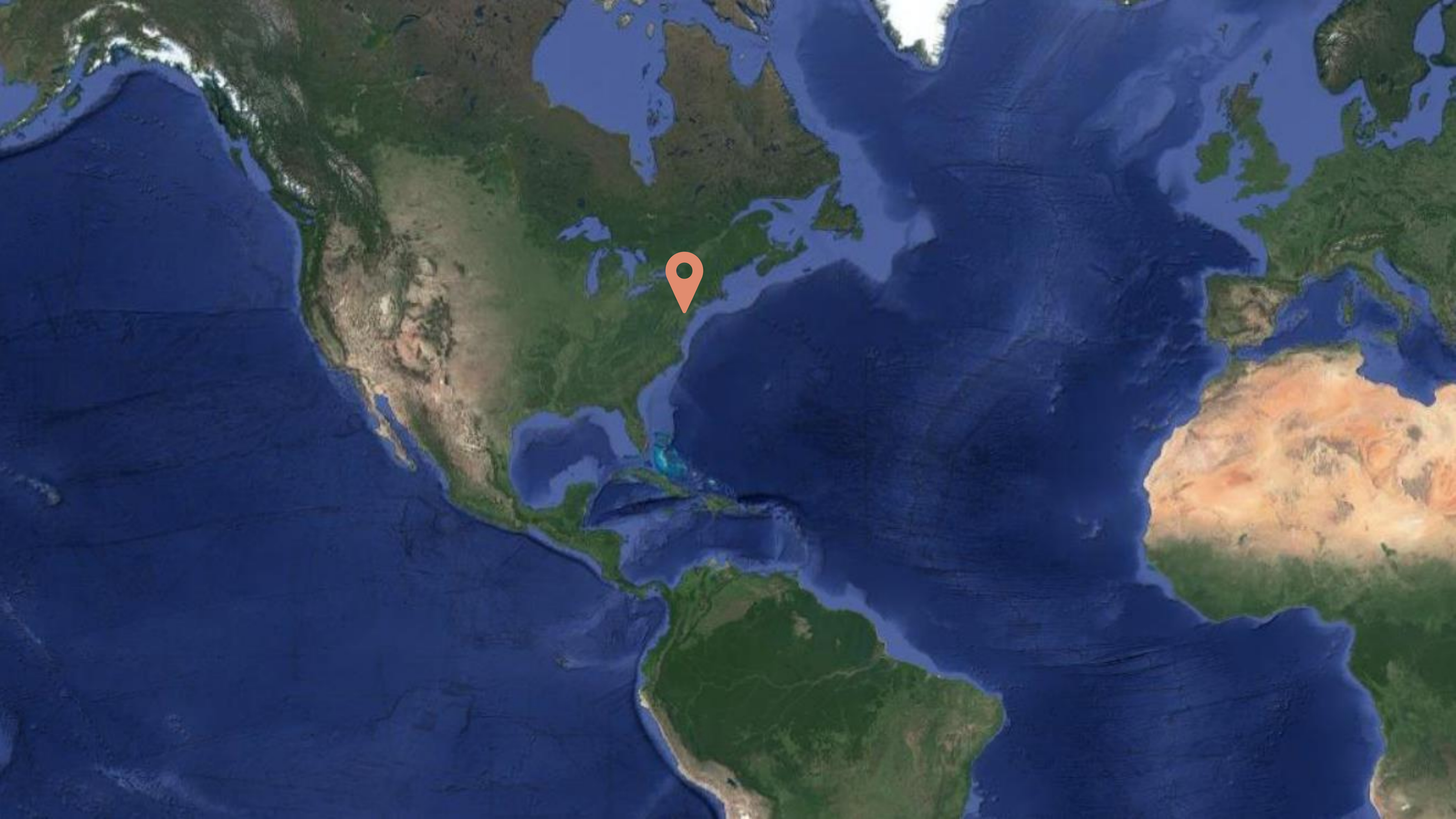
l.escolafarras@uva.nl

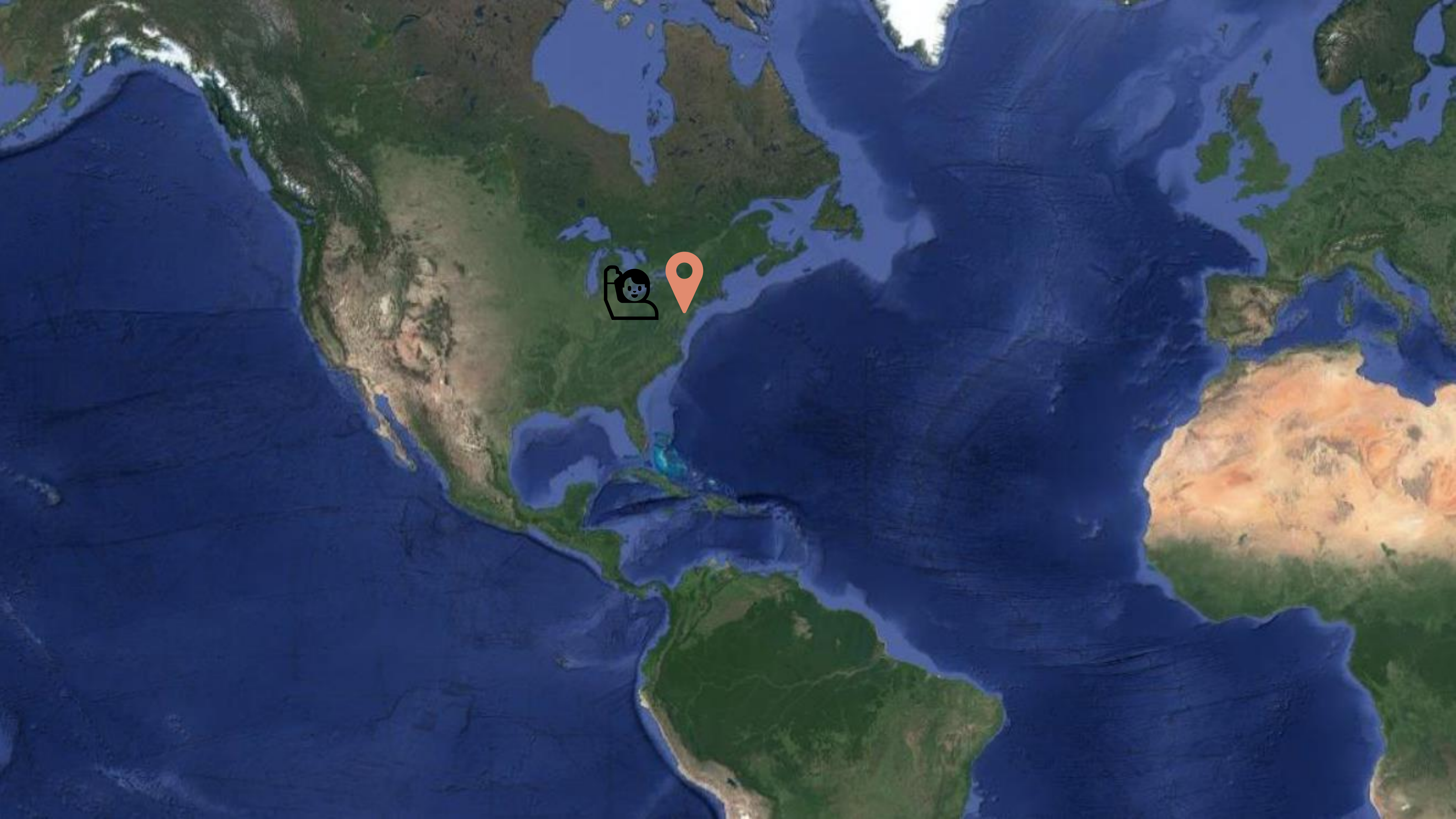
QuSoft Research Center for Quantum Software

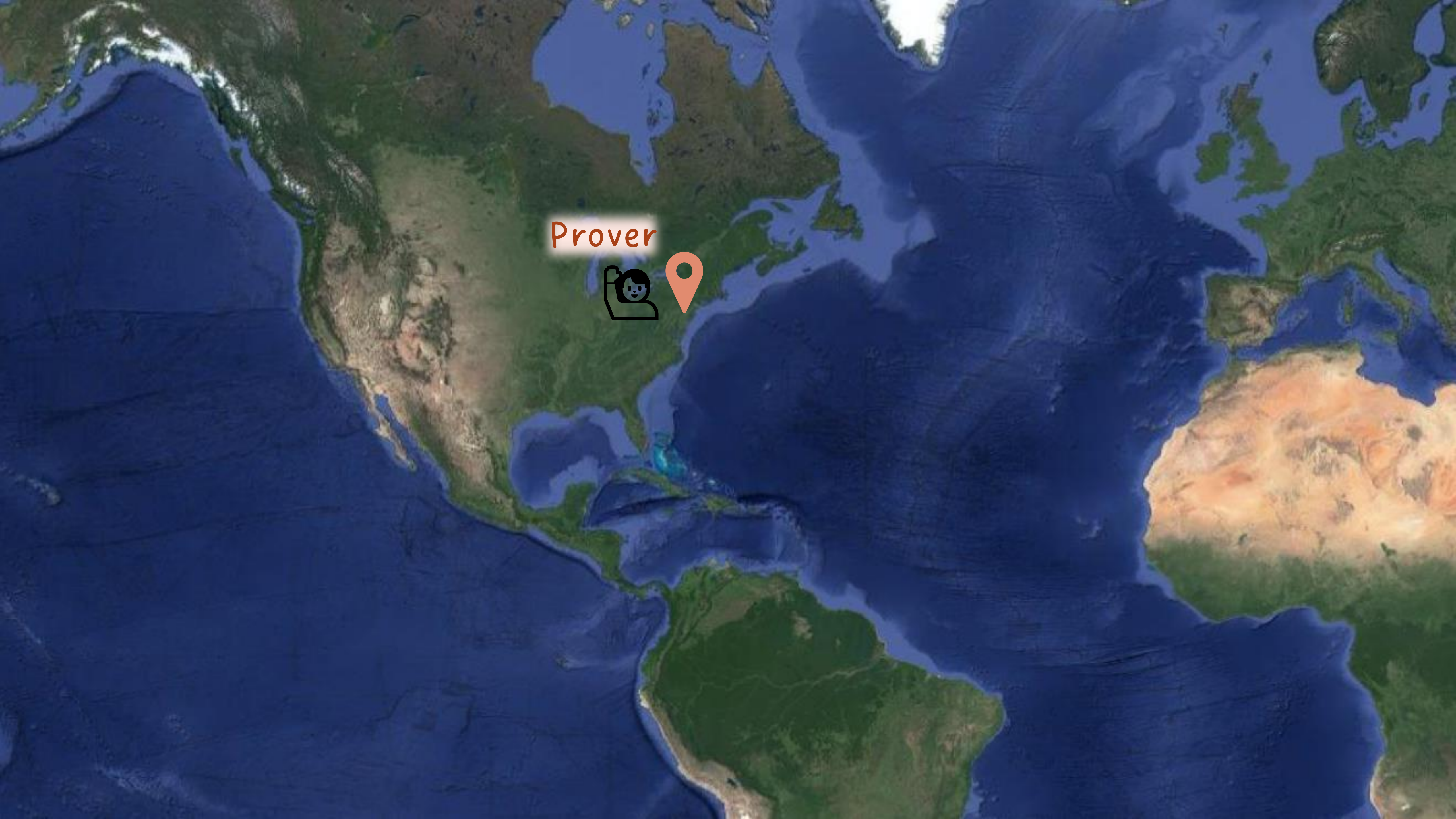
Universiteit van Amsterdam

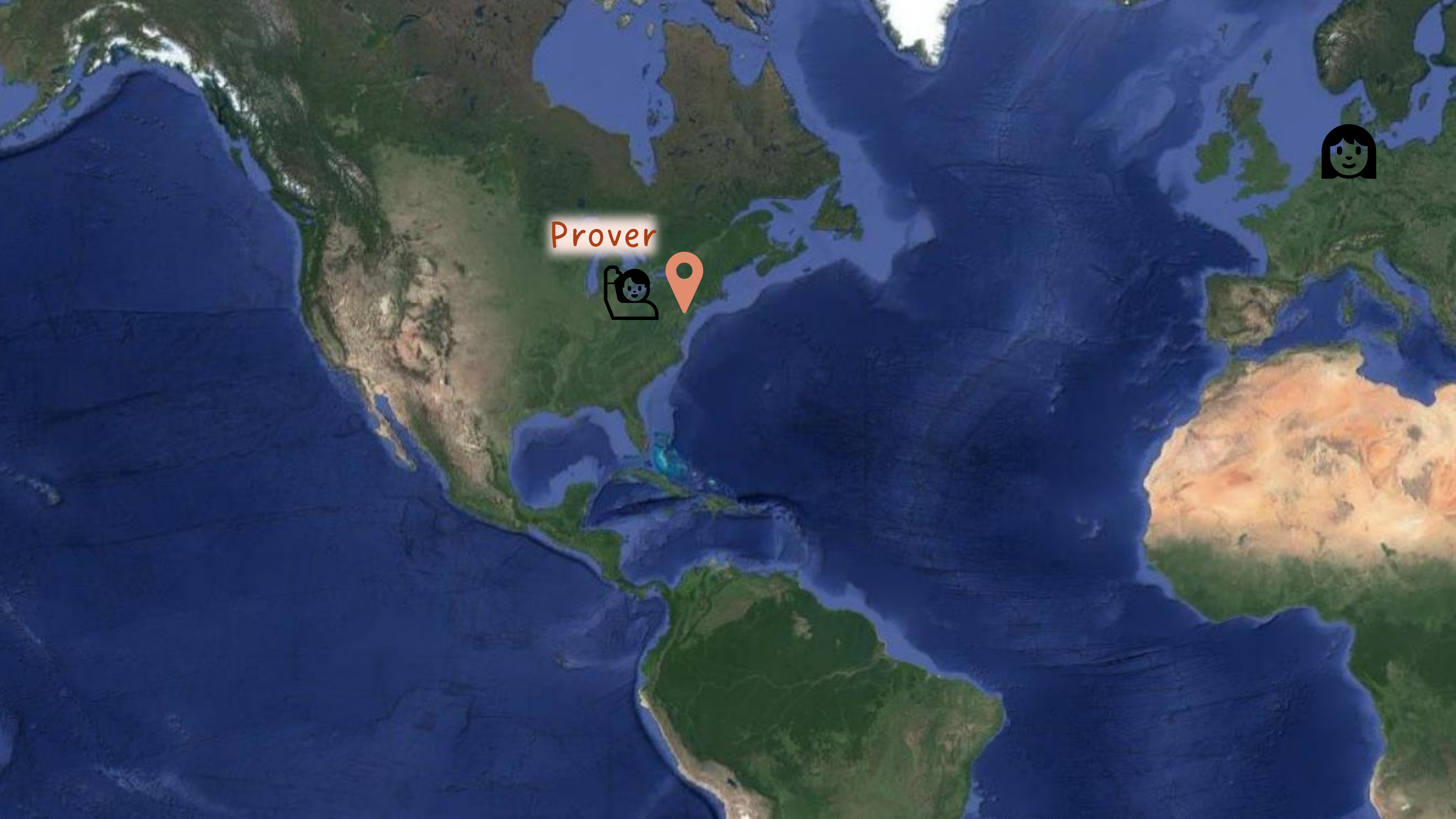
What is Position Verification?

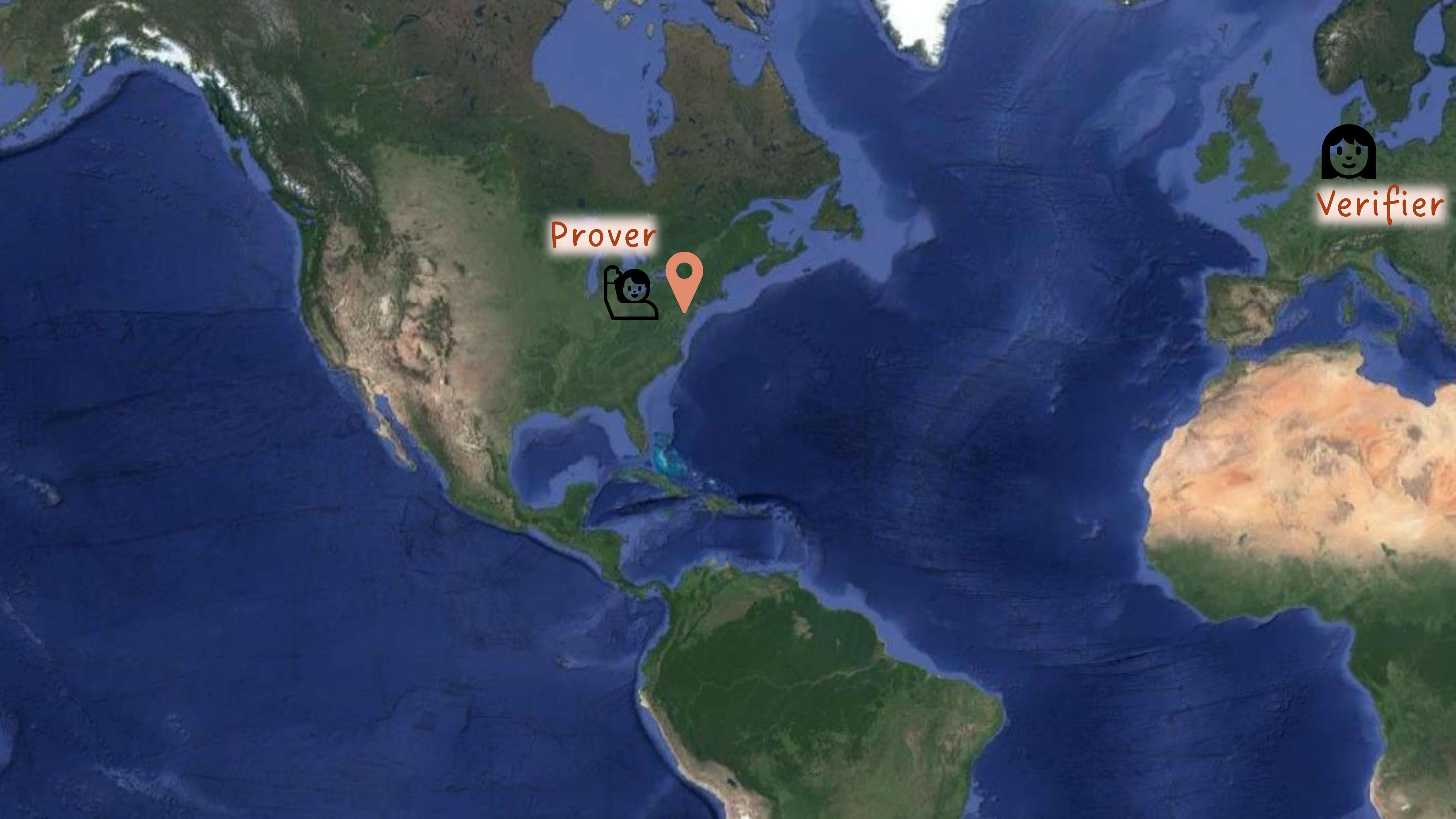


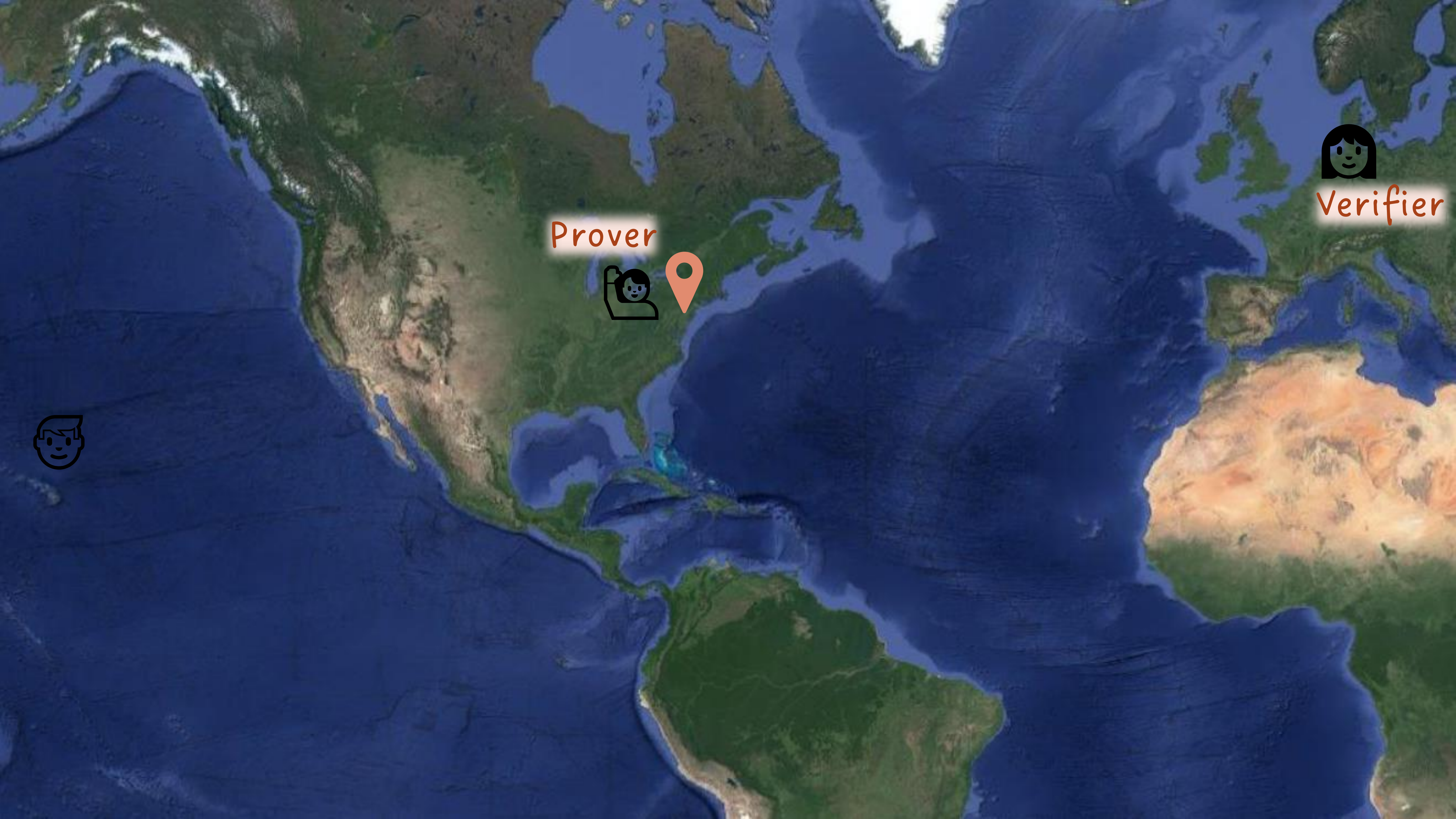


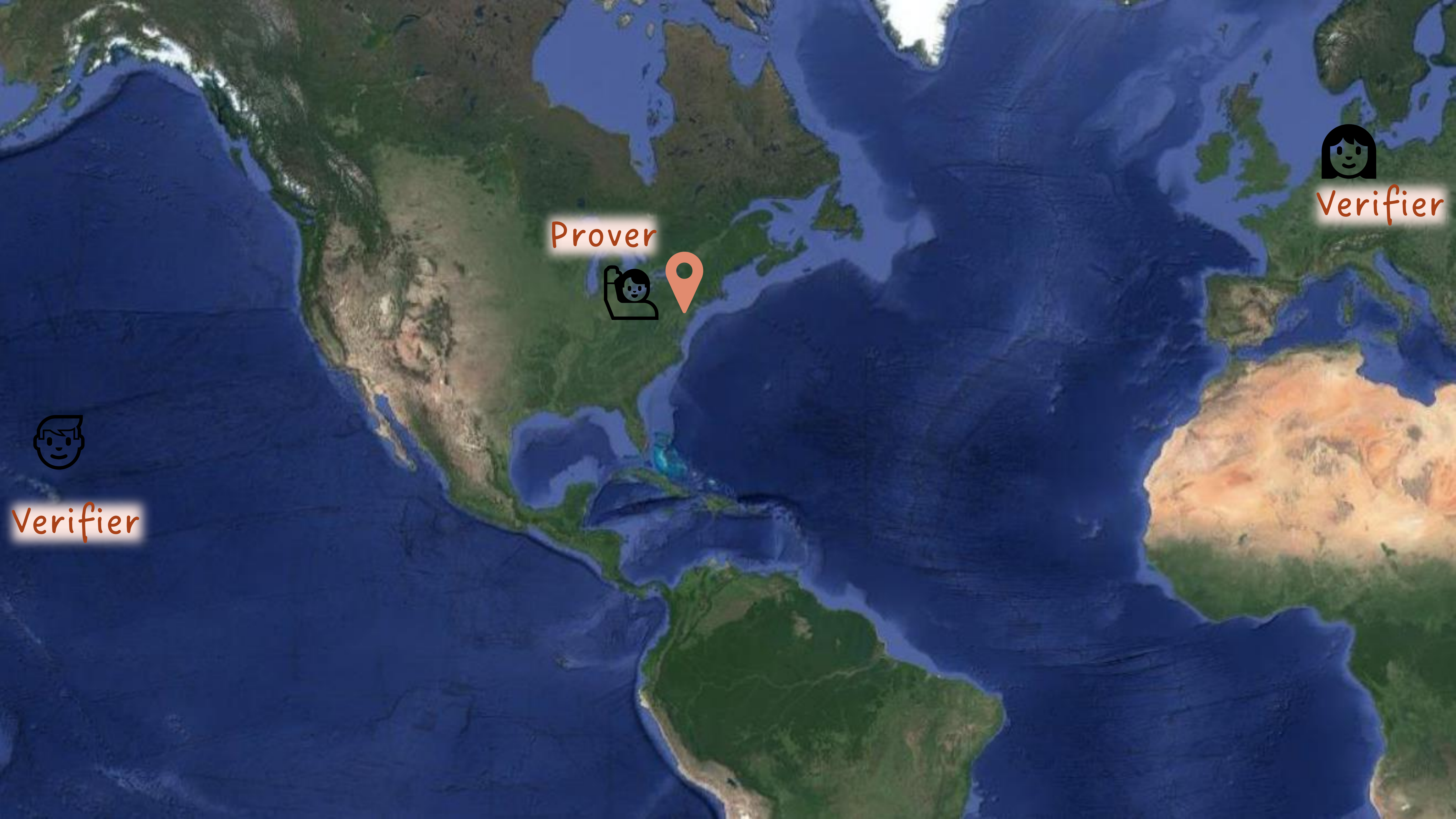


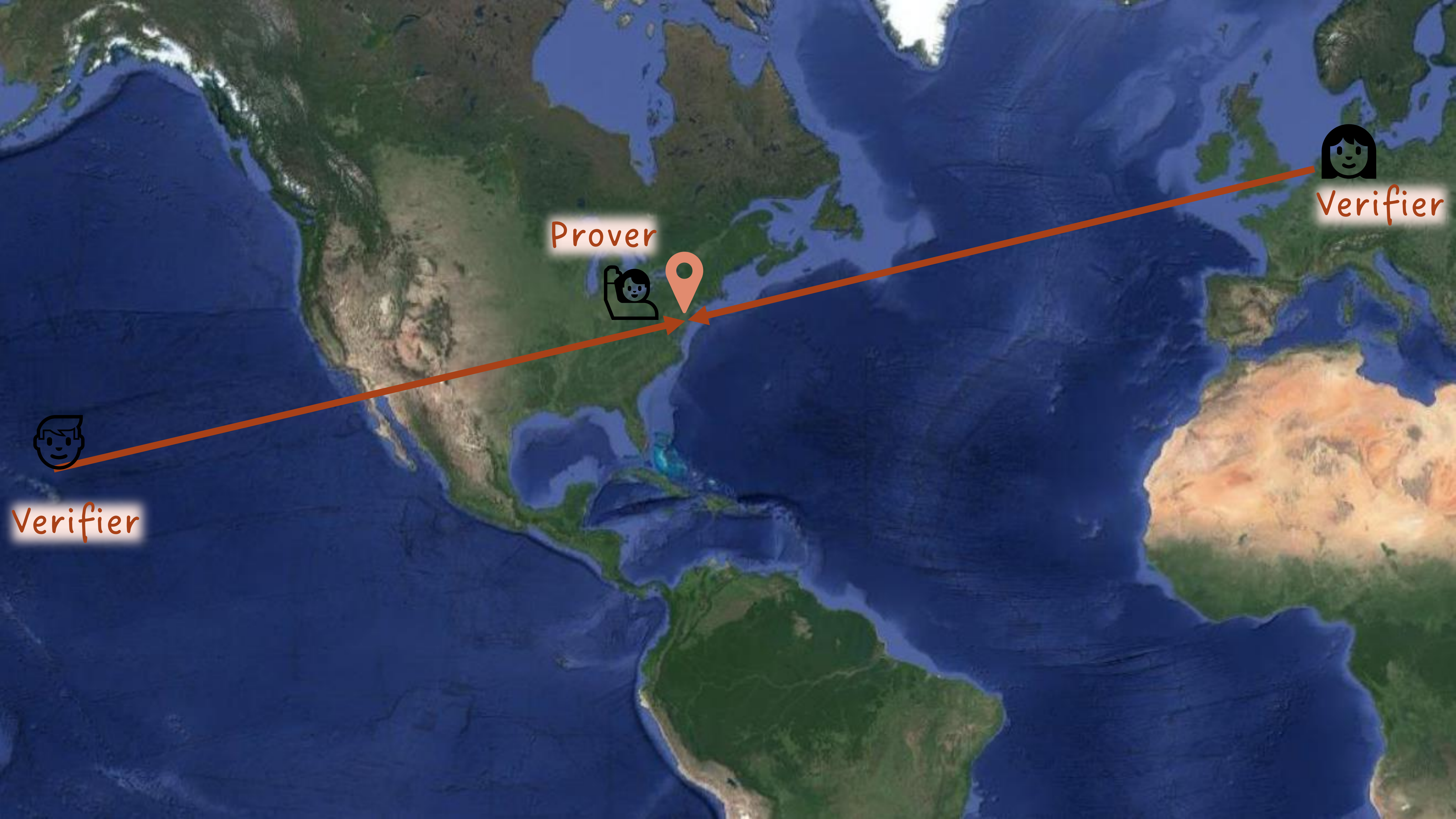

Prover

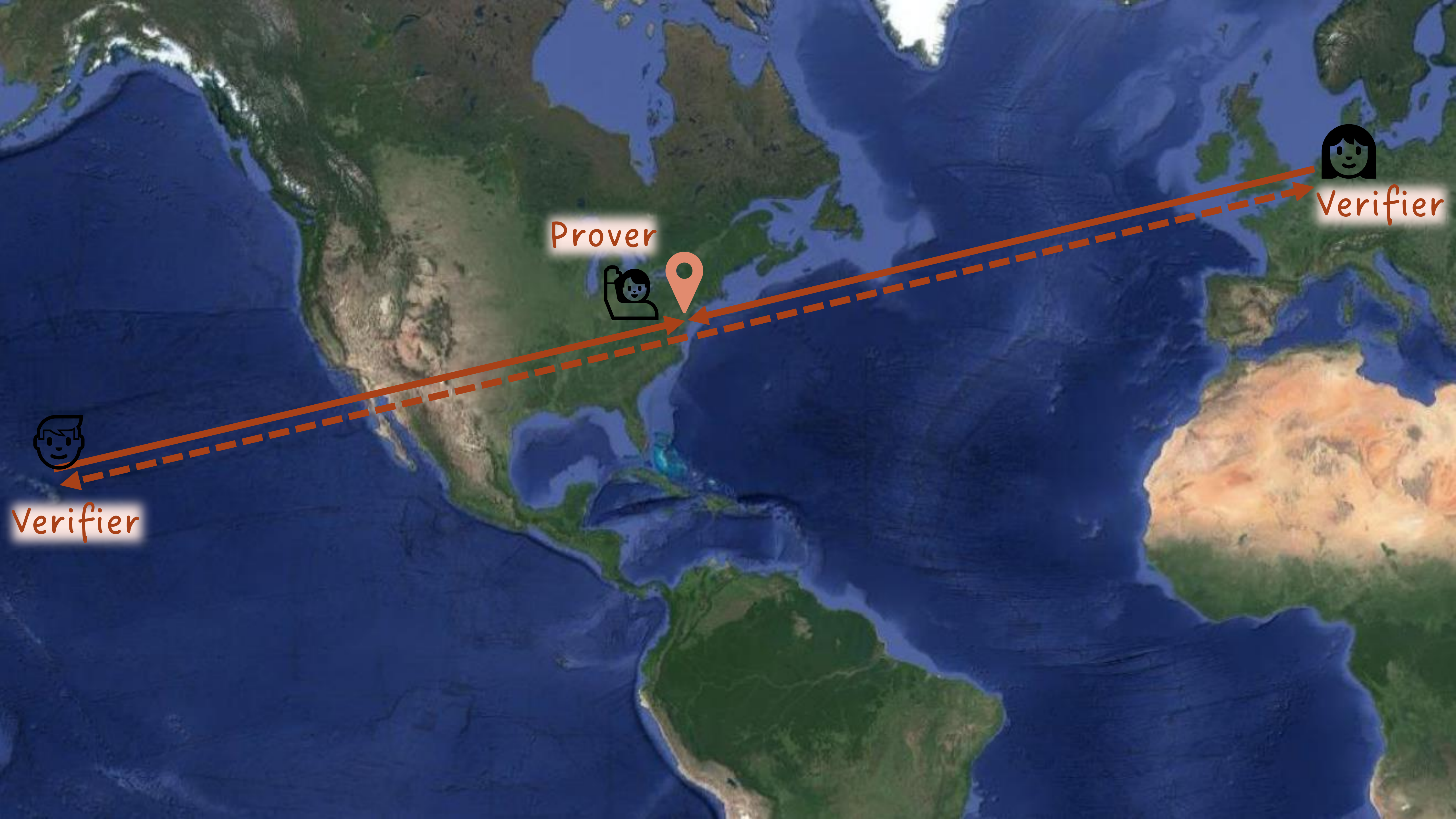

Prover


Prover
Verifier


Prover
Verifier

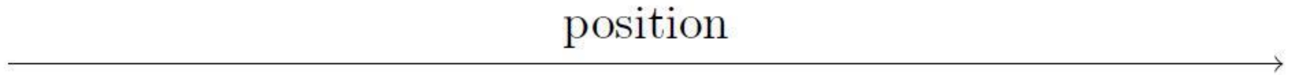

Prover
Verifier
Verifier


Prover
Verifier
Verifier

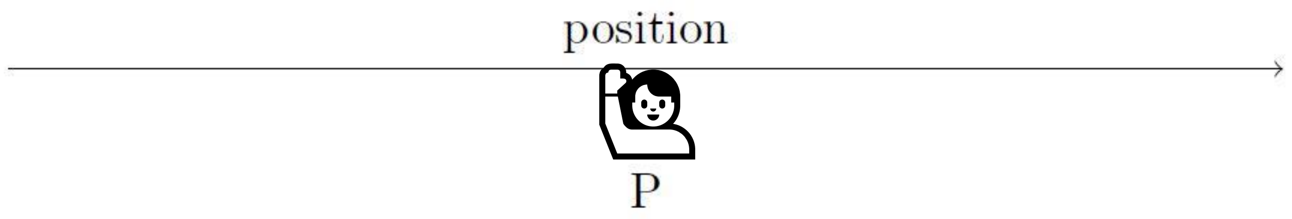

Prover
Verifier
Verifier

Classical Position Verification

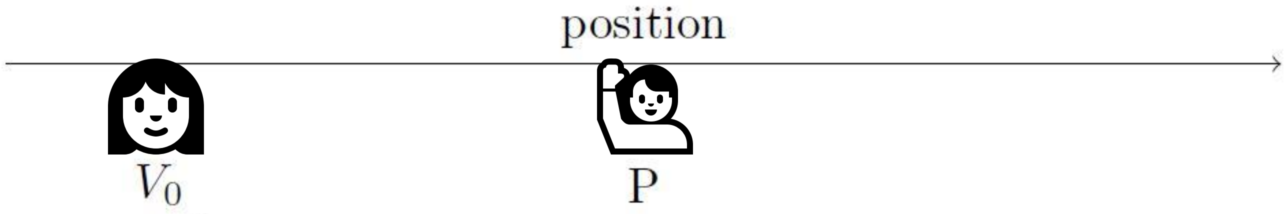
Classical Position Verification



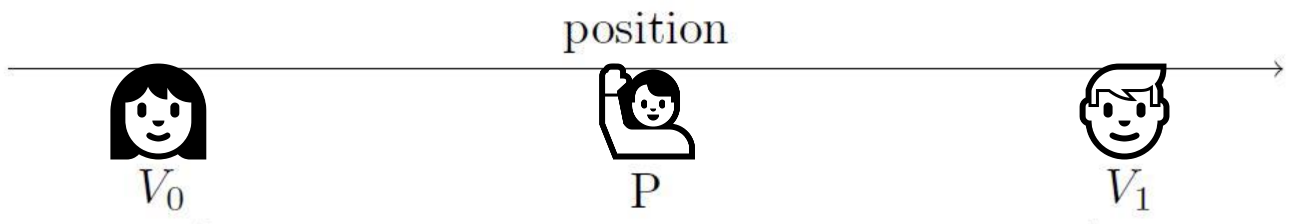
Classical Position Verification



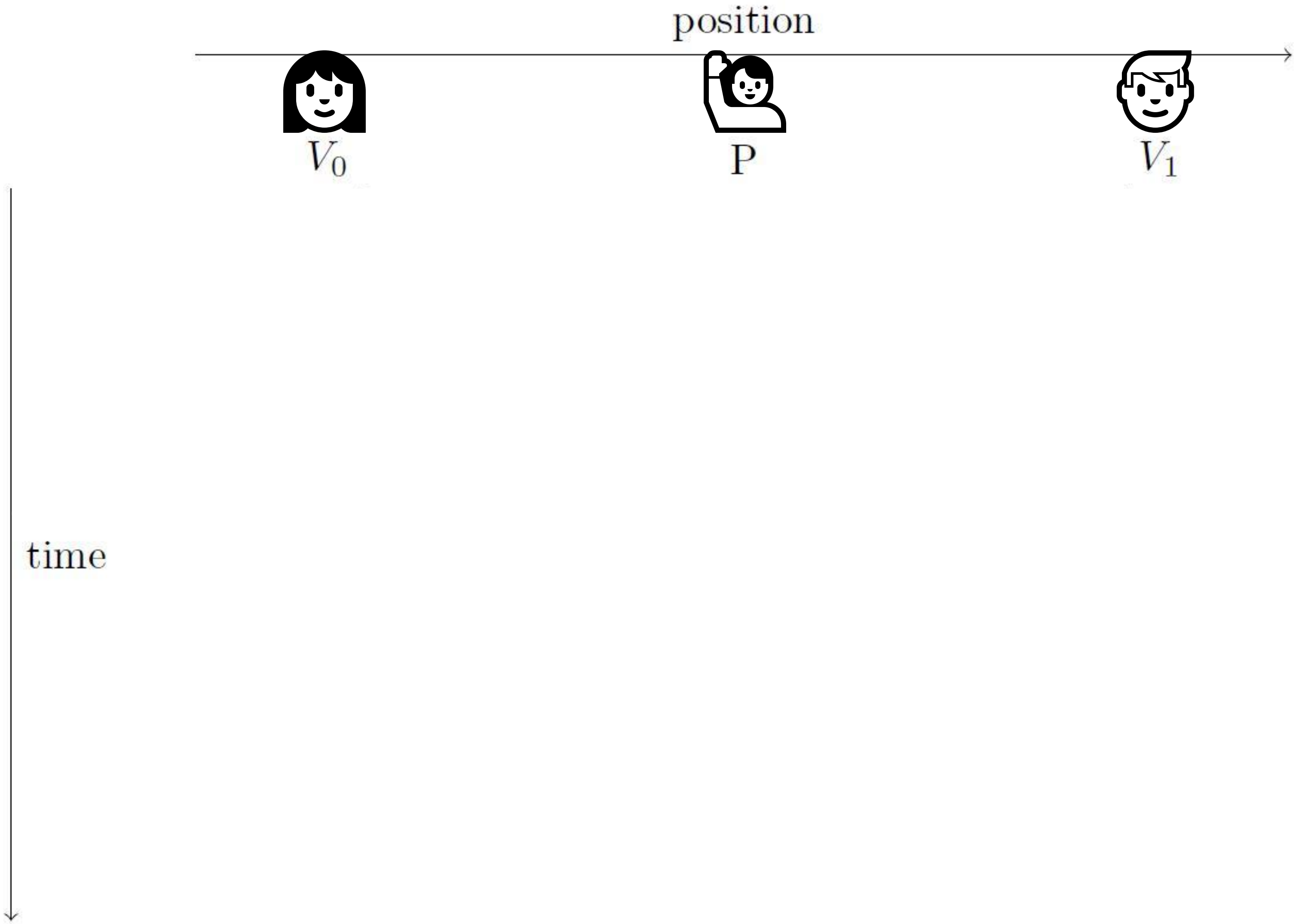
Classical Position Verification



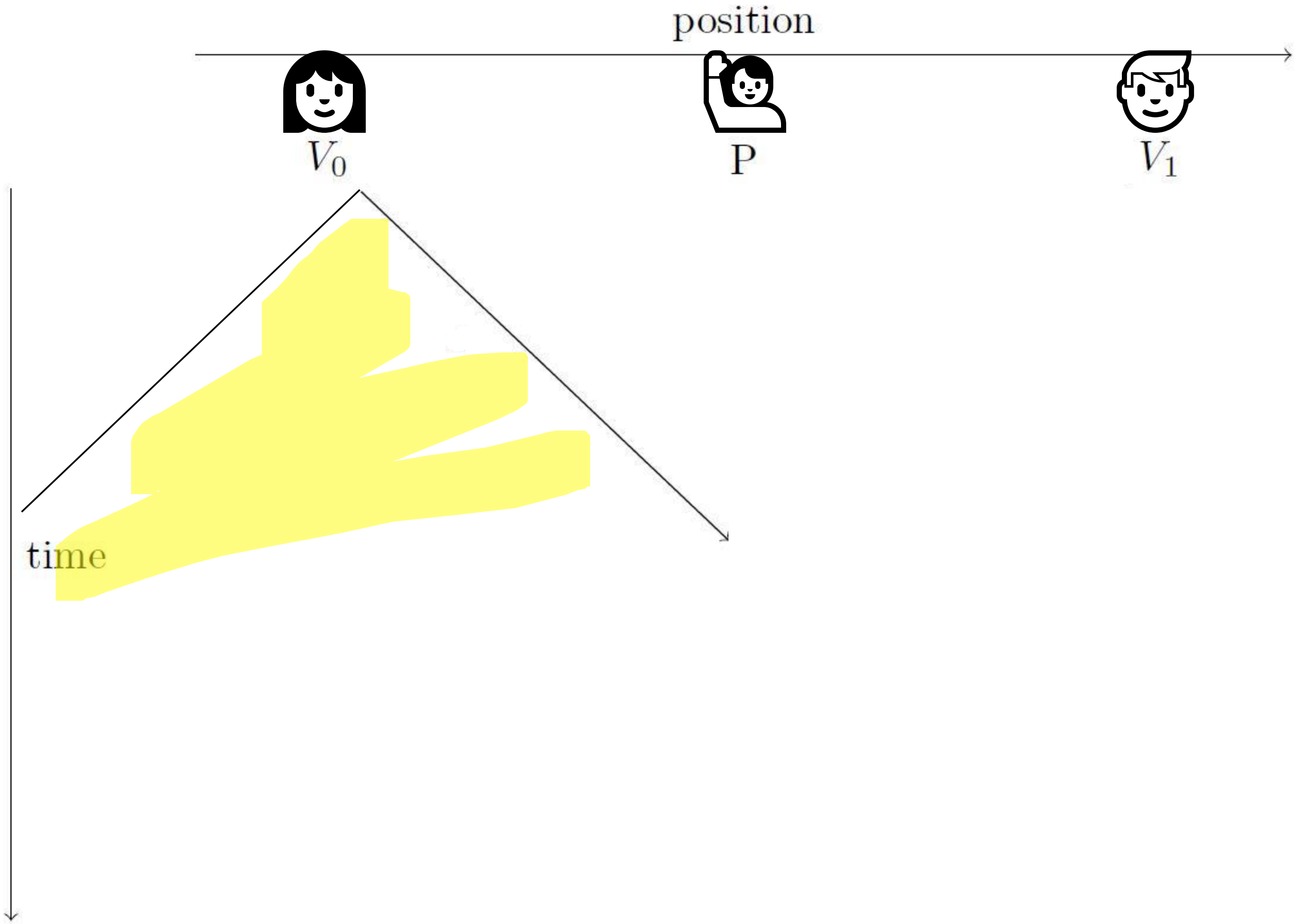
Classical Position Verification



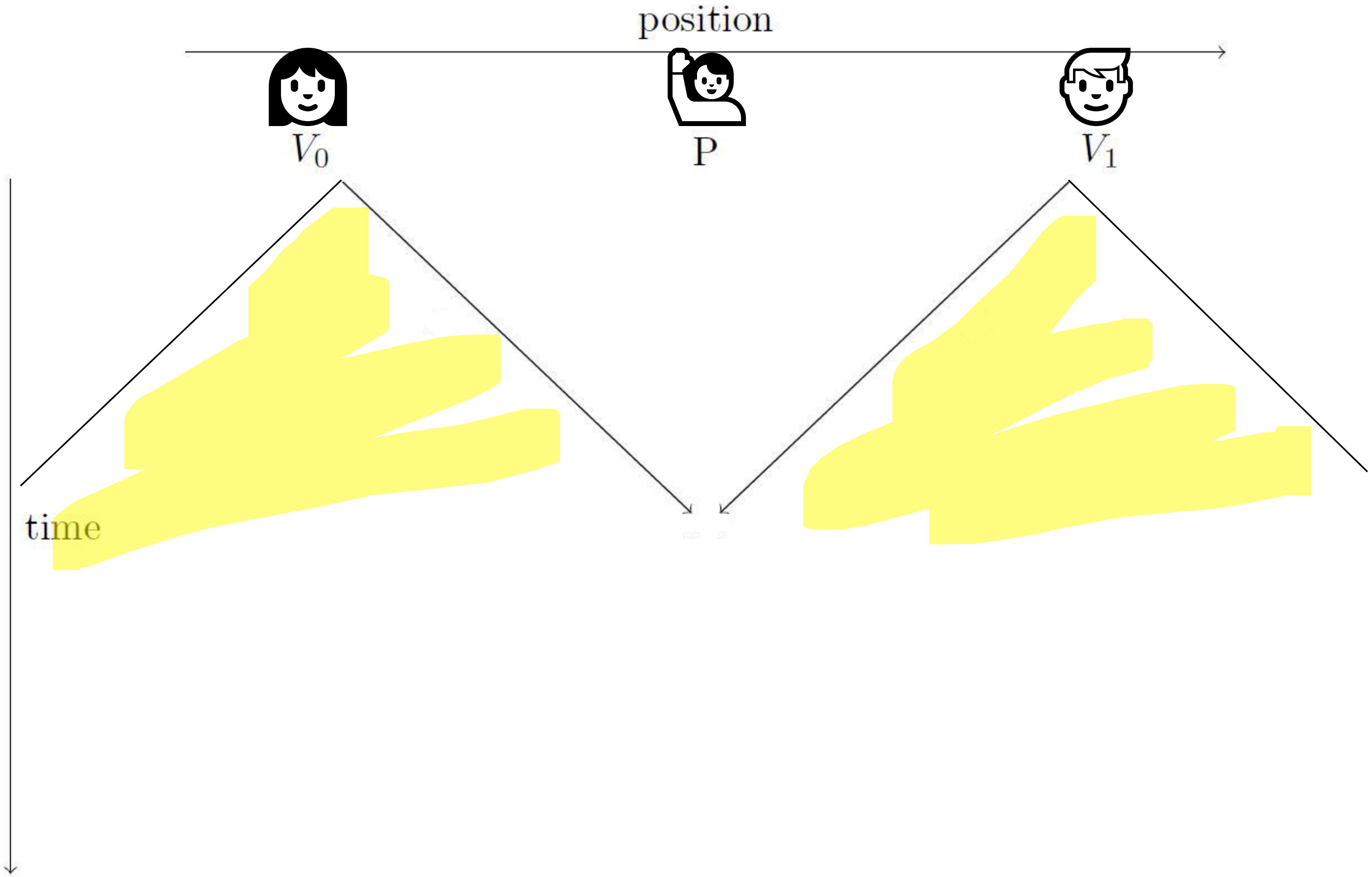
Classical Position Verification



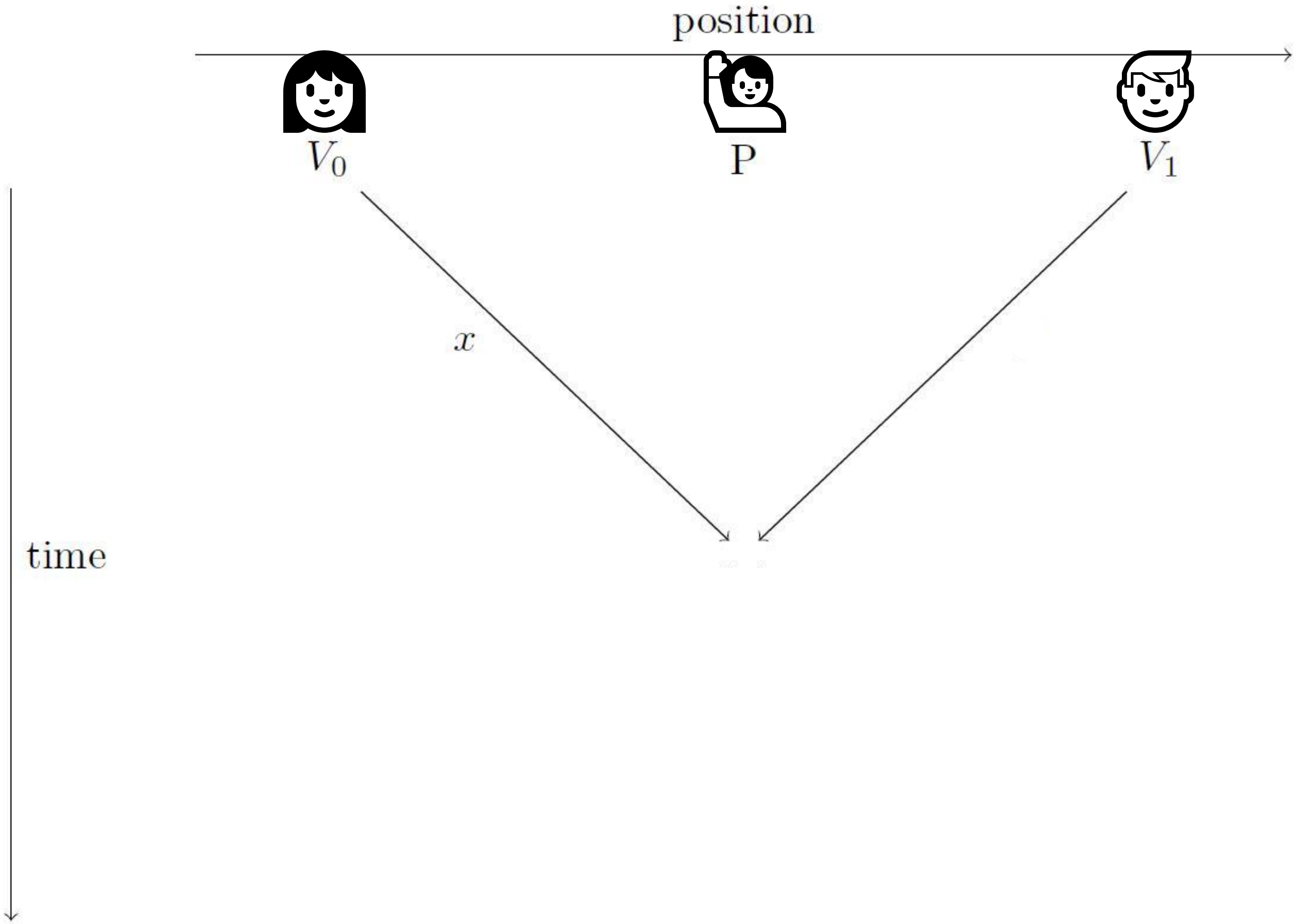
Classical Position Verification



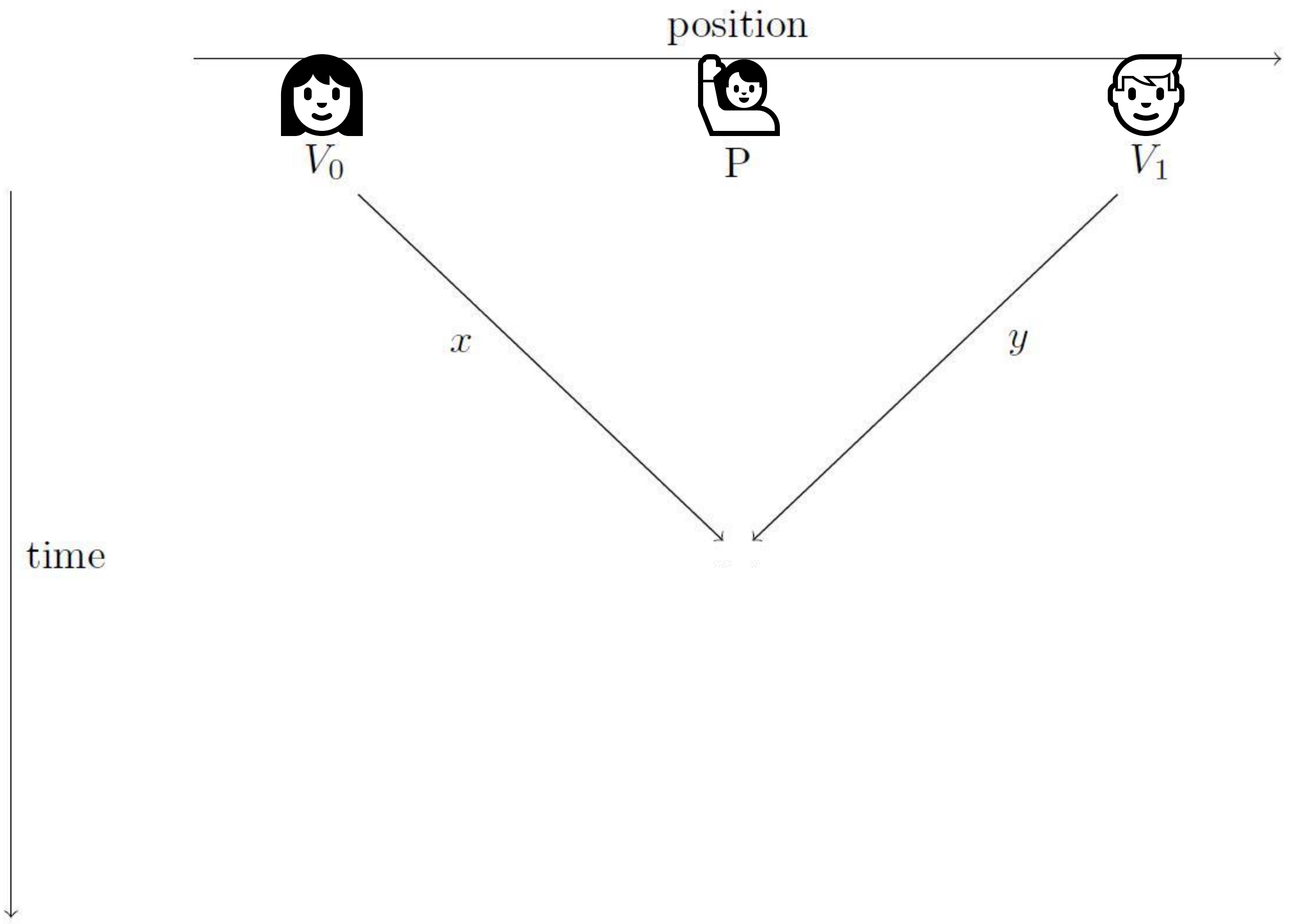
Classical Position Verification



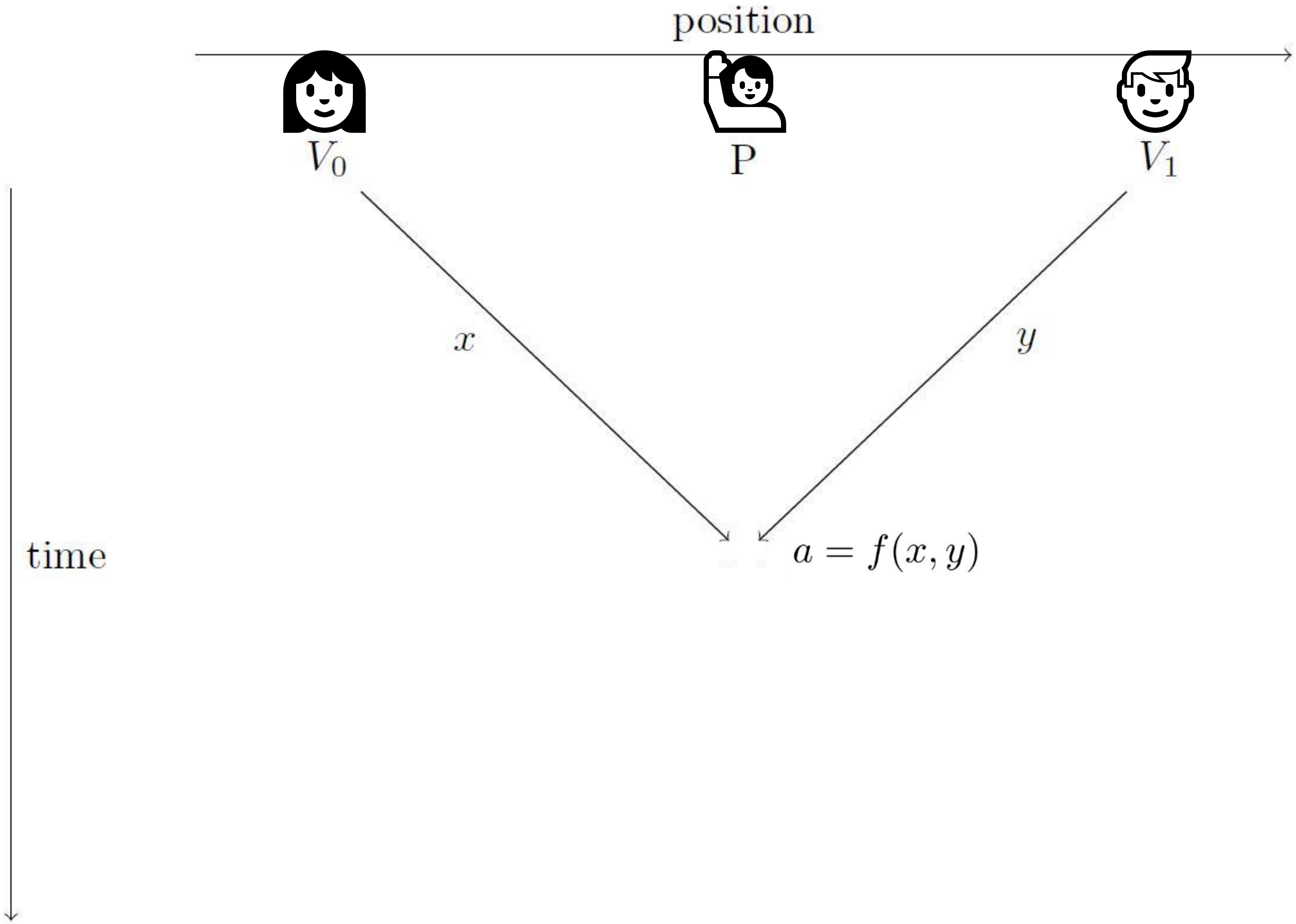
Classical Position Verification



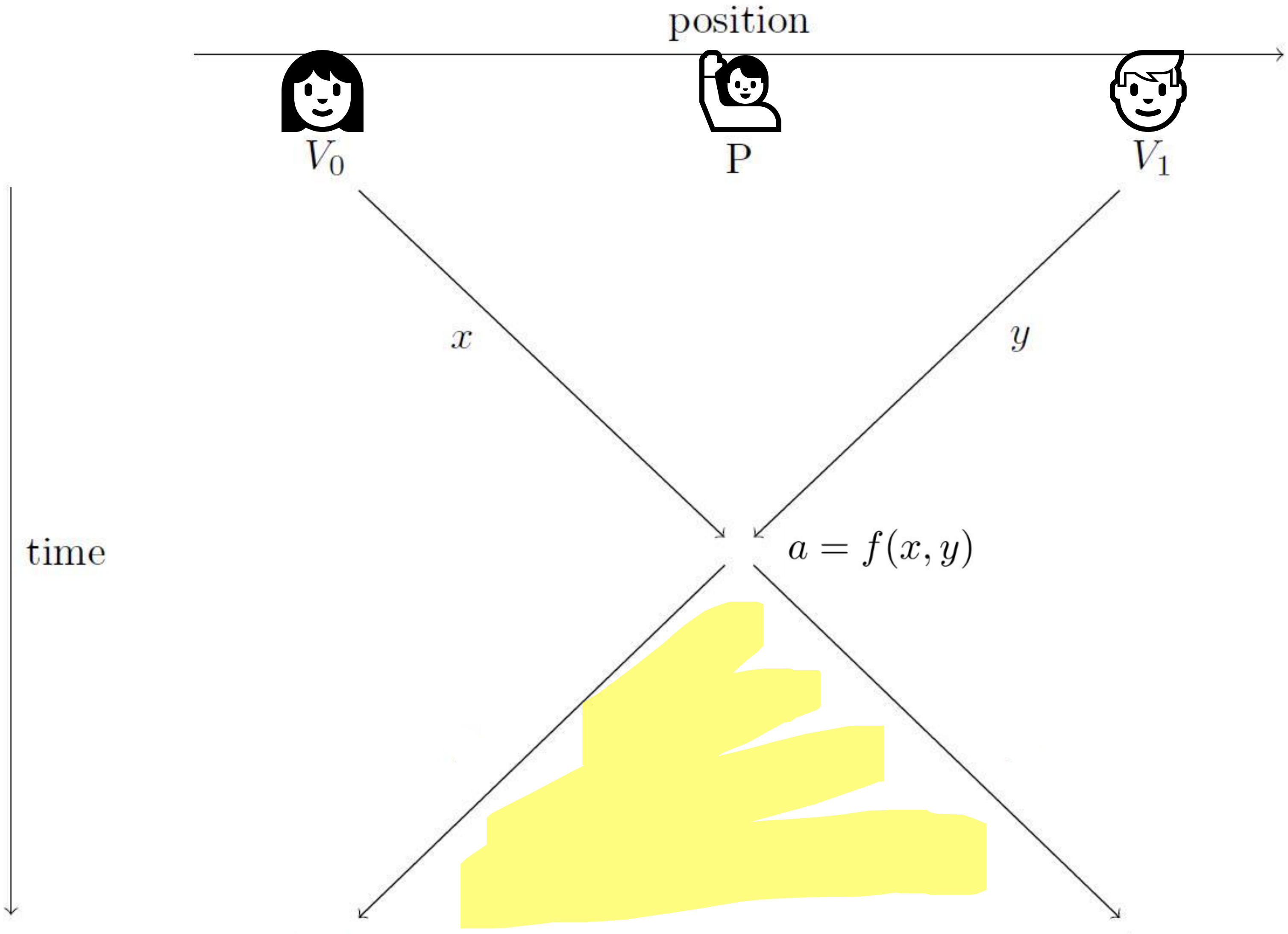
Classical Position Verification



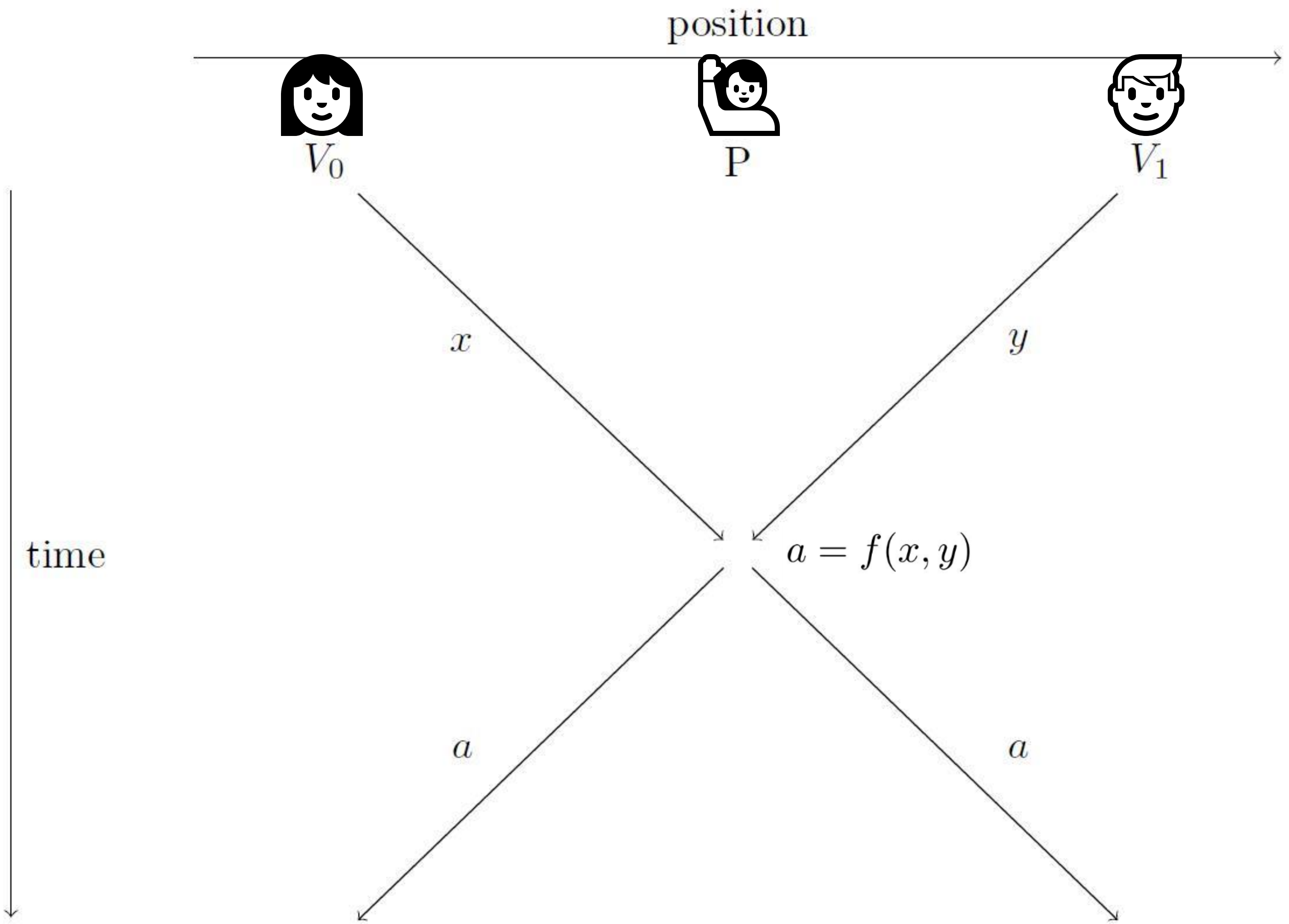
Classical Position Verification



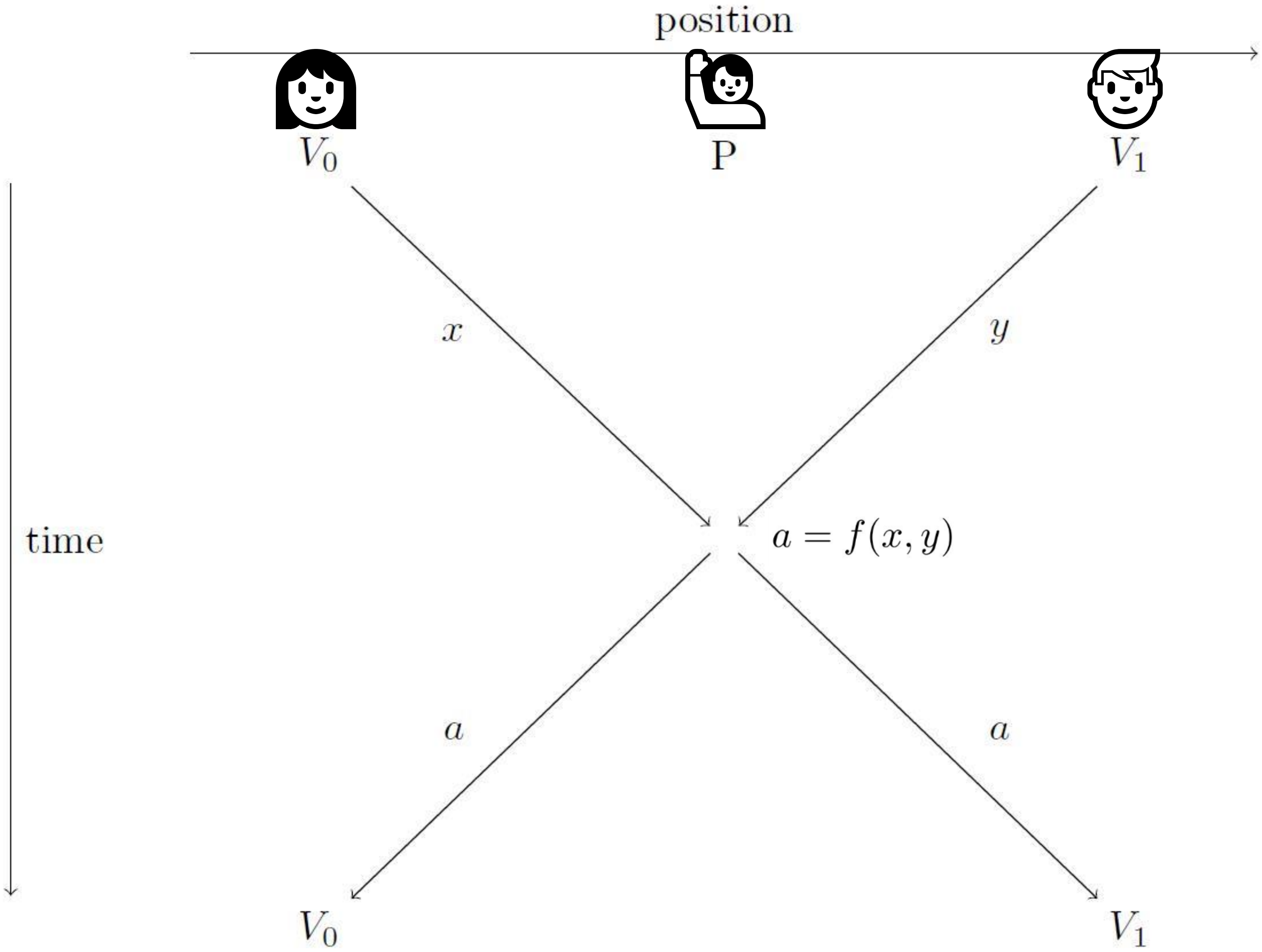
Classical Position Verification



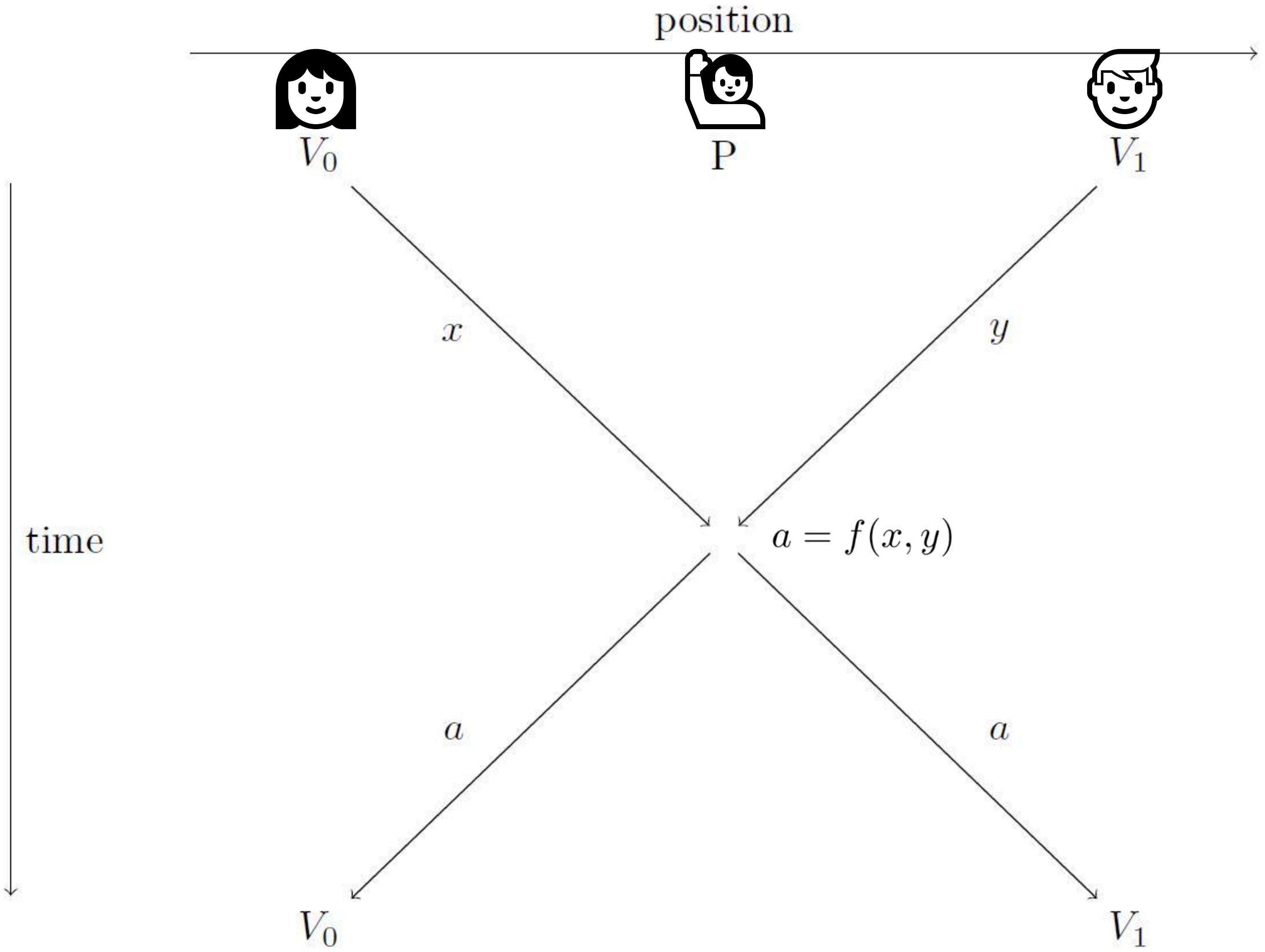
Classical Position Verification



Classical Position Verification

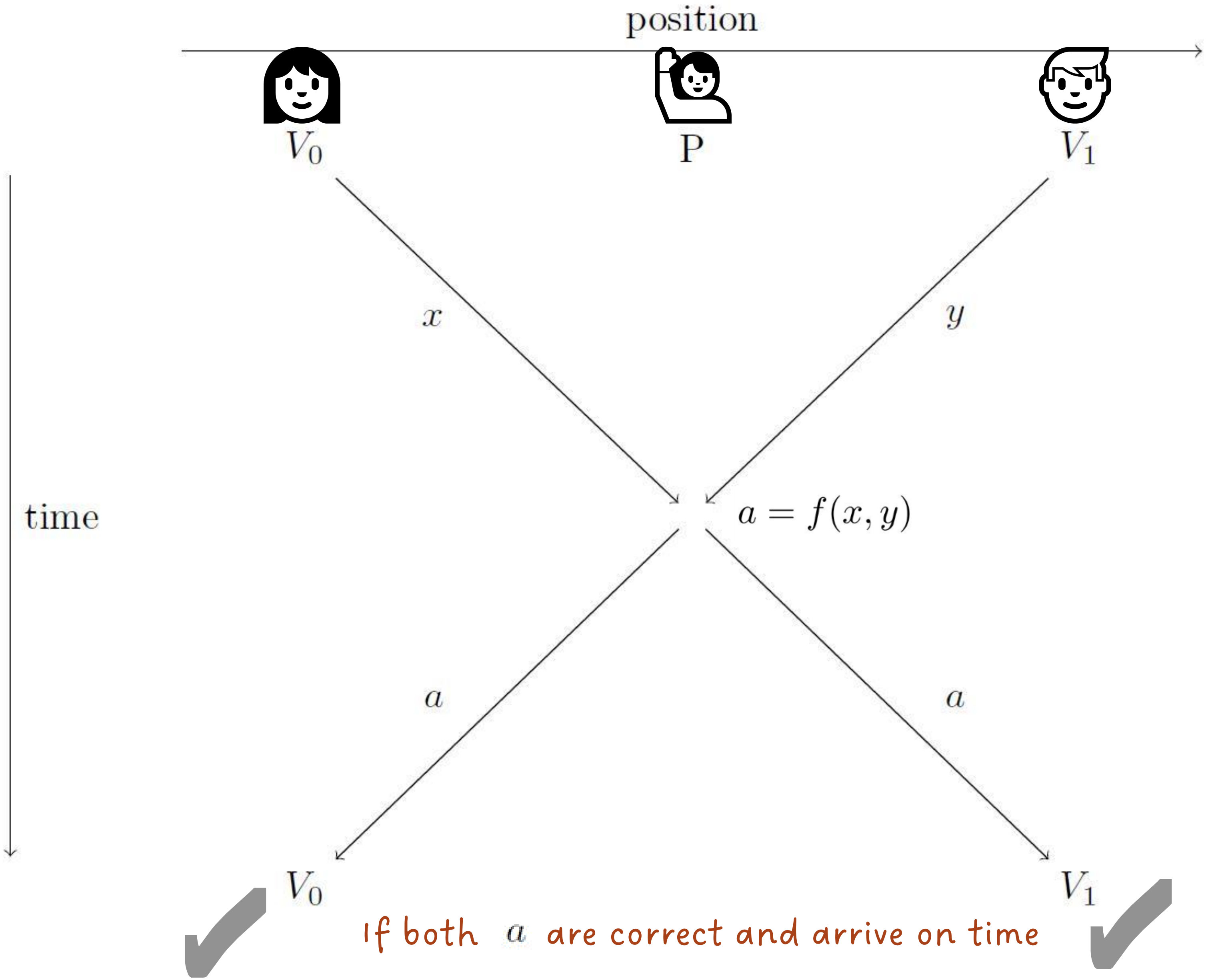


Classical Position Verification



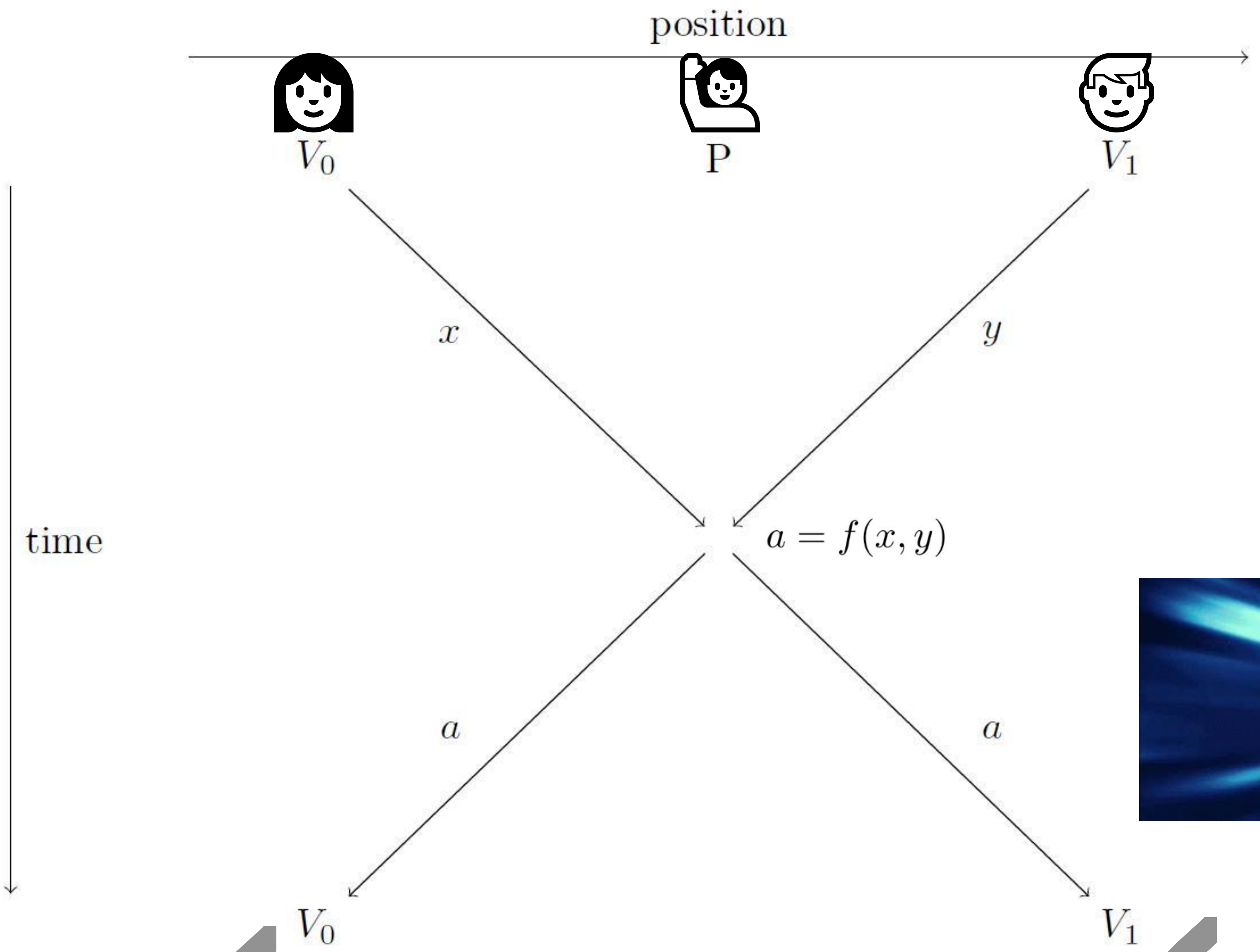
If both a are correct and arrive on time

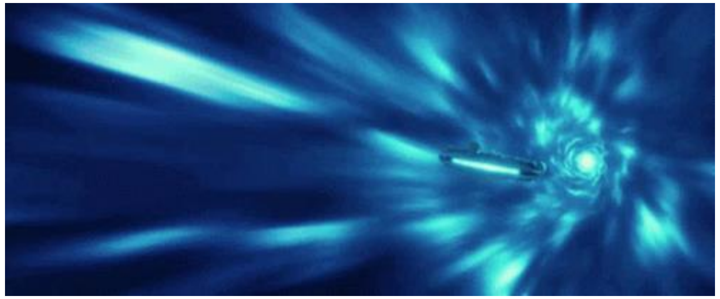
Classical Position Verification



If both a are correct and arrive on time

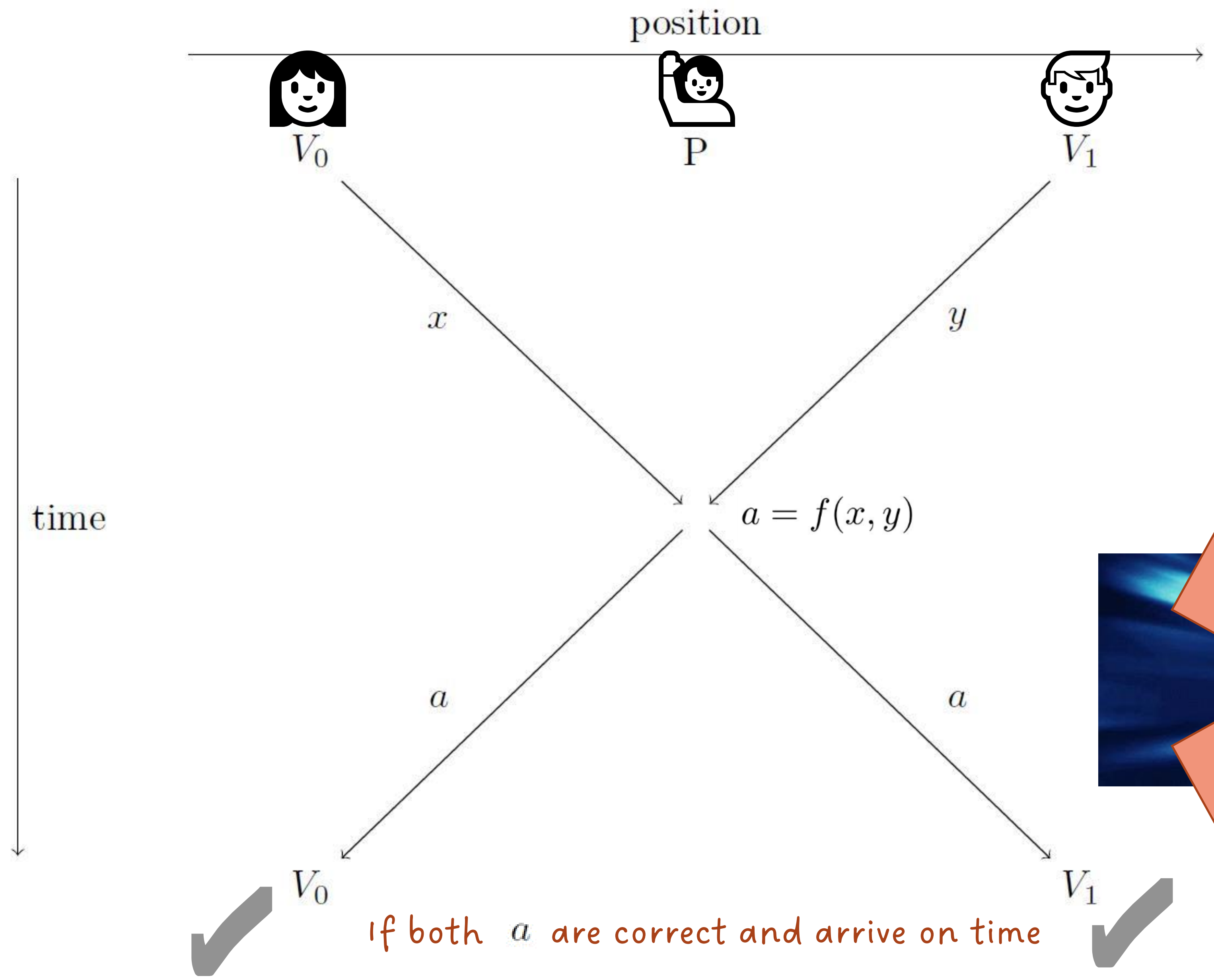
Classical Position Verification

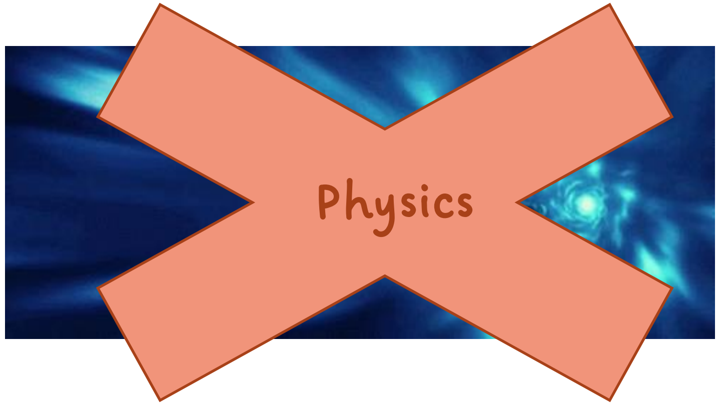




If both a are correct and arrive on time

Classical Position Verification



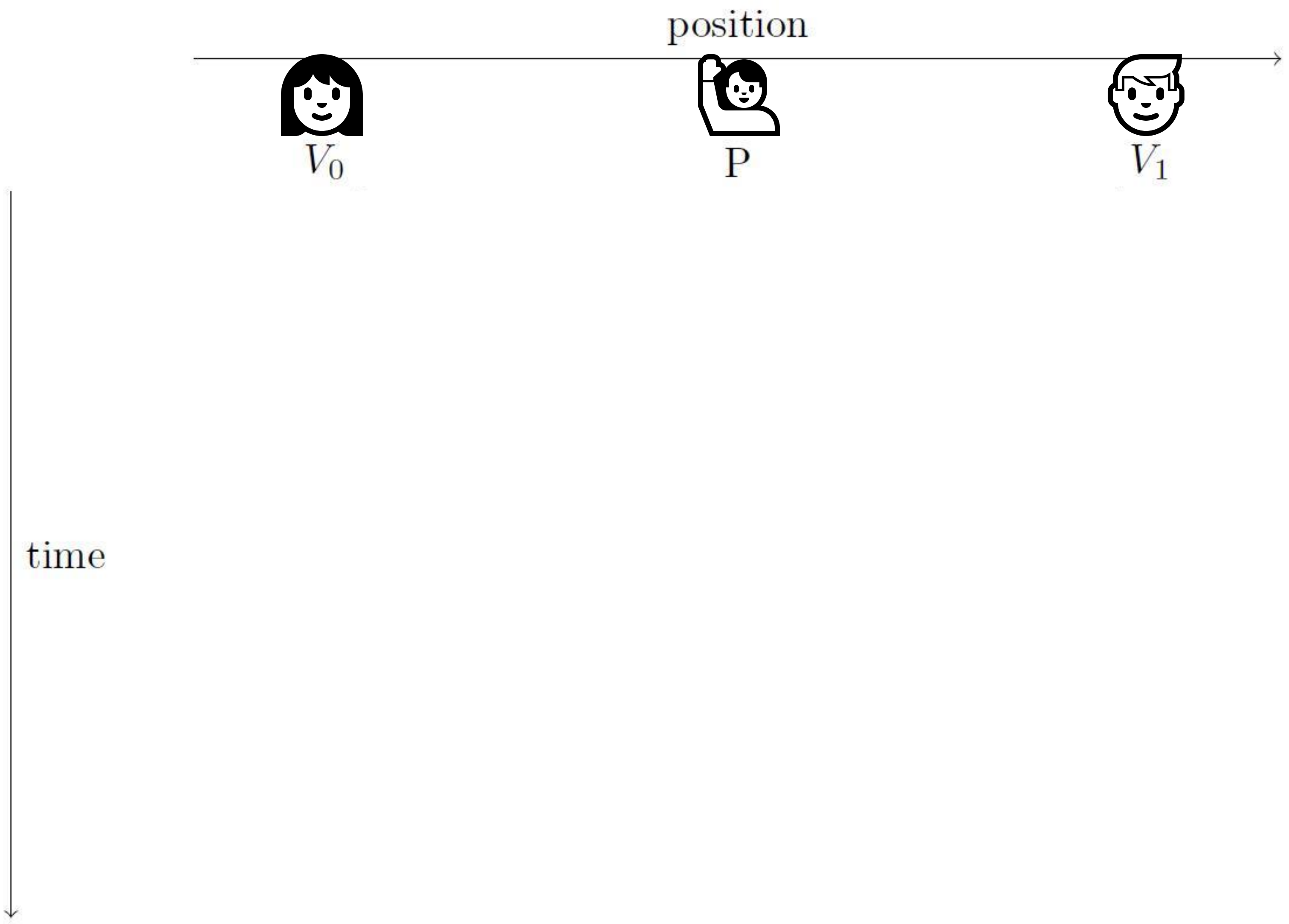


If both a are correct and arrive on time

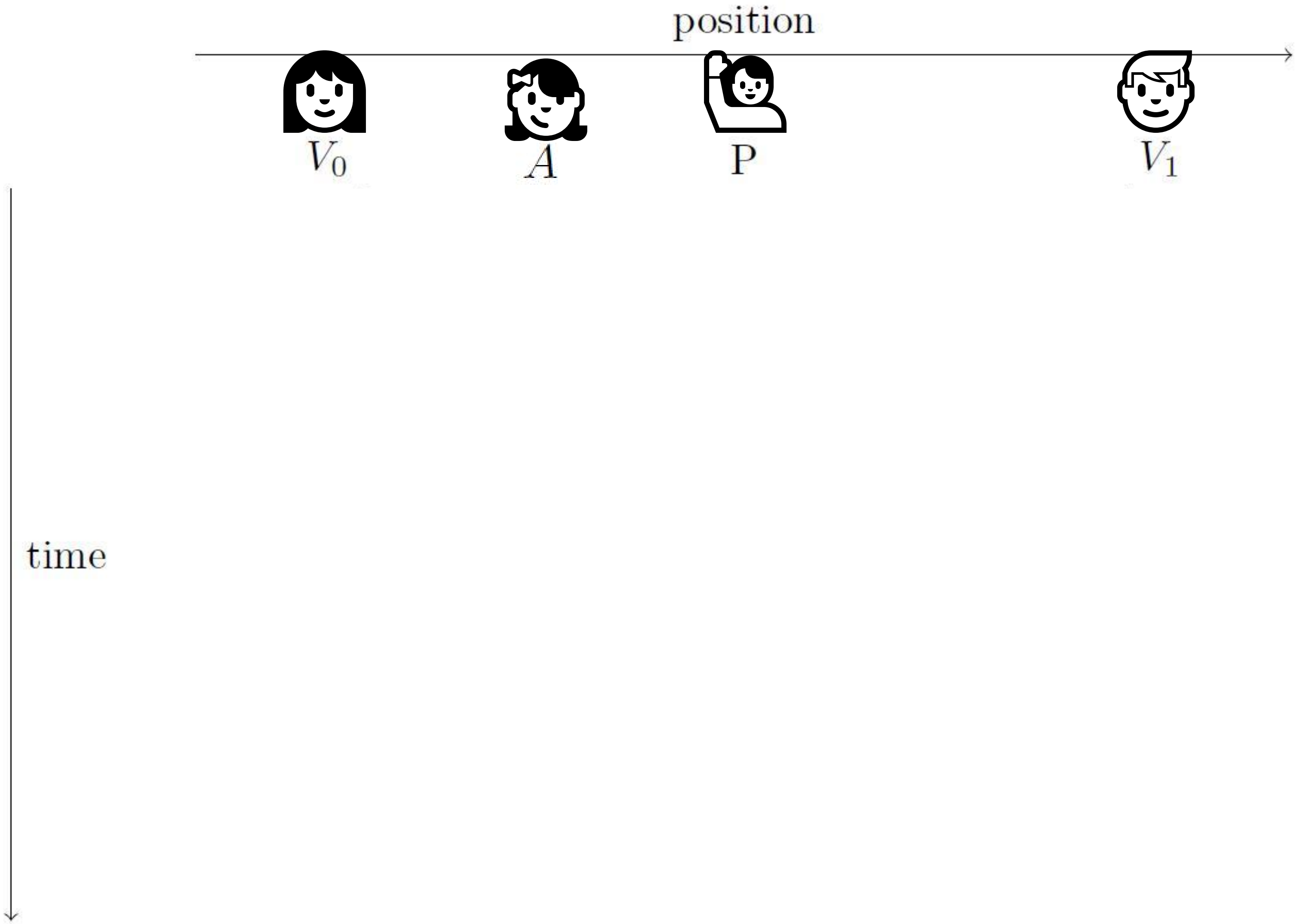
But…

Universal attack

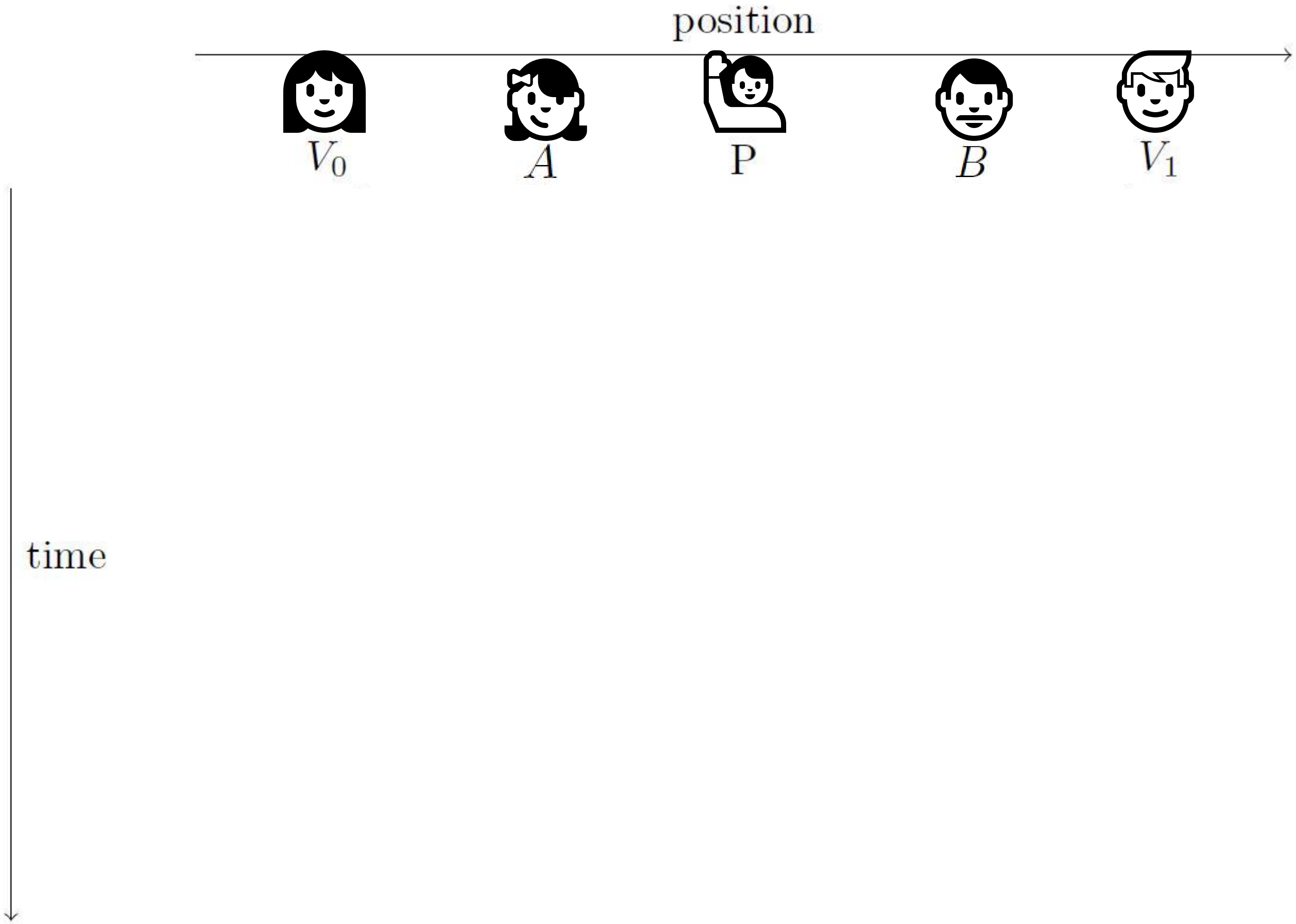
Classical universal attack



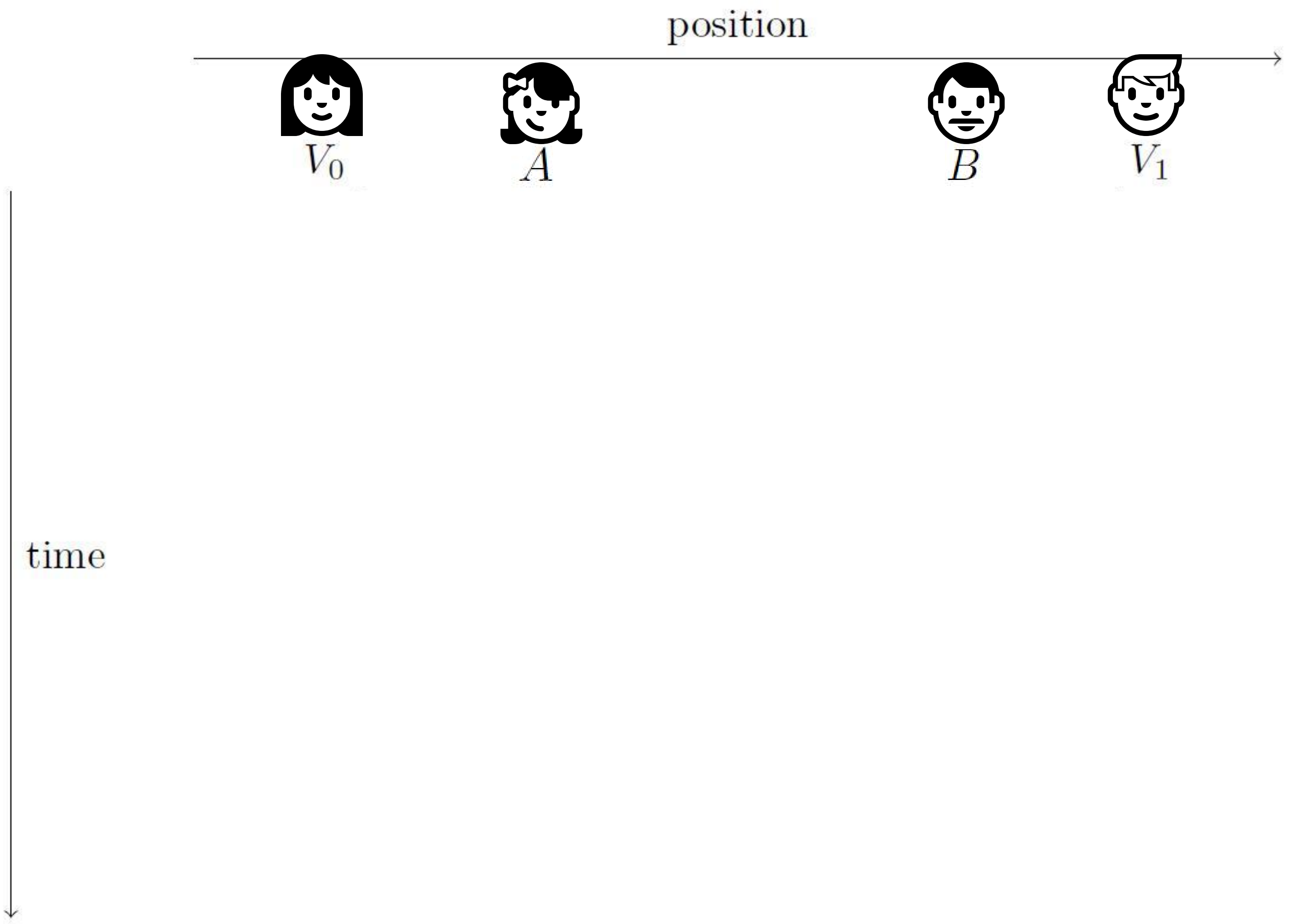
Classical universal attack



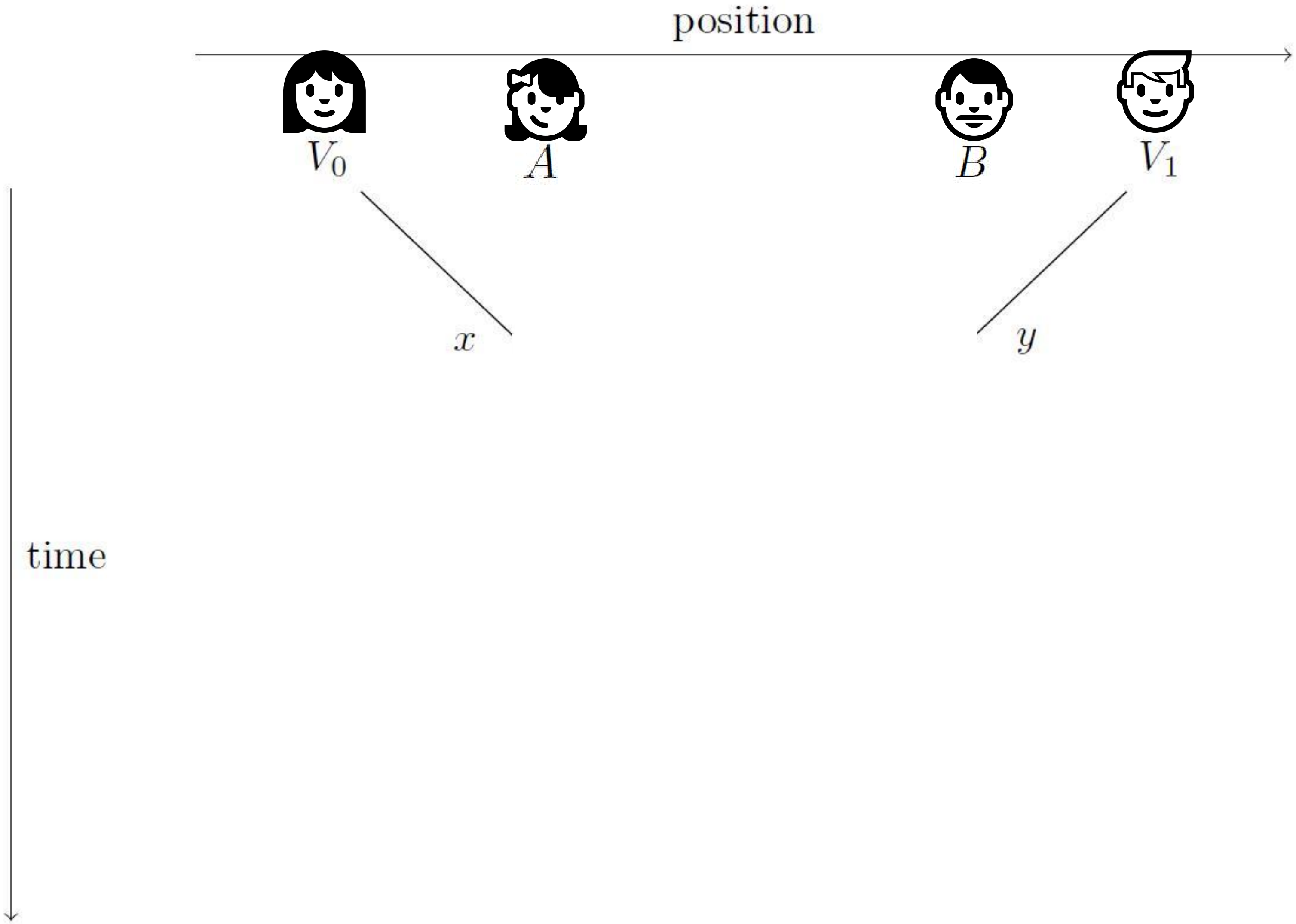
Classical universal attack



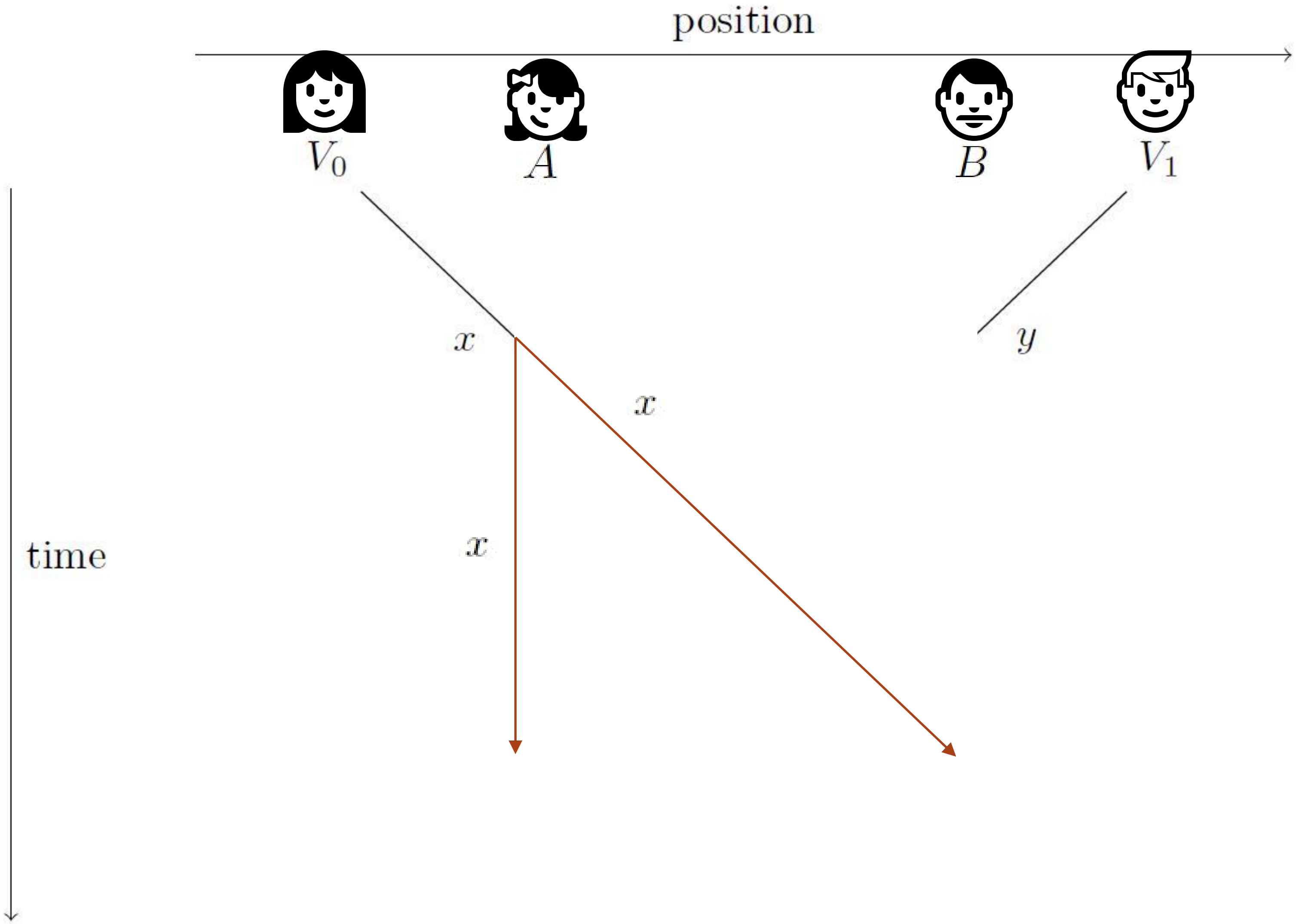
Classical universal attack



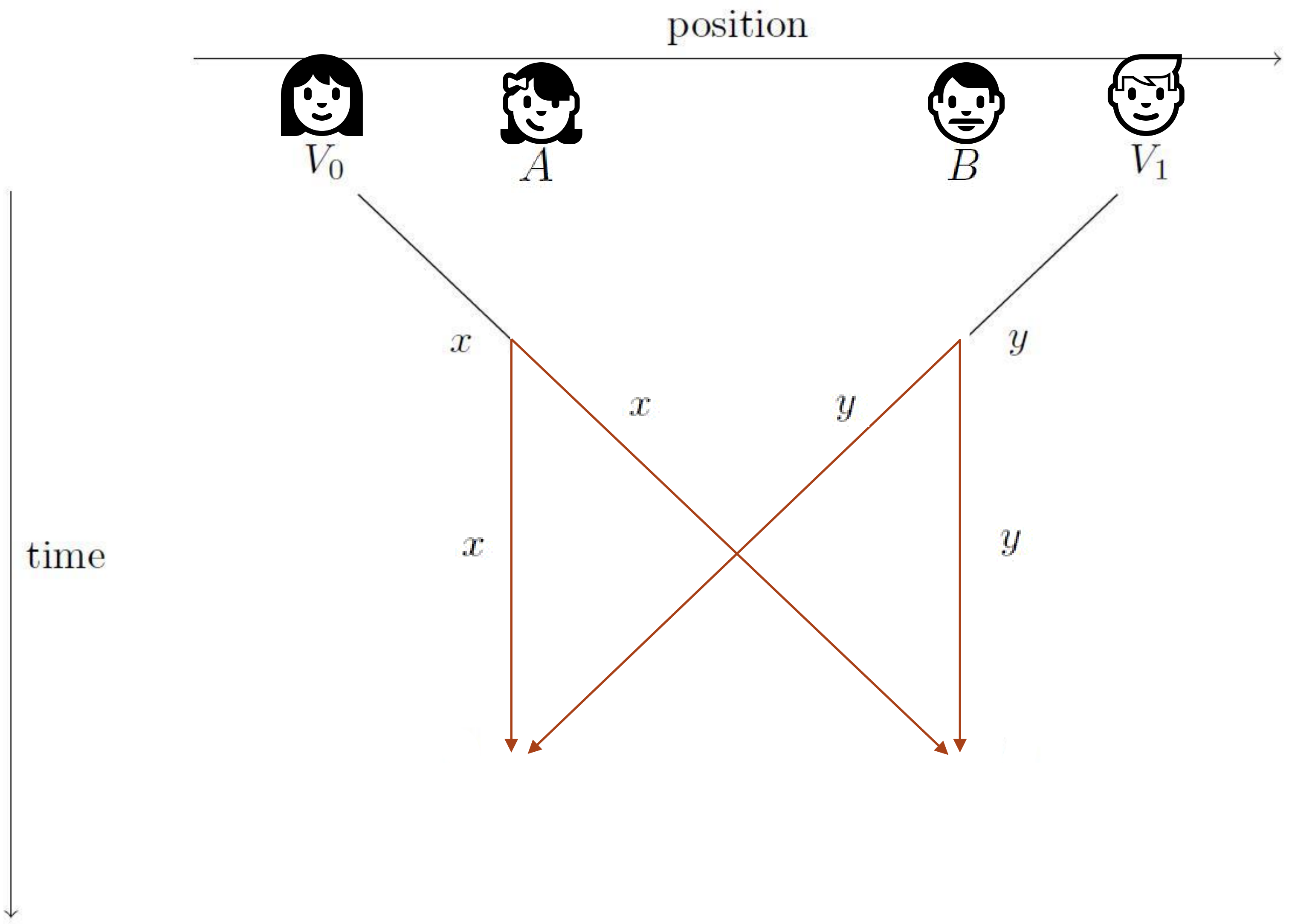
Classical universal attack



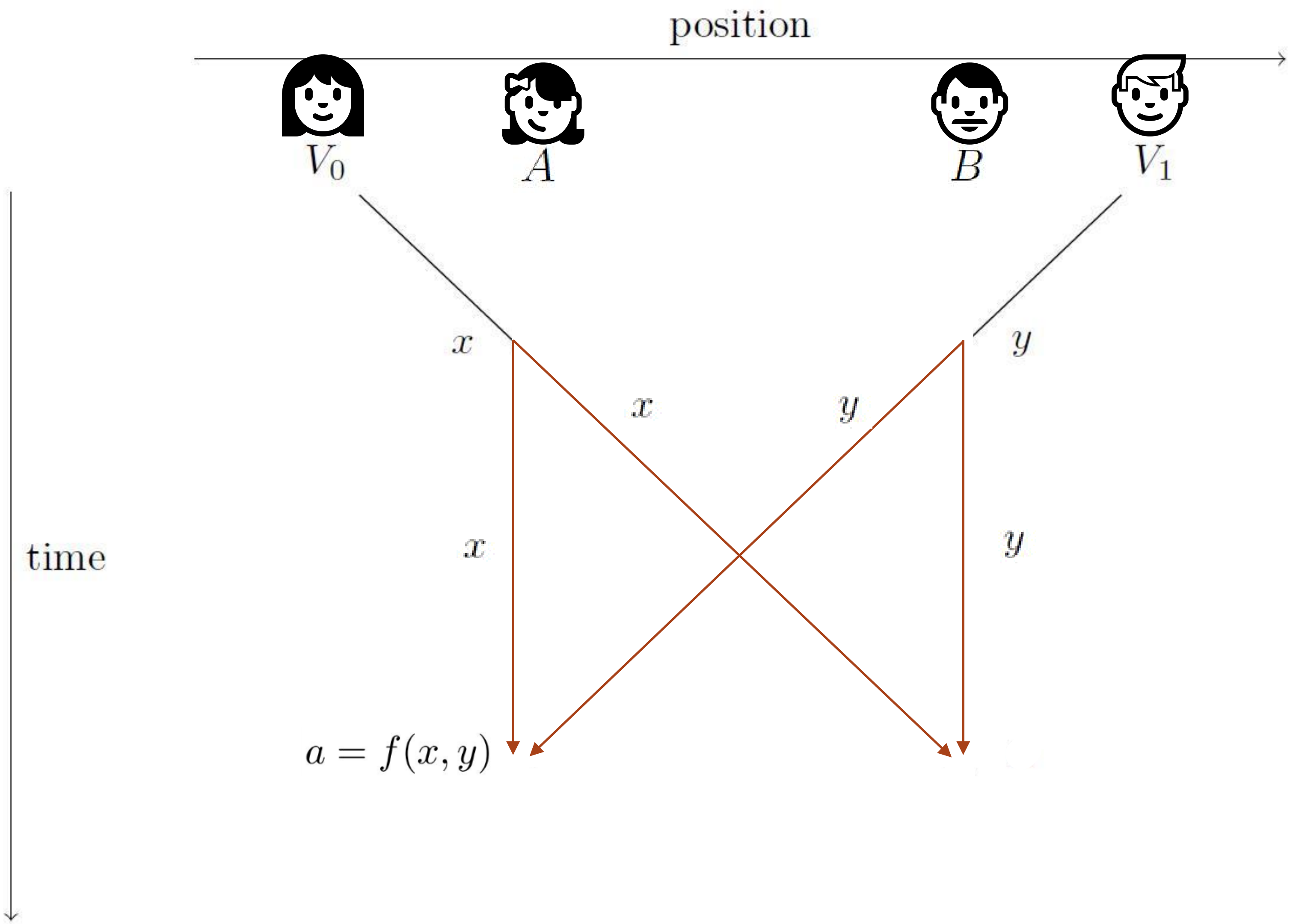
Classical universal attack



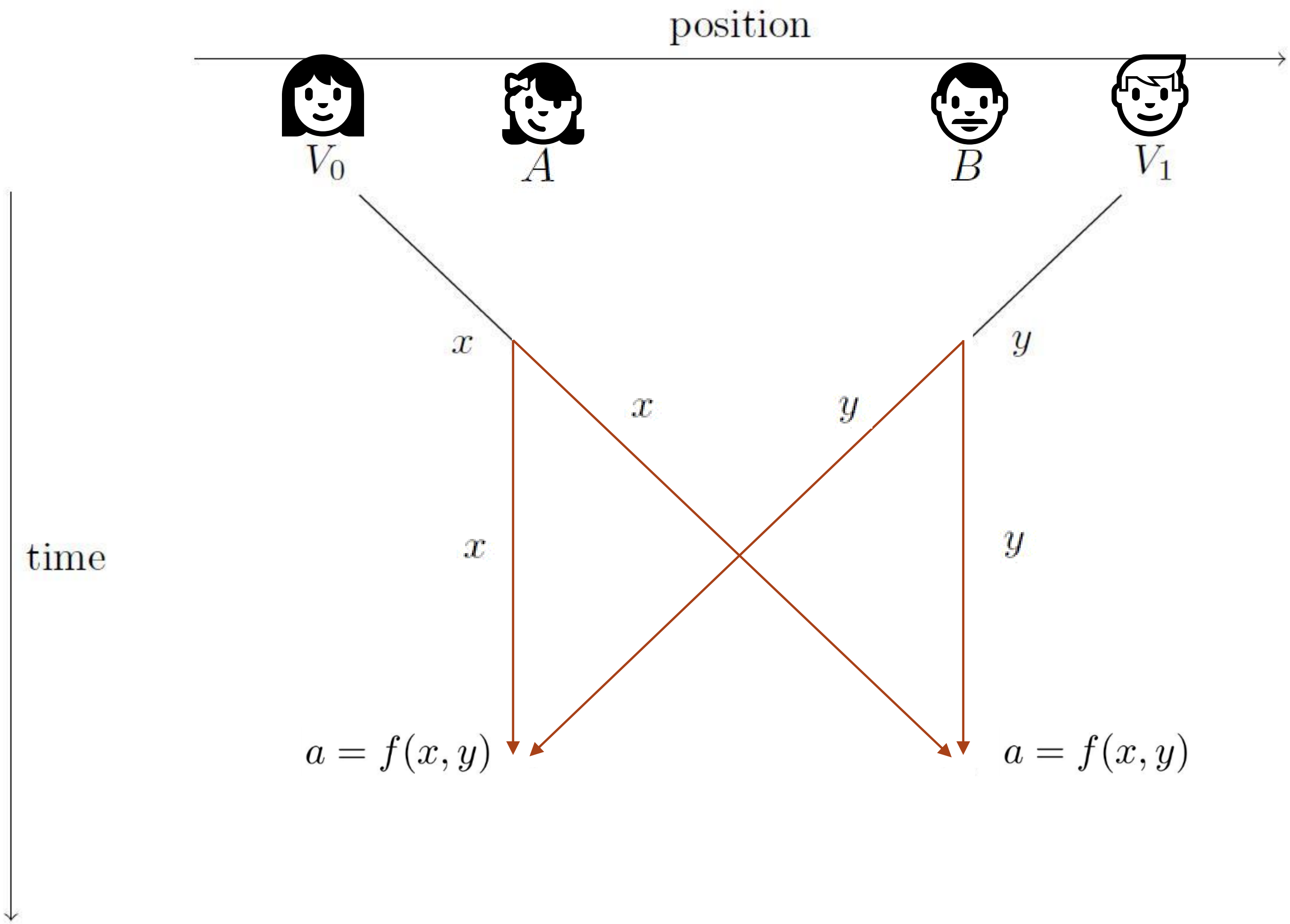
Classical universal attack



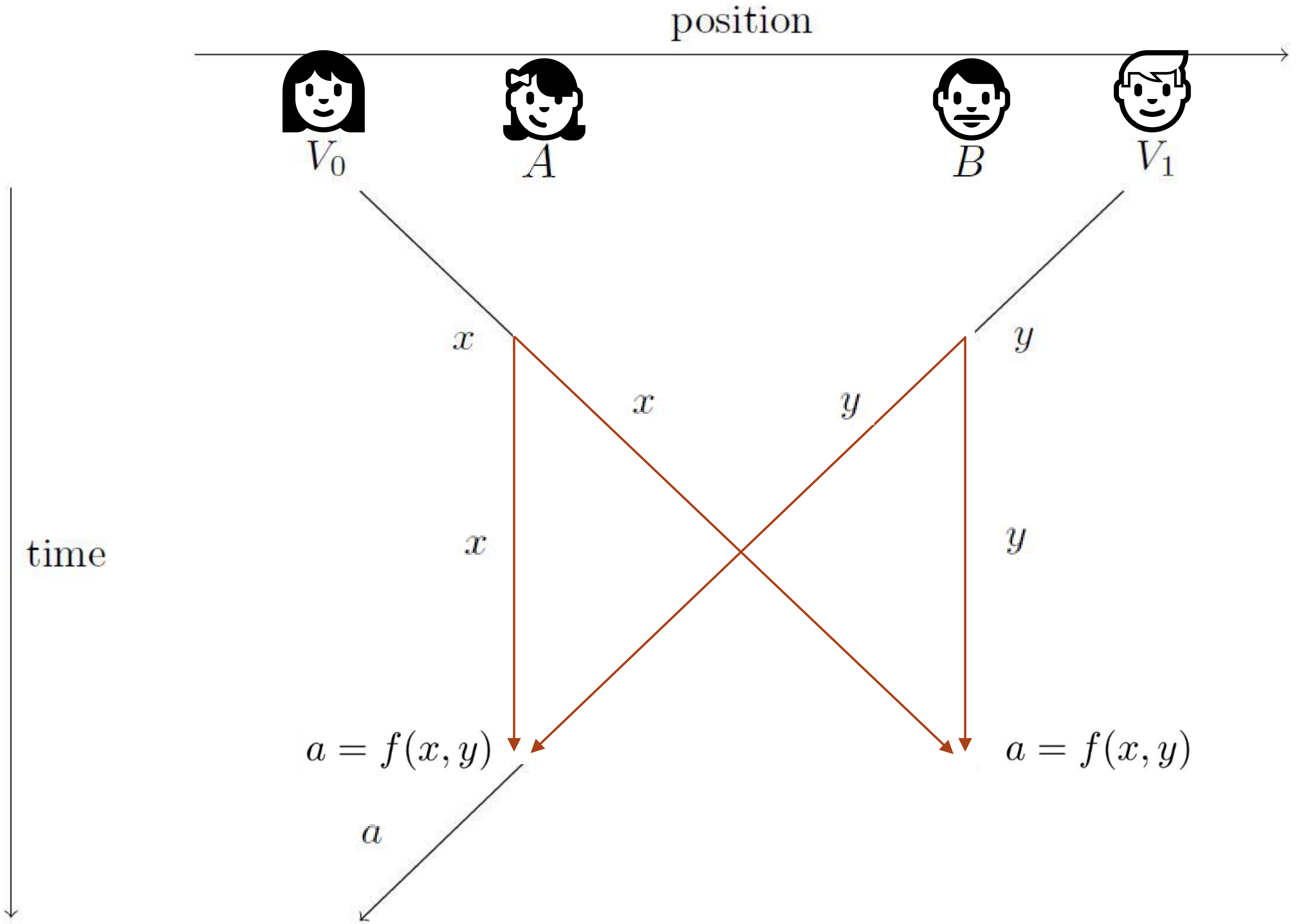
Classical universal attack



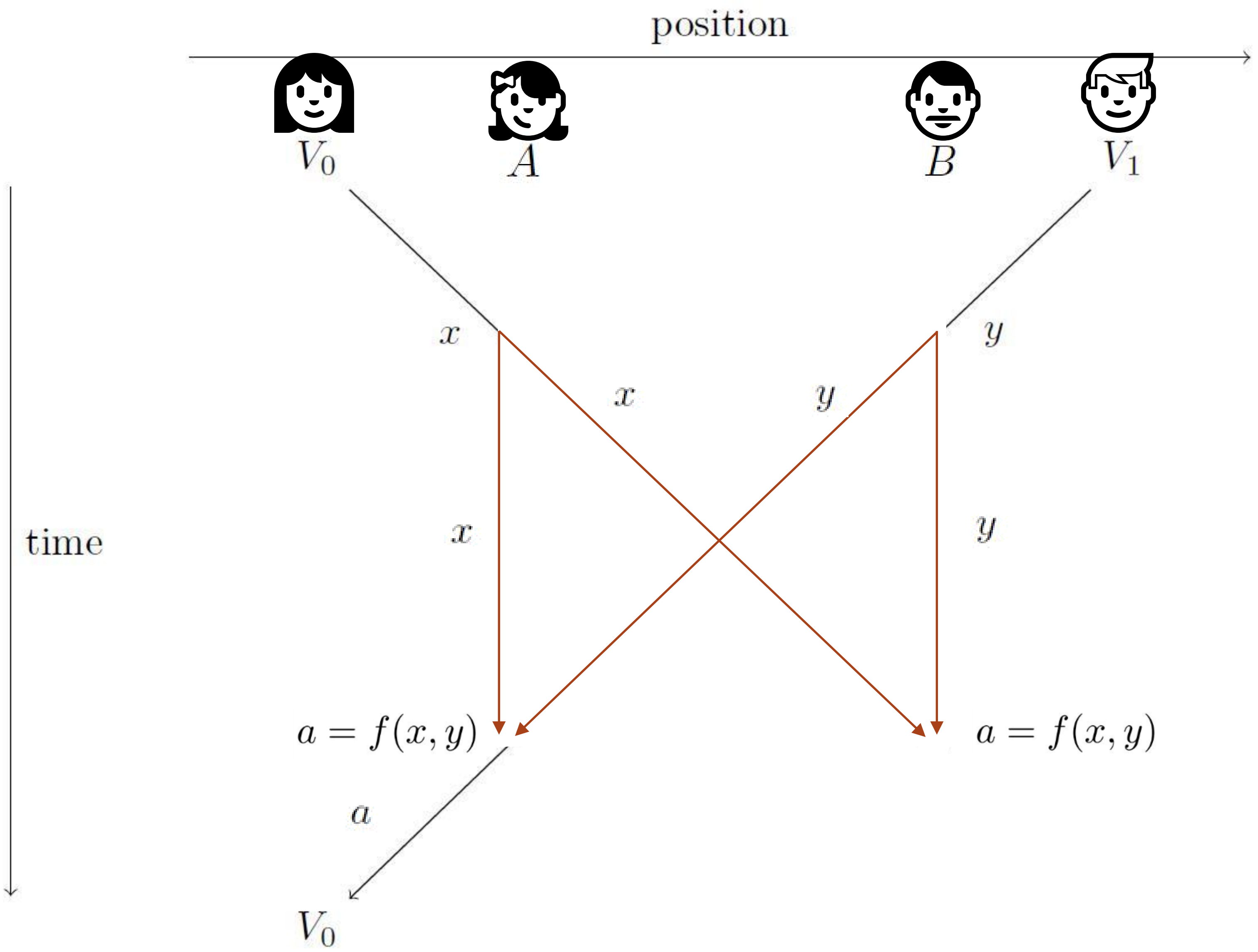
Classical universal attack



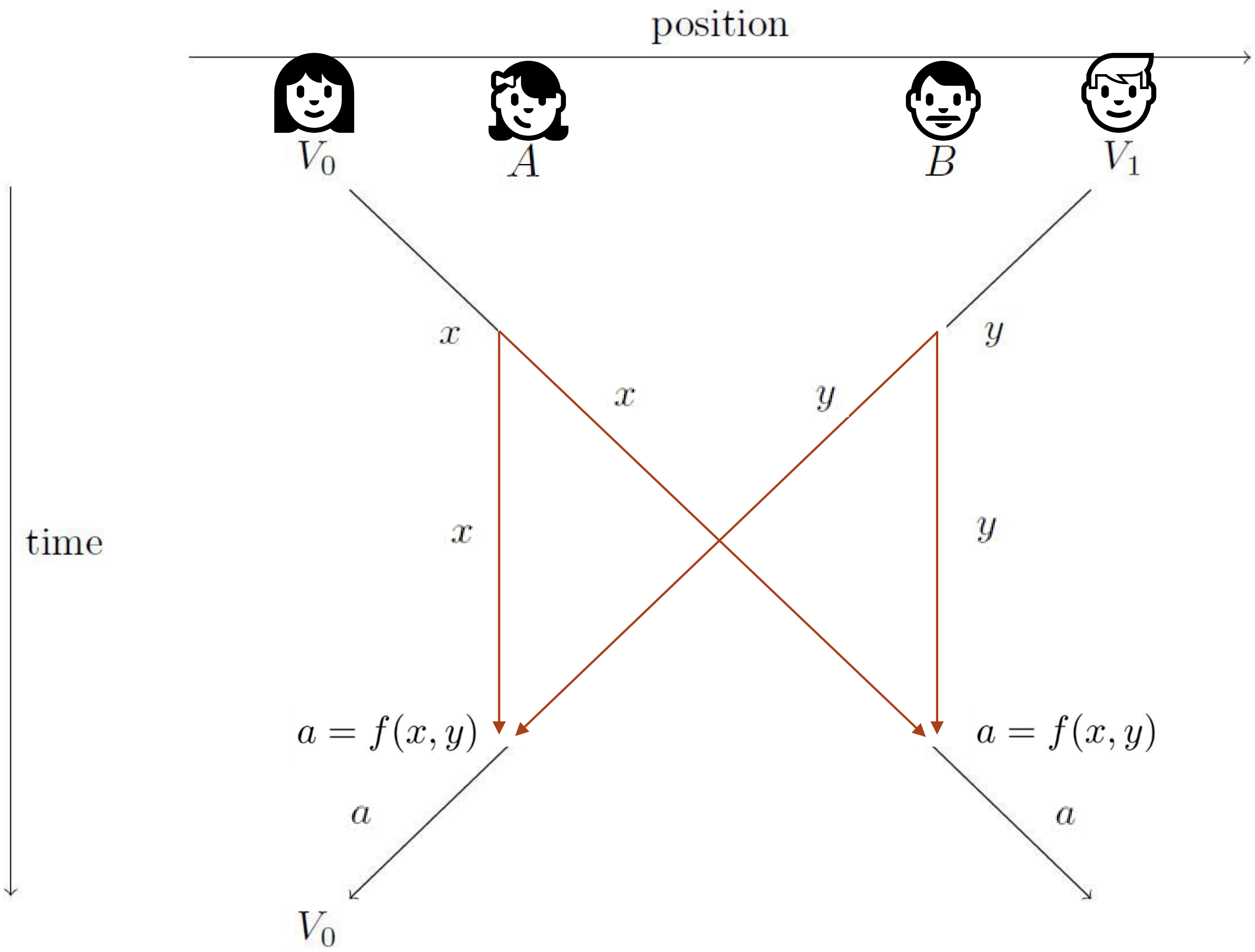
Classical universal attack



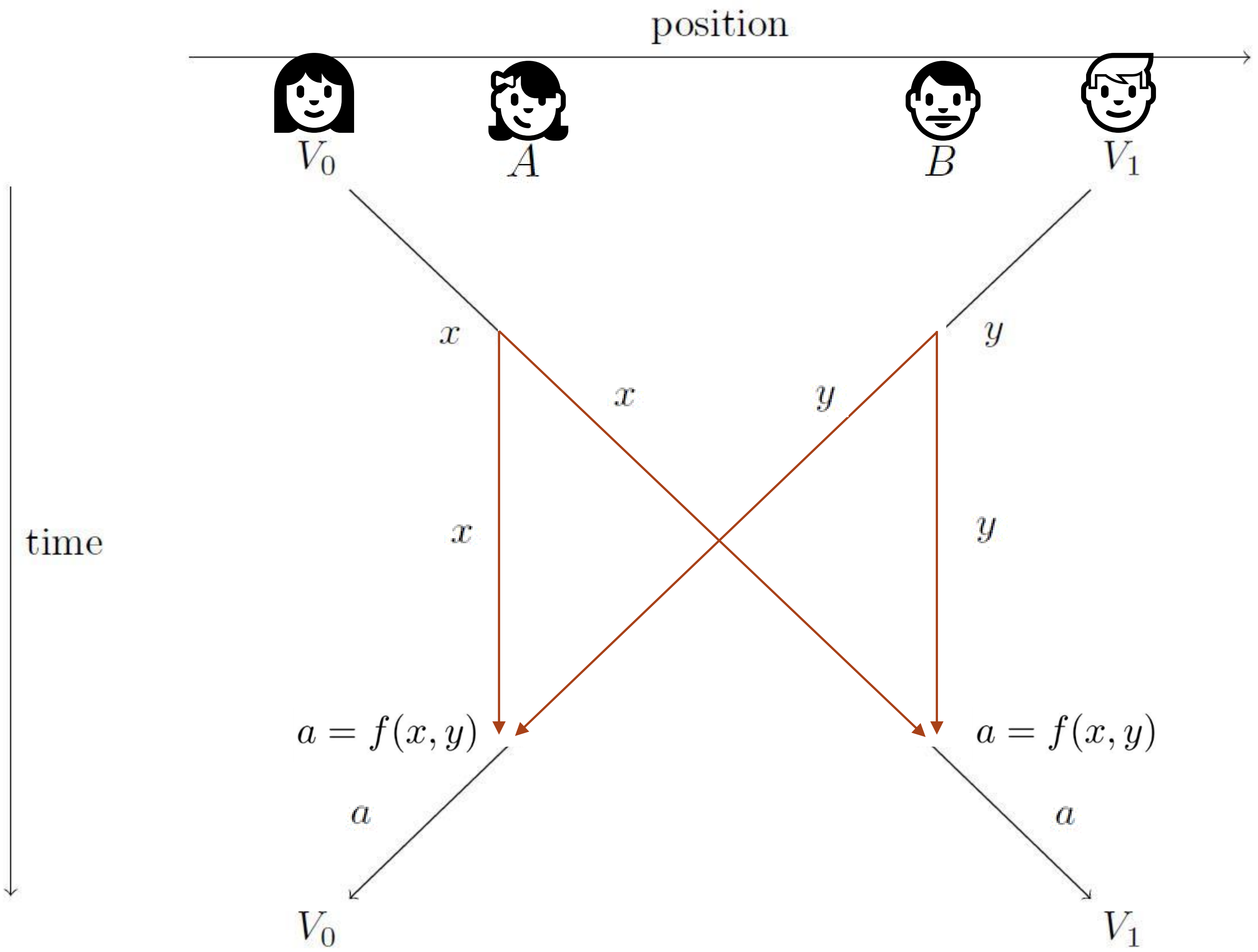
Classical universal attack



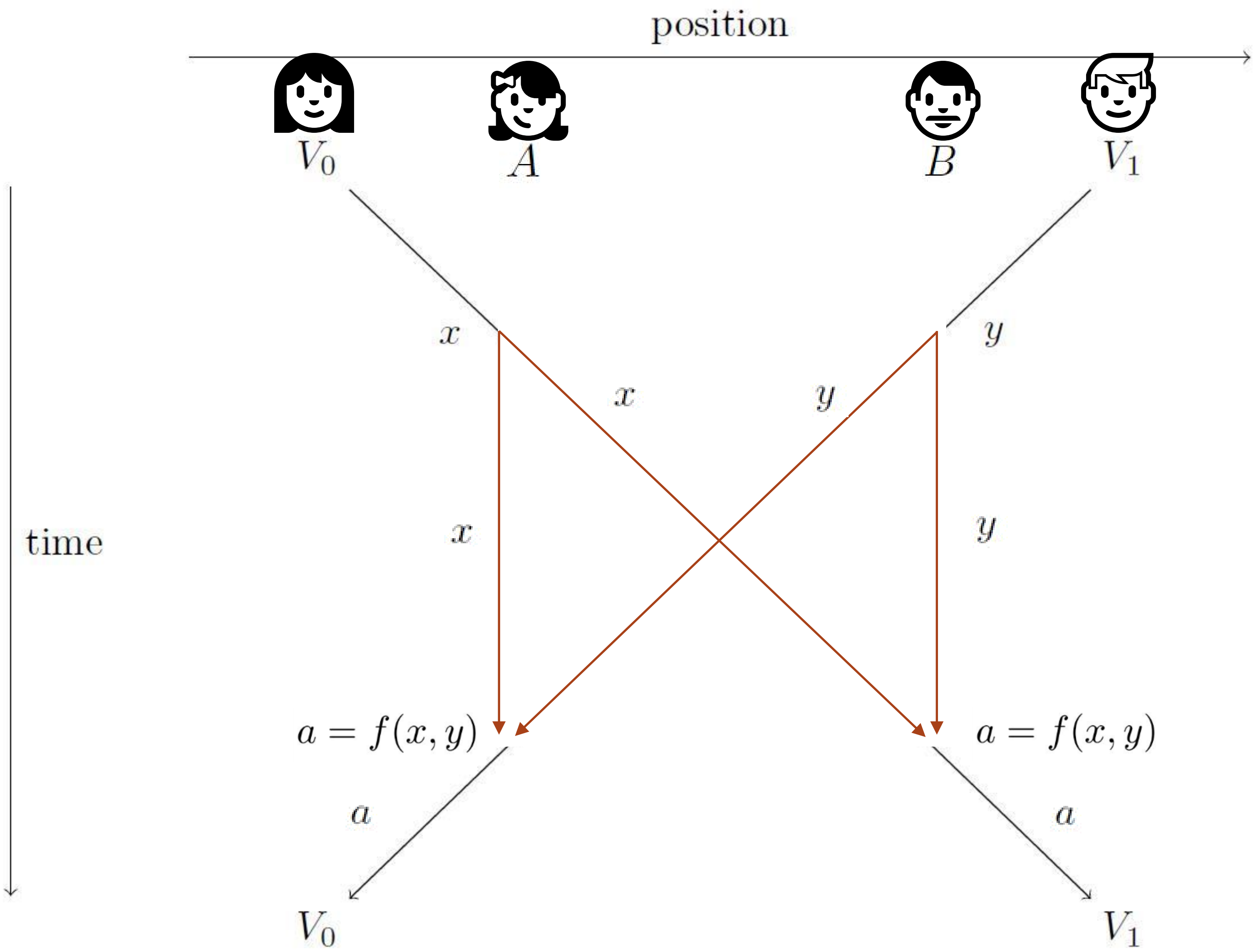
Classical universal attack



Classical universal attack

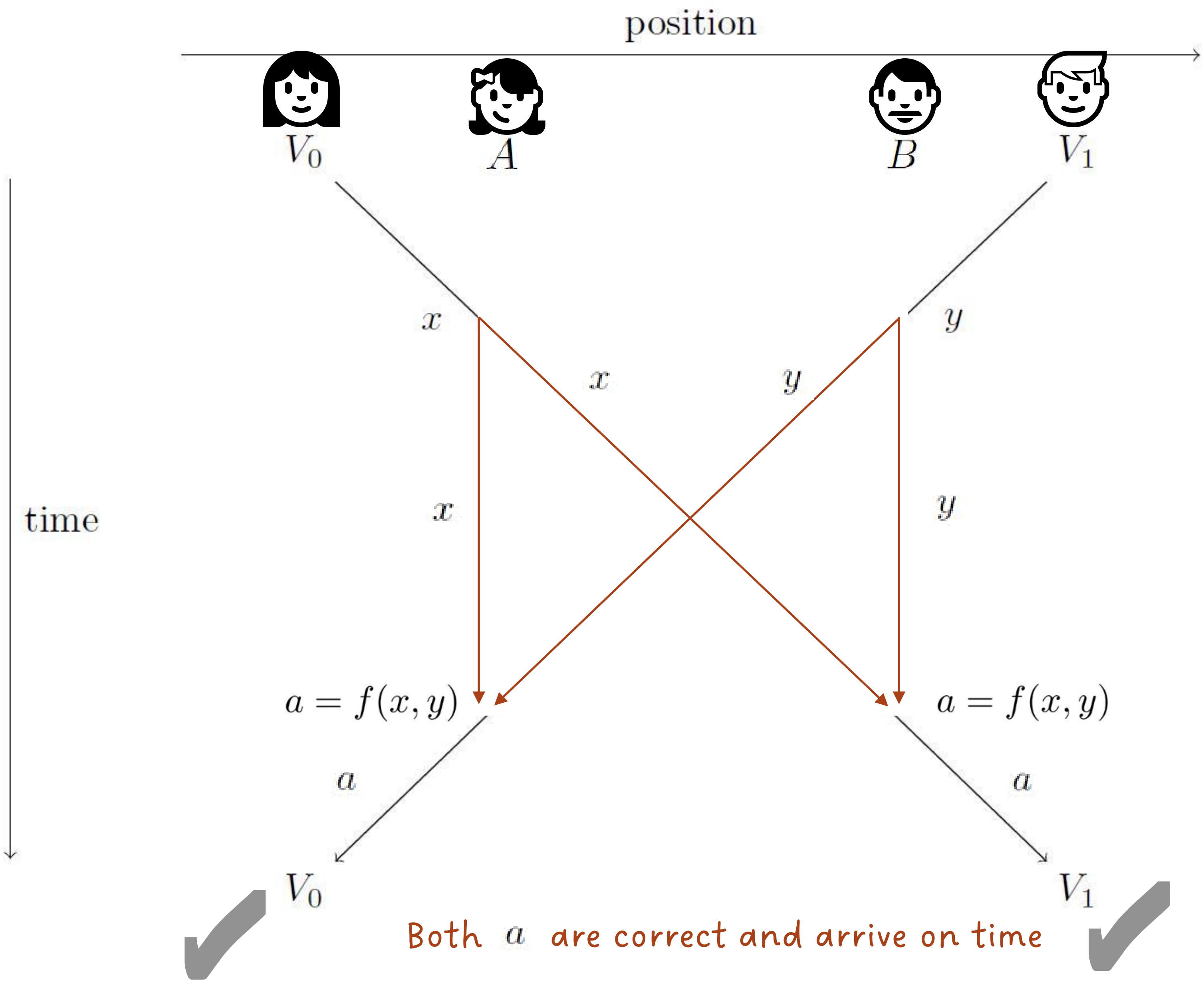


Classical universal attack



Both a are correct and arrive on time

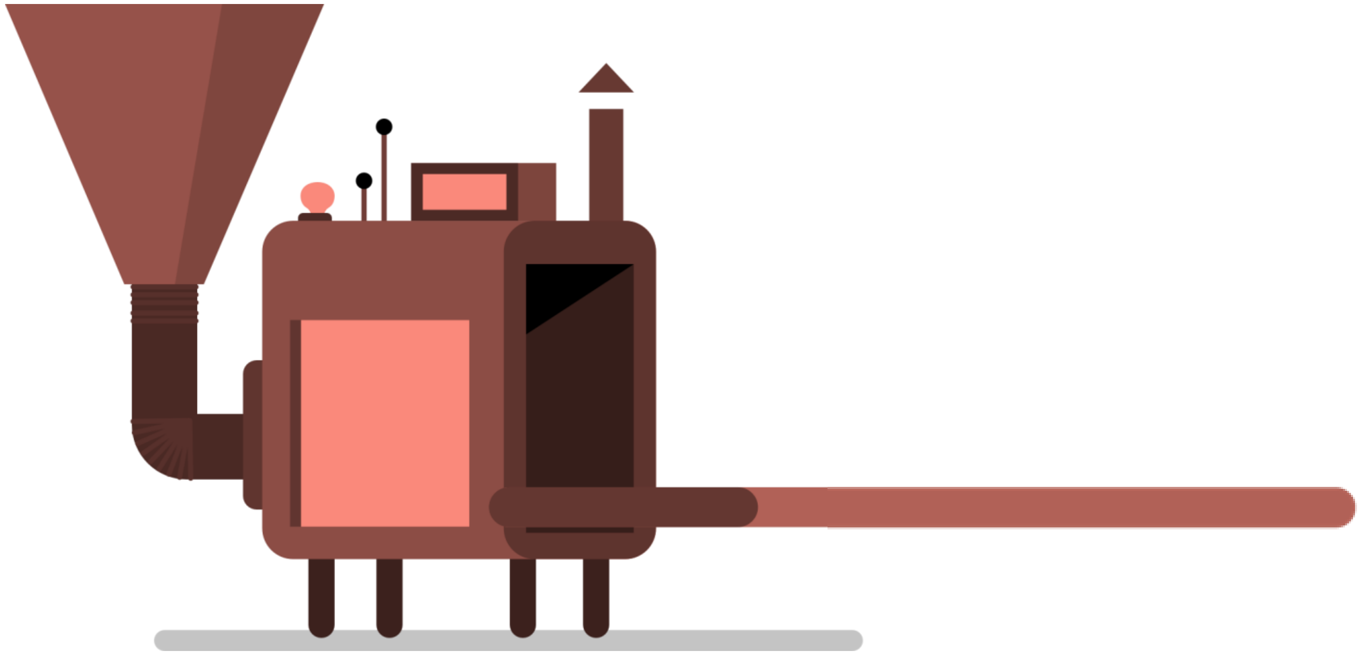
Classical universal attack



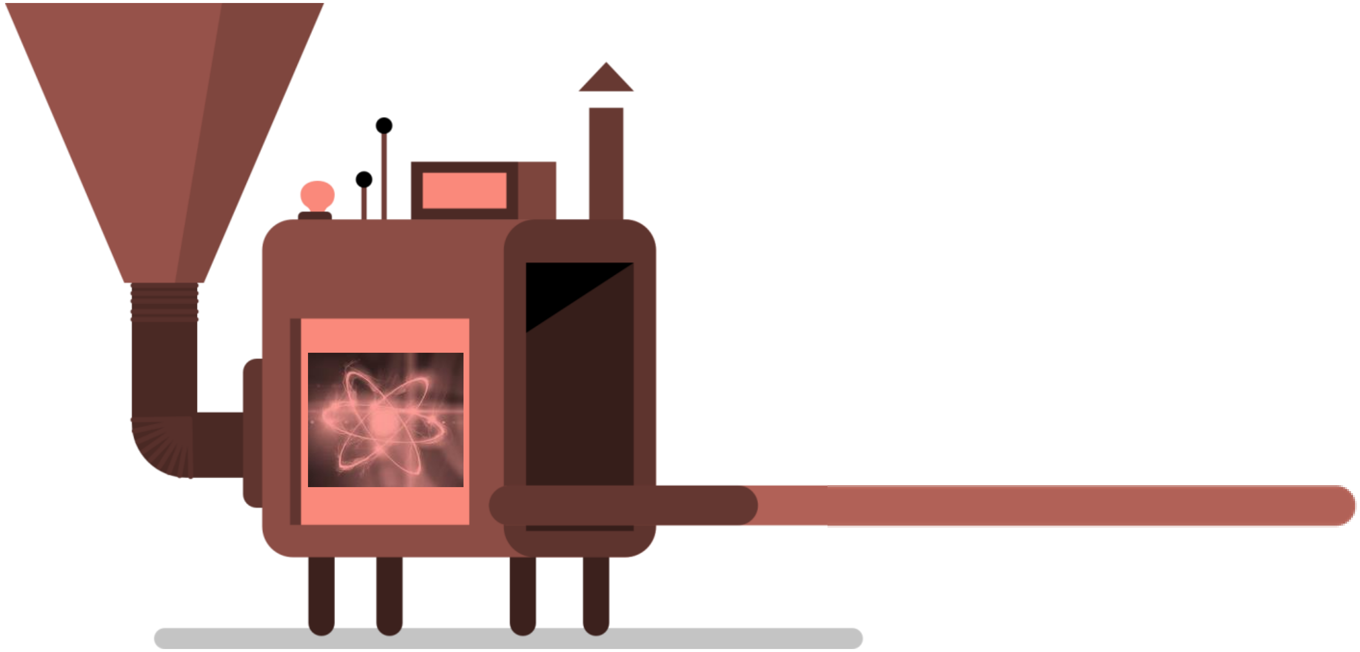
Both a are correct and arrive on time

No-cloning theorem

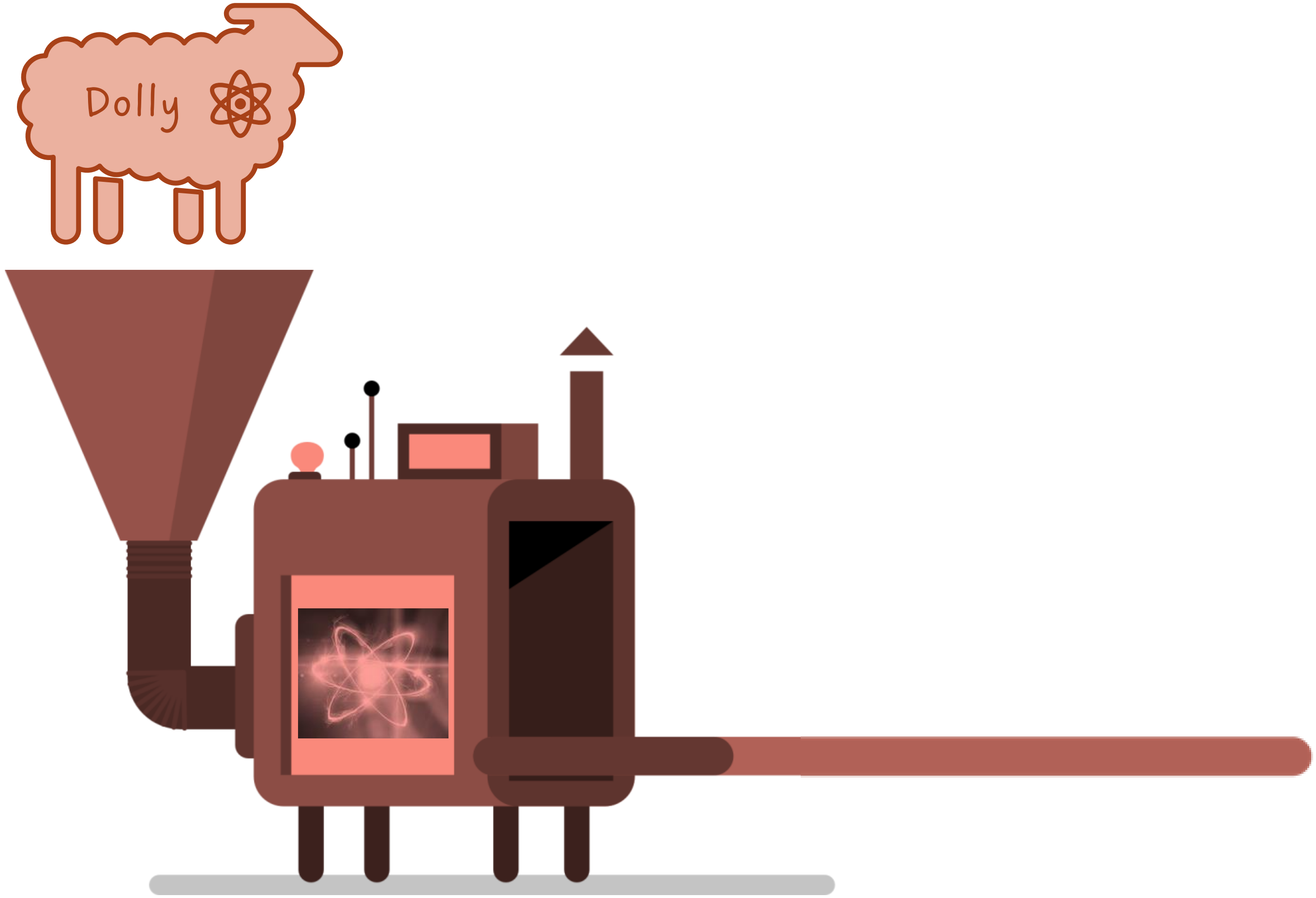
No-cloning theorem



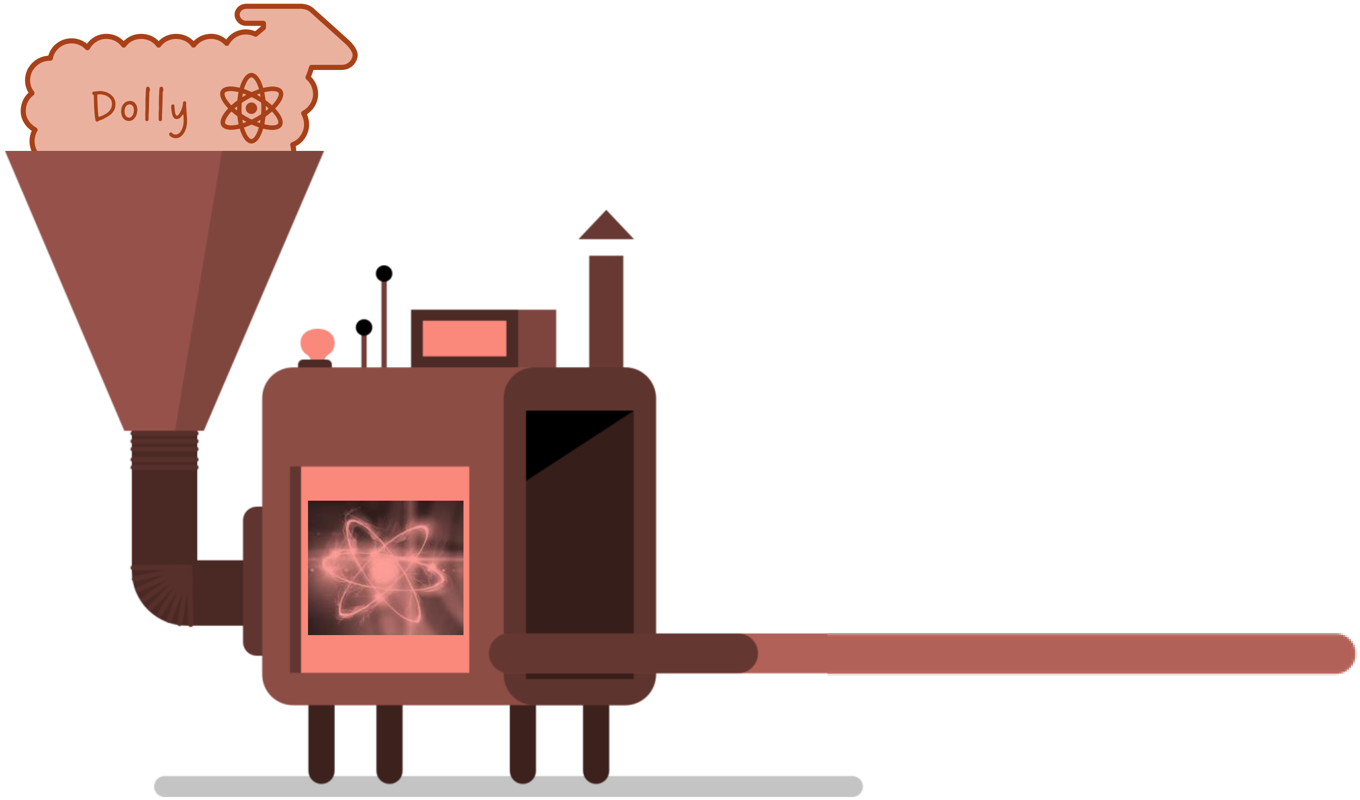
No-cloning theorem



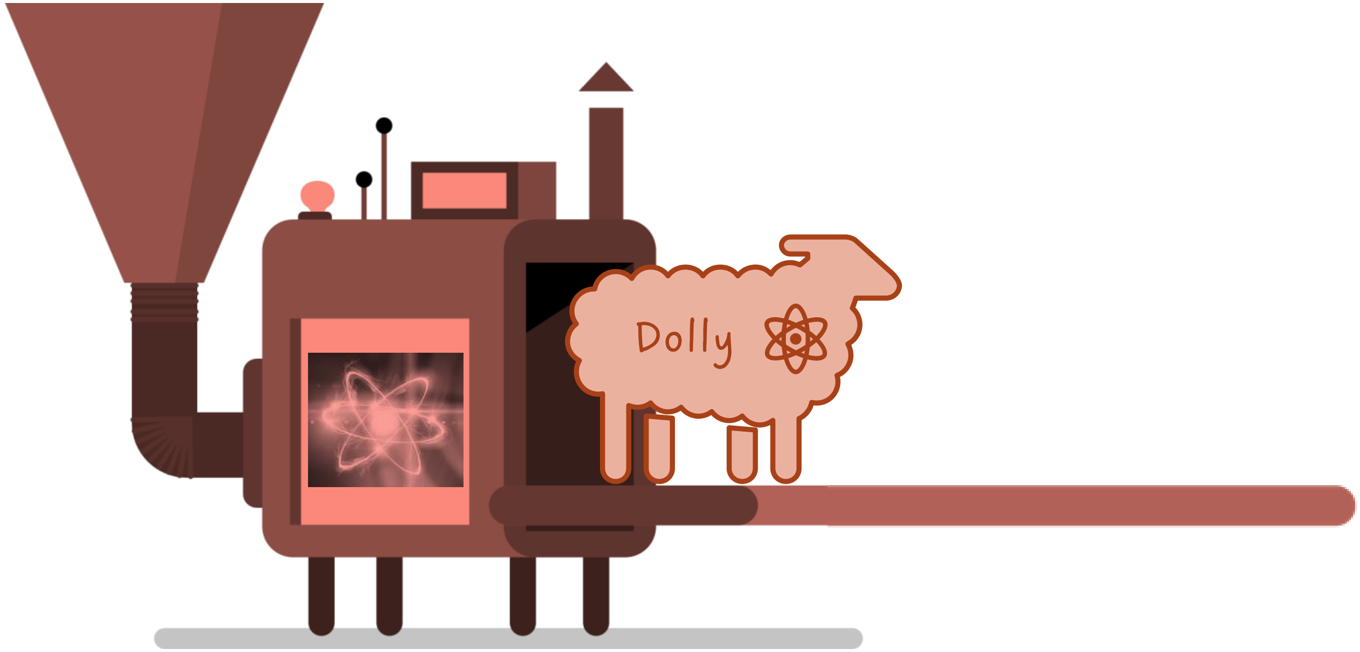
No-cloning theorem



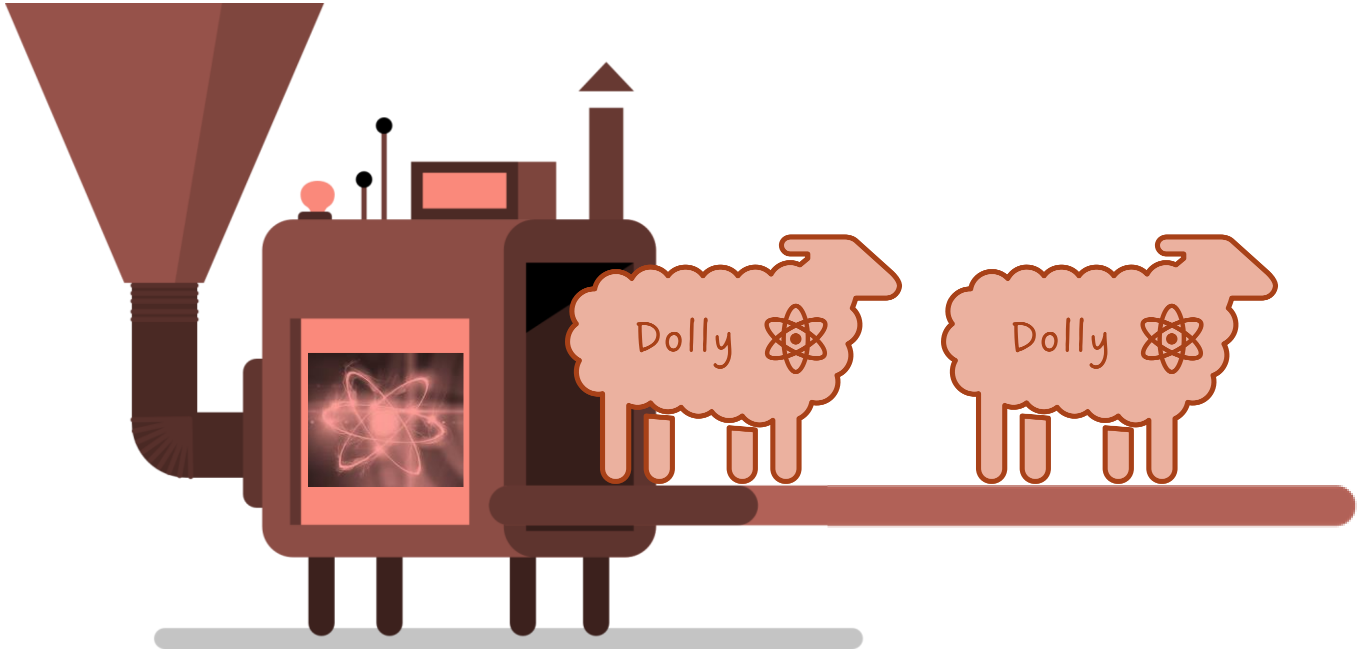
No-cloning theorem



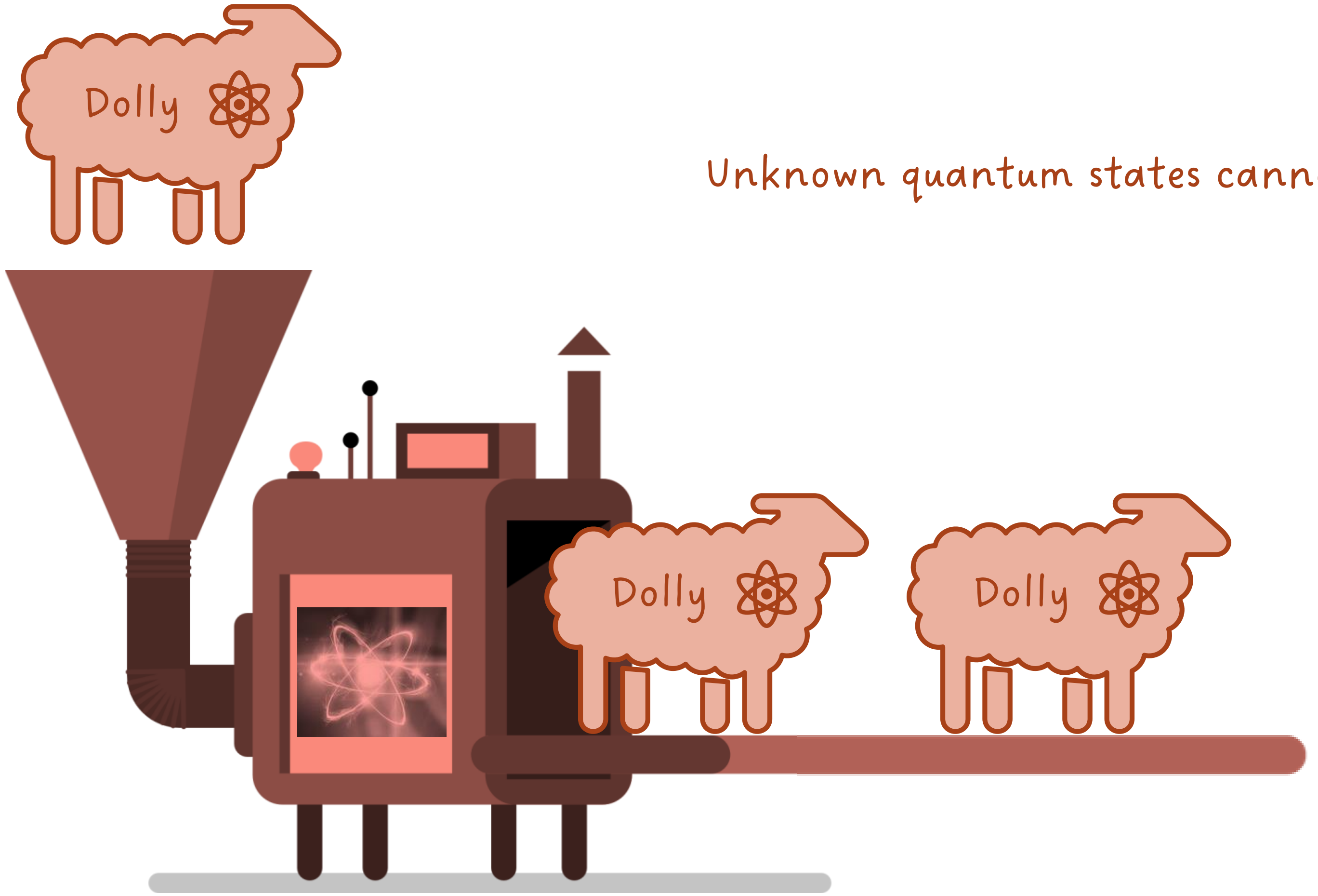
No-cloning theorem



No-cloning theorem



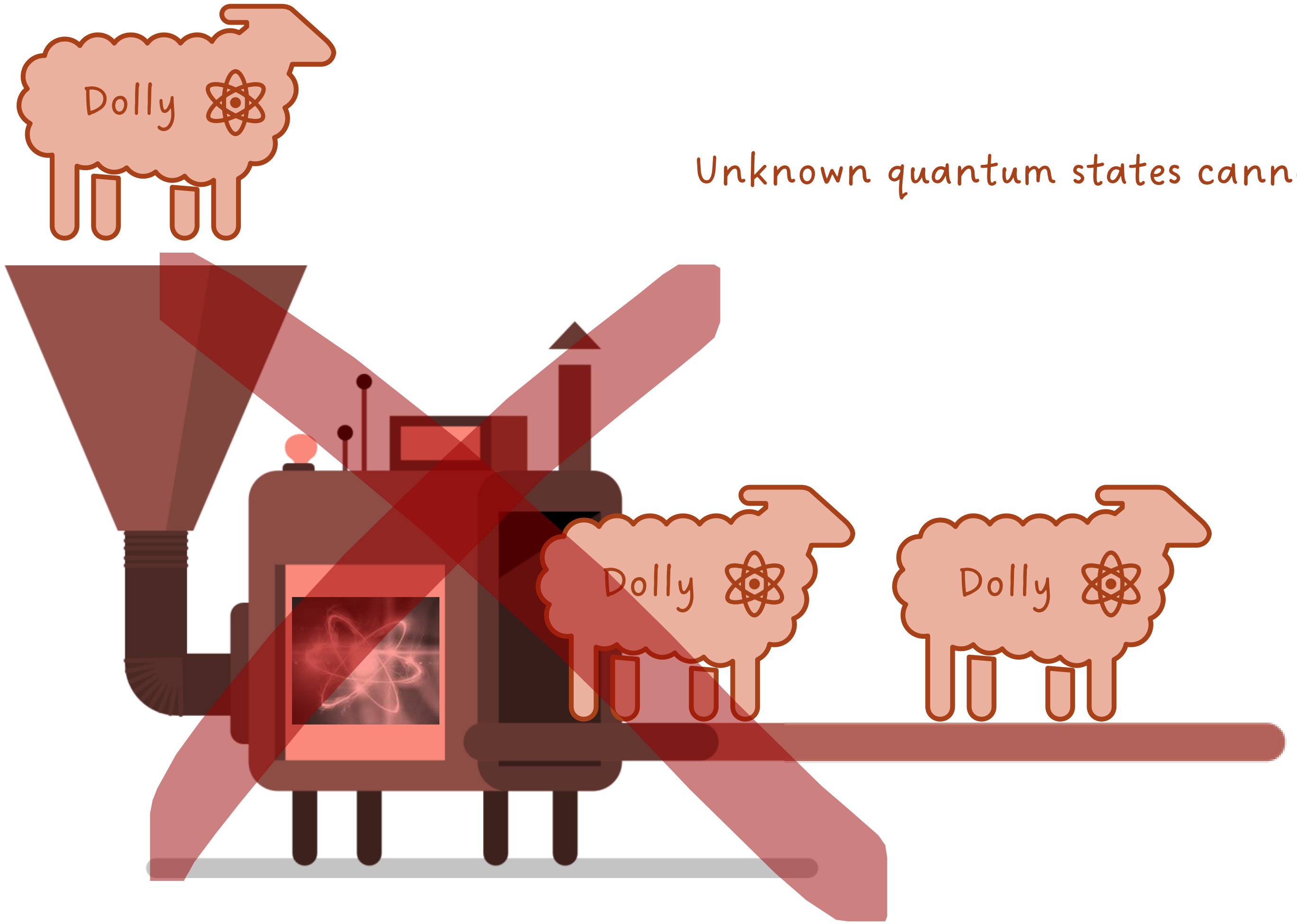
No-cloning theorem



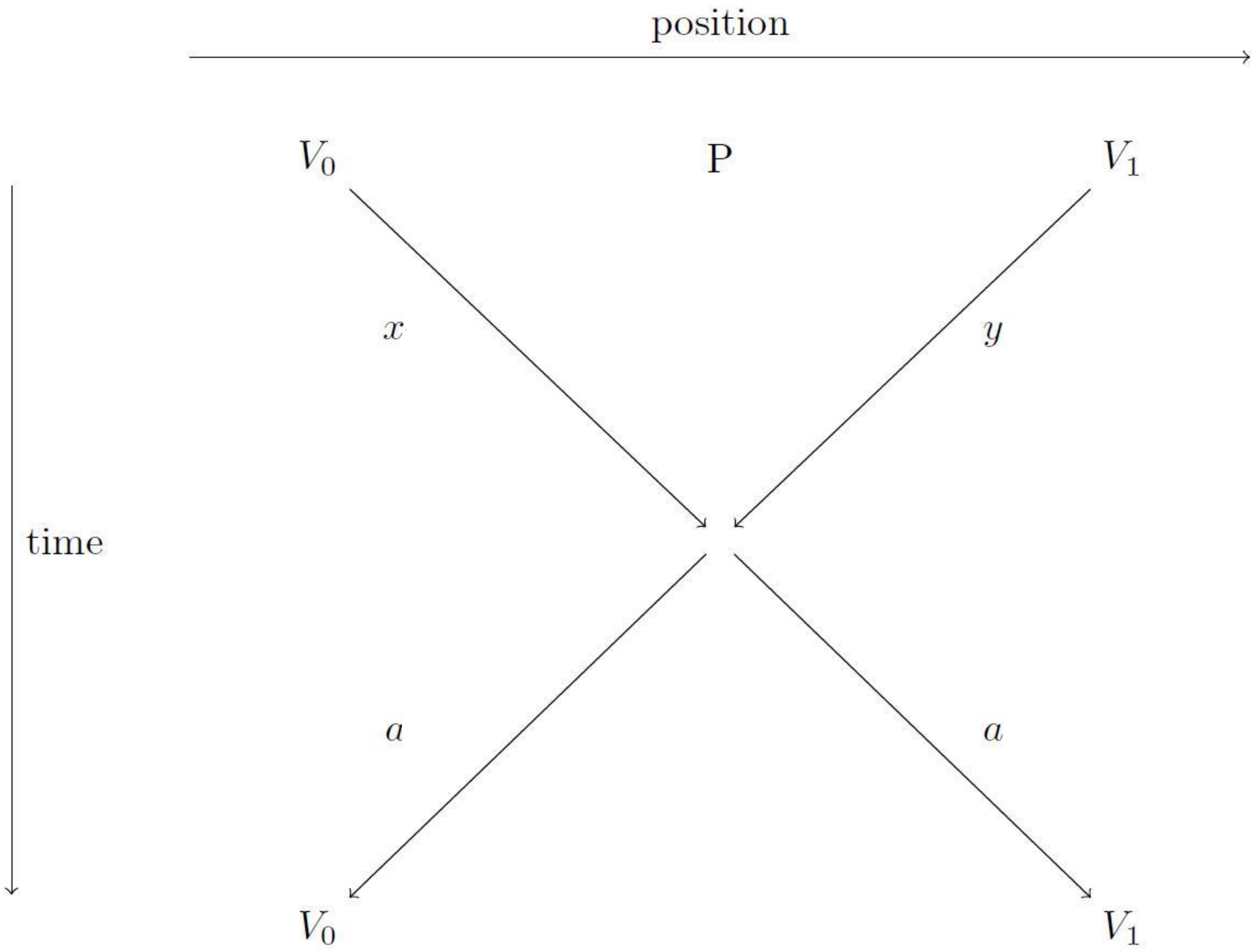
Unknown quantum states cannot be copied

No-cloning theorem

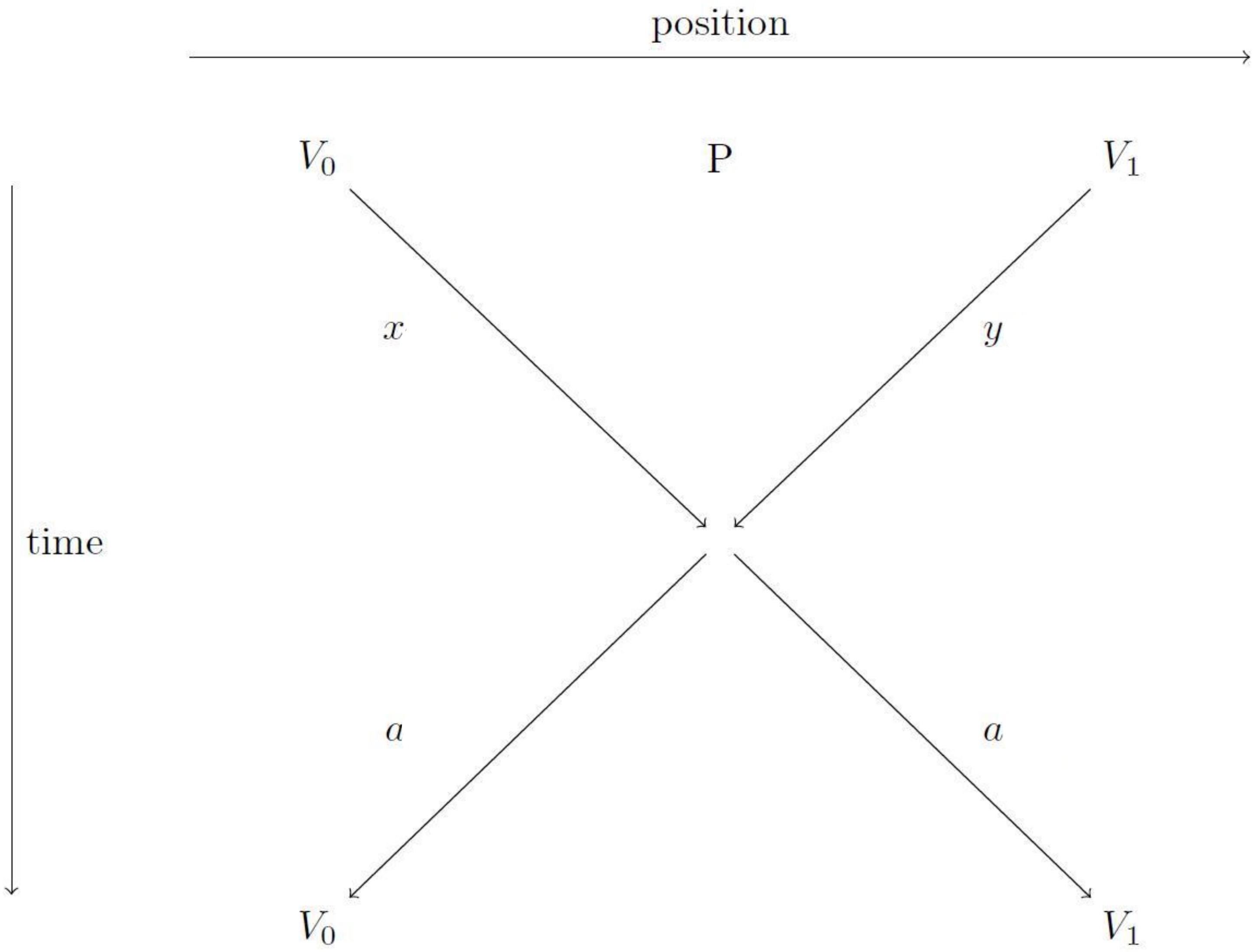
Unknown quantum states cannot be copied



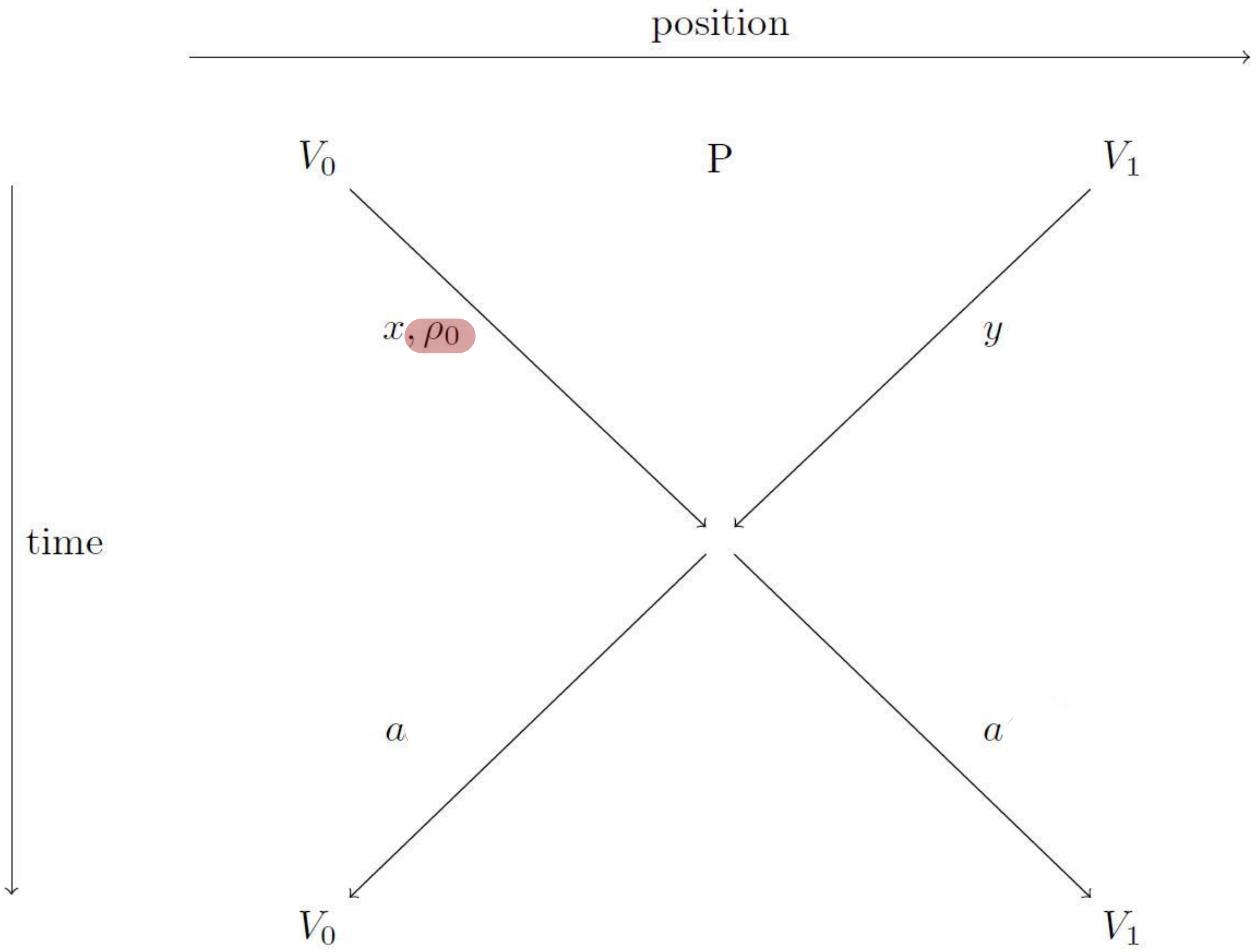
Position Verification (PV)



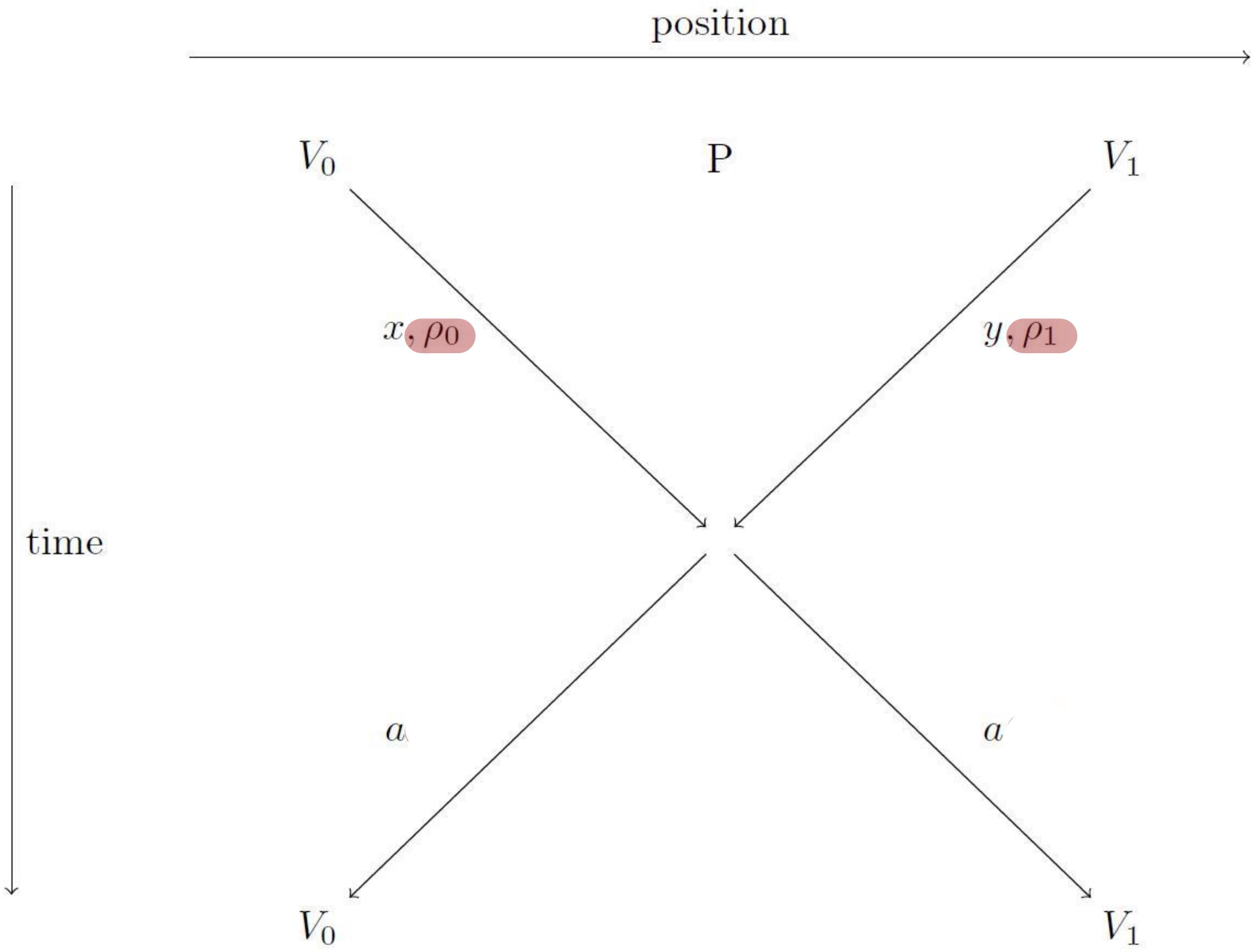
Quantum Position Verification (QPV)



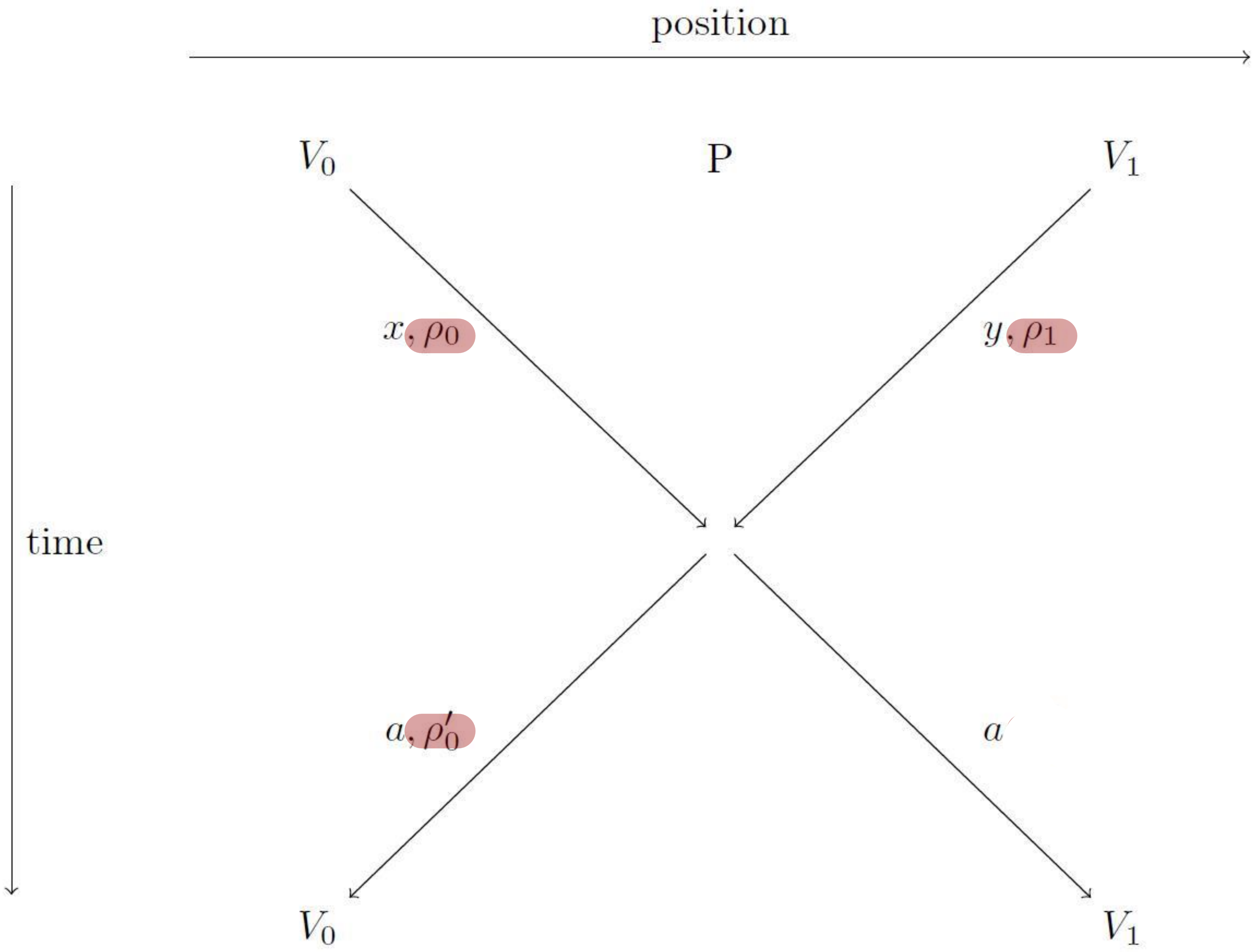
Quantum Position Verification (QPV)



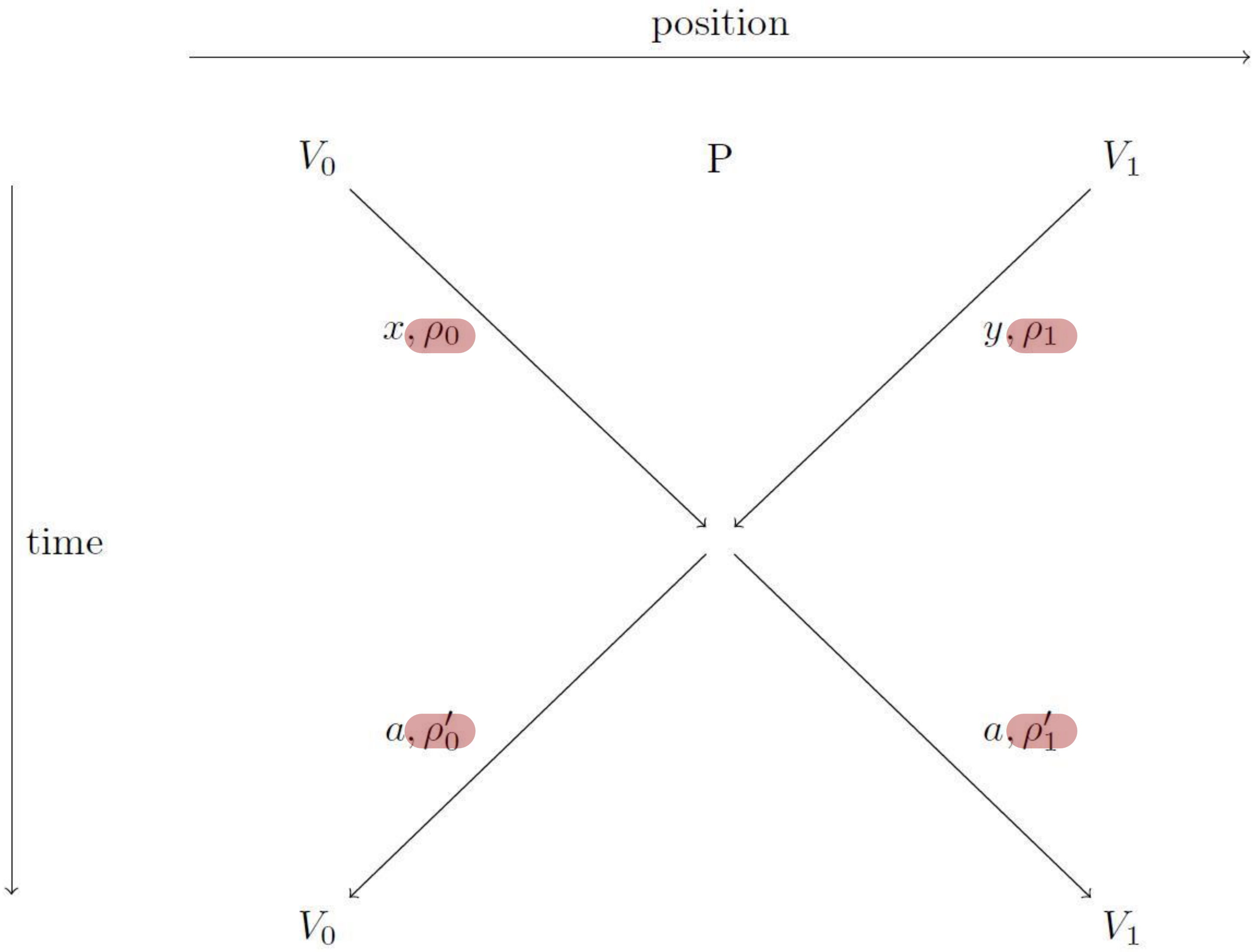
Quantum Position Verification (QPV)



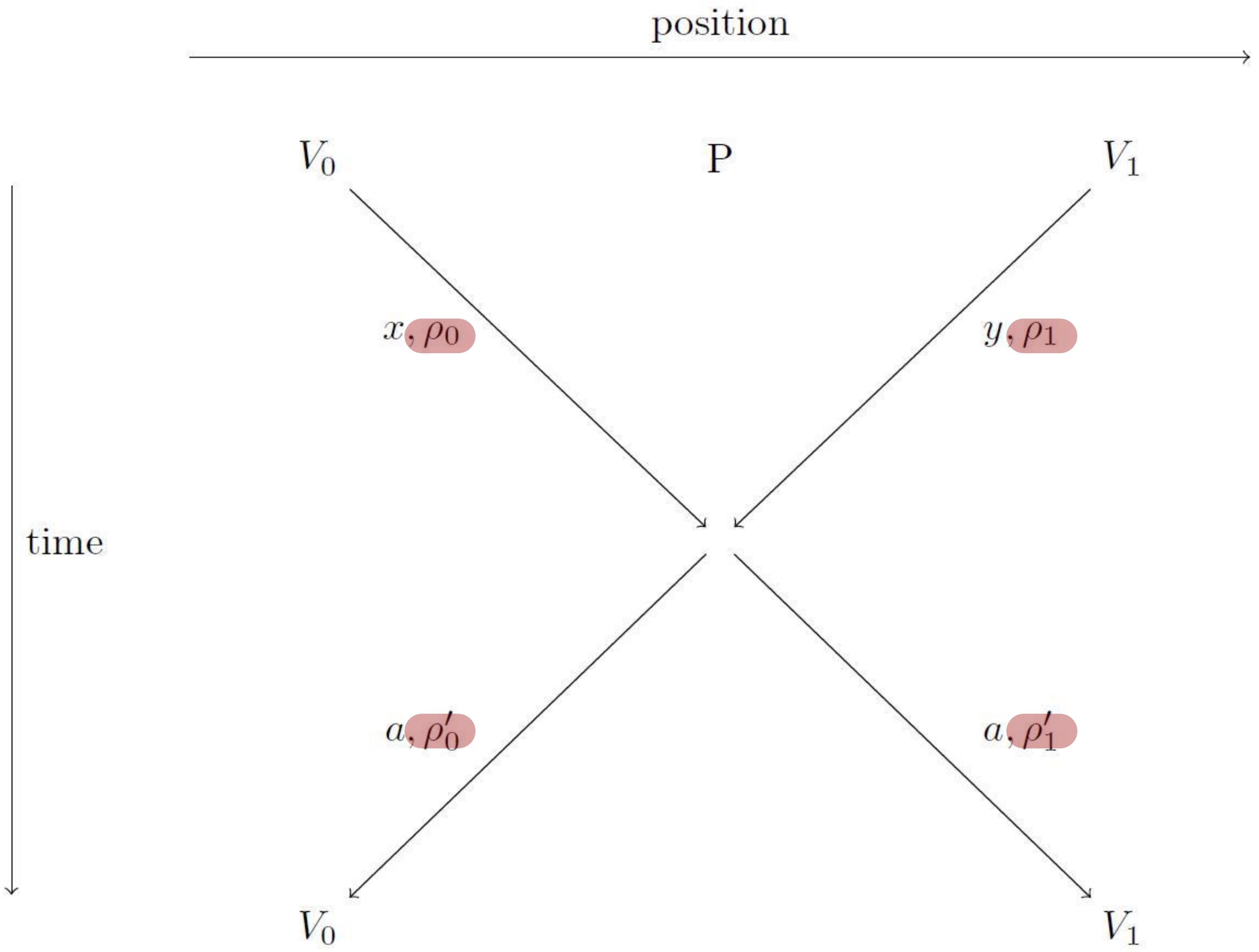
Quantum Position Verification (QPV)



Quantum Position Verification (QPV)

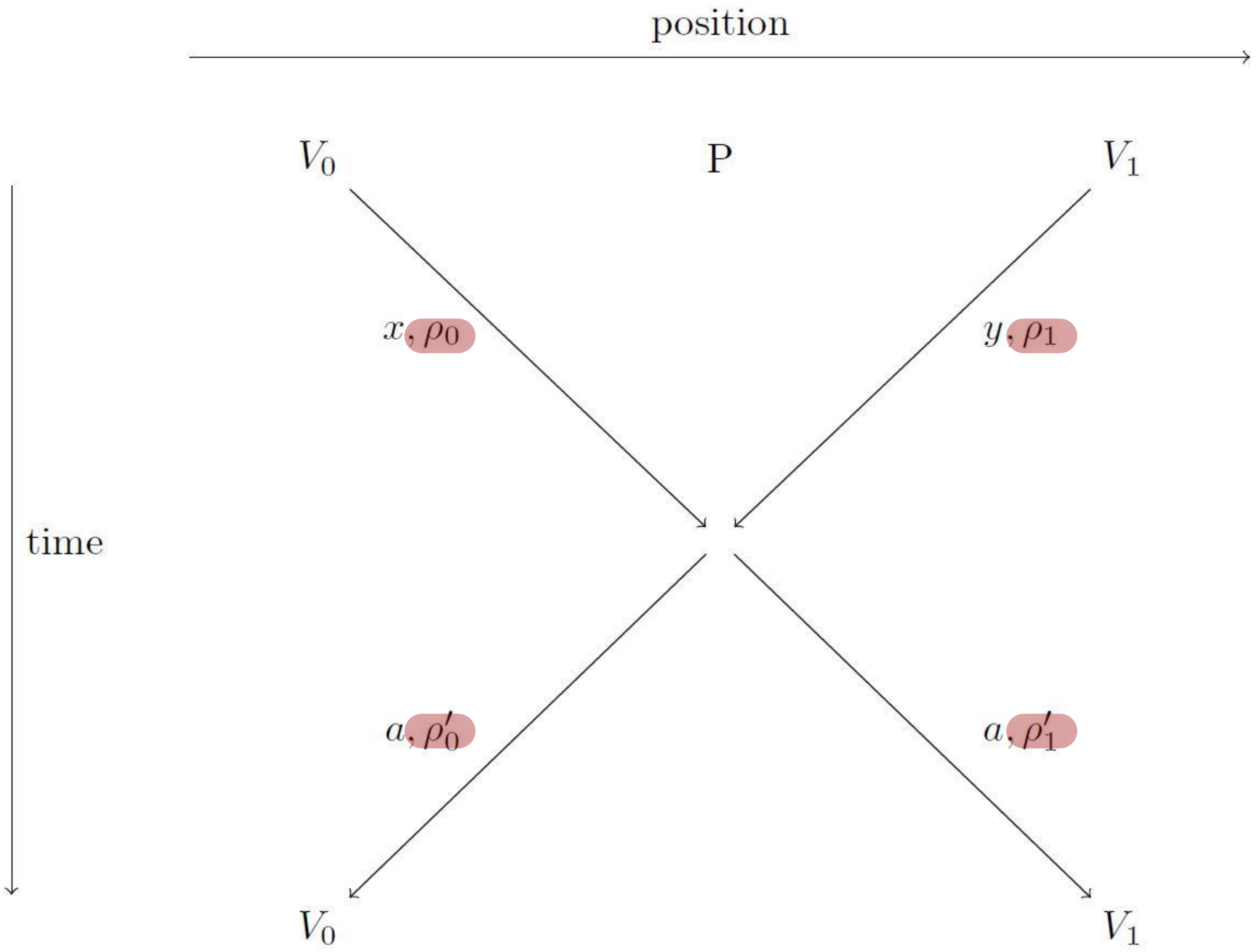


Quantum Position Verification (QPV)

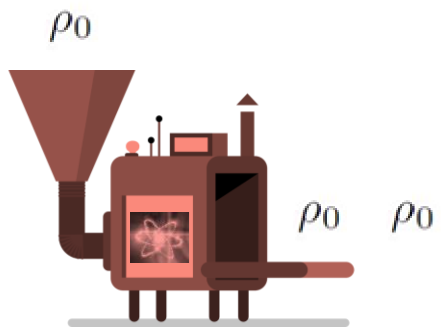


This prevents copying attacks

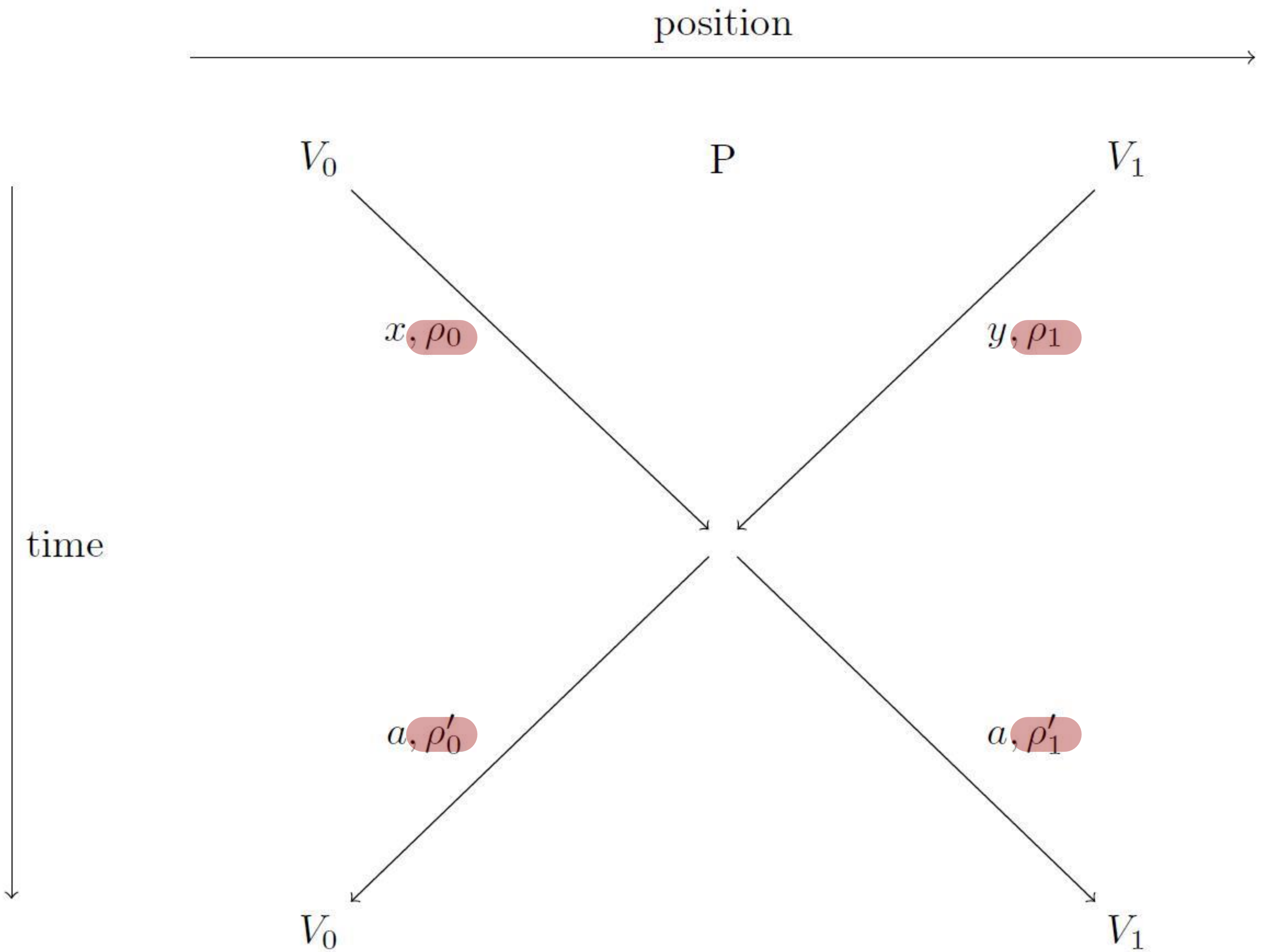
Quantum Position Verification (QPV)



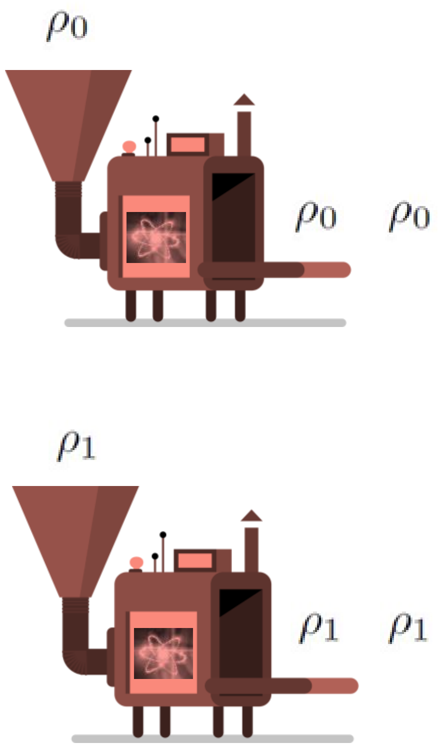
This prevents copying attacks



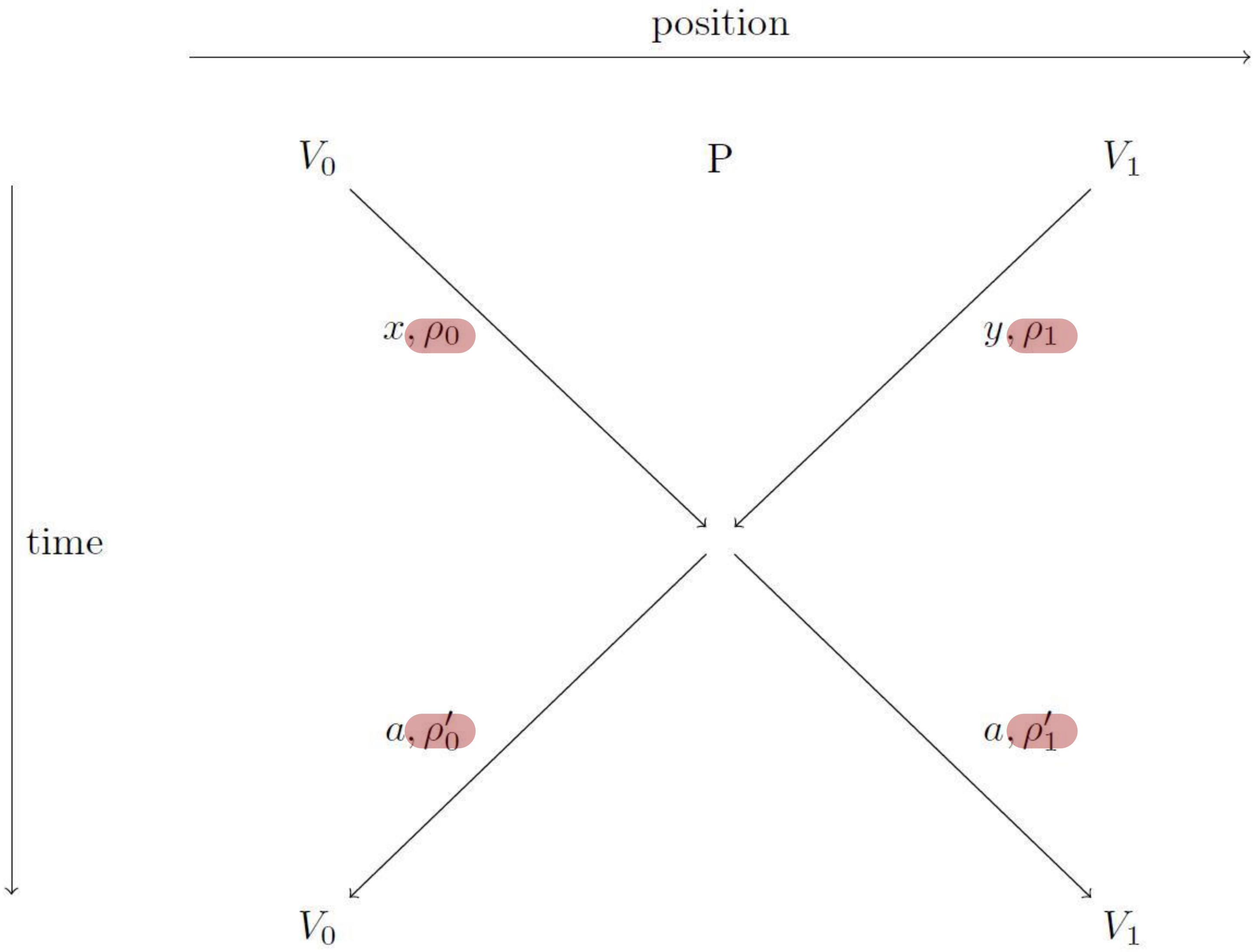
Quantum Position Verification (QPV)



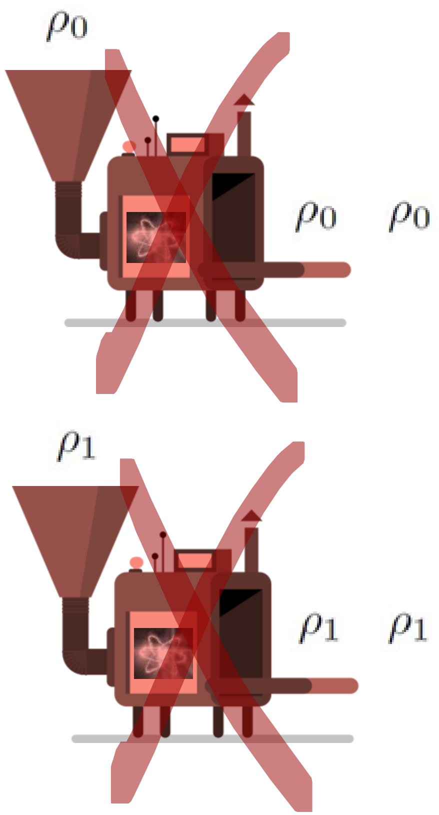
This prevents copying attacks



Quantum Position Verification (QPV)



This prevents copying attacks

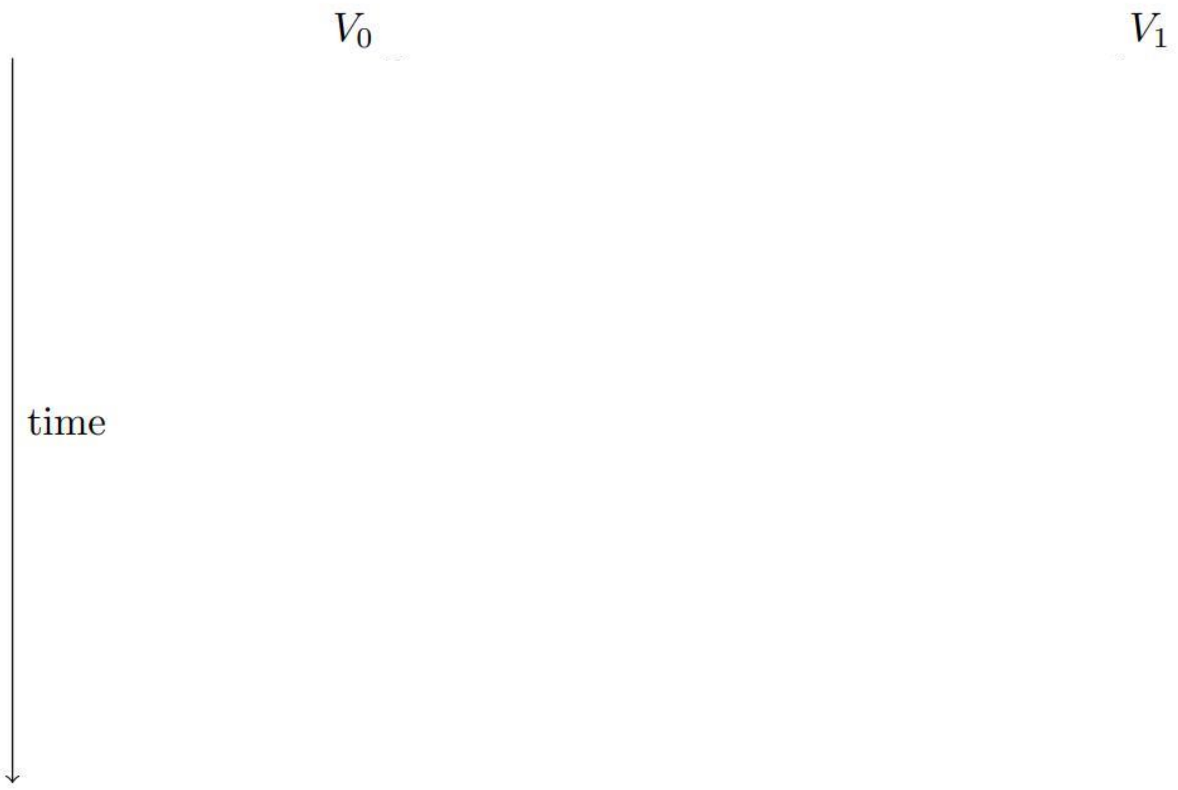


A concrete QPV protocol

$\mathrm{QPV}_{\mathrm{BB84}}$

Kent, Munro, and Spiller [KMS11]

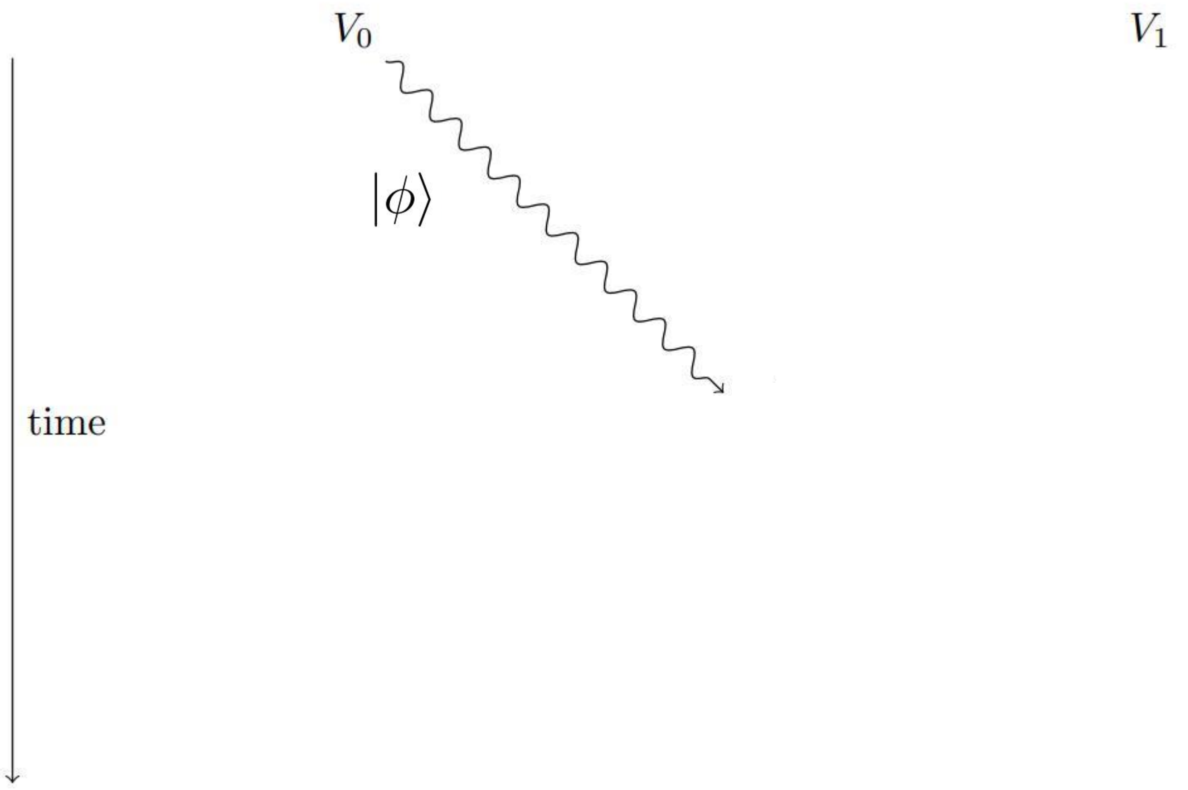
$|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



$\mathrm{QPV}_{\mathrm{BB84}}$

Kent, Munro, and Spiller [KMS11]

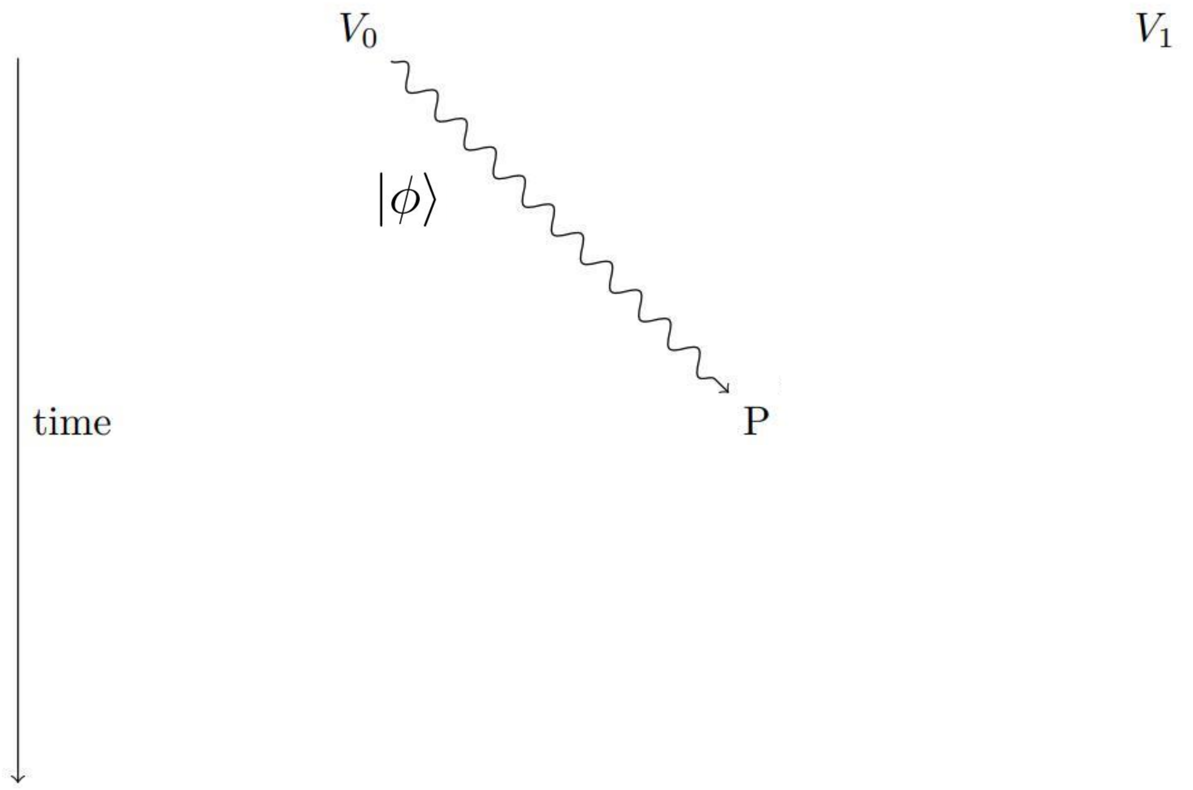
$|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



$\mathrm{QPV}_{\mathrm{BB84}}$

Kent, Munro, and Spiller [KMS11]

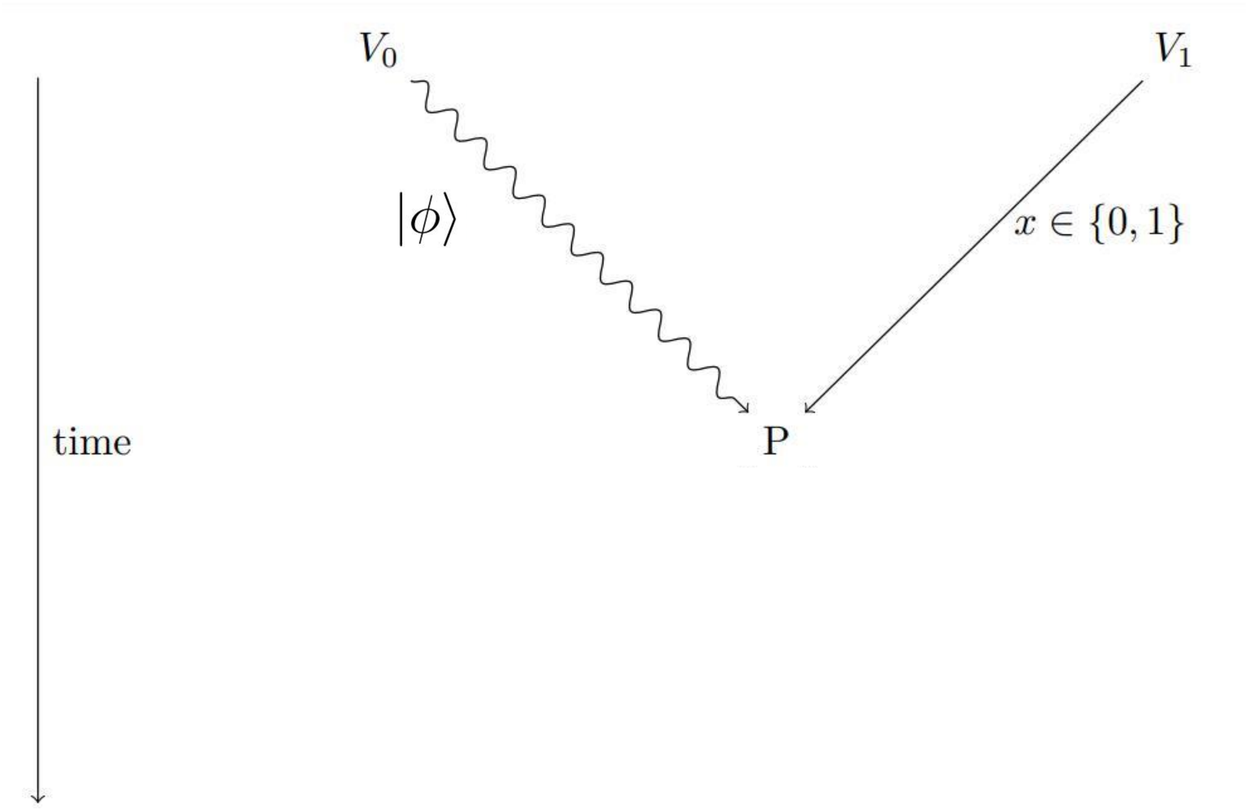
$|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



QPV_{BB84}

Kent, Munro, and Spiller [KMS11]

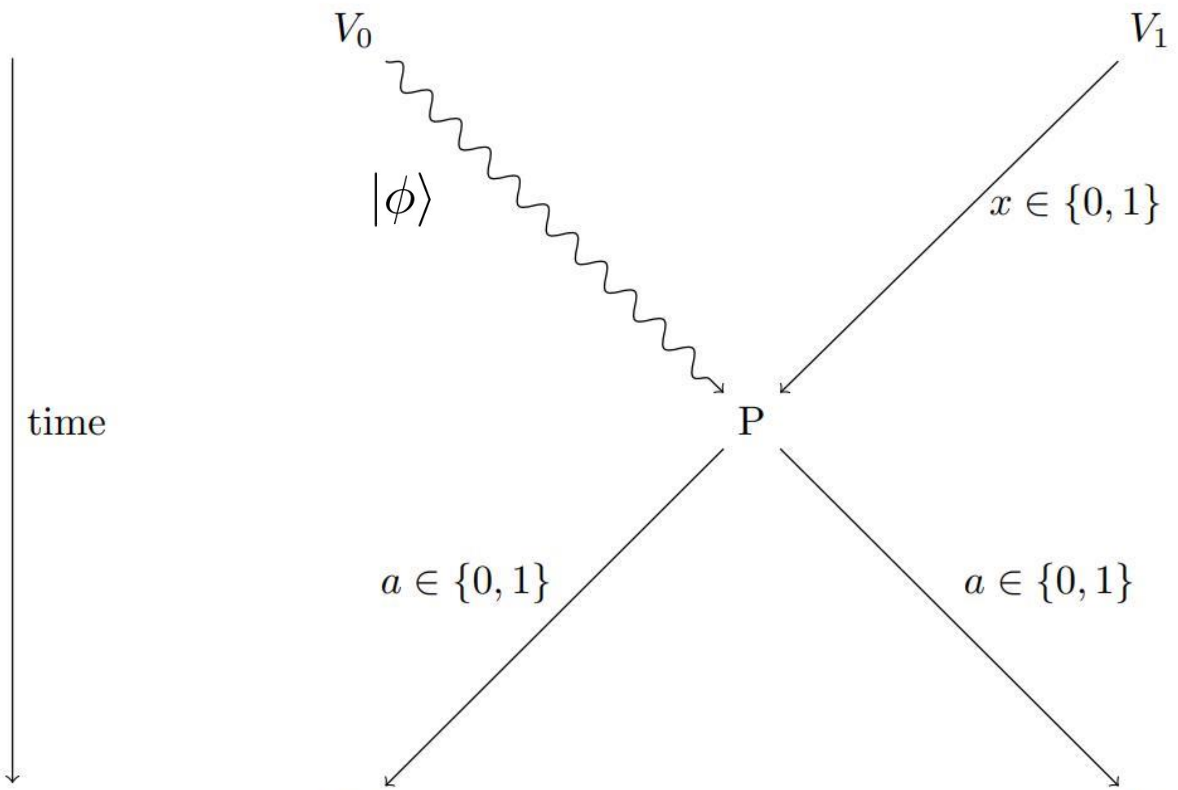
$|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



$\mathrm{QPV}_{\mathrm{BB84}}$

Kent, Munro, and Spiller [KMS11]

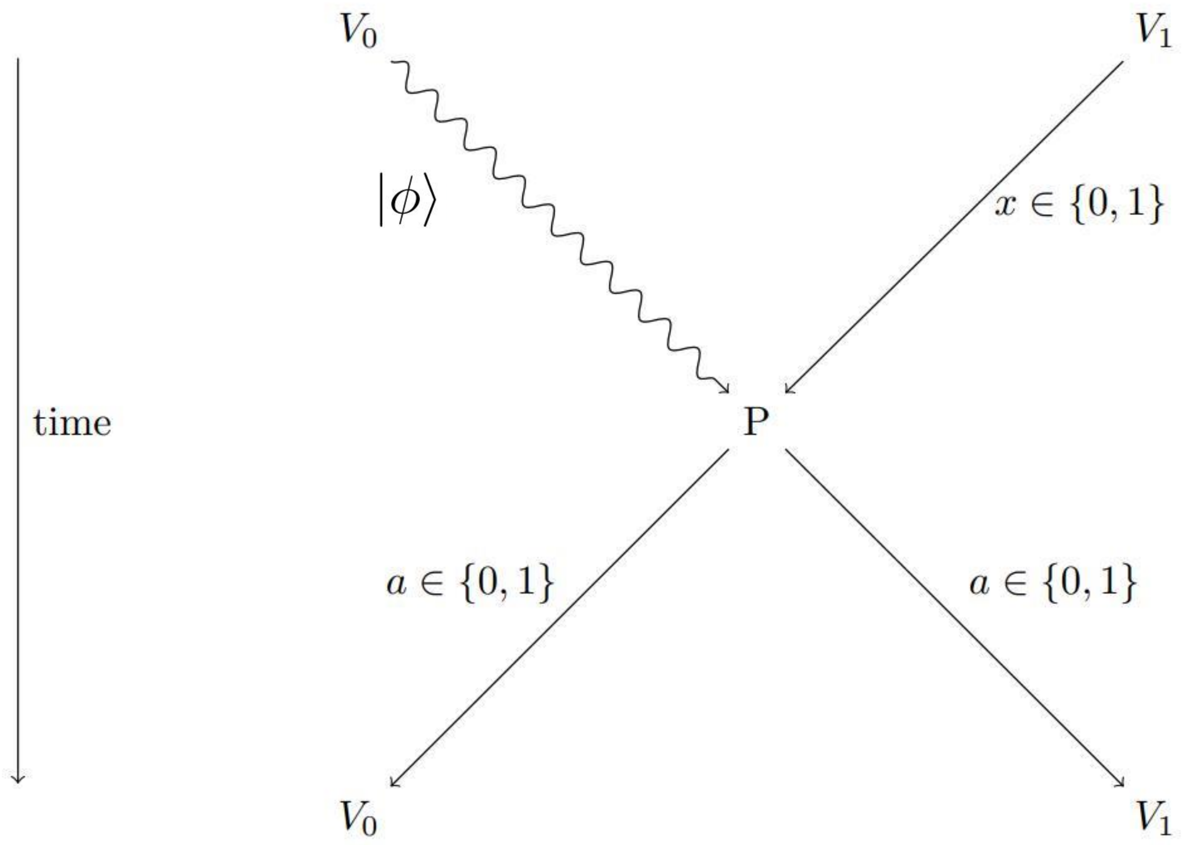
$|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



QPV_{BB84}

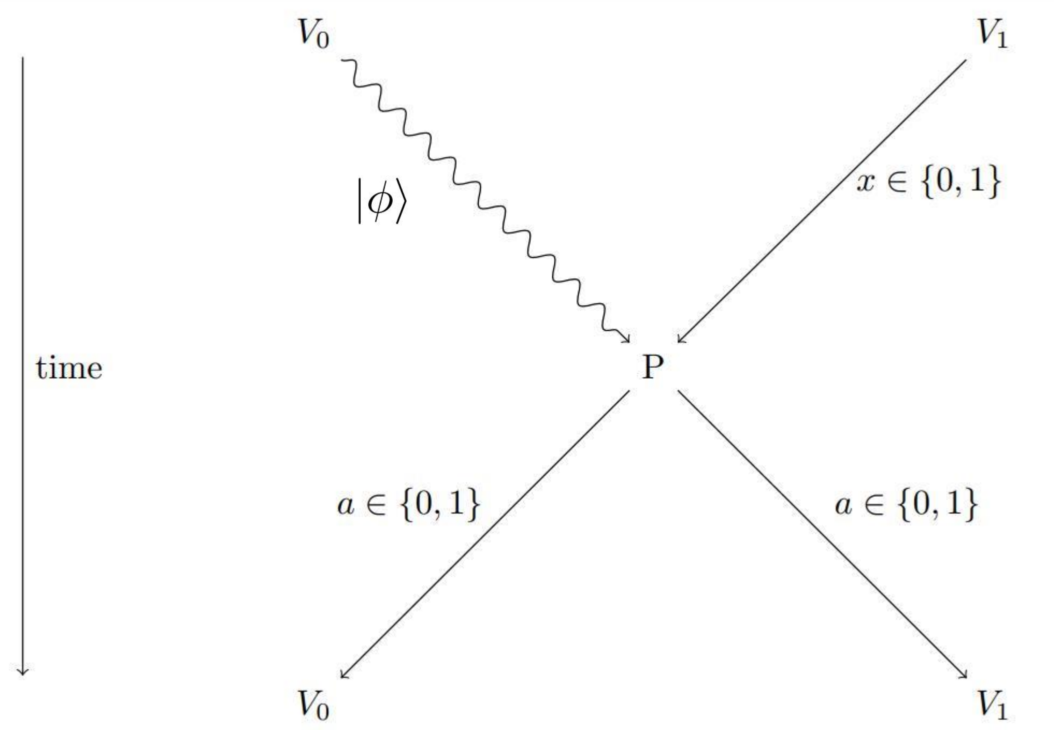
Kent, Munro, and Spiller [KMS11]

$|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$

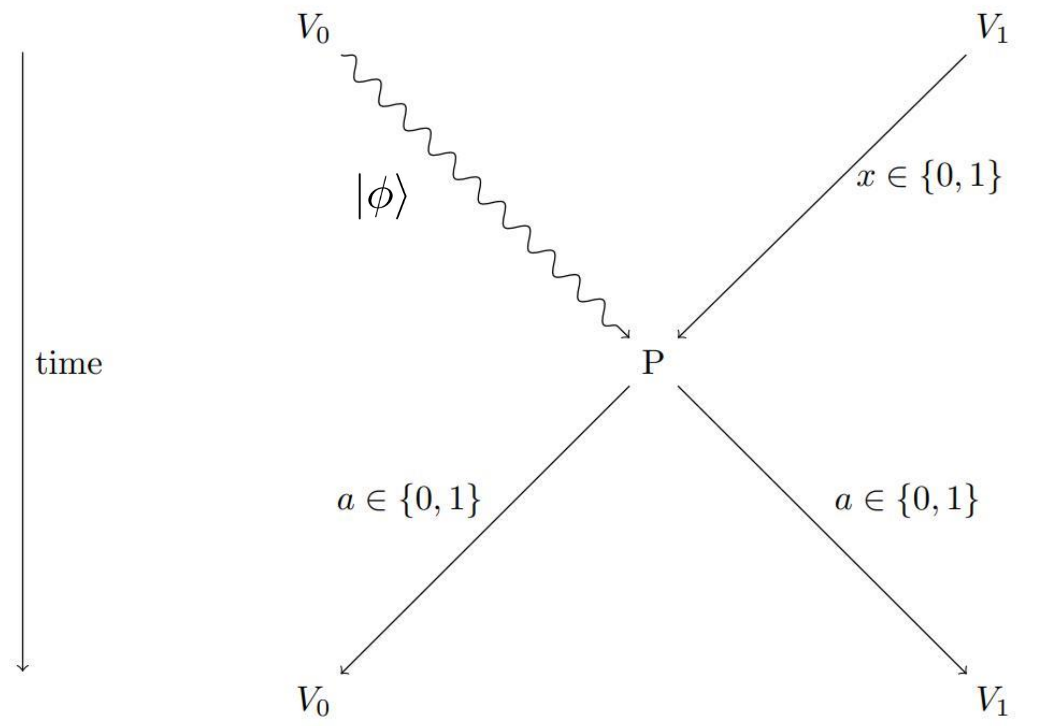


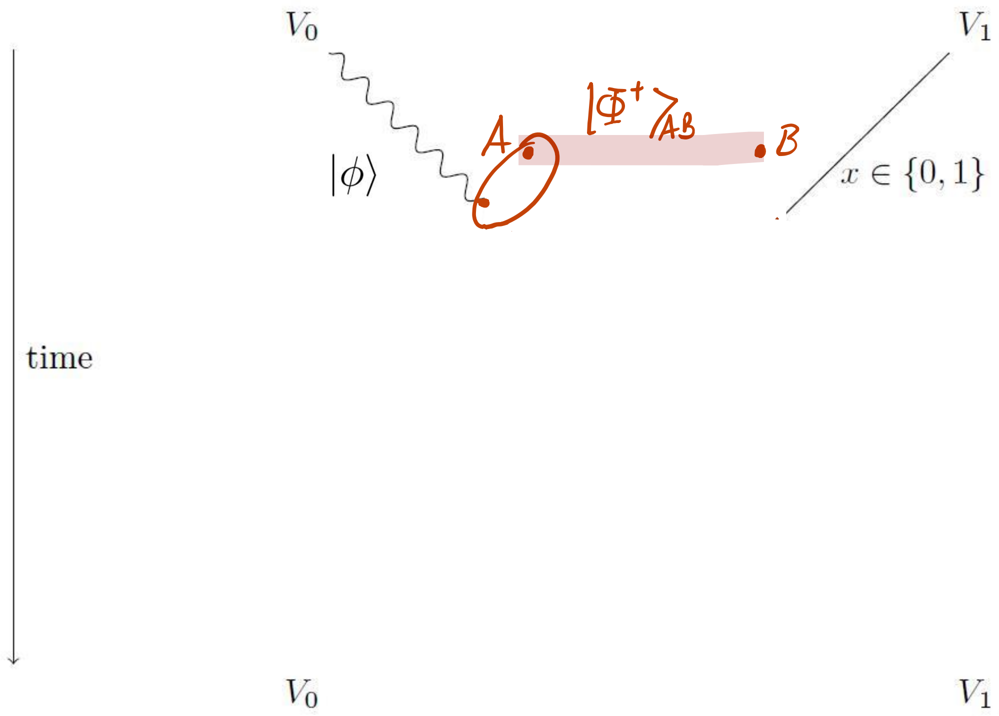
Attacks

Attack pre-sharing entanglement [KMS11]

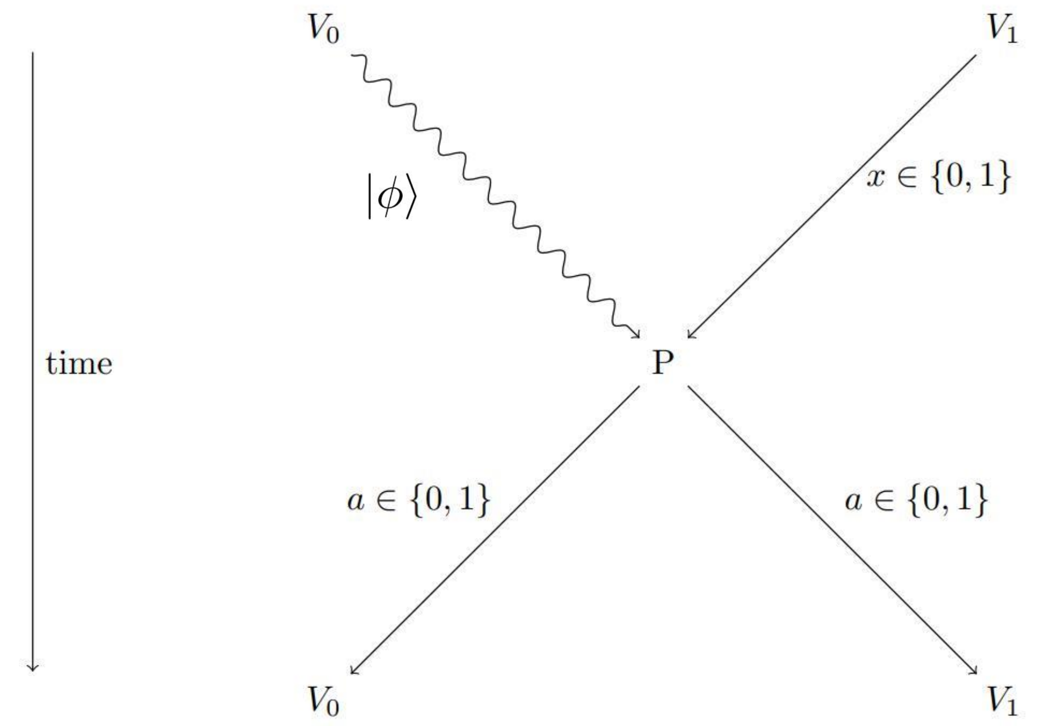


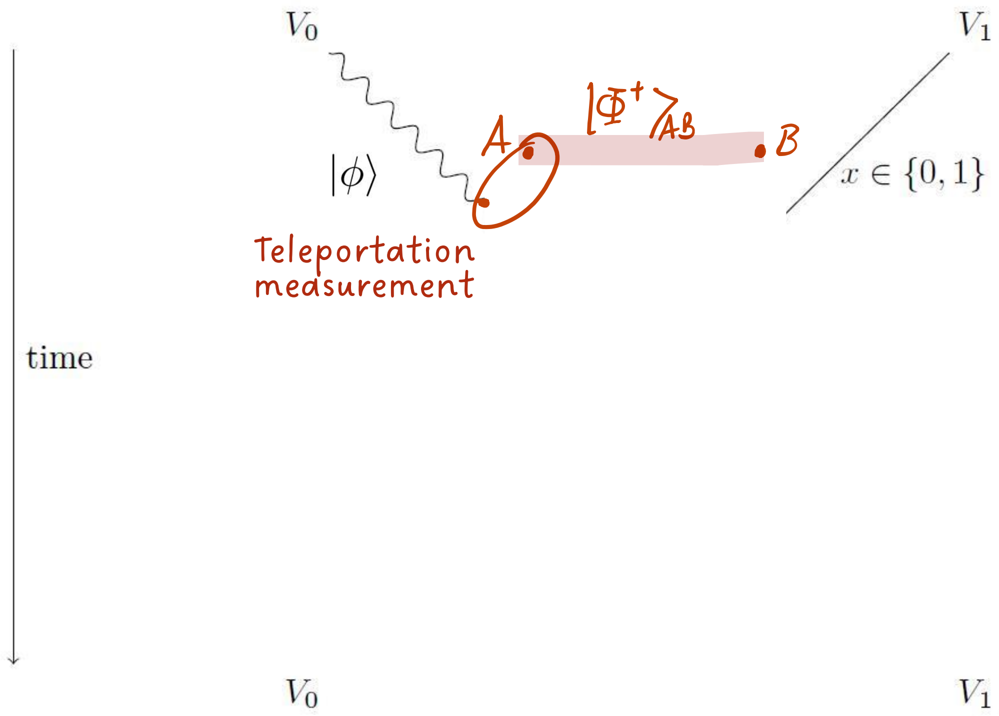
Attack pre-sharing entanglement [KMS11]



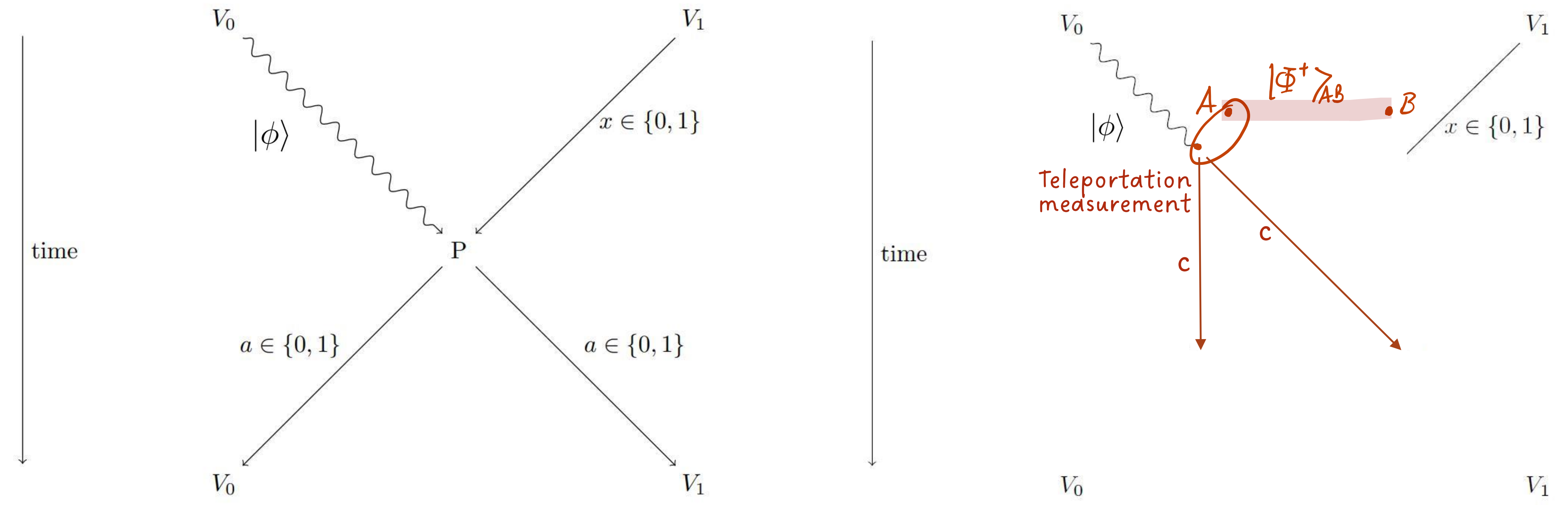


Attack pre-sharing entanglement [KMS11]

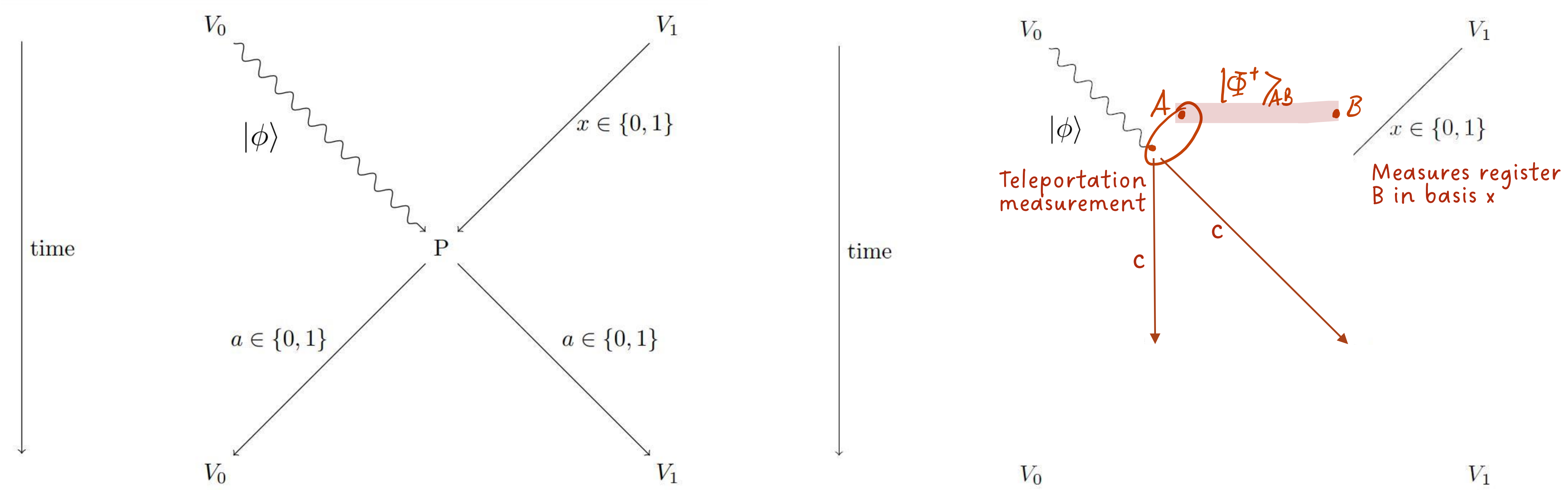




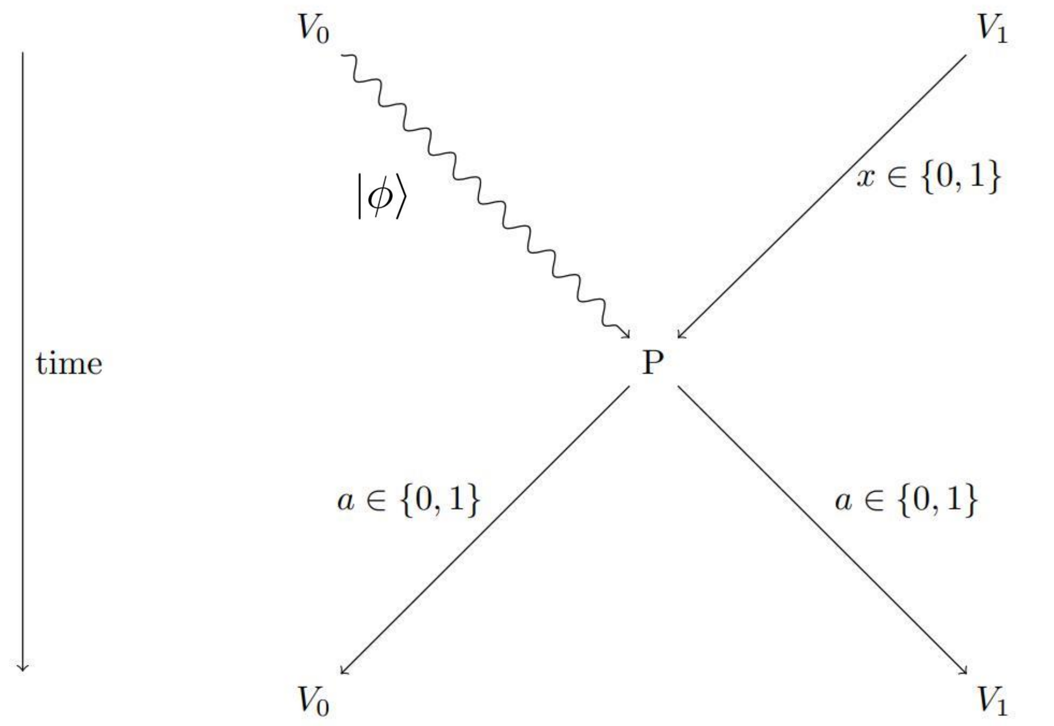
Attack pre-sharing entanglement [KMS11]

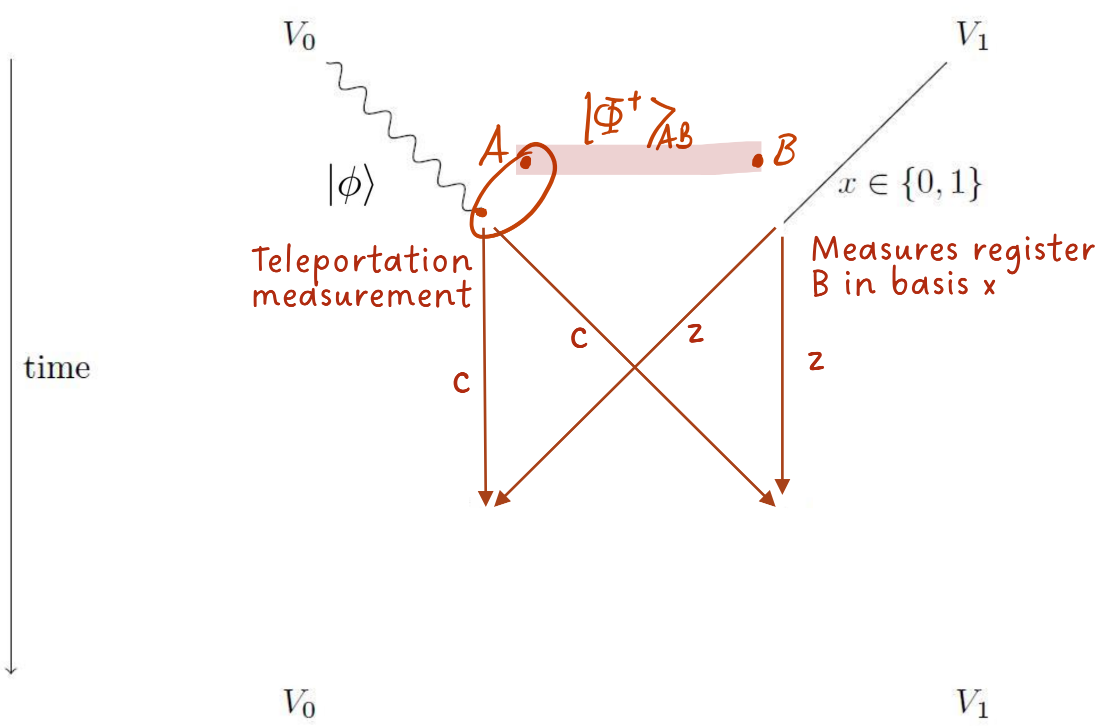


Attack pre-sharing entanglement [KMS11]

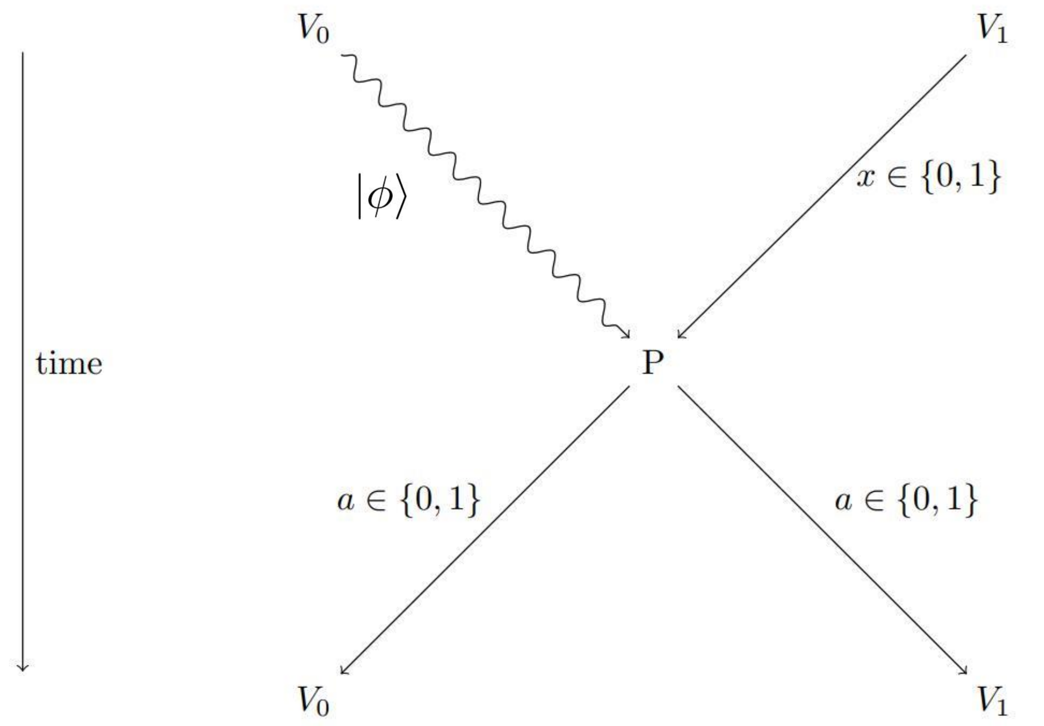


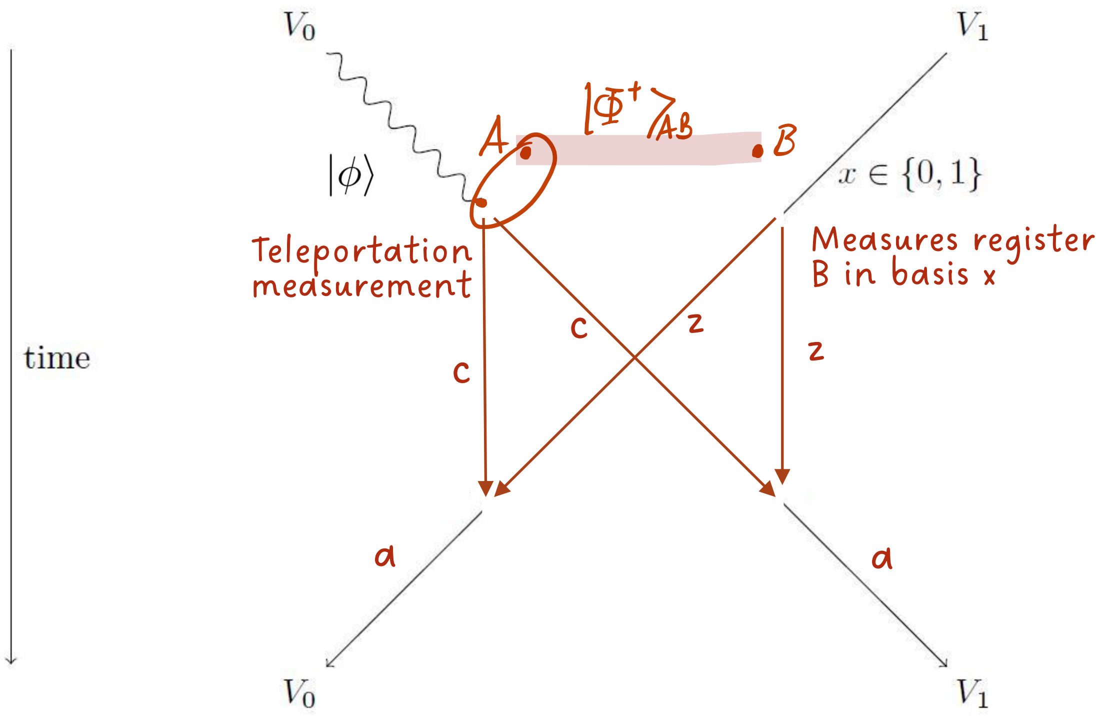
Attack pre-sharing entanglement [KMS11]



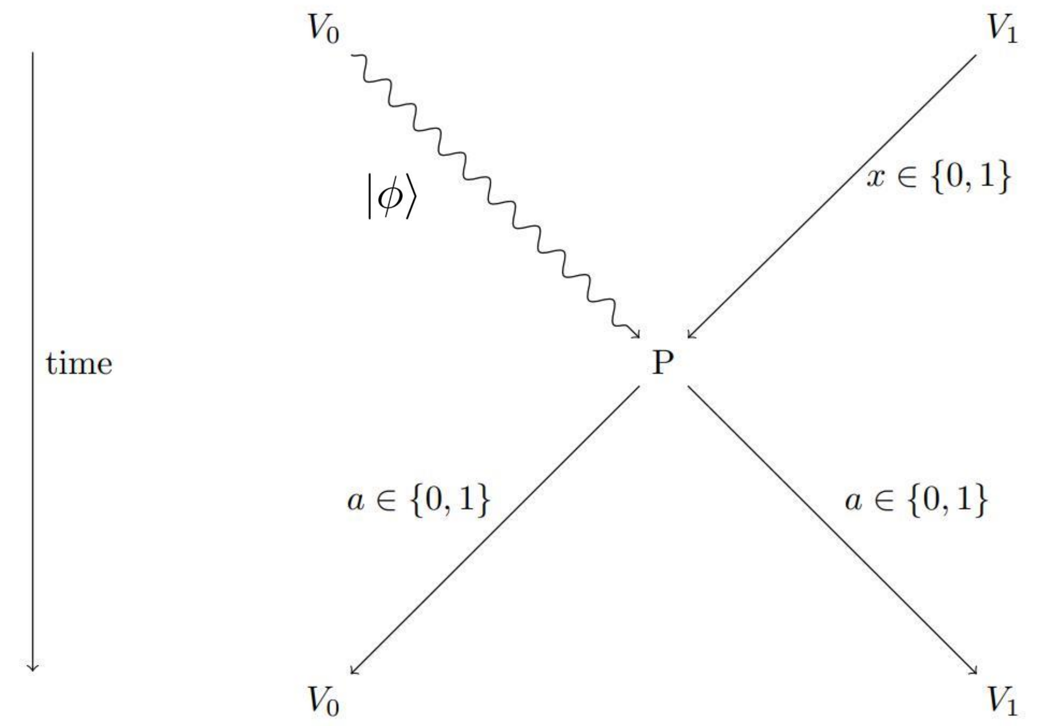


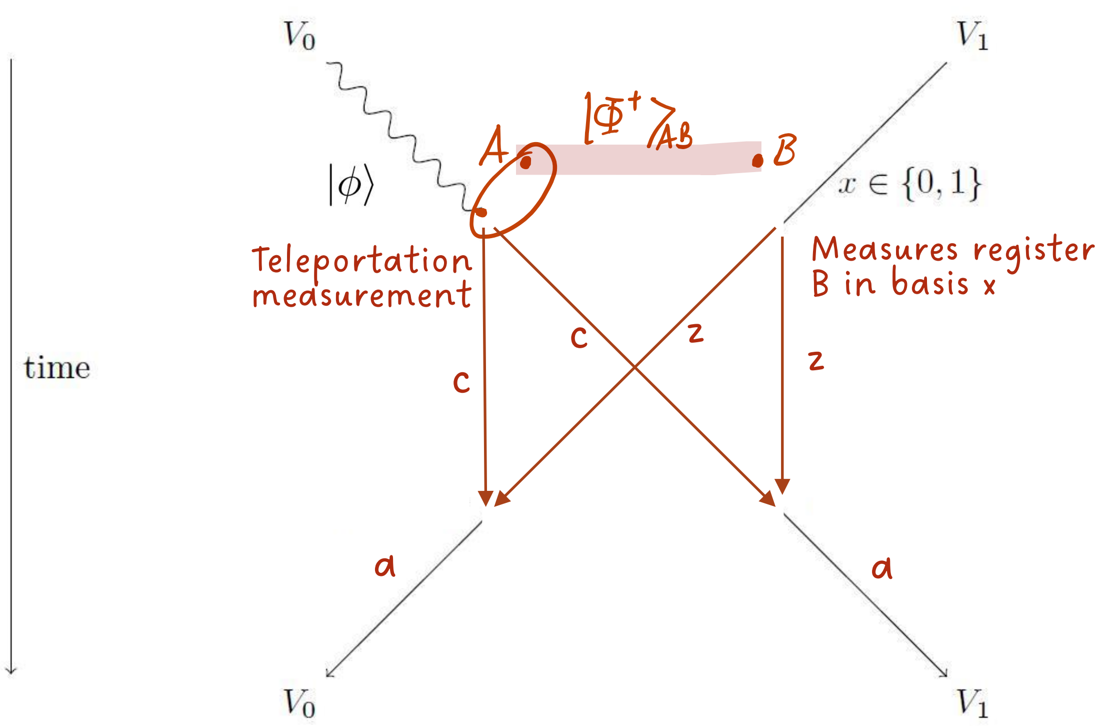
Attack pre-sharing entanglement [KMS11]





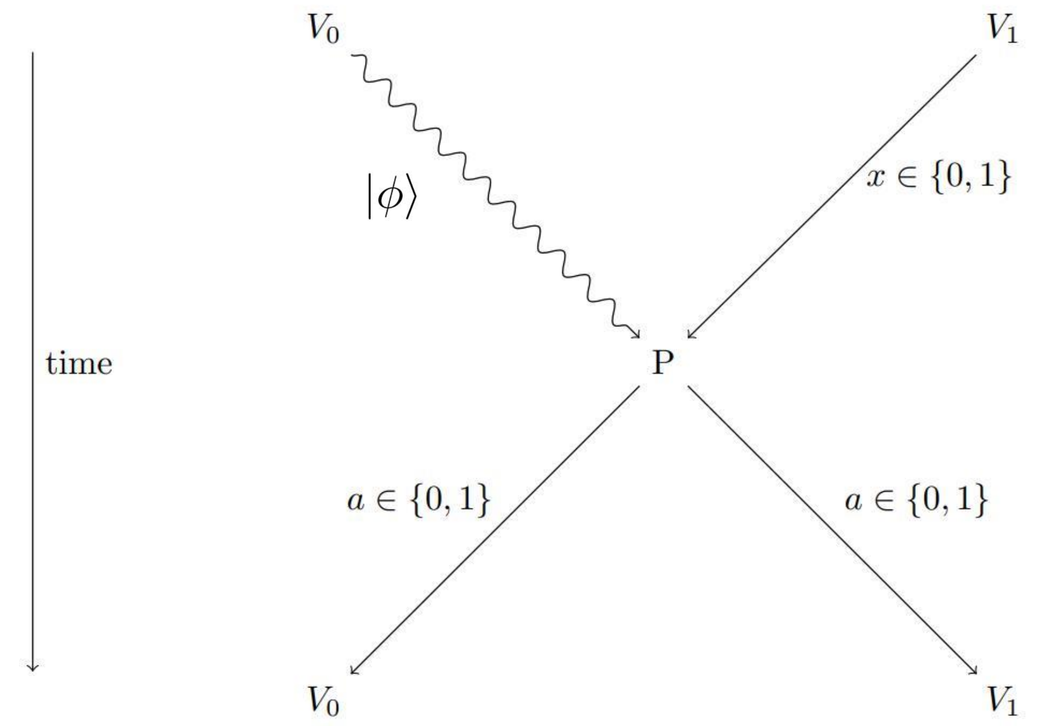
Attack pre-sharing entanglement [KMS11]

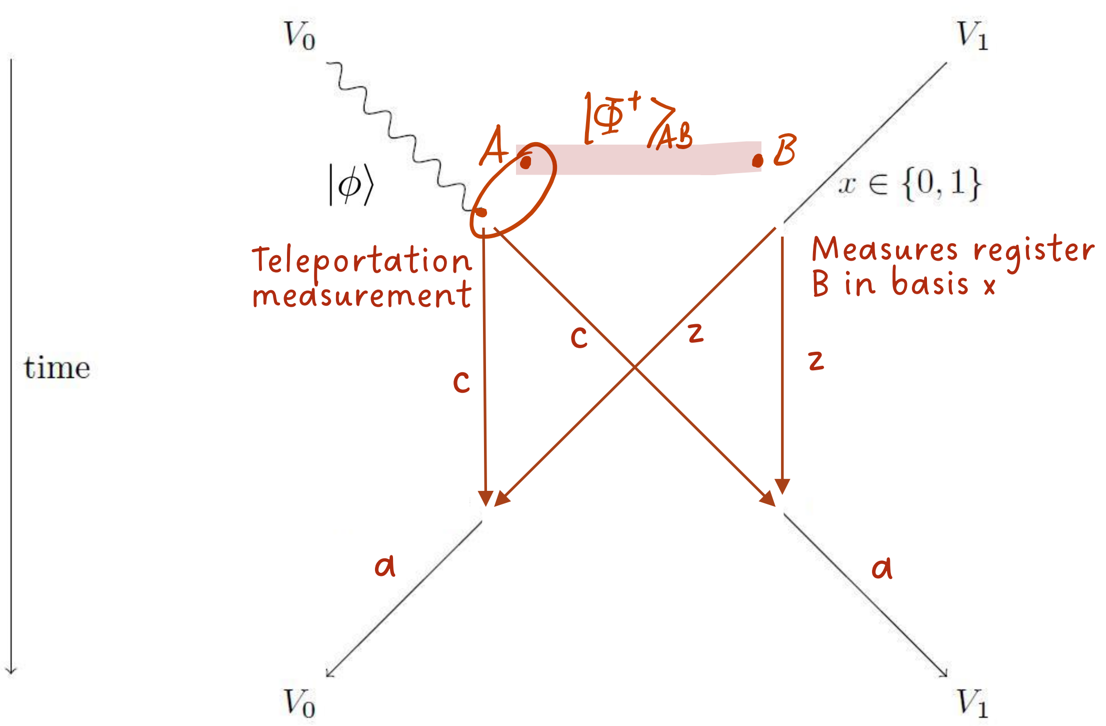




If no pre-shared entanglement [TFKW13]:

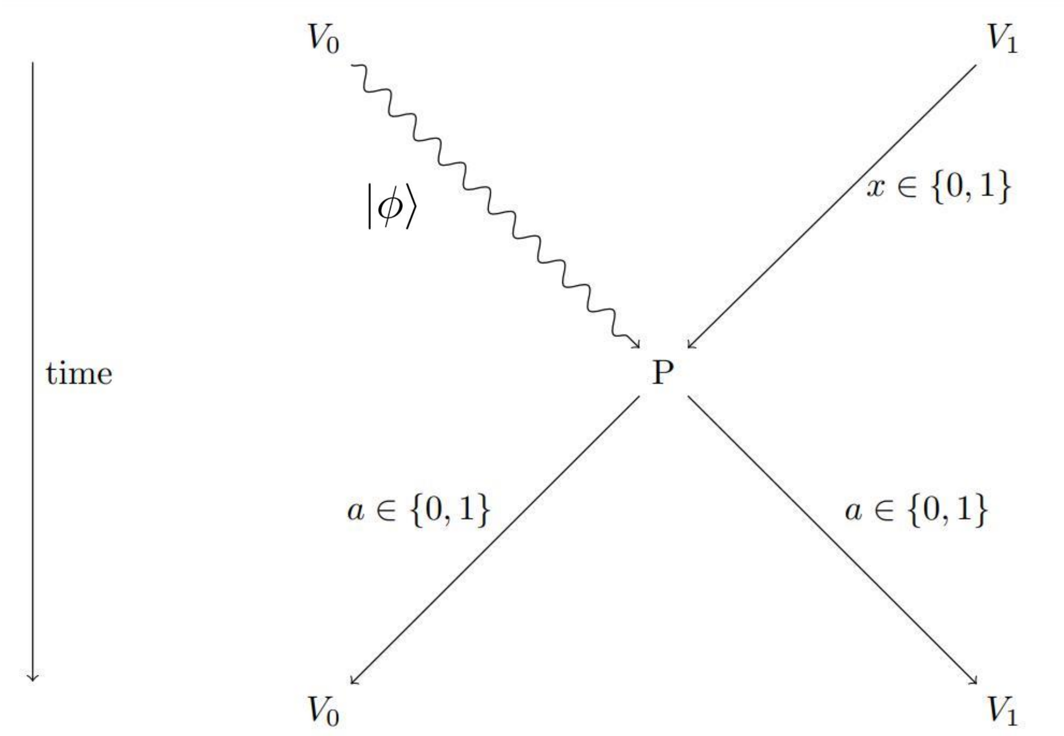
Attack pre-sharing entanglement [KMS11]

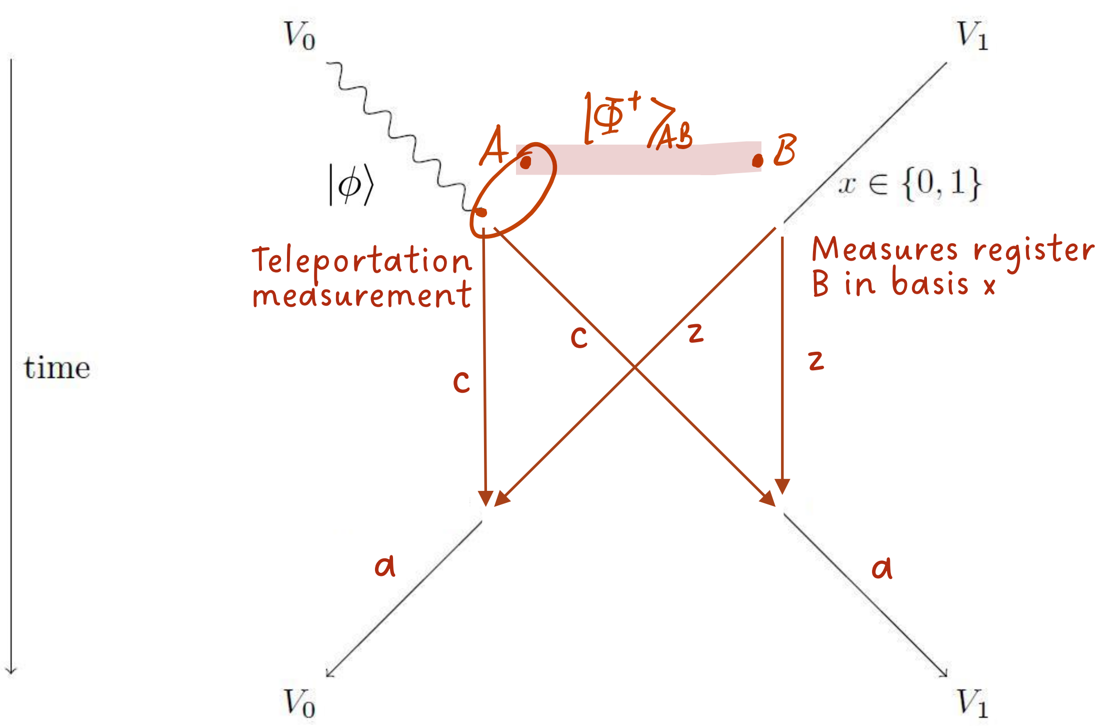




If no pre-shared entanglement [TFKW13]: $\mathbb{P}_{attack} \leq \cos^2\left(\frac{\pi}{8}\right)$

Attack pre-sharing entanglement [KMS11]





If no pre-shared entanglement [TFKW13]: $\mathbb{P}_{attack} \leq \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$

All quantum position verification protocols can be attacked... [BCFGGOS11]

All quantum position verification protocols can be attacked… [BCFGGOS11]

…the best know general attack requires exponential amount of pre-shared entanglement.

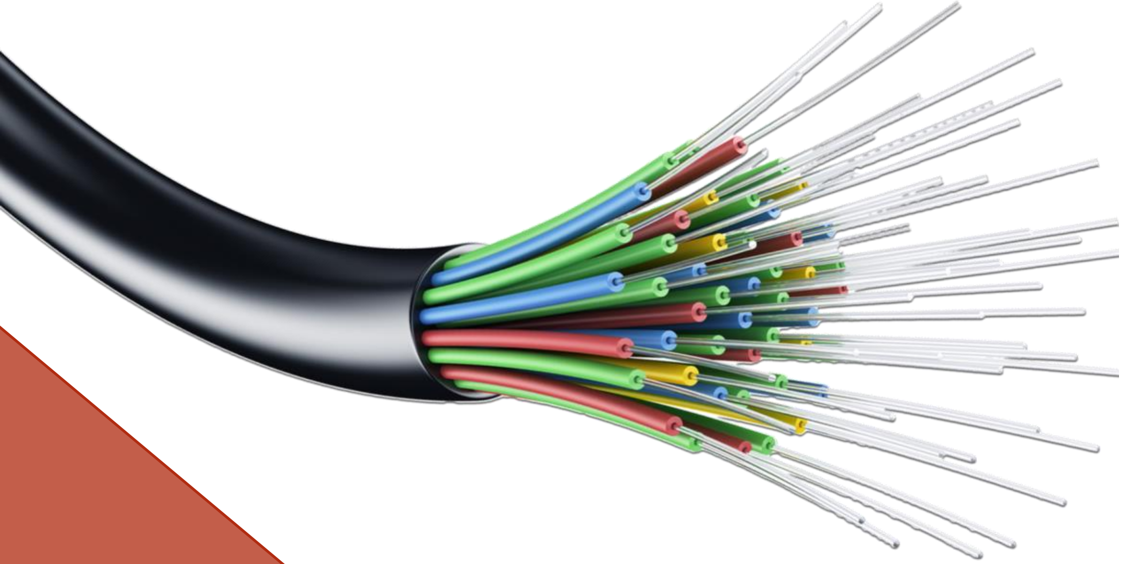
All quantum position verification protocols can be attacked… [BCFGGOS11]

…the best know general attack requires exponential amount of pre-shared entanglement.

Goal: easy protocol which is very difficult to attack.

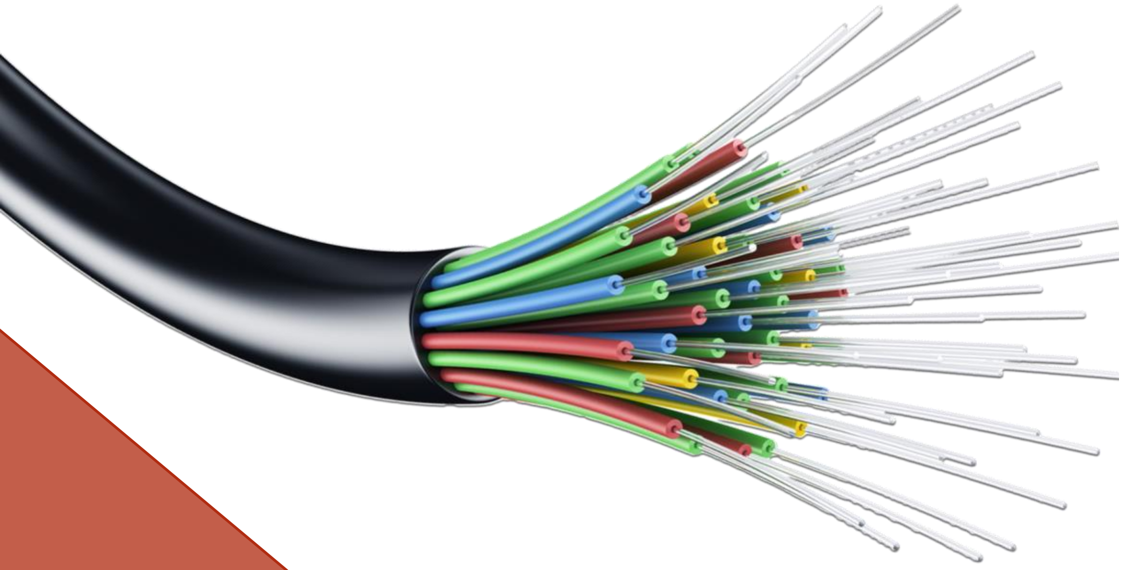
Experimental implementation encounters problems

Experimental implementation encounters problems



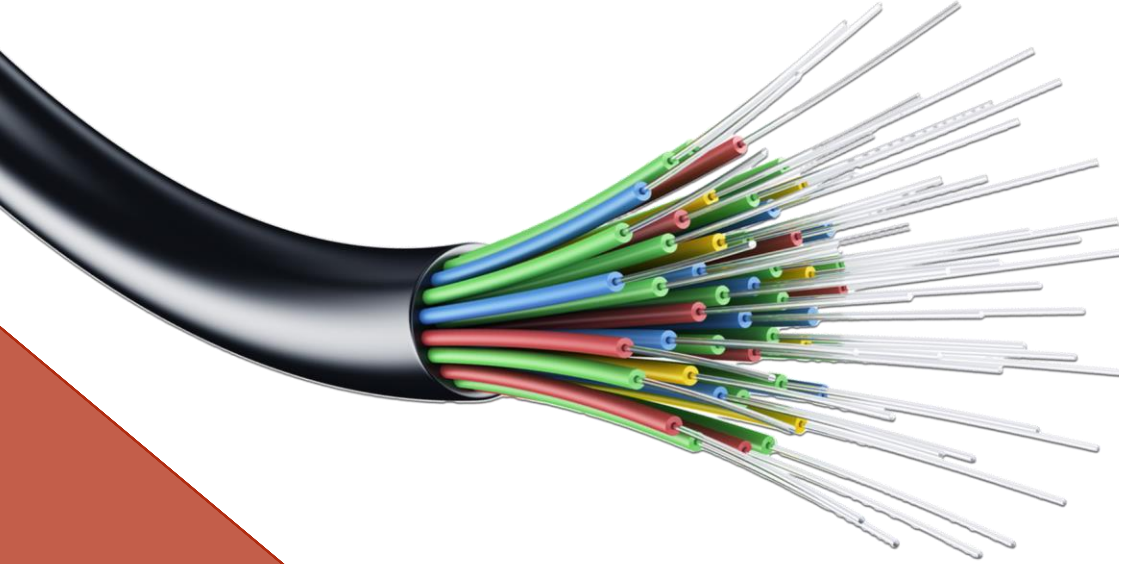
Experimental implementation encounters problems

Photon loss



Experimental implementation encounters problems

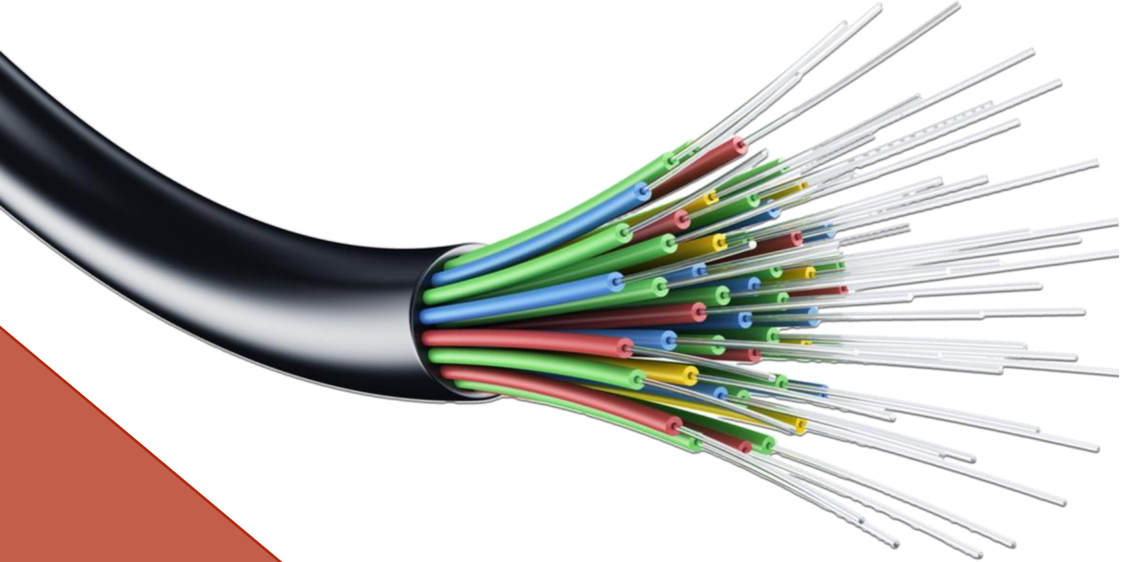
Photon loss



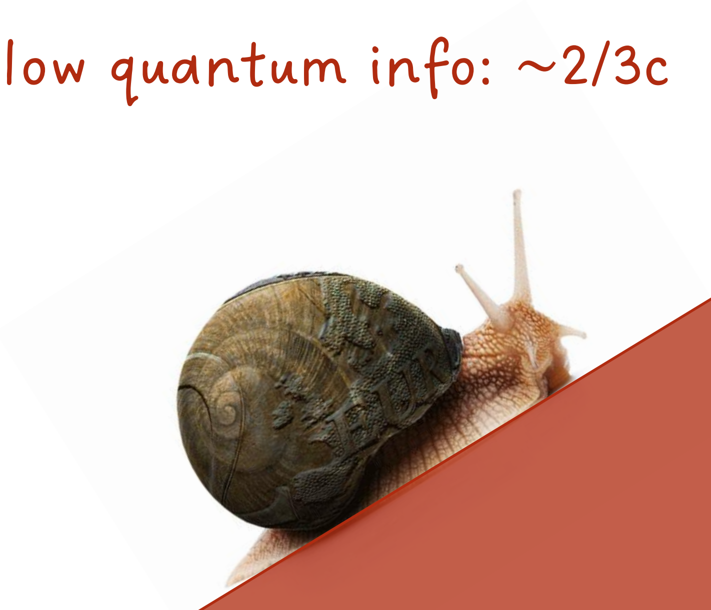
Slow quantum info: ~2/3c

Experimental implementation encounters problems

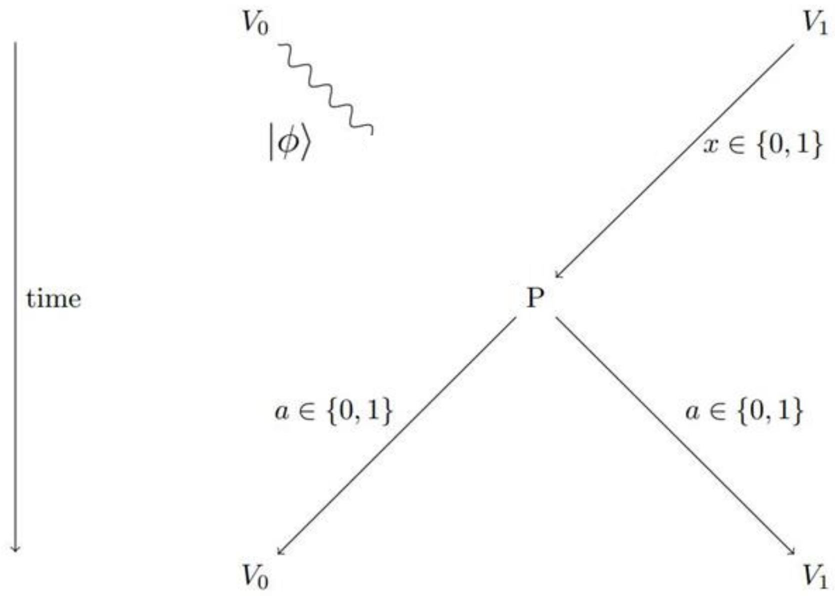
Photon loss



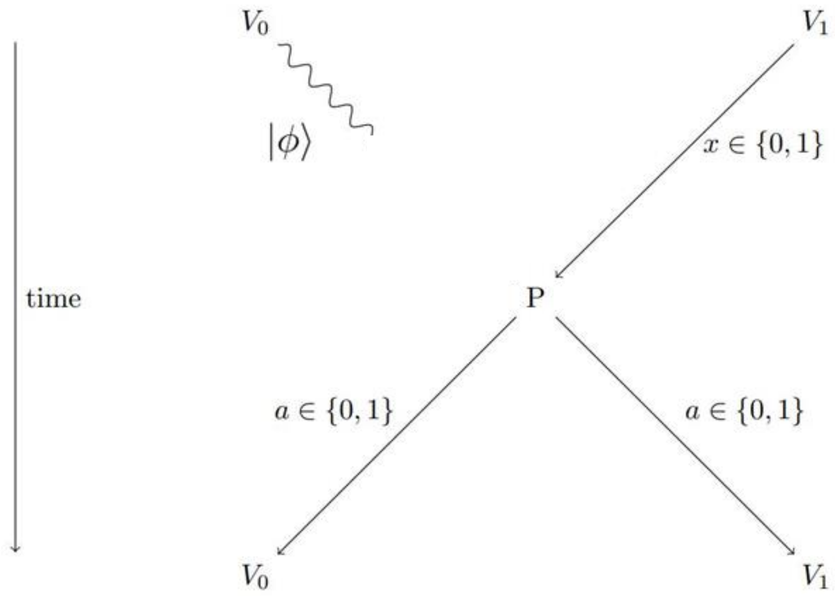
Slow quantum info: ~2/3c

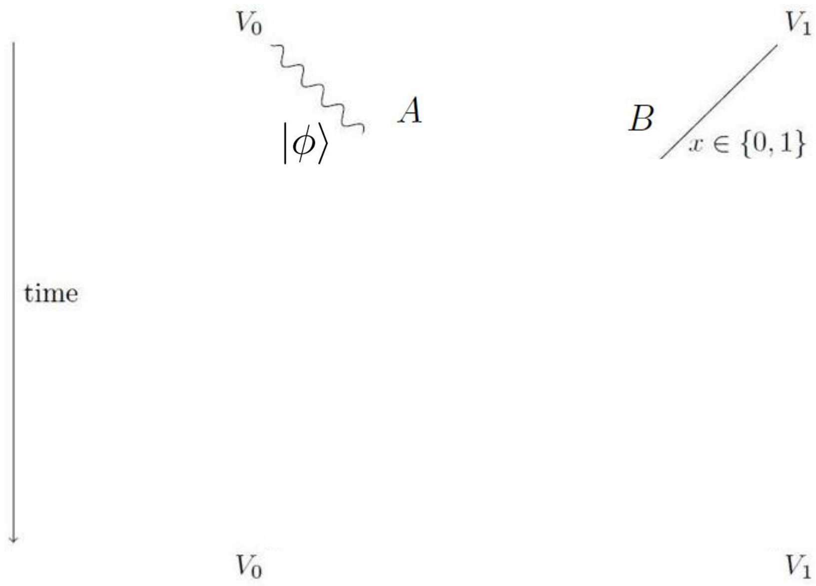


Taking advantage of photon loss

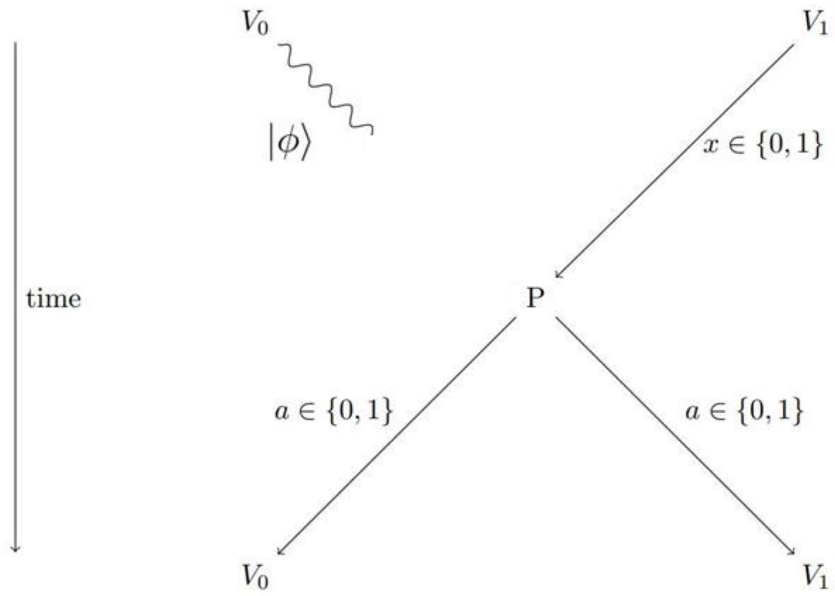


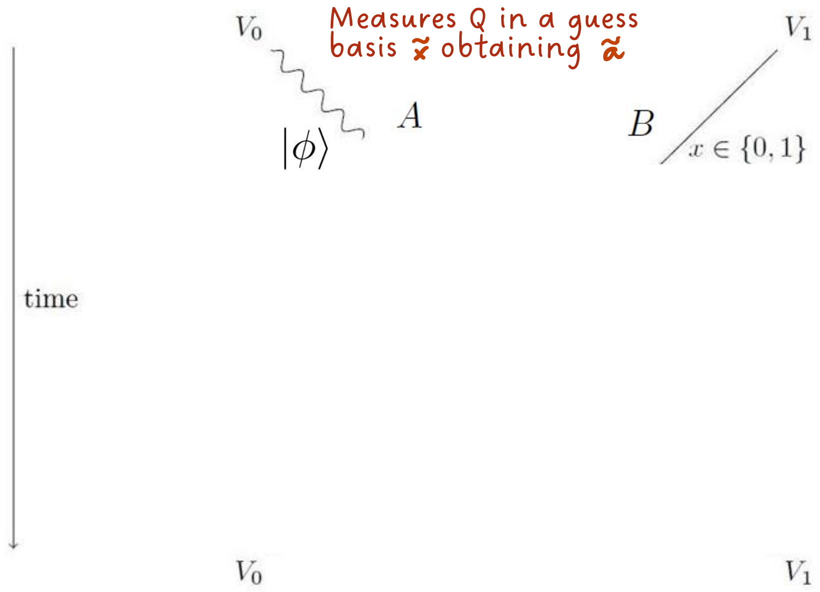
Taking advantage of photon loss



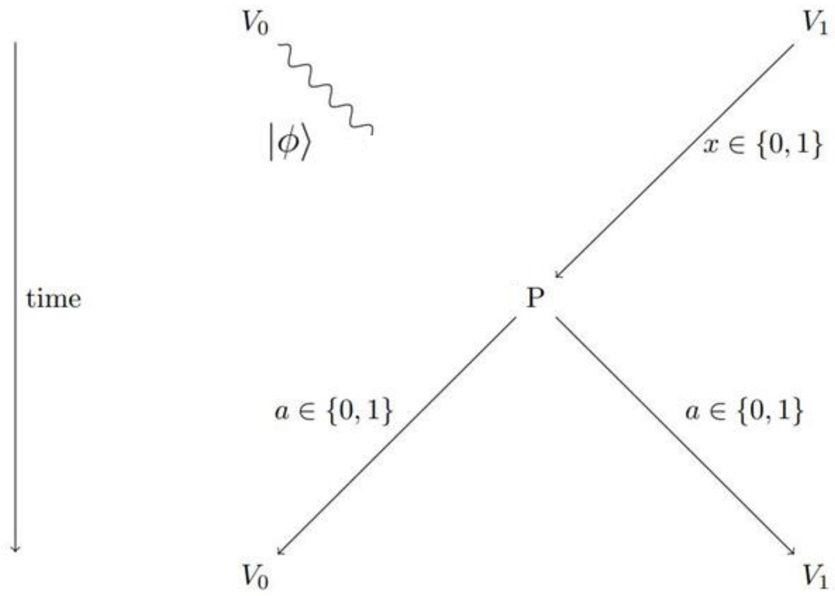


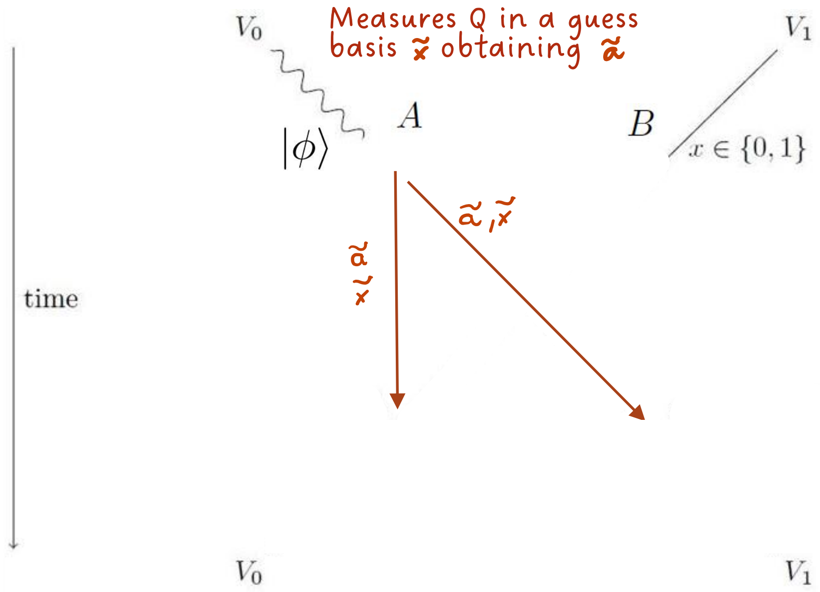
Taking advantage of photon loss



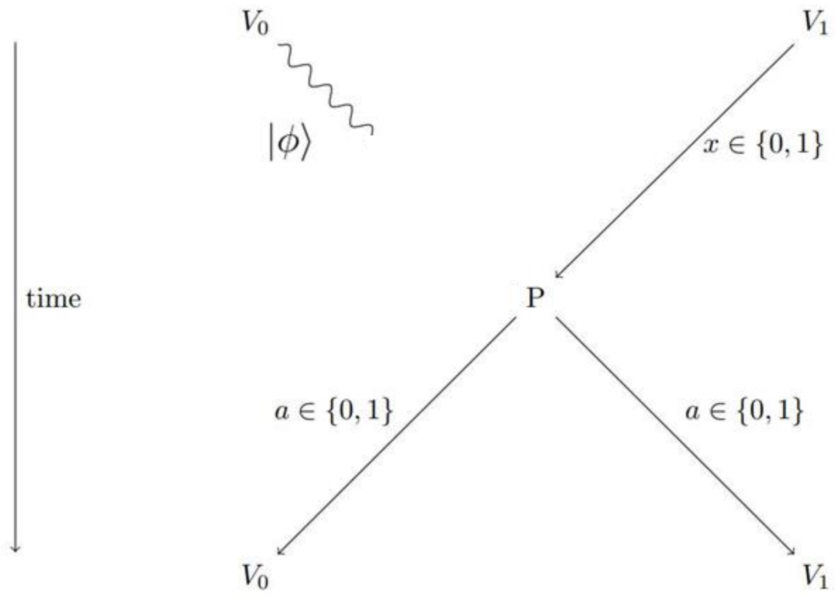


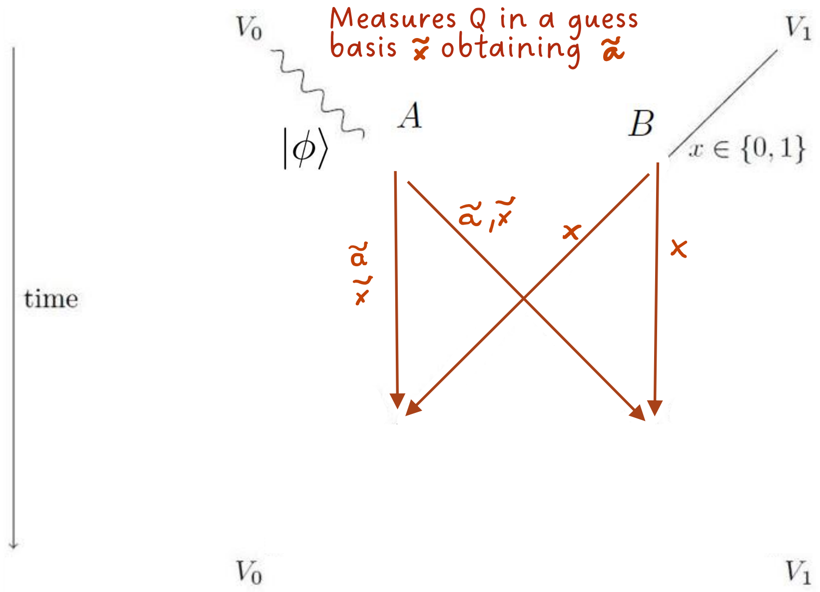
Taking advantage of photon loss



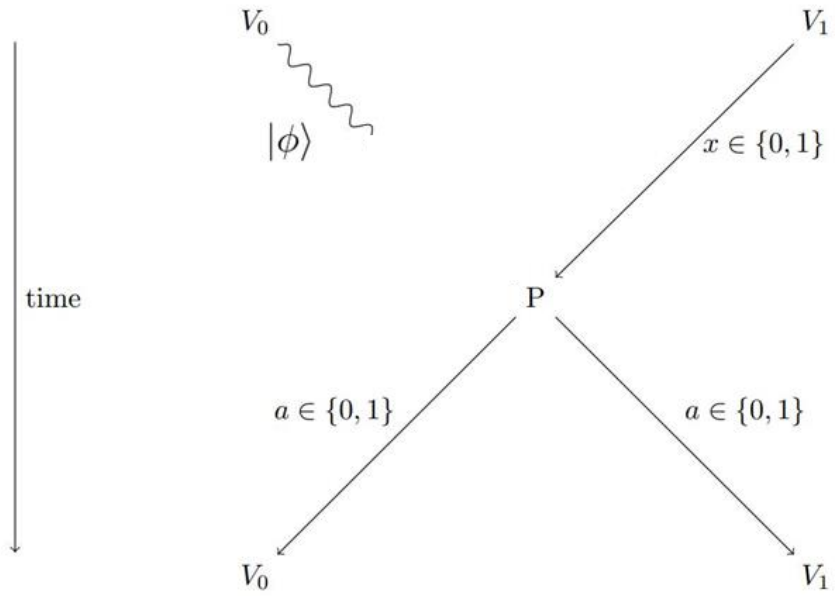


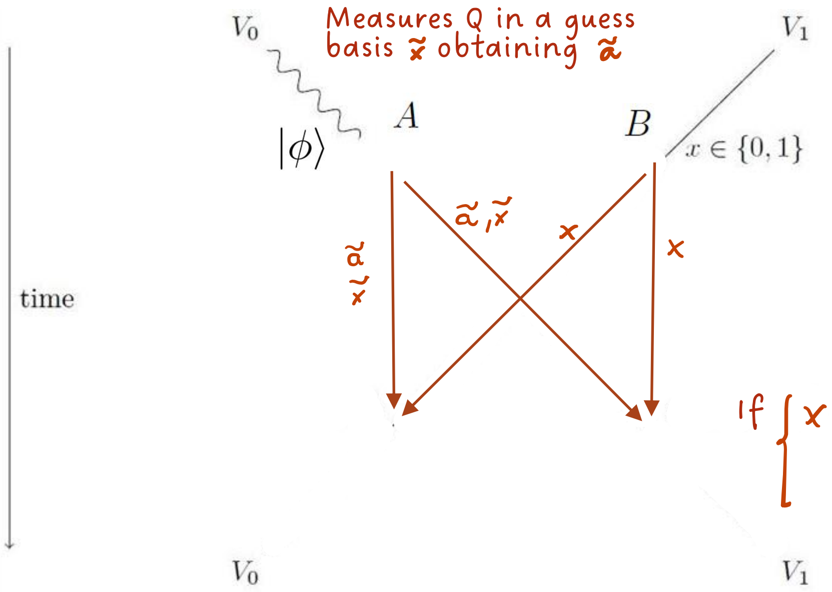
Taking advantage of photon loss





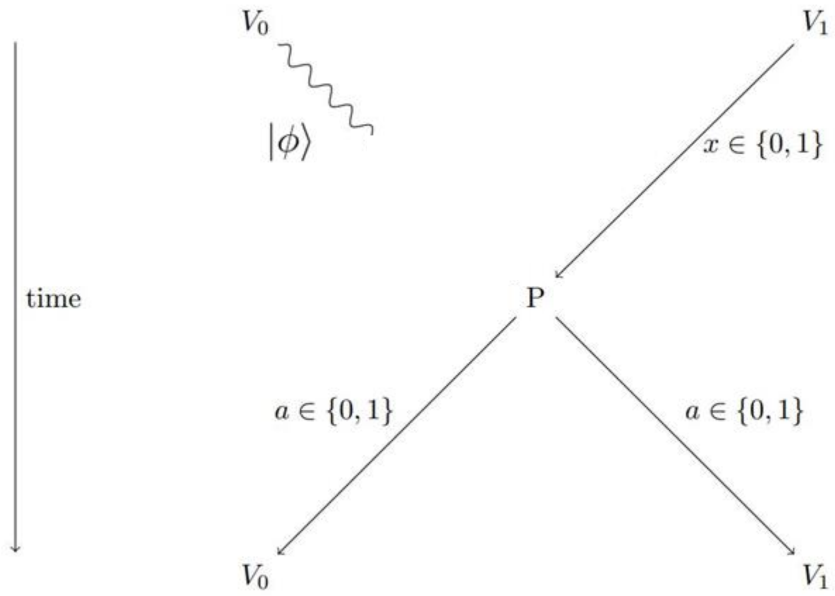
Taking advantage of photon loss

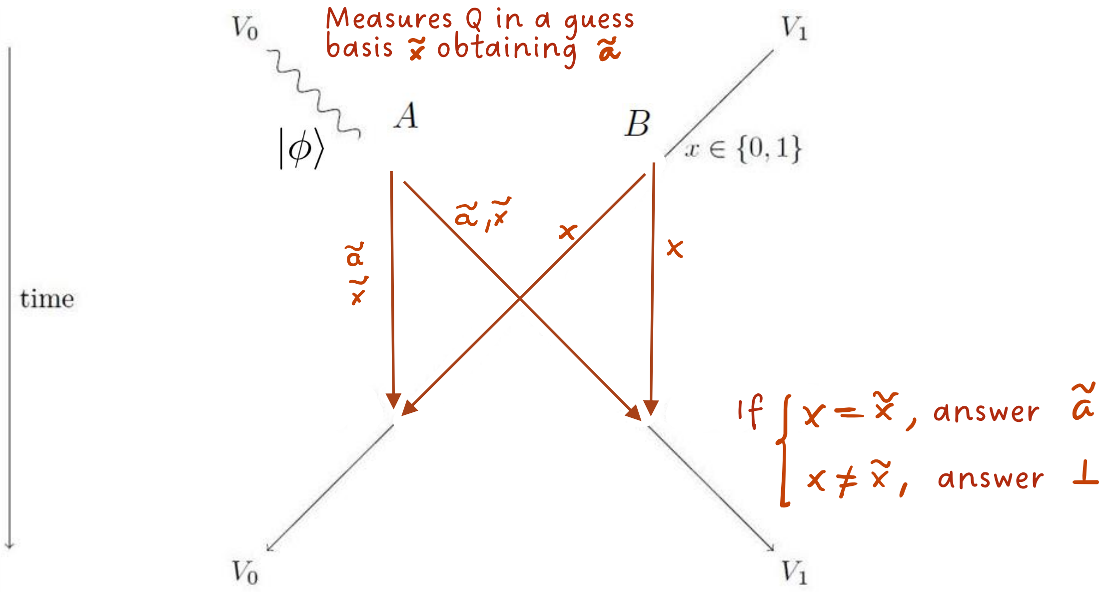




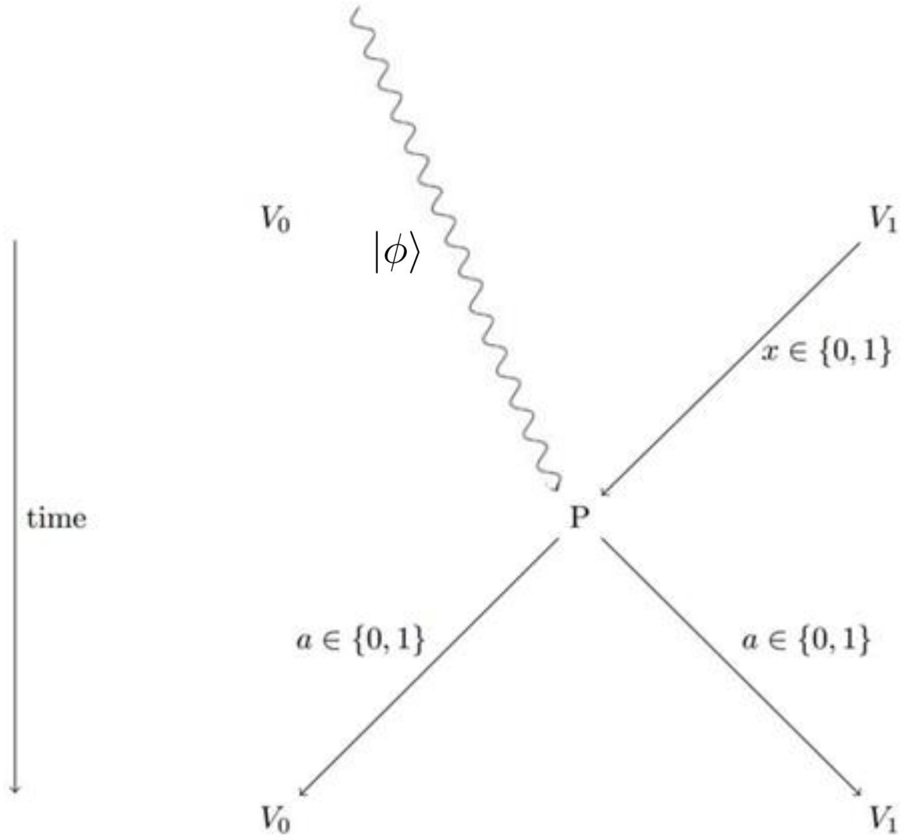
If $\begin{cases} x = \tilde{x}, \text{ answer } \tilde{a} \end{cases}$

Taking advantage of photon loss

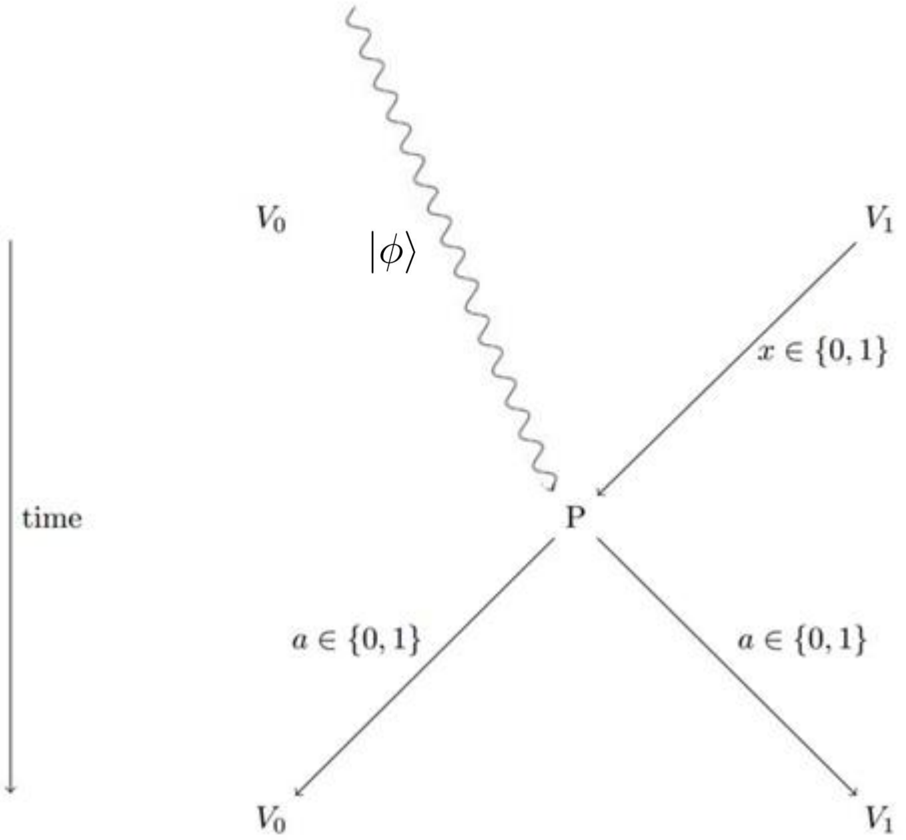


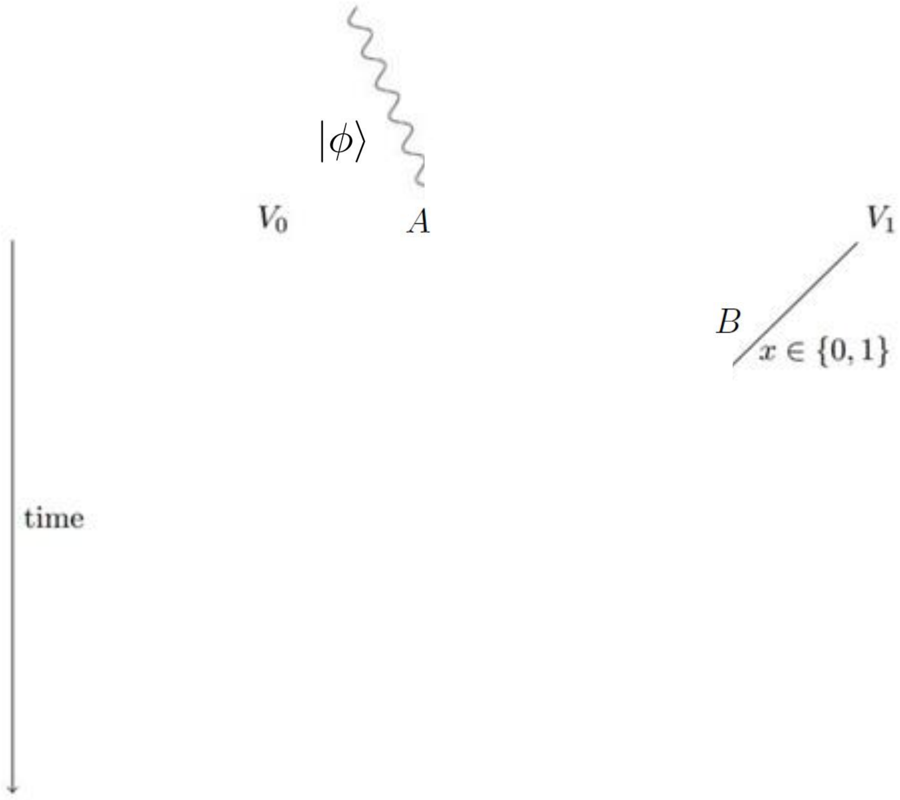


Taking advantage of slow quantum information

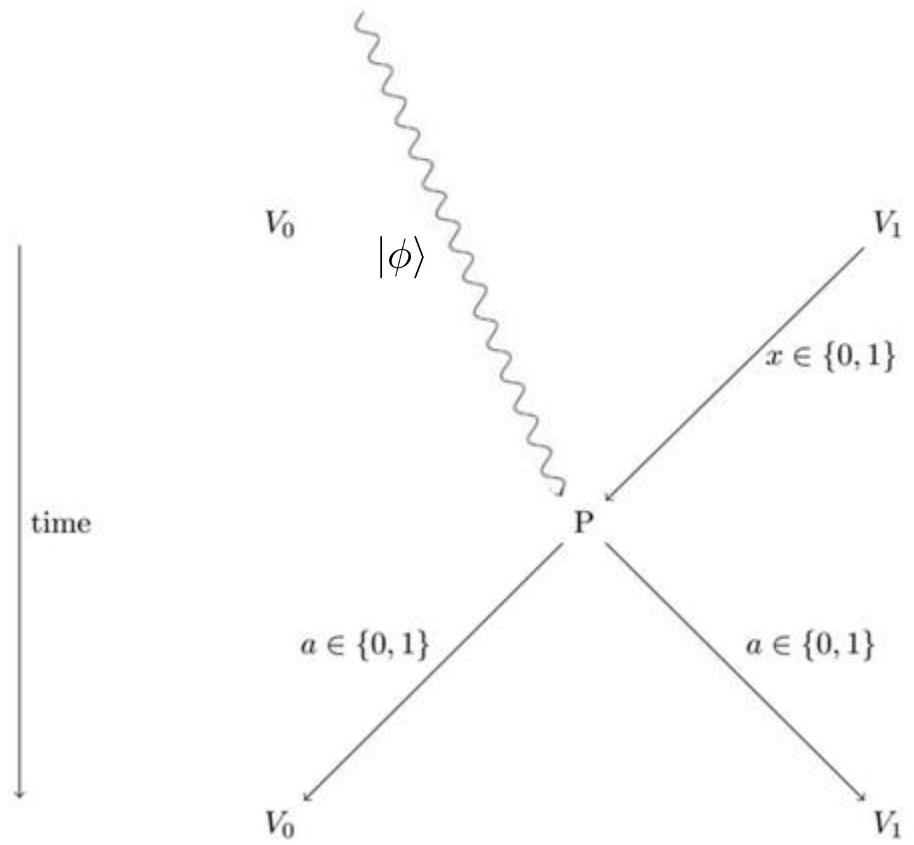


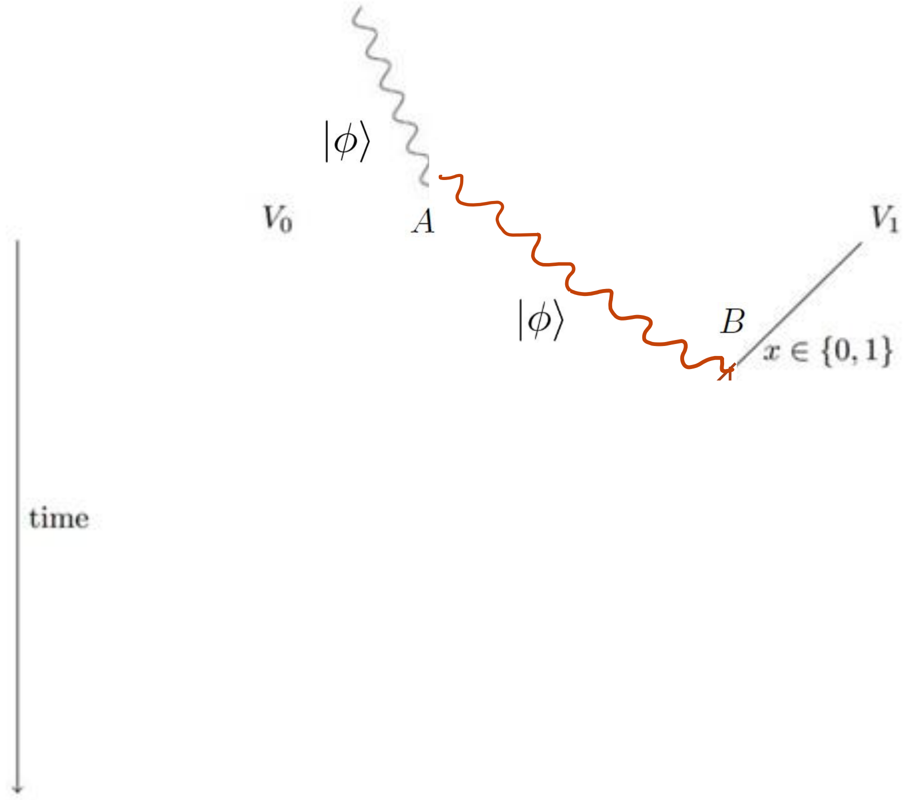
Taking advantage of slow quantum information



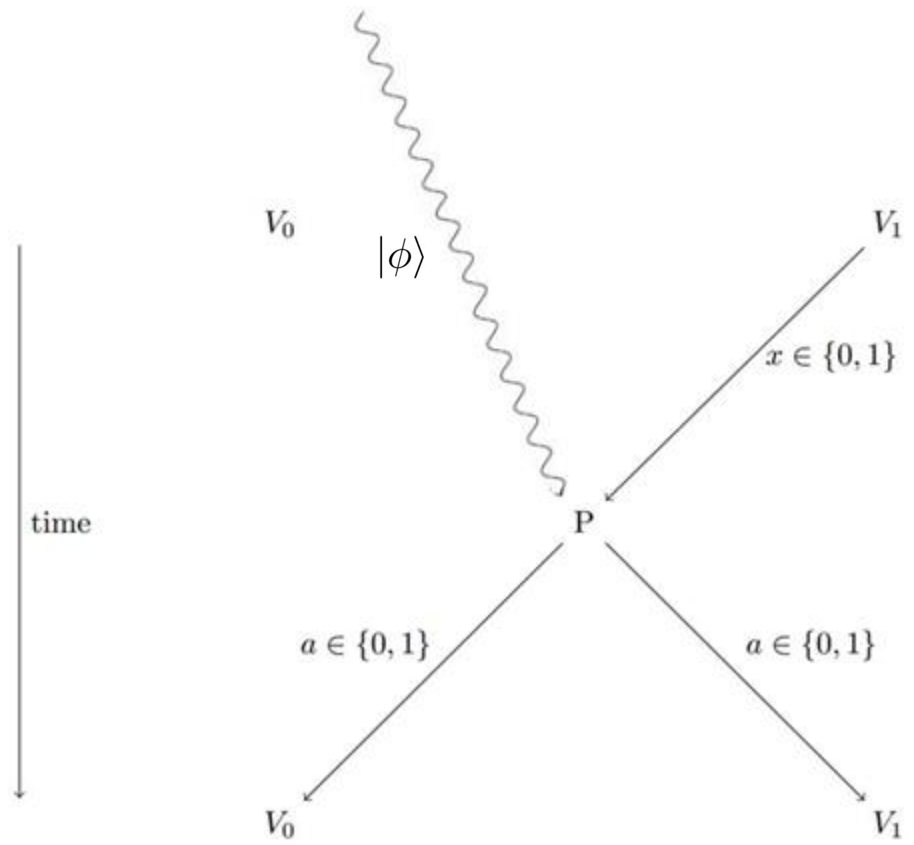


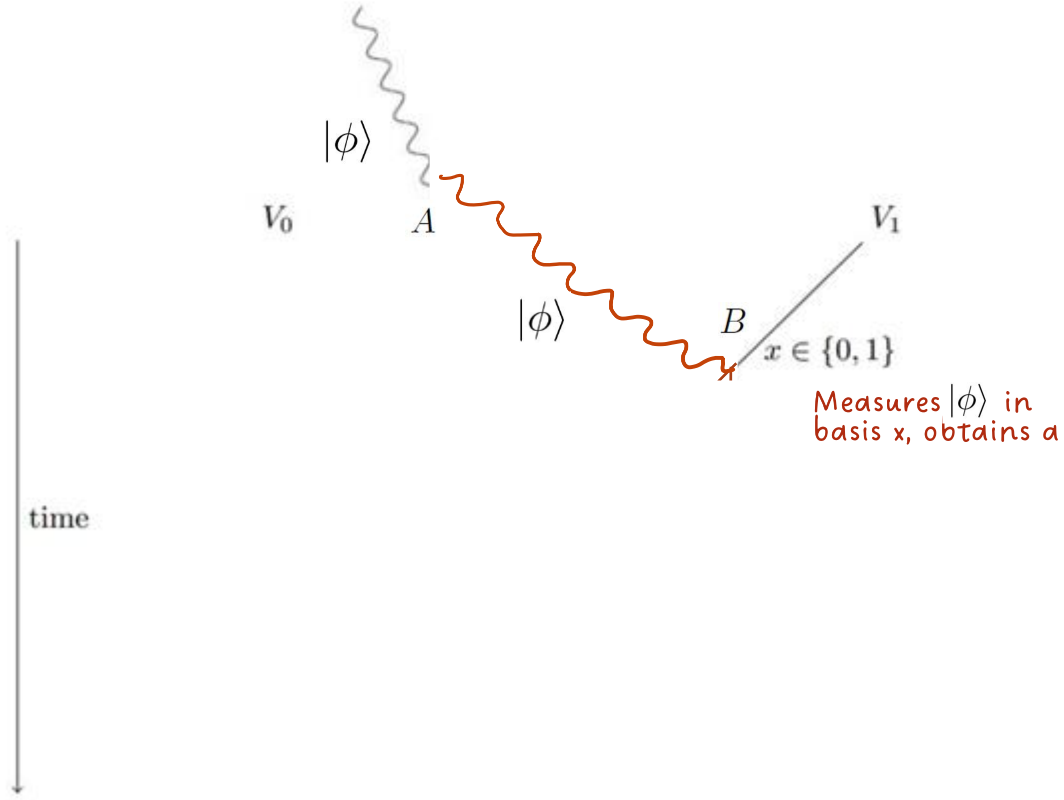
Taking advantage of slow quantum information



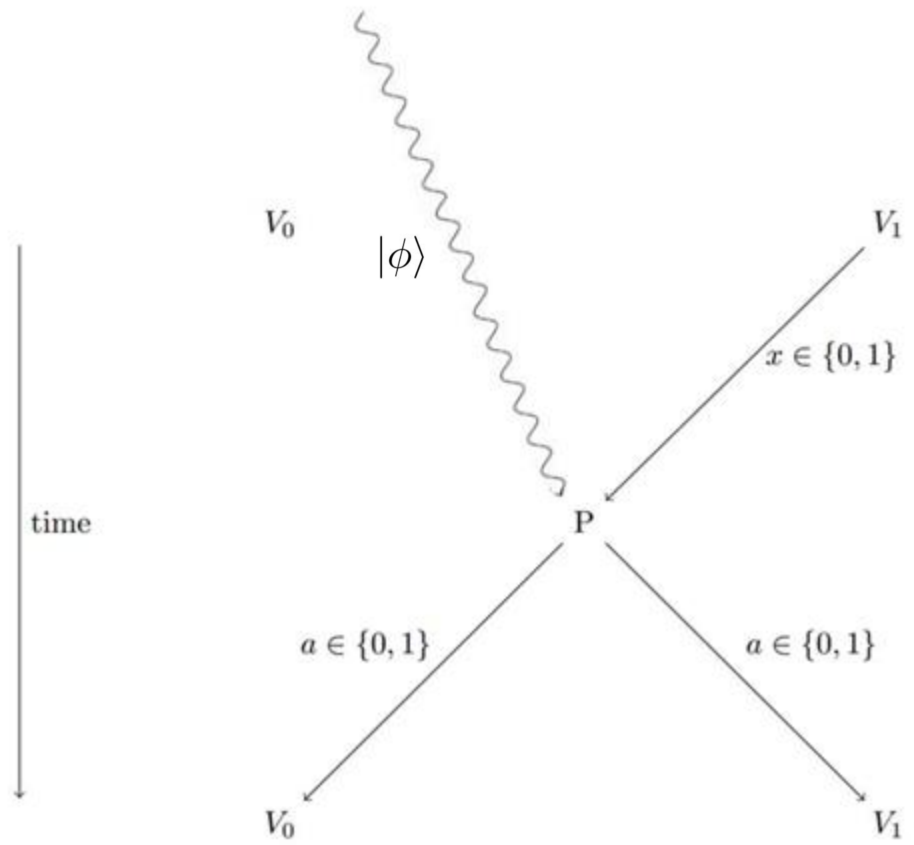


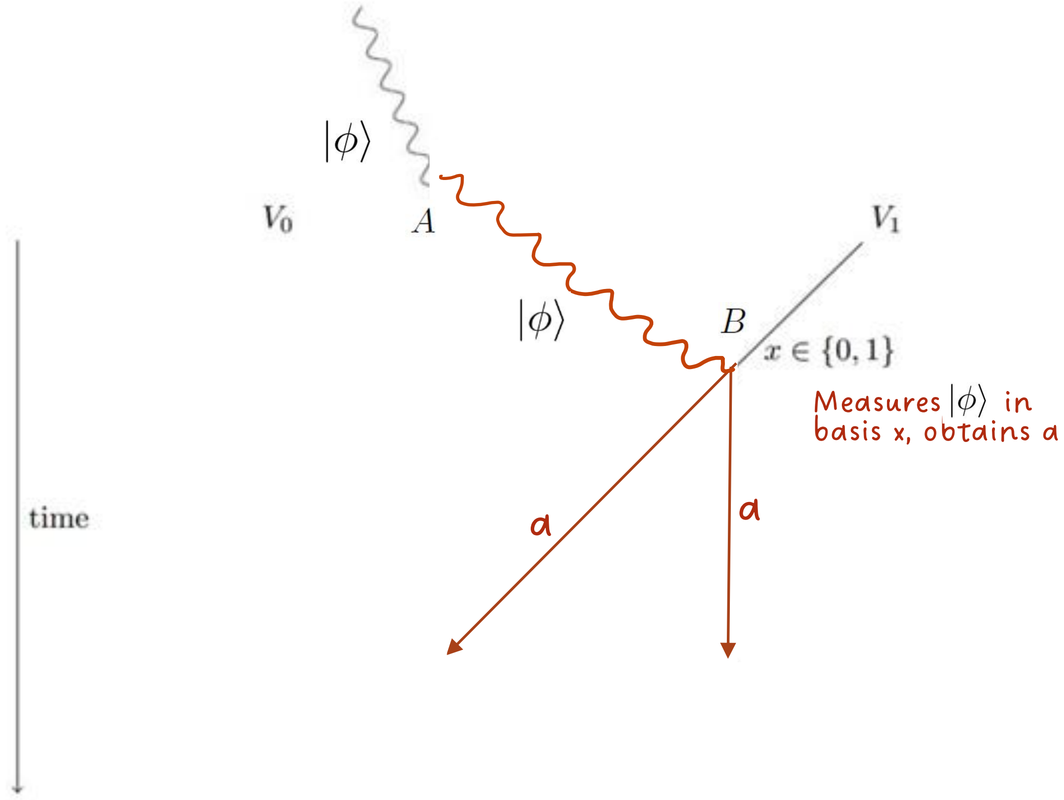
Taking advantage of slow quantum information



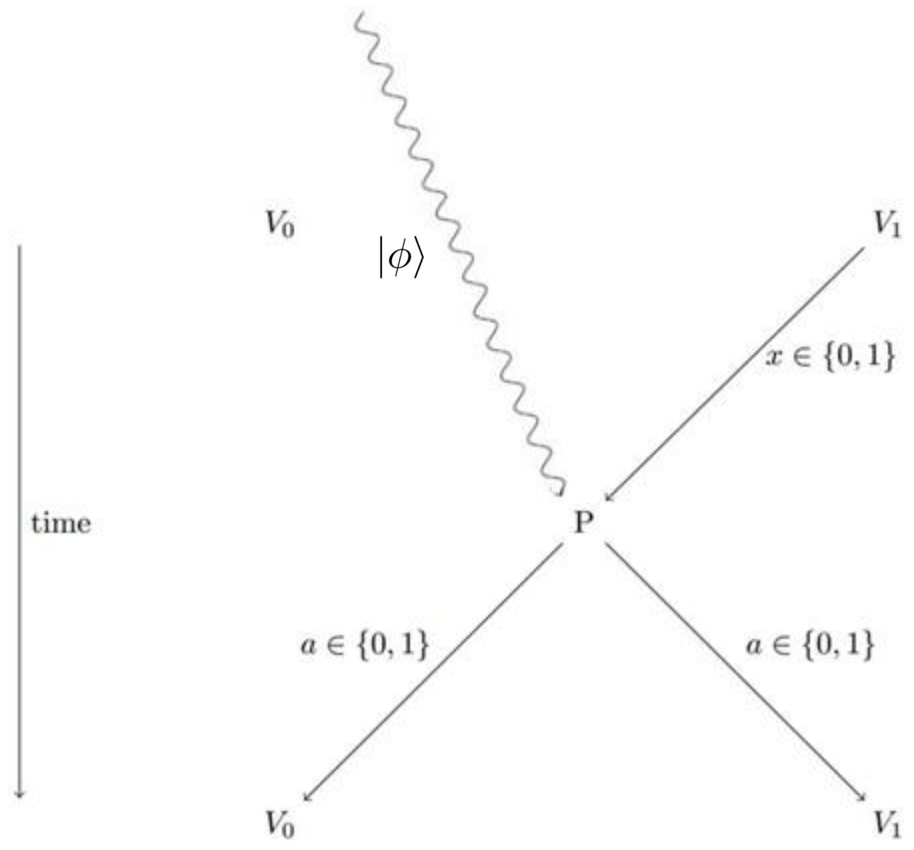


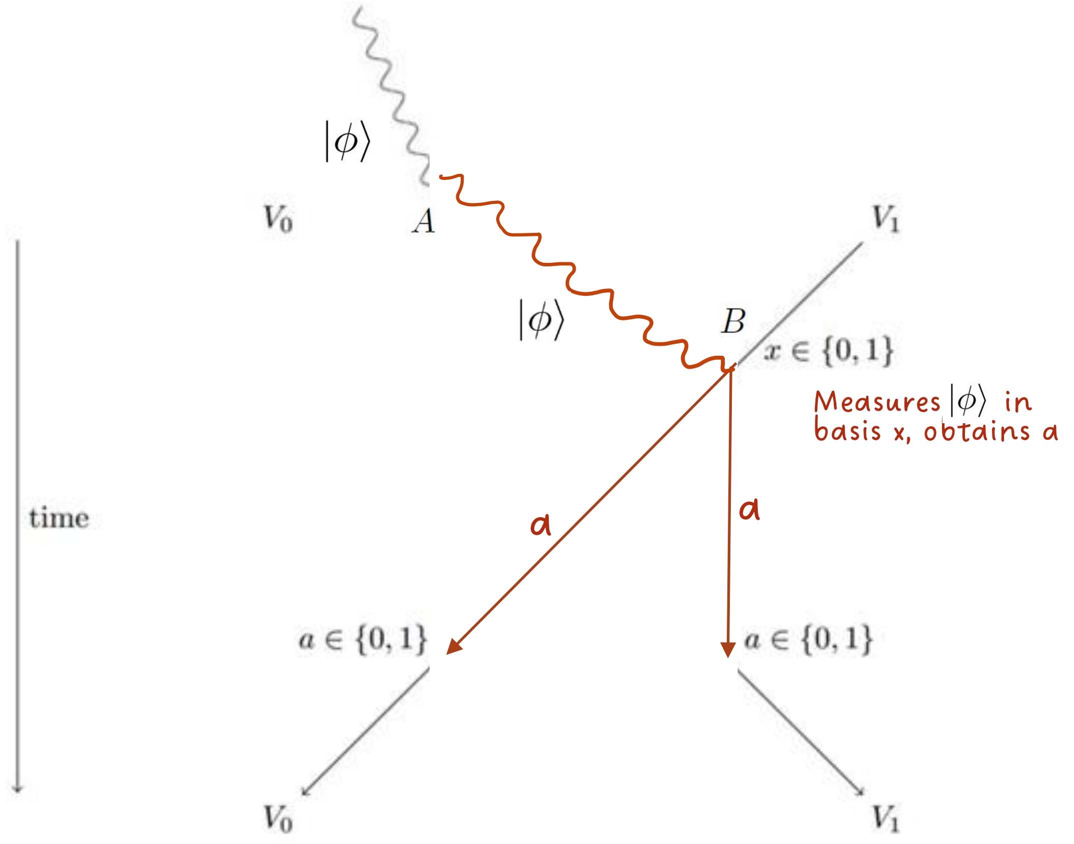
Taking advantage of slow quantum information





Taking advantage of slow quantum information





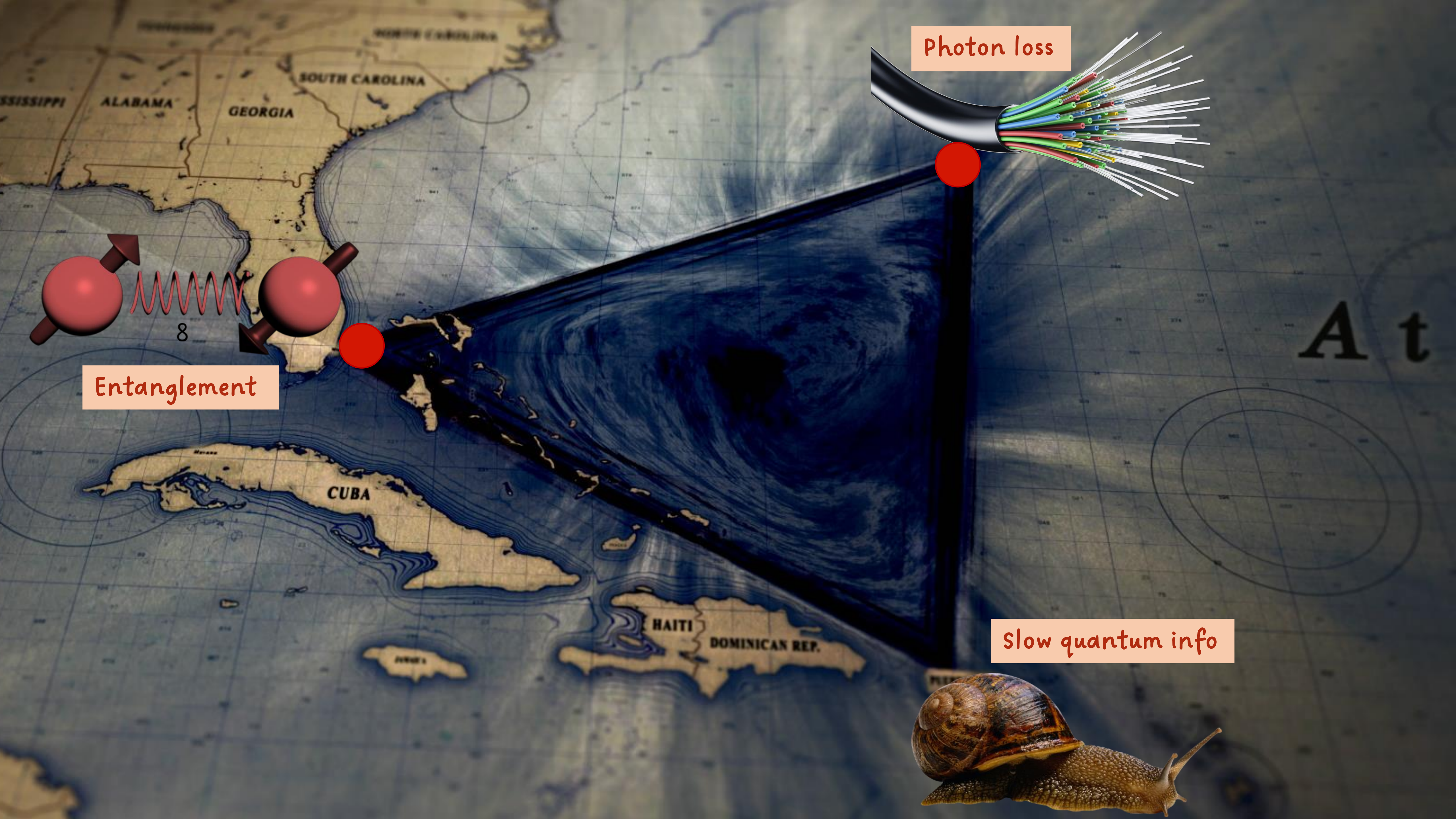

NORTH CAROLINA
SOUTH CAROLINA
ALABAMA
GEORGIA
FLORIDA
BERMUDA
CUBA
HAITI
DOMINICAN REP.
PUERTO RICO

Photon loss
SOUTH CAROLINA
ALABAMA
GEORGIA
FLORIDA
CUBA
HAITI
DOMINICAN REP.


Photon loss
Slow quantum info
NORTH CAROLINA
SOUTH CAROLINA
ALABAMA
GEORGIA
FLORIDA
CUBA
HAITI
DOMINICAN REP.

Photon loss
Entanglement
Slow quantum info
NORTH CAROLINA
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.


Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.


Photon loss
NORTH CAROLINA
SOUTH CAROLINA
ALABAMA
GEORGIA
SSISSIPPI
8
Entanglement
CUBA
HAITI
DOMINICAN REP.
Slow quantum info
A t

Photon loss
Entanglement
8
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.

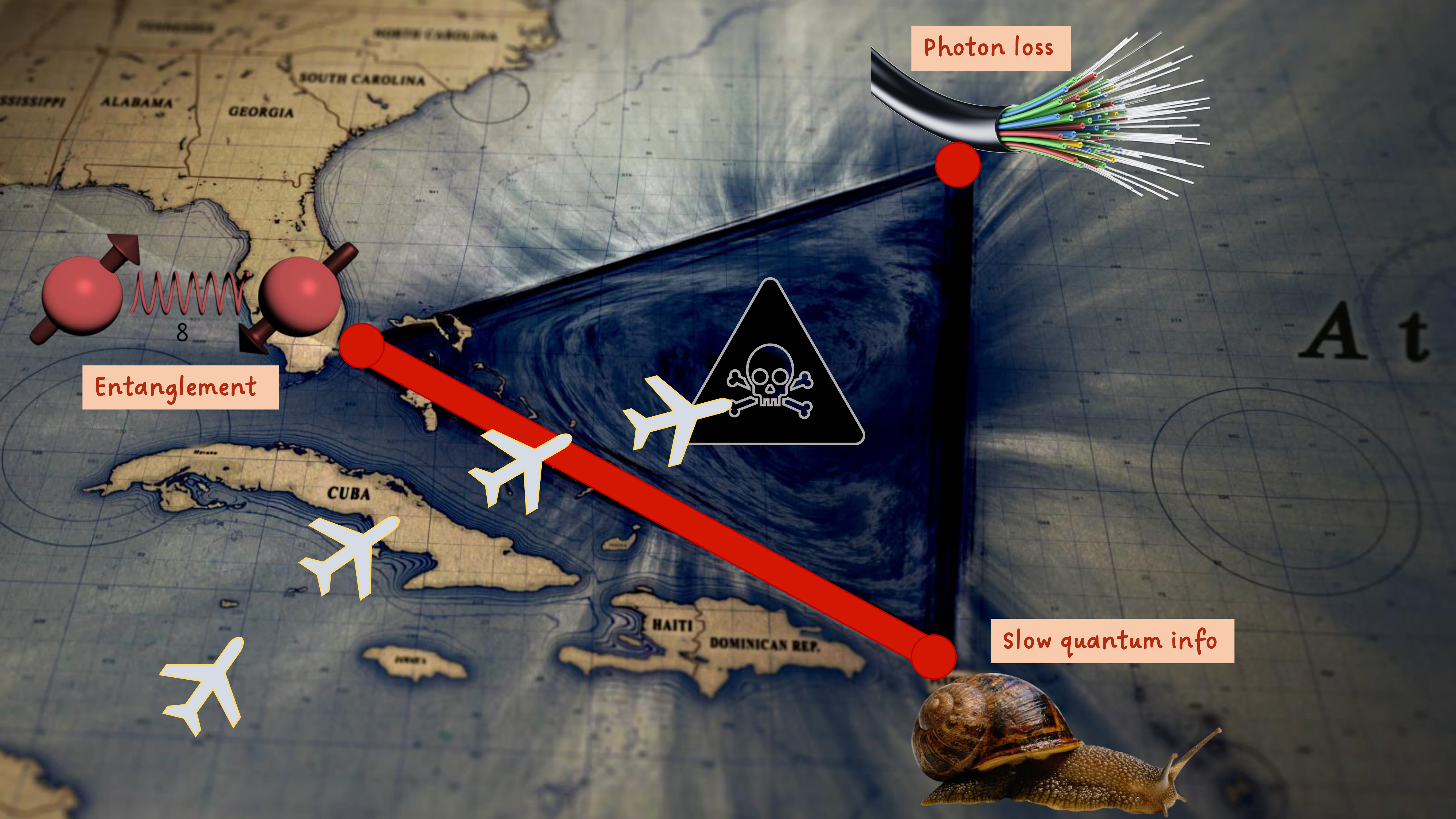

Photon loss
SOUTH CAROLINA
ALABAMA
GEORGIA
8
Entanglement
CUBA
HAITI
DOMINICAN REP.
Slow quantum info

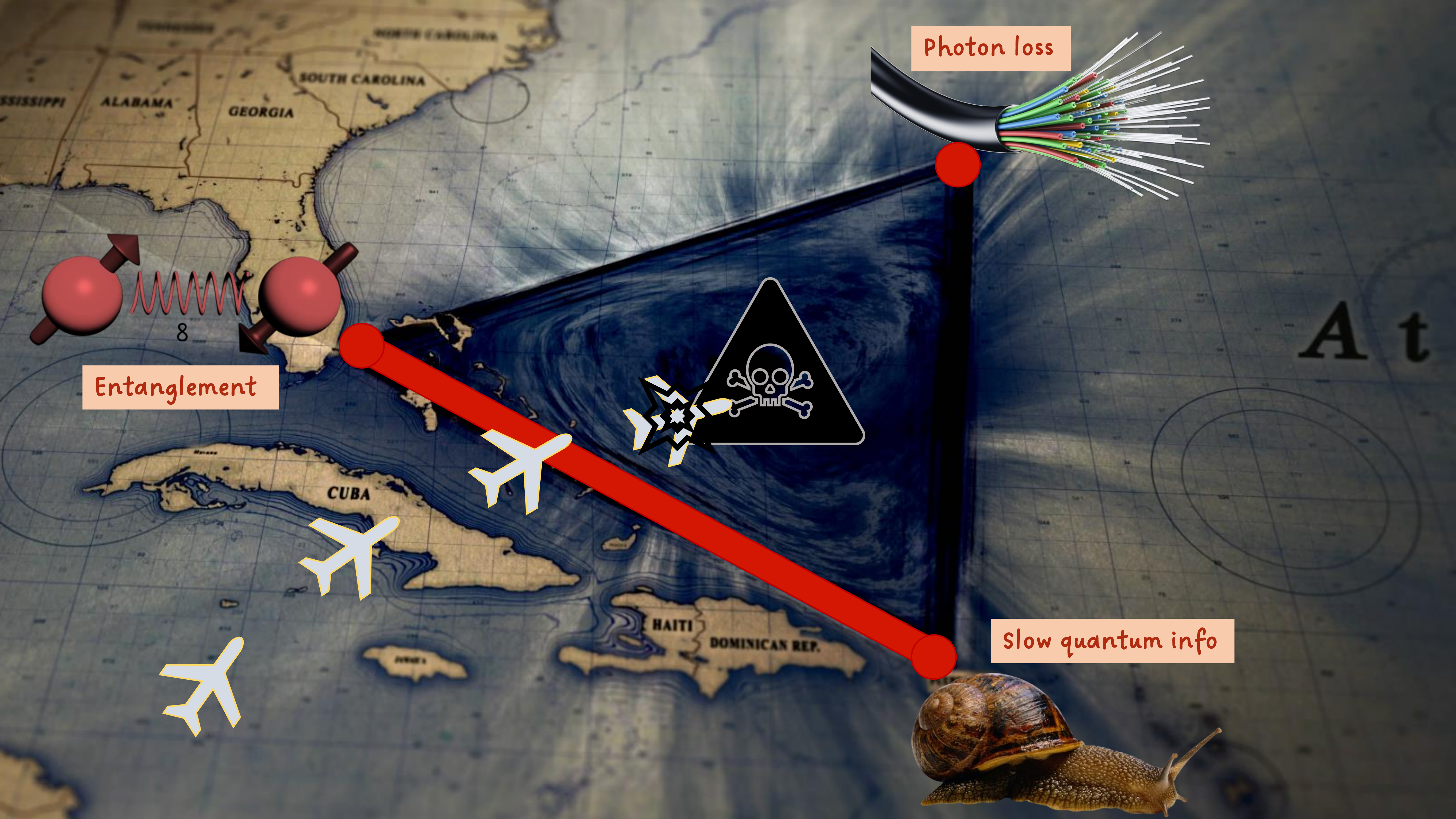

Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.

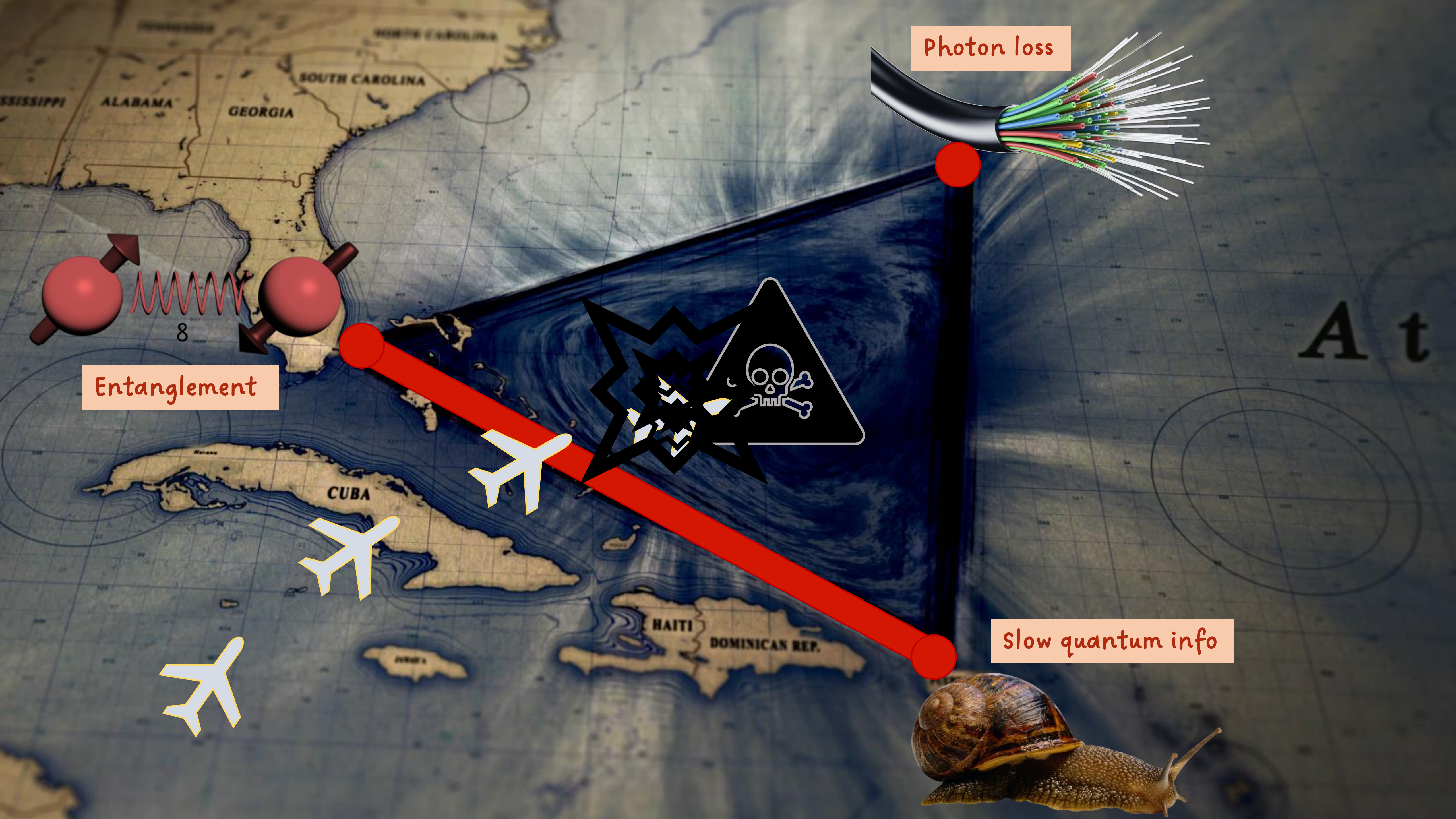

Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.


Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.

Photon loss
Entanglement
Slow quantum info
NORTH CAROLINA
SOUTH CAROLINA
SSISSIPPI
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.


Photon loss
Entanglement
8
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.

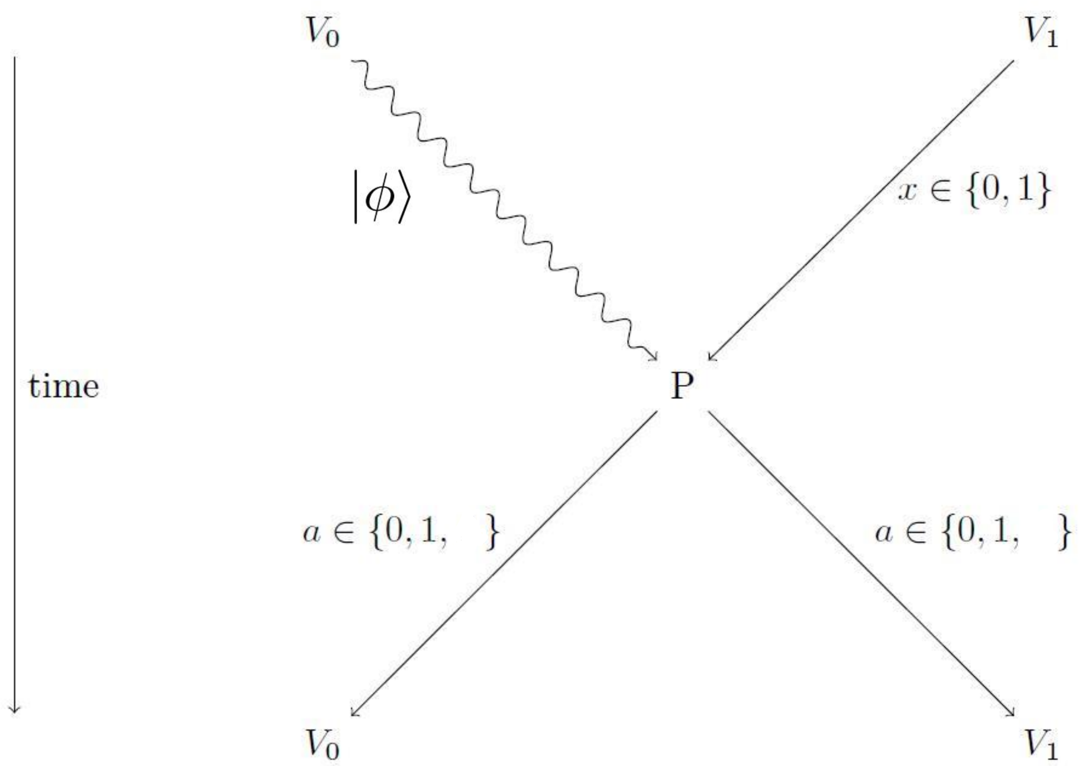

Photon loss
Entanglement
8
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.



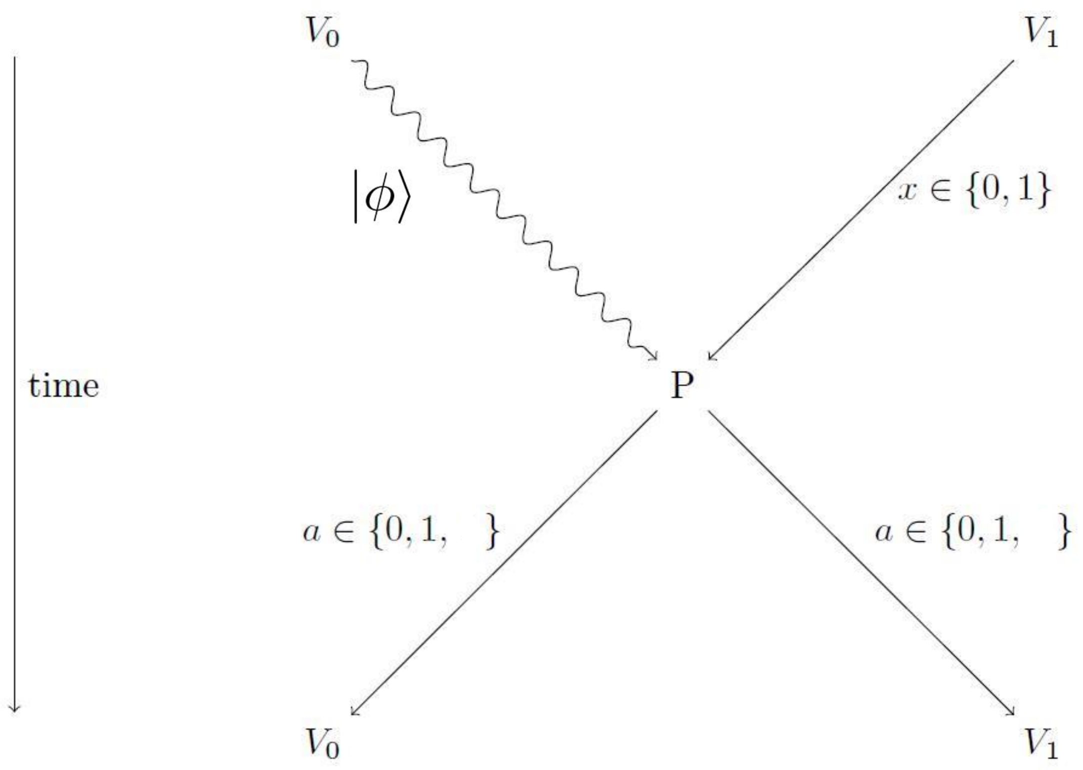
Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.

Step 1. Let's analyze the loss

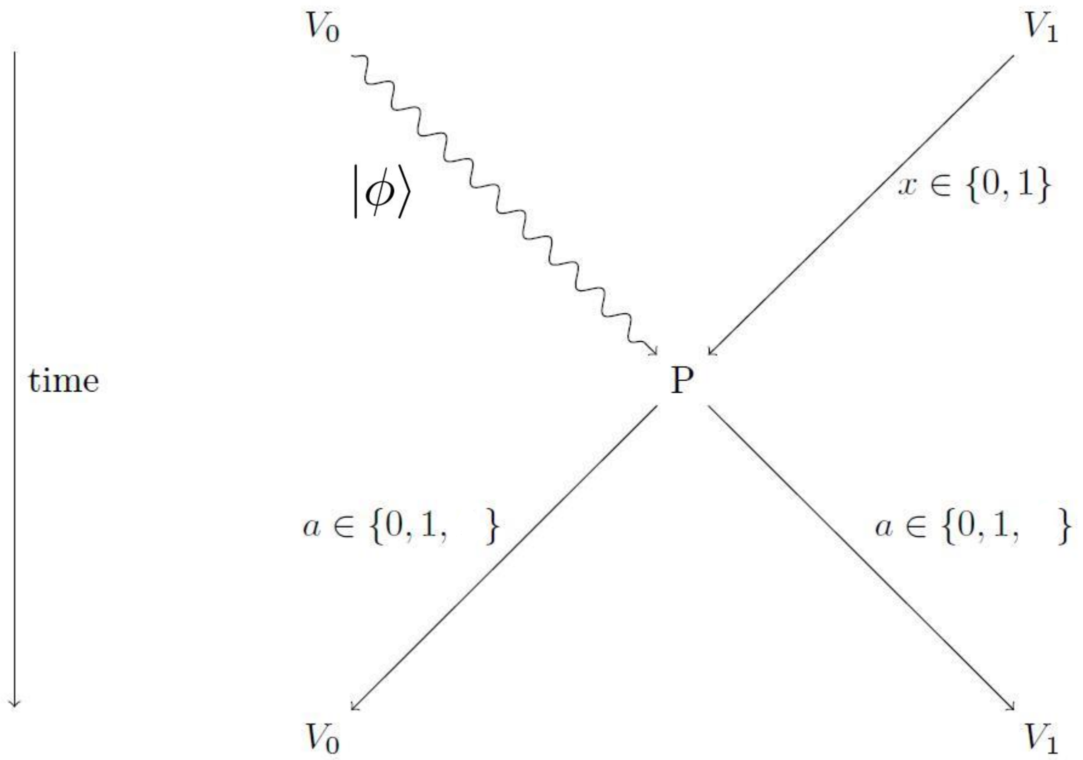
$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$



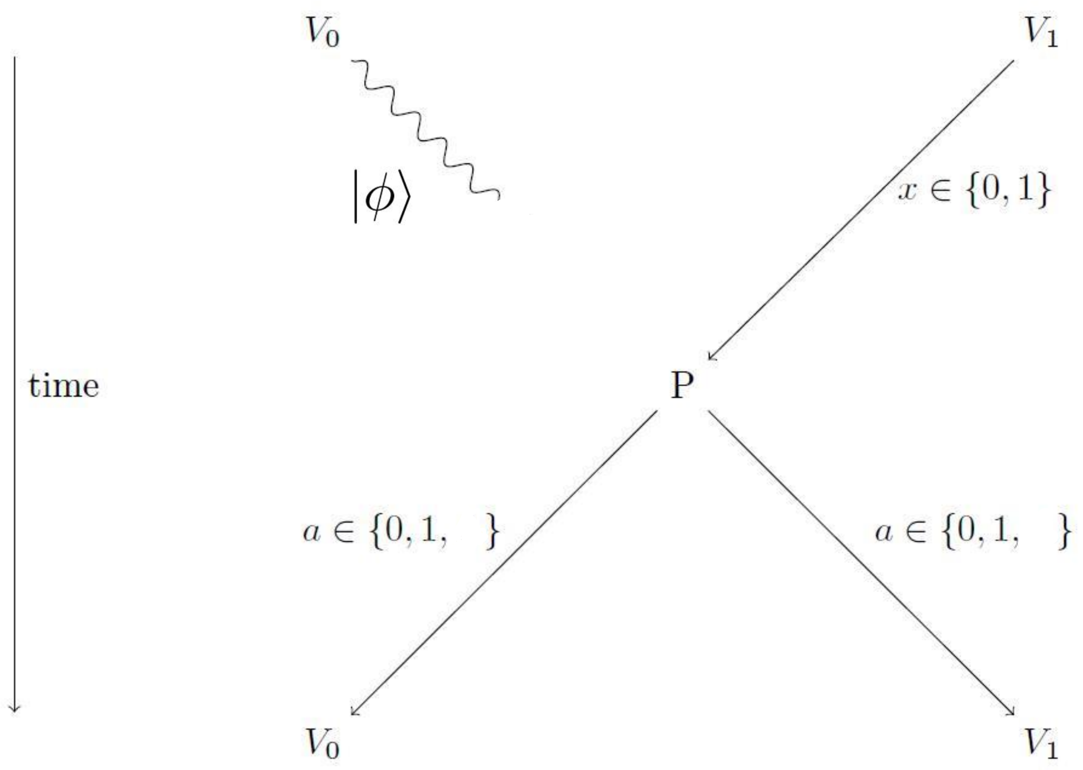
$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$



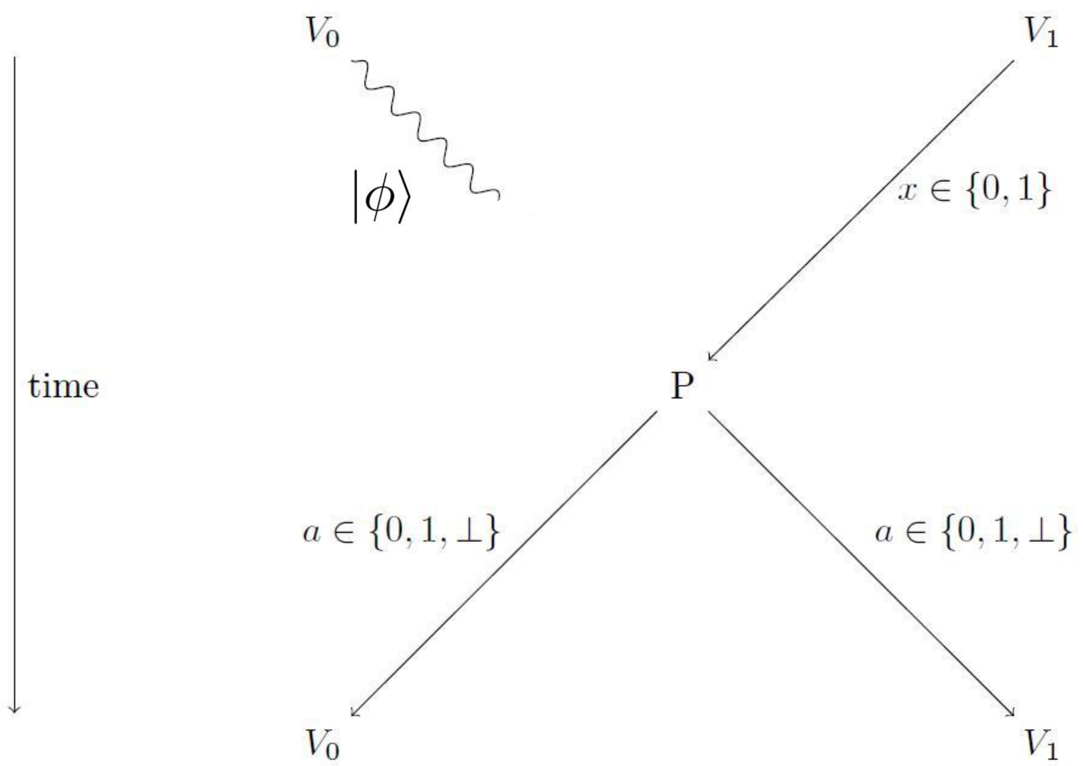
$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$



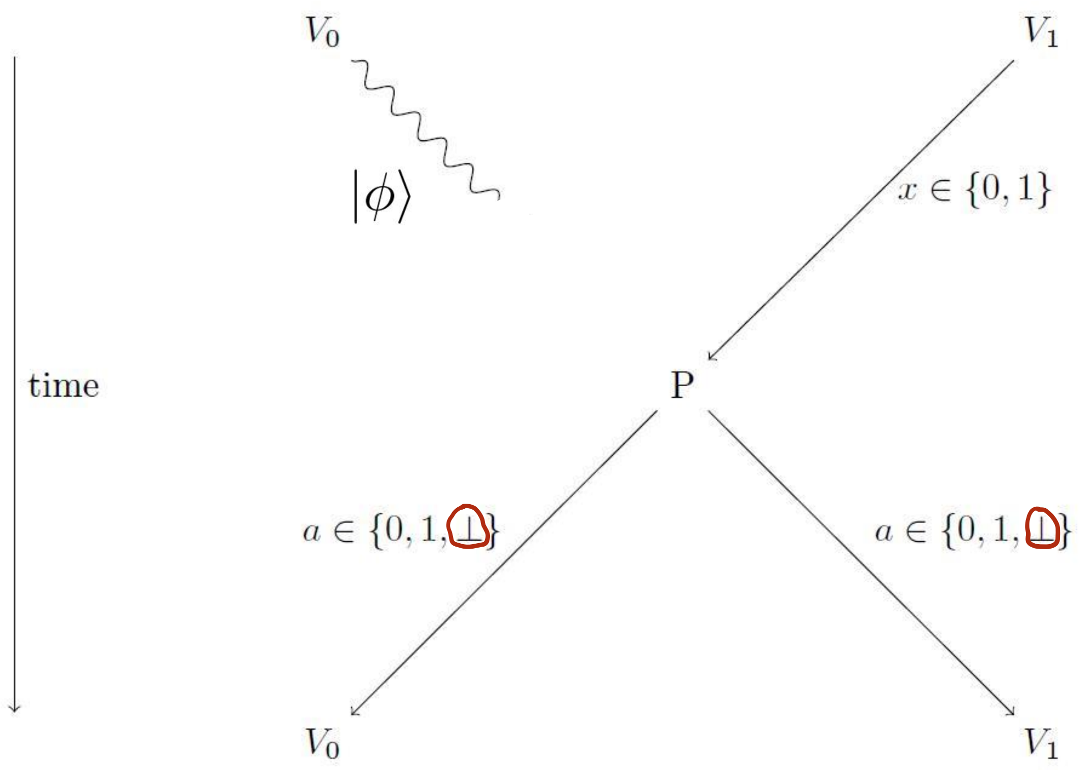
$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$



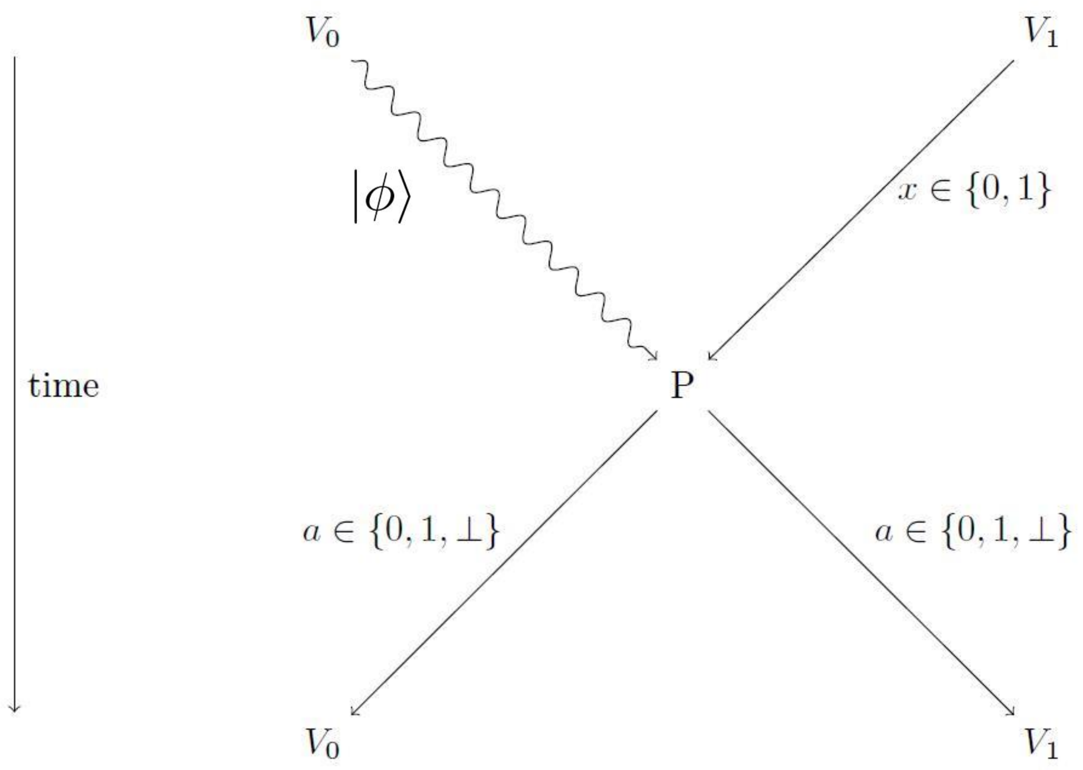
$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$



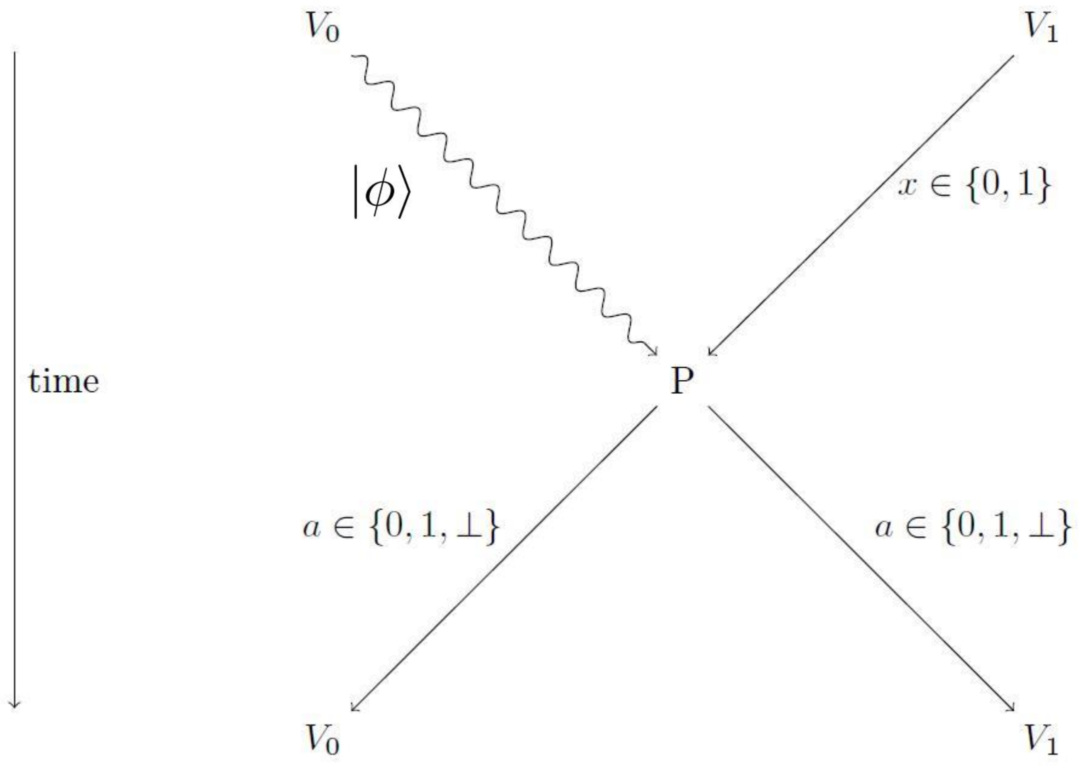
$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$



$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

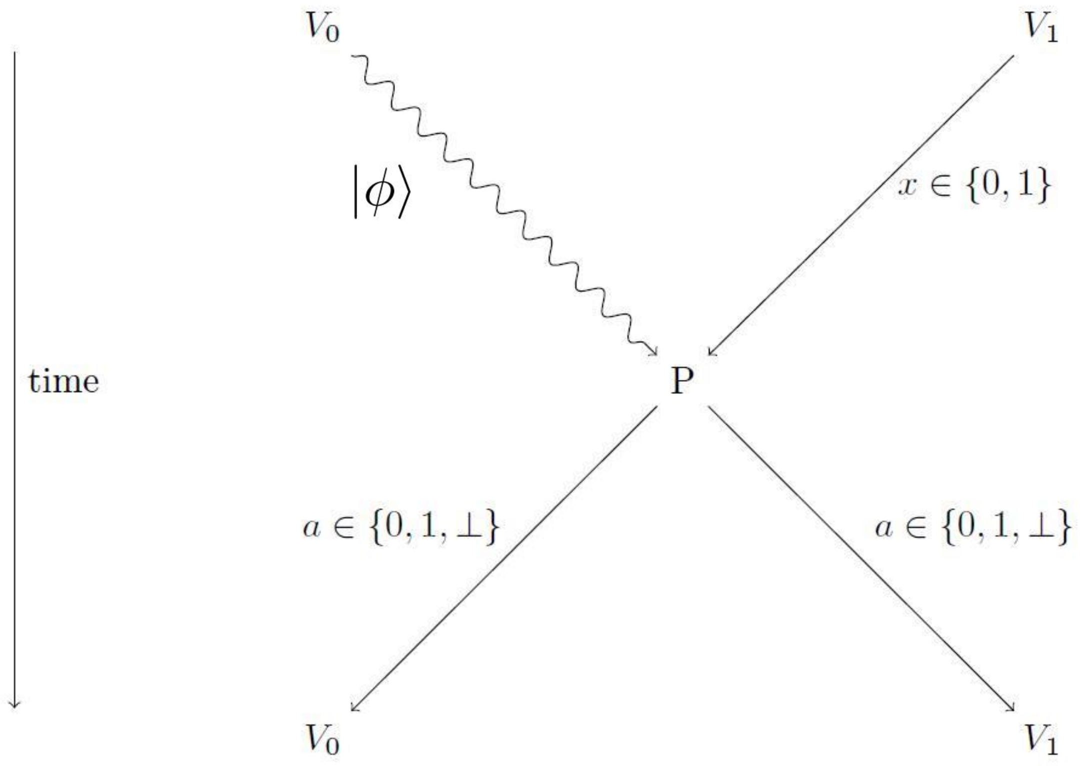


$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$



Given an error p_{err},
the prover is going to be correct w.p.

$$\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$$



Given an error p_{err},
the prover is going to be correct w.p.

$$p_{\mathrm{C}} = \eta(1 - p_{err})$$

Security:
unentangled attackers

$$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$$

Security:
unentangled attackers

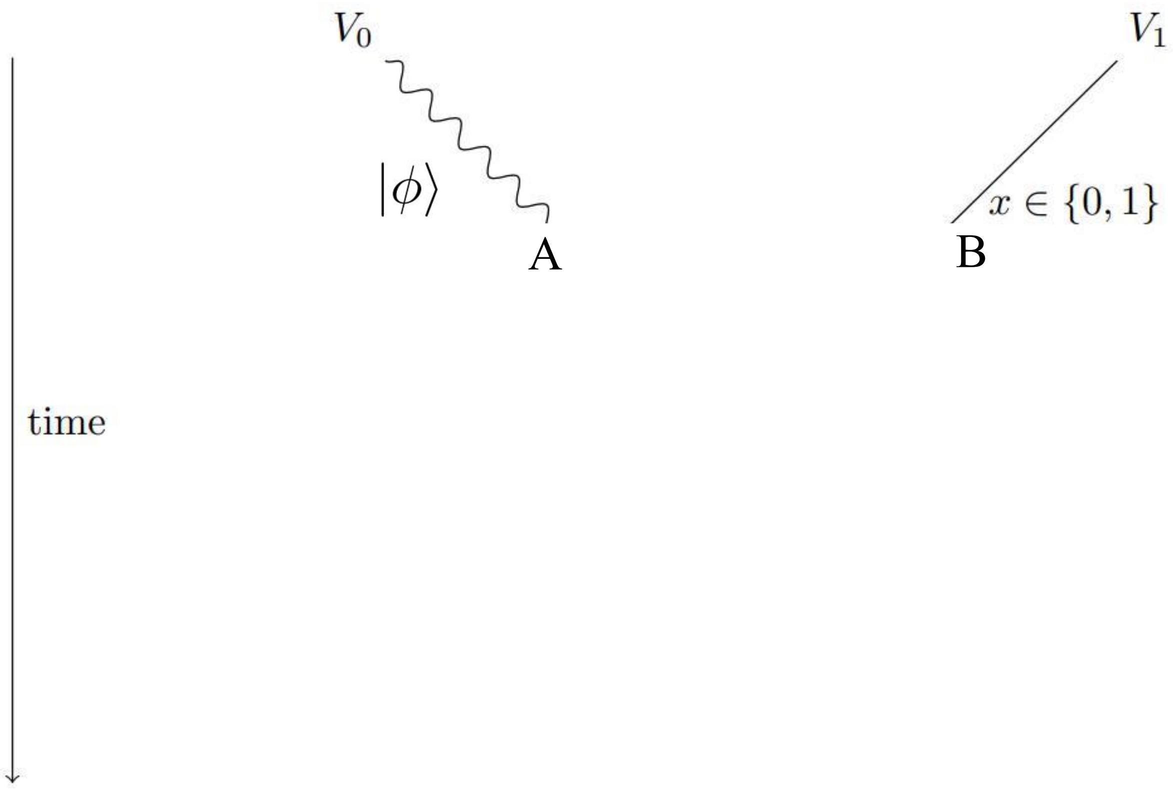
$$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$$

Goal: to upper bound attackers' prob of answering correctly q_{C}

$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

Security:
unentangled attackers

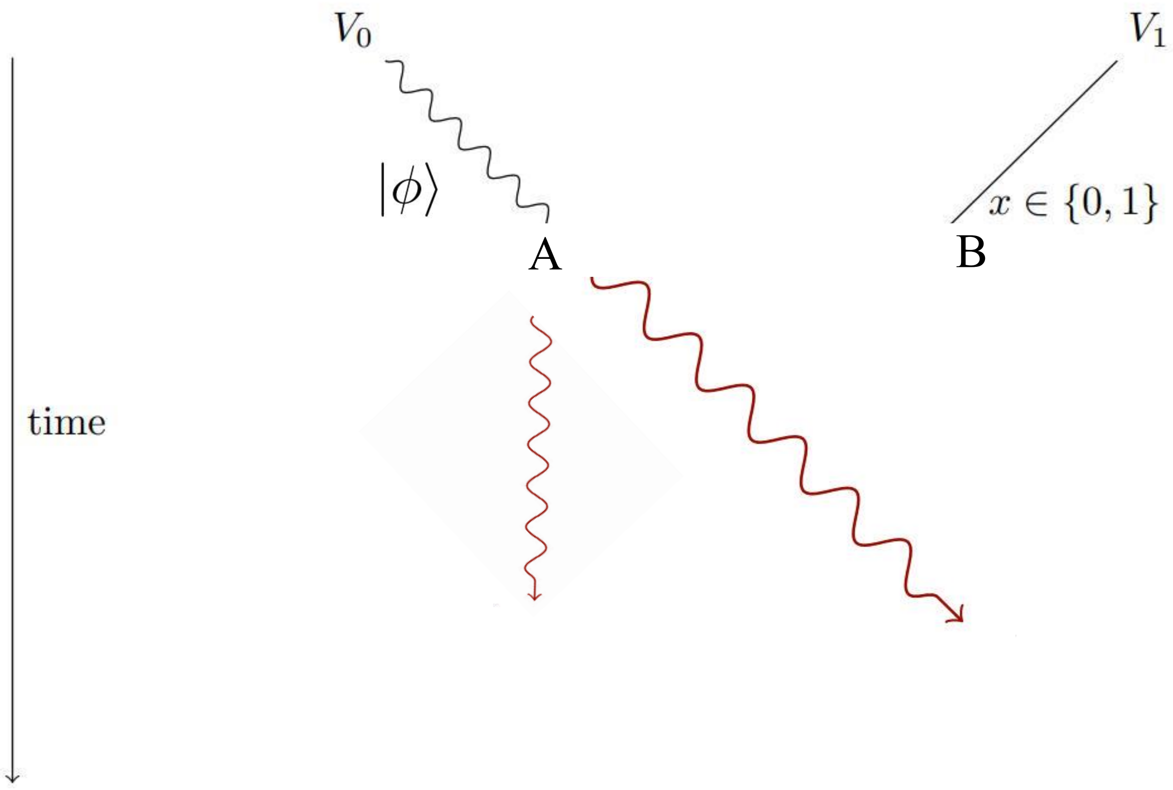
Goal: to upper bound attackers' prob of answering correctly q_{C}



Security:
unentangled attackers

$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

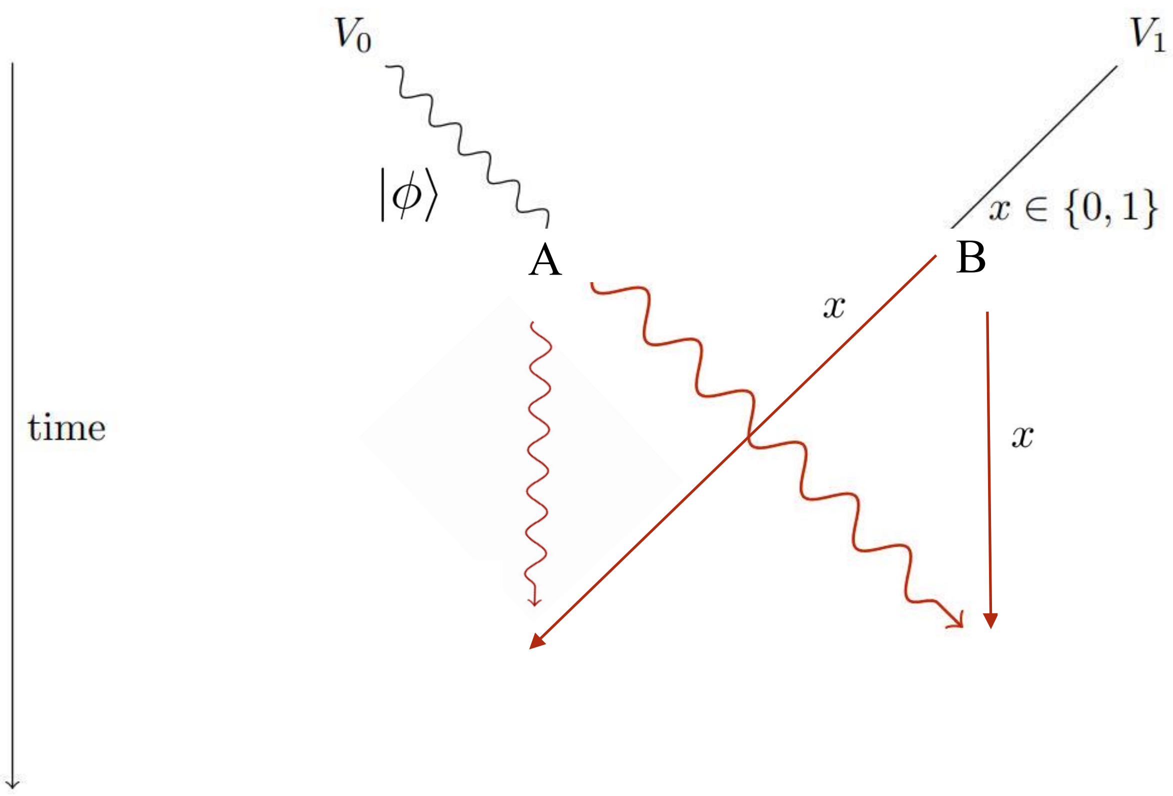
Goal: to upper bound attackers' prob of answering correctly q_{C}



Security:
unentangled attackers

$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

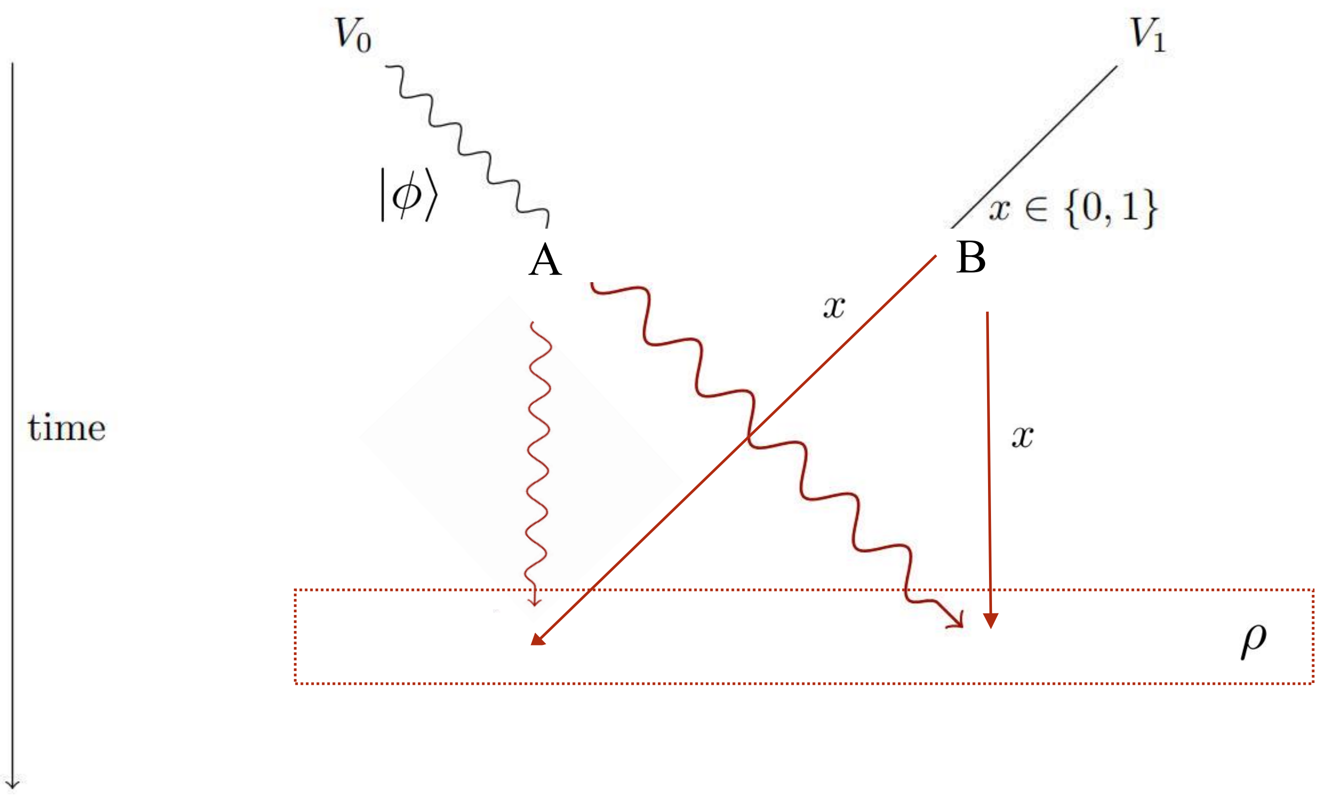
Goal: to upper bound attackers' prob of answering correctly q_{C}



Security:
unentangled attackers

$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

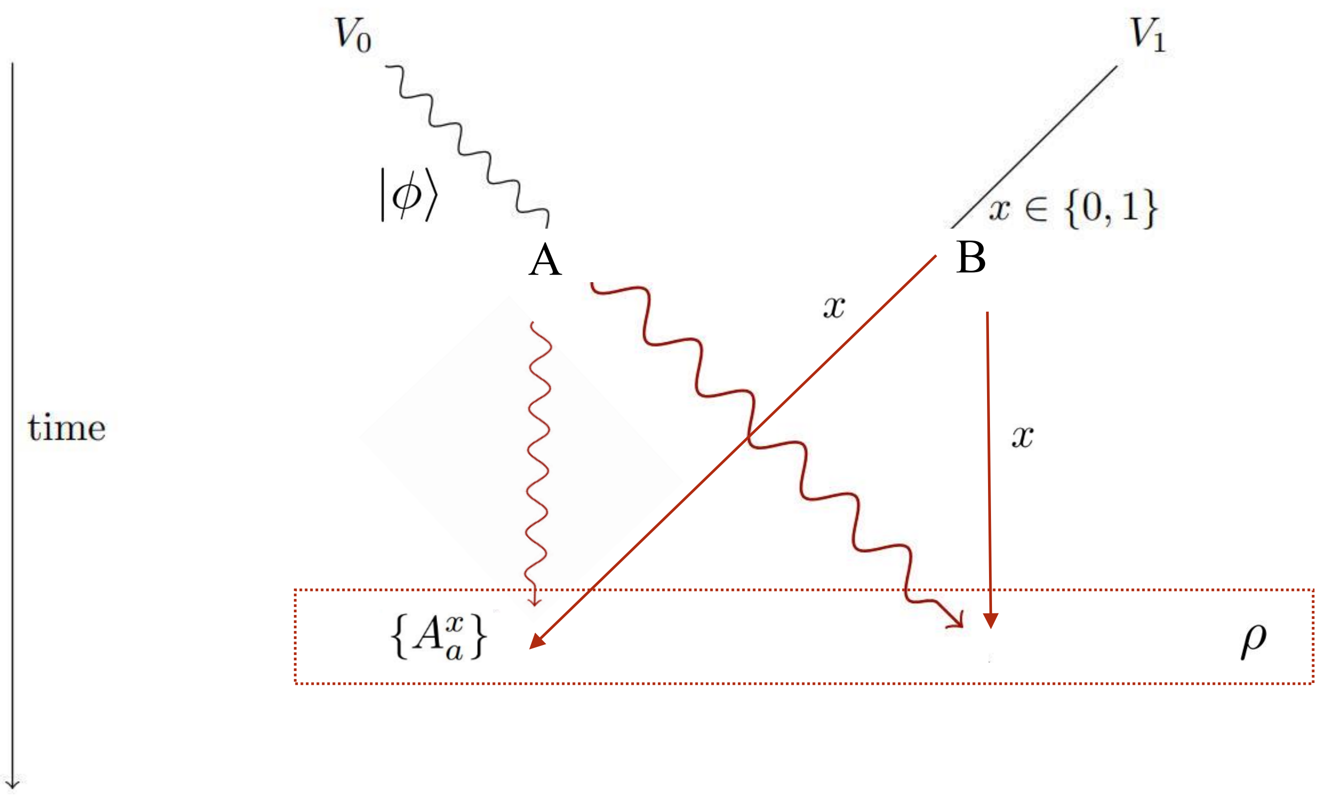
Goal: to upper bound attackers' prob of answering correctly q_{C}



Security:
unentangled attackers

$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

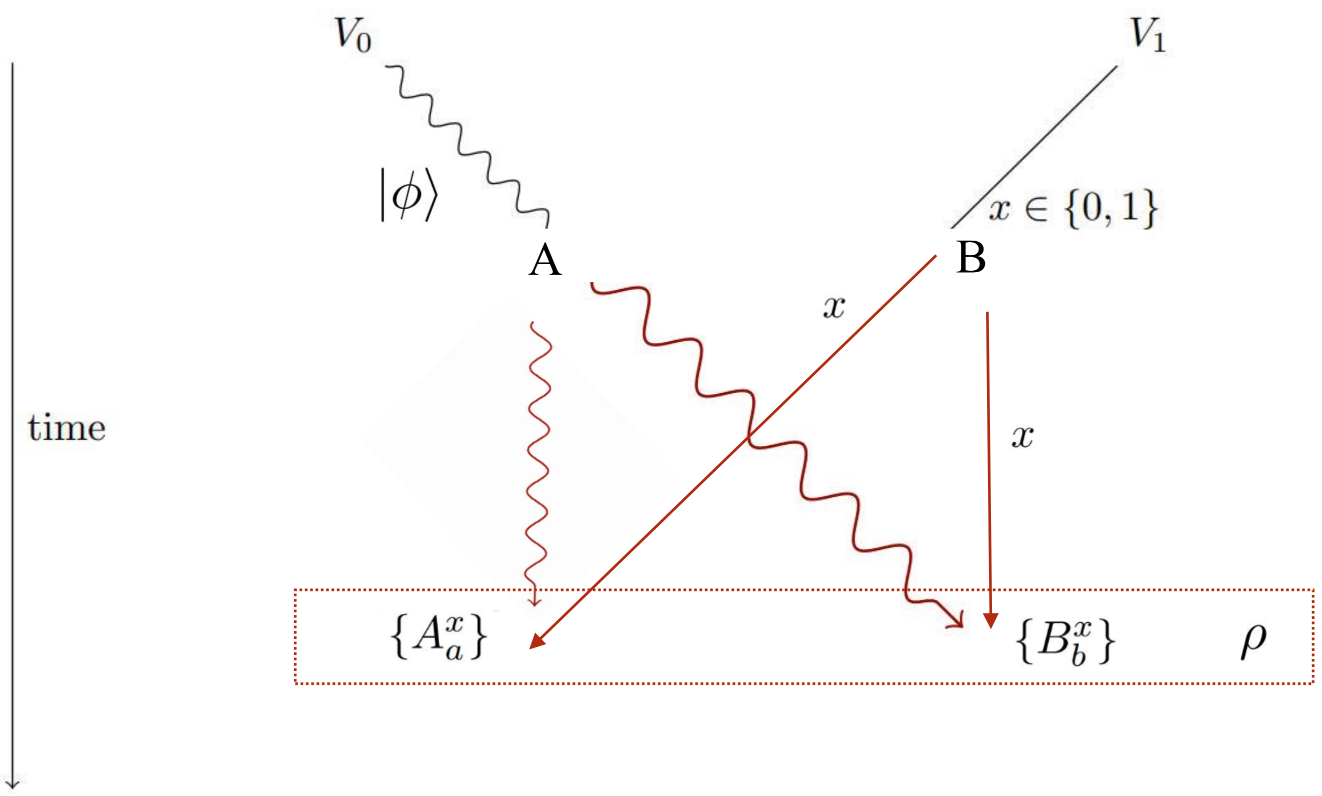
Goal: to upper bound attackers' prob of answering correctly q_{C}



Security:
unentangled attackers

$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

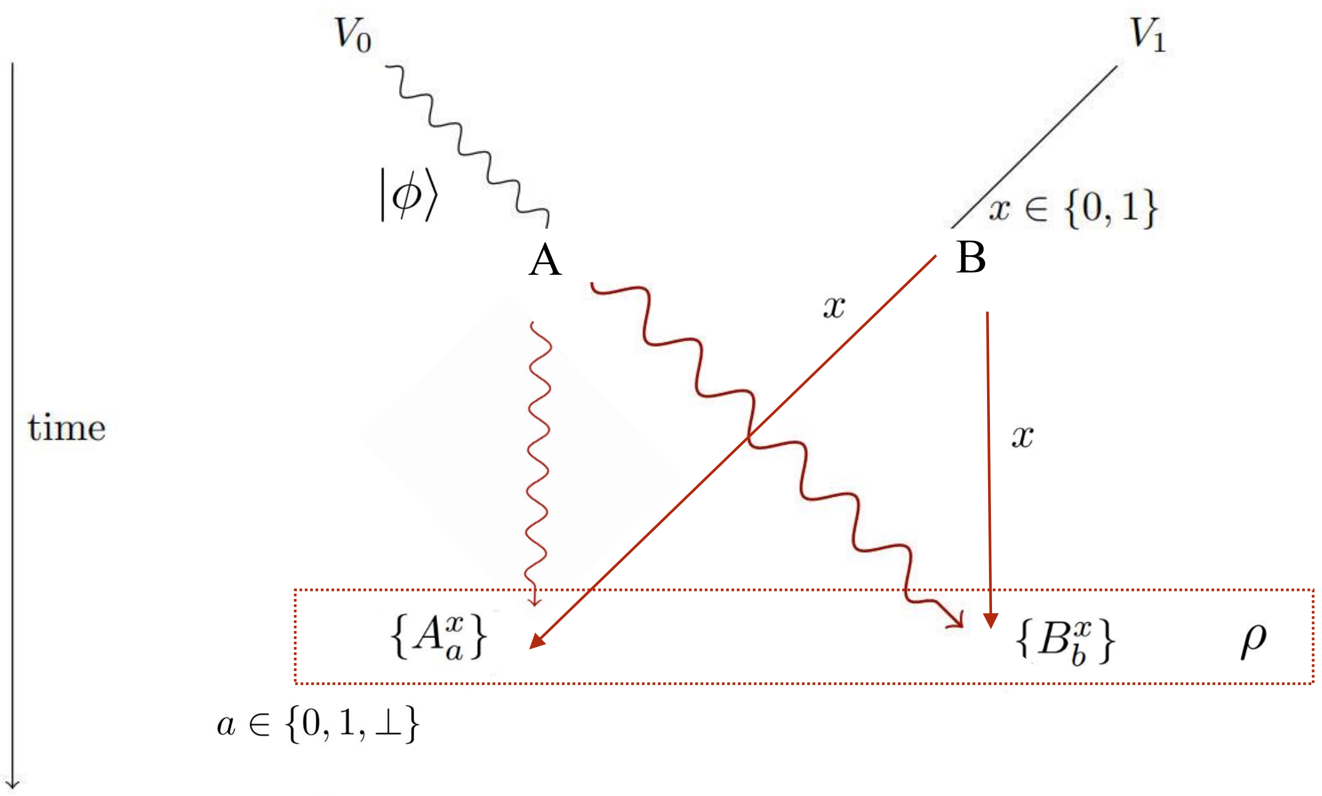
Goal: to upper bound attackers' prob of answering correctly q_{C}



Security:
unentangled attackers

$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

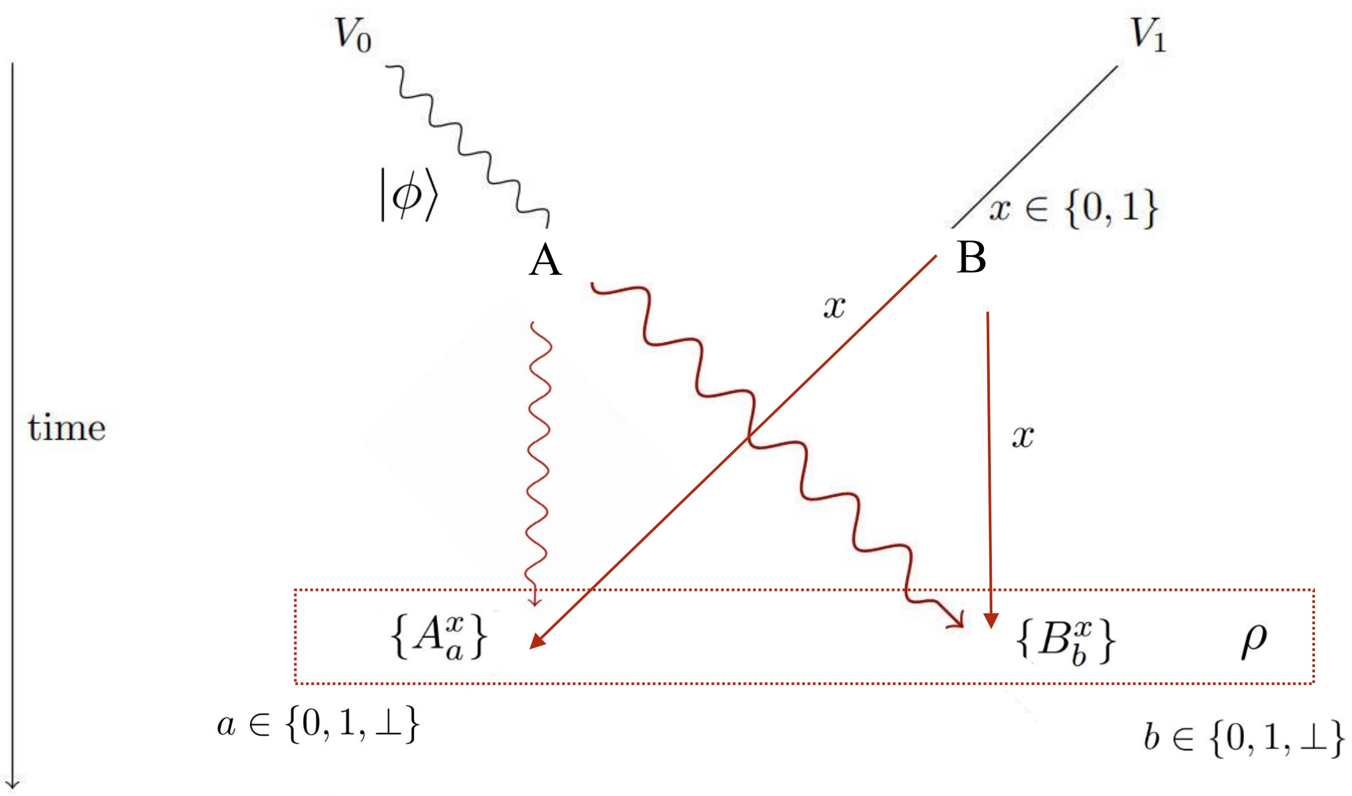
Goal: to upper bound attackers' prob of answering correctly q_{C}



$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

Security:
unentangled attackers

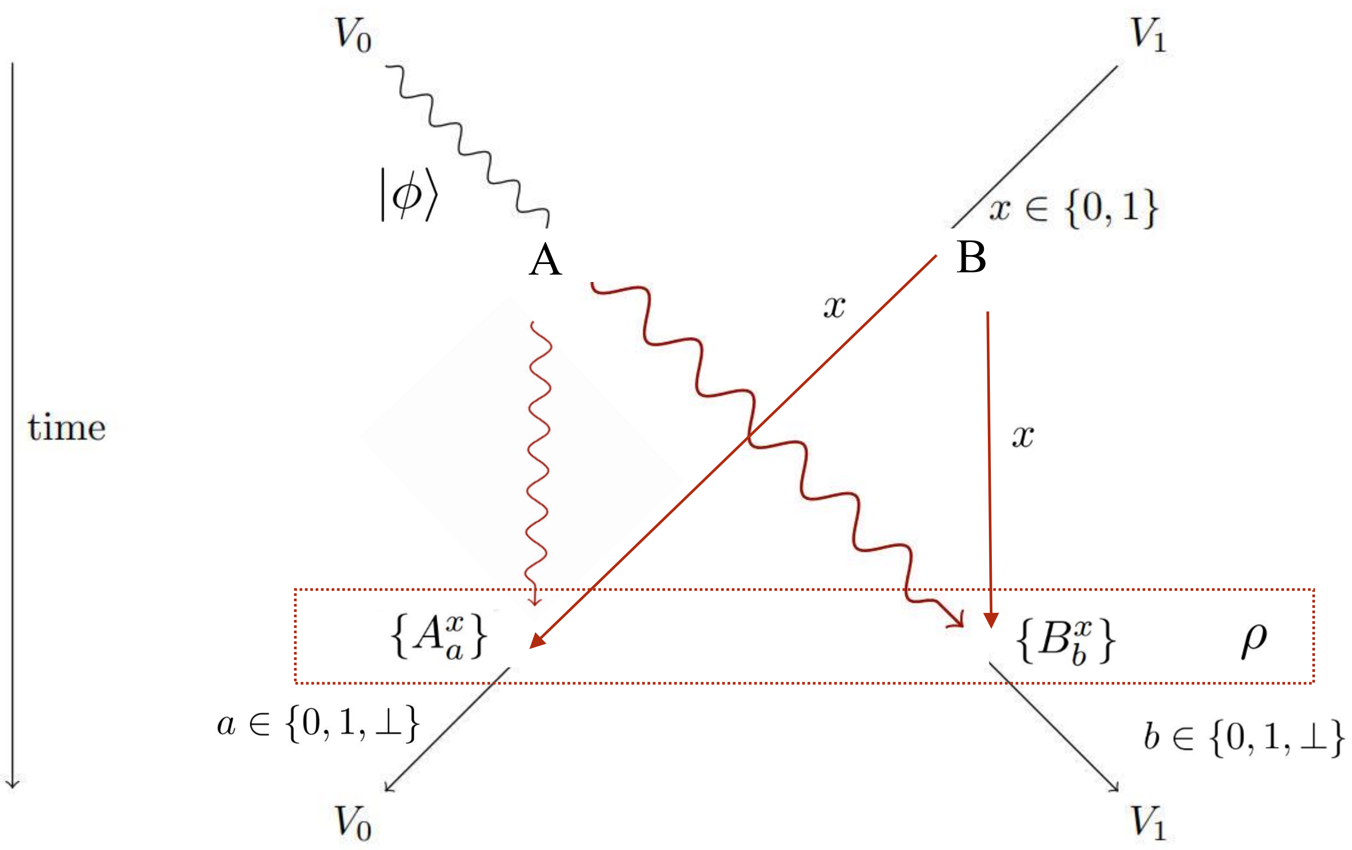
Goal: to upper bound attackers' prob of answering correctly q_{C}



Security:
unentangled attackers

$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

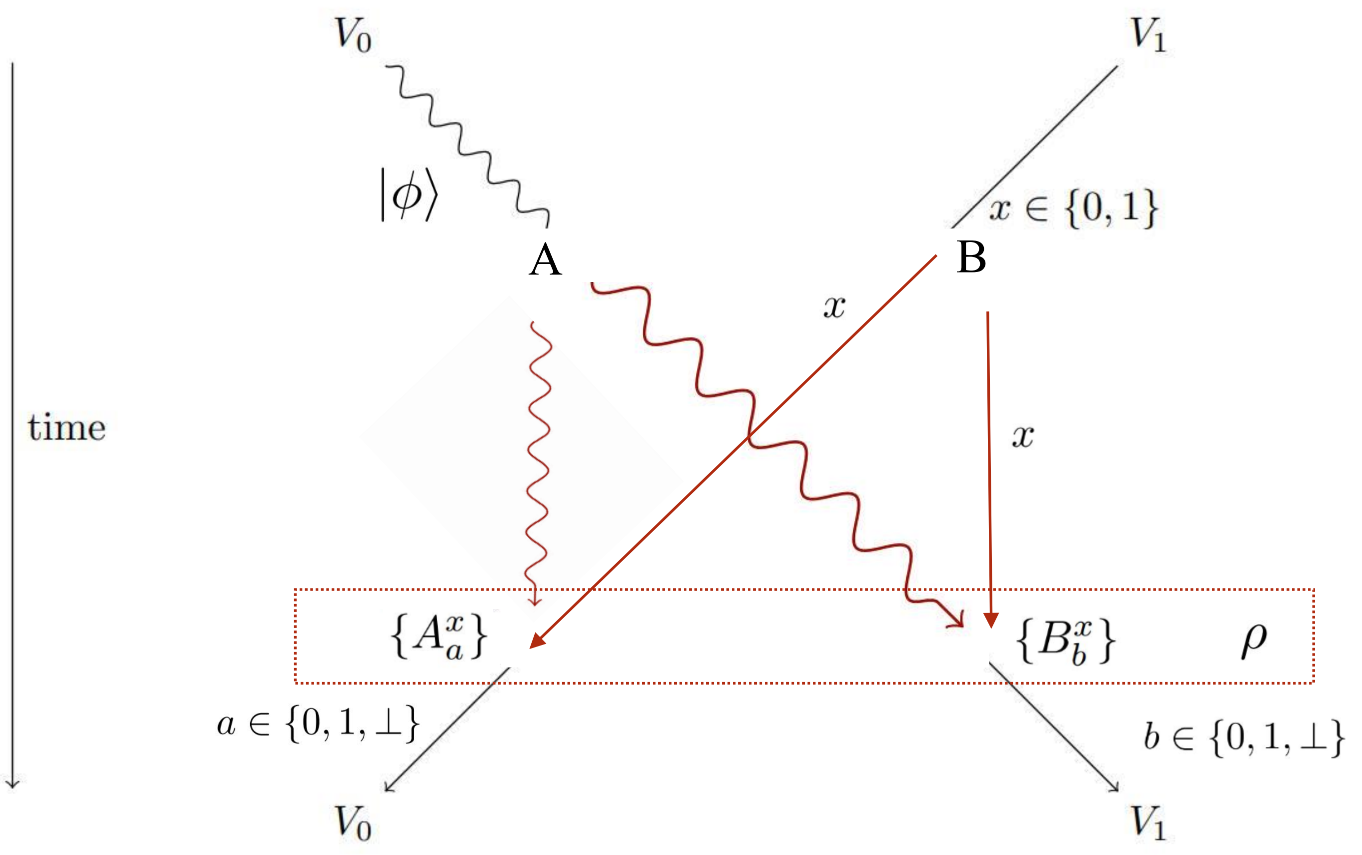
Goal: to upper bound attackers' prob of answering correctly q_{C}



Security:
unentangled attackers

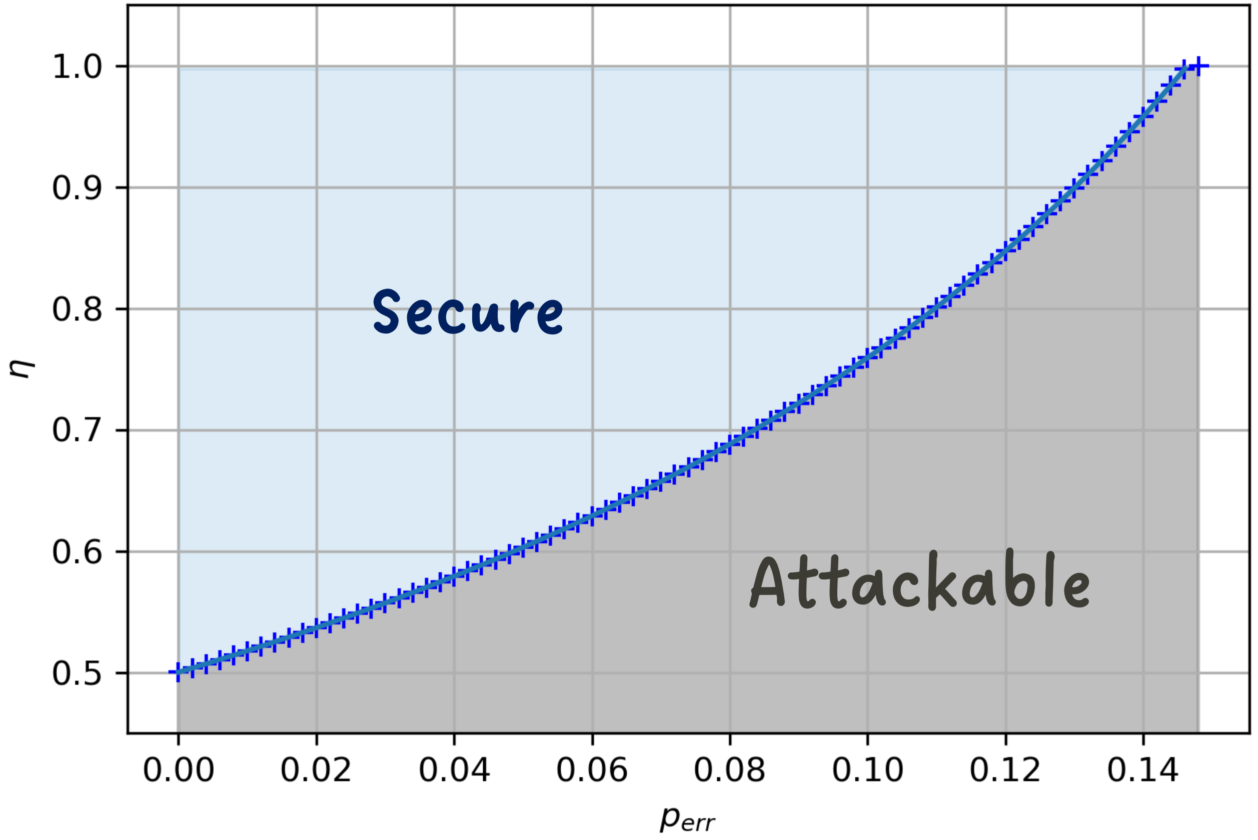
$\mathrm{QPV}^{\eta}_{\mathrm{BB84}}$

Goal: to upper bound attackers' prob of answering correctly q_{C}



Result $\quad q^*_{\mathrm{C}} = \cos^2\left(\frac{\pi}{8}\right)\eta + \sin^2\left(\frac{\pi}{8}\right)(1-\eta) \qquad \forall\ \eta \in [\frac{1}{2}, 1]$

In experimental parameters, the result translates to

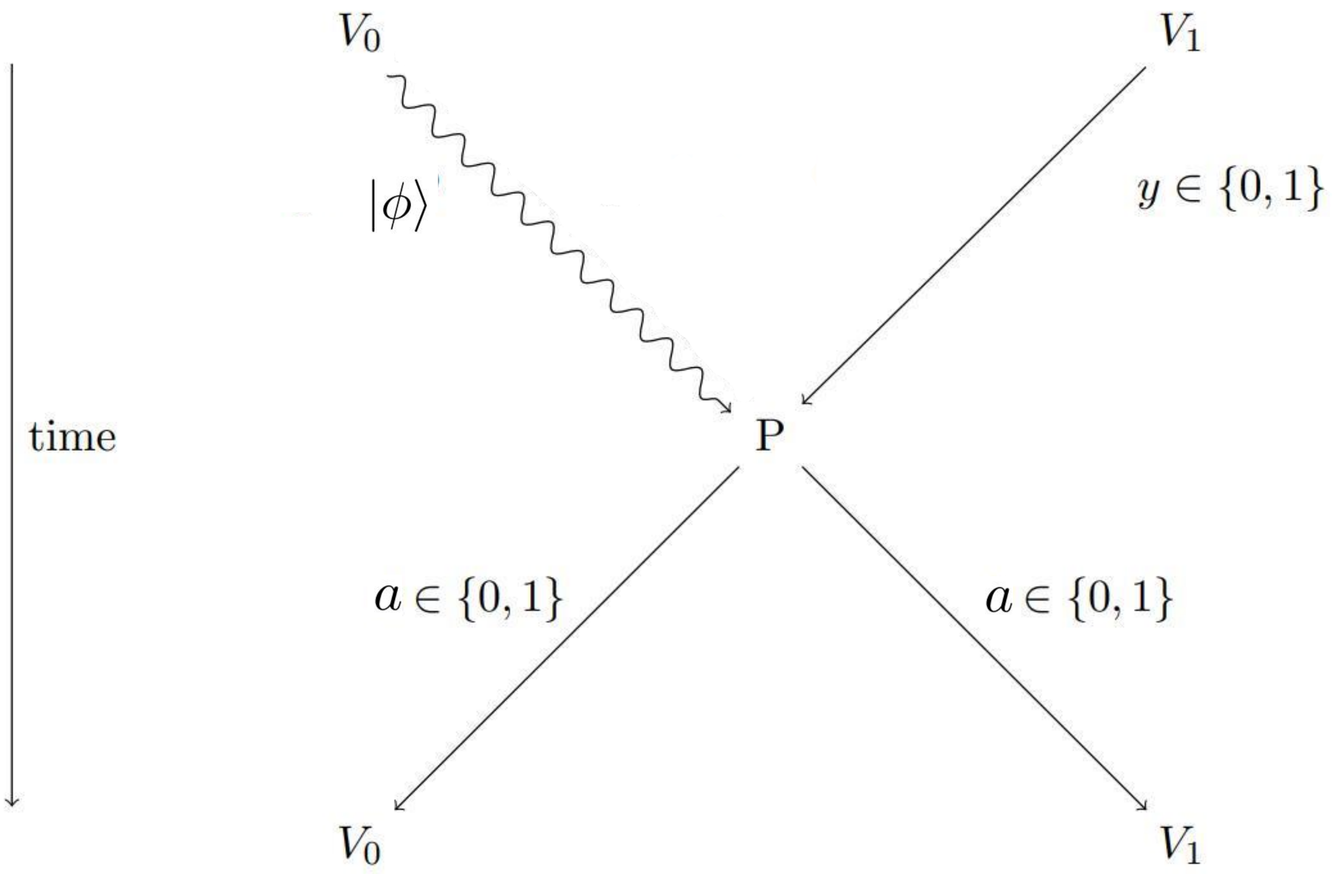


But still insecure if the attackers pre-share one EPR pair

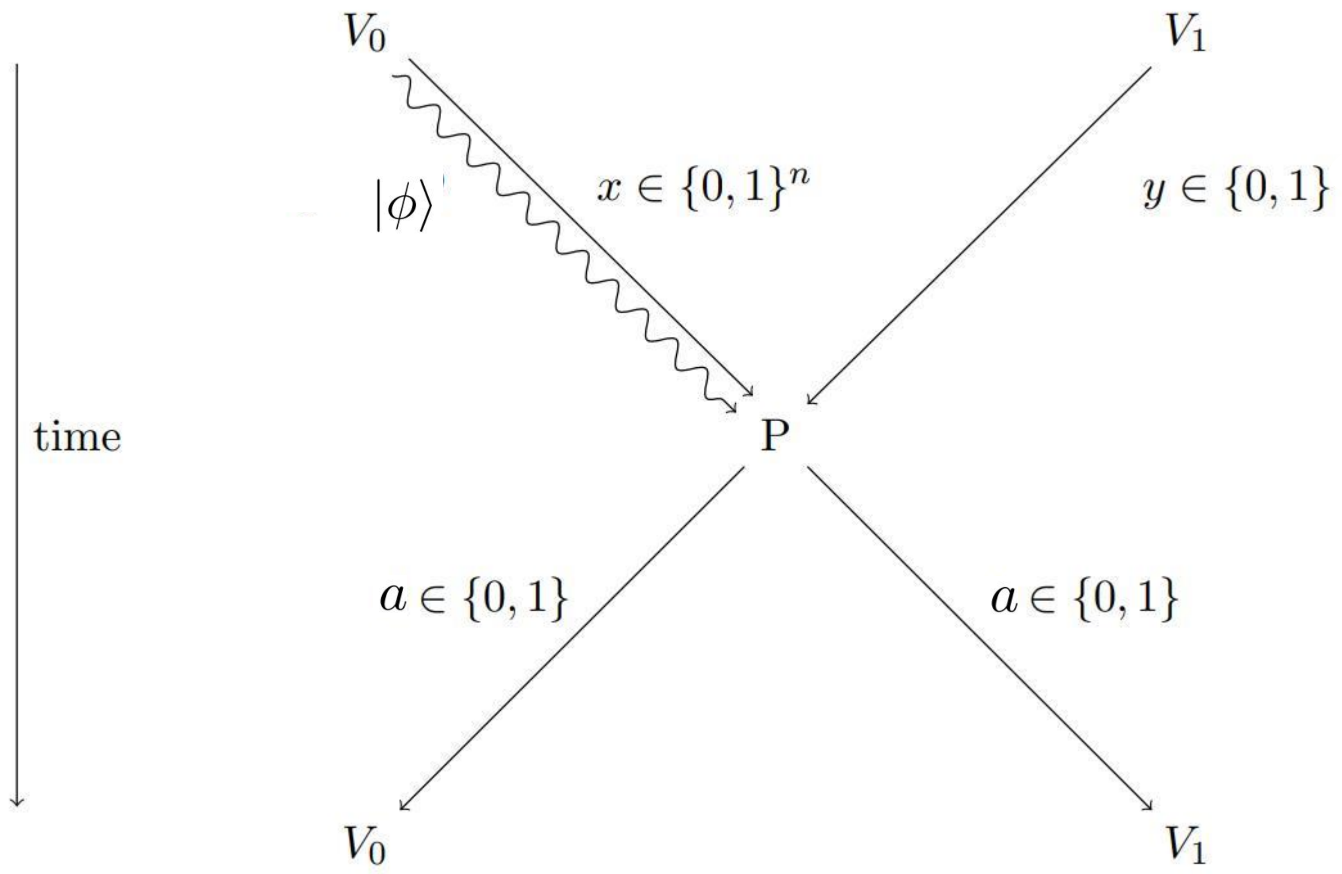
But still insecure if the attackers pre-share one EPR pair

Step 2. Using Step 1 to fix it

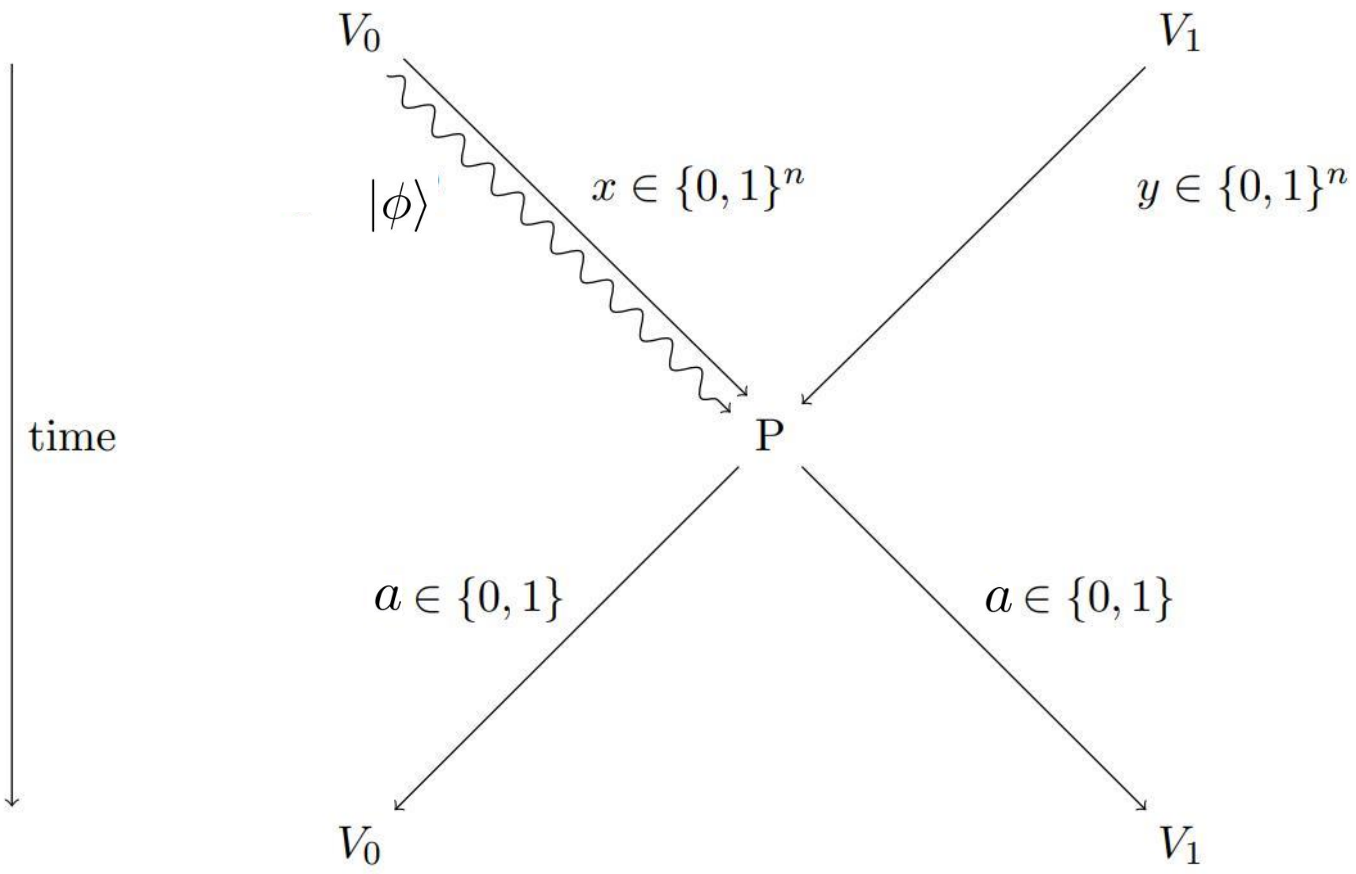
$\mathrm{QPV}_{\mathrm{BB84}}^{,f}$



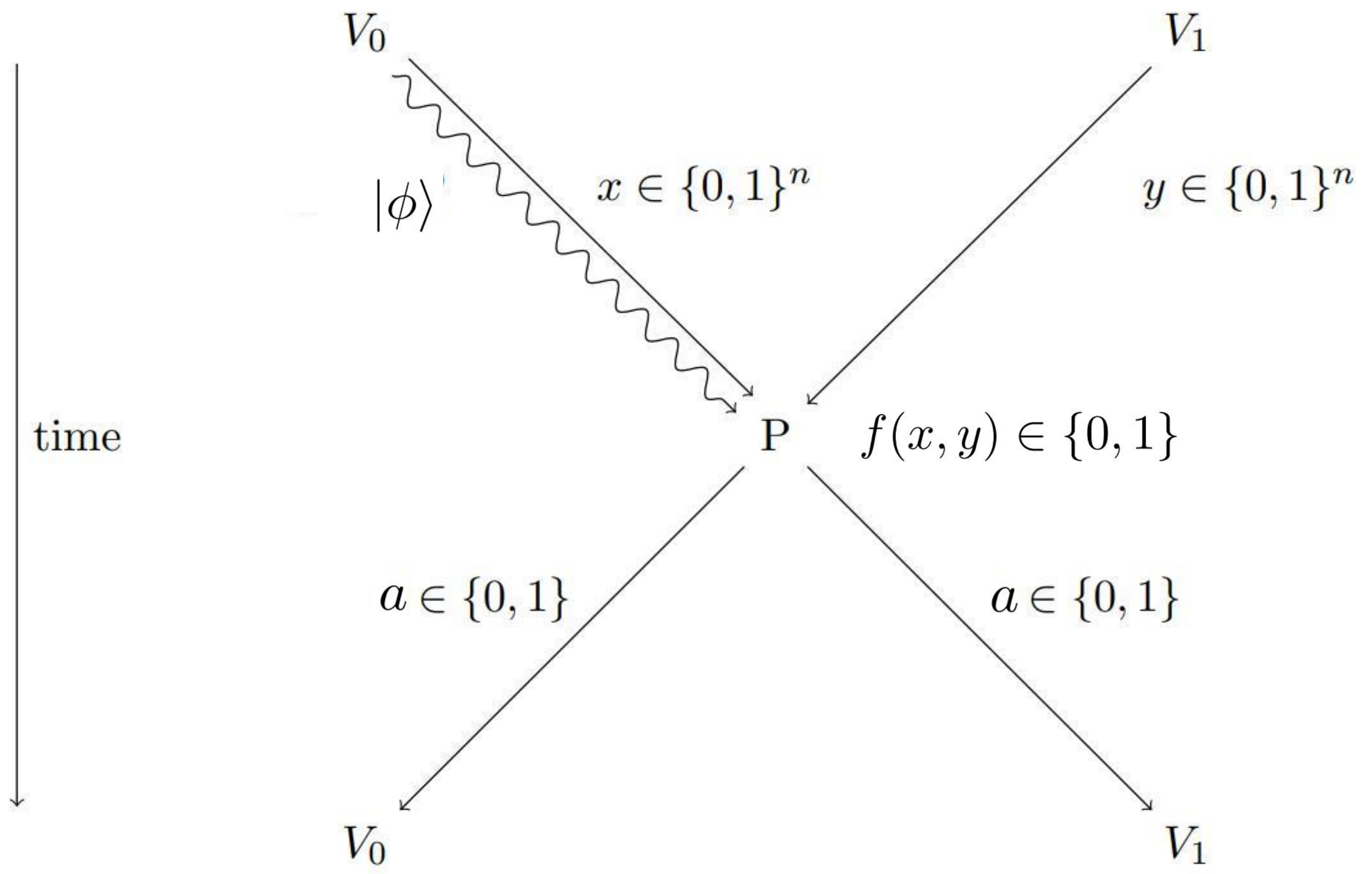
$\mathrm{QPV}_{\mathrm{BB84}}^{,f}$



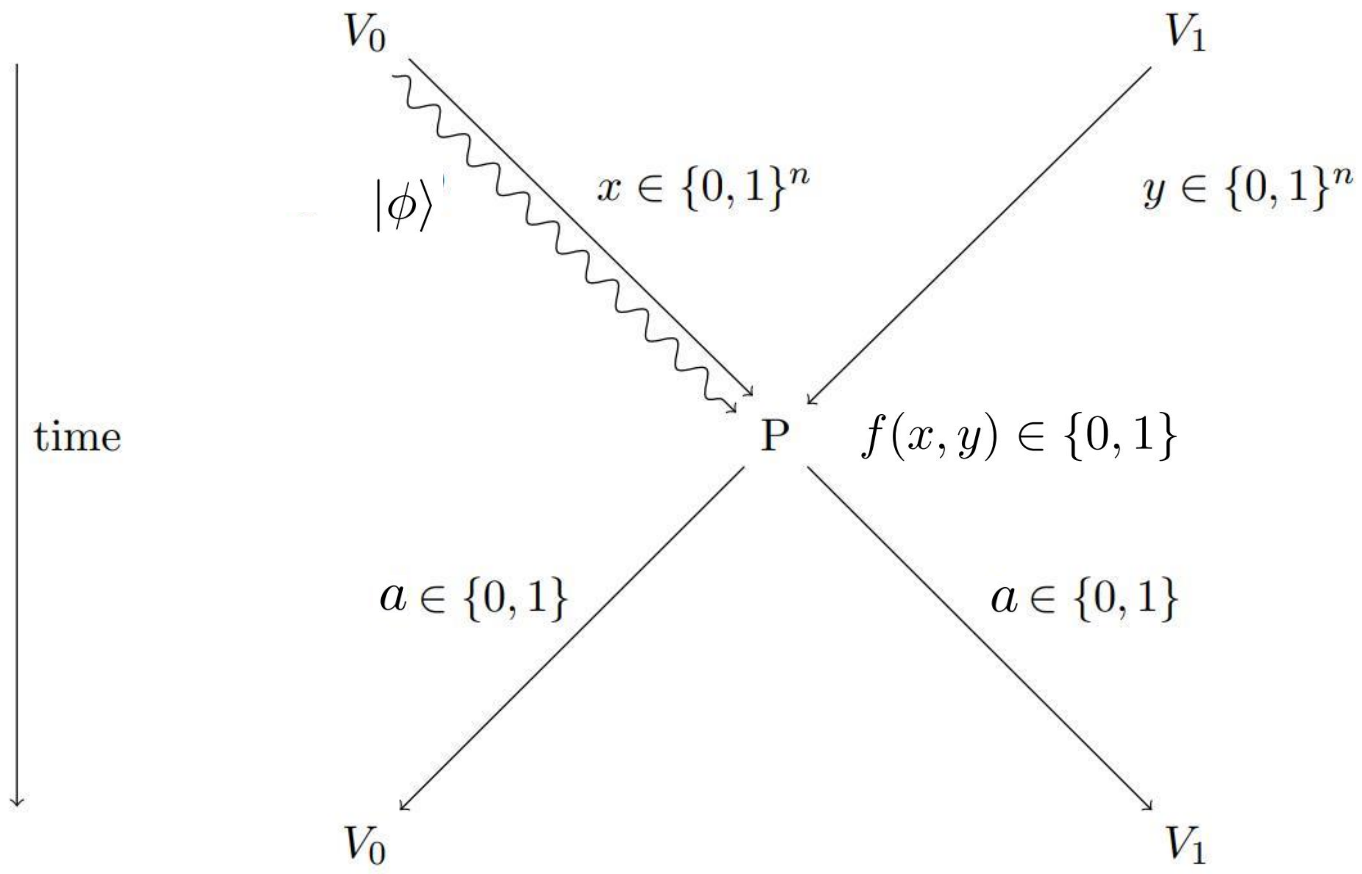
$\mathrm{QPV}^{,f}_{\mathrm{BB84}}$



$\mathrm{QPV}_{\mathrm{BB84}}^{,f}$

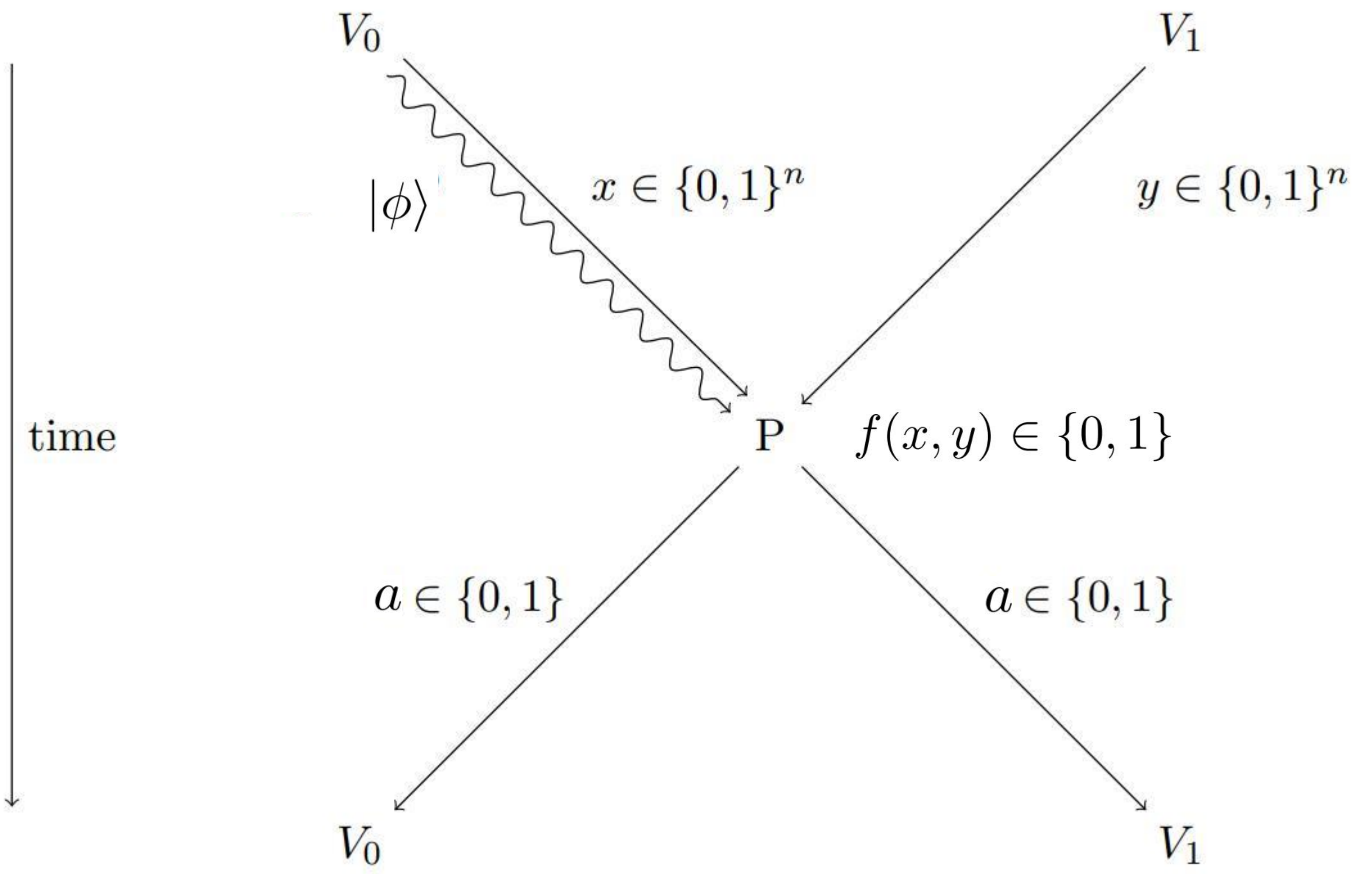


$\mathrm{QPV}^{,f}_{\mathrm{BB84}}$



Extension proven secure [BCS22]

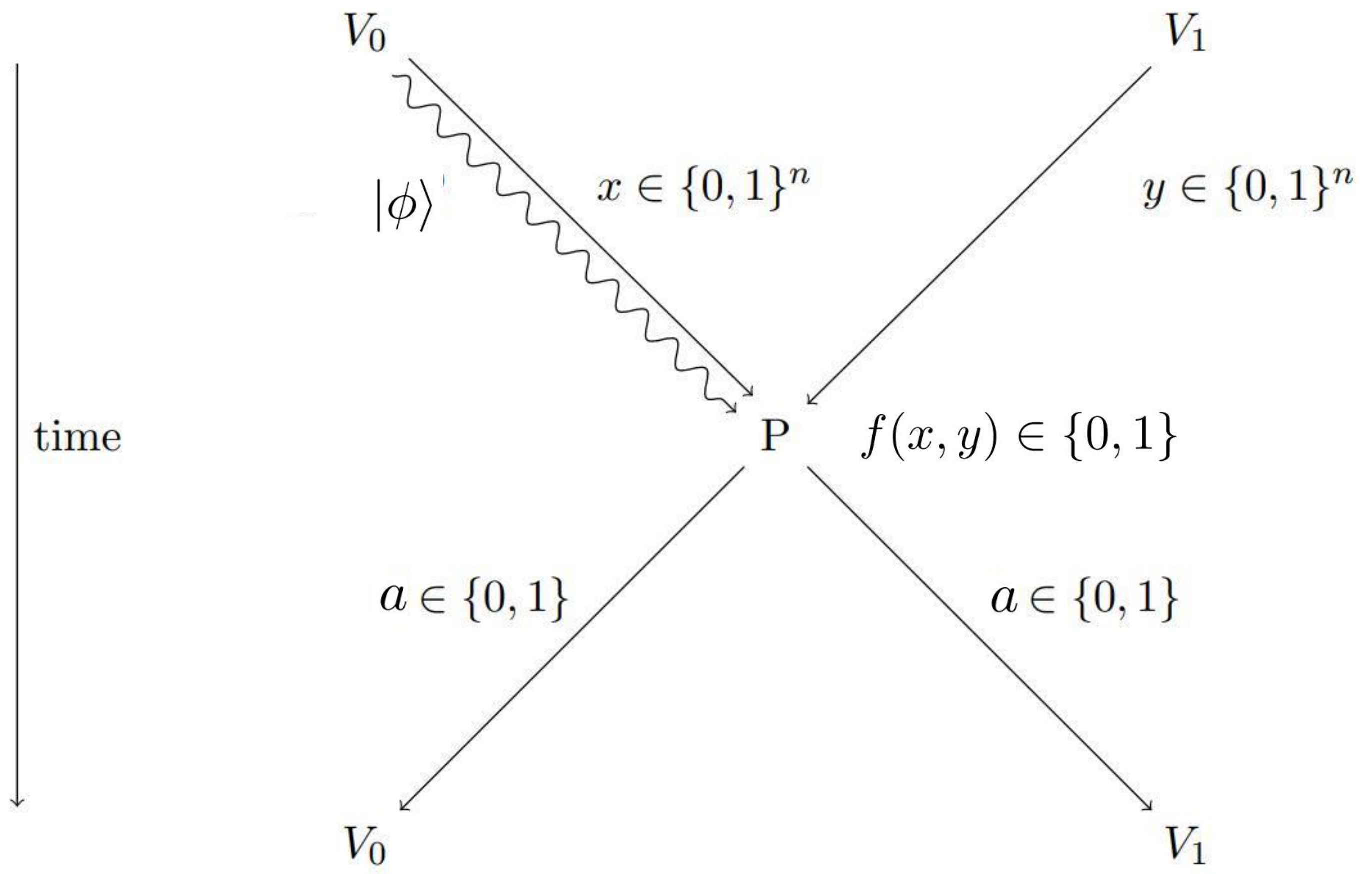
$\mathrm{QPV}_{\mathrm{BB84}}^{,f}$



Extension proven secure [BCS22]

1. by attackers that pre-share entanglement, and

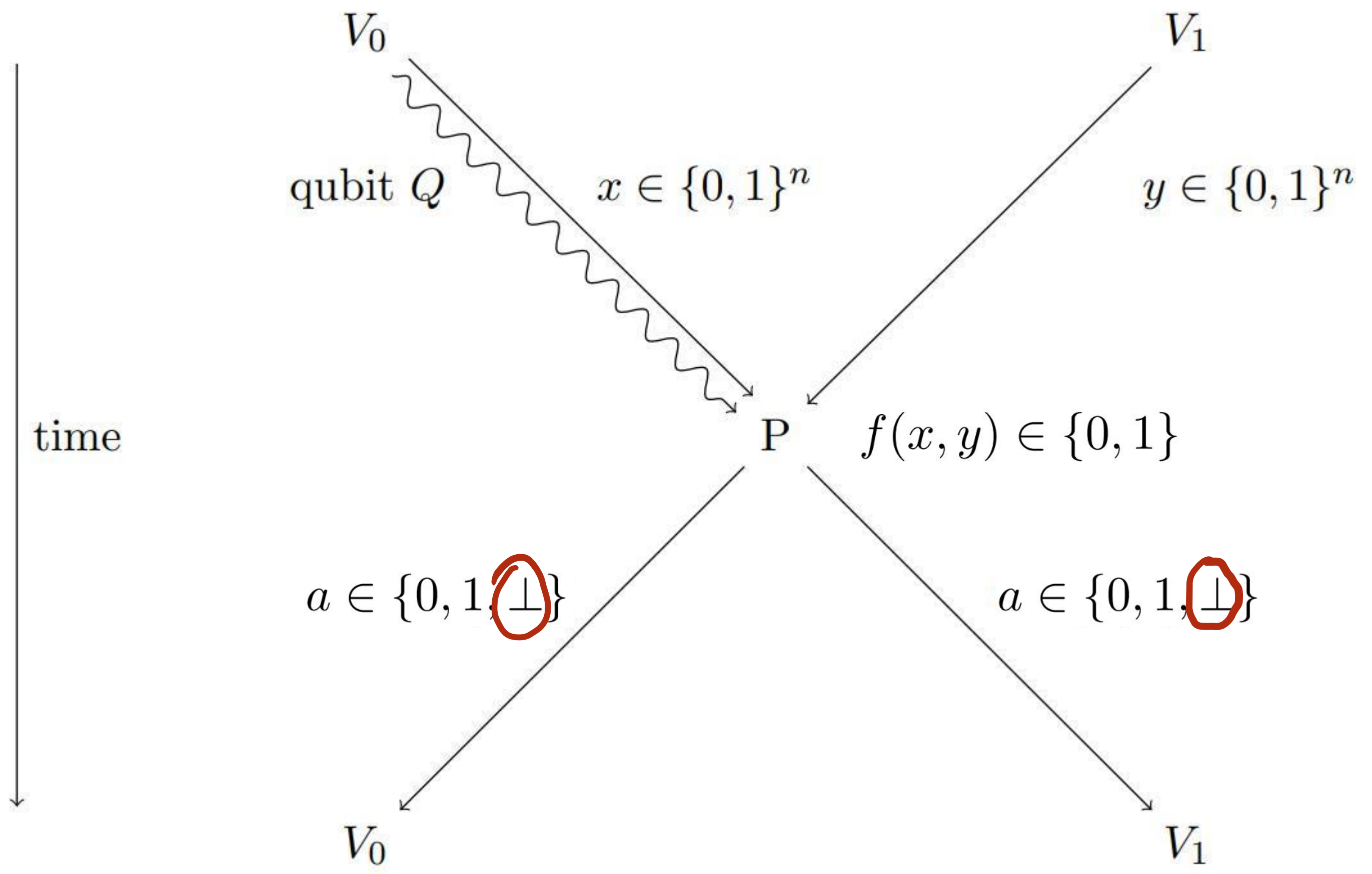
$\mathrm{QPV}_{\mathrm{BB84}}^{,f}$



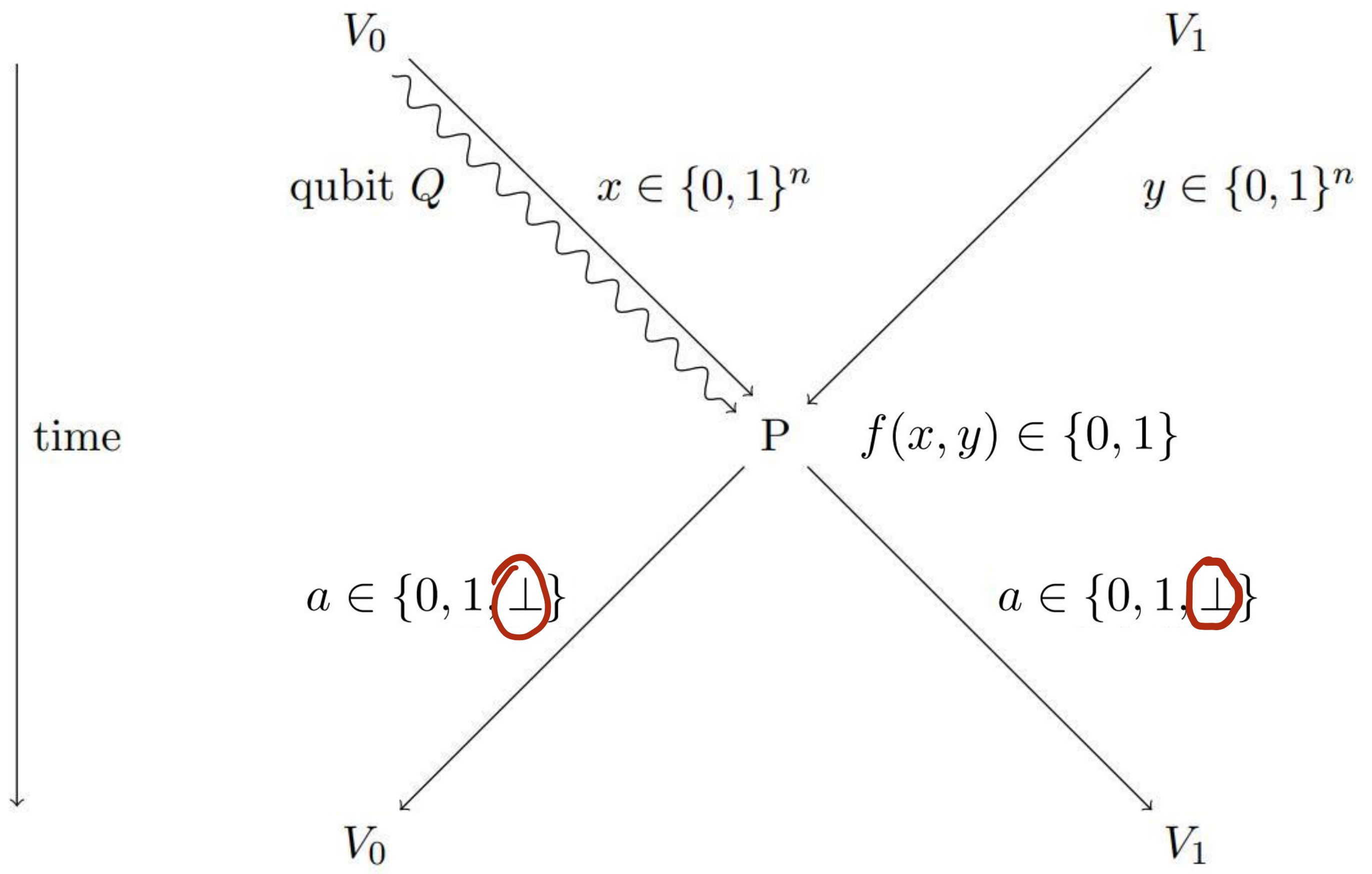
Extension proven secure [BCS22]

1. by attackers that pre-share entanglement, and
2. arbitrary slow quantum information

We introduce $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$

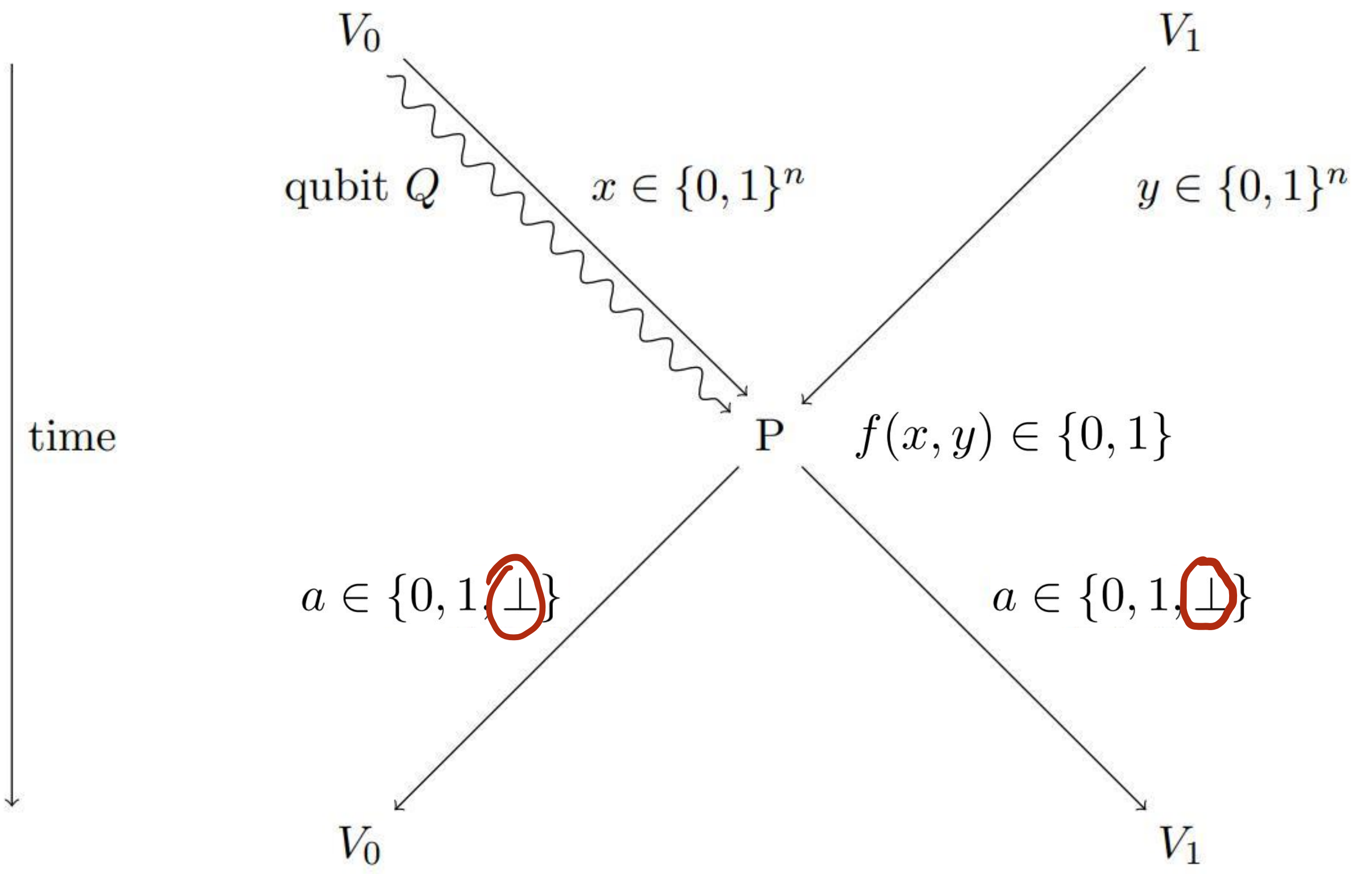


$\mathrm{QPV}_{\mathrm{BB84}}^{\eta, f}$

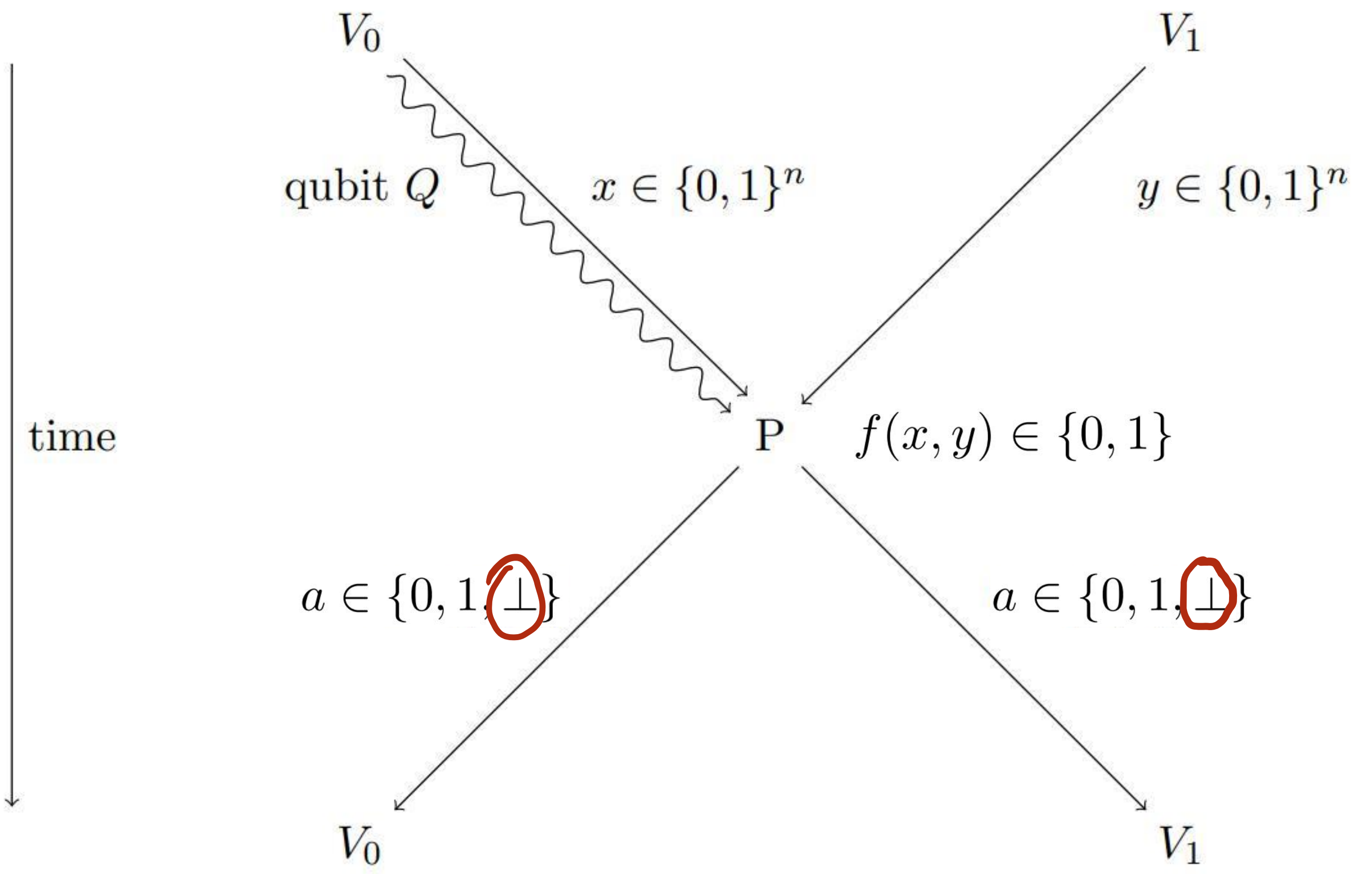


$\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$

Previous result with loss

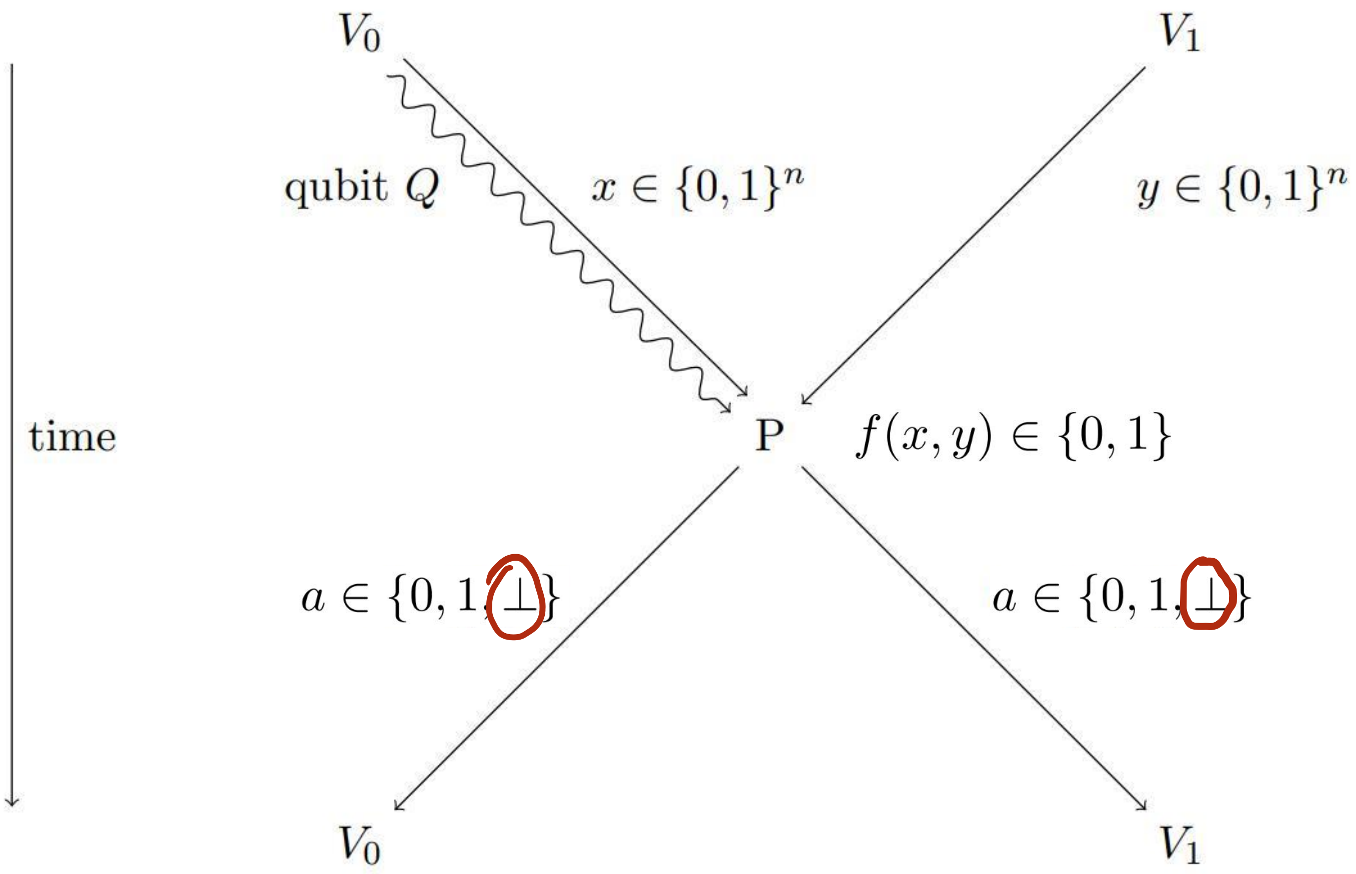


$\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$



Previous result with loss

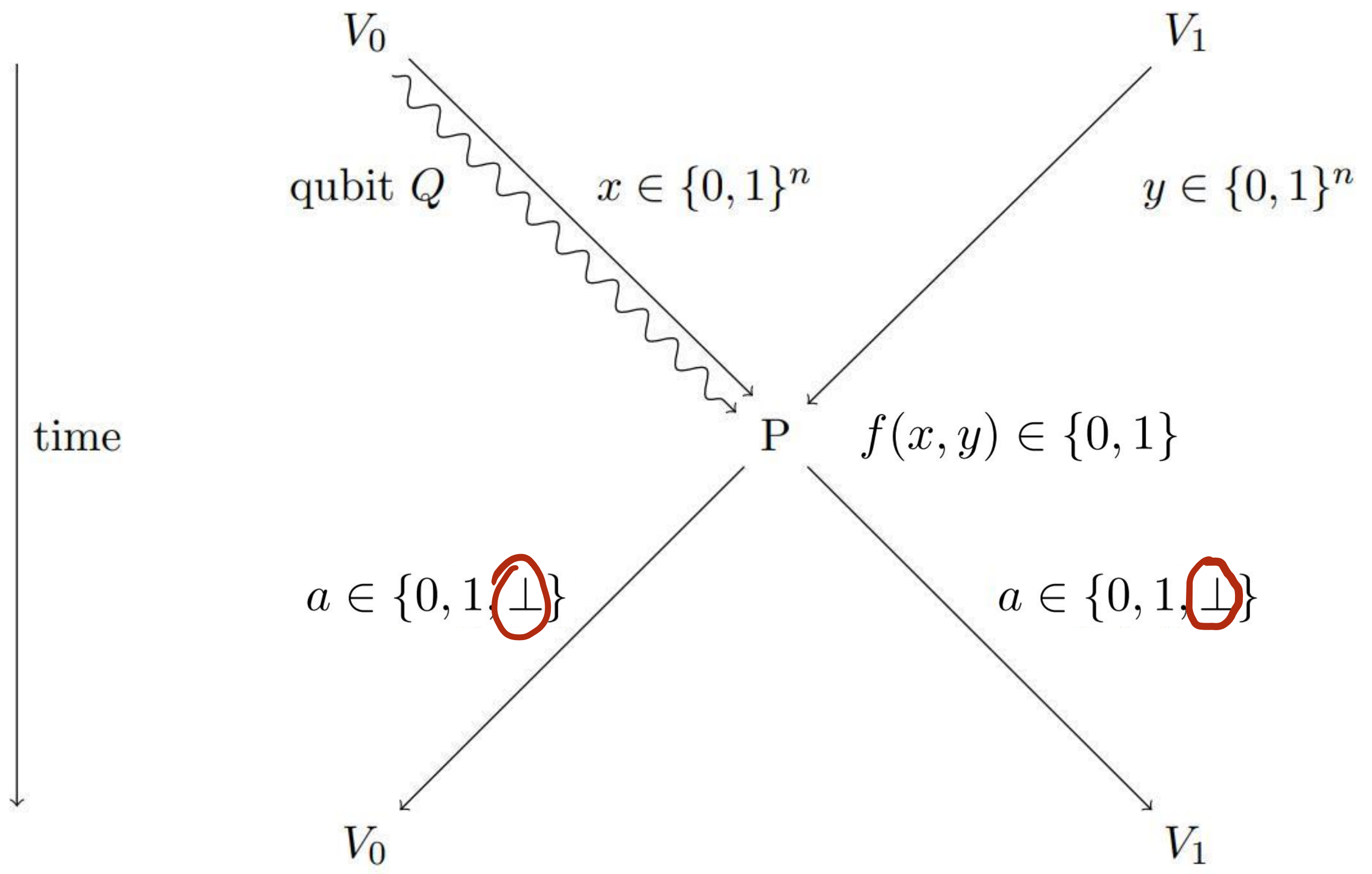
$\mathrm{QPV}_{\mathrm{BB84}}^{\eta, f}$



Previous result with loss

Technical lemma

$$\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$$



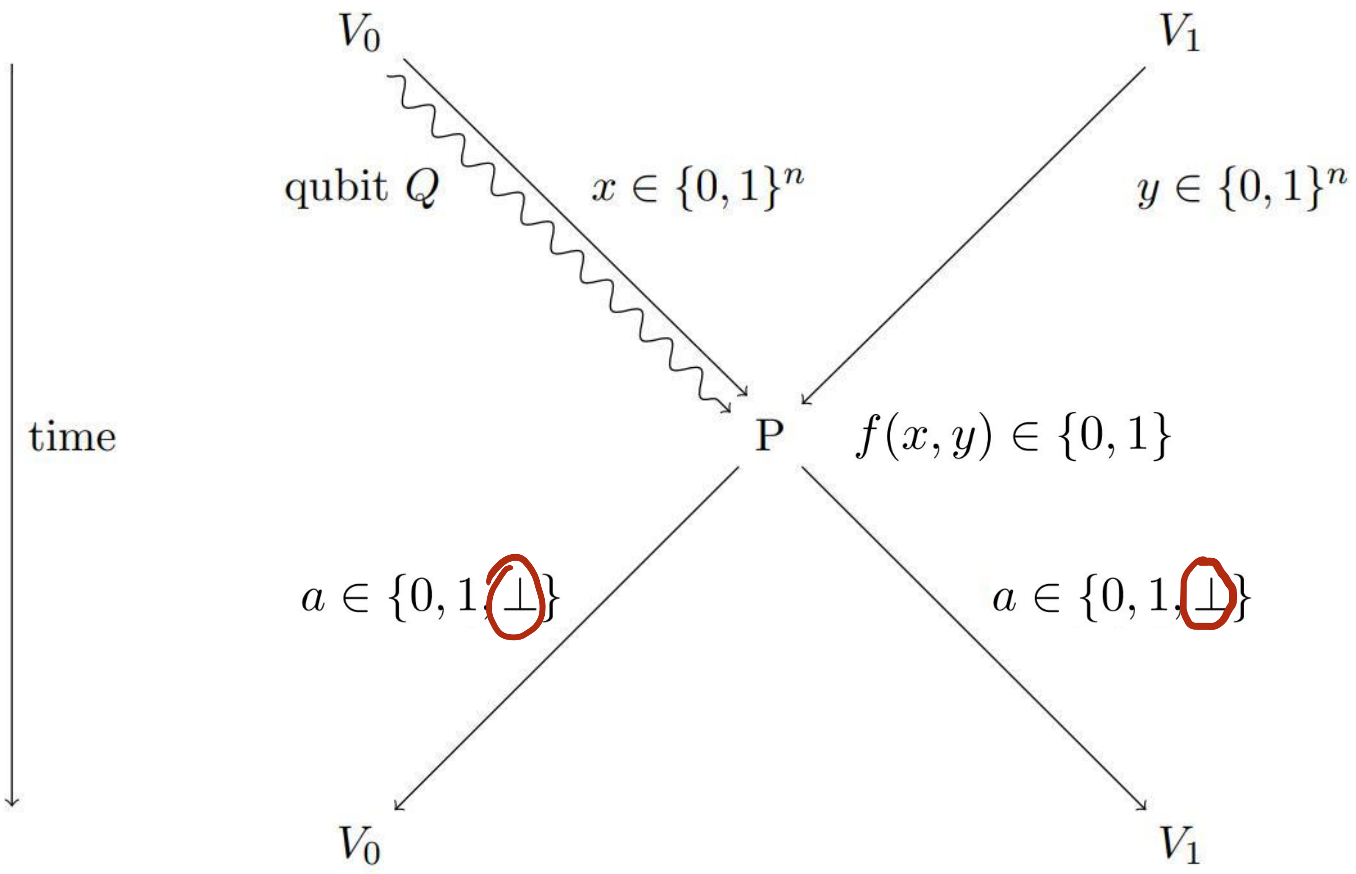
Previous result with loss

↓

Technical lemma

+

$\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$



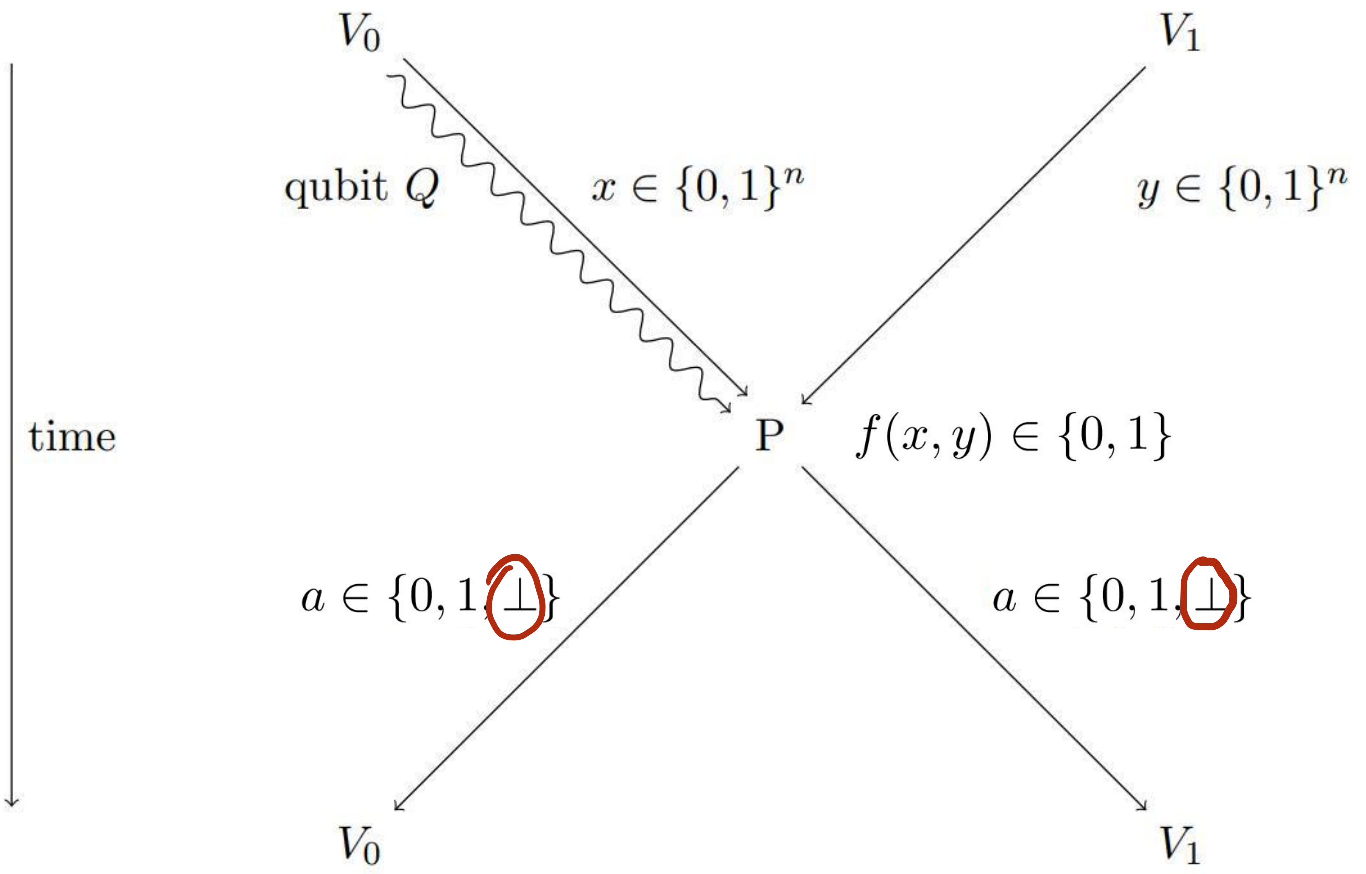
Previous result with loss

Technical lemma

+

Techniques: security without loss [BCS22]

$\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$



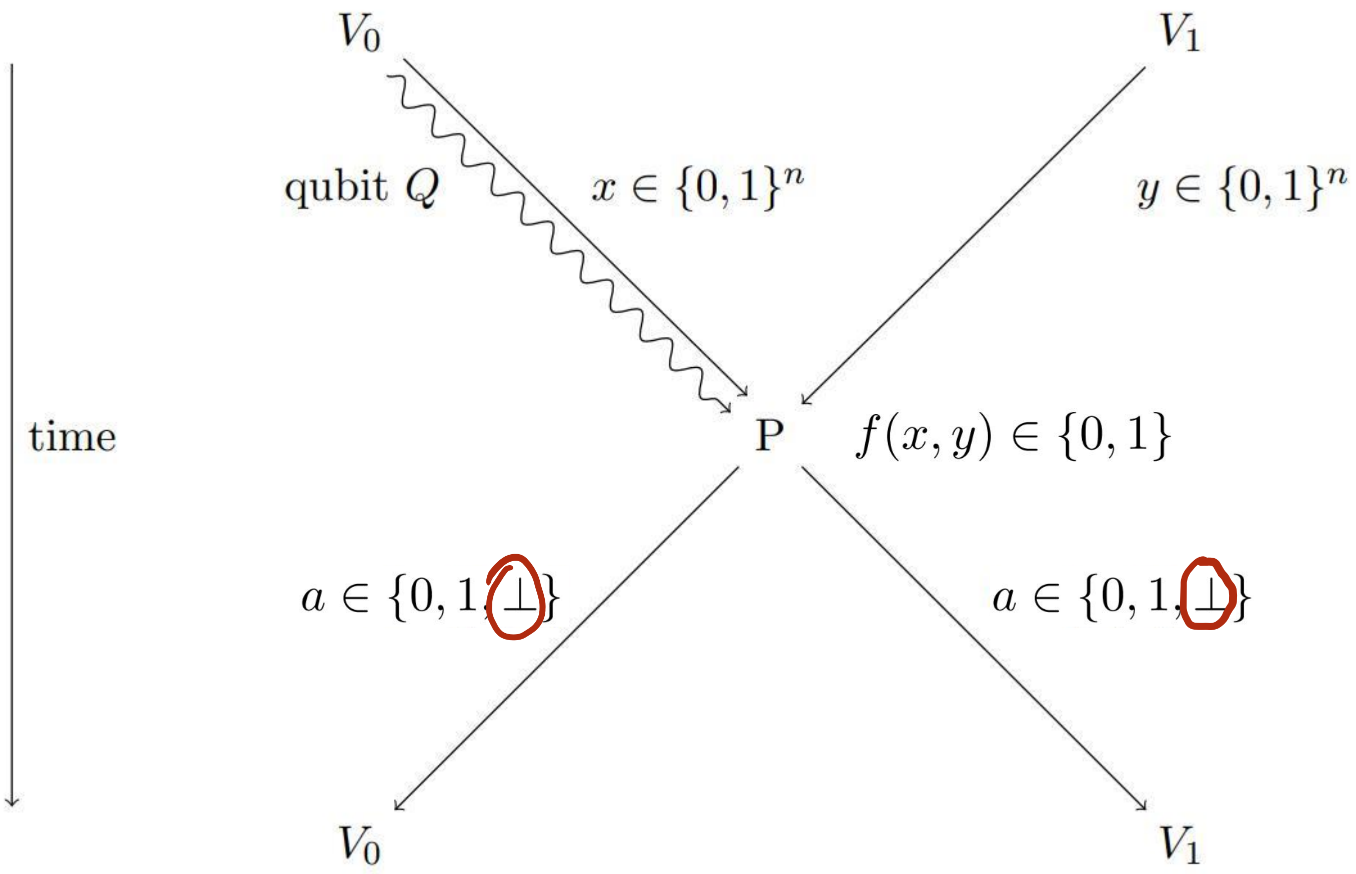
Previous result with loss

Technical lemma

+

Techniques: security without loss [BCS22]

$$\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$$



Previous result with loss

Technical lemma

+

Techniques: security without loss [BCS22]

Main result

Main result

Main result

If

Main result

If

- number of pre-shared qubits $\leq n/2-5$ (ENTANGLED attackers),
- quantum info arbitrarily slow
- photon loss

⟹ the protocol is still SECURE

Main result

If

- number of pre-shared qubits $\leq$ n/2-5 (ENTANGLED attackers),
- quantum info arbitrarily slow,
- photon loss

the protocol is still SECURE

Main result

If

- number of pre-shared qubits $\leq n/2-5$ (ENTANGLED attackers),
- quantum info arbitrarily slow,
- photon loss

the protocol is still SECURE

Main result

If

- number of pre-shared qubits $\leq n/2-5$ (ENTANGLED attackers),
- quantum info arbitrarily slow,
- photon loss

→ the protocol is still SECURE

Main result

If

- number of pre-shared qubits $\leq n/2-5$ (ENTANGLED attackers),
- quantum info arbitrarily slow,
- photon loss

➡ the protocol is still SECURE

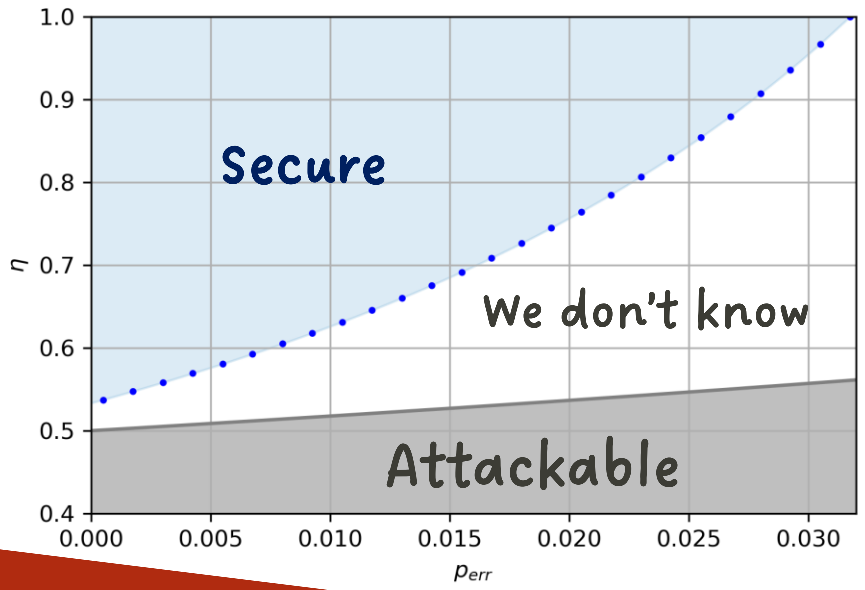
Main result

If

- number of pre-shared qubits ≤ n/2-5 (ENTANGLED attackers),
- quantum info arbitrarily slow,
- photon loss

⇒ the protocol is still SECURE

In experimental parameters



This means

This means

👩 🙋 👦

Protocol

This means

Protocol

Attack

This means

Protocol
(With loss)

Attack

This means

Protocol
(With loss)

Attack

Classical info

This means

	 Protocol (With loss)	 Attack
Classical info	2n	2n

This means

	Protocol (With loss)	Attack
Classical info	2n	2n
Qubits		

This means

	Protocol (With loss)	Attack
Classical info	2n	2n
Qubits	1 qubit	

This means

	Protocol (With loss)	Attack
Classical info	2n	2n
Qubits	1 qubit	n/2-5 entangled qubits (at least)

This means

	Protocol (With loss)	Attack
Classical info	2n	2n
Qubits	1 qubit	n/2-5 entangled qubits (at least)
e.g. n=1kB		

This means

	Protocol (With loss)	Attack
Classical info	2n	2n
Qubits	1 qubit	n/2-5 entangled qubits (at least)
e.g. n=1kB		
Qubits		

This means

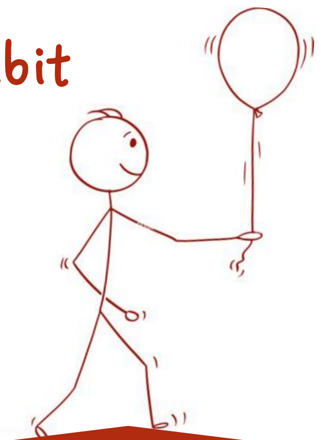
	👩 🙋 👦 Protocol (With loss)	👧 👨 Attack
Classical info	2n	2n
Qubits	1 qubit	n/2-5 entangled qubits (at least)
e.g. n=1kB		
Qubits	1 qubit	

This means

	Protocol (With loss)	Attack
Classical info	2n	2n
Qubits	1 qubit	n/2-5 entangled qubits (at least)
e.g. n=1kB		
Qubits	1 qubit	4.000 entangled qubits

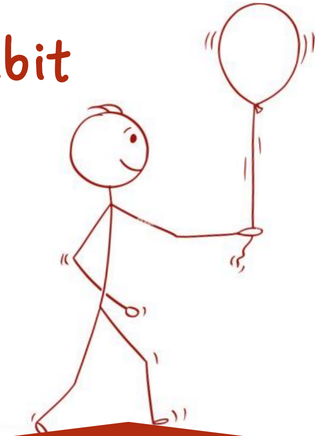
This means

	 Protocol (With loss)	 Attack
Classical info	2n	2n
Qubits	1 qubit	n/2-5 entangled qubits (at least)
e.g. n=1kB		
Qubits	1 qubit	4.000 entangled qubits



This means

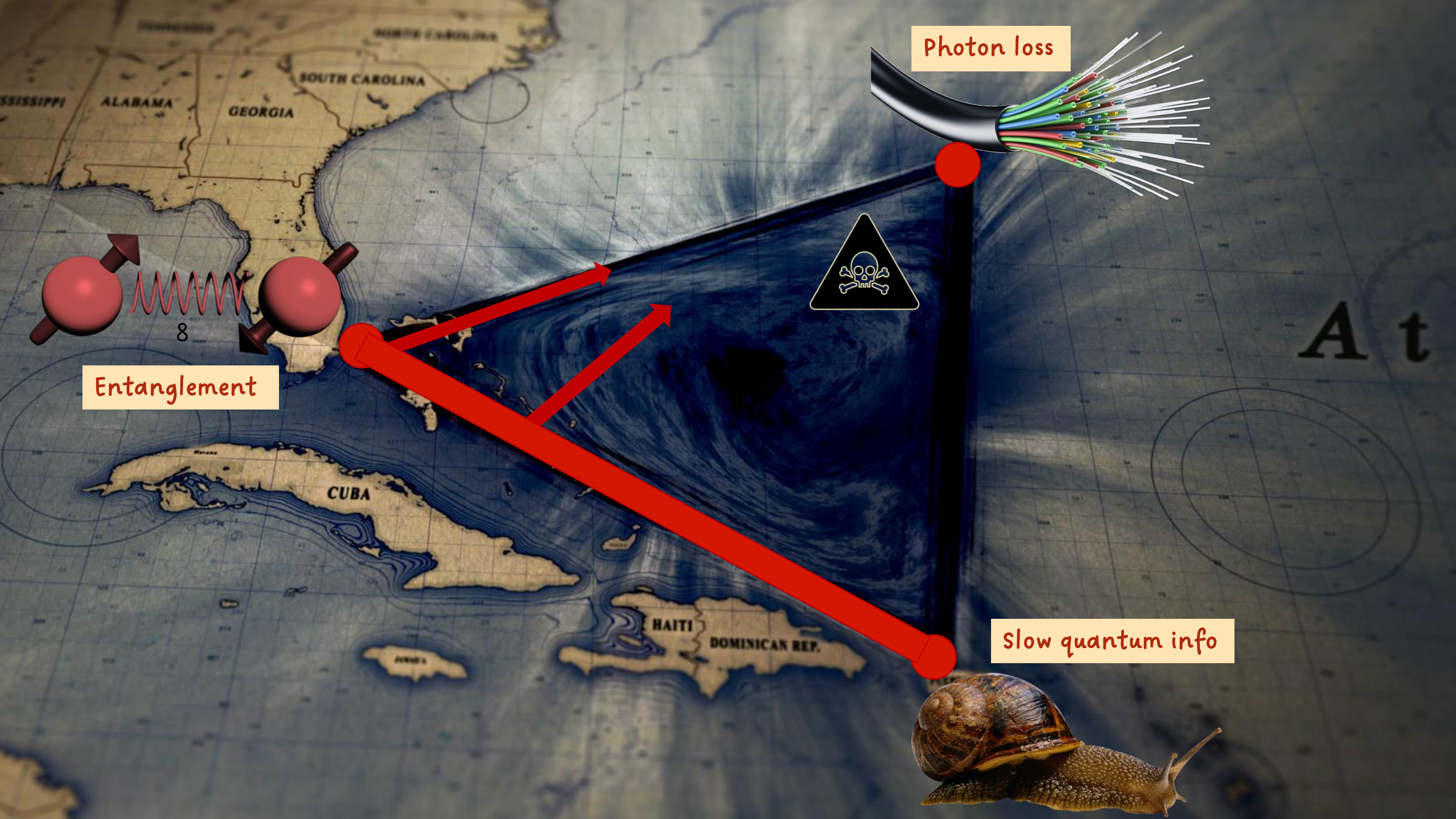
	👩 🙋 👦 Protocol (With loss)	👧 👨 Attack
Classical info	2n	2n
Qubits	1 qubit	n/2-5 entangled qubits (at least)
e.g. n=1kB		
Qubits	1 qubit	4.000 entangled qubits

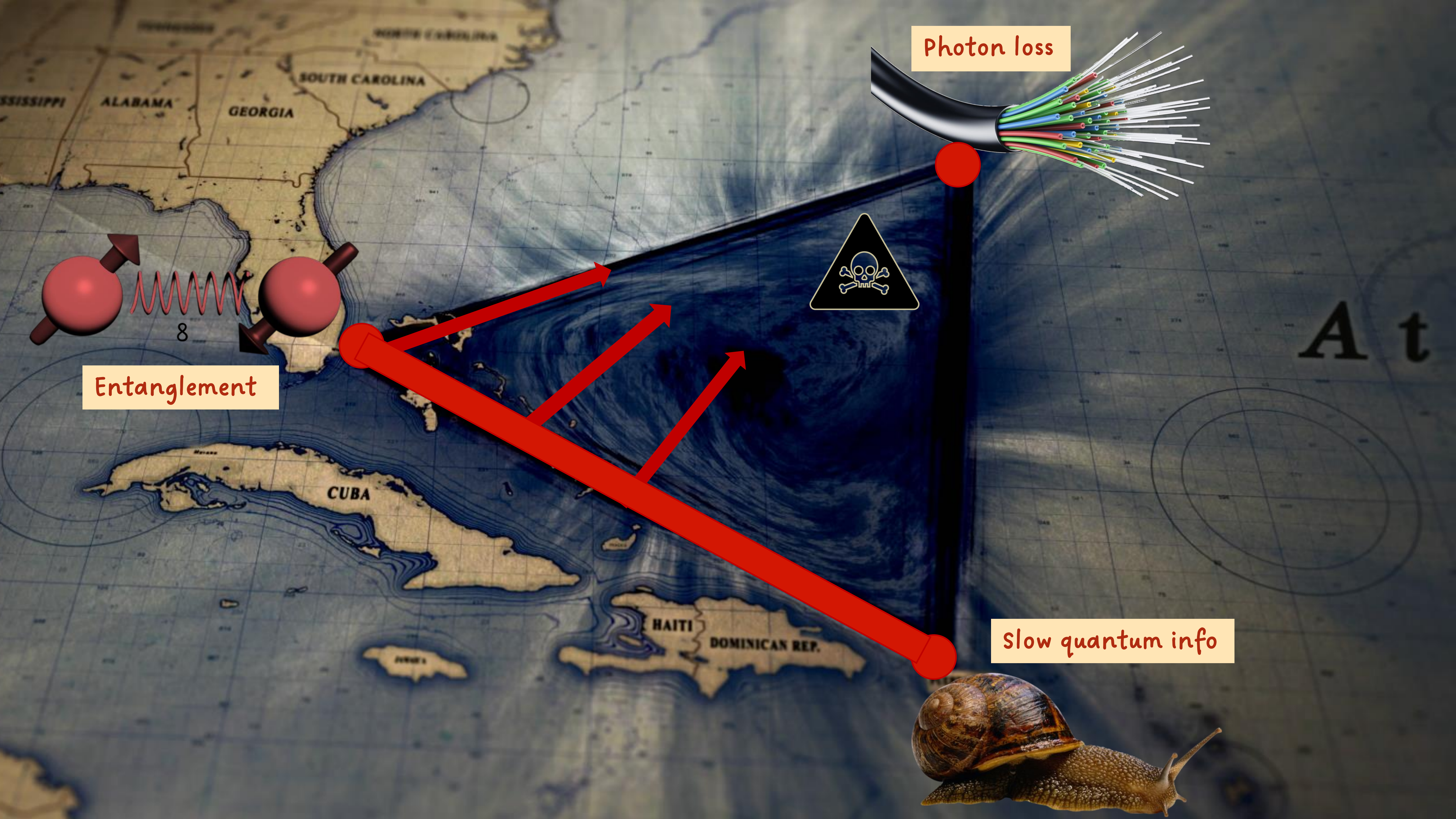


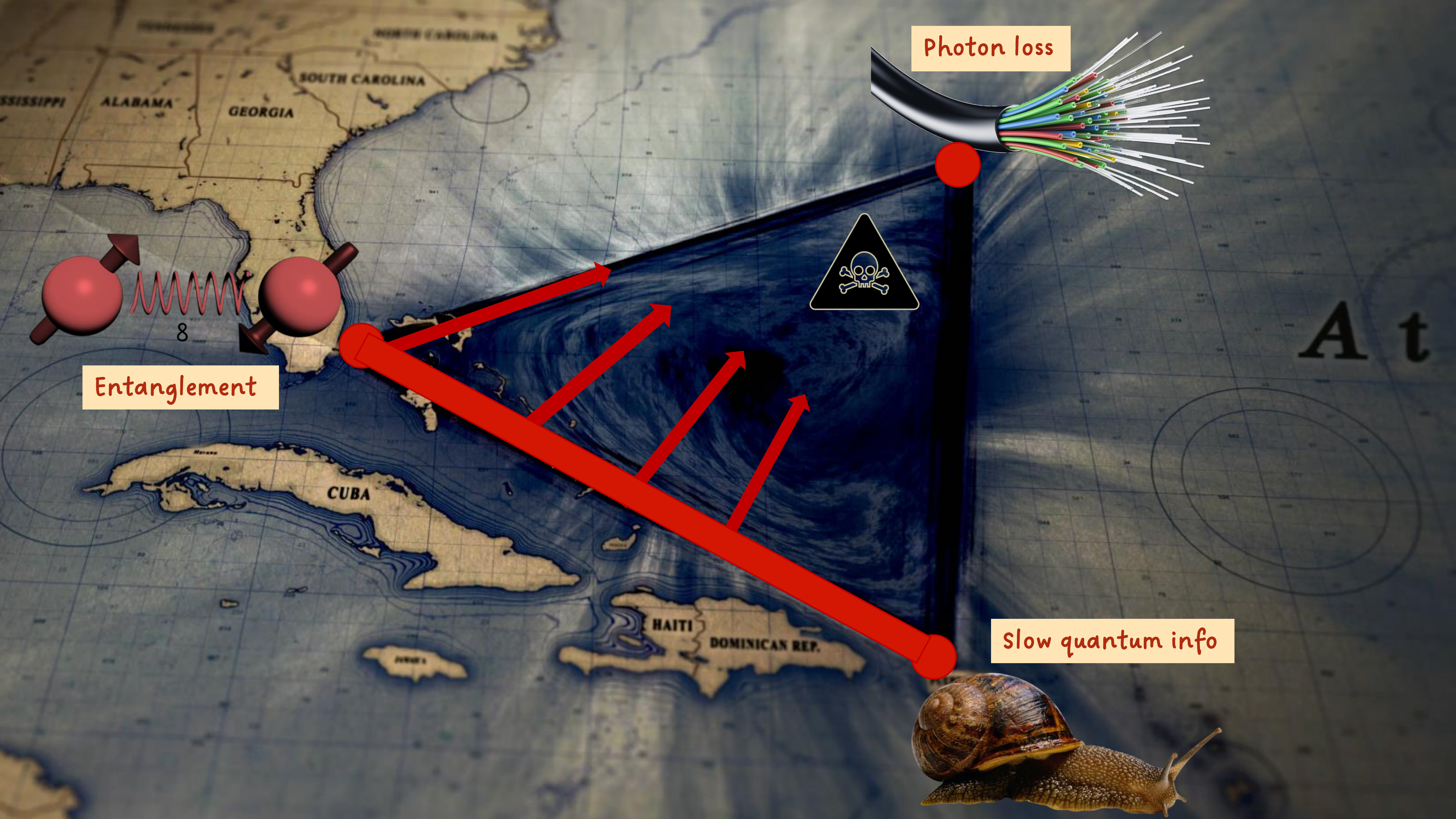

Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.

Photon loss
Entanglement
Slow quantum info
ALABAMA
GEORGIA
SOUTH CAROLINA
CUBA
HAITI
DOMINICAN REP.

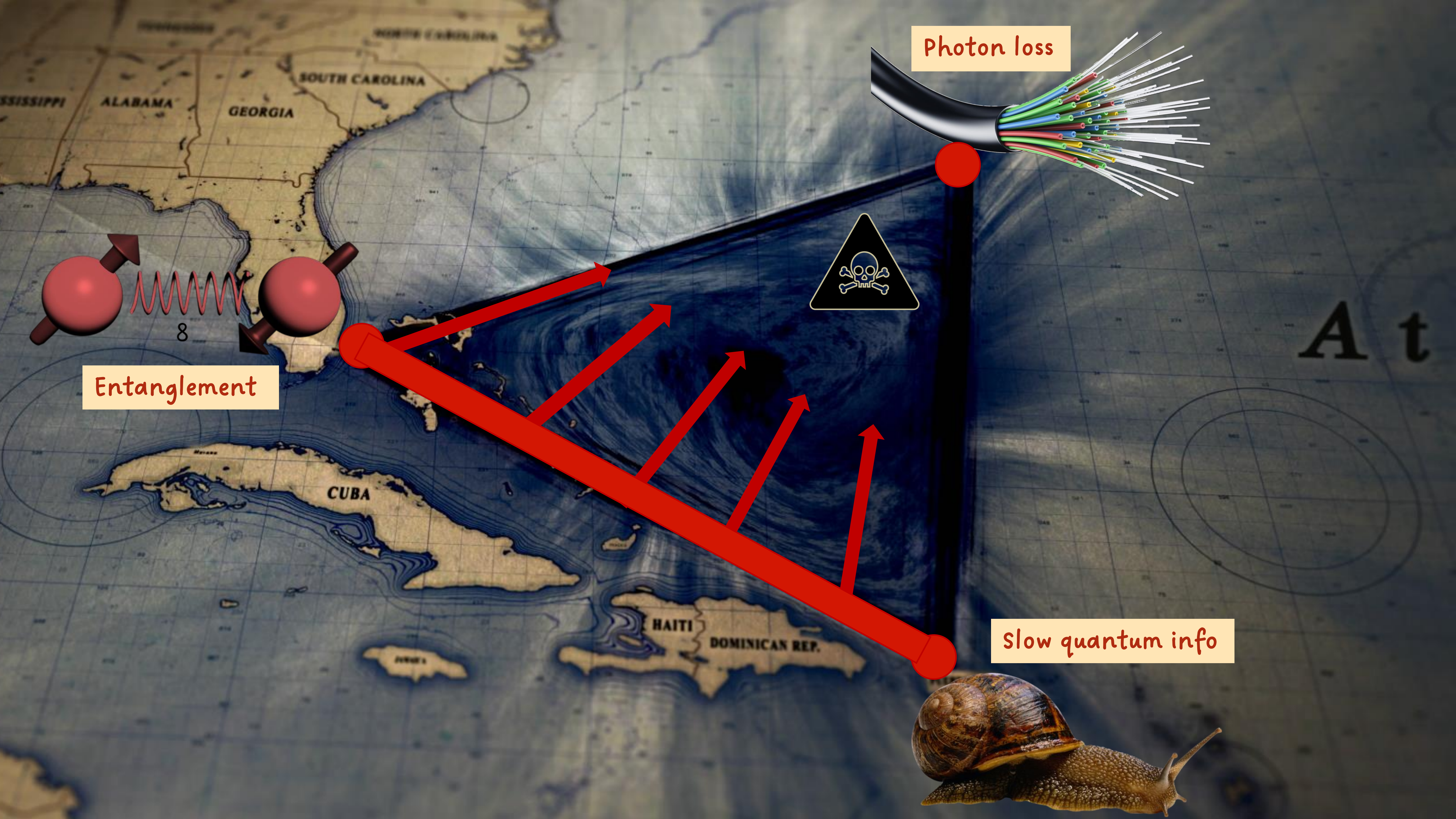

Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.


Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.

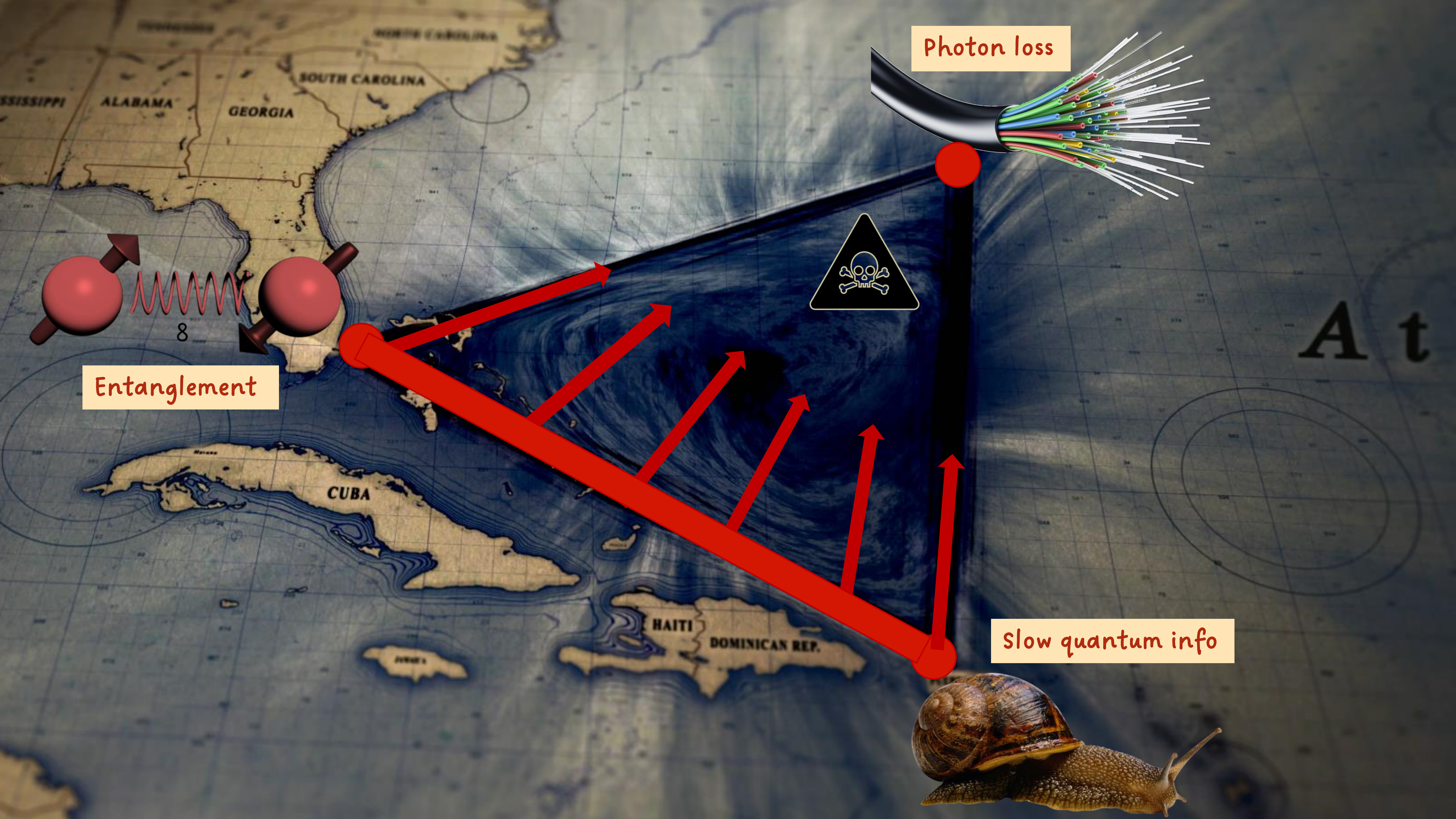

Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.

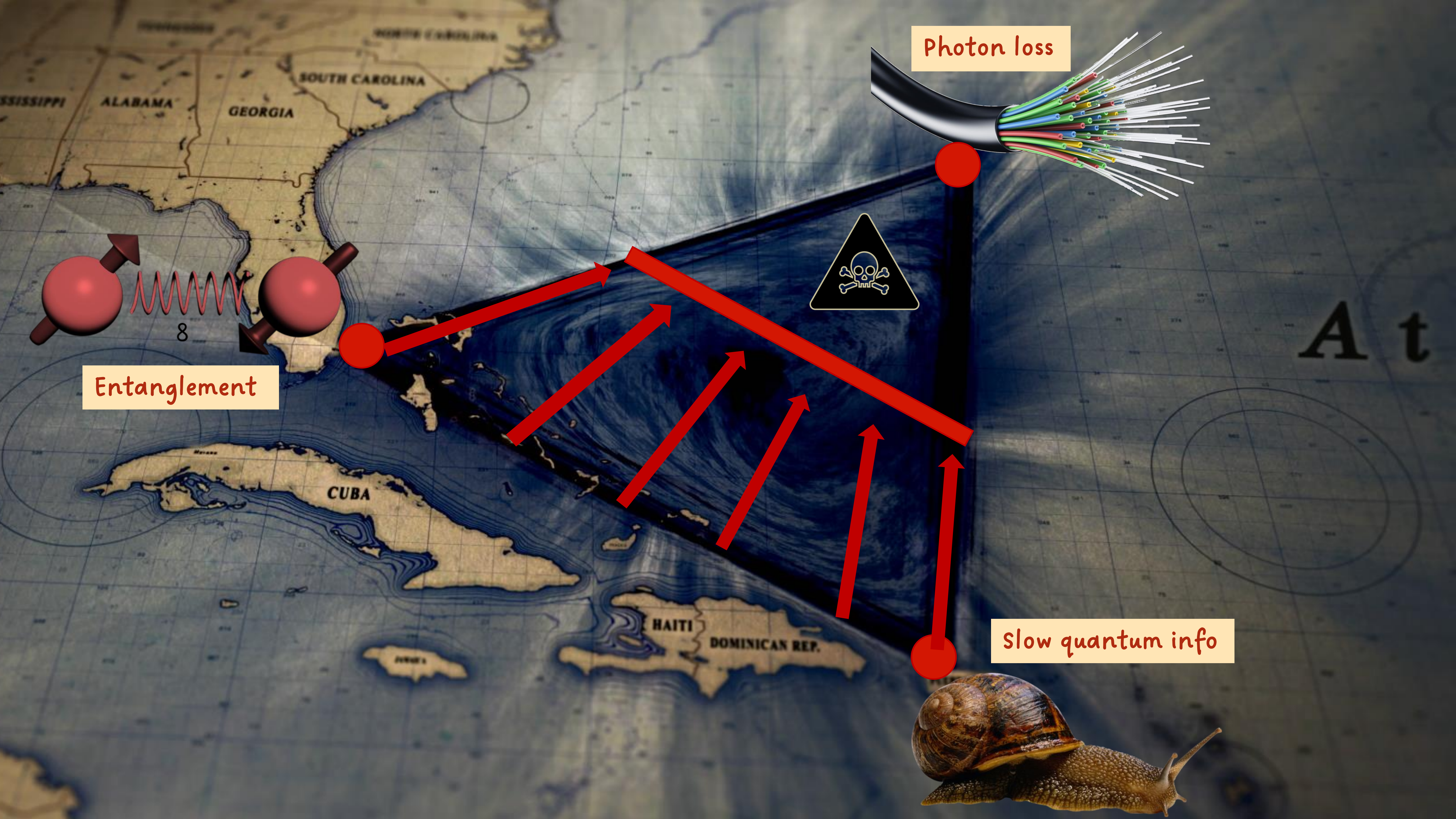


Photon loss
Entanglement
8
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.

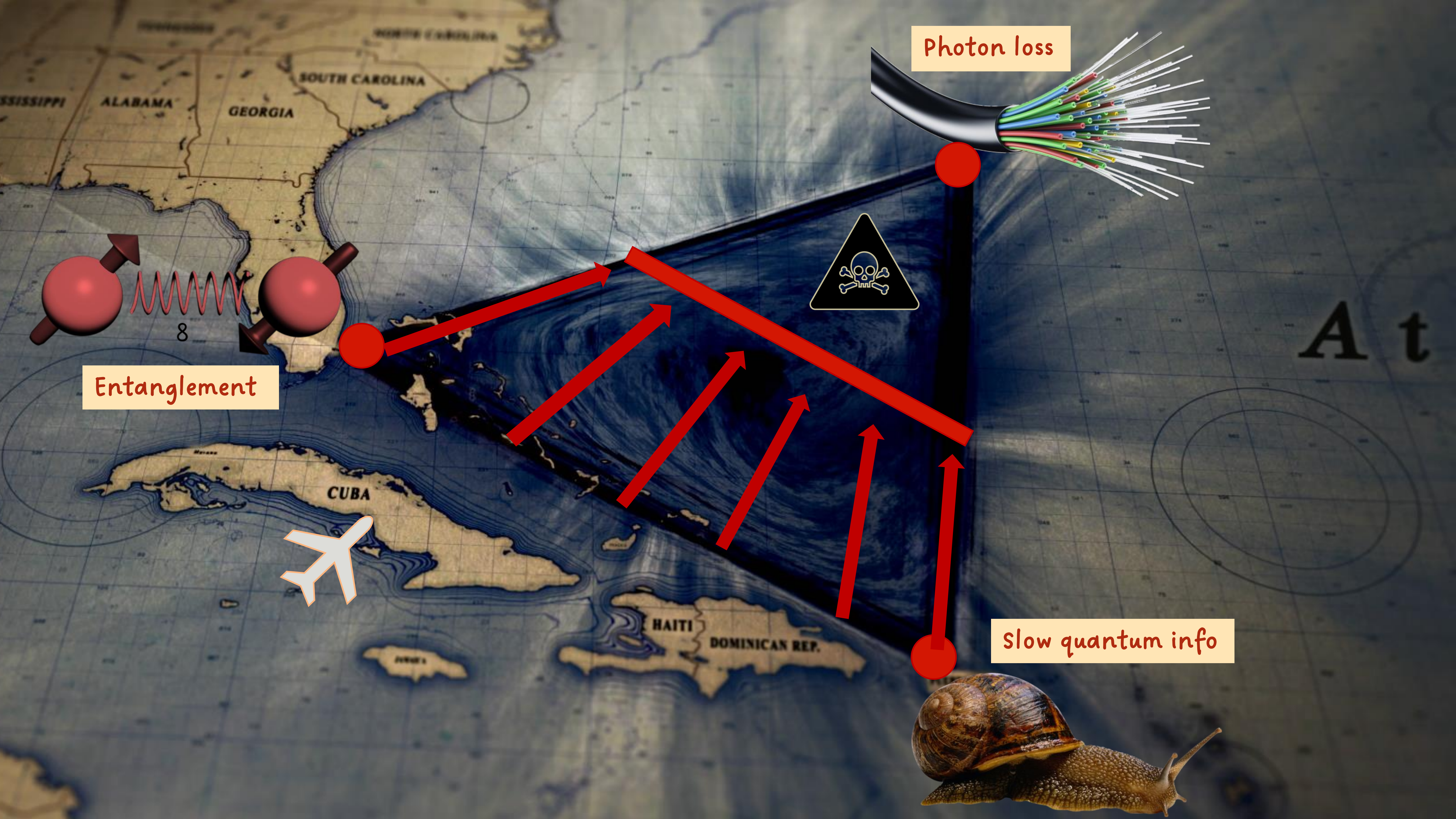


Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.

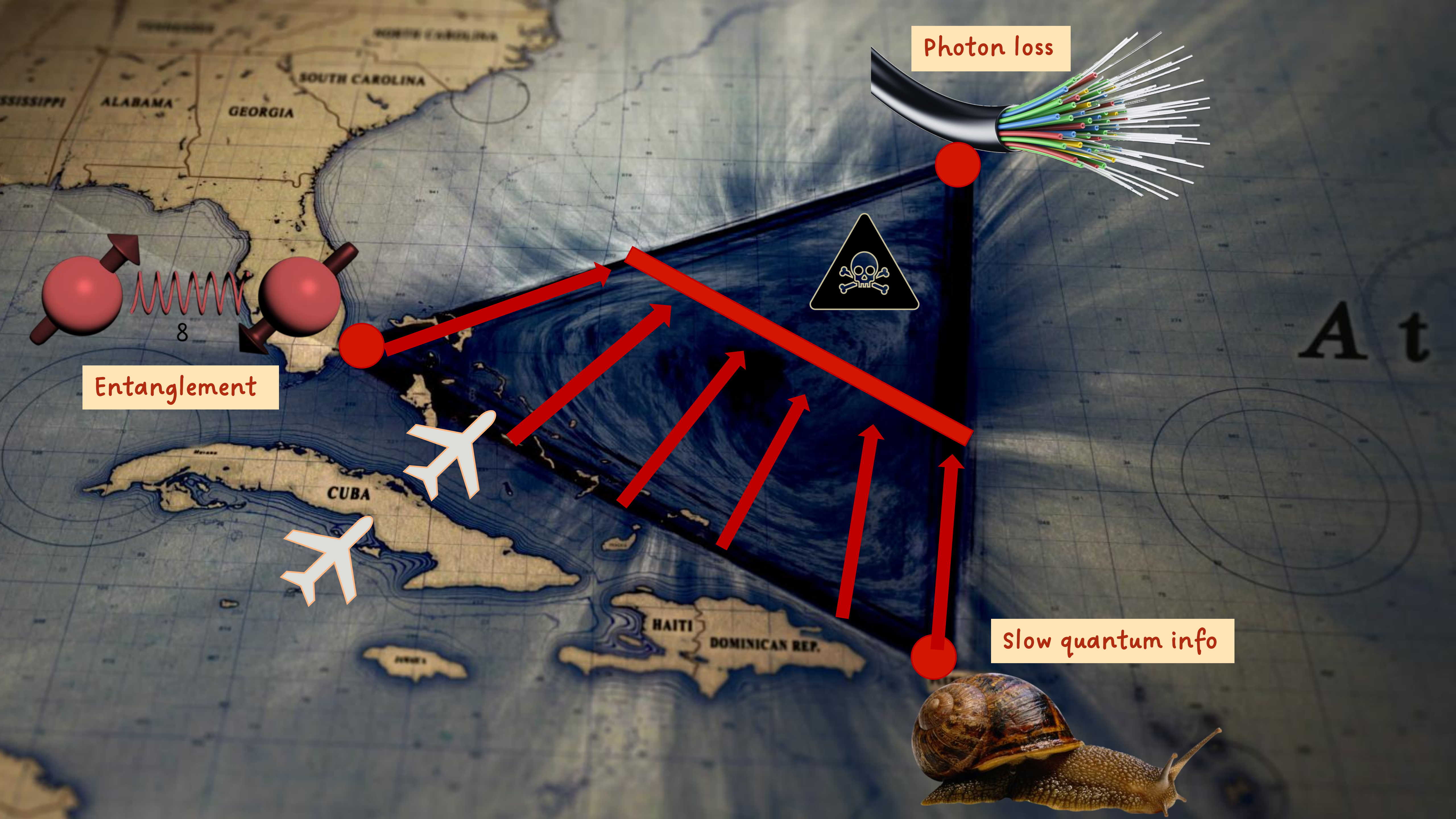

Photon loss
Entanglement
Slow quantum info
8
CUBA
HAITI
DOMINICAN REP.
GEORGIA
ALABAMA
SOUTH CAROLINA
At



Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.



Photon loss
Entanglement
Slow quantum info
8
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.



Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.

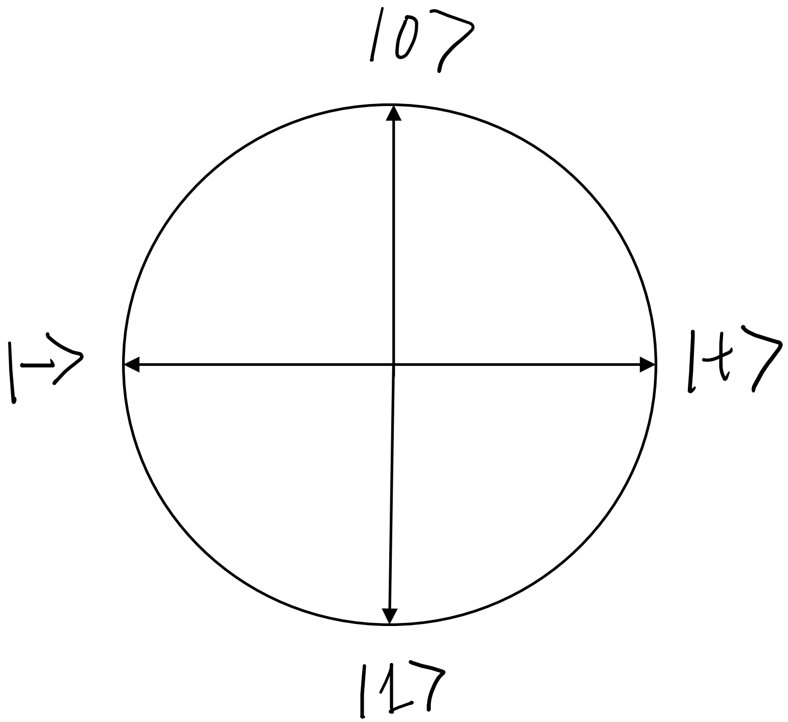
Photon loss
Entanglement
Slow quantum info
CUBA
HAITI
DOMINICAN REP.
SOUTH CAROLINA
GEORGIA
ALABAMA

Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.

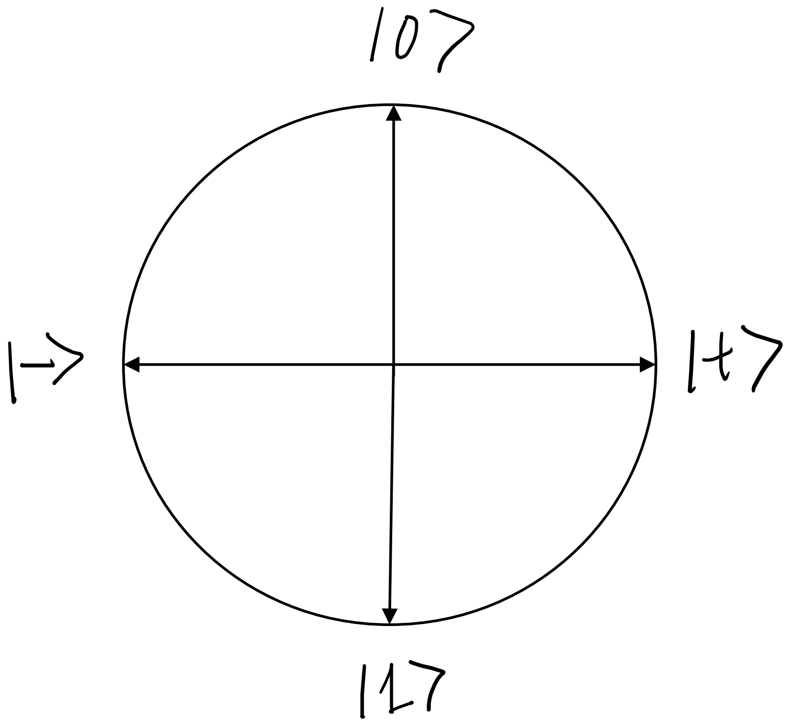
Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

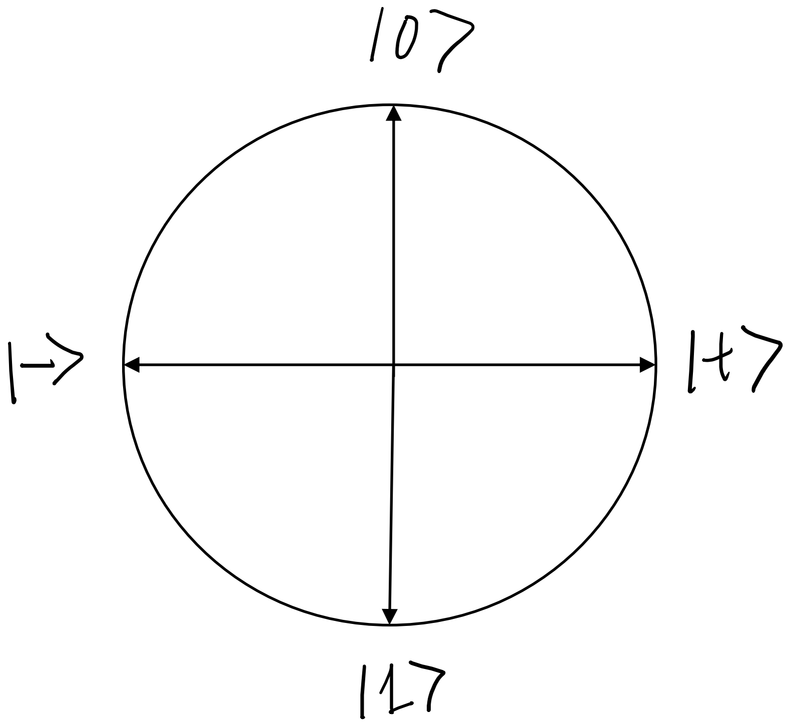


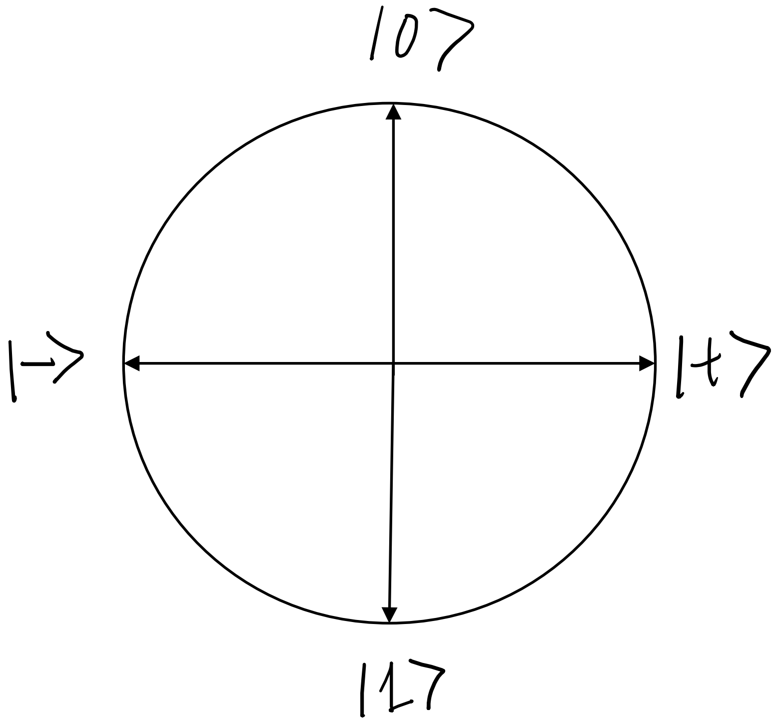
The results can be extended to **multiple bases** and we show that is **more loss-tolerant**



$\eta \geq \frac{1}{2}$

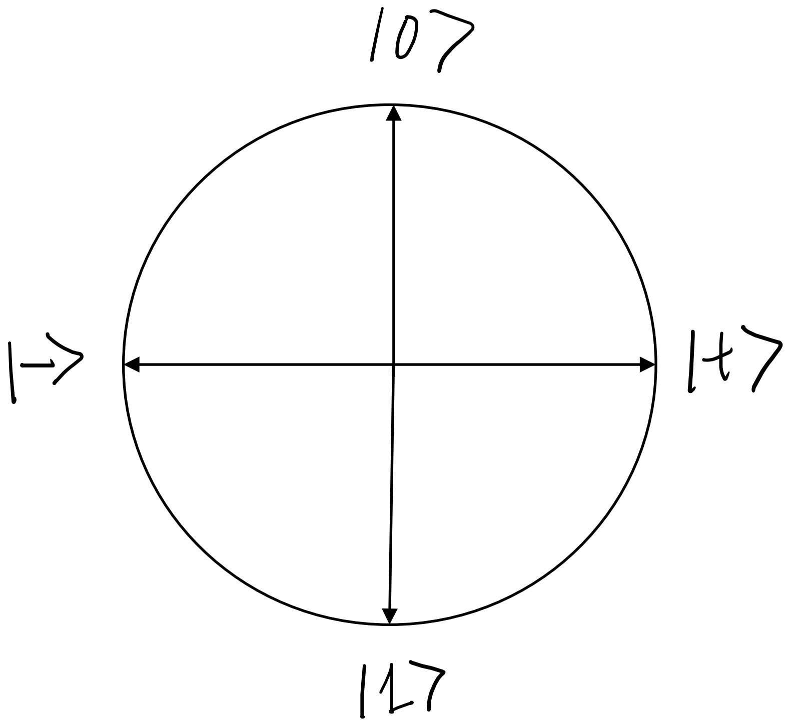
The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

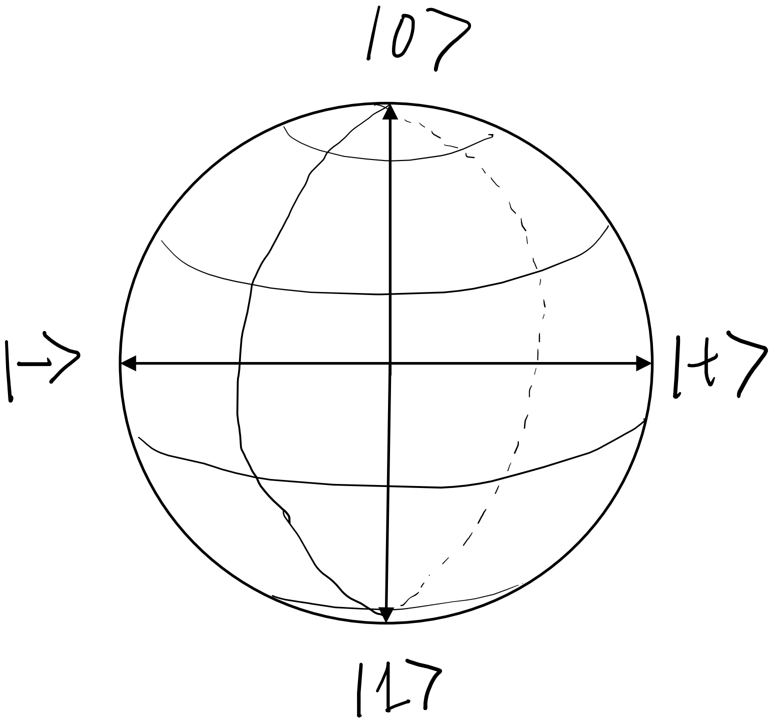




$\eta \geq \frac{1}{2}$

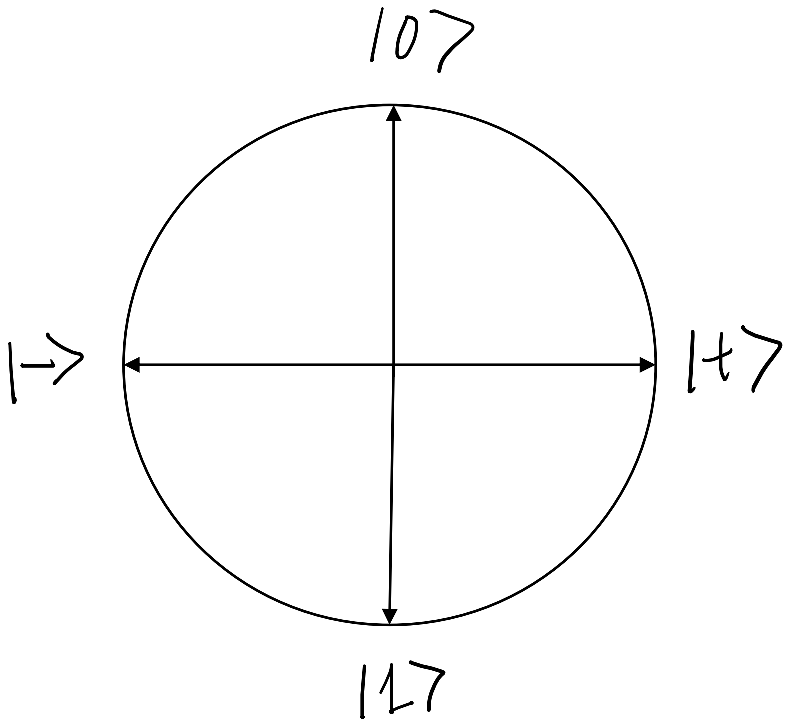
The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

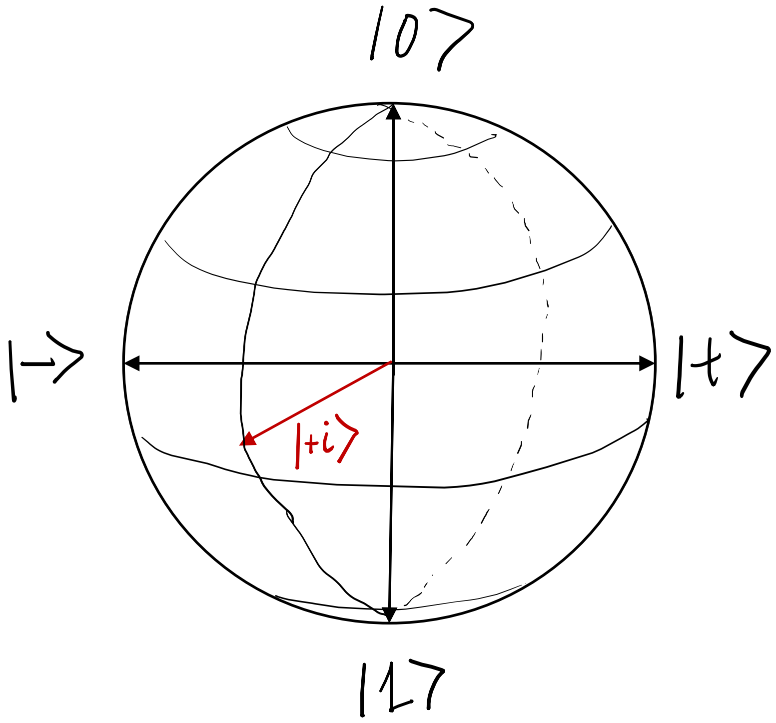




$\eta \geq \frac{1}{2}$

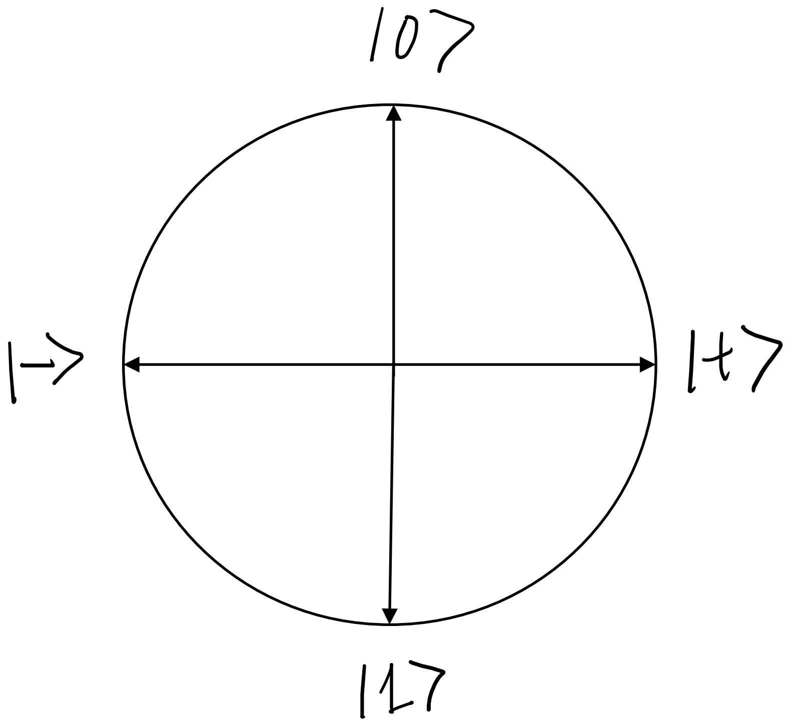
The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

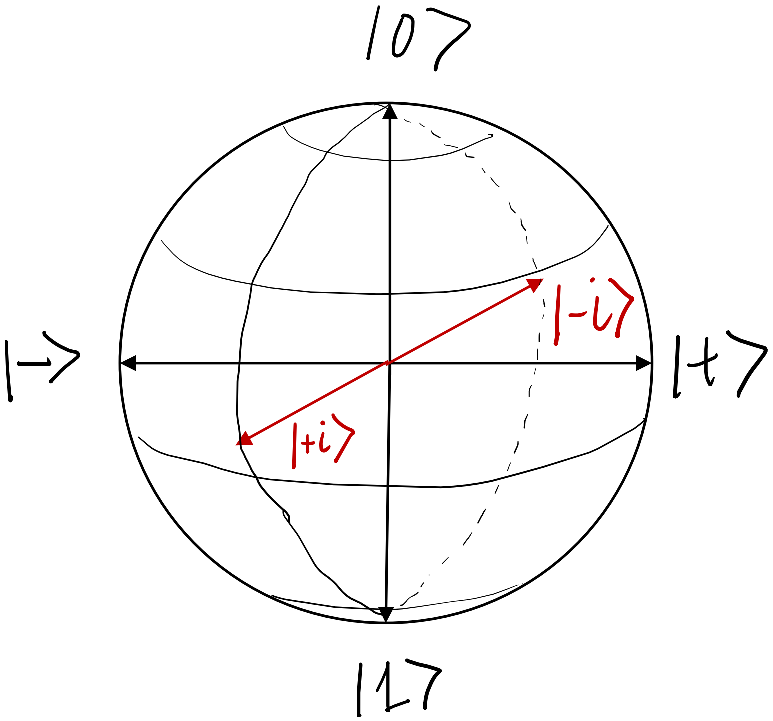




$\eta \geq \frac{1}{2}$

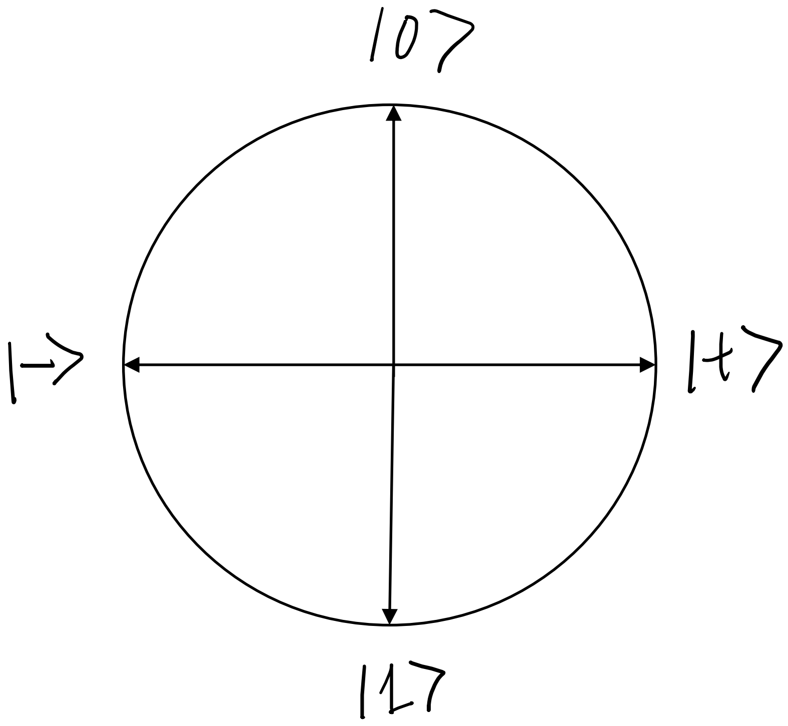
The results can be extended to **multiple bases** and we show that is **more loss-tolerant**



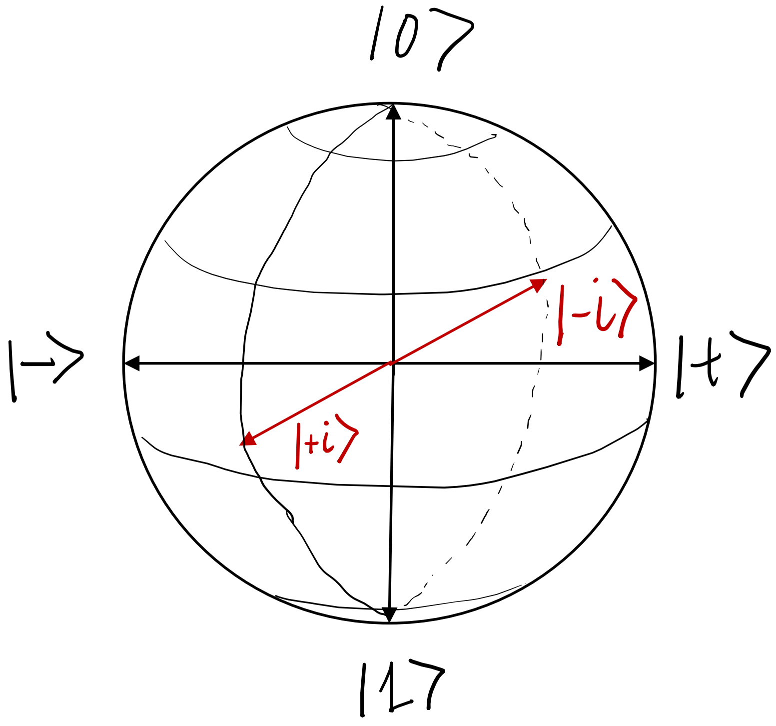


$\eta \geq \frac{1}{2}$

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

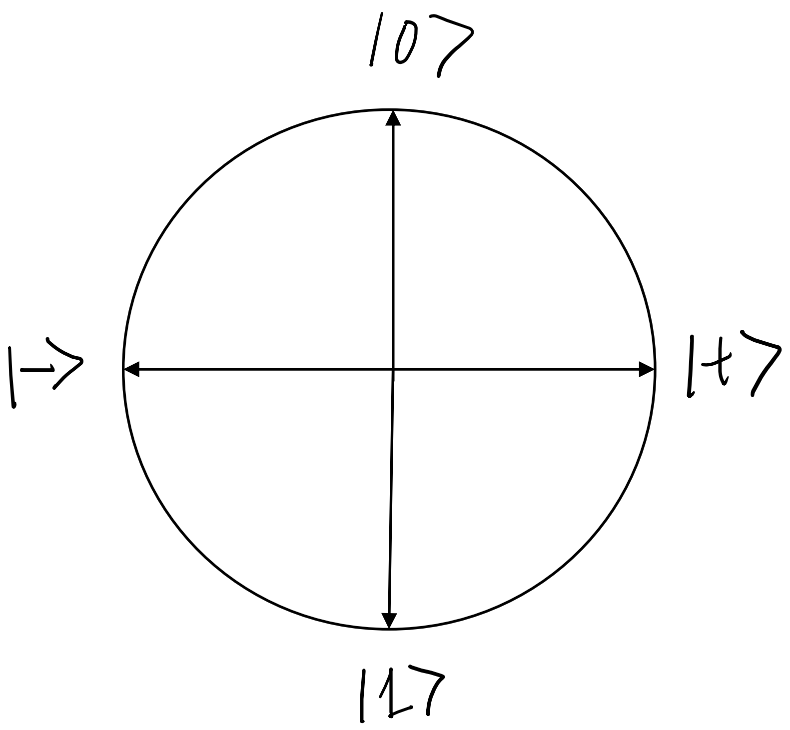


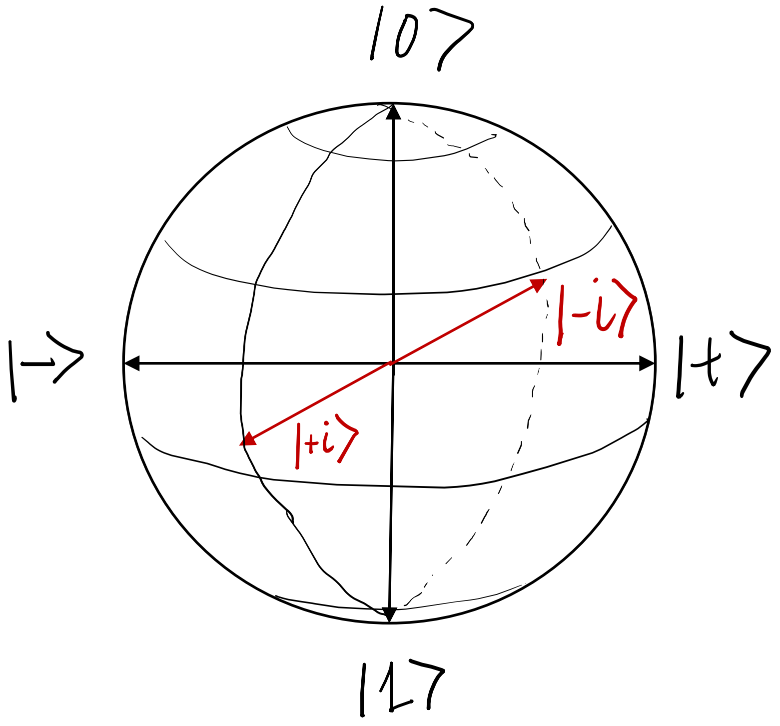
$\eta \geq \frac{1}{2}$



$\eta \geq \frac{1}{3}$

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**





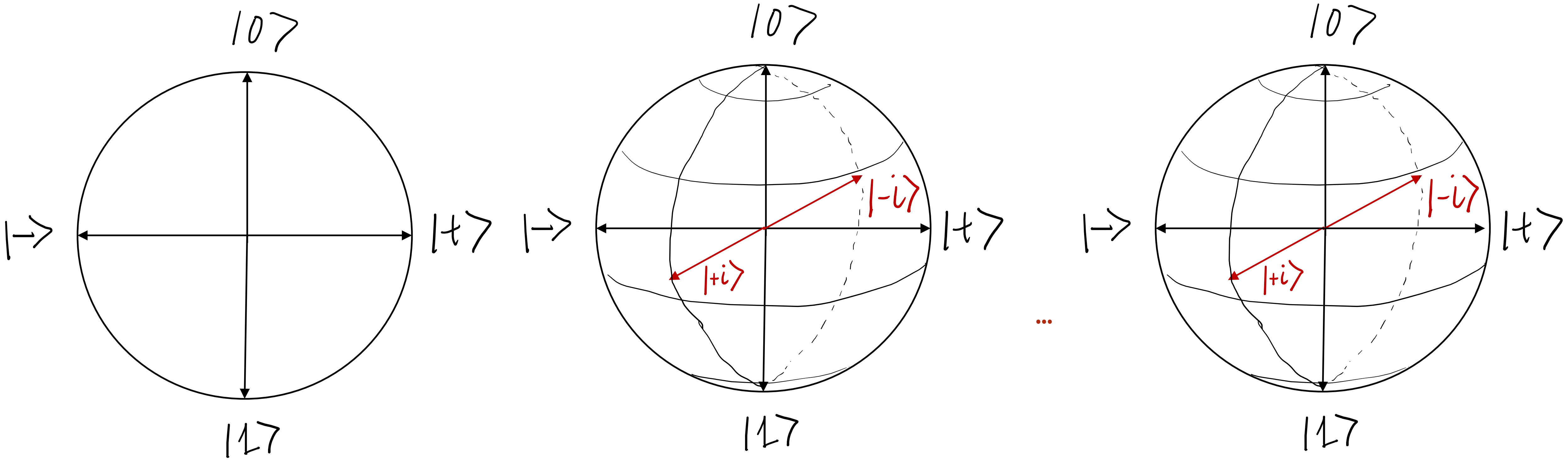
...

$\eta \geq \frac{1}{2}$

$\eta \geq \frac{1}{3}$

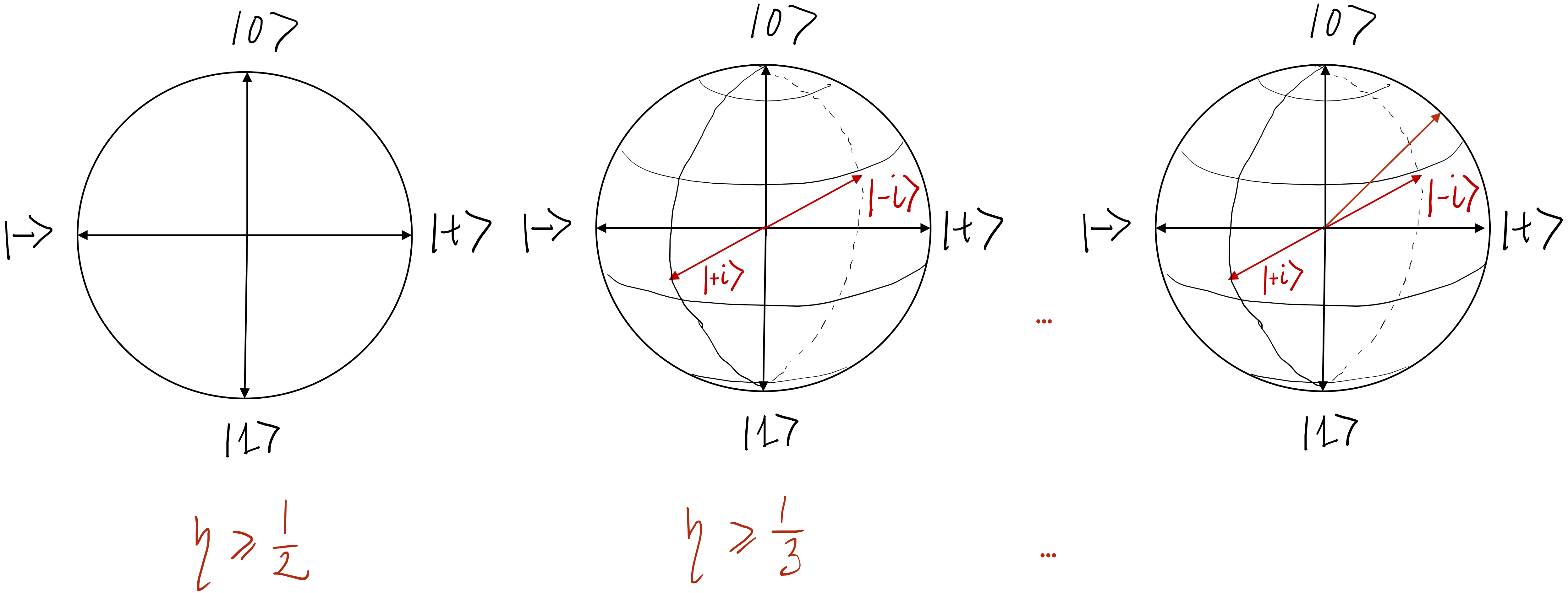
...

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

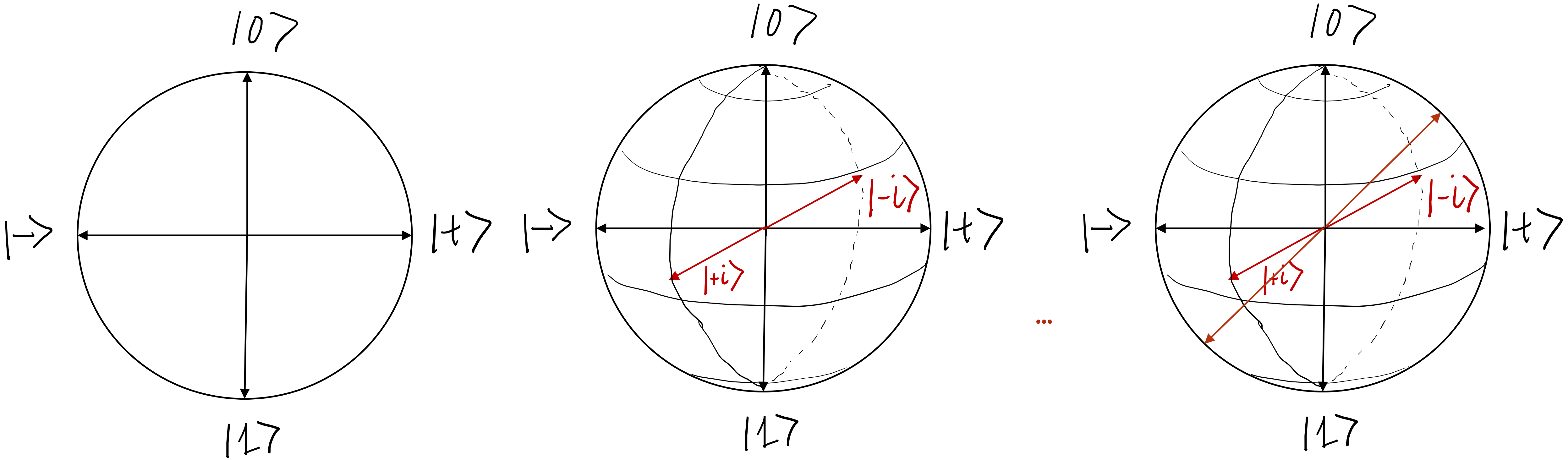


$\eta \geqslant \frac{1}{2}$ $\eta \geqslant \frac{1}{3}$ ...

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

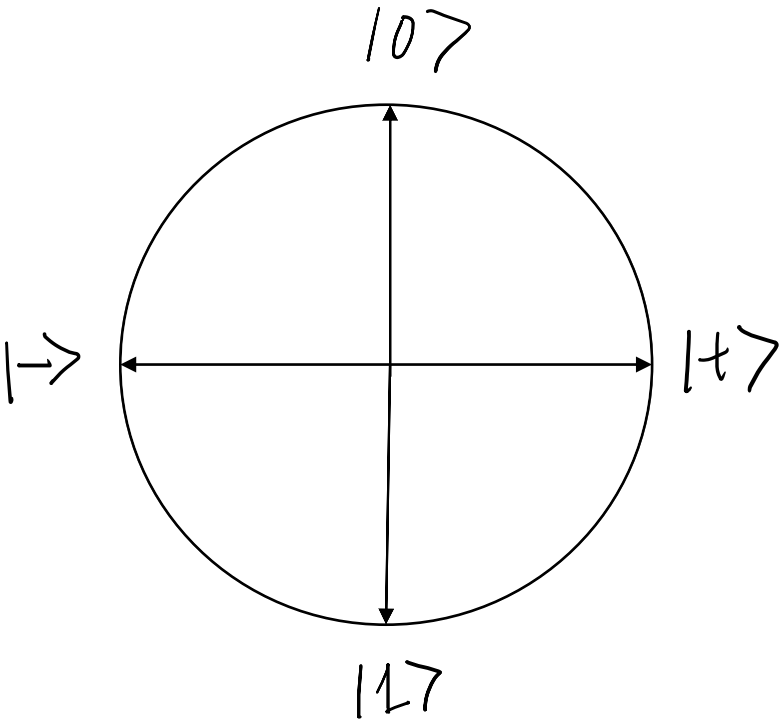


The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

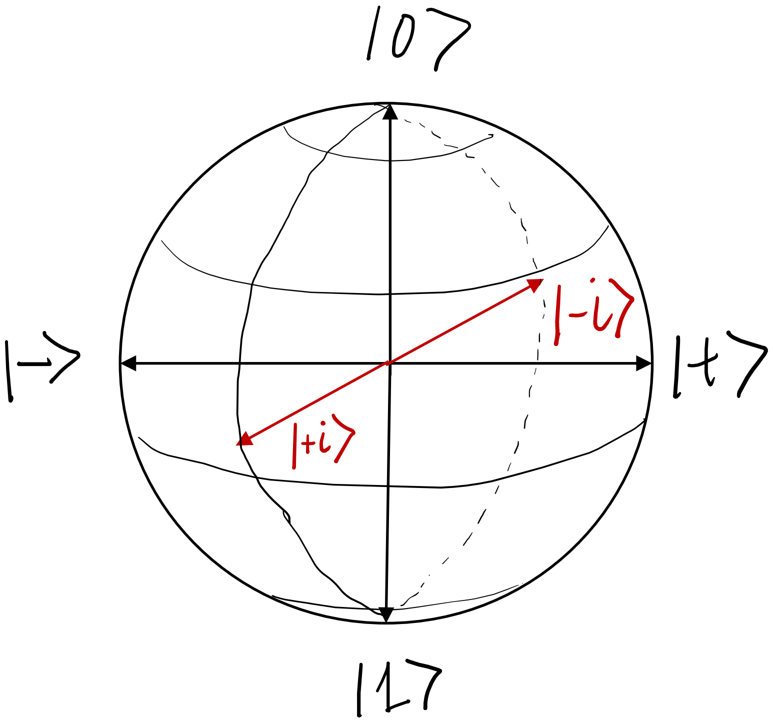


$\eta \geq \frac{1}{2}$ $\eta \geq \frac{1}{3}$ ...

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**

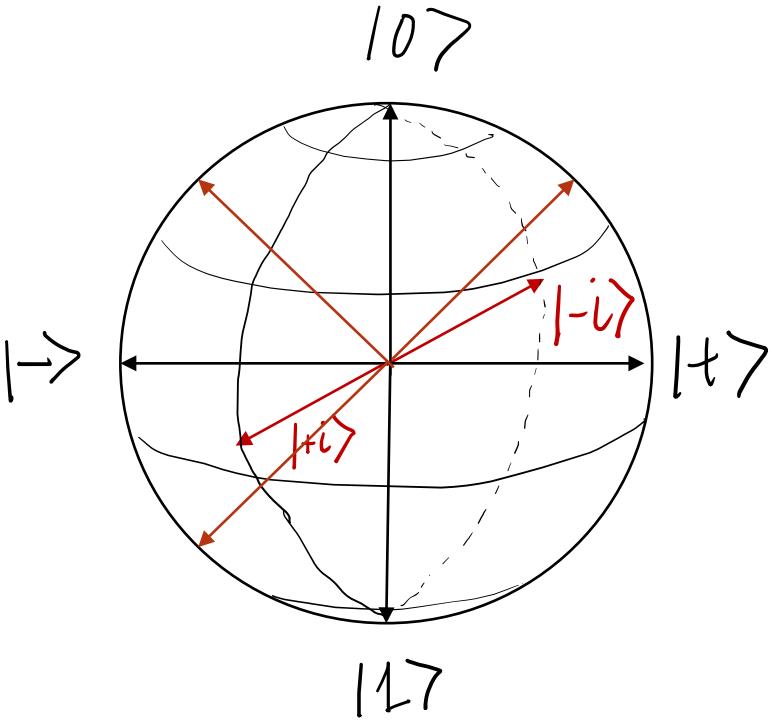


$\eta \geq \frac{1}{2}$



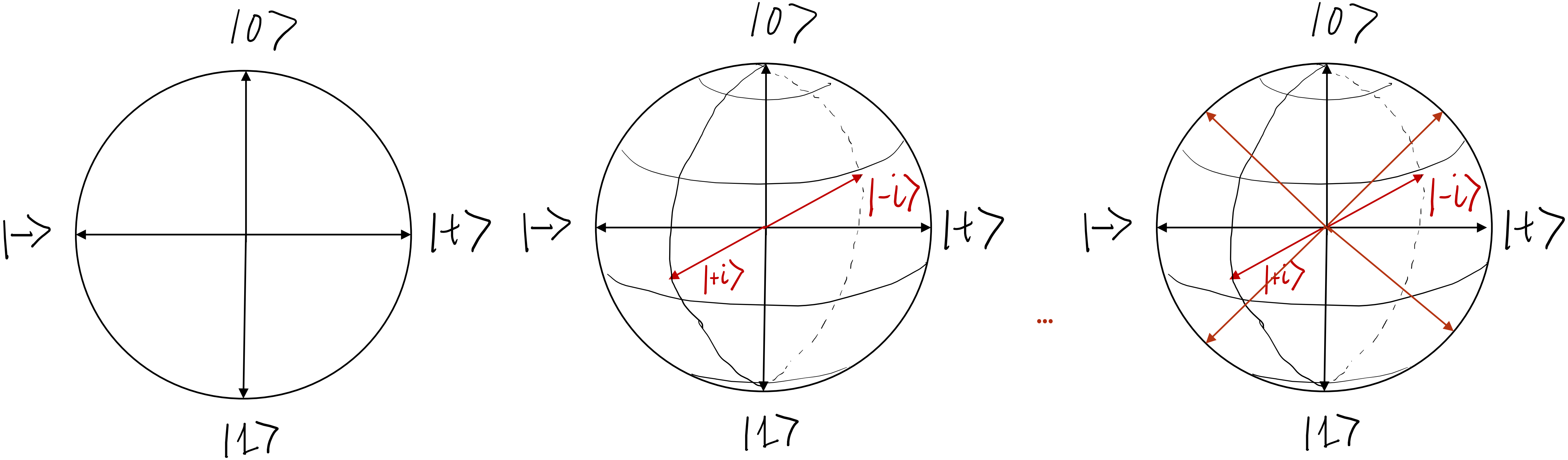
$\eta \geq \frac{1}{3}$

...



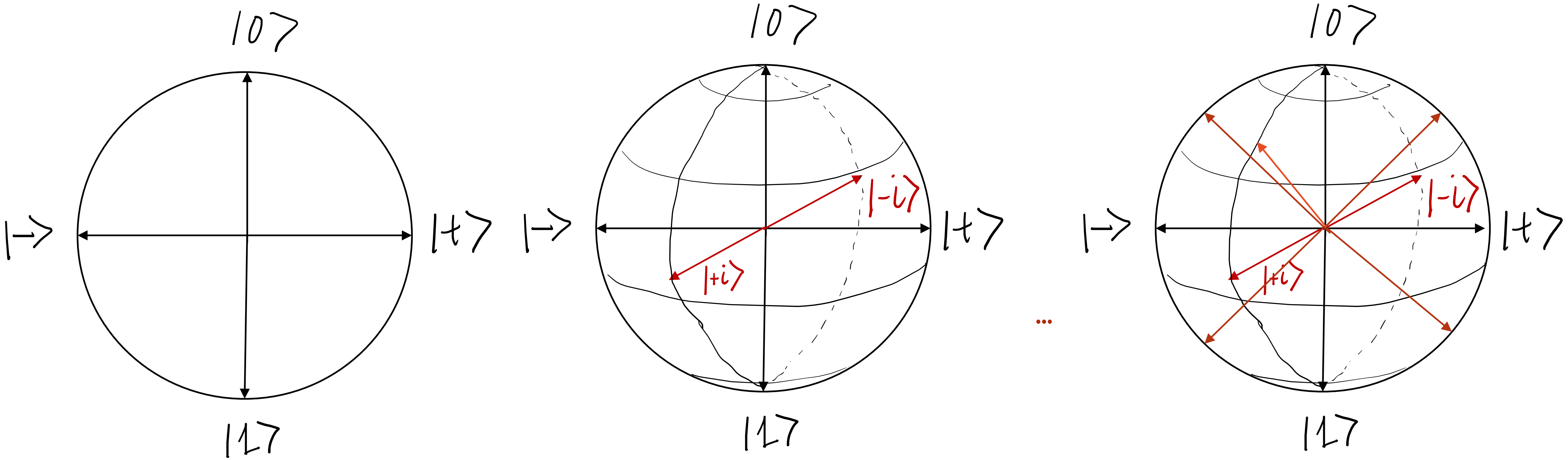
...

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**



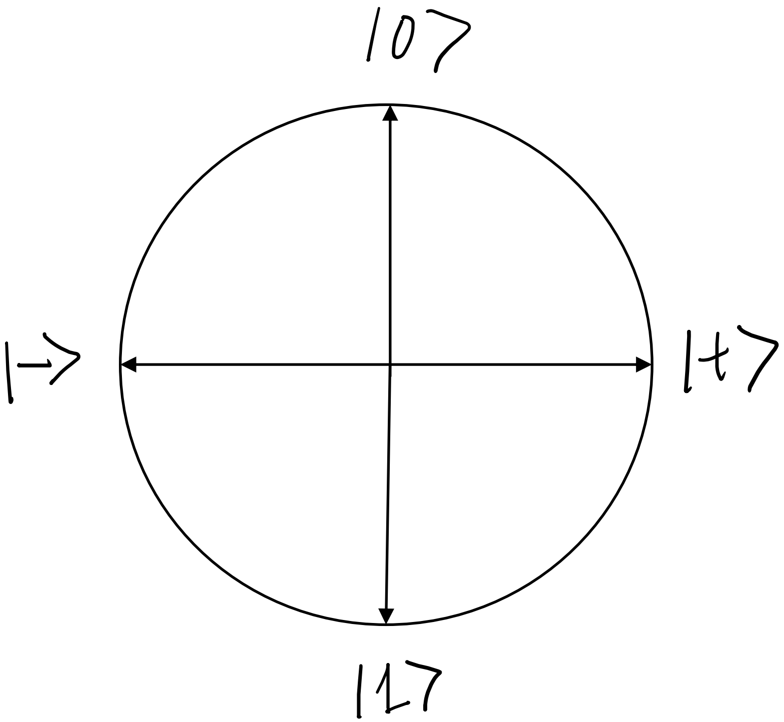
$\eta \geqslant \frac{1}{2}$ $\eta \geqslant \frac{1}{3}$ ...

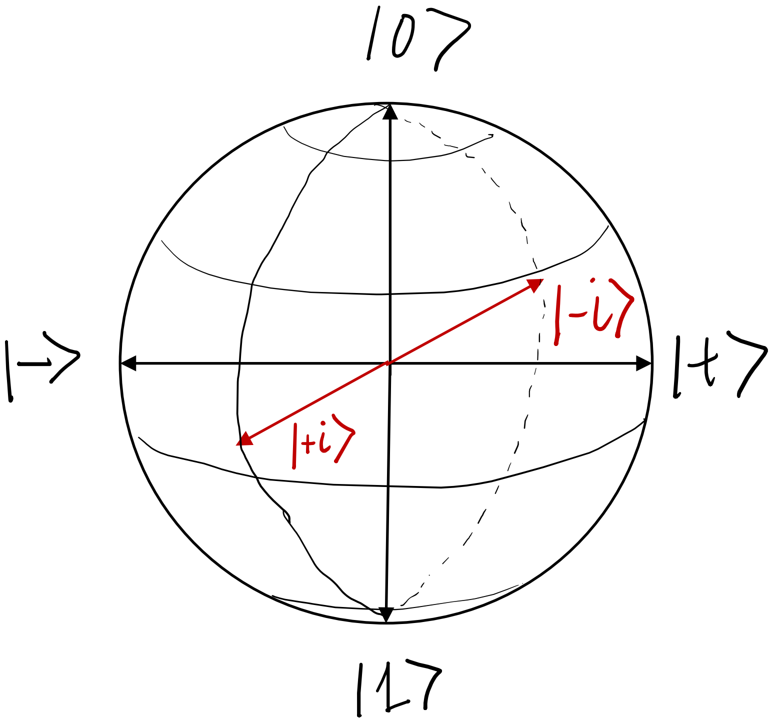
The results can be extended to **multiple bases** and we show that is **more loss-tolerant**



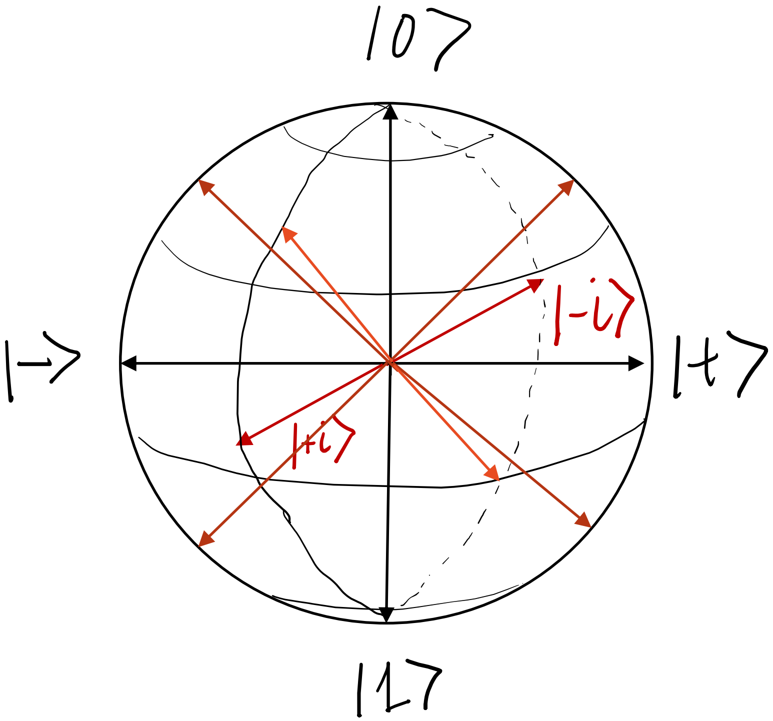
$\eta \geq \frac{1}{2}$ $\eta \geq \frac{1}{3}$ ...

The results can be extended to **multiple bases** and we show that is **more loss-tolerant**





...

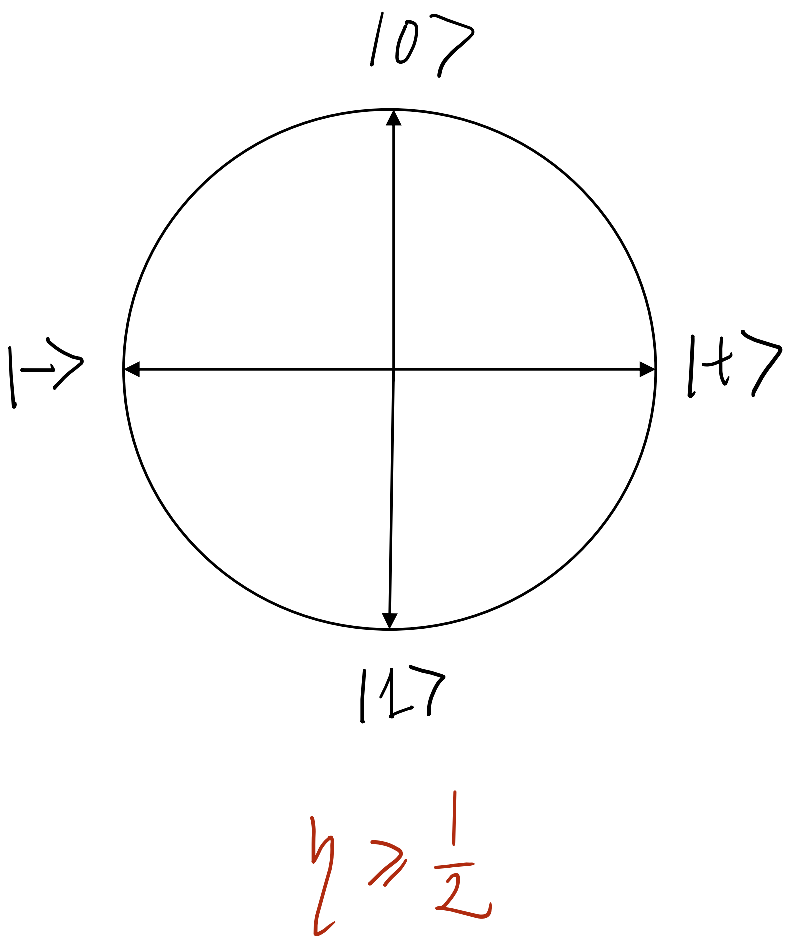


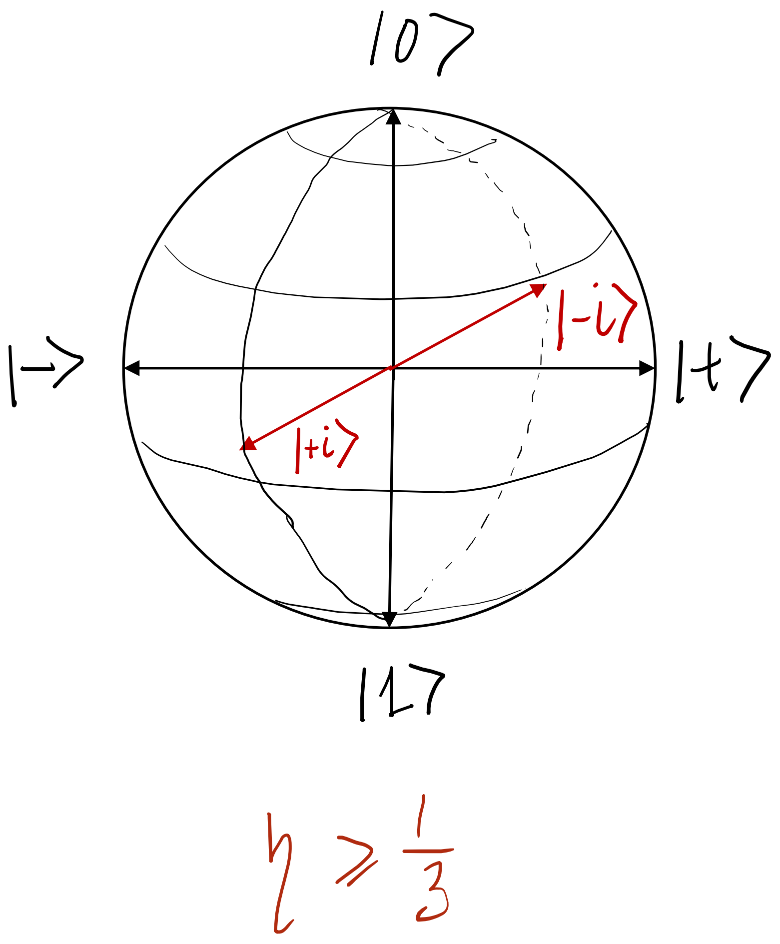
$\eta \geq \frac{1}{2}$

$\eta \geq \frac{1}{3}$

...

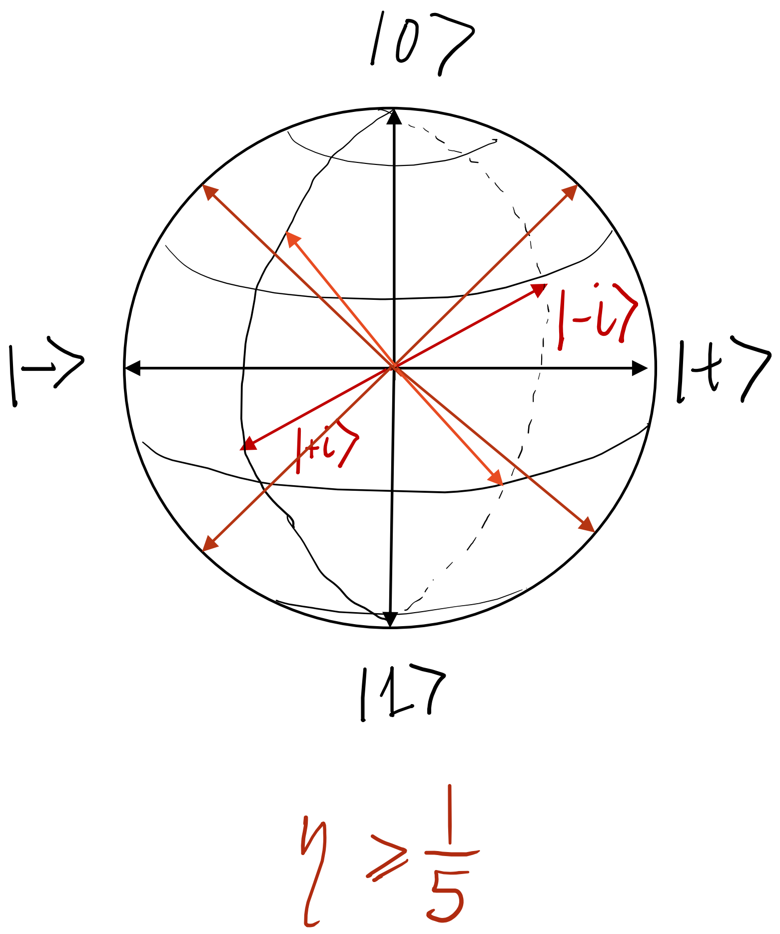
The results can be extended to **multiple bases** and we show that is **more loss-tolerant**



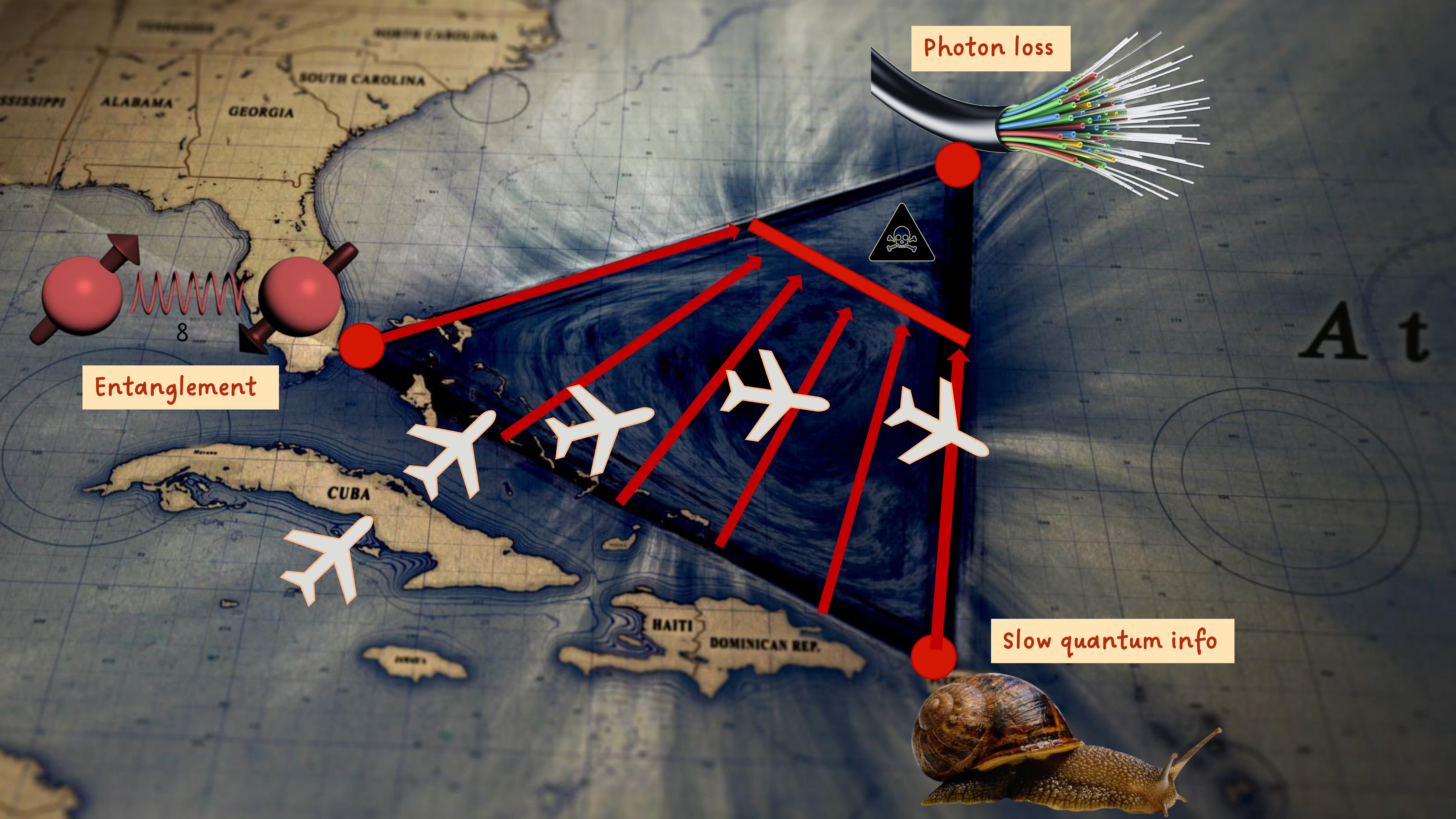


...

...




Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
GEORGIA
ALABAMA
CUBA
HAITI
DOMINICAN REP.
At



Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.

Photon loss
Entanglement
Slow quantum info
SOUTH CAROLINA
ALABAMA
GEORGIA
CUBA
HAITI
DOMINICAN REP.

Thanks for you attention!

Llorenç Escolà Farràs, PhD candidate

l.escolafarras@uva.nl

QuSoft

Research Center for Quantum Software

Universiteit van Amsterdam