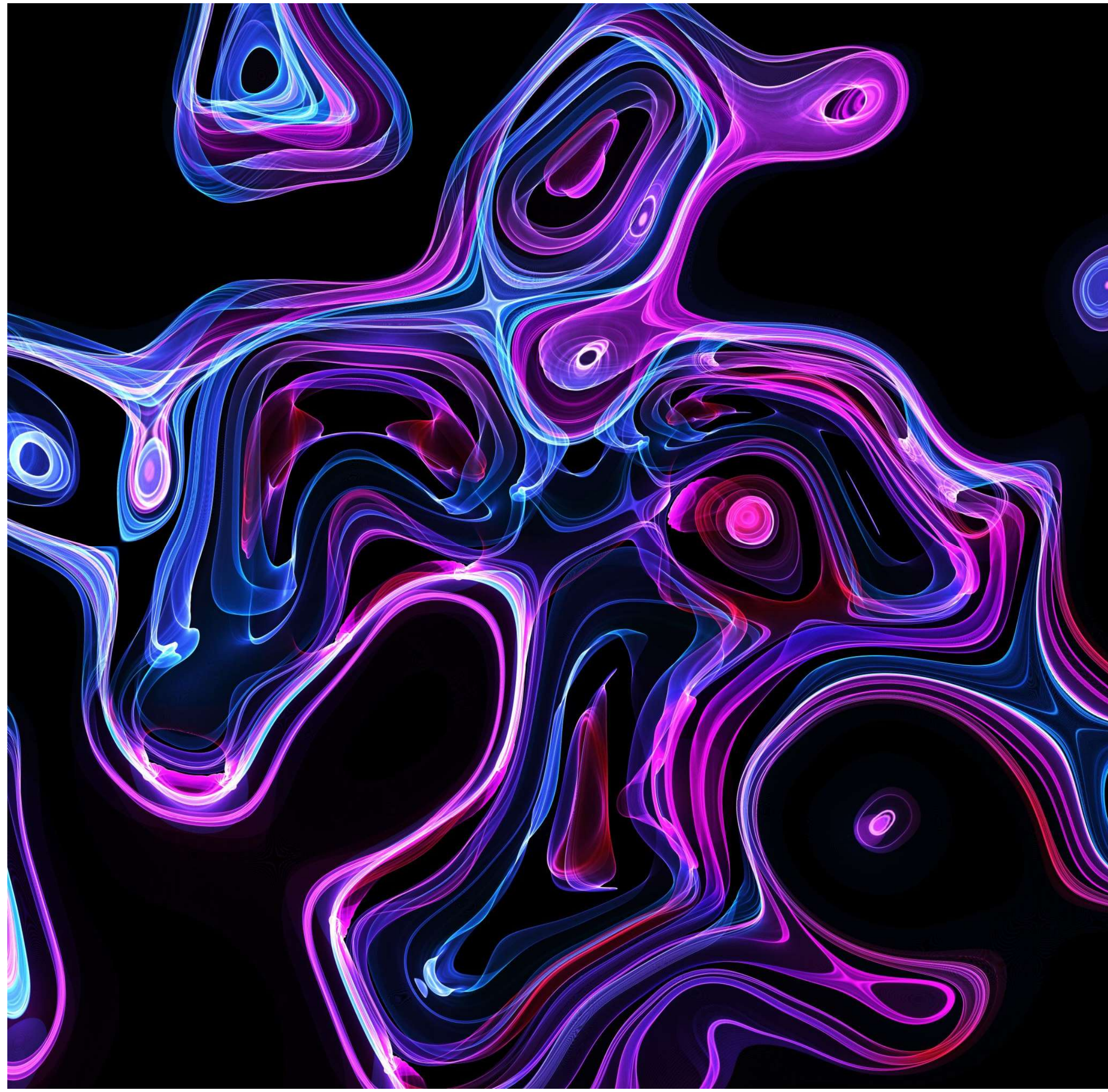
Quantum Position Verification

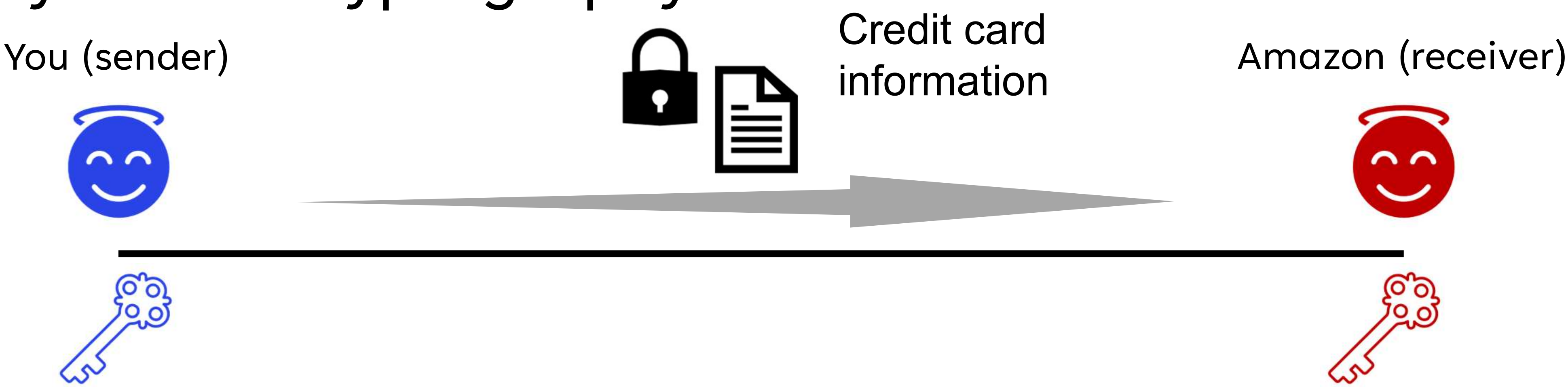
Team 8
Yuta Hirasaki, Wenrong Huo,
Yudi Huang, Jierui Hu,
Wenhan Hua and Soroush Hoseini



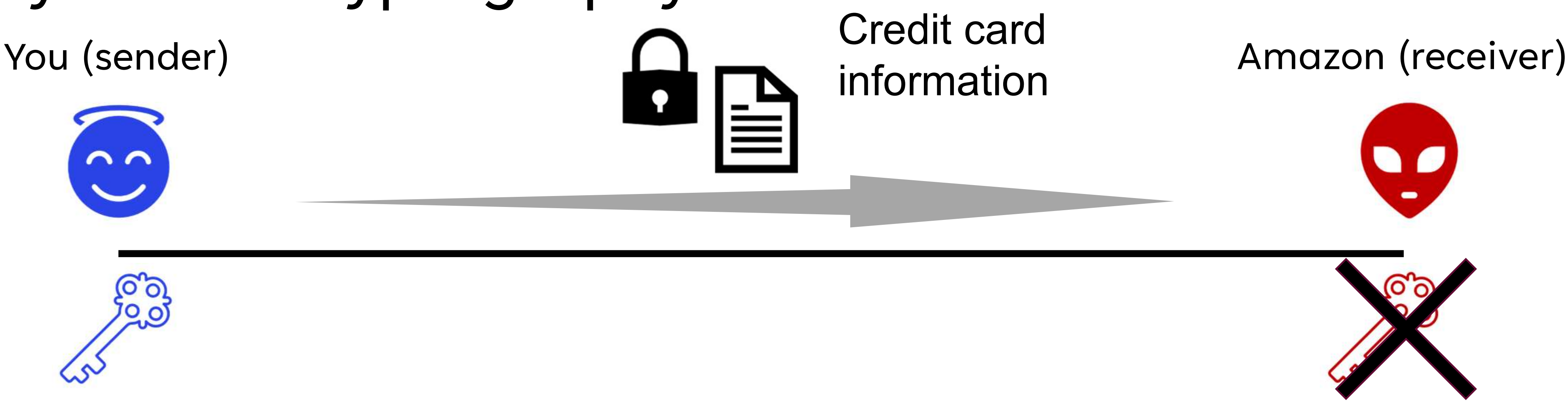
Reference:

– Allerstorfer, Rene, et al. "Making existing quantum position verification protocols secure against arbitrary transmission loss." *arXiv:2312.12614* (2023).

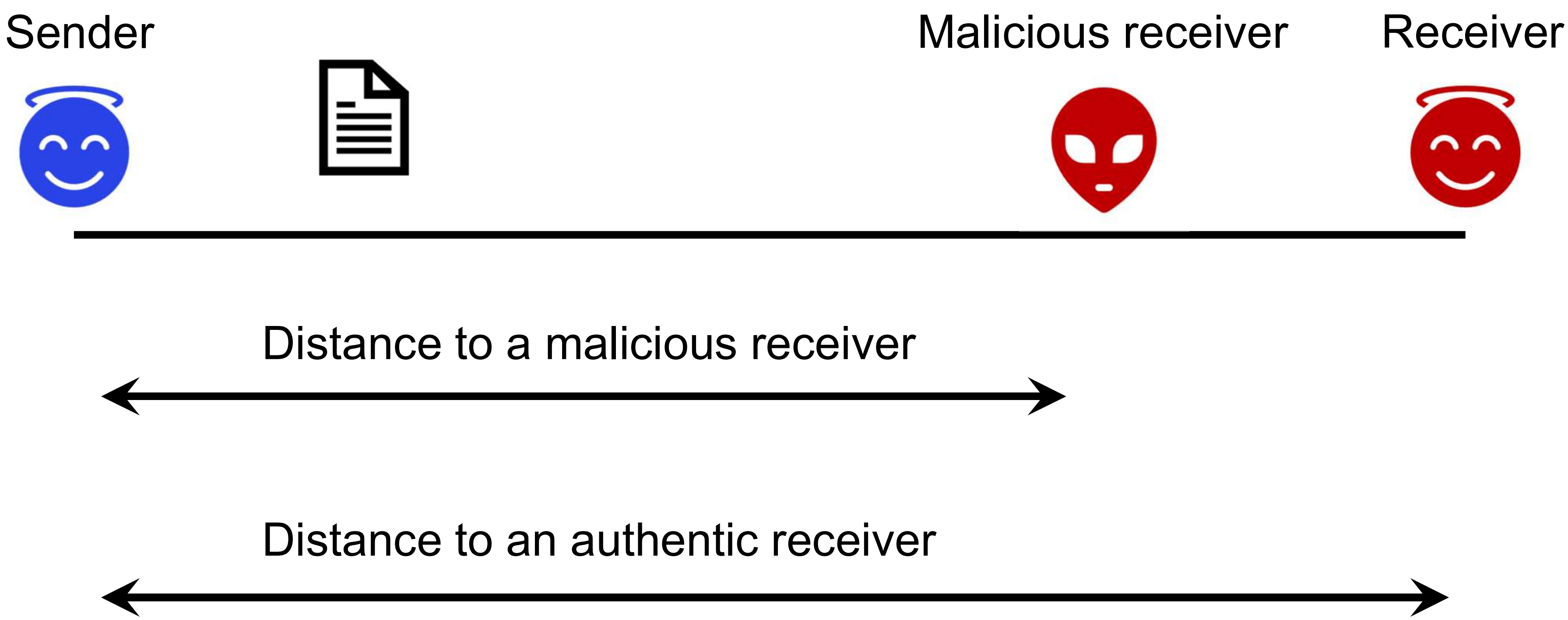
Key based cryptography



Key based cryptography



Position based communication



Communicating information based on the position of the receiver !

Quantum position verification verifies the position securely!

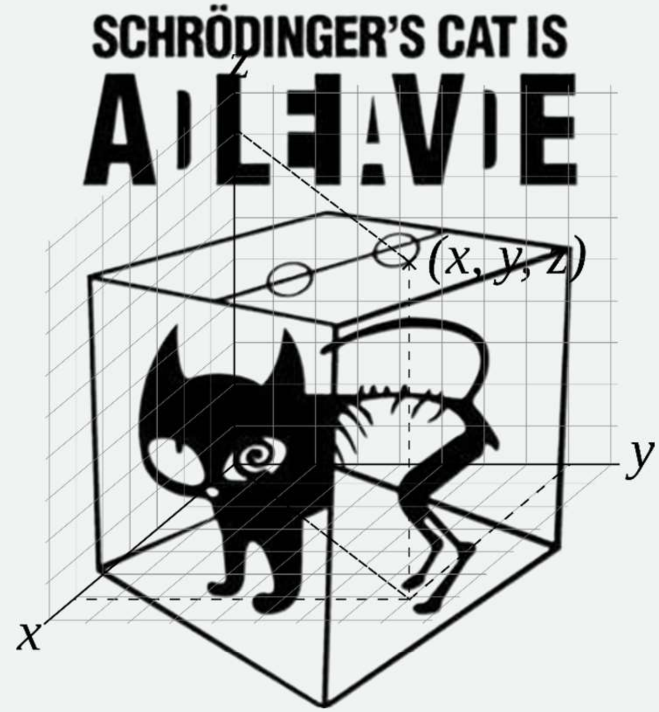
Classical Position Verification (CPV)

- Frame for position verification? – A platform to work on

- CM – Cartesian coordinate systems (or others)
  - Mass, position, force…

- QM – Hilbert space
  - States, operators…

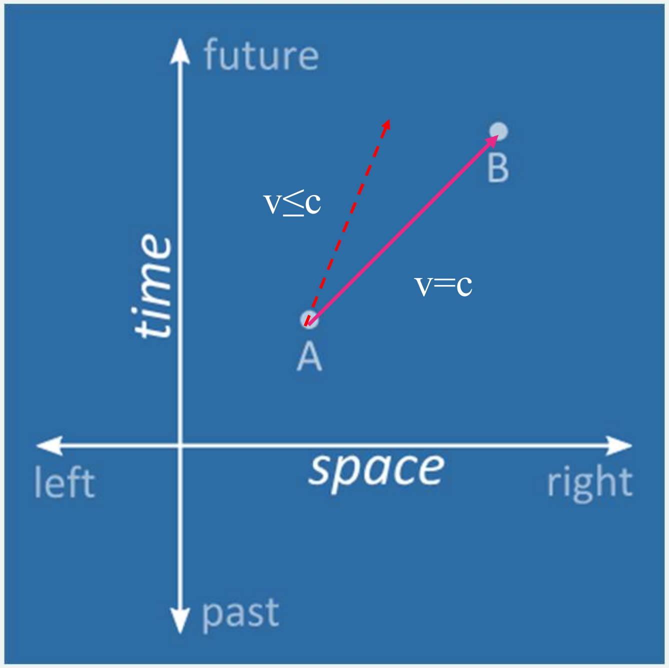
Cartesian coordinates



Why space-time diagram in CPV?

- Special Relativity – Spacetime diagram
  - Similar to what we want!

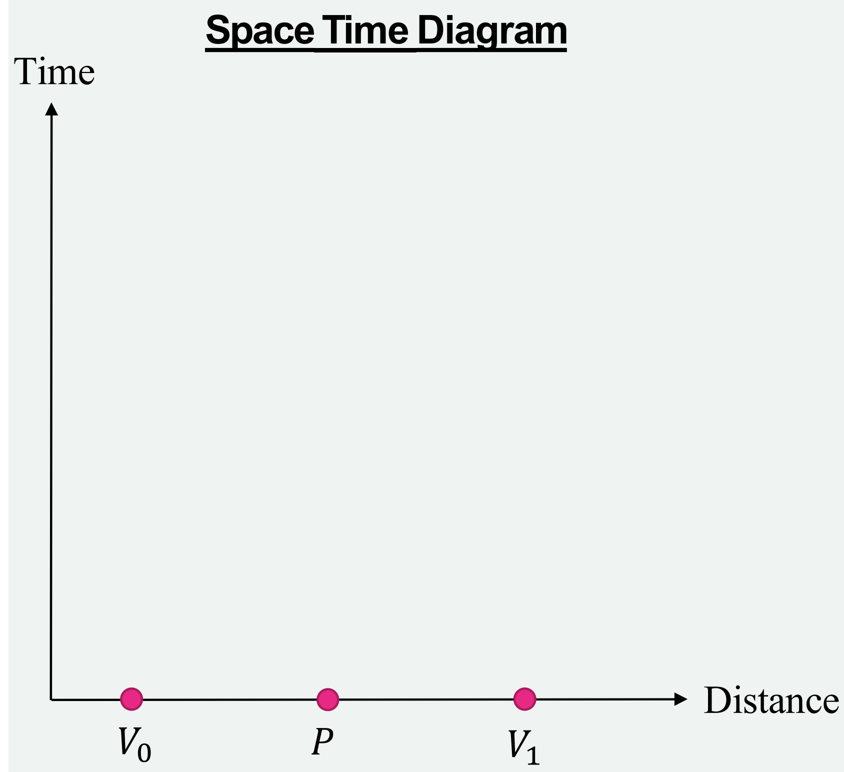
- Convention:
  - Solid and dashed arrows: classical and quantum signal



CPV: Setup

– Prover – wants to be proved

– Verifiers – use an approach to verify the prover

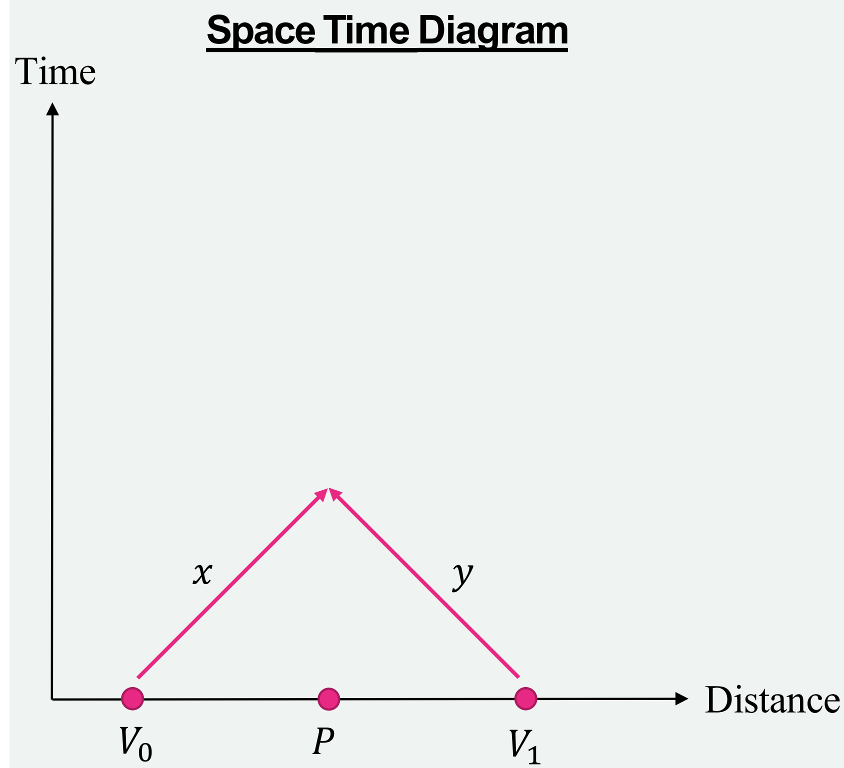


CPV: Transmit Signal

– Simple Protocol

  – V_0 and V_1 each send a classical bit of verification information: $x, y \in (0,1)^n$ sequence

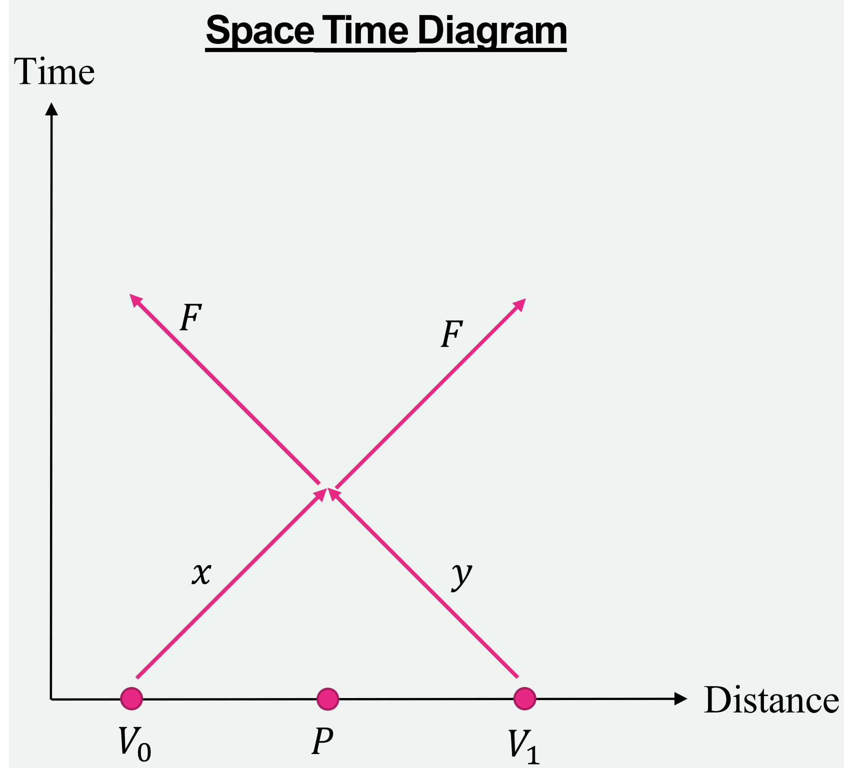
  – Synchronization: x, y arrive simultaneously at P



CPV: Feedback

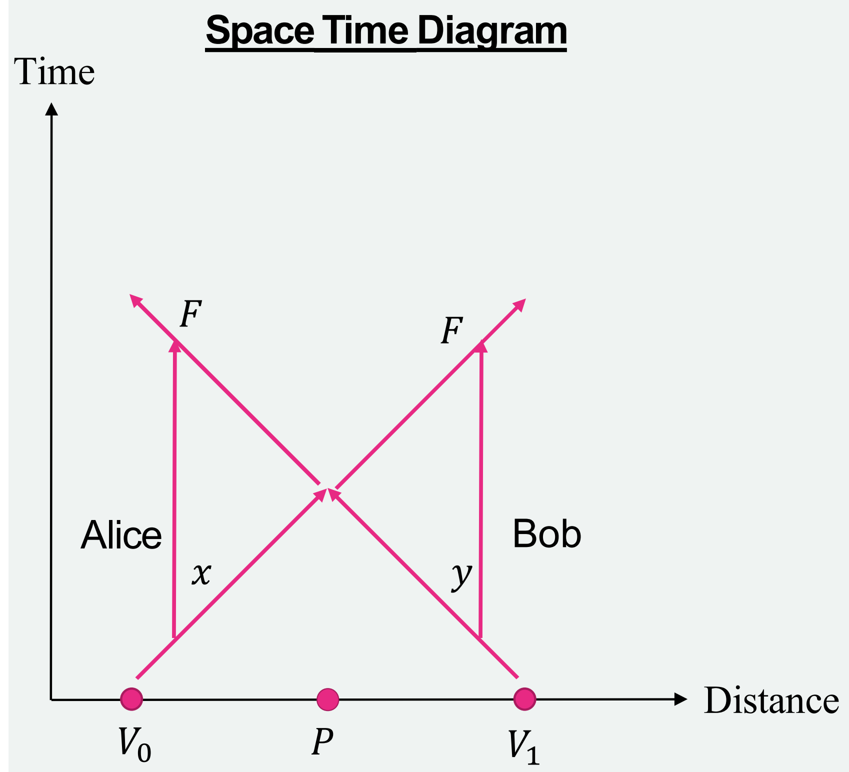
– Position Verification:

  – P calculate: $F = XOR(x, y)$ and send it back. V_0 and V_1 verify F. Timing and Accuracy → Verification



Attacks on CPV

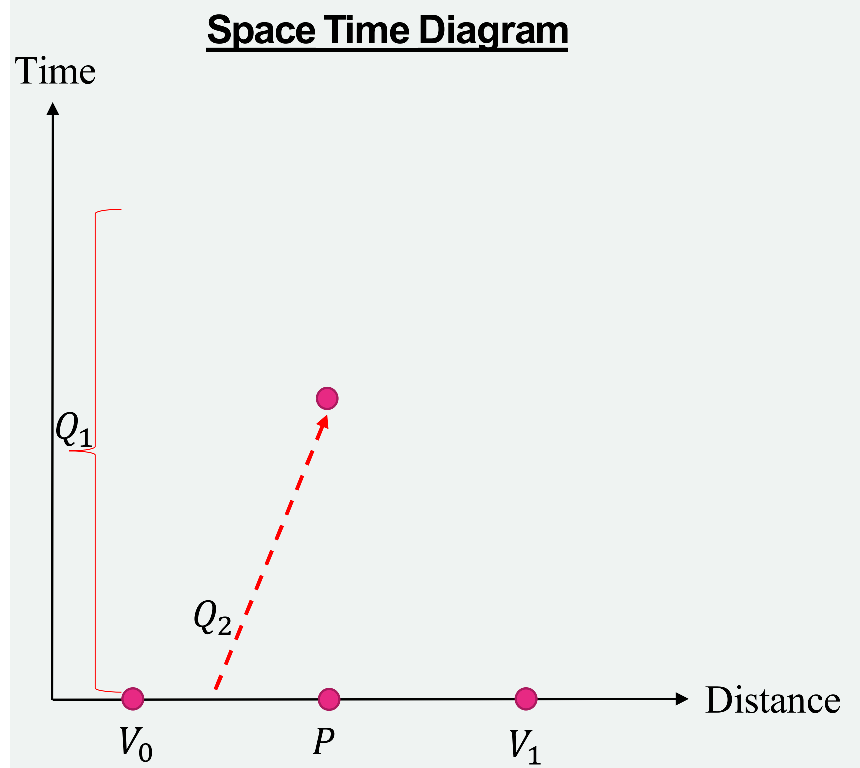
- Two Colluding Attackers can do as follows:
  - Alice and Bob both intercept : x, y and send each other a copy
  - Using their copies of x, y Alice and Bob independently calculate $F = XOR(x, y)$, and send their results to V_0 and V_1 to verify



Quantum Position Verification

– QPV BB84

– V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1

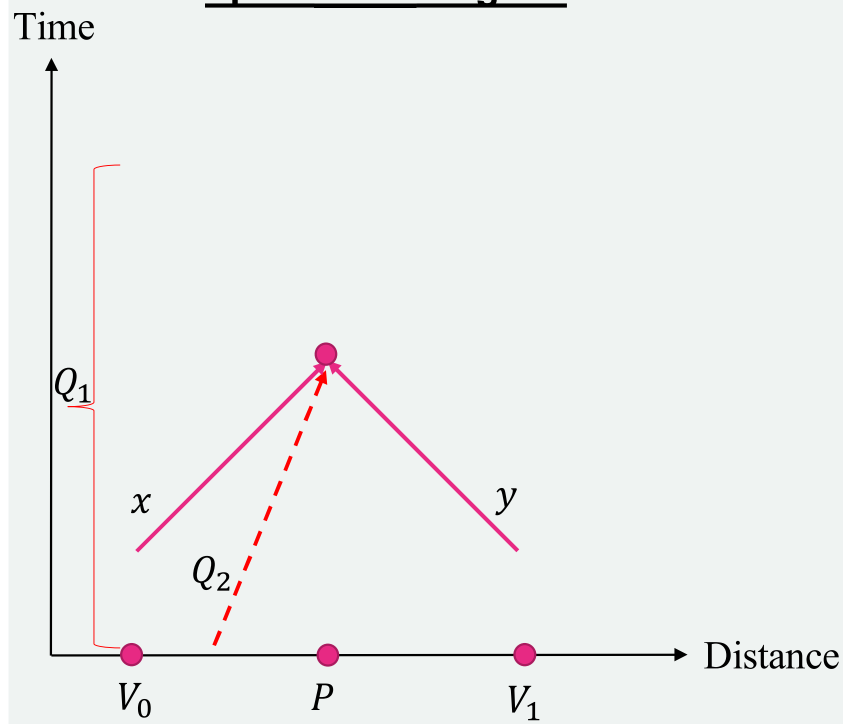


Quantum Position Verification

– QPV BB84

- V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1
- V_0 and V_1 send x, y such that they arrive simultaneously with Q_2 at P

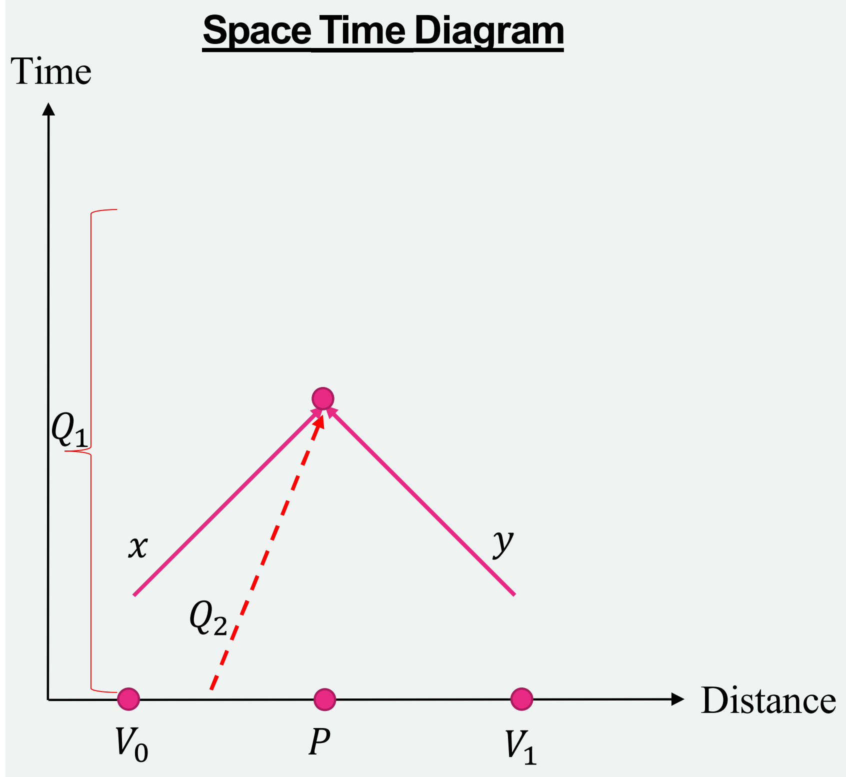
Space Time Diagram



Quantum Position Verification

– QPV BB84

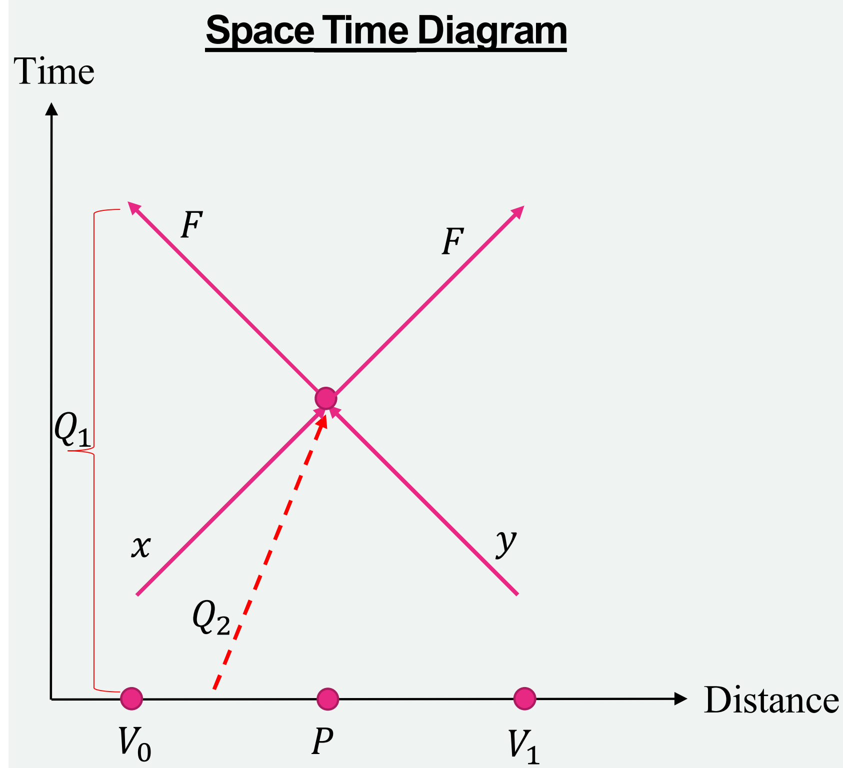
- V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1
- V_0 and V_1 send x, y such that they arrive simultaneously with Q_2 at P
- Basis function $\langle XOR(x,y)|Q_2\rangle$: Project Q_2 onto Computational basis or Hadamard basis.
- Computational basis: |0> and |1>
- Hadamard basis: $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$



Quantum Position Verification

– QPV BB84

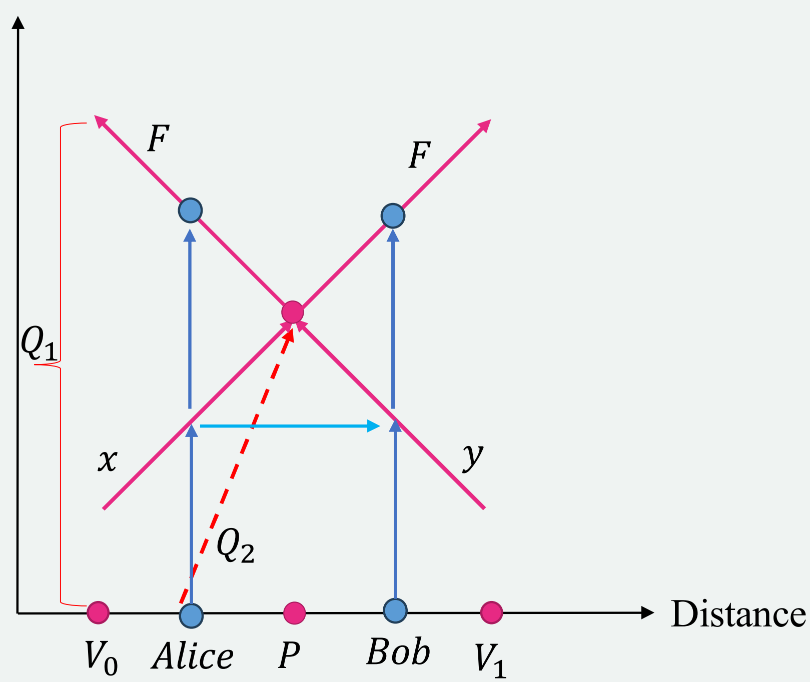
- V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1
- V_0 and V_1 send x, y such that they arrive simultaneously with Q_2 at P
- P returns $F = \langle XOR(x, y)|Q_2\rangle$ and transmits it to V_0 and V_1, along with y to V_0
- V_0 calculates $A = \langle XOR(x, y)|Q_1\rangle$ and compares it with F to compare



Attack on QPV

– **Pre-Shared Entanglement**
  – Alice and Bob share entangled pairs (typically EPR pairs) before the QPV protocol begins.

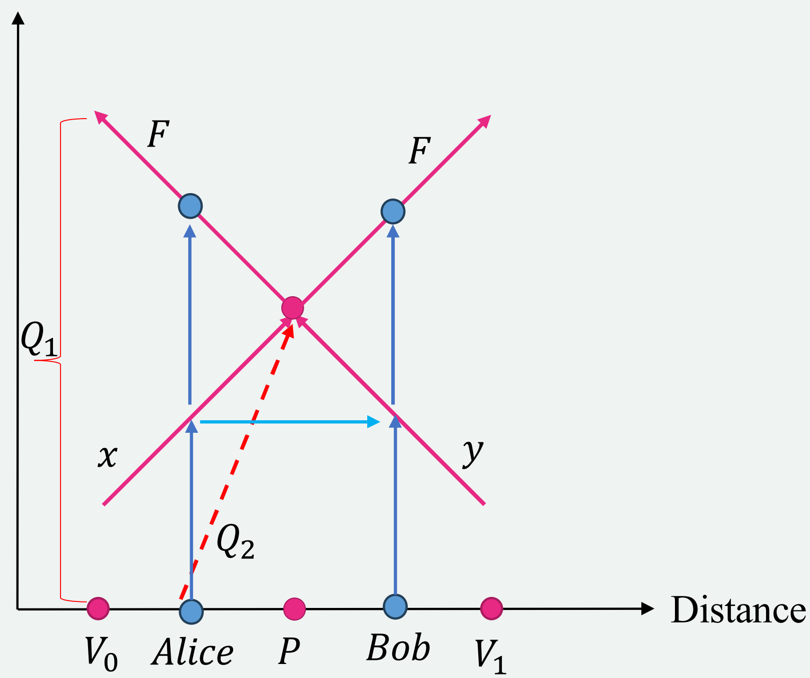
Space Time Diagram



Attack on Quantum Position Verification

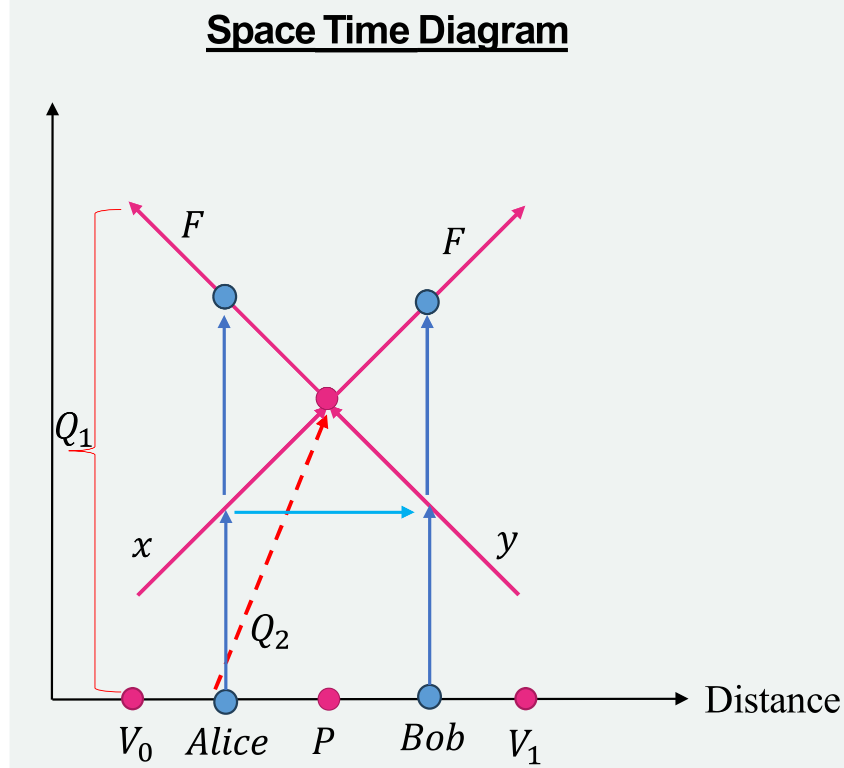
- Pre-Shared Entanglement
  - Alice and Bob share entangled pairs (typically EPR pairs) before the QPV protocol begins.
- **Teleportation Process**
  - Using quantum teleportation, Alice can transfer the intercepted quantum state to Bob using their entanglement. This happens instantaneously across any distance. (**Entanglement swapping**.)

Space Time Diagram



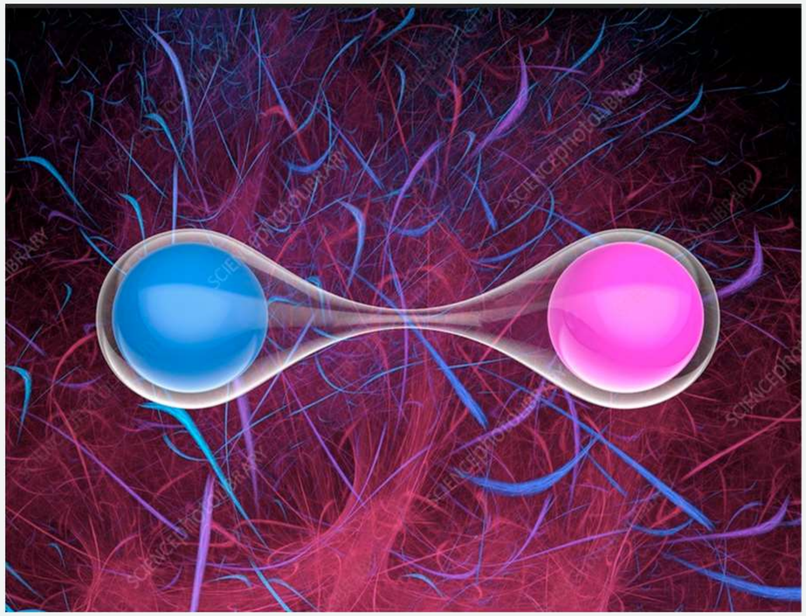
Attack on Quantum Position Verification

- **Pre-Shared Entanglement**
  - Alice and Bob share entangled pairs (typically EPR pairs) before the QPV protocol begins.
- **Teleportation Process**
  - Using quantum teleportation, Alice can transfer the intercepted quantum state to Bob using their entanglement. This happens instantaneously across any distance. (**Entanglement swapping**.)
- **Simulating the Prover**
  - After receiving classical information, attackers measures the quantum state and sends the appropriate response to the verifiers.



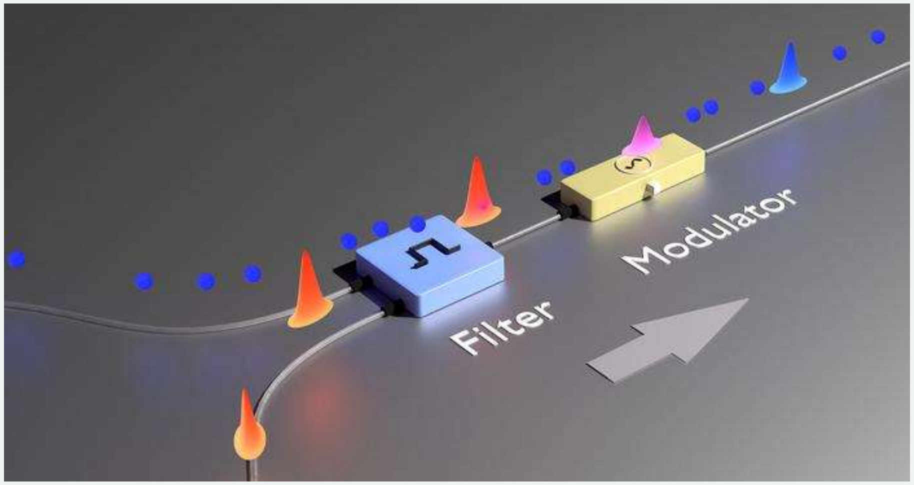
Limitations with QPV

- In general, all QPV protocols are **weak** against the use of **entangled pairs**
- The goal is to prove the location of a fair user **easily**, while attackers would need **infeasible** amounts of quantum resources to succeed



Requirement for QPV

- **Transmission loss** can significantly impact QPV security.
- By selectively choosing when to **respond** and when to remain **silent**, the attackers reduced the overall chance of being detected.



How do we overcome transmission loss?

– Answer: QPV with commitment, i.e. **cQPVBB84 protocol**

– **Making commitment:**

1. Prover needs to identify before making a measurement whether or not they received it

2. This decision needs to be made before the basis choices are sent, and the measurement is made

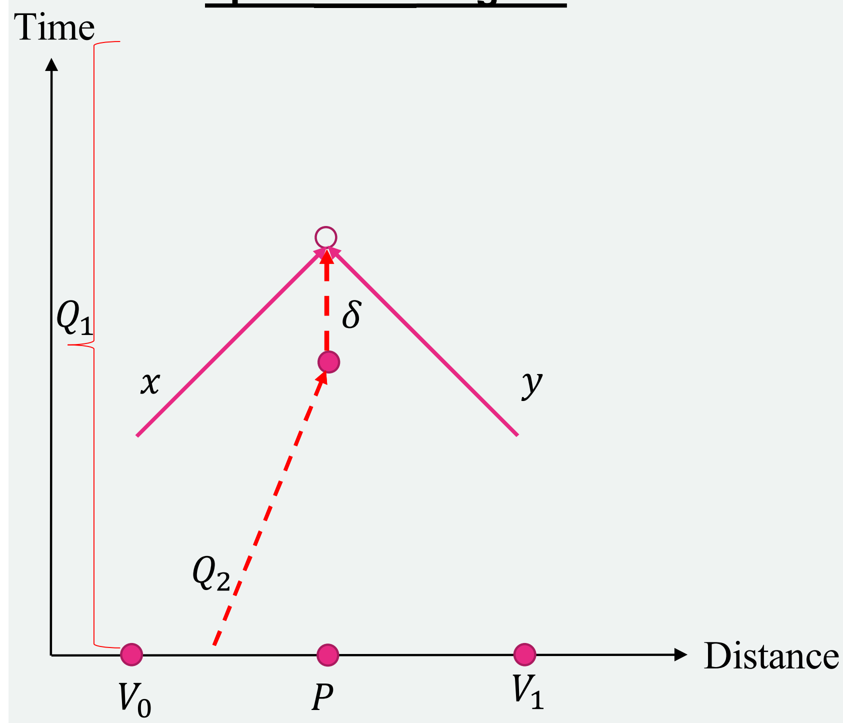
– New Requirement:
a **non demolition measurement** of the photon

cQPVBB84 Protocol

– Protocol

- V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1
- V_0 send Q_2 early such that it arrive at a time δ before x, y at P

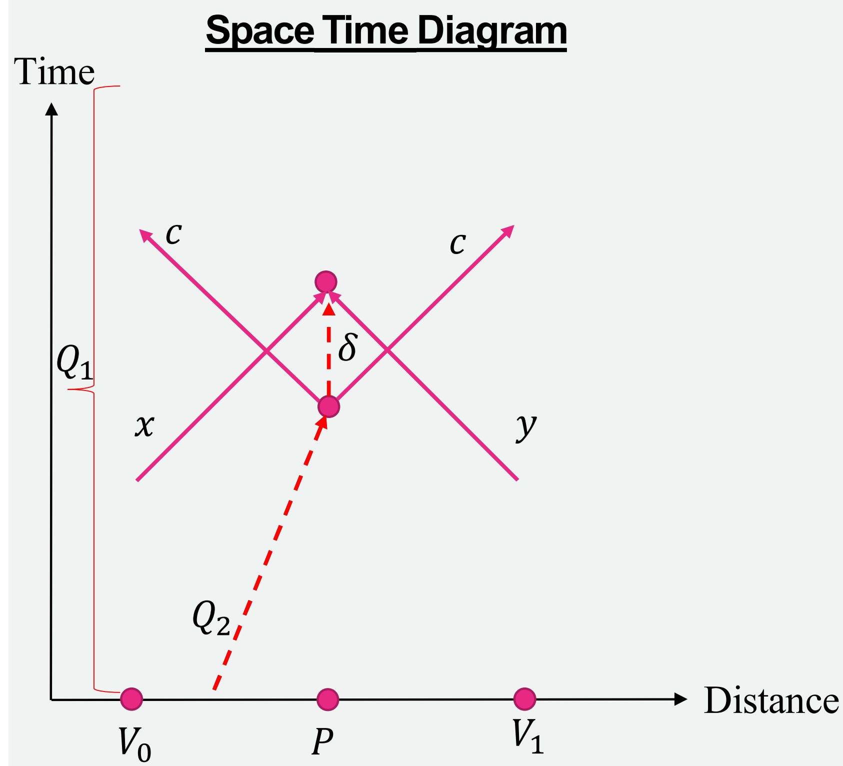
Space Time Diagram



cQPVBB84 Protocol

– Protocol

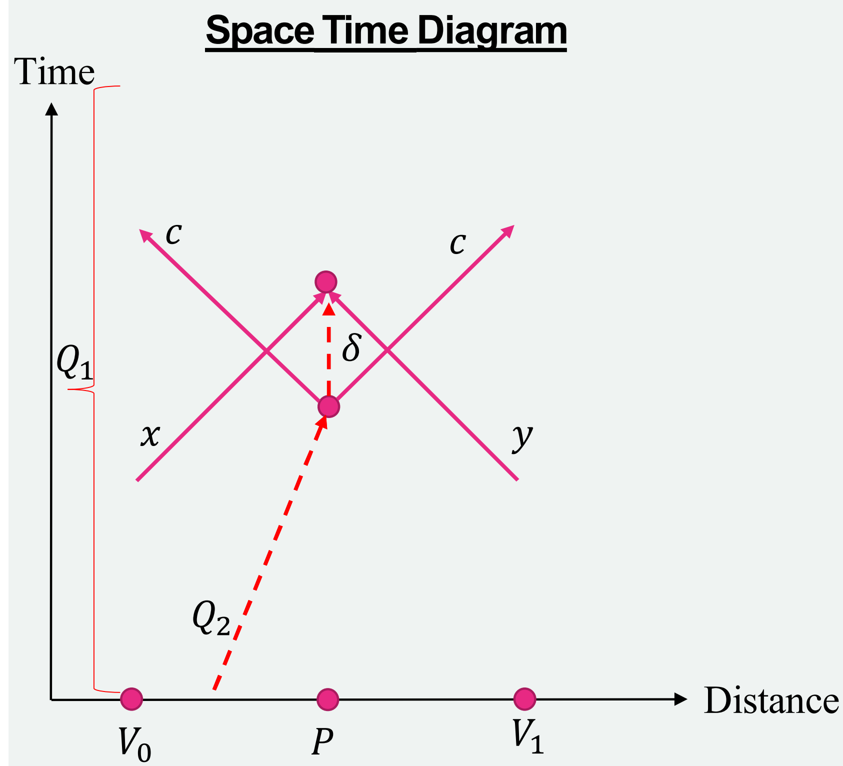
- V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1
- V_0 send Q_2 early such that it arrive at a time δ before x, y at P
- P then submits $c \in \{0{,}1\}$ where 0 denotes no detection, 1 denotes a non demolition detection event



cQPVBB84 Protocol

– Protocol

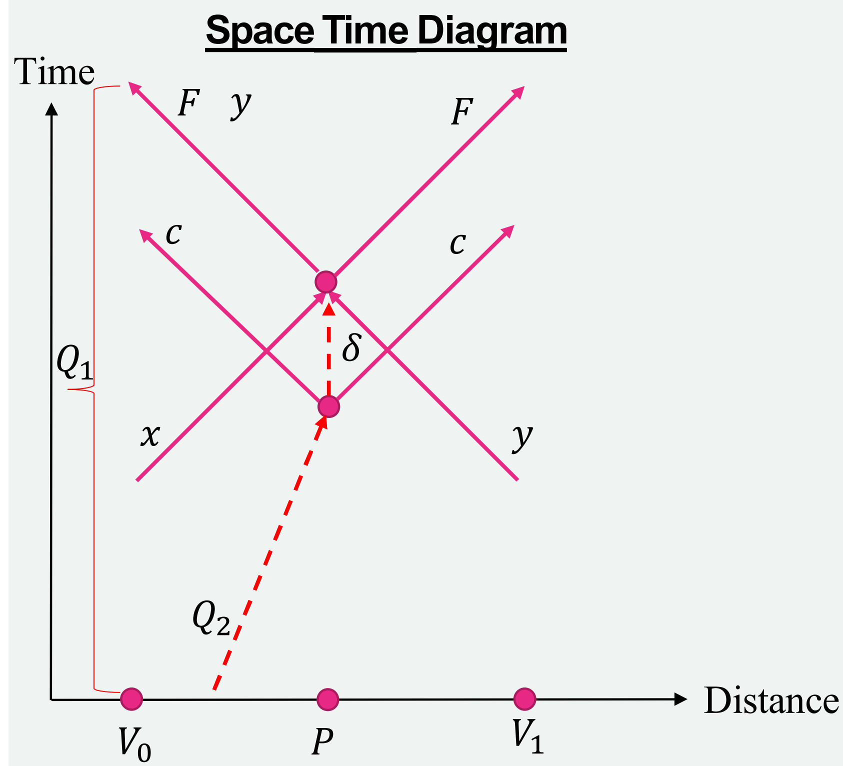
- V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1
- V_0 send Q_2 early such that it at a time δ before x, y at P
- P then submits $c \in \{0,1\}$ where 0 denotes no detection, 1 denotes a non demolition detection event
- P then receives x, y



cQPVBB84 Protocol

– Protocol

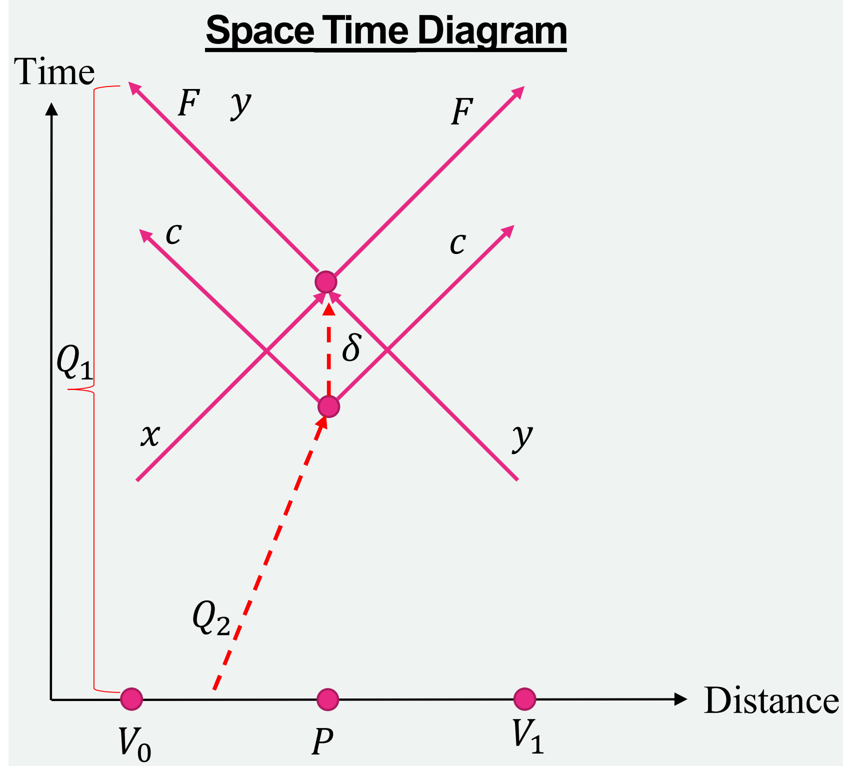
- V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1
- V_0 send Q_2 early such that it arrive at a time δ before x, y at P
- P then submits $c \in \{0,1\}$ where 0 denotes no detection, 1 denotes a non demolition detection event
- P then receives x, y
- P returns $F = \langle XOR(x,y)|Q_2\rangle$ and transmits it to V_0 and V_1, along with y to V_0
- V_0 calculates $A = \langle XOR(x,y)|Q_1\rangle$ and compares it with F



cQPVBB84 Protocol

– Protocol

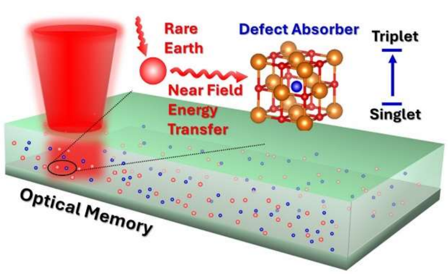
- V_0 prepares the state $Q = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, sending Q_2 to P and storing Q_1
- V_0 send Q_2 early such that it arrive at a time δ before x, y at P
- P then submits $c \in \{0,1\}$ where 0 denotes no detection, 1 denotes a non demolition detection event
- P then receives x, y
- P returns $F = \langle XOR(x, y)|Q_2\rangle$ and transmits it to V_0 and V_1, along with y to V_0
- V_0 calculates $A = \langle XOR(x, y)|Q_1\rangle$ and compares it with F

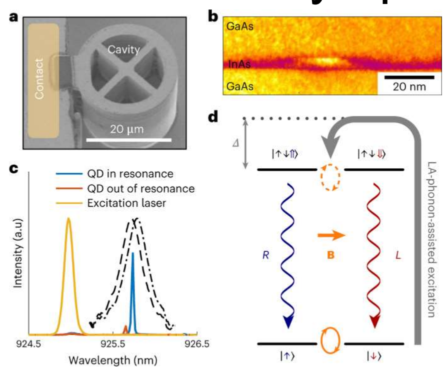


Summary

- Quantum Position Verification (QPV) has advantages over Classical Position Verification (CPV) due to No-cloning theorem.

- But there are still many limitations on QPV, such as transmission loss, and may still be attacked via quantum memory / pre-shared entangled pairs.





i.e. spin-photon entanglement for a quantum memory

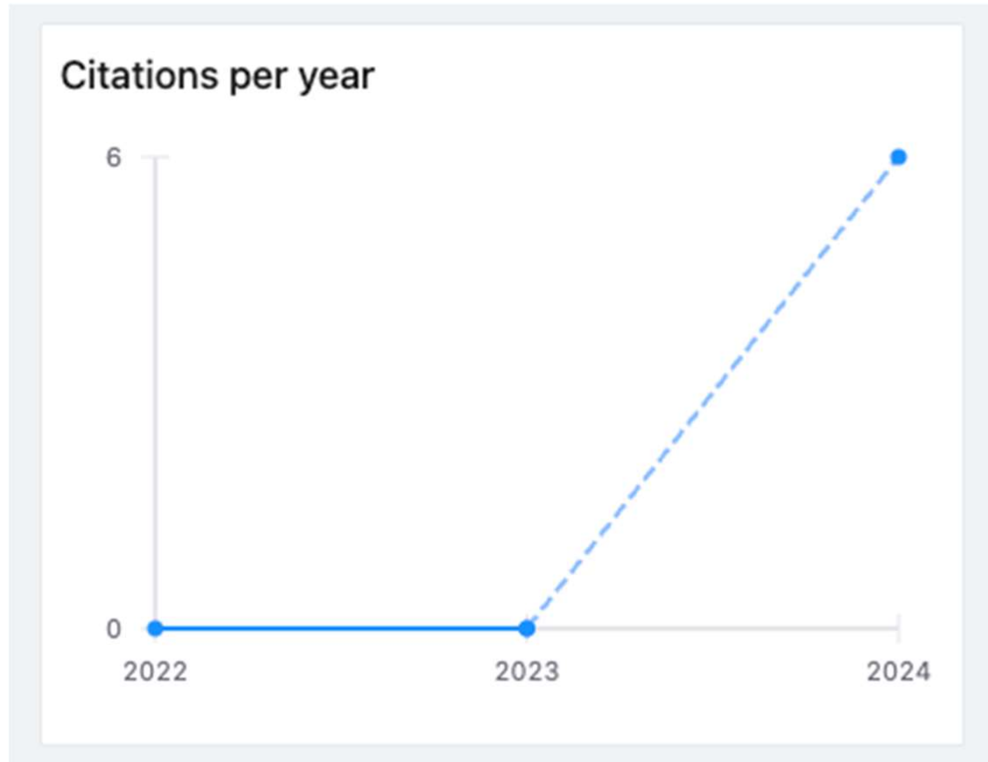
- In this paper, authors devise a new protocol named cQPVBB84 Protocol, which can overcome transmission loss. This protocol is also more secure.

Citation of the paper

Allerstorfer, Rene, et al.

"Making existing quantum position verification protocols secure against arbitrary transmission loss."

arXiv preprint arXiv:2312.12614 (2023).



(Reproduced from inspire HEP 12/4/2024)

Critical Analysis

Pros:

- QPV is robust against classical interception
  - No cloning theorem
- cQPV BB84
  - Improvement of past QPV protocols that enables full loss tolerance.
  - More secure against attackers
    - successful attacks need more resource
- In principle feasible in experiments.

Cons:

- The experimental limitations of quantum non demolition measurements
  - Measuring the existence of a photon without collapsing the state
  - Heralding the existence by using teleportation - the efficiency is low
- Generally, QPV is weak against the use of quantum memories and entangled pairs