Untrusted Entanglement Node Strategy for Quantum Repeaters Using Quantum Teleportation

Richard Tjörnhammar

June 29, 2025

1 Overview

This document sketches a strategy for quantum communication using untrusted intermediate nodes (quantum repeaters), leveraging quantum teleportation to maintain end-to-end security and to conform with the no-cloning theorem. This corresponds to a hypothetical setup where an untrusted third party performs entanglement swapping in order to act as a signal repeater. Although hypothetical and speculative, some suggestions for designs are given. Other optical parts are required for dark (1550nm) fiber photonics.

1.1 Acronyms

- **SPDC** Spontaneous parametric down-conversion
- **BSM** Bell-state measurement
- **PBS** Polarizing beam splitter
- **HWP** Half Waveplate
- **QWP** Quarter Waveplate

2 Core Concepts

- **No-Cloning Theorem**: Prohibits copying of an unknown quantum state.
- **Quantum Teleportation**: Enables the transfer of a quantum state using shared entanglement and classical communication.
- **Entanglement Swapping**: Enables entanglement between remote qubits via an intermediate Bell-state measurement (BSM).

3 Schematic Overview

Actors

- Alice (A): Trusted sender
- Bob (B): Trusted receiver
- Charlie (C): Untrusted node

Protocol Flow

1. Alice prepares Bell pair $(Q1_A, Q2_A)$
2. Bob prepares Bell pair $(Q1_B, Q2_B)$
3. Alice sends $Q2_A$ to Charlie
4. Bob sends $Q2_B$ to Charlie
5. Charlie performs BSM on $Q2_A$ and $Q2_B$
6. Charlie announces BSM result (classically)
7. $Q1_A$ and $Q1_B$ are now entangled
8. Alice can now teleport a quantum state $|\psi\rangle$ to Bob

4 Protocol Sketch

Assumptions

- Classical channels are authenticated
- Quantum channels are lossy but not actively adversarial
- Charlie is untrusted

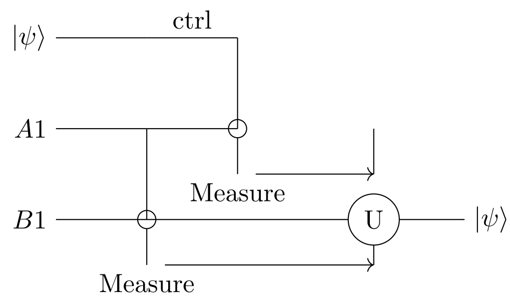
Steps

1. Alice prepares $|\Phi^+\rangle_{A1,A2} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. Bob prepares $|\Phi^+\rangle_{B1,B2} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
3. Alice sends $A2$ to Charlie; Bob sends $B2$ to Charlie
4. Charlie performs a BSM on $A2$ and $B2$, obtains result $m \in \{00, 01, 10, 11\}$
5. Charlie broadcasts m
6. Now $A1$ and $B1$ are entangled
7. To teleport $|\psi\rangle$ from Alice to Bob:
   (a) Alice performs BSM on $|\psi\rangle$ and $A1$, gets result n
   (b) Alice sends n to Bob
   (c) Bob applies $U_n \cdot U_m$ to $B1$ to recover $|\psi\rangle$

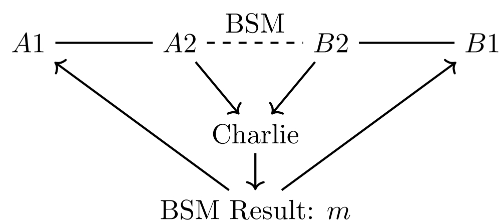
5 Security Properties

- Charlie learns nothing about $|\psi\rangle$
- No cloning is violated: state is destroyed at sender
- Entanglement is established securely end-to-end

6 Quantum Circuit Diagram



7 Entanglement Swapping Visualization



After BSM: $A1 \leftrightarrow B1$ entangled

8 Suggested Experimental Layouts for Alice, Bob, Charlie

- **Alice (A)**:
  - Entangled photon source (e.g., SPDC)
  - Delay line and quantum memory (optional)
  - BSM device (for teleportation phase)
  - Classical communication module
- **Charlie (C)**:
  - Bell-State Analyzer (e.g., beam splitter, detectors, polarizers)
  - Synchronization detectors
  - Classical broadcast unit (BSM result)
- **Bob (B)**:
  - Entangled photon source (paired with A)
  - Quantum memory (optional)
  - Unitary correction device (waveplates, EOMs)
  - Classical receiver

9 Experimental Considerations

- **BSM fidelity**: Requires high-fidelity Bell-state measurements. Optical setups may use beam splitters and photon detectors; matter-based implementations might use trapped ions or NV centers.
- **Photon indistinguishability**: Photons from Alice and Bob must be indistinguishable in frequency, polarization, and timing. This often requires careful spectral filtering and stabilization of photon sources.
- **Synchronization**: Precise timing is needed so qubits from Alice and Bob arrive simultaneously at Charlie. This can involve pulsed lasers, time-tagging, and classical synchronization pulses.
- **Loss mitigation**: Channel losses can be addressed through heralded entanglement generation, quantum error correction, or multiplexed sources to increase successful entanglement rate.
- **Entangled photon source**: Can use spontaneous parametric down-conversion (SPDC) or quantum dots. Matter-based systems may require optical cavities for efficient photon collection.
- **Quantum memory (optional)**: If extended synchronization is needed, quantum memories (e.g., rare-earth doped crystals, atomic ensembles) may buffer qubits.
- **Classical communication**: Fast and authenticated classical channels must be available for sharing BSM results and teleportation corrections.

10 Hybrid Quantum Repeater Strategy with Partial Trust

In certain quantum network architectures, it is practical to assume that not all intermediate nodes are equally untrusted. A hybrid strategy leverages partially trusted nodes to improve performance without compromising end-to-end security.

Trust Model

- Some intermediate nodes are partially trusted to perform specific operations (e.g., entanglement purification, state storage).
- Untrusted nodes are only used for entanglement swapping and BSM.
- Trusted nodes do not have access to raw quantum data from users.

Protocol Enhancements

- **Entanglement Purification**: Partially trusted nodes can perform purification of Bell pairs received from untrusted nodes to increase fidelity.
- **Quantum Memory at Trusted Nodes**: Storage of high-fidelity entangled pairs enables more effective coordination for long-range entanglement.
- **Multiplexing and Entanglement Routing**: Trusted nodes may handle dynamic routing and prioritization of entanglement resources based on network conditions.

Security Considerations

- Even partially trusted nodes are assumed to be semi-honest; they follow the protocol but may attempt passive attacks.
- End-to-end security is preserved via quantum teleportation, ensuring that raw quantum states are never exposed to intermediate nodes.
- Classical channels between trusted nodes must be authenticated and possibly encrypted.

11 Charlie's Optical Table: Components and Suppliers

Component	**Suggested Type**	**Purpose**	**Edmund Optics Example / Equivalent**
Single-Photon Source	SPDC with Type-II PPKTP or Quantum Dot + Pump Laser	Generate entangled photons	Use nonlinear crystals from partner suppliers (e.g., Raicol); Edmund sells precision lens mounts, filters, and laser modules
Delay Line	Motorized translation stage or fiber spool	Align photon arrival times	*Motorized Linear Stage (25 mm)*
Beam Splitter (BS)	50:50 Non-Polarizing Cube or Plate	Overlap photons for BSM	*#68-356: 50:50 NPBS Cube, 780–820nm*
Wave Plates (optional)	Half/Quarter-Wave Zero-Order	Polarization alignment	*Zero-Order Mounted Waveplates (810 nm)*
Polarizers (optional)	PBS Cube or Glan-Thompson Prism	Polarization filtering or analysis	*PBS Cube e.g. #47-995*
Single-Photon Detectors	SNSPD or Si-APD	Detect photons post-BSM	Integrate 3rd-party modules (e.g., Excelitas, IDQ); Edmund supplies compatible mounts
Coincidence Logic	FPGA-based Time Tagger or TDC	Detect two-photon coincidence	External; mount electronics on Edmund breadboards
Classical Communication	TTL/EOM or fiber lines	Transmit BSM result	*#66-052 FC/PC to Free Space Collimator*
Optical Mounts	Kinematic Mounts, Mirror Mounts	Stable optical alignment	*Kinematic Mounts*; RS Series
Optical Table	Steel honeycomb breadboard	Reduce mechanical vibrations	*Steel Honeycomb Breadboard, Damped*

12 Conclusion

Untrusted quantum repeaters using entanglement swapping and teleportation allow for secure and scalable quantum networks. This method respects the no-cloning theorem and provides a path to practical device-independent quantum communication. Implementing such systems requires precise control over entanglement sources, timing, and measurement fidelity, but recent experimental advances make this a promising direction for long-range quantum networks.

13 Addendum: ABCD Station Layout with Entanglement Swapping

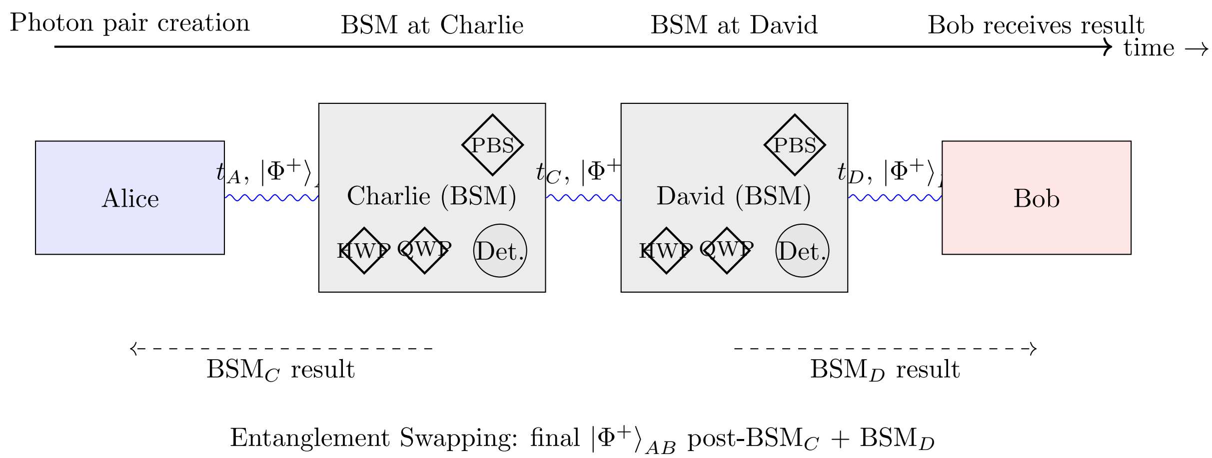


Figure 1: Extended repeater setup: Alice–Charlie–David–Bob configuration with optical elements, detectors, and temporal sequencing.

13.1 State Evolution Through Entanglement Swapping

Assume initially:

$$\left|\Phi^+\right\rangle_{AC} = \frac{1}{\sqrt{2}}(|00\rangle_{AC}+|11\rangle_{AC}), \quad \left|\Phi^+\right\rangle_{CD} = \frac{1}{\sqrt{2}}(|00\rangle_{CD}+|11\rangle_{CD}), \left|\Phi^+\right\rangle_{DB} = \frac{1}{\sqrt{2}}(|00\rangle_{DB}+|11\rangle_{DB})$$

After Bell-state measurement (BSM) at Charlie:

$$\mathrm{BSM}_C \Rightarrow \left|\Phi^+\right\rangle_{AD} \text{ (up to Pauli correction)}$$

Then, BSM at David:

$$\mathrm{BSM}_D \Rightarrow \left|\Phi^+\right\rangle_{AB} \text{ (entanglement successfully swapped)}$$

This process teleports the quantum correlations across untrusted nodes, preserving entanglement without directly transmitting qubits.

13.2 David's Optical Table: Components and Requirements

Component	**Suggested Type**	**Purpose**	**Example / Supplier**
Single-Photon Input	Fiber-coupled from Charlie and Bob	Photon arrival for BSM	High-NA collimators or fiber couplers
Wave Plates	QWP and HWP	Polarization alignment	*Mounted Waveplates (810 nm)*
Beam Splitter	50:50 NPBS	Overlap photons	*Edmund Optics NPBS*
PBS	Cube or Glan-type	Polarization filtering	*PBS Cube*
Detectors	SNSPD / Si-APD	Detect Bell-state outcomes	IDQ / Excelitas modules
Coincidence Logic	FPGA / TDC	Two-photon detection	External electronics on breadboard
Classical Comm.	TTL/EOM to Bob	Send BSM outcome	TTL modulators or fiber