Theory and Practice of Science and Technology
2025, VOL. 6, NO. 6, 5-10
DOI: 10.47297/taposatWSP2633-456901.20250606

# Designing a Quantum Communication Protocol Leveraging Quantum Switching Centers

Deyong Huang

School of Materials and Energy Southwest University, Beibei, Chongqing, 400715, China

**ABSTRACT**
Quantum communication technology has emerged as a revolutionary field, promising unprecedented security and efficiency in data transmission. This thesis explores the current research status of quantum communication, proposes a novel quantum communication protocol based on quantum switching centers, and delves into the fundamental principles of quantum mechanics that underpin this protocol. The study also discusses the future prospects of quantum communication, highlighting its potential to transform global communication networks. The proposed protocol aims to enhance the scalability and reliability of quantum networks by utilizing quantum switching centers as intermediaries for secure key distribution and information exchange.

**KEYWORDS**
Quantum communication; Quantum switching centers; Quantum protocols; Quantum mechanics; Secure key distribution; Quantum networks

## 1 Introduction

Quantum communication technology harnesses the principles of quantum mechanics—such as superposition, entanglement, and no-cloning—to enable secure and innovative data transmission methods. The field has evolved significantly, with quantum key distribution (QKD) emerging as a cornerstone application, alongside advancements in quantum teleportation and quantum networks. This chapter explores the current research status, highlighting recent breakthroughs, ongoing challenges, and a technology roadmap for future development. As shown in Figure 1, this flowchart illustrates the interaction between the quantum switching center and two users (Alice and Bob).

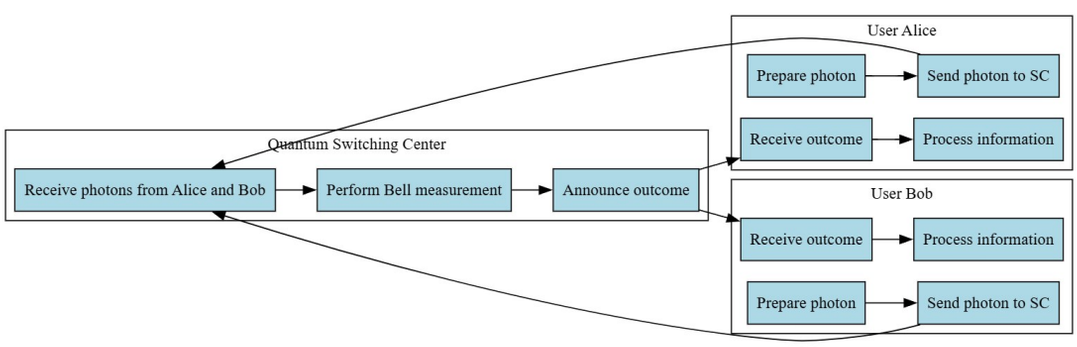


Figure 1 Flowchart Design for MDI and QKD Protocols

By integrating BB84's point-to-point security with E91's entanglement-based verification, the resulting protocol can flexibly operate over a variety of network topologies—ranging from direct fiber links to entanglement-switched quantum repeaters. The security of each component rests firmly on foundational quantum-mechanical principles:

(1) Superposition allows qubits to occupy nonorthogonal states (e.g., rectilinear vs. diagonal bases).

(2) Entanglement enables spatially separated parties to share strongly correlated outcomes that cannot be reproduced by any classical, local hidden-variable model.

(3) No-cloning theorem forbids an eavesdropper from perfectly copying an arbitrary, unknown qubit without introducing detectable disturbances.

Below, we rederive and unify the security arguments for BB84 and E91, highlighting how each protocol detects eavesdropping. We then show how to integrate them into a single hybrid architecture that seamlessly switches between "prepare-and-measure"(BB84) and "entangled-photon" (E91) modes, adapting to the underlying quantum-network infrastructure.

## 2 BB84 protocol: security via the no-cloning theorem

There is a risk of secret key theft by a third party under the BB84 protocol, and the flow of the profile can be seen in the Figure 5. Next, we conduct a specific analysis.

### 2.1 State preparation and measurement bases

#### 2.1.1 Preparation (Alice)

Alice encodes each bit of her raw key onto a single photon (qubit) chosen uniformly at random from one of four polarization states:

$$\begin{cases} |0\rangle \quad (\text{rectilinear"0"}), \\ |1\rangle \quad (\text{rectilinear “1”}), \\ |+\rangle = \dfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \quad (\text{diagonal"+"}), \\ |-\rangle = \dfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \quad (\text{diagonal"−"}). \end{cases}$$

She selects her basis (rectilinear or diagonal) with probability $\frac{1}{2}$ and then chooses one of the two basis states to encode a bit value (“0” or “1”).

#### 2.1.2 Measurement (Bob)

Upon reception, Bob independently and uniformly at random chooses either the rectilinear or diagonal basis to measure each incoming qubit. He records a bit (“0” or “1”) according to the measurement outcome.

#### 2.1.3 Sifting

After all qubits have been transmitted and measured, Alice and Bob publicly announce (over an authenticated classical channel) which basis they used for each qubit—but not the actual bit values. They discard all rounds where their chosen bases disagree. The remaining bits (where both used the same basis) form the sifted key.

### 2.2 Eavesdropping model and induced error

Suppose an eavesdropper, Eve, attempts to gain information by performing an intercept‑resend attack. That is, for each qubit sent by Alice:

① Eve’s measurement

Eve intercepts the photon and measures it in either the rectilinear or diagonal basis, each with probability $\frac{1}{2}$.

n If Eve’s basis $\beta_E$ matches Alice’s original basis $\beta_A$, Eve learns the correct bit without disturbing the state.

n If $\beta_E \neq \beta_A$, her measurement projects the qubit into one of the two states of the wrong basis, effectively randomizing the original information.

② Resending

Eve then prepares a new photon in the state corresponding to her measurement outcome and sends it onward to Bob.

③ Bob’s Measurement

Bob, unaware of Eve’s interference, measures the received photon in his chosen basis (rectilinear or diagonal, each with probability $\frac{1}{2}$).

We now compute the probability that Bob’s measurement result differs from Alice’s original bit, as a function of Eve’s intervention.

### 2.3 Case 1: eve chooses the correct basis

Probability that Eve picks the same basis as Alice:

$$P\left(\beta_E = \beta_A\right) = \frac{1}{2}$$

In this case, Eve obtains the correct bit value without disturbing the state. She resends the exact same state to Bob. If Bob also chooses the same basis, he obtains the correct bit; if he chooses the other basis, the situation reverts to the usual

BB84 basis‑mismatch scenario (which yields a random outcome). However, when Alice and Bob eventually compare bases, they will discard the rounds where Bob's basis did not match Alice's.

Error introduced in the sifted key (when Bob's basis = Alice's basis)?

Zero, because Eve perfectly passed along the correct state.

### 2.4 Case 2: eve chooses the wrong basis

Probability that Eve picks the basis opposite to Alice's:

$$P\left(\beta_E \neq \beta_A\right) = \frac{1}{2}$$

Example (rectilinear vs. diagonal). Suppose Alice sent $|0\rangle$ (rectilinear), and Eve measures in the diagonal basis. She obtains either $|+\rangle$ or $|-\rangle$ each with probability $\frac{1}{2}$. Whichever she obtains, she resends that diagonal‑basis state to Bob.

Now, if Bob measures in the rectilinear basis (and suppose Alice's basis was rectilinear), the state $|+\rangle$ yields "0" or "1" with equal probability $\frac{1}{2}$, and similarly for $|-\rangle$. Hence, Bob's outcome is completely random relative to Alice's original "0." Thus, whenever Bob's basis matches Alice's, Eve's wrong‑basis measurement causes a bit-flip half of the time (i.e., a 50% error probability).

Error contribution:

$$P\left(\text{error}|\beta_E \neq \beta_A, \beta_B = \beta_A\right) = \frac{1}{2}$$

### 2.5 Total error rate induced by eve

We are only concerned with rounds that remain in the sifted key, i.e., when Bob's basis $\beta_B$ equals Alice's basis $\beta_A$. Conditioned on $\beta_B = \beta_A$, we compute the probability that Bob's measurement outcome differs from Alice's original bit if Eve has intercepted:

① Eve picks the correct basis (probability $\frac{1}{2}$). Then no disturbance arises:

$$P\left(\text{error}|\beta_E = \beta_A, \beta_B = \beta_A\right) = 0$$

② Eve picks the wrong basis (probability $\frac{1}{2}$). Then Bob's bit is randomized relative to Alice's, giving a $\frac{1}{2}$ chance of error:

$$P\left(\text{error}|\beta_E \neq \beta_A, \beta_B = \beta_A\right) = \frac{1}{2}$$

Therefore, the total error probability per sifted bit is:

$$P_{error} = P\left(\beta_E = \beta_A\right) \times 0 + P\left(\beta_E \neq \beta_A\right) \times \frac{1}{2} = \frac{1}{2} \times 0 + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$$

In other words, Eve introduces a 25% error rate into the sifted key. By comparing a randomly chosen subset of bits from the sifted key (over an authenticated but public classical channel), Alice and Bob can estimate this error rate. If it significantly exceeds the expected error from intrinsic device imperfections, they conclude that eavesdropping has occurred and abort the protocol.

## 3 E91 protocol: security via violation of bell's inequalities

Where BB84 relies principally on the no‑cloning theorem and basis‑mismatch disturbances, the E91 scheme builds security upon quantum entanglement and the statistical violation of a Bell inequality. We summarize the E91 setup and rederive the key inequality test. We next begin to explore the basic quantum mechanical theoretical processes of the E91 protocol.

### 3.1 Entangled-photon source and measurement settings

#### 3.1.1 Generation of singlet states

A trusted source (which could be centrally located or distributed via entanglement swapping) produces photon pairs in the singlet state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$

where subscripts $A$ and $B$ denote the photons sent to Alice and Bob, respectively.

### 3.1.2 Measurement angles

Alice's three possible measurement bases: choose angles

$$a = 0° \quad a' = 45° \quad a'' = 90°$$

relative to some reference polarization axis.

Bob's three possible measurement bases: choose angles

$$b = 22.5° \quad b = 67.5° \quad b'' = 112.5°$$

In an ideal implementation, Alice and Bob each randomly select one of their three angles for each incoming photon.

### 3.1.3 Outcome labeling

Each measurement yields a binary outcome, which we label as +1 or −1. For instance, in polarization terms, measuring along angle $\theta$:

$$\left|\theta,+1\right\rangle = \cos(\theta)\left|0\right\rangle + \sin(\theta)\left|1\right\rangle, \quad \left|\theta,-1\right\rangle = -\sin(\theta)\left|0\right\rangle + \cos(\theta)\left|1\right\rangle$$

## 3.2 CHSH-type bell inequality

In the Clauser–Horne–Shimony–Holt (CHSH) formulation, one considers four correlation functions:

$$E(a,b) = \left\langle A(a)\,B(b)\right\rangle,$$
$$E(a,b') = \left\langle A(a)\,B(b')\right\rangle$$
$$E(a',b) = \left\langle A(a')\,B(b)\right\rangle$$
$$E(a',b') = \left\langle A(a')\,B(b')\right\rangle$$

Where $A(x)\in\{+1,-1\}$ is Alice's outcome when measuring at angle $x$, and $B(y)\in\{+1,-1\}$ is Bob's outcome when measuring at angle $y$. Define the CHSH parameter

$$S = E(a,b') + E(a',b) + E(a',b) + E(a',b')$$

Under any local hidden-variable (LHV) theory, Bell's theorem implies

$$|S| \le 2$$

However, quantum mechanics predicts that for an entangled singlet state and suitably chosen angles, one obtains

$$|S| = 2\sqrt{2} \approx 2.828 > 2$$

The violation of the bound 2 certifies that the shared state cannot be described by any LHV model—hence confirming genuine quantum entanglement.

## 3.3 Explicit calculation for the singlet state

For $\left|\psi^-\right\rangle$, the correlation for measurements along angles $\alpha$ (Alice) and $\beta$ (Bob) is

$$E(\alpha,\beta) = \left\langle \psi^-\right|\left(\vec{\sigma}_A\cdot\hat{n}_\alpha\right)\otimes\left(\vec{\sigma}_\beta\cdot\vec{n}_\beta\right)\left|\psi^-\right\rangle = -\cos(\alpha-\beta)$$

Where $\vec{\sigma}$ is the Pauli-vector operator and $\hat{n}_\theta$ denotes the unit vector at angle $\theta$. In particular, choose:

$$\begin{cases} a = 0° & ,a' = 45.0° \\ b = 22.5° & ,b' = 67.5° \end{cases}$$

Then:

1. $E(a,b) = -\cos(0° - 22.5°) = -\cos(22.5°)$.
2. $E(a,b') = -\cos(0° - 67.5°) = -\cos(67.5°)$.
3. $E(a',b) = -\cos(45° - 22.5°) = -\cos(22.5°)$
4. $E(a',b') = -\cos(45° - 67.5°) = -\cos(-22.5°) = -\cos(22.5°)$

Hence the CHSH parameter becomes

$$S = E(a,b) - E(a,b') + E(a',b) + E(a',b')$$
$$S = \left[-\cos(22.5°)\right] - \left[-\cos(67.5°)\right] + \left[-\cos(22.5°)\right] + \left[-\cos(22.5°)\right]$$
$$S = -\cos(22.5°) + \cos(67.5°) - 2\cos(22.5°)$$
$$S = -3\cos(22.5°) + \cos(67.5°)$$

Numerically,

$$\cos(22.5°) \approx 0.9239 \quad , \quad \cos(67.5°) \approx 0.3827$$

So

$$S \approx -3 \times 0.9239 + 0.3827 = -2.7717 + 0.3827 = -2.3890$$

Therefore, $|S| \approx 2.389 > 2$, clearly violating the LHV bound.

## 4 Detecting eavesdropping via bell-violation

If Eve attempts to measure one photon of each entangled pair (for example, by intercepting Bob's photon before it reaches him), she necessarily disturbs the joint state:

① Collapse of entanglement

Eve's measurement projects Bob's photon (and thereby, via entanglement, Alice's photon) onto a product state. The resulting bipartite system no longer exhibits singlet-state correlations.

② Reduced chsh parameter

Post - eavesdropping, Alice and Bob's measurement outcomes satisfy local realism to a good approximation. Accordingly, any subsequent calculation of the CHSH parameter $S$ (over a sufficiently large sample of rounds) will satisfy $|S| \leq 2$.

③ Statistical test

Alice and Bob reserve a random subset of their joint measurement outcomes for parameter estimation.

They compute the sample correlations $E(a,b)$, $E(a,b')$, $E(a',b)$, $E(a',b')$ and then evaluate $S$.

If $|S| \approx 2.389$ (close to the ideal quantum value $2\sqrt{2}$), they conclude no eavesdropper is present.

If $|S| \leq 2$ (or even just below some security threshold, e. g., 2.3), they abort, concluding that Eve has measured or otherwise disturbed the entangled pairs.

Thus, the E91 protocol's security derives from a Bell-test: genuine entanglement (and hence secrecy) is certified by a statistically significant violation of the CHSH inequality.

## 5 Hybrid protocol integration

Real-world quantum networks often combine direct fiber links (suitable for BB84) with entanglement-swapping stations or quantum repeaters (where entangled E91-style links are most efficient across long distances). A hybrid protocol leverages the best features of both:

Table 1 Table of Comparing BB84 and E91 Protocols

| Aspect | BB84 (Short-Distance, Point-to-Point) | E91 (Long-Distance, Repeater-Assisted) |
|---|---|---|
| Use Case | Short-distance, directly connected nodes (e.g., within a metropolitan area) | Long-distance segments with repeaters |
| Protocol Mechanism | Standard BB84 protocol between adjacent nodes | Distributes entangled photon pairs; uses entanglement swapping at repeaters to extend link |
| Security Check | Compare subset of sifted bits to estimate QBER; *QBER* ≳ 25% indicates full-basis intercept-resend attack | Perform Bell tests, estimate CHSH parameter; $\|S\| \leq 2$ indicates compromised entanglement |
| Key Generation | Produces local secret key per link | Yields key via correlated measurement outcomes |
| Key Chaining | Linkwise one-time-pad encryption for trusted repeater chaining | Supports end-to-end entanglement swapping for direct key sharing without cleartext transmission |
| Security Check in Topology | QBER check for each BB84 segment | Bell-violation check for E91 segment |
| Key Combination | Partial keys combined into final secure key if all segments pass security checks | Partial keys combined via key-linking or entanglement swapping if all segments pass security checks |

Overall, as the Table 1 shows, although the BB84 protocol has some problems with transmission security, it is still a low-cost hybrid protocol solution for short distances and after the E91 protocol has completed the exchange. By hybridizing the BB84 and E91 protocols, one can tailor the QKD approach to each physical link, thereby maximizing overall key-rate, tolerable distance, and robustness against eavesdroppers.

## About the Author

* Corresponding Author : Deyong Huang, coolerxde@gt.ac.cn

## References

[1] Azuma, K., et al. Quantum repeaters: From quantum memories to the quantum internet. Nature Reviews Physics, 2023, 5(6):345-360.

[2] Chen, J., et al. Twin-field quantum key distribution with discrete-phase-randomized sources. Nature Communications, 2022, 13(1):1-10.

[3] Lu, H., et al. Metropolitan quantum network with entanglement distribution. Science Advances, 2022, 8(15), eabn7814.

[4] Pirandola, S., et al. Quantum communication networks: Challenges and opportunities. IEEE Communications Magazine, 2023, 61(4):28-34.

[5] Wehner, S., et al. Quantum internet: A vision for the road ahead. Science, 2023, 362(6412), eaam9288.

[6] Yin, J., et al. Entanglement-based secure quantum cryptography over 1,200 kilometres. Nature, 2021, 582(7813), 501-505.

[7] Le Roy-Deloison, T., Lobo, E. P., Pauwels, J., & Pironio, S. Device-independent quantum key distribution based on routed Bell tests. PRX Quantum, 2025, 6(2), 020311.

[8] Wang, W., Tamaki, K. & Curty, M. Measurement-device-independent quantum key distribution with leaky sources. Sci Rep 11, 1678 (2021).

[9] Humble, T. S., Sadlier, R. J., Williams, B. P., & Prout, R. C. Software-defined quantum network switching. In Disruptive Technologies in Information Sciences (Vol. 10652, 106520B). SPIE. (2018).

[10] Das, D., & Bandyopadhyay, S. Quantum communication using a quantum switch of quantum switches. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2022, 478(2260), 20220231.

[11] Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., & Voznak, M. Quantum key distribution: A networking perspective. ACM Computing Surveys, 2000, 53(5), Article 96.

[12] Tang, G. -Z., Sun, S. -H., & Li, C. -Y. Experimental point-to-multipoint plug-and-play measurement-device-independent quantum key distribution network. Chinese Physics Letters, 2019, 36(7), 070301.

[13] Peña, L. F., Koepke, J. C., Dycus, J. H. et al. Modeling Si/SiGe quantum dot variability induced by interface disorder reconstructed from multiperspective microscopy. npj Quantum Inf 10, 33 (2024).

[14] Stephanie Wehner et al. ,Quantum internet: A vision for the road ahead.Science362,eaam9288(2018).

[15] Chen, TY., Jiang, X., Tang, SB. et al. Implementation of a 46-node quantum metropolitan area network. npj Quantum Inf 7, 134 (2021).

[16] Feng, Q., Chu, S.-C., Pan, J.-S., Wu, J., & Pan, T.-S. Energy-efficient clustering mechanism of routing protocol for heterogeneous wireless sensor network based on bamboo forest growth optimizer. Entropy, 2022, 24(7), 980.