Nigerian Journal of Theoretical and Environmental Physics (NJTEP)
ISSN Print: 3026-9601
ISSN Online: 1597-9849
DOI: https://doi.org/10.62292/njtep.v4i3.2026.146
Volume 4(3), September 2026

Teleportation-Based Quantum Communication: A Comparative Review of Security Principles and Protocol Architectures

Olayinka Tosin Comfort and *Adewara Samuel Olayemi

Department of Computing, College of Science and Computing, Wellspring University, Benin City, Edo State, Nigeria.

*Corresponding author's email: upsuccess1@gmail.com
ORCID ID: https://orcid.org/0009-0001-1636-105X

Keywords:
Quantum Teleportation, Quantum Communication, Quantum Key Distribution, Quantum Secure Direct Communication, Quantum Networks.

ABSTRACT

Widely deployed public-key cryptography is vulnerable to sufficiently capable quantum computers, motivating post-quantum and quantum-cryptographic responses. This structured narrative review examines foundational theory and selected literature, drawing on a screening of 71 publications, of which 38 were retained and cited, principally from 2020 to 2025, to assess quantum teleportation within secure communication architectures. The analysis establishes that teleportation is an entanglement-assisted state-transfer primitive, not an autonomous source of security. It distinguishes conventional quantum key distribution (QKD) from teleportation-assisted QKD, separates entanglement swapping from payload teleportation, and compares teleportation-based quantum secure direct communication (QSDC) with repeater-supported networking. Recent experiments demonstrate capability expansion in high-dimensional states, logical code spaces, non-neighbouring network nodes, heterogeneous hardware interfaces, and coexistence with high-capacity classical fibre traffic. Deployment nevertheless remains constrained by loss, entanglement-generation rate, memory coherence, Bell-measurement efficiency, synchronisation, device trust, authentication, and cost. Teleportation can broaden quantum-network functionality, but confidentiality and authenticity depend on the complete protocol, threat model, verification procedures, and implementation assumptions.

INTRODUCTION

Secure digital infrastructures depend extensively on public-key cryptography, particularly Rivest-Shamir-Adleman (RSA) and elliptic-curve schemes. Efficient factorisation would defeat RSA, while elliptic-curve cryptography depends on the assumed classical hardness of the elliptic-curve discrete-logarithm problem. Shor (1994) established polynomial-time quantum algorithms for both problem classes. A practical attack would still demand a large, error-corrected quantum computer, and it remains unclear when, or with what resources, such machines will actually be built (Gidney & Ekerå, 2021; Roetteler et al., 2017). The security consequence is already relevant because encrypted traffic with a long confidentiality lifetime can be collected now and retained for decryption once quantum cryptanalytic capability arrives. This harvest-now, decrypt-later exposure, and the slow migration of cryptographic infrastructure, justify transition planning before a cryptographically relevant quantum computer exists (Chen et al., 2016; Kagai et al., 2025).

Two broad responses need to be kept apart. Post-quantum cryptography remains a classical cryptographic approach and derives computational security from mathematical problems believed to be intractable for both classical and quantum adversaries. Quantum cryptographic protocols instead exploit the preparation, transmission and measurement of quantum states; some protocols use distributed entanglement, while security is inferred from observed statistics within a specified adversarial and device model. Under explicit protocol and implementation assumptions, quantum key distribution (QKD) can generate keys with quantified information-theoretic security. The full claim still has to account for authentication, finite-key statistics, classical post-processing, device behaviour and implementation side

channels (Lo et al., 2014; Pirandola et al., 2020). QKD does not eliminate classical cryptography: its public classical communication must be authenticated, although it need not ordinarily be confidential. QKD-derived keys are subsequently supplied to classical applications, where user data are typically protected using symmetric encryption or authenticated encryption.

Quantum teleportation is a tool that transfers quantum states across a network using pre-shared entanglement. As Bennett et al. (1993) first demonstrated, moving an unknown quantum state requires a sender to perform a local Bell-state measurement and transmit two classical bits, allowing the receiver to apply a precise hardware correction. Because the physical input system never actually travels through the channel, the protocol remains completely dependent on prior entanglement distribution and classical communication networks. Teleportation, then, neither enables superluminal communication nor replaces communication infrastructure.

It also needs separating from related quantum-network operations. Without teleporting an independent input state, the Ekert 1991 (E91) protocol uses entangled correlations for key generation and eavesdropping detection (Ekert, 1991), whereas the original Bennett-Brassard 1984 (BB84) protocol operates as a prepare-and-measure protocol that requires neither Bell-state reconstruction nor pre-shared entanglement (Bennett & Brassard, 1984). Meanwhile, shorter links are connected via entanglement swapping to establish entanglement over longer distances. Payload teleportation transfers an independent state using an established entangled link (Żukowski et al., 1993). Quantum repeaters extend quantum connectivity through operations such as entanglement generation, storage and swapping. These operations support applications including teleportation and entanglement-based QKD without making the functions identical (Briegel et al., 1998; Sangouard et al., 2011).

Foundations, security, protocols, experiments, and network engineering are the key areas spanned by quantum-communication research. That breadth complicates comparison across differing metrics and assumptions. This review examines whether properties attributed to teleportation instead arise from verification, QKD post-processing, entanglement tests, authentication, or device and channel models. An earlier Nigerian contribution presented quantum teleportation through Einstein-Podolsky-Rosen (EPR) entanglement, qubits, elementary quantum gates, Bell states and the conventional teleportation circuit (Olayinka & Olayinka, 2014). That work provides a relevant local point of departure. The present review extends the analysis by separating the state-transfer primitive from protocol-level security, network architecture and implementation assumptions.

This paper takes up this gap as it characterises teleportation as an infrastructure-dependent primitive, comparing three principal settings: teleportation-assisted QKD, teleportation-based quantum secure direct communication (QSDC), and repeater-supported multi-hop state transfer. The review also explores these subjects in detail by systematically analysing key advancements from 2020 to 2025 such as multi-particle teleportation milestones, classical-quantum fibre coexistence, novel coding and error-management proposals and application-level network integration. The article does not report original experiments or simulations. Its contribution is an analytical framework for determining where teleportation adds functional value, where it does not alter the source of security, and which physical and operational constraints govern scalability.

Review Scope and Approach

Thirty-eight (38) publications were ultimately retained and cited in this review out of seventy-one (71) initially identified and screened. The remaining thirty-three (33) papers were set aside as duplicates, off-topic studies, or because stronger and more directly relevant sources were available. This literature pool was gathered between November 2025 and March 2026 from English-language searches run across IEEE Xplore, Google Scholar, arXiv, and Web of Science using combinations of 'quantum teleportation', 'cryptography', and 'post-quantum RSA'. Instead of employing a formal systematic review or meta-analysis, this study utilises a structured narrative review design. Inclusion criteria required peer-reviewed studies and verifiable archival sources (including standards, technical reports, and preprints) that directly address teleportation-based or teleportation-adjacent secure quantum communication. Literature between 2020 and 2025 was the primary publication window required for the selected literature, for which each source also had to provide enough experimental or methodological rigour to allow for a direct comparison. Despite these limits, earlier foundational works were still included where necessary for security or theoretical grounding. Conversely, exclusion criteria removed studies confined to abstract teleportation theory with no cryptographic or communication connection, as well as sources lacking verifiable bibliographic detail. The analysis classified the literature by foundational theory, security model, protocol architecture, experimental validation, and hybrid classical-quantum integration. It compared studies by mechanism, threat model, fidelity or key-rate implications, resource demand, maturity, and scalability, while identifying recurrent limitations to integrate findings into a common conceptual account. Though traceable, the procedure is not exhaustive, utilising no PRISMA flow process, fixed universal search string, formal risk-of-bias instrument, or statistical aggregation. Consequently, the conclusions remain interpretive and

apply strictly to the selected evidence rather than to every publication in the field.

MATERIALS AND METHODS

Classical and Quantum Security Foundations

Classical cryptosystems have different quantum vulnerabilities. Grover's algorithm gives a quadratic acceleration for generic key search, so suitable symmetric-key lengths can retain a substantial security margin. Remaining purely computational, post-quantum cryptography includes lattice-, code-, hash-, and multivariate-based constructions, whereas Shor's algorithm poses a direct threat to RSA and elliptic-curve cryptography by efficiently solving factorisation and discrete-logarithm problems. QKD instead exploits incompatible measurements, disturbance and, in some protocols, quantum correlations. Its security follows from the complete protocol and implementation model, not merely from a quantum channel (Lo et al., 2014; Pirandola et al., 2020).

At the quantum-state level, a pure qubit is a normalised state in a two-dimensional Hilbert space:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

Where α and β are complex amplitudes satisfying $|\alpha|^2 + |\beta|^2 = 1$. Relative amplitudes and phase determine interference, while measurement produces an outcome in the selected basis. Mutually unbiased bases are central to BB84-type QKD because measuring a state in the other basis produces unpredictable outcomes (Bennett & Brassard, 1984).

Figure 1 locates a pure single-qubit state by polar angle θ and azimuthal angle φ.

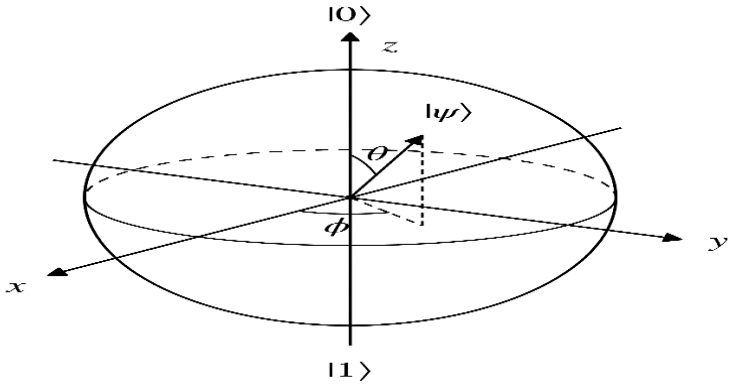

Figure 1: Bloch-sphere geometry of a pure single-qubit state

Figure 2 relates the computational Z basis to the mutually unbiased X and Y bases.

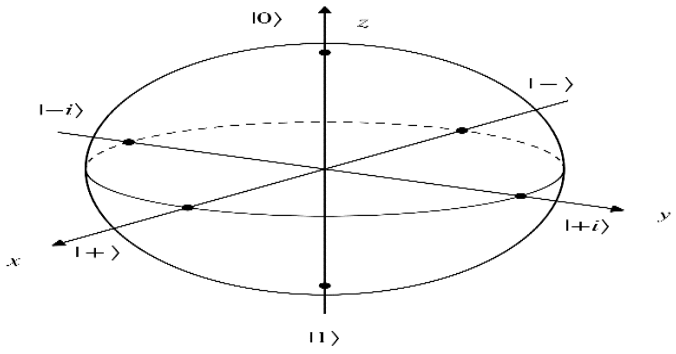

Figure 2: Computational and mutually unbiased basis states on the Bloch sphere

Entanglement is the non-separability of a composite quantum state. A maximally entangled Bell state is

$$|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \quad (2)$$

Measurements in corresponding bases produce correlated outcomes, but local statistics cannot transmit information superluminally. A maximally entangled pure pair also cannot share entanglement with a third system, a restriction relevant to some security arguments (Horodecki et al., 2009). Entanglement nevertheless has protocol-specific roles: standard BB84 requires no physical distribution of entangled pairs, although entanglement-based representations may be used in its security proof (Pirandola et al., 2020; Shor & Preskill, 2000).

Figure 3 presents the entangled resource shared before teleportation.

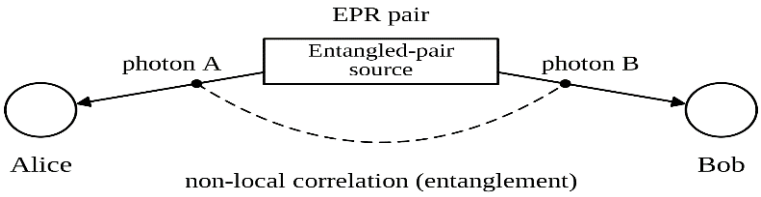

Figure 3: Entangled EPR photon pair shared by Alice and Bob

Securing a positive secret key in practical QKD requires finite-key analysis, error-correction leakage considerations, and privacy amplification to sufficiently bound adversarial knowledge (Tomamichel et al., 2012). This process relies on quantities like quantum bit error rate (QBER) to support statistical parameter estimation. While the underlying quantum security is anchored by the no-cloning theorem, which forbids perfect universal copying of arbitrary unknown quantum states to stop adversaries from copying and forwarding undisturbed signals (Wootters & Zurek, 1982). It leaves vulnerabilities open. Specifically, the theorem does not prevent attacks directed at detectors, sources, authentication, or post-processing stages. No single quantum principle guarantees implementation security.

Quantum Teleportation Mechanism

For teleportation, Alice holds an unknown input state

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad (3)$$

And shares an entangled pair with Bob. She performs a Bell-basis measurement and sends its two-bit result to Bob, who applies the corresponding Pauli correction. Ideally, his qubit then acquires $|\psi\rangle$. Teleportation therefore requires shared entanglement, classical feed-forward and conditional correction, while respecting no-cloning because the input state is destroyed rather than duplicated (Bennett et al., 1993). A comparable circuit-level treatment was presented by Olayinka and Olayinka (2014), who described the shared Bell-state resource, Alice's local gate operations, measurement of the sender-side qubits and Bob's outcome-dependent recovery operation.

Figure 4 condenses the operation into entanglement distribution, Bell-state measurement, classical communication, and receiver correction.

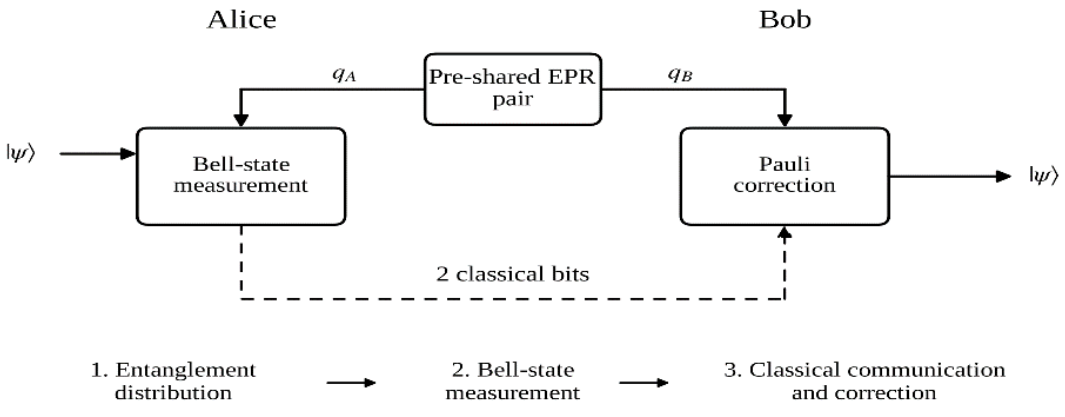

Figure 4: Operational stages of quantum teleportation

Table 1 lists the receiver correction associated with each Bell-state outcome.

Table 1: Bell-State Measurement Outcomes and Receiver Correction Operations

Bell-state outcome	Bob's corrective operation
$\|\Phi^+\rangle$	Identity operation, I
$\|\Phi^-\rangle$	Pauli-Z operation, Z
$\|\Psi^+\rangle$	Pauli-X operation, X
$\|\Psi^-\rangle$	Combined XZ operation (equivalent up to global phase)

The classical message does not contain a complete classical description of $|\psi\rangle$; two classical bits only identify the required correction. Teleportation therefore cannot transmit useful information without the classical channel and cannot operate before entanglement distribution. These requirements prevent superluminal communication and establish the main architectural trade-off: direct transmission of the payload carrier is replaced by advance distribution of an entangled resource plus classical coordination. The replacement can be valuable in distributed quantum processing or segmented networks, but it creates demands for entanglement generation, storage, verification, timing, and control.

Teleportation-Based Communication Architectures

Quantum Key Distribution and Teleportation-assisted QKD

Alice prepares states in randomly selected bases, and Bob measures in independently selected bases to begin the prepare-and-measure BB84 protocol (Bennett & Brassard, 1984; Lo et al., 2014). The subsequent steps require them to sift compatible events, estimate errors, reconcile their keys, and apply privacy amplification. This sequence serves as the authenticated classical post-processing through which QKD converts correlated quantum-measurement data into a shared secret key. Standard BB84 requires no independent unknown input state, pre-shared EPR pair, Bell-state measurement or teleportation-style Pauli correction. E91 instead uses measurements of distributed entangled pairs for key generation and Bell-type security testing but does not reconstruct an independent payload state at Bob (Ekert, 1991). Entanglement-based QKD is therefore not inherently teleportation-based.

Figure 5 records the ordinary BB84 sequence and separates quantum transmission from authenticated classical post-processing.

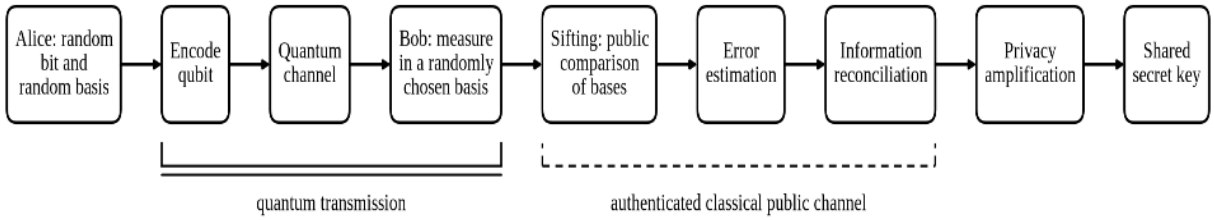

Figure 5: BB84 quantum key distribution sequence

Teleportation-assisted QKD is a narrower hybrid category. In this review, the term denotes a protocol in which an independent, protocol-relevant quantum state is operationally teleported using an entangled resource whose quality and trust assumptions are specified. Such designs typically add Bell-state measurement, classical feed-forward, conditional correction and entanglement management to conventional QKD operations. Ahammed and Kadir (2024), for example, propose a simulated entanglement- and teleportation-assisted scheme incorporating quantum Fourier transform (QFT) operations and report higher key-rate metrics than their selected BB84 benchmarks. This model-specific result neither redefines BB84 nor establishes a general teleportation advantage.

Security still arises from the complete protocol and proof. Classical authentication, device assumptions, parameter estimation, finite-key statistics, reconciliation leakage and privacy amplification remain necessary. Altering how a quantum state is transferred via teleportation fails to eliminate side-channel attacks, certify the entangled resource, or authenticate users on its own. Even advanced device-independent and measurement-device-independent methods, which reduce particular trust assumptions, must retain authenticated communication and secure post-processing (Lo et al., 2014; Portmann & Renner, 2022).

BB84 highlights this ongoing dependence through its operational pipeline: sifting isolates compatible-basis events, parameter estimation bounds errors and

adversarial knowledge, reconciliation fixes disagreements at the cost of leaked information, privacy amplification destroys residual knowledge, and authentication blocks impersonation. A teleportation-assisted variant must preserve these functions or justify replacements through its own proof. Its additional entanglement, measurement and feed-forward components also introduce assumptions and failure modes that require explicit modelling.

Quantum Secure Direct Communication

QSDC transmits confidential messages directly through a quantum protocol rather than first generating a key for subsequent encryption (Deng & Long, 2004). Some schemes explicitly use teleportation. In this review, that designation is reserved for protocols in which an independent message-bearing state is consumed in a Bell-basis measurement and reconstructed at the receiver after classical feed-forward and conditional correction. Entanglement, dense coding or Bell measurements alone do not constitute teleportation (Cao & Song, 2006).

Teleportation does not independently secure QSDC. A complete protocol must authenticate participants and classical control messages, test the relevant quantum resource, detect interception or substitution and address implementation leakage. Teleportation-based designs additionally require suitable entanglement, reliable Bell-state measurement and feed-forward; some also require quantum memory. QSDC can reduce key management associated with payload encryption, but authentication remains necessary. Although QSDC has progressed from theoretical proposals to experimental and network-oriented studies, its deployment and standardisation remain less developed than those of QKD (Pan et al., 2024; Zhang et al., 2017).

Entanglement Swapping, Repeaters, and Multi-Hop State Transfer

Loss and operational noise limit direct long-distance entanglement distribution. Entanglement swapping combines shorter links: if A-B and C-D are entangled, a Bell-state measurement on B and C can conditionally entangle A and D, with any required correction applied or tracked classically (Żukowski et al., 1993). No independent payload state need be teleported; the immediate output is an extended entangled resource.

A repeater network may generate and store elementary-link entanglement, extend it through swapping and then use the end-to-end pair for teleportation or entanglement-based QKD. Alternatively, a state may be teleported sequentially between adjacent nodes. These architectures differ in memory, synchronisation, measurement, correction and trust requirements. Quantum repeaters comprise several designs that may use heralded entanglement generation, memories, swapping, purification, multiplexing, quantum error correction or encoded transmission (Briegel et al., 1998; Muralidharan et al., 2016; Sangouard et al., 2011).

In this review, repeater-assisted QKD denotes key distribution supported by a repeater network, whereas teleportation-assisted QKD additionally requires reconstruction of an independent protocol-relevant input. Distributing entanglement for E91 measurements is not by itself payload teleportation.

Repeater generations manage errors differently. First-generation designs rely on heralding and purification and are constrained by two-way signalling and memory coherence. Second- and third-generation designs introduce quantum error correction, reducing some waiting penalties while increasing gate, qubit and fault-tolerance requirements. Multiplexing can raise link-success rates but requires multiple modes and control capable of matching successful resources. Meaningful comparison must therefore report node trust, memory access, loss, operations and error propagation, not distance alone.

Security Properties and Implementation Boundaries

Measurement disturbance, no-cloning and entanglement monogamy constrain adversaries but do not constitute complete security protocols. Their use requires specified statistics, thresholds, finite-size treatment, threat models, device assumptions, authentication and a composable security criterion. No-cloning prevents universal perfect copying but does not eliminate source, detector, side-channel or impersonation attacks. Entanglement tests likewise require quantitative treatment of imperfect states and measurements (Horodecki et al., 2009; Lo et al., 2014; Portmann & Renner, 2022).

Classical communication has protocol-specific roles. Teleportation conveys the joint-measurement outcome needed for correction; QKD coordinates sifting, parameter estimation, reconciliation and privacy amplification; repeater networks use it for heralding, memories, swapping and routing. These messages generally require authentication and integrity, not secrecy. Without authentication, an adversary can impersonate the endpoints. Altered teleportation outcomes or repeater-control records may corrupt operations or cause denial of service. Endpoint control logic, credentials and post-processing therefore remain within the trust or verification boundary.

Operational labels should follow the task. Although these operations may coexist, they are not interchangeable:

BB84 prepares and measures states in incompatible bases; E91 measures distributed entanglement for key generation and testing; swapping establishes remote entanglement; teleportation reconstructs an independent input state; and repeaters extend quantum connectivity across segmented links.

Teleportation reports should identify the input, entangled resource, joint measurement, classical result, correction and success criterion. Producing only remote entanglement is distribution or swapping, whereas correlated measurements yielding key material constitute entanglement-based QKD. Precise terminology prevents demonstrations from inheriting security or scalability claims that were not tested.

Advances from 2020 to 2025

Moving increasingly beyond demonstrations of elementary single-qubit teleportation, work published from 2020 to 2025 expanded into logical encoding, complex states, heterogeneous hardware interfaces, multi-node operation, and coexistence with conventional telecommunications traffic. These diverse advancements do not fit into a single linear scale of maturity. Rather, they represent independent efforts utilising different success criteria, resource assumptions, state encodings, physical platforms, and solutions to distinct bottlenecks. Experimental evidence must therefore be separated from simulation, theoretical protocol design and application-oriented review. Within the reviewed literature, five advances are especially well supported: high-dimensional state teleportation, transfer into logical code spaces, teleportation between non-neighbouring network nodes, interfaces between dissimilar quantum hardware, and coexistence with high-capacity classical fibre traffic. At the architectural level, this period also reinforced the view that teleportation cannot be treated as an isolated endpoint operation. It requires an entangled resource, a suitable joint measurement, classical communication of the result and an outcome-dependent receiver operation. Network deployment consequently requires coordination between quantum resources and classical control rather than the addition of a teleportation device to an otherwise unchanged classical network (Cacciapuoti et al., 2020).

High-Dimensional and Complex-State Teleportation

Hu et al. (2020) experimentally demonstrated teleportation of three-dimensional quantum states using the spatial mode of a photon within a six-photon system. Two auxiliary entangled photons were employed to implement a three-dimensional Bell-state measurement, and the reconstructed process was shown to be non-classical and genuinely three-dimensional. The significance of this result lies in the expansion of teleportation beyond two-level qubit states. Higher-dimensional systems provide a larger state space and may become relevant where network or computational tasks require the transfer of more complex quantum information.

The result should not, however, be interpreted as a demonstration of a scalable high-dimensional network. It was a controlled optical experiment involving demanding state preparation, interference and multiphoton detection. It did not establish a sustained transmission rate, multi-user routing method, field-deployed channel or practical resource advantage over qubit-based alternatives. Its demonstrated contribution is therefore the experimental feasibility of genuine three-dimensional teleportation, not the operational maturity of high-dimensional quantum networking.

Logical Encoding and Fault-Tolerant Interfaces

Luo et al. (2021) addressed a different problem by experimentally teleporting quantum information from a physical qubit into an error-correctable logical qubit. The authors first created an entangled resource linking a physical qubit and a logically encoded qubit and then used that resource to transfer the physical-qubit information into the logical code space. They reported teleportation fidelities of up to 0.786 and presented the scheme as a step towards teleportation-based quantum error correction and scalable quantum information processing.

This result is important because future quantum systems will need interfaces between physical information carriers and encoded logical states. It also illustrates the use of teleportation as a computational operation rather than only as a communications mechanism. While the authors stated that the scheme could be designed to become fully fault tolerant, they did not claim that full fault tolerance had already been achieved; nevertheless, the experiment itself did not demonstrate a complete repeater architecture, fault-tolerant end-to-end communication, or wide-area networking. Luo et al. should therefore be classified as evidence of logical-code integration, not as a field demonstration of quantum-network interoperability.

Teleportation between Non-Neighbouring Network Nodes

A more direct network advance was reported by Hermans et al. (2022), who demonstrated qubit teleportation between non-neighbouring nodes in a three-node solid-state quantum network. The nodes used nitrogen-vacancy (NV) centres in diamond and were connected through

optical links. Entanglement was first generated across the two elementary links, after which a Bell-state measurement at the intermediate node swapped the entanglement to the outer nodes. The resulting end-to-end entangled state was stored in a memory qubit before an independently prepared input state was teleported between the outer nodes.

The experiment achieved an average teleportation fidelity of 0.702(11), exceeding the classical limit of 2/3, at an experimental rate of approximately one accepted event per 117 seconds. It therefore demonstrated the complete distinction between entanglement swapping and payload teleportation: swapping first created the remote resource, and a later Bell-state measurement transferred the independently prepared input state.

This was a genuine step beyond directly connected endpoint demonstrations because the communicating nodes did not share a direct quantum link. It remains, however, a three-node laboratory network rather than a routed metropolitan or wide-area service. The low event rate, memory requirements, heralding process, local-gate errors and specialised hardware show why successful multi-node teleportation does not by itself establish scalable network operation.

Heterogeneous Interfaces and Memory-Compatible States

Iuliano et al. (2024) demonstrated teleportation between physically dissimilar quantum systems. Their interface connected a 795-nm photonic time-bin qubit, chosen to be compatible with established thulium- and rubidium-based quantum-memory wavelengths, to the spin qubit of a diamond NV centre. Two-stage low-noise quantum-frequency conversion and waveform shaping were used to match the temporal and spectral properties of the incoming photon to those of the photon emitted by the solid-state node. A Bell-state measurement and real-time feed-forward completed the teleportation, with fidelity above the classical bound.

The advance here is interoperability rather than distance. Practical quantum networks are unlikely to use one physical platform for every function. Photons are suited to transmission, while matter systems may provide processing or storage, but these systems can operate at different wavelengths, bandwidths and timescales. Teleportation can serve as an interface once sufficient indistinguishability, conversion efficiency and feed-forward control are achieved.

The experiment was nevertheless a proof of concept. The input wavelength was compatible with specified quantum memories, but the work did not demonstrate storage in those memories, multi-hop routing between heterogeneous nodes or long-term operation across a deployed network. Its verified contribution is the transfer of a photonic time-bin qubit into a solid-state spin node through a frequency-converted interface.

Coexistence with Classical Telecommunications Traffic

Thomas et al. (2024) addressed a deployment constraint by demonstrating teleportation over 30.2 km of optical fibre carrying a 400-Gbit s−1 C-band classical communications signal. The Bell-state measurement was performed at the midpoint of the quantum links. Because strong classical traffic produces spontaneous Raman-scattering noise across neighbouring spectral regions, the experiment used O-band quantum channels, narrow spectral and temporal filtering and multiphoton coincidence detection to preserve teleportation fidelity under the tested launch-power conditions.

This result is significant because it demonstrates that teleportation need not always require fibre reserved exclusively for quantum signals. It moves the engineering question from basic physical possibility towards coexistence with high-capacity telecommunications infrastructure. It also shows that coexistence depends on the complete optical configuration, including wavelength allocation, launch power, channel spacing, filtering, detector timing and coincidence criteria.

The result remains configuration specific. It did not establish that arbitrary production fibres, amplifiers, traffic loads or wavelength plans can support the same performance. Nor did it remove the underlying constraints of attenuation, probabilistic photon generation, detector efficiency, Bell-state-measurement success and entanglement rate. It provides strong evidence of carefully engineered quantum-classical coexistence, not a universal operating distance or commercially qualified service.

Coding, Protocol Control and Application-oriented Expansion

Alongside these experimental advances, theoretical and simulation studies broadened the functions attached to teleportation. Cane et al. (2020) investigated a model in which turbo coding was applied to classical and quantum components of a teleportation system operating over imperfect channels. Their numerical results indicated improved reliability and easier detection of the specified eavesdropping condition under the adopted coding and noise models. The work did not show that turbo coding independently provides cryptographic security or eliminates the need for a complete threat model.

Ahammed & Kadir (2024) proposed an entanglement- and teleportation-assisted QKD architecture incorporating QFT operations. Their simulations reported improved QBER, reconciliation and secure-key-rate metrics relative to the selected BB84 benchmarks. These outcomes belong to the authors' channel, attack and implementation model and do not demonstrate a general advantage over standard BB84 or supply an experimental or composable security proof.

The 2025 literature in the reviewed set continued this protocol-level expansion but did not add an equivalent field-scale experimental milestone. Taufiqi et al. (2025) proposed a theoretical encrypted controlled-teleportation protocol and assessed it against a specified "steal-away" attack. Mehrinezhad Chobari et al. (2025) proposed circuits for generating and teleporting three- and four-particle W states and validated them through Qiskit simulation; the latter remained an arXiv preprint rather than a physical implementation. These studies expand the space of controlled and multipartite designs, but their results should not be placed at the same maturity level as the experiments of Hu, Luo, Hermans, Iuliano or Thomas.

Application-oriented reviews also widened the discussion beyond general-purpose networking. Paudel et al. (2023), for example, examined possible quantum-communication applications in energy systems, including secure smart-grid data transmission, infrastructure monitoring and sensing. Such work identifies sector-specific requirements and possible use cases rather than demonstrating operational teleportation in an energy network. Timing, reliability, compatibility with legacy control systems, photonic-device performance and network-management requirements remain unresolved deployment questions.

RESULTS AND DISCUSSION

Fidelity, QBER, secret-key rate, message rate, entanglement-generation rate, and distance cannot be ranked on a single scale because they measure fundamentally different tasks. Therefore, a meaningful comparison is only possible within like-for-like categories. To maintain this distinction, prepare-and-measure QKD must be evaluated for key establishment, while teleportation-assisted QKD is treated as a specialised hybrid serving that same goal. These are fundamentally separate from QSDC, which transmits confidential message content directly, and multi-hop teleportation or repeater-assisted networking, which extends entanglement or quantum-state transfer.

Comparison Criteria

This review compares architectures by their objective, security basis, operational mechanism, appropriate performance metrics, resource requirements, evidence level and scalability. Security analysis asks what is protected, against which adversary, under which device and trust assumptions, and through which verification, authentication and post-processing steps. Performance must match the task: teleportation fidelity and success probability assess state reconstruction; QBER and secret-key rate assess QKD; and entanglement rate, memory lifetime, latency and throughput assess network-resource distribution.

Six analytical levels are separated. The physical level covers states, channels, loss, noise, coherence and devices. The primitive level distinguishes entanglement generation, measurement, swapping, teleportation and correction. The protocol level identifies the task, such as key establishment, direct messaging or processor interconnection. The security level specifies the threat model, trust assumptions, authentication and proof. The network level covers routing, memory scheduling, synchronisation and interoperability. The evidence level distinguishes theory, simulation, laboratory demonstration, field trial and operational service. Teleportation is a primitive; its usefulness and security depend on the protocol and architecture in which it operates.

Table 2 synthesises the reviewed distinctions among prepare-and-measure QKD, teleportation-assisted QKD, teleportation-based QSDC, and repeater-assisted networking, drawing on established QKD security analyses, the selected hybrid-QKD proposal, QSDC reviews, and quantum-repeater architectures (Ahammed & Kadir, 2024; Lo et al., 2014; Muralidharan et al., 2016; Pan et al., 2024; Sangouard et al., 2011).

Table 2: Comparison of Selected Quantum-Communication Architectures

Architecture	Objective and security basis	Appropriate metrics and evidence	Additional resources and present status
Prepare-and-measure QKD	Establishes a shared key. Security follows from the complete QKD protocol and proof under stated device and adversarial assumptions.	QBER, secret-key rate, finite-key parameters, distance and availability. Extensive theoretical, experimental and field evidence exists.	Quantum-state source, channel, detector, authenticated classical communication, reconciliation and privacy amplification. Standard BB84 requires no shared entanglement or Bell-state measurement.
Teleportation-assisted QKD	Establishes a key while using teleportation as an explicit state-transfer stage. Security still follows from the complete QKD protocol.	QBER and secret-key rate, together with teleportation fidelity or success probability where relevant. Evidence is mainly scheme-specific proposal and simulation.	Entangled resource, joint Bell measurement, feed-forward and conditional correction in addition to ordinary QKD processing.
Teleportation-based QSDC	Transfers confidential message content directly. Security follows from the complete QSDC construction, channel tests and authentication assumptions.	Message error or transmission rate, security parameters, fidelity and success probability. Evidence remains protocol- and platform-dependent.	Message encoding, entanglement, joint measurement and correction where teleportation is genuinely used; some designs also require quantum memory.
Multi-hop or repeater-assisted networking	Extends entanglement or state transfer across segmented links. The endpoint application determines the security objective.	End-to-end entanglement rate and fidelity, link success, memory lifetime, latency, throughput and, for QKD, secret-key rate.	Entanglement generation, repeater nodes, memories, swapping, scheduling and architecture-dependent purification or quantum error correction.

Note: The rows represent different tasks. Study-specific performance values are not generalised into universal category ranges.

Interpretation of the Comparison

Teleportation-assisted QKD retains the objective of key establishment. Teleportation changes how a protocol-relevant quantum state is transferred but does not independently provide authentication, parameter estimation, reconciliation, privacy amplification or device security. Relative to prepare-and-measure BB84, the additional operations may support specialised network designs but increase resource and coordination requirements. Ahammed and Kadir (2024) report favourable QBER, reconciliation and secure-key-rate results for their simulated QFT-based construction, but those results remain conditional on the selected model and benchmarks; they do not establish a general advantage for teleportation-assisted QKD.

Teleportation-based QSDC has a different objective because it seeks direct recovery of confidential message content. This does not remove the need for authentication, quantum-resource testing or leakage analysis. QSDC has progressed through theoretical and experimental work, but its protocols, performance measures and network assumptions remain heterogeneous. Pan et al. (2024) document both experimental advances and unresolved challenges in extending QSDC towards networked operation; the evidence therefore supports continuing development rather than a single standardised long-distance service model.

Multi-hop teleportation and quantum repeaters address network reach rather than supplying a security protocol by themselves. Their performance and cost depend on link quality, memory and swapping behaviour, error management and classical coordination; shorter elementary links may improve individual-link success, but additional hops introduce more control and failure points. Because repeater architectures manage loss and operational errors in different ways, their rates and resource costs are not represented by one universal distance figure.

The principal comparative conclusion is that security and scalability are system properties. QKD security follows from a defined key-distribution protocol and proof; QSDC security follows from the complete direct-communication construction; and repeater-assisted

security depends on link verification, node trust, error management and end-to-end composition. Teleportation may be one component of any of these architectures, but entanglement and Bell-state measurement alone do not establish confidentiality or authenticity.

Performance claims require the same discipline. Teleportation fidelity measures agreement between an intended input state and its reconstructed output; it is not a secret-key rate, message throughput or security proof. A high-fidelity transfer may coexist with unauthenticated control messages or device leakage, while conventional QKD may establish a secure key without teleporting an unknown state. Distance is likewise ambiguous unless identified as direct fibre length, total network span, elementary-link length, free-space range or number of repeater segments. Defensible comparison must therefore report the task, state, distributed resources, heralding method, classical exchanges, trust assumptions and proved security claim.

Practical Implications, Limitations and Research Priorities

Advances expand state dimensionality, logical encoding, topology, heterogeneous interfaces and classical-traffic coexistence without uniform maturity. Near-term deployment should use teleportation selectively in hybrid classical-quantum networks, retain classical infrastructure for authentication, orchestration, error management and most traffic, and add quantum links where QKD, state transfer, sensing or processor interconnection offers measurable advantage without presuming infrastructure replacement.

Engineering priorities follow from the limitations observed across the reviewed experiments. Entanglement sources require higher generation rates, indistinguishability, stability and integration. Quantum memories require longer coherence, efficient writing and retrieval, multimode capacity and compatibility with photonic interfaces. Bell-state measurements require improved efficiency, detector performance and tolerance of imperfect interference. Multiplexing, purification and quantum error correction should be evaluated by their effect on end-to-end rate and resource cost, rather than by fidelity improvement alone. To prevent stored states from losing coherence, a series of complex operations must be synchronised by network controllers (Hermans et al., 2022; Iuliano et al., 2024; Muralidharan et al., 2016). These tasks include routing, feed-forward mechanisms, and failure recovery. They also require the real-time management of memory allocation, entanglement swapping, and probabilistic entanglement generation. Repeater studies confirm that reduced signalling delay or improved rate generally requires greater local gate fidelity, qubit resources or fault-tolerance capability.

Security proofs must match implementations by specifying adversarial models, trusted nodes and devices, randomness, authentication, finite-size treatment, leakage and composability. Teleportation analysis must cover entangled-resource provenance and quality, joint measurement, classical outcome and correction; QKD or QSDC guarantees cannot be attributed to teleportation. Device-independent and measurement-device-independent methods reduce device-trust assumptions but retain authenticated classical communication and demanding rate, detection and implementation requirements (Lo et al., 2014; Portmann & Renner, 2022; Xu et al., 2020).

Standardisation should define interfaces and security for teleportation, entanglement swapping, repeater control and QKD. QKD-network standards address authentication, integrity, access control, node protection and control-plane security, but do not secure architectures outside their scope (International Telecommunication Union [ITU], 2020, 2024).

Application, economic and operational evaluations should be service-specific and task-matched: telecommunications, energy, defence and distributed computing differ in latency, availability, distance, and confidentiality lifetime and trusted-node tolerance. Reports should cover input/output states, fidelity, teleportation and entanglement-generation rates, classical overhead, memory time, latency, failure handling and security assumptions; fibre tests should report launch power, wavelength, filtering, traffic and margins, and satellite studies atmospheric, availability, orbital and ground-segment data. Costs should cover acquisition, integration, maintenance and secure lifecycle support for quantum hardware and control software, plus classical authentication, control, key management, monitoring and orchestration. Evidence maturity must remain explicit: simulations are not sustained operation; Thomas et al. show configuration-specific coexistence, while energy studies remain application-oriented (Paudel et al., 2023; Thomas et al., 2024). Baselines are direct transmission or repeaters for state transfer, conventional or trusted-node QKD for key establishment and post-quantum cryptography for classical communications; rate, reliability, security and operational burden must justify the architecture.

This narrative review is neither exhaustive nor systematic; it used no meta-analysis, PRISMA selection process, risk-of-bias instrument or reproducible database search. Theoretical, simulation, review, laboratory, field-coexistence and preprint evidence cannot be pooled

without equating unlike tasks, platforms and evidence levels; conclusions identify patterns and attribution boundaries rather than universal performance ranges or architectural prevalence.

Future research should address three linked questions. First, which combinations of sources, memories, interfaces and repeater operations can deliver useful end-to-end rates under realistic loss, device efficiency, coherence and classical-control delay? Second, how can composable security be maintained across entanglement generation, swapping, teleportation and endpoint applications without unexamined trust at intermediate nodes? Third, which hybrid architectures demonstrate an operational advantage over task-matched alternatives after hardware, classical control, security and maintenance costs are included? Answering these questions requires common benchmarks, interoperable testbeds, transparent threat models and experiments that measure complete service performance rather than isolated component fidelity.

The near-term research problem is therefore not whether teleportation can be demonstrated, but when it provides a verified service advantage under realistic resource, security and operational constraints.

CONCLUSION

Distributed quantum processing, multi-node state transfer, and specialised QKD and QSDC designs can all be supported by quantum teleportation, which transfers an unknown quantum state to a remote system. This transfer process is achieved through the combined use of shared entanglement, a joint Bell-state measurement, classical feed-forward, and conditional correction. Teleportation does not by itself authenticate participants, certify the entangled resource, protect classical-control integrity or eliminate device and side-channel attacks. It is therefore an infrastructure-dependent state-transfer primitive, not an autonomous source of security.

The review establishes corresponding operational boundaries. Prepare-and-measure BB84 and entanglement-based E91 generate keys without teleporting an independent input state. Entanglement swapping establishes longer-distance entanglement, whereas payload teleportation reconstructs a separately supplied state. Quantum repeaters extend quantum connectivity through architecture-dependent combinations of entanglement generation, memories, swapping, purification or error correction. These operations may coexist, but their security, performance and maturity must be assessed at the level of the complete protocol and threat model.

Although coding, control, and sector-specific designs were broadened by theoretical, simulated, and application-oriented studies, they do not carry the same evidential weight as physical demonstrations. This experimental progress was clearly visible from 2020 to 2025, during which physical demonstrations expanded teleportation across five dimensions: coexistence with high-capacity classical fibre traffic, heterogeneous hardware interfaces, non-neighbouring network nodes, logical code spaces, and high-dimensional states. Collectively, the literature shows controlled capability expansion rather than uniform commercial readiness.

Teleportation's future value will therefore depend on whether verified state transfer can deliver a measurable service advantage under realistic constraints involving loss, entanglement rate, memory coherence, Bell-measurement efficiency, synchronisation, trust, interoperability and cost. The central analytical conclusion is that teleportation may enable secure communication architectures, but security and scalability remain properties of the complete system in which it is embedded.

REFERENCES

Ahammed, M. F., & Kadir, M. I. (2024). Entanglement and teleportation in quantum key distribution for secure wireless systems. IET Quantum Communication, 5(4), 551–566. https://doi.org/10.1049/qtc2.12092

Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. Theoretical Computer Science 560, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

Bennett, C. H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters, 70(13), 1895–1899. https://doi.org/10.1103/PhysRevLett.70.1895

Briegel, H.-J., Dür, W., Cirac, J. I., & Zoller, P. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. Physical Review Letters, 81(26), 5932–5935. https://doi.org/10.1103/PhysRevLett.81.5932

Cacciapuoti, A. S., Caleffi, M., Van Meter, R., & Hanzo, L. (2020). When entanglement meets classical communications: Quantum teleportation for the quantum internet. IEEE Transactions on Communications, 68(6), 3808–3833. https://doi.org/10.1109/TCOMM.2020.2978071

Cane, R., Xie, W., & Ng, S. X. (2020). Turbo-coded secure and reliable quantum teleportation. IET Quantum Communication, 1(1), 16–21. https://doi.org/10.1049/iet-qtc.2020.0004

Cao, H.-J., & Song, H.-S. (2006). Quantum secure direct communication scheme using a W state and teleportation. Physica Scripta, 74(5), 572–575. https://doi.org/10.1088/0031-8949/74/5/015

Chen, L., Jordan, S. P., Liu, Y.-K., Moody, D., Peralta, R. C., Perlner, R. A., & Smith-Tone, D. C. (2016). Report on post-quantum cryptography. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Deng, F.-G., & Long, G. L. (2004). Secure direct communication with a quantum one-time pad. Physical Review A, 69(5), 052319. https://doi.org/10.1103/PhysRevA.69.052319

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433. https://doi.org/10.22331/q-2021-04-15-433

Hermans, S. L. N., Pompili, M., Beukers, H. K. C., Baier, S., Borregaard, J., & Hanson, R. (2022). Qubit teleportation between non-neighbouring nodes in a quantum network. Nature, 605, 663–668. https://doi.org/10.1038/s41586-022-04697-y

Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). Quantum entanglement. Reviews of Modern Physics, 81(2), 865–942. https://doi.org/10.1103/RevModPhys.81.865

Hu, X.-M., Zhang, C., Liu, B.-H., Cai, Y., Ye, X.-J., Guo, Y., Xing, W.-B., Huang, C.-X., Huang, Y.-F., Li, C.-F., & Guo, G.-C. (2020). Experimental high-dimensional quantum teleportation. Physical Review Letters, 125(23), 230501. https://doi.org/10.1103/PhysRevLett.125.230501

International Telecommunication Union [ITU]. (2020). Security framework for quantum key distribution networks. In ITU-T Recommendation X.1710. International Telecommunication Union. https://handle.itu.int/11.1002/1000/14452

International Telecommunication Union [ITU]. (2024). Security requirements and measures for quantum key distribution network – Control and management. In ITU-T Recommendation X.1717. International Telecommunication Union. https://handle.itu.int/11.1002/1000/16169

Iuliano, M., Slater, M.-C., Stolk, A. J., Weaver, M. J., Chakraborty, T., Loukiantchenko, E., do Amaral, G. C., Alfasi, N., Sholkina, M. O., Tittel, W., & Hanson, R. (2024). Qubit teleportation between a memory-compatible photonic time-bin qubit and a solid-state quantum network node. Npj Quantum Information, 10, 107. https://doi.org/10.1038/s41534-024-00910-0

Kagai, F., Branch, P., But, J., & Allen, R. (2025). Harvest-now, decrypt-later: A temporal cybersecurity risk in the quantum transition. Telecom, 6(4), 100. https://doi.org/10.3390/telecom6040100

Lo, H.-K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, 8(8), 595–604. https://doi.org/10.1038/nphoton.2014.149

Luo, Y.-H., Chen, M.-C., Erhard, M., Zhong, H.-S., Wu, D., Tang, H.-Y., Zhao, Q., Wang, X.-L., Fujii, K., Li, L., Liu, N.-L., Nemoto, K., Munro, W. J., Lu, C.-Y., Zeilinger, A., & Pan, J.-W. (2021). Quantum teleportation of physical qubits into logical code-spaces. Proceedings of the National Academy of Sciences, 118(36), e2026250118. https://doi.org/10.1073/pnas.2026250118

Mehrinezhad Chobari, S. A., Aghababa, H., & Kolahdouz, M. (2025). Generation and teleportation of three and four-particle W states. In arXiv. https://doi.org/10.48550/arXiv.2501.18743

Muralidharan, S., Li, L., Kim, J., Lütkenhaus, N., Lukin, M. D., & Jiang, L. (2016). Optimal architectures for long distance quantum communication. Scientific Reports, 6, 20463. https://doi.org/10.1038/srep20463

Olayinka, T. C., & Olayinka, A. S. (2014). Quantum teleportation: An alternative means to transportation. Journal of the Nigerian Association of Mathematical Physics, 27, 251–256.

Pan, D., Long, G.-L., Yin, L., Sheng, Y.-B., Ruan, D., Ng, S. X., Lu, J., & Hanzo, L. (2024). The evolution of quantum secure direct communication: On the road to the Qinternet. IEEE Communications Surveys & Tutorials, 26(3), 1898–1949. https://doi.org/10.1109/COMST.2024.3367535

Paudel, H. P., Crawford, S. E., Lee, Y.-L., Shugayev, R. A., Leuenberger, M. N., Syamlal, M., Ohodnicki, P. R., Lu, P., Mollot, D., & Duan, Y. (2023). Quantum

communication networks for energy applications: Review and perspective. Advanced Quantum Technologies, 6(10), 2300096. https://doi.org/10.1002/qute.202300096

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502

Portmann, C., & Renner, R. (2022). Security in quantum cryptography. Reviews of Modern Physics, 94(2), 025008. https://doi.org/10.1103/RevModPhys.94.025008

Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. In Advances in Cryptology – ASIACRYPT 2017 (Vol. 10625, pp. 241–270). Springer International Publishing. https://doi.org/10.1007/978-3-319-70697-9_9

Sangouard, N., Simon, C., de Riedmatten, H., & Gisin, N. (2011). Quantum repeaters based on atomic ensembles and linear optics. Reviews of Modern Physics, 83(1), 33–80. https://doi.org/10.1103/RevModPhys.83.33

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124–134. https://doi.org/10.1109/SFCS.1994.365700

Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters, 85(2), 441–444. https://doi.org/10.1103/PhysRevLett.85.441

Taufiqi, M., Purwanto, A., Subagyo, B. A., Sukamto, H., & Yuwana, L. (2025). Encrypted quantum controlled teleportation protocol. International Journal of Theoretical Physics, 64, 110. https://doi.org/10.1007/s10773-025-05973-z

Thomas, J. M., Yeh, F. I., Chen, J. H., Mambretti, J. J., Kohlert, S. J., Kanter, G. S., & Kumar, P. (2024). Quantum teleportation coexisting with classical communications in optical fiber. Optica, 11(12), 1700–1707. https://doi.org/10.1364/OPTICA.540362

Tomamichel, M., Lim, C. C. W., Gisin, N., & Renner, R. (2012). Tight finite-key analysis for quantum cryptography. Nature Communications, 3, 634. https://doi.org/10.1038/ncomms1631

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. Nature, 299(5886), 802–803. https://doi.org/10.1038/299802a0

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., & Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), 025002. https://doi.org/10.1103/RevModPhys.92.025002

Zhang, W., Ding, D.-S., Sheng, Y.-B., Zhou, L., Shi, B.-S., & Guo, G.-C. (2017). Quantum secure direct communication with quantum memory. Physical Review Letters, 118(22), 220501. https://doi.org/10.1103/PhysRevLett.118.220501

Żukowski, M., Zeilinger, A., Horne, M. A., & Ekert, A. K. (1993). "Event-ready-detectors" Bell experiment via entanglement swapping. Physical Review Letters, 71(26), 4287–4290. https://doi.org/10.1103/PhysRevLett.71.4287