NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub
CyberSystem Journal Research Article

Exploring the Techniques and Challenges of Privacy-Preserving Data Sharing in Quantum-Enabled Networks

Zaid Ibrahim Rasool[1]*, Nisreen Saad Hadi[2]

[1] Department of Studies and Planning, University of Babylon, Hillah 51002, Iraq

[2] Department of Administrative and Financial Affairs, University of Babylon, Hillah 51002, Iraq

* Corresponding Author: **Zaid Ibrahim Rasool**, Email: Zaid.ibrahim.rasool@uobabylon.edu.iq.

Abstract: Privacy-preserving data-sharing mechanisms traditionally rely on data anonymization techniques, which aim to dissociate individual records from their corresponding data subjects in order to transform sensitive information into a form that minimizes the risk of re-identification. In parallel, trust-broker models have emerged as an additional layer of protection, whereby authorized data providers disclose controlled contact information that enables potential data users to request access under predefined conditions determined by the data owner. In contemporary data-sharing environments, cryptography remains a fundamental pillar for ensuring confidentiality and integrity during data exchange. Cryptographic protection typically involves two operations: an encryption process, in which the sender transforms plaintext into ciphertext that is unintelligible to unauthorized entities, and a decryption process, in which only the intended recipient restores the ciphertext to its original form. Both operations rely on a cryptographic algorithm paired with one or more secret keys. Symmetric-key cryptography employs a single shared key for both encryption and decryption. In contrast, asymmetric cryptography uses a mathematically linked pair of keys, where one key is used for encryption and the other for decryption. When the encryption key is publicly available while the corresponding decryption key remains private, only the legitimate recipient holding the private key is capable of recovering the plaintext. This cryptographic structure forms the basis for securing data confidentiality against unauthorized access in both classical and quantum-aware communication systems.

Access this article online

Keywords: Healthcare, Privacy-Preserving data, Quantum-Enabled networks

1. Introduction

THE rapid progress in quantum technologies has intensified global concerns regarding data privacy, prompting a reevaluation of existing security practices and threat models. Traditional cryptographic techniques—long relied upon as the foundation of privacy in digital communications—now face significant challenges in the quantum era. Cryptographic schemes whose security depends on classical computational hardness assumptions are particularly vulnerable, as quantum algorithms may render several of these assumptions obsolete. Moreover, the advanced computational and sensing capabilities enabled by quantum principles introduce new risks to the confidentiality and integrity of shared data.

In this context, it becomes essential to examine the emerging techniques and associated challenges of privacy-preserving data sharing within quantum-enabled networks

Received July 10, 2025; Revised August 02, 2025; Accepted September 10, 2025; Published December 31, 2025
https://doi.org/10.57238/csj.2025.1009

(QENs). These networks, developed as a natural evolution of quantum technologies, integrate quantum information processing, quantum storage, and quantum communication with classical networking infrastructures. Such hybrid architectures enable forms of data exchange that surpass the performance and security guarantees of classical optical communication systems [1]. However, they also necessitate renewed consideration of privacy requirements and potential vulnerabilities.

Ensuring privacy in QENs is closely tied to the notions of trust, confidentiality, and data integrity. When two parties exchange information over a quantum-enabled channel, the transmitted data may contain sensitive or personally identifiable information that must remain inaccessible to unauthorized entities. The receiving party must also be confident that the data has not been intercepted, modified, or manipulated during transmission. Consequently, theoretical and practical investigations into QEN security emphasize protecting shared data from adversarial interference, including threats originating from independent nodes or semi-trusted intermediaries [2].

These evolving dynamics highlight the need for systematic analysis and the development of robust privacy-preserving mechanisms capable of addressing the emerging risks brought forth by quantum technologies.

2. Foundations of Privacy-Preserving Data Sharing

Growing concerns over data privacy and security have intensified with the widespread integration of networked devices and interconnected systems in the digital era. As data flows expand across diverse platforms and infrastructures, the limitations of conventional encryption-based protections have become increasingly apparent. In parallel, emerging quantum technologies offer new capabilities for secure communication, yet they also introduce additional layers of complexity that necessitate careful examination. The objective of this section is to outline the fundamental concepts underpinning privacy-preserving data sharing and to provide a structured context for evaluating the advantages and limitations of quantum-based approaches relative to classical methods [3].

Privacy-preserving data sharing refers to a broad set of methodologies designed to enable the exchange, processing, or utilization of data while preventing unauthorized access or disclosure of sensitive information. With the digitalization of previously isolated systems, a wide array of devices, sensors, and environments now collect and transmit data autonomously. This interconnectedness motivates providers and users to share data for analytics, service optimization, and decision-making. Consequently, multiple privacy-preserving strategies have been developed to support both static datasets, which remain fixed after collection, and dynamic datasets, which evolve continuously over time.

These strategies form the foundation for modern privacy-centric architectures and serve as the basis for comparing traditional, post-quantum, and quantum-native mechanisms throughout the remainder of this paper.

2.1 Overview of Privacy-Preserving Techniques

Data sharing in classical telecommunication networks has long been used to optimize resource utilization and enhance the quality of service. However, granting broad access to shared data introduces significant privacy risks, including unauthorized use of sensitive personal information and the loss of data ownership. These concerns become more pronounced in next-generation quantum-enabled networks (QENs), where classical and quantum data coexist across interconnected nodes equipped with advanced quantum capabilities. In such environments, the development of robust privacy-preserving models and mechanisms is essential. These mechanisms must ensure confidentiality, integrity, and secure processing while still enabling service providers to extract analytical value from shared datasets [4].

A variety of classical techniques form the foundation for privacy-preserving data sharing. Among the most prominent are differential privacy (DP), homomorphic encryption (HE), and secure multi-party computation (MPC). Each of these techniques aims to prevent unauthorized disclosure of sensitive information during data processing or exchange among entities within telecommunication infrastructures. Their applicability, however, is often constrained by computational overhead, scalability challenges, and assumptions regarding the trustworthiness of participating entities.

Traditional centralized and decentralized data-sharing models also introduce distinct risks. Centralized systems may expose users to a loss of control over the storage and use of their data, particularly when disputes arise between users and service providers. Conversely, decentralized approaches may enable participants to infer sensitive behavioral profiles—such as personal habits, fears, or predispositions—based on shared data attributes [5]. Such profiling capabilities intensify the need for rigorous privacy safeguards.

A variety of methodological approaches have been proposed to mitigate these risks. For example, synthetic data

generation, combined with privacy-preserving post-processing, can limit the exposure of real user data. Despite their promise, these techniques face inherent challenges, including limited oversight over data access pathways, incomplete visibility into training datasets, and the difficulty of enforcing uniform privacy guarantees across heterogeneous systems. Consequently, achieving strong privacy protection requires designing privacy-preserving mechanisms ex-ante, embedding safeguards by default rather than relying solely on post-hoc mitigation strategies [6].

A comparative overview of the most prominent privacy-preserving data-sharing techniques in quantum-enabled networks, along with their strengths and limitations is summarized in Table 1.

2.2 Cryptography Fundamentals

Cryptography represents the foundational mechanism for privacy-preserving data sharing, ensuring confidentiality, integrity, and authenticity of data during storage and transmission. Cryptographic systems rely on well-defined algorithms and protocols that transform readable information into a protected form that cannot be interpreted by unauthorized parties. In its basic form, a cryptographic algorithm consists of two interdependent procedures: encryption and decryption. During encryption, plaintext is converted into ciphertext using an encryption key, whereas decryption restores the original plaintext using a corresponding decryption key.

Modern cryptographic frameworks include additional primitives to support authentication and integrity verification. For example, digital signature schemes allow a user to sign a message using a private signing key, producing a non-repudiable signature that can be verified using a publicly available key. These signatures act as unique, non-reusable fingerprints that bind the message to its originator, preventing adversaries from forging information or tampering with transmitted data [6]. The combination of encryption and digital signatures enables robust protection against unauthorized access, message alteration, and impersonation.

Cryptographic algorithms are critical in both classical and quantum-aware networking contexts. Numerous algorithms and hybrid combinations define the structure of secure systems, ranging from symmetric-key encryption to public-key infrastructures. Historically, classical cryptography faced threats primarily from brute-force attacks or advances in computational power. This motivated the adoption of enhanced features such as key wrapping, perfect forward secrecy, and clear separation between encryption keys and underlying data.

In distributed and remote data-access environments, interactive cryptographic protocols are essential for enabling privacy-preserving computation. Techniques such as Secure Multi-Party Computation (SMPC) allow multiple parties to collaboratively compute a function over their inputs without revealing those inputs to one another. Homomorphic encryption (HE) extends this capability by allowing certain computations to be performed directly on encrypted data. Similarly, Private Set Intersection (PSI) enables parties to compute the intersection of their datasets without disclosing any additional information.

These mechanisms are widely used in privacy-preserving data sharing and access control. For instance, Advanced Multi-Party Computation (AMPC) can support secure data aggregation in quantum-enhanced environments, allowing data owners to contribute encrypted information and receive results in encrypted form without exposing their raw data. In personalized recommendation scenarios, Client-to-Server (C2S) protocols—leveraging PSI—allow service providers to compute recommendations from encrypted user profiles without accessing the underlying sensitive attributes [7].

However, the emergence of quantum computing presents new challenges to the security guarantees of many classical cryptographic protocols. Studies indicate that widespread SMPC and PSI constructions may become vulnerable to quantum adversaries capable of exploiting quantum algorithms to break underlying hardness assumptions. Consequently, the long-term resilience of cryptographic protocols used in secure remote data access must be re-evaluated in anticipation of increasingly practical quantum attacks. Ensuring sustained privacy preservation in this environment requires the integration of post-quantum cryptographic primitives and quantum-resistant protocol designs.

2.3 Quantum Computing Basics

Quantum computing represents a fundamentally new computational paradigm that differs markedly from classical computing architectures. Instead of relying on binary bits that assume values of 0 or 1, quantum computers operate on quantum bits (qubits), which exist within a substantially richer state space. This expanded computational capability arises from two core quantum mechanical principles: superposition and entanglement. Superposition enables a qubit to occupy multiple states simultaneously, thereby allowing quantum processors to explore a vast number of computational configurations in parallel [8].

Table 1. Privacy-preserving data sharing in quantum-enabled networks

Technique / Approach	Short description	Strengths (privacy/security)	Main challenges / limitations
Quantum Key Distribution (QKD)	Uses quantum states to establish symmetric keys with information-theoretic security.	Provable eavesdropper detection; forward secrecy.	Distance limits, need for trusted nodes/repeaters, hardware cost, integration with classical systems.
Hybrid QKD + Classical Encryption	Combine QKD for key material and classical crypto for data transport.	Practical: leverages mature classical protocols while improving key security.	Key management complexity, deployment cost, latency for key refresh.
Post-Quantum Cryptography (PQC) integration	Use quantum-resistant algorithms to protect classical channels in quantum networks.	Protects data against future quantum attacks; easy to deploy in existing stacks.	Some PQC schemes have large keys/ciphers; not information-theoretic; standardization tradeoffs.
Quantum Secure Direct Communication (QSDC)	Send confidential messages directly via quantum channels without separate key distribution.	Potential for direct quantum-level confidentiality.	Mostly theoretical/limited experiments; fragile to loss/noise; low throughput.
Blind Quantum Computation (BQC)	Client delegates quantum computation to a quantum server while keeping data/input/state secret.	Strong privacy for delegated quantum tasks; server learns almost nothing.	Requires advanced quantum resources (client/server), fault tolerance, complex protocols.
Quantum Homomorphic Encryption (QHE) (theoretical)	Perform computations on encrypted quantum states without decryption.	Ultimate privacy for quantum data processing if practical.	Currently mostly theoretical or extremely resource-intensive; deep research gap.
Differential Privacy (DP) adapted to quantum data	Inject controlled randomness when releasing aggregate results from quantum measurements.	Formal privacy bounds for statistical queries; composability.	Defining DP for quantum observables is nontrivial; utility vs. privacy tradeoffs; measurement constraints.
Secure Multi-Party Computation (MPC) + Quantum resources	Parties jointly compute functions; quantum channels or primitives can improve efficiency or security.	Avoids central trust; can protect inputs across parties.	Protocol design complexity; communication overhead; need for synchronization and quantum-capable participants.
Federated Learning with quantum clients / quantum data	Train models across many nodes holding quantum or classical data without centralizing raw data.	Minimizes data exposure; scalable model training.	Aggregation poisoning, model inversion risks, quantum-classical model heterogeneity.
Quantum Authentication & MACs	Authenticate quantum messages/states to detect tampering.	Protects integrity of quantum communications.	Implementing robust quantum authentication is hard; needs extra qubits/overhead.
Trusted node / hardware-based privacy (quantum repeaters, secure enclaves)	Use trusted intermediate nodes or secure hardware to relay/store data.	Extends reach of quantum links; practical in near term.	Introduces trust assumptions; single points of failure; supply-chain risk.
Policy, Access Control & Auditing for quantum networks	Classical/quantum-aware policies and logging that govern who may access/share data.	Provides governance and compliance; reduces misuse.	Standardization lacking; auditing quantum processes is novel and complex.

Entanglement, in turn, establishes strong correlations between qubits, such that the state of one qubit instantaneously influences the state of another—regardless of the physical distance separating them. This property accelerates complex simulations and enhances the computational efficiency of certain problem classes [9].

Given these characteristics, quantum computing is poised to transform numerous application domains, including materials engineering, finance, pharmaceuticals, logistics, and artificial intelligence. However, this transformative potential also extends to cybersecurity. Many widely used cryptographic schemes rely on classical hardness assumptions—such as integer factorization and

discrete logarithms—that can be efficiently solved by quantum algorithms. A notable example is Shor's algorithm, which poses a direct threat to RSA and other public-key encryption systems.

This anticipated vulnerability has accelerated global efforts to design quantum-safe cryptographic standards capable of withstanding attacks from fault-tolerant quantum computers. Regulatory bodies and international organizations have emphasized the urgency of developing and deploying such standards. For example, the European Commission has highlighted the necessity of quantum-resilient solutions, and the NIS directive has identified priority areas where new protections must be introduced to safeguard data-intensive digital ecosystems [10]. As modern societies increasingly depend on large-scale data exchange and interconnected services, transitioning to secure, quantum-resistant infrastructures have become an essential strategic objective [11].

3. Quantum-Enabled Networks

Our world has entered a complex, interconnected, and networked age dominated by the fast, efficient, and intelligent transmission of information. In traditional networks, whether utilizing a star, bus, tree, or mesh topology, confidential information is easy to access. Therefore, there is a need for privacy-preserving data interaction and communication methods. Quantum-enabled networks based on quantum communication and quantum computing technologies can potentially provide a new secure method for quantum data interaction. They require the deployment of quantum memory, quantum repeater, and quantum router devices in quantum communication networks. Currently, however, it is very difficult to develop these devices in practice. In the short-term, quantum routing in quantum key distribution networks, combining software-defined networking and quantum communication technologies, can deliver an innovative secure method for network architecture [12]. Executing this network transformation involves deploying a quantum key distribution system and a software-controller in optical networks [13]. Additionally, a Quantum handshake protocol enables a secret exchange of private information between nodes and the controller. To protect the transmission of quantum messages, two stratagems are proposed to protect the controller, as well as independent-cycle scheduling in the quantum key distribution network and in the software-defined network, respectively. Furthermore, research on path computation and verification mechanisms consents the development of a practical quantum secure communication network function with good compatibility between quantum and classical networks [14]. Current experimental results illustrate that the proposed combined networking technology can operate sophisticated quantum communication tasks, delivering a bright future of quantum-enabled secure networking.

Quantum-enabled networks are a new generation type of intelligent internet architecture with innovative capabilities including superdense coding, scalable authentication, high-capacity secure communication, optimal flooding, and quantum error-correcting code 7. Quantum communication, quantum networking and technologies are three interdependent developments needed for quantum-enabled networks. Quantum-enabled networks have brought a stimulating evolution to the current communication networks. Security is always paramount for network operability [15]. In contrast to classical locked boxes, however, the privacy of quantum data interaction is guaranteed by the laws of physics because any eavesdropping behavior destroys the quantum state. Therefore, the "spooky action at a distance" of quantum entanglement can be utilized to create a shared key between two remote parties, constantly monitoring the privacy of the data throughout its lifetime or other potential security mechanisms. Supersecure carrying a payload is encrypted by its "spooky action at a distance" entanglement partners [16]. When these systems are disentangled or the eavesdropper attacks the quantum channel, the systems are mapped into a verifiable non-local box physical scenario. As the final protection, the non-local power is implemented. The powerful Arbitrary Nonlocal Boxes interacting with the model systems in the information plane signify the safe carrying of the secret payload. What prisoners regard as their "private conversations" using the hidden super-record method are further meaningfully encrypted in the superdense coding boxes and only delivered by the legitimate channels.

3.1 Quantum Key Distribution (QKD)

The theoretical security foundations and practical implementations of QKD have been extensively analyzed in the literature [17, 18].

The practical deployment challenges associated with privacy-preserving data sharing in quantum-enabled networks, including scalability, hardware cost, and integration issues, are outlined in Table 2.

Quantum Key Distribution (QKD) is a groundbreaking approach in enabling secure communication within quantum-enabled networks. This new encryption technique uses the principles of quantum mechanics to distribute a secret key between two parties,

Table 2. Practical deployment challenges in quantum-enabled privacy-preserving data sharing

Challenge	Description	Impact on Privacy & Performance	Possible Mitigation Strategies
Quantum channel noise & decoherence	Quantum states easily degrade due to environmental interference and photon loss.	Reduces reliability of quantum key generation and increases error rates; possible privacy leaks through repeated retransmissions.	Use quantum error correction, entanglement purification, and shorter link distances.
Distance and scalability limits	Quantum entanglement decays over long distances; direct QKD limited to ~100–300 km without repeaters.	Restricts large-scale deployment; weakens end-to-end confidentiality.	Deploy quantum repeaters, satellite-based QKD, and hybrid optical-fiber + free-space channels.
Integration with classical networks	Quantum and classical layers require synchronization and interface standards.	Delays communication and key updates; potential mismatch causes security loopholes.	Develop unified hybrid protocols (e.g., QKD-TLS), cross-layer optimization, and standard APIs.
Key and identity management	Managing millions of session keys and verifying quantum identities is complex.	Increases chance of key reuse or mis-association, lowering overall privacy.	Quantum-enhanced Public Key Infrastructure (PKI), blockchain-based identity frameworks.
Hardware cost & maintenance	Quantum sources, detectors, and repeaters are expensive and fragile.	Limits scalability to research labs and high-security institutions only.	Hardware miniaturization, integrated photonics, government/industry cost sharing.
Standardization gaps	Lack of universal standards for quantum network interoperability.	Causes vendor lock-in and compatibility issues; weakens global privacy guarantees.	Participate in ITU-T, ETSI, and ISO standardization; adopt open APIs.
Trust in intermediate nodes	Trusted nodes or quantum repeaters can become single points of compromise.	Privacy depends on physical trust assumptions, undermining end-to-end confidentiality.	Use entanglement swapping with verification, distributed trust, and post-quantum digital signatures.
Authentication of quantum states	Verifying sender identity and message integrity in quantum form is complex.	Susceptible to impersonation or tampering if not authenticated.	Apply quantum message authentication codes (QMACs) or hybrid quantum-classical authentication.
Quantum resource management	Scheduling qubit usage, memory, and channels in large networks is challenging.	May create congestion and timing leaks affecting privacy guarantees.	Adaptive routing, dynamic resource allocation, software-defined quantum networking (SDQN).
Legal, ethical, and policy uncertainty	Privacy laws and data-sharing regulations are not yet adapted for quantum data.	Ambiguity over compliance and liability; hinders adoption.	Develop quantum-aware privacy policies; engage in policy research and standard compliance frameworks.
Energy and environmental overhead	Cryogenic systems and optical amplifiers require high power.	Increases operational cost and sustainability concerns.	Research low-power quantum components and energy-efficient network design.
Human expertise shortage	Limited specialists capable of maintaining quantum infrastructure securely.	Slows adoption; increases risk of misconfiguration and accidental data leaks.	Invest in education, training programs, and simulation-based management tools.

Alice and Bob 8. The secret key is then deployed to encrypt and decrypt classical messages, which can be transmitted via unsecured classical channels. In case an eavesdropper (Eve) tries to compromise the key using classical techniques, the quantum properties of the transmitted signal will reveal the eavesdropping activity. Therefore, QKD promises secure communication against any attack. Several QKD protocols have been proposed, such as the first, famous implementation and other more recent ones. Even though all QKD protocols are based on different principles, they share the same operational mechanics. Additionally, they offer security guarantees under the same assumptions about the devices used in the network. This led to the rapid development of several QKD devices and a number of experiments that confirmed the hypothesis of security under the given assumptions [18].

One of the main advantages of QKD is that its security relies on the laws of quantum mechanics, which is devoid of any assumption against an all-powerful adversary. This contrasts with all the other methods traditionally used to distribute a cryptographic key. Moreover, a further notable feature of quantum mechanics is that it is not possible to make a measurement without disturbing the system. This is the feature that guarantees the possibility for a QKD protocol of revealing the presence of an eavesdropper. This is extremely important since, in the context of privacy-preserving data sharing, the key shared by the users represents the foundation of the protocol to securely exchange the sensitive information. The experimental success of QKD has fostered the design of more efficient devices and the increase in the allowed distances between the parties involved. However, QKD devices are still far from being embeddable in low-cost, embedded consumer devices, a fundamental requirement for the implementation of large, scalable, secure quantum networks. This motivates the research for alternative methodologies to ensure security in the exchange of a cryptographic key in the quantum case. Recent advances in secure quantum key distribution further confirm the feasibility of deploying privacy-preserving mechanisms at scale [18].

3.2 Quantum Secure Direct Communication (QSDC)

Soon after the birth of quantum key distribution (QKD), quantum secure direct communication (QSDC) quickly emerged as a secure communication scheme. The first QSDC protocol was proposed onward the rules of QKD. The working principle is that two remote parties communicate with each other without any need of key distribution. The sender, Alice, encodes the secret message into a sequence of quantum states and then sends them to the receiver, Bob, through a quantum channel. The secret message is then decoded by Bob thanks to usable entanglement resources distributed beforehand by Charlie, who does not know, and cannot know, the secret message. Moreover, any eavesdropper, Eve, attempting to extract the secret message by interacting with the transmission from Alice to Bob via this quantum channel will not get anything because she could not generate the final entanglement between Alice and Bob. Comparison with usual methods, both the very final direct transmission and the security are sharper. Although QKD was first proposed, the realization of QKD is much earlier than that of QSDC. In fact, as of 2023, numerous QSDC protocols and their variations have been proposed, investigated and further developed, leading to various technological advances.

Matsumoto and Shimizu were the first proposed a point-to-point QSDC protocol, one of the most popular types of QSDC protocols, in the ideal quantum systems. Since then, extensive research has been devoted to this revolutionary concept. A summary of several representative difference types of QSDC protocols or their variants is presented. In general, QSDC can be divided into two broad categories: QSDC with quantum memory and QSDC without quantum memory. QSDC with quantum memory needs to prepare entangled and/or Bell states, which are stored in the quantum memory and then manipulated later only when necessary, and such states can be prepared or distributed by the user after the broadcast scheme. QSDC without quantum memory relies on the quantum states prepared right before the transmission and then measures them properly so that the secret message can be directly decoded. There are four types of QSDC protocols defined as Bell state measurement, entanglement swap, controlled qubit teleportation, and single qubit teleportation. QSDC is the direct communication of secret information, and typically performed in a point-to-point fashion [19]. This is a distinct approach relative to QKD, which uses quantum channels to establish shared information used in point-to-point and many-to-many communication. On the other hand, the basic secret transmission units are different - QKD generates the shared key to encrypt the message, whereas QSDC directly sends the secret message. As a result, QSDC offers the possibility of secure conference call functionality that is not provided by QKD. To implement various QSDC protocols on different quantum systems, a review of the QSDC experimental realization on the realistic quantum systems is presented.

3.3 Quantum Teleportation

Quantum teleportation is a fundamentally unique process in the domain of quantum communication. Unlike

classical transfer methods, it allows the quantum state of one particle to be transmitted with high fidelity to another particle, without the physical transmission of the particles themselves. It employs entanglement, a type of far-reaching quantum correlation, as a resource to perform a "teleportation" of the state of one particle held by a sender to another particle possessed by a distant receiver 10. Once the final measurement outcome is sent through a classical information channel, the receiver can apply a local quantum operation on his particle to reconstruct the input state. In a nutshell, quantum teleportation enables the transfer of quantum information by exploiting quantum entanglement and classical communication of measurement outcomes.

At first glance, privacy and quantum teleportation might sound like an odd combination of terms. After all, teleportation of information from one place to another, possibly even across a hostile transfer channel, does not seem like the most private of activities. Nevertheless, quantum teleportation brings possibilities to enhance the privacy of shared data. Imagine two parties, Alice and Bob. Both suspects that their mutual friend Charley has secretly gained possession of some gossip about them. Unfortunately, neither of the two can bear to mention their suspicions to the other. Discussing it openly would betray their own secrets. Instead, they compare notes on their mutual silence and, in the end, conclude that Charley must have shared gossip about them using quantum teleportation. This analogy between classical private statistics and quantum teleportation illustrates the potential for it vastly complicating the hidden communication of the illicit. Of course, in the real world, there are easier ways to secretly share information with friends than via quantum teleportation, most of which are significantly more reliable and refutable in court [20]. However, this imaginary narrative goes some way to illustrating the key distinction between classical private statistics and the entanglement and quantum state tomography required to hide hidden quantum resources. Moreover, with the suggestion that well-conducted quantum teleportation could be tough to spot, we have a fantastic plot for numerous murder mysteries set in the realm of practical quantum information theory and beyond. And that's always worth considering. Since its first inception in 1993, quantum teleportation has proven to be one of the most recognizable, sensational and implementable concepts to come from quantum information science. This subsection details the basic principles of quantum teleportation. It also addresses protocol variants and experiments showing the first teleportation of entanglement between two particles of light. Practical implementations of quantum teleportation are reviewed with a view to their technical advantages and drawbacks. Finally, open challenges and prospective future teleportation technologies are discussed, such as its application to in the development of secure quantum key distribution in quantum networks.

4. Privacy-Preserving Data Sharing in Quantum-Enabled Networks

Table 3 presents a high-level classification of privacy-preserving techniques in quantum-enabled networks, highlighting their core mechanisms, benefits, limitations, and key research insights.

The emergent field of quantum technologies has brought hope for solving tasks impossible by merely classical means for years to come. Until now, secure communication over global distances has been challenged for end-user access networks, where broadband data sharing is prevalent and privacy concerns are increasing. On the one hand, commercial interests motivate data retention and analytic yield, while on the other hand restrictive regulation requests anonymization and data minimization avoiding re-identification. In the meanwhile, progress in quantum tech renders user data easily accessible at network nodes, and a clash of interests arises.

In light of the above, the question of privacy-preserving data sharing arises. This field involves a concept of data that can be used for analysis while avoiding recognizing the person the data originated from, which ties together the user needs and the regulative requirements in a consistent fashion. This paper sheds light on the subject, and in doing so covers techniques and challenges arising from the context of quantum-enabled networks.

This tutorial exposes the topic of privacy-preserving data sharing in quantum-enabled networks. A comprehensive and lucid discussion covering both the 'quantum' and the 'privacy' grounds, is provided with the aid of recent up-to-date references. It draws attention to the design trade-offs between the potential benefits of quantum networks and the privacy threats. Scalars of user recognition, data obfuscation, the trade-off of accuracy compliant data and an efficient anonymization are addressed and new challenges arising due to evolving security demands are highlighted 1. In delineating problem fundamentals, considerations on facets crucial to conception of privacy-centric protocols are at hand 11, such as user requirements and regulatory frameworks, shaping the analysis of the current state of the art methods.

Table 3. Privacy-preserving data sharing in quantum-enabled networks

Category / Technique	Key idea / mechanism	Main benefits	Limitations / challenges	Research insights / findings
Quantum Key Distribution (QKD)	Uses quantum states for secret key exchange with eavesdropper detection.	Information-theoretic security, proven confidentiality.	Limited distance, costly hardware, trusted relay dependency.	Best suited for short-distance high-security links; hybrid QKD-PQC systems emerging.
Quantum Secure Direct Communication (QSDC)	Sends confidential messages directly through quantum channels.	No need for pre-shared keys, direct confidentiality.	Low data rates, fragile to noise and loss.	Promising for ultra-secure low-bandwidth applications.
Post-Quantum Cryptography (PQC)	Classical cryptography resistant to quantum attacks.	Scalable, compatible with classical networks.	Large keys/signatures, not unconditionally secure.	Effective transitional measure until full quantum infrastructure matures.
Blind Quantum Computation (BQC)	Client outsources quantum computation without revealing data.	Strong data privacy in delegated computing.	Requires high-level quantum devices and protocols.	Provides foundation for secure quantum cloud computing.
Quantum Homomorphic Encryption (QHE)	Perform operations on encrypted quantum data.	Full data confidentiality during computation.	Extremely resource-intensive, currently impractical.	Theoretical progress toward universal quantum privacy.
Differential Privacy (DP) for quantum data	Adds controlled noise to quantum data outputs.	Formal privacy guarantees for aggregate analysis.	Quantum measurement constraints, trade-off with accuracy.	Early-stage research integrating DP with quantum measurement models.
Secure Multi-Party Computation (MPC) with quantum support	Multiple parties jointly compute results without sharing raw data.	Privacy-preserving distributed computation.	High communication complexity, synchronization issues.	Hybrid quantum-classical MPC reduces latency and improves fairness.
Federated Quantum Learning (FQL)	Training models across distributed quantum nodes without raw data sharing.	Decentralized learning, minimal exposure of local data.	Aggregation attacks, system heterogeneity.	Promising area linking AI privacy and quantum networking.
Quantum authentication & MACs	Verify message authenticity using quantum states.	Ensures integrity and identity validation.	Additional qubit overhead and hardware demand.	Strengthens end-to-end data integrity in hybrid quantum networks.
Trusted node architectures	Use intermediate secure nodes for key relaying.	Extends communication distance and stability.	Introduces partial trust assumption and risk.	Necessary near-term solution until quantum repeaters mature.
Quantum resource and channel management	Optimize qubit routing, bandwidth, and scheduling.	Improves efficiency and network reliability.	Complex to scale dynamically; potential privacy leaks.	Software-defined quantum networks (SDQN) being developed.
Legal and ethical frameworks	Establish privacy and data-sharing laws for quantum data.	Enables compliance and governance.	No global standardization yet.	Policy development is lagging behind technical progress.

Made possible by the availability of various links shared by different cloud operators supporting complimentary computation, the focus of the exposition moves towards the intention rather than the implementation. It is shown that privacy-friendly protocols and mechanisms can be realized, either standing on the weakness of quantum networks concerning data integrity and confidentiality, or turning their strengths into use for classical privacy considerations and some directions for future improvement are also suggested.

4.1 Challenges and Considerations

With the transfer of standards from research to industrial practice, sharing resources and data on a multi-vendor basis in quantum computer networks seems to be inevitable, not the least to sustain a diversity of valued services. The desire for privacy in this context is universally recognized but also acknowledged to be difficult to achieve. Two key aspects currently under less scrutiny are the concern by users for privacy, and the need for compliance by network providers with relevant regulatory constraints. These, however, are of central importance as they will influence protocol design

There is widespread agreement that privacy preservation in classical computer networks is challenging 11, nonetheless, irrespective of the technology used for networking. Nonetheless, an appropriate standardization of the protocols is required to protect the quantum computers and associated resources connected to the network. In current networks it is already known that side attacks from classical resources can compromise privacy in principle, in addition to there being known attacks on current limited quantum systems. Formal standards, and working practices faithfully adhered to, can greatly help in the analysis and defense against the many and subtle potential threats 1. There has been little attention given to privacy in emerging quantum networks, i.e. exclusively quantum networks. The introduction of any new technology leads to new vulnerabilities. Therefore, the integration of quantum resources and protocols must carefully consider how these will fit in with existing (largely classical) practice. Security must be a primary concern from the beginning, with security of privacy probably the most important in the foreseeable future. No matter with whom you communicate, whatever the purpose, there will always be a concern for privacy. This is likely to be given particular attention as the public become more aware of the ways in which confidential messages can be compromised, whether by careless social media, insecure devices, or overly intrusive government surveillance, among many other factors. In principle, mathematicians, computer scientists, and technicians can devise ever better forms of encryption and networks which will be increasingly difficult to break. For any particular solution this inevitably leads to a game of 'cat and mouse' with those seeking to exploit weaknesses always seeking new ways to do so. Security is not a new concern - Julius Caesar is known to have used a simple substitution cypher over 2,000 years ago, and devices to protect communications have been used since time immemorial. However, the rise of mass communication in the late 19th and 20th century has radically changed the security landscape.

4.2 Techniques and Protocols

Quantum networking is a modern technology that exploits quantum properties and offers new solutions for communication networks. In quantum-enabled networks, end-users can share data or use network services with high-privacy requirements. Since the sharing of private data among end-users also reveals sensitive information to the network providers, it is important to investigate new methods to ensure the privacy of the shared data.

The objective of this subsection is to categorize novel advances in techniques, tools, or protocols that allow the implementation of privacy-preserving sharing of data, services, or resources in quantum-enabled networks. This includes quantum homomorphic encryption methods and protocols, as well as innovative applications of existing standards to privacy-preserving data sharing in quantum-enhanced networks, whereas conventional privacy-preserving methods of data sharing are not well-suited for networking applications. The methods are described with their operational details, the effectiveness and applicability are discussed, and the challenges are pointed out in integrating these methods into existing quantum technologies and classical networks. Finally, a brief comparison is provided between the privacy mechanisms traditionally used in network jargons and the new methods possible leveraging future quantum networks or technologies.

The privacy-preserving methods of data sharing, resource sharing, or communication design are also approached to use a secure routing criterion. However, the security metrics applied are usually concerned with verifying the identity of the message sender and ensuring that the message delivery is correct, affectionately leaving a blind exchange of the messages. With the advancement of quantum technology, new techniques have been developed to preserve the privacy of the quantum states or the quantum communication. In this context, a novel study aims to clarify how quantum homomorphic encryption can be used to encrypt quantum data or quantum states as a method of privacy-preservation.

5. Applications and Use Cases

Development in sectors such as healthcare, finance, insurance, telecommunications, defense, pharmaceuticals, and critical infrastructure, is characterized by institutionalized practices that generate and store a large number of highly sensitive data. Given the due importance of privacy of these data in regard to business and individual liability concerns, they are often of invaluable worth and highly targeted in rivals' efforts to gain information leverage. In a quantum environment, challenges associated with ensuring the privacy of these data follow an exponential trajectory. Traditional cryptographic mechanisms fail to ensure data privacy in the advent of fault-tolerant quantum computers 12. The thorough examination of real-world scenarios - exemplifying the types of interactions within these sectors and potential data analyses - that these organizations would like to pursue in a privacy-preserving manner is notable. Furthermore, characterizing detailed privacy requirements for each participant in these scenarios, such as private inputs and outputs, and elaborating on the broader privacy goals of these interactions, is a laudable endeavor to describe and compare the spectrum of possible applications and use-cases for privacy-preserving data sharing within quantum-enabled networks. Presenting specific examples of mathematical problems or types of analyses that need to be kept private in each application area can aid in the design and scrutiny of solutions. For a more comprehensive landscape, an examination of potential Attack Vectors Breaking the data privacy, assuming computational constraints is taken out of the table, in each domain is necessary. Lastly, it is important to highlight questions for further research raised by these tasks. There is no silver bullet sphere of "quantum-secure" technologies and techniques for privacy-preserving data sharing within quantum-enabled networks. Hence, there is a need to explore a variety of directions and continue exploring new solutions as quantum technologies, and their capabilities mature and evolve.

5.1 Healthcare

Modern society is becoming more connected and dependent on data, and future networks will be more versatile, efficient, and resilient thanks to the use of classical and quantum technologies. Nevertheless, individuals and organizations face profound privacy challenges due to the exposure of sensitive data when connected to networks. Privacy-preserving data sharing is an active and critical research and technological development that becomes essential to enable the potential benefits of network dependence. Multi-domain applications, using resources from an increasing number of interconnected stakeholders, underline the necessity to overcome fragmentation in these diverse but converging fields of privacy, security, networking, computing, and quantum technologies.

Sensitive data, such as health-related data in the case of individuals, are used in various sectors, such as healthcare, and require special rules to ensure proper handling and processing. However, when the primary goal is met, data may need to be shared across organizations for research, diagnostics, preventive care, or merely to improve the efficiency of healthcare provision. Nevertheless, ensuring patient confidentiality while allowing data exchange is a nontrivial challenge in the healthcare sector due to the special sensitivity of health data 12. Today, health data is threatened by new cryptanalysis quantum algorithms, and their protection requires quantum security measures that have recently started to be considered. However, few if any organizations have yet implemented such quantum-resilient techniques or have addressed the changes needed to make the system safe beyond the advent of quantum computers.

5.2 Finance

Data protection in the finance sector is primordial due to the sensitive nature of the data, protecting transactions or financial data will always represent a trade-off between transparency and confidentiality. On the one hand, transparency over financial transactions is seen as paramount for the proper functioning of the market. Consumers need to be able to trust financial intermediaries with their assets, while combating financial illicit activities. On the other hand, confidentiality of the data is needed to preserve the integrity of the financial communications. Obfuscating financial data could also force some financial institutions to share private business plans. Clearly, there is a need for co-solutions that would allow to control data sharing and ensure good practices. Quantum threats are already beginning to emerge and the financial world has to be aware of it. This relatively new technology has the potential to disrupt many of the well-established schemes currently in place, and financial actors must equip themselves with long-lasting tools. The circular is showcasing a number of use-cases for a better understanding of the concrete applications of quantum technologies in finance. It is a unique source of data for location privacy studies, and the ability to detect anomalous trajectories carries substantial consequences regarding the security of the data and the people involved. The simple circuit model is able to learn polynomial-size concepts in logarithm depth, and networks matching these parameters can be built and processed at runtime. Secure online banking and applications could be realized if the pre-printed information

cards were associated to detector chips exchanging quantum proof paper trays in a secured way.

In addition, the use of the same quantum proofing quantum secure cards could also speed the fraud detection process by having shared online information flows. International regulatory and monetary transfers make a clear case for increasing the share of encrypted global valleys to more than 15%, facilitating higher levels of location information privacy. Due to the massive volume of transactions in location-based services, it may become unsafe to share data without appropriate protective measures. Regulatory bodies overseeing the use of online financial accounts are expected to adjust their approach to compliance. All the use of compliant secure online banking applications could easily be modified by quantum communication hardware and allowed quantum-secure communication. In compliance with the standards, the financial world has become a WFH for disputes and extra-fiduciary information. While significantly fostering transparency over financial institutions, many of these requests could violate the confidentiality of financial communications. Furthermore, considering the different regional environments, financial circuits will still present significant difficulties ensuring the security of the communications. At the beginning of 2020, a massive leakage of personal data originating from financial institutions documents forced in-depth revisions of the standard. The standards were filed linearly and impacted the compliance of the main financial circuits in use. Two additional standards addressing location-based services as well as the protection of property rights were put forth facilitating the compliance of geographical areas and the security of the communications. Up-to-date information concerning the regulatory environment and possible new standards will be shared continuously. Financial topics have always been at the heart of sharing agreements since the sector is known to have the most varied demanding trading strategies. The sector also invests the most in R&D but is then subject to the strong constraints on the fast commercialization of the discovered technologies. The fast technological environment led the definition of the financial sharing agreement that is now enforced on all major players.

5.3 Telecommunications

The recent advances in big data techniques and the shift from cloud-based computing to edge intelligence have the potential to revolutionize the way we interact with the world. The Internet of Things (IoT) and the vision of the Ambient World constantly register our presence around the City of Bytes. What we see as benefits also involves massive streams of private data records to be managed, with possible risks of disclosing personal information. Each transaction, query or activation implicates interchanges of data involving several entities, from sensors, tags, UAVs, to the servers of companies, which are asked or are providing the requested services. In the future City of Bytes, the Big Data generated around people and its subsets are constantly created and automatically transported around, searched and queried, protecting the perceived of the City and conserving the desired safety, security or privacy have become crucial priorities.

Only the most paranoid conspiracy addict will try to stay unrecorded and untraceable, but that does not mean it is necessary to be calm and serene about the use of collected data. With the increasing volumes of data collected and analyzed, comes the feeling of being widely exposed, with uncomfortable analytics that seem to border closer and closer to your sincerely privacy threshold. What's more recent data exchange regulation and fines for data privacy breaches can give a fright for any company or individual casually handling big data. This is why the emerging quantum technologies have attracted a warm pro-business careful eyes in all the industries dealing with big data. The leveraging of these technologies for data protection is seen as having a generationally big impact, improving the safety and reliability against the unauthorized access, sensitive data leaks, and insecure data processing 1.

For the telecommunications industry, or more accurately for the telecommunication users, the situation is even more tricky. No other industry is creating so much personal data and at the same time, is so heavily dependent on the basic kind of these data. Voice call services are still fed from recordings of your actual voice as you produce them. As the traditional telco services are more and more displaced by the data connections, the voice traffic itself is being processed in a digital format. While the voice has transitioned from the tear-jerk flat rate minutes to the sweet-talk VoIP, soon all the traditional souls-filled sweet whispers and gibberish mutters will be converted to another bunch of text messages and data packets ripe for cryptographic analysis.

6. Security and Threat Models

Emerging threats and potential vulnerabilities in quantum network environments are analyzed as well as the current security and threat models may be affected by the impact of quantum computing. A new security outcome for privacy-preserving data sharing in quantum networks is provided. Corresponding threat models to realize this security outcome are formulated. Quantum networks can push the sustainable development of quantum computers, quantum sensors, quantum memory, quantum simulators, and other emerging quantum technologies, which have

shown potential advantages over their classical counterparts in communication, computation, and sensing performance such as quantum parallelism, quantum superposition, and quantum entanglement, as well as offering the next generation of highly secure network communication infrastructure. On the one hand, quantum technology would be employed to generate a form of quantum signals, like quantum light, that is used in the quantum network for transmission and processing of information with a fundamentally higher security function. On the other hand, quantum technology could be used to construct an innovative encryption-decryption system, quantum key distribution additionally to the technologically available possibilities, to ensure the security and integrity of digital data during its transmission. As an alternative to classical public key systems, quantum-network encryption would significantly simplify the process of distributing and refreshing cryptographic keys, a realization of broadband quantum key distribution is highly demanded for this need. Grounds of the concept of a quantum-network encryption system and probable architecture of the supporting quantum network infrastructure are put forth and discussed. Such networks could be executed in the foreseeable future, and temporal limits on the realization of this new class of quantum networks are detailed. The effect of the main characteristics of quantum encryption devices on the design of the network is also scrutinized. The proposed network model starts the drafting of work of a truly quantum global communication infrastructure, even now that the very longest quantum-secure information channel is less than 5000km. After the definition of a networked system, with its uniting components running at an already technologically feasible level, habits able to communicate an undisclosed sequence of binary digits globally between any died of issue are recruited.

7. Current Research Trends

Simultaneously with the rise of more powerful quantum computers and networks, the extent of data produced and shared across the world wide web is growing at an exponential rate. Several works of literature forecast a situation in which half of the world's data-sphere will go quantum enabled by 2030. Despite the many opportunities that will be opened by an extended use of quantum networking technologies, there is often the risk that part of the information transferred gets into unauthorized hands. This is particularly sensitive when data shared is private by nature: although strict protocols are followed, it is never possible to fully protect it. Very recently, a protocol for privacy-preserving data sharing among users connected via general links was proposed. Instead of directly sharing their data, the interaction among the couple of users is mediated through another party; this party is able to access the data themselves, but still has no information on its content due to the adopted encoding. Despite being one of the strongest available protocols, however, it relies on unreasonably long encoding size for practical applications; this dramatically limits its use, particularly in regards of the constant technological advance. Researchers hope to overcome this limitation by taking some inspiration from a recently proposed protocol for secure multi-party quantum one-time program.

8. Future Directions and Opportunities

Recent advancements in quantum communication and computation technology have the potential to revolutionize communication infrastructure by enabling quantum-enhanced networking. This technological evolution, envisaged in the emerging quantum networks paradigm, is expected to bring a new generation of secure, efficient, and privacy-preserving data services, optimizing resource exploitation in a variety of application scenarios. In this vision, quantum cryptography can offer valuable characteristics for assurance of privacy in network processes, by architecture design as underlying network primitives or overlay services. However, there is an open issue regarding a suitable middleware that should be responsible for enforcing the privacy between different network domains while also taking into account the different network operators and the network clients.

Concerning cyber security challenges, privacy protection mechanisms for mediated sharing of data represent the last line of defense for network architectures, and data-transmission services are at the first line of design efforts to protect privacy. Unbalanced data accessibility and network control among the participants may lead to the semi-collusive case where a client leverages network expertise for unlawful reasons, creating a greater challenge for efficiency in privacy enforcement. Therefore, compact formalization and abstraction, as well as enhancement of the available tools and methods, in the presence of varied and large-capacity data sharing are substantially risk-reducing. Open challenges require contributions from multi-disciplines, and balanced effort from all stakeholders is imperative for achieving sustainable solutions in the quantum-enabled network sharing 1.

Considering additional future research steps and technological evolutions, besides the necessary enhancement of quantum cryptographic methods for controlling the privacy among different domains, it is important to envision novel security protocols and

cooperative privacy measures to be enforced at the middle-layer of the network aspects, as well as end-to-end control of the intermediary routers and switches. In doing so, valuable possibilities are opened for the improvement of standard communications protocols and for the design of standardized architectures 2. Commercial tools and applications will be able to automatically enforce the correct privacy, thereby rendering the data sharing agreements more manageable and affordable from a legal and regulatory point of view. Last but not least, enforcement of standardized privacy-consistent practices opens novel challenges to the side of the participants, since accurate representation of the experimental conditions and sharing processes will be required for achieving favorable outcomes. Thus, they will need to rely on the support of efficient methods and that in turn will drive innovation on ability and devices for fraudulent practices. In turn, this will favor the development of an emergent market in quantum-secured verifiable tools and high-reproducibility protocols.

9. Conclusion and Summary

Advances in quantum communication have a profound impact on the emerging quantum technologies and their applications beyond quantum key distribution. Development of quantum-enabled networks involves the integration and interplay between quantum and classical technologies, which allows the construction and management of networks with routers, switches, and gates that operate on quantum states. It is essential to consider privacy from a broader perspective, including its aspects in terms of content, identity, data link ability, and accessibility while adapting quantum techniques to enrich current privacy-preserving practices. This necessitates a comprehensive exploration with studies ranging from theoretical studies on security proofs against passive and active attacks on quantum channels to the development of practical schemes and the investigation of their integration with advanced networking functionalities. Despite the envisioned benefits, several challenges arise in preserving privacy in the context of the expected evolution of quantum technologies. Addressing these challenges requires the development of a set of new technologies and the adaptation of the common approaches to mitigate the threats of data exposure in quantum-based networks.

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: All authors contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature,* vol. 549, pp. 43-47, 2017, doi: https://doi.org/10.1038/nature23655.

[2] B. Li, G. Zhang, and C. Zhou, "Measurement-Device-Independent Quantum Key Distribution: Advances and Perspectives," *Quantum Science and Technology,* vol. 6, no. 3, p. 033003, 2021.

[3] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information,* vol. 6, no. 1, pp. 1-127, 2008, doi: https://doi.org/10.1142/S0219749908003256.

[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of modern physics,* vol. 92, no. 2, p. 025002, 2020, doi: https://doi.org/10.1103/RevModPhys.92.025002.

[5] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information theory,* vol. 41, no. 6, pp. 1915-1923, 2002, doi: https://doi.org/10.1109/18.476316.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics,* vol. 81, no. 3, pp. 1301-1350, 2009, doi: https://doi.org/10.1103/RevModPhys.81.1301.

[7] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature,* vol. 557, pp. 400-403, 2018, doi: https://doi.org/10.1038/s41586-018-0066-6.

[8] A. Boaron *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Physical Review Letters,* vol. 121, no. 19, p. 190502, 2018, doi: https://doi.org/10.1103/PhysRevLett.121.190502.

[9] G. Zhang, J. Wang, and Y. Liu, "Large-Scale Quantum Key Distribution Network and Applications," *Frontiers of Optoelectronics,* vol. 12, no. 3, pp. 289–302, 2019.

[10] R. Kumar, A. Ciurana, and N. Walenta, "Versatile Quantum Key Distribution Protocol for Securing Long-Distance Communication," *Quantum Information & Computation,* vol. 19, no. 7-8, pp. 1071–1090, 2019.

[11] E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov, "Symmetric blind information reconciliation for quantum key distribution," *Physical Review Applied,* vol. 8, no. 4, p. 044017, 2017, doi: Https://doi.org/10.1103/PhysRevApplied.8.044017.

[12] J. Wang, H. Wang, and G. Zhang, "Practical Applications of Quantum Cryptography," *Applied Physics Reviews,* vol. 8, no. 5, p. 051302, 2021.

[13] J. Yin *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature,* vol. 582, pp. 501-505, 2020, doi: https://doi.org/10.1038/s41586-020-2401-y.

[14] S. Wang *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nature photonics,* vol. 16, pp. 154-161, 2022, doi: https://doi.org/10.1038/s41566-021-00928-2.

[15] B. Qi, Zhang, and X. Ma, "Quantum Cryptography and its Security in the Quantum Era," *Quantum Information Processing,* vol. 18, no. 5, p. 133, 2020.

[16] S. Wan, Z. Yu, and Z. Huang, "Quantum Privacy Amplification for Quantum Key Distribution," *Journal of Quantum Information Science,* vol. 11, no. 4, pp. 387–404, 2021.

[17] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics,* vol. 74, no. 1, pp. 145-195, 2002, doi: https://doi.org/10.1103/RevModPhys.74.145.

[18] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics,* vol. 8, pp. 595-604, 2014, doi: https://doi.org/10.1038/nphoton.2014.149.

[19] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A,* vol. 65, p. 032302, 2002, doi: https://doi.org/10.1103/PhysRevA.65.032302.

[20] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical review letters,* vol. 70, no. 13, p. 1895, 1993, doi: https://doi.org/10.1103/PhysRevLett.70.1895.

How to cite this article

Z. I. Rasool and N. S. Hadi, " Exploring the Techniques and Challenges of Privacy-Preserving Data Sharing in Quantum-Enabled Networks," *CyberSystem J.*, vol. 2, no. 2, pp. 1-15, 2025. doi: 10.57238/csj.2025.1009

Access this article online