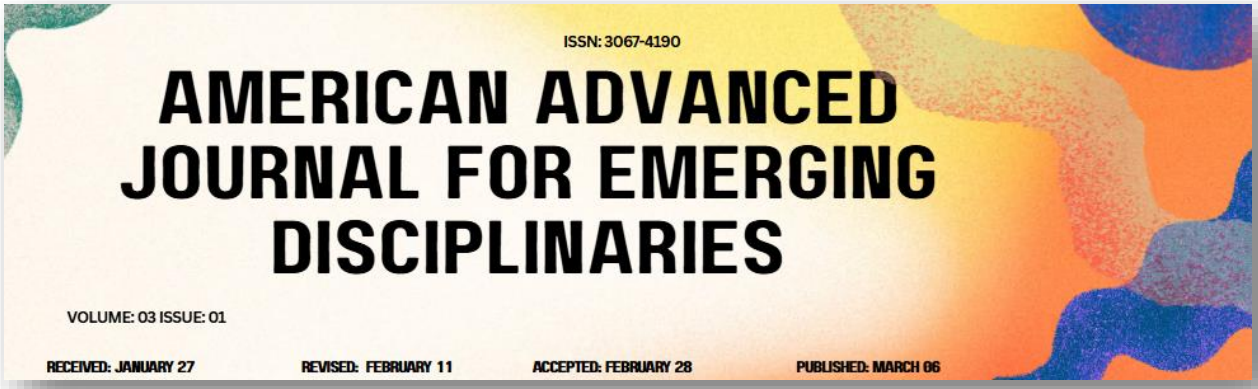


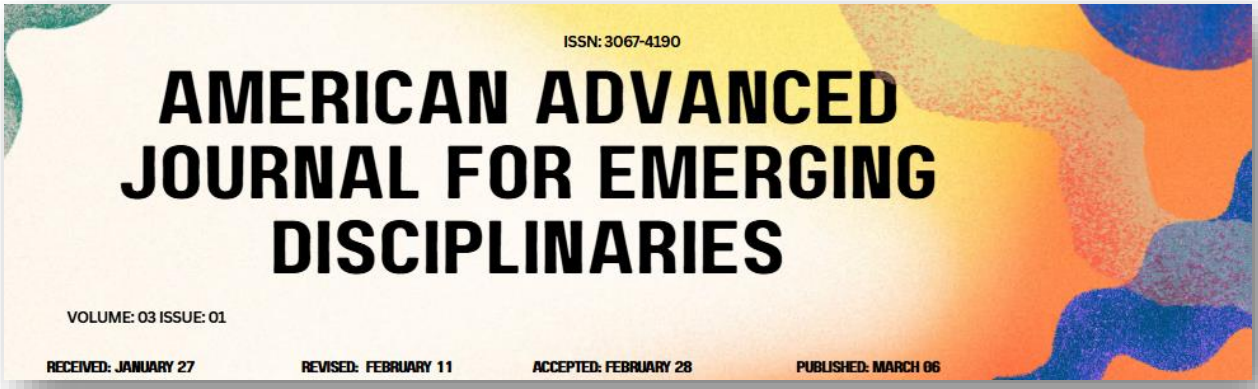
Architecture and Communication Protocols

Anumandla Mukesh
Independent Researcher
mukeshanumand@gmail.com

Abstract

Quantum communication and the quantum internet are converging subfields of research based on the application of quantum mechanics to the exchange of information, either to enhance existing protocols or to enable entirely new ones. Milestones in this journey include Bell inequalities, indistinguishability-proof secret-key distribution, uncertainty, and no-cloning; the proof of the quantum channel capacity theorem; and the exponential advantage of quantum teleportation over the classical teleportation of qubits. The quantum internet is fundamentally layered, akin to the classical internet but enabling the orchestration of quantum mechanics in a protocol stack that may span multiple administrations. Achievements to date cover many ground-layer requirements for quantum key distribution and entanglement distribution, enabling basic demonstrations of provably secure secret-key generation between metropolitan quantum networks. A threat model for quantum networks and a thorough discussion on security and privacy emphasize the unique nature of quantum mechanics as a potential asset in devising security protocols.

Quantum communication is defined as the exchange of information between physical systems described by quantum mechanics, and entanglement is perhaps the most distinctive aspect of quantum information theory. Quantum channels connect separated quantum systems, allowing the distribution of quantum information over distance. In networked quantum information, a number of parties need not only prepare or measure quantum information but also rely on the successful transmission of quantum information over a quantum network. End-to-end quantum communication protocols supporting specific tasks—quantum key distribution; indistinguishability-proof secret-key distribution; quantum teleportation; state transfer and entanglement swapping in quantum relays; and entanglement distribution—have been formulated and investigated from a physical-layer perspective. Each protocol is examined according to vulnerability to nonideal conditions and realistic operation requirements, enabling comparisons of achievable performance. While advantages of quantum protocols are becoming practical, their exploitation in practice demands careful attention to nonideal performance and the avoidance of unrealistic assumptions.



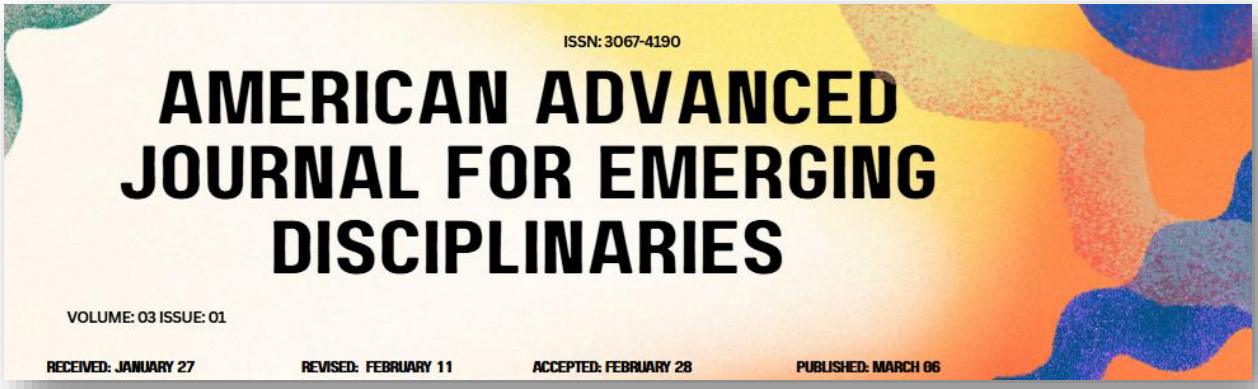
Keywords: Quantum Communication, Quantum Internet Architecture, Quantum Information Exchange, Quantum Mechanics Protocols, Bell Inequalities, No-Cloning Principle, Quantum Channel Capacity, Quantum Teleportation Advantage, Layered Quantum Networks, Quantum Protocol Stack, Quantum Key Distribution, Entanglement Distribution, Metropolitan Quantum Networks, Quantum Network Threat Models, Quantum Security And Privacy, Quantum Channels, Networked Quantum Information, End-To-End Quantum Protocols, Entanglement Swapping, Nonideal Quantum Performance.

1. Introduction

Quantum communication employs quantum systems to transmit information, and enables new functionalities that surpass classical capabilities within a quantum network. The key quantum resource is the use of entangled states, which introduce correlations between distant parties surpassing those of classical correlations. Such networks for quantum communication can also be considered a quantum internet: a global infrastructure that enables the detection and manipulation of quantum systems at a distance, and supports various applications beyond standard communication.

Along with quantum key distribution (QKD), action-at-a-distance schemes such as teleportation, entanglement swapping, and state transfer constitute the core of quantum communication. Teleportation was introduced as a technique for transferring a state between distant parties, raising the question of how much entangled resource is needed. Most communication problems involve not just the transmission of quantum states but rather the transfer of quantum information that may not be encoded on physical states. In the simplest yet most fundamental communication scenario, one party might wish to send a specific quantum state directly to another, and the quantum channel capacities quantify the optimal performance for this single-user scenario. Adding noise reveals other sources of difficulty, and models of realistic quantum channels allow estimation of the capacity for reliable quantum communication and identification of possible error-correcting methods that approach capacity. Formal results like the no-cloning theorem and Bell inequalities also have implications for practical implementations and security.

1.1. Overview of Quantum Communication Concepts



Quantum communication exploits the laws of quantum mechanics to achieve tasks that are impractical, impossible, or infeasible using only classical (non-quantum) communication resources and protocols. Quantum channels transfer quantum states between sender and receiver using quantum properties such as superpositions and entangled correlations. If receivers are no longer present, entangled states can nevertheless be sent through teleportation and state-transfer protocols, which require communicating only classical information. Quantum states can be multicast in such a way that it is impossible for eavesdroppers to learn anything about them without an observable disturbance, a property that surpasses all classical multicast -security protocols. If the communication is one-to-many, i.e., the sender wants to send quantum states to many receivers using an entangled resource, it has been shown that entanglement swapping allows achieving this goal while being secure against eavesdroppers. The quantum channel capacities show that, when quantum resources are present, certain quantities can be transmitted using less classical shared randomness, can be sent noiselessly over noisy channels in a smaller amount of time, or can be sent faster than with the power of quantum sending-only resources.

Quantum communications will ultimately allow the full-scale deployment of the quantum internet, a grossly parallel endeavor that will build a network of quantum computers that harnesses the power of quantum computing over long distances in a compact and fast fashion. The last decades have seen tremendous theoretical and experimental advances in quantum-key-distribution (QKD) security proofs and implementations, which include schemes that are not only proven secure but also composably secure—notably, Can QKD Be A Secure Key Distribution Service?—and implanted in fully fledged dynamic systems based on a plug-and-play add/drop multiplexing architecture. Security proofs have also made novel developments possible, such as those using squeezed states, nonlocal detectors, measurement-device-independent QKD, and the certification of quantum operations using the simpler and thus easier-to-achieve task of endorsing idempotent states.

ISSN: 3067-4190

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 03 ISSUE: 01

RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06

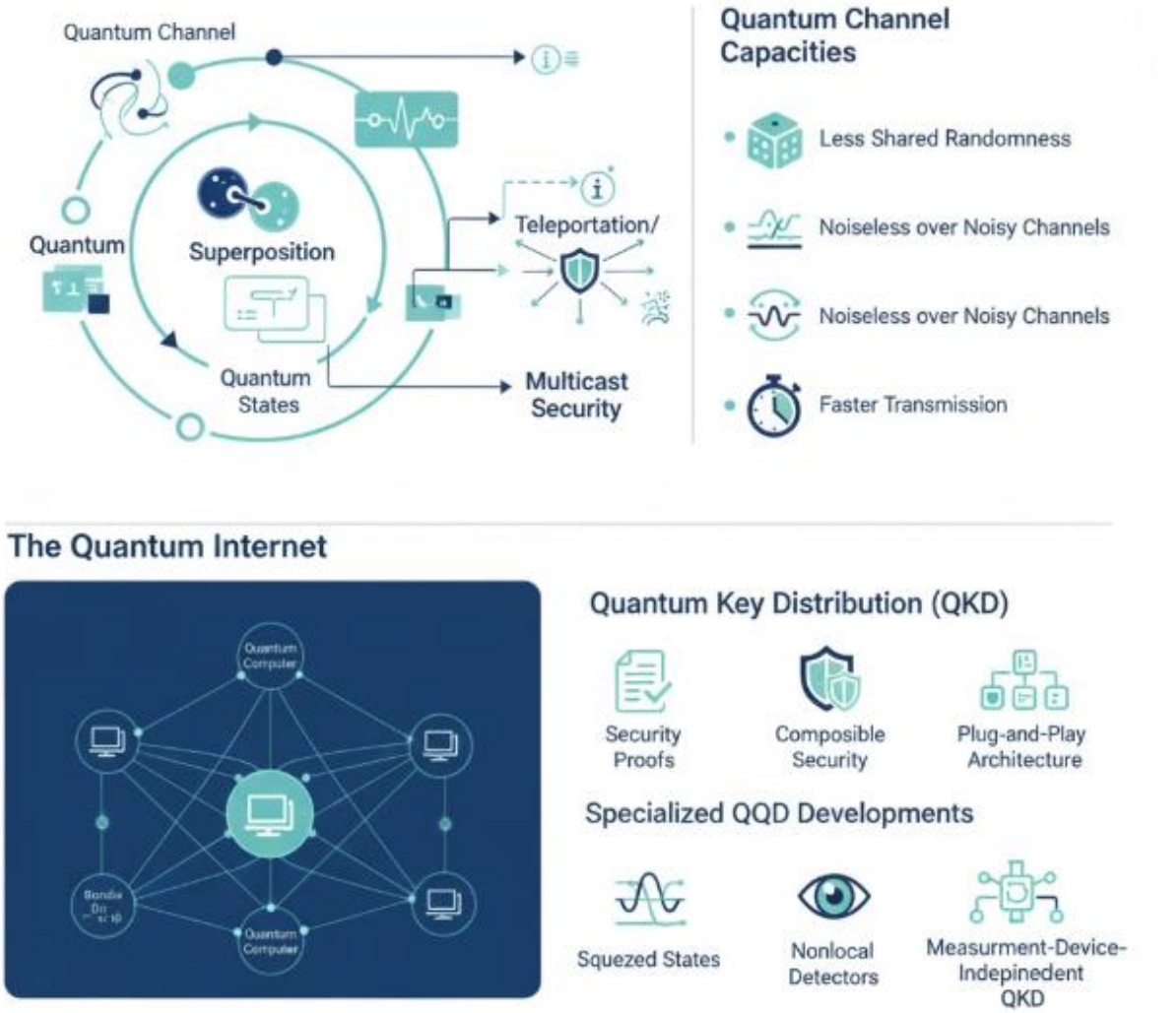


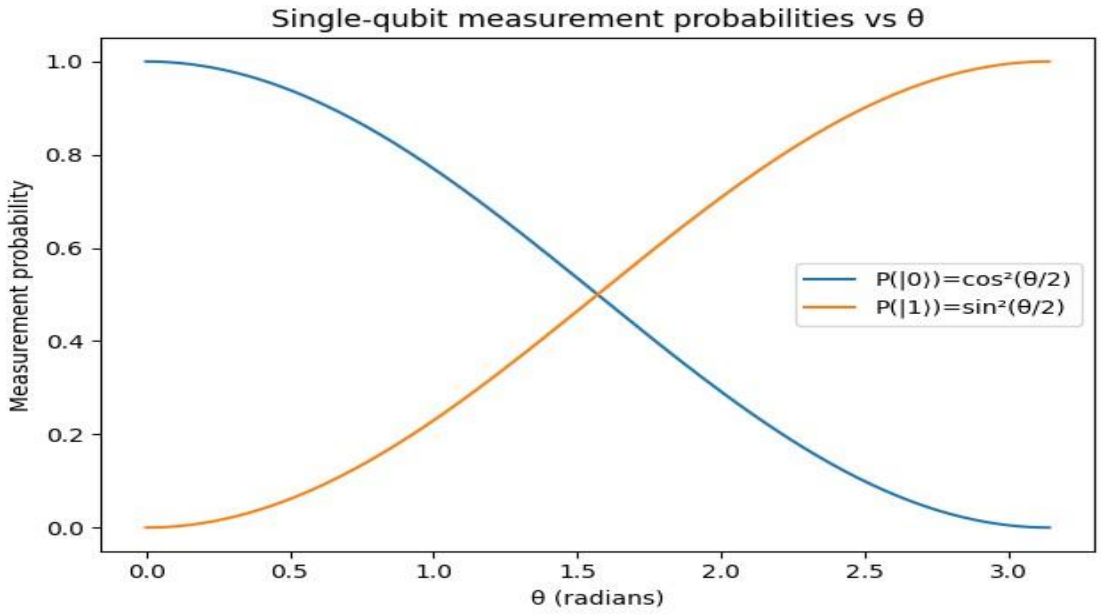
Fig 1: Foundations of the Quantum Internet: Entanglement-Based Communication, Composably Secure QKD, and Advanced State-Transfer Protocols

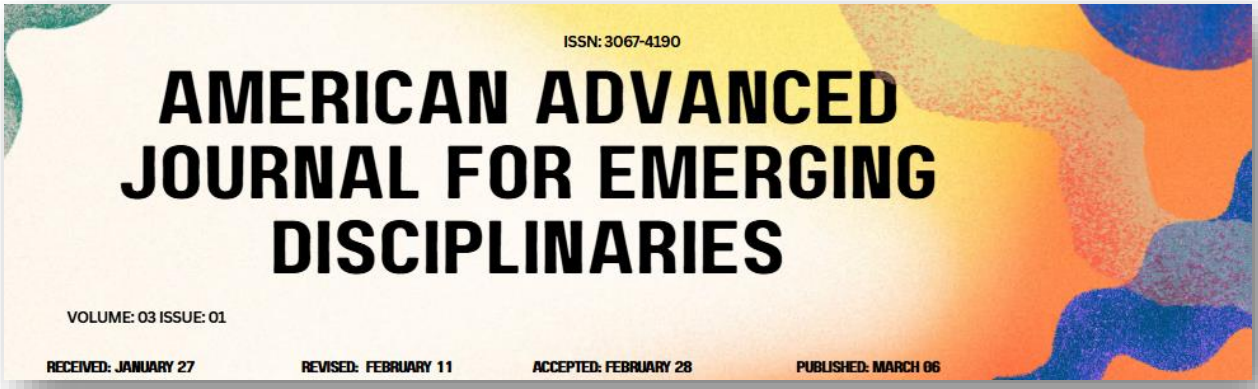
2. Foundations of Quantum Communication

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06

The principles of quantum communication are derived from the laws of quantum mechanics and the mathematical properties of quantum states combined with the properties of quantum mechanical systems that allow them to be used for the communication of information. Quantum states are mathematical constructs used to model nature at small scales, including communications at small scales. These states can be thought of as the preferred mode of communication between the quantum mechanics of nature and quantum information, in this case, encoded in classical information.

The central difference between classical and quantum communication lies in whether the qubit, or the quantum analogue of a bit, can be cloned. Classical communication allows one to copy and reuse the shared classical channel. Whether this change or not has advantages over classical communication is regulated by the encoding and the transformation used. Non-cloning is one of the rules that interlinks all the fundamental no-go theorems that governs the behaviour of quantum protocols. Qubits as a resource can be flagged into required groups either being faithful for communication-no-show or being unlimited and not faithfully provable by whatever is done. Entanglement and other requirements may also lead to the protocol being showable with no new resources added when copying is not restricted.





Equation 1) Single-qubit state (Bloch-sphere form)

The defines a general qubit as

$$|\psi\rangle = \cos(\theta/2)e^{i\phi/2}|0\rangle + \sin(\theta/2)e^{-i\phi/2}|1\rangle, \quad \theta \in [0,\pi],\ \phi \in [0,2\pi).$$

Step-by-step derivation from the most general qubit

Step 1 (start general): any qubit can be written

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad \alpha,\beta \in \mathbb{C}.$$

Step 2 (normalization constraint):

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1.$$

Step 3 (remove global phase): write $\alpha = |\alpha|e^{i\gamma}$. Multiply the whole state by $e^{-i\gamma}$ (physically irrelevant global phase), giving an equivalent state with α real and non-negative:

$$|\psi\rangle \sim |\alpha| \quad |0\rangle + \beta e^{-i\gamma}|1\rangle.$$

Let $|\alpha| = \cos(\theta/2)$ for some $\theta \in [0,\pi]$. Then automatically

$$|\beta| = \sin(\theta/2)$$

because $|\alpha|^2 + |\beta|^2 = 1 \Rightarrow \cos^2(\theta/2) + |\beta|^2 = 1$.

Step 4 (encode the relative phase): write the remaining complex phase of β as $e^{-i\phi}$:

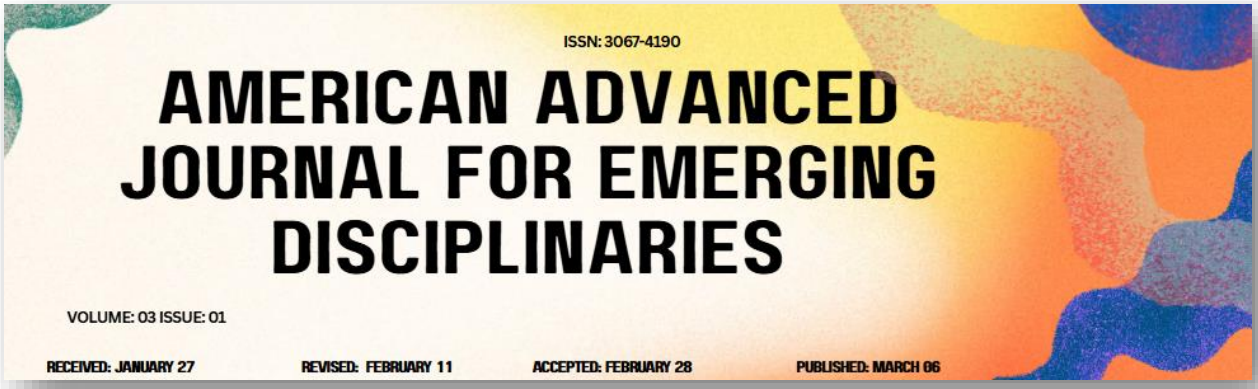
$$\beta e^{-i\gamma} = \sin(\theta/2)e^{-i\phi}.$$

So one standard form is

$$|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{-i\phi}|1\rangle.$$

Step 5 (symmetrize phases to match the article): factor $e^{-i\phi/2}$ overall:

$$|\psi\rangle = e^{-i\phi/2}(\cos(\theta/2)e^{i\phi/2}|0\rangle + \sin(\theta/2)e^{-i\phi/2}|1\rangle).$$



Dropping the global factor $e^{-i\phi/2}$ yields exactly the article's expression.

2.1. Quantum Bits and Entanglement

Quantum information and its fundamental unit, the qubit, play a central role in both quantum communication and quantum computation. A qubit can be physically realized using various physical systems such as atoms, ions, photons, and superconducting circuits. In the concept of Quantum Supremacy, a qubit is a physical quantum system that is under the influence of the laws of quantum mechanics. A qubit, in contrast to a classical bit which is either 0 or 1, can exist in superposition of both states. It is a quantum state denoted as $|\psi\rangle = \cos(\theta/2)e\{i\phi/2\}|0\rangle + \sin(\theta/2)e\{-i\phi/2\}|1\rangle \in C2$, where $\theta \in [0,\pi], \phi \in [0,2\pi)$ and $|0\rangle, |1\rangle$ are the two basis states. Entanglement emerges as one of the most intriguing phenomena in quantum mechanics that can not only not be explained but can also not be reproduced by classical physics. Yet, proofs of existence of entanglement were based on detection of violation of Bell inequalities and not on an implementation of a Bell test. Any two-qubit pure state can be written as $|\Phi\rangle AB = \cos(\varphi)|00\rangle AB + \sin(\varphi)|11\rangle AB$ or $|\Phi\rangle AB = |00\rangle AB + |11\rangle AB + (1/\mathrm{sqrt}(2))(|01\rangle AB + |10\rangle AB)$, with the latter displaying a key property for QKD and enabling the transfer of a state from one node to another with a help of an entangled channel, without moving a qubit along the channel. Further, it has been recognized that no-cloning theorem plays a key role in QKD. Quantum channels can accommodate the whole of networked quantum information theory, including tasks such as quantum secret sharing, quantum teleportation, state transfer, entanglement swapping, quantum digital signatures, and quantum key distribution; hence a survey of these protocols and their performance is meaningful.

Due to the richness of the quantum theory, several different qualities of quantum channels affect the operation of the above protocols: the capacity of the channel, i.e., the entanglement or quantum capacity; the quality of the transmitted states; and the character of the noise. A survey of protocols realizing different tasks against realistic quantum channels has been performed. For QKD, which is the most popular task, distinct protocols are considered, enabling a mapping of the most popular protocols, proving security under different models, and classifying devices used. It is further possible to analyze the impact of finite key size and to identify either a rate–distance trade-off or trade-offs involving additional device requirements either via the channel or via the authenticated channel.

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06

Bell outcome (Alice)	j label	Bob correction $\mathcal{D}$j (Pauli)
$\|\Phi^+\rangle$	0	I
$\|\Phi^-\rangle$	1	Z
$\|\Psi^+\rangle$	2	X
$\|\Psi^-\rangle$	3	XZ (or −iY up to global phase)

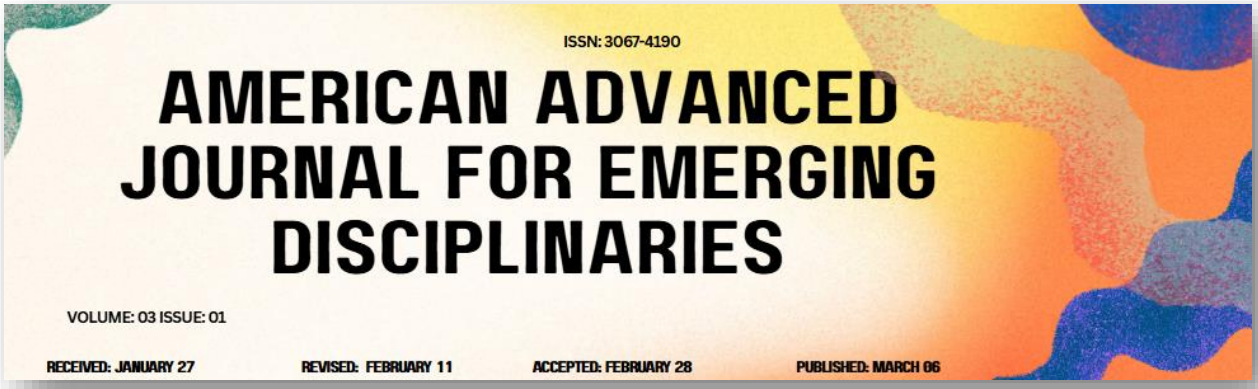
3. Core Quantum Communication Protocols

Quantum communication protocols are the foundational building blocks of a quantum network enabling quantum information transfer. Protocols serve specific high-level tasks, which can be further divided into subtasks and realized through different methods. Performance can be evaluated in terms of resource overhead, suitability for the underlying architecture and the conditions in which they operate. Specific figures of merit vary according to the considered task and should be assessed under realistic conditions.

Nine families of quantum communication protocols—quantum key distribution (QKD), quantum secret sharing, quantum secure direct communication, quantum bit commitment, quantum authentication, quantum blind signature, quantum teleportation, quantum state transfer, and entanglement swapping—have been identified and reviewed. Many are subtasks or variants of a larger task for which different solutions are available, similar to classical communication. Focusing on QKD, quantum teleportation, state transfer, and entanglement swapping sheds light on the key aspects of core quantum communication protocols.

Quantum key distribution is the only quantum communication protocol used in practice today, with operational commercial and research-grade QKD networks as well as connections in larger metropolitan networks. No provably secure QKD protocols, however, guarantee full protection against all types of attacks. Analysing the composable security of QKD provides insights into its advantages and disadvantages; several existing rate-distance and device-related bounds also highlight the possibility of QKD over real-world channels. Quantum teleportation, state transfer, and entanglement swapping have proven useful in both theoretical studies and experiments, and they have been or are being demonstrated with realistic rates.

3.1. Quantum Key Distribution Protocols



Quantum key distribution (QKD) protocols use information-theoretic security to allow two parties (Alice and Bob) to establish a secret key in the presence of a passive adversary (Eve) who can overhear the public discussion and has the ability to store the information exchanged by Alice and Bob, but is not permitted to send false information to either party. QKD is an essential component that enables a variety of higher-layer quantum communication protocols like quantum secure direct communication (QSDC), the one-time pad (OTP), and quantum secret-sharing. Many QKD protocols may be practically implemented using fiber-optic communications, free-space channels, and satellite links. In practice, QKD does not guarantee security in isolation; however, security can be demonstrated relative to a larger hypothetical protocol as desired.

The first experimental demonstration of quantum key distribution used the BB84 protocol and an imperfect implementation that did not include a security proof. Thenceforth, a large cadre of QKD protocols have been proposed and implemented. The broadest class of security proofs considers a realistic experimental setup in which the quantum channel is fully controlled by Eve, but Alice and Bob's devices are trusted—a condition that is difficult or impossible to satisfy in practice. Often a weaker security definition can be proved under the physical assumption that untrusted devices do not introduce additional security vulnerabilities. A high-level taxonomy distinguishes between device-dependent security proofs and those that do not assume trusted devices. A second, hierarchical, categorization divides QKD protocols by the techniques used and their security guarantees.

ISSN: 3067-4190

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES

VOLUME: 03 ISSUE: 01

RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06

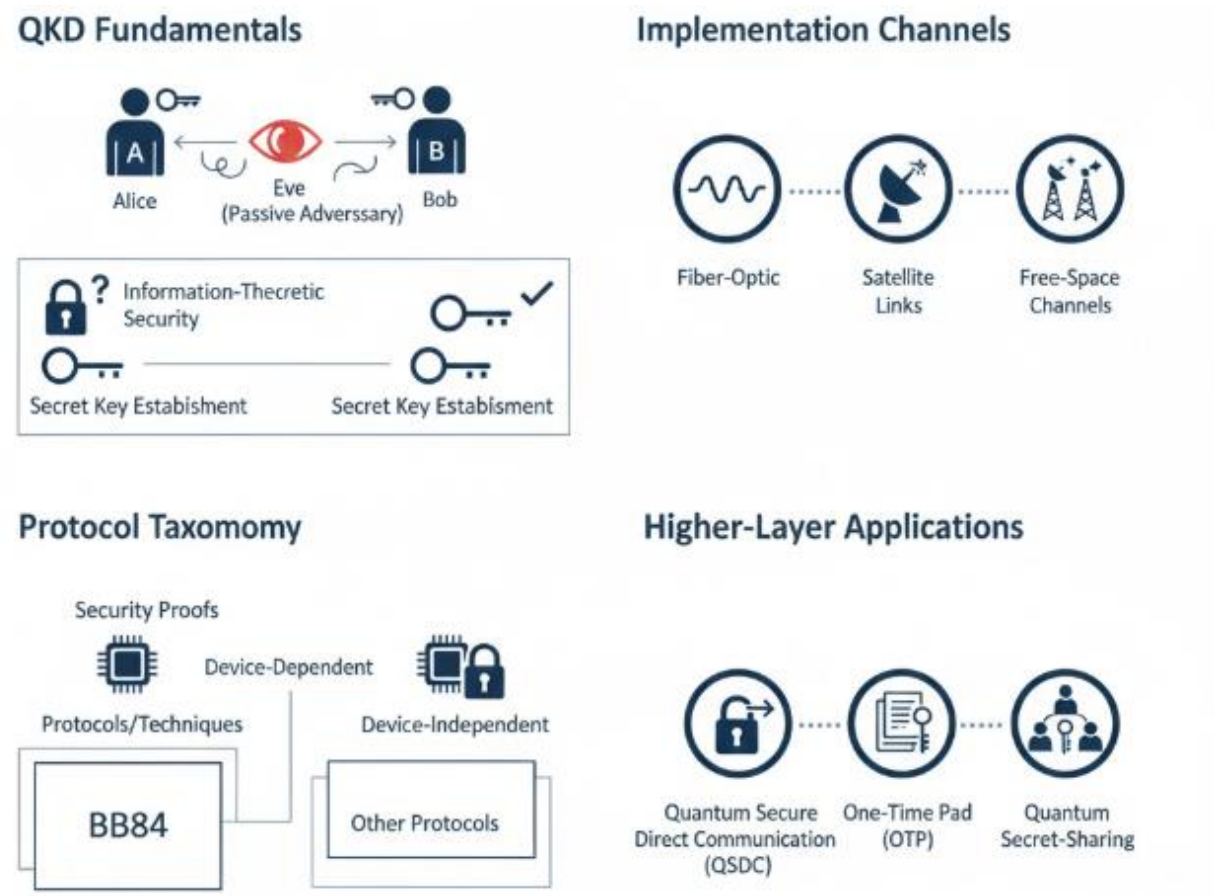
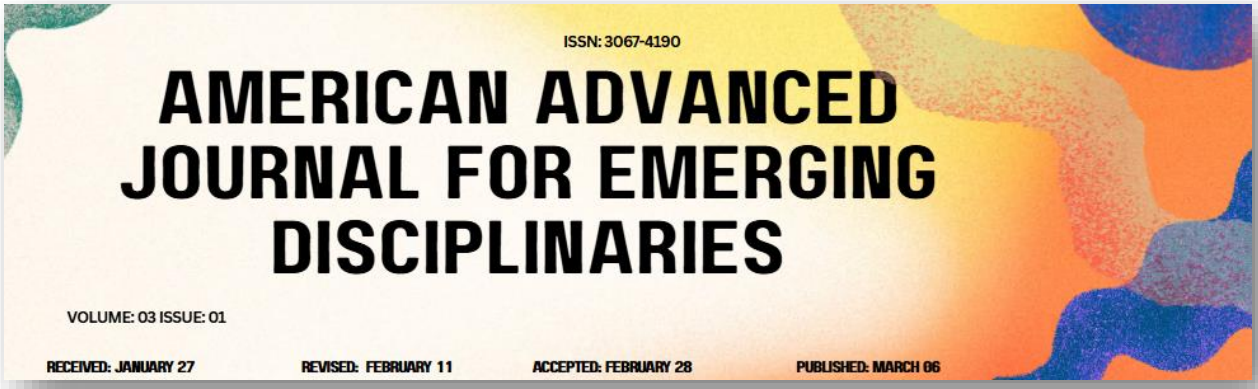


Fig 2: Information-Theoretic Security in Quantum Key Distribution: A Taxonomy of Security Proofs and Device Dependency

3.2. Quantum Teleportation and State Transfer

Quantum teleportation—a unique technique allowing the transfer of qubit information, even over considerable distances—provides a method for the transfer of general states. The teleportation process uses two qubits at spatially distinct locations that share an entangled state, typically a Bell state. The teleportation scheme, while intuitive, is best understood with the aid of mathematical notation and detail. Consider Alice, who possesses qubit \(\rho\) (whose state she

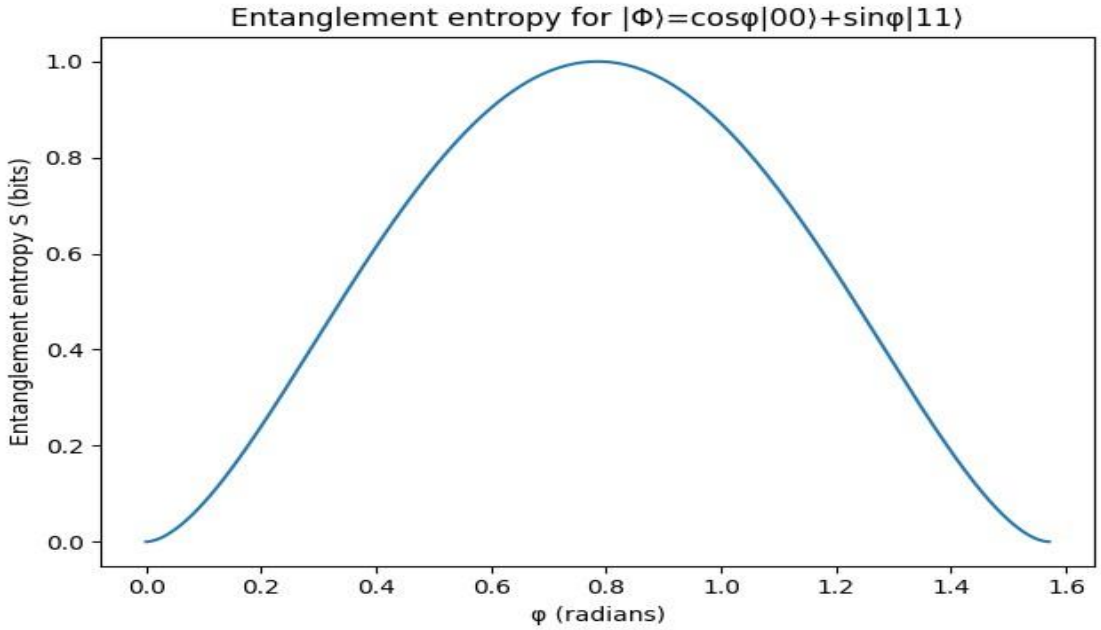


wishes to transfer to Bob) together with one qubit of a pre-established Bell pair. This allows Alice to perform a joint measurement on these two qubits in the Bell basis, yielding an outcome \(j\) with probability \(P(j)\). The result is subsequently communicated to Bob through a classical channel.

Bob (who possesses the second qubit of the Bell pair deemed by Alice to have been measured in the state associated with outcome \(j\)) then needs to perform the operation \(\mathcal{D}_j\) on his qubit to reconstruct Alice's original state. Because classical channels are not yet regarded as quantum channels, the teleportation process is not truly a transport process; the joint measurement at Alice's site increases the correlation of the two subsystems, while with the communication of the outcome, the correlation across the three systems reduces the total information content.

An undeniable, fundamental necessity for any quantum teleportation scheme is that an entangled state between the involved parties exists in order for state transfer to occur. If Alice and Bob separate their qubit states by a distance \(d > 0\) and an entangled state between the systems that they each possess is shared, then usually—although not always—quantum teleportation can occur. Quantum teleportation is, of course, not confined to just qubits; it is a general procedure for the teleportation of any two-dimensional quantum state, e.g., qudits. In particular, state teleportation can apply to multimode states in discrete and continuous degrees of freedom or any other quantum information carrier.

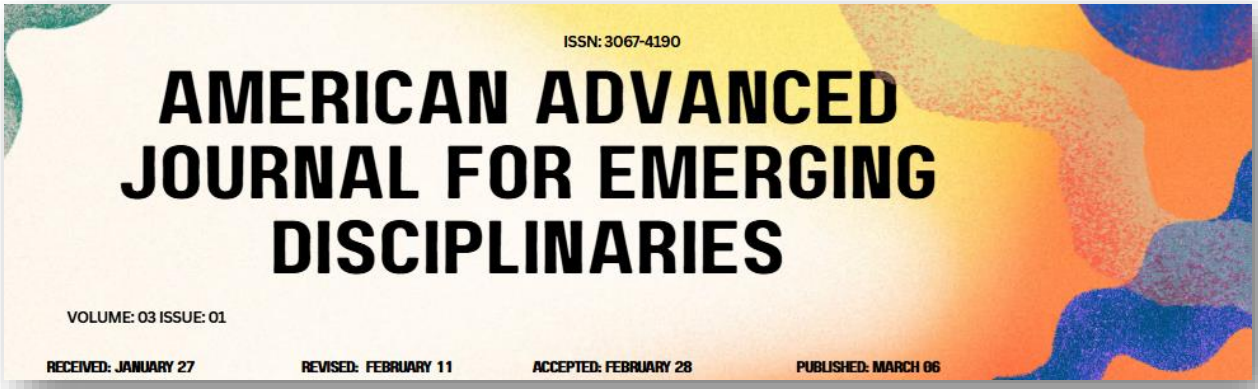
ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06



4. Architecture of the Quantum Internet

The architecture of the Quantum Internet is under discussion by various groups. The quantum internet comprises a set of global networked quantum devices with a dedicated Quantum Internet Protocols stack over a Transmission Control Protocol or Internet Protocol-style architecture. At any city level, perhaps even metropolitan level, these networks will be simpler to design and deploy. A telecommunication-stack-like architecture allows the design of layered protocols and network devices. Yet quantum networks are quantum–classical hybrids because quantum keys, secrets, and data must still be routed out of the Quantum Internet with classical channels. Introduction of dedicated quantum Network Control and Network Management Plane control functions are possible.

The architectural implications of this interplay of quantum–classical resources are not yet fully understood. Formulation of Quantum-Orchestrated Value Networks—cross-layer, cross-domain allocation of control, management, and service orchestration resources—will enable end-to-end QoS buying just as present telecommunication networks provide telcos the offering of high QoS paths across all available telecommunication end-to-end services. Telecommunication



people do not understand Transport Layers like the people who worked on Quantum Key Distribution in the first place. People in telecommunications are becoming even more comfortable with this and relaxing Transport Layer control whenever possible to accommodate emerging technologies. As Satan squeezed the juices from the loopers, so too is the Transverse Layer more accepting of new mind-bending ideas like quantum control celestial crossings.

Equation 2) Two-qubit pure state forms (Schmidt form + entanglement)

The states a two-qubit pure state can be written as

$$|\Phi\rangle_{AB} = \cos(\varphi)|00\rangle_{AB} + \sin(\varphi)|11\rangle_{AB}.$$

Step-by-step Schmidt decomposition idea (why this form is generic "up to local bases")

Step 1 (general two-qubit state):

$$\left|\Psi\rangle = \sum_{i,j\in\{0,1\}} a_{ij}\right| i\rangle_A|j\rangle_B.$$

Step 2 (view coefficients as a matrix): let

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}.$$

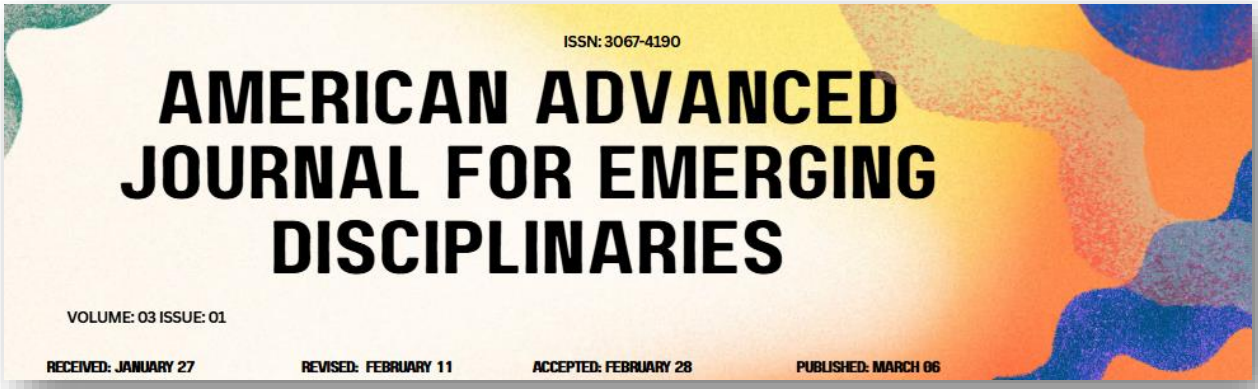
Step 3 (singular value decomposition): any complex 2×2 matrix has an SVD

$$A = U \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_1 \end{pmatrix} V^{\dagger},$$

where U, V are unitary and $\lambda_0, \lambda_1 \geq 0$.

Step 4 (absorb U, V into local basis choices): local unitaries correspond to basis changes on A and B, so in new local bases the state becomes

$$|\Psi\rangle = \lambda_0|0'\rangle_A|0'\rangle_B + \lambda_1|1'\rangle_A|1'\rangle_B.$$



Step 5 (parameterize Schmidt coefficients): normalization gives $\lambda_0^2 + \lambda_1^2 = 1$. Set

$$\lambda_0 = \cos\varphi, \quad \lambda_1 = \sin\varphi, \quad \varphi \in [0, \pi/2],$$

4.1. Network Layers and Protocol Stacks for Quantum Networks

Within the context of quantum communication networks, it can be useful to apply a layered architecture similar to that used for classical TCP/IP networks, as this allows consideration of individual elements which together enable the operation of the entire facility. Functions such as routing and scheduling, which are logically separated in classical networks yet tightly coupled in the quantum case, can be studied independently for particular deployment scenarios. The architecture of a quantum communication network can be considered at three levels: the interconnection layer, which is shared with the classical communication networks and consists of the physical assets operated by the telecommunications carrier; the quantum connection layer, which implements the quantum communication resources between end-users; and the control layer, which manages the dynamic operation of any bandwidth allocation or routing within the quantum resources. A wider view including both the quantum connections and their embedded classical channels is often represented as the quantum transport layer.

Logical protocols are often conceptualized using a layered approach similar to the OSI model. Network orchestration combines elements of the transport and control planes into a single layer, which schedules lightpaths or directs quantum key distribution (QKD) traffic based on the current status of all the layers below. Physical implementations of these layers must respect the unique requirements of quantum communications, especially those relating to split classical and quantum operation, attendant noise and loss characteristics, and the sensitivity to security threats. Although the security provided by the quantum capabilities ensures that the underlying classical channels do not need to be trusted, the interface with existing TCP/IP networks must be carefully considered to avoid introducing vulnerabilities that compromise the advantage of using quantum resources. The requirement for simple interoperation between quantum networks and the current Internet is particularly evident in metropolitan networks, where the distance covered by pure quantum communications is too short to maintain quantum advantage in security or multiplexing capability.

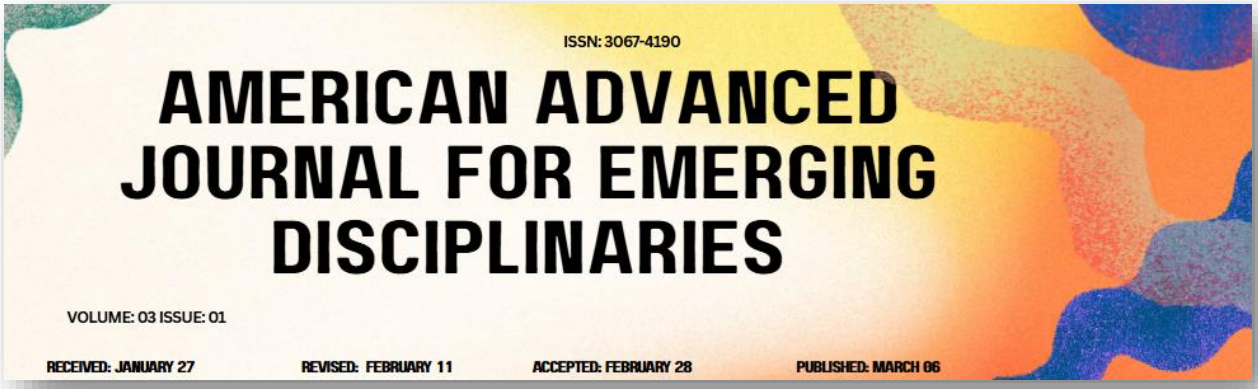
ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06

Security model	Main trust assumption	Practical trade-off
Device-dependent (trusted devices)	Alice/Bob devices behave as modeled	Simpler & higher rates, but vulnerable to implementation bugs/side channels
Measurement-device-independent (MDI)	Measurement device can be untrusted; sources still assumed characterized	Removes detector side-channel class; more complexity and lower rates
Device-independent (DI)	Minimal device trust; security from observed nonlocal correlations (Bell-inequality style)	Strongest assumptions relaxation; hardest experimentally (loss/noise sensitive)

5. Security, Privacy, and Certification in Quantum Networks

Security ensures that an entity's private communication cannot be monitored or tampered with. Privacy guarantees that even if a third party can access and analyze the communication, the secret keys remain unknown. Therefore, security and privacy are closely related. Users may accept certain risks, expressed by a security or privacy risk model. A risk assessment quantifies the expected costs borne by all parties involved. The risk depends on the security of the system or protocol and on the value of the information transmitted. Risk-active security proof methods, which account for the value of the secret key when determining security, are currently under investigation.

In classical and quantum settings, the security and privacy of keys can be defined. High-level security definitions have yet to be established for quantum networks with realistic detection devices, though they are available for quantum key distribution. Such a definition should capture both security and privacy and be consistent with existing risk-based definitions for quantum key distribution. In security definitions, it is assumed that the secret keys generated during the communication are not disclosed, regardless of the resources available to an adversary. A k-zero-secret-key-conditional-privacy definition requires that the third-party credentials conditioned on k keys defined by the communicating parties follow a distribution as close as possible to a specific distribution. The better the conditioned credentials' distribution, the more privacy the system has.



While technology for traditional Internet access control methods—such as user identification and secret key distribution—has been developed for three-party models, it is yet to be implemented in quantum networks. Users can be identified via a trusted third party, e.g., when entering a quantum network host. When accessing subnets via a router, a registration and authorization protocol based on a trusted third party may be used. A network gateway can establish concealment and anonymity for users applying virtual keys by means of quantum key distribution or classical methods. Besides concealment and anonymity, other modes of privacy, including full-location privacy, legitimate-location privacy, and full-launch-eavesdropping, have been explored. Various quantum communications require distinct modes of privacy. In addition to effective security assessment, the practical implementability, cost and robustness of these privacies remain open questions.

5.1. Security Models for Quantum Communication

Security is a first-order consideration for all networked information transfer services, since any exposed vulnerability is rapidly exploited by adversaries. The application of quantum mechanics opens up the possibility of information-theoretic security that cannot be achieved using classical channels, where confidentiality can only be mathematically guaranteed provided the adversary is limited in resources.

To be usable in practice, though, if quantum communication is to retain this clear advantage over its classical counterparts, it must also be secure in a more standard and extensive sense that incorporates the inevitable imperfections of the equipment used to implement the protocols and relies on more realistic trust assumptions—such as whether honest parties share \textit{trusted} devices or simply a common location. This gives rise to a range of security definitions and threat models for quantum networks, of which \textit{device-independent} and \textit{measurement-device-independent} definitions have received particular attention. The latter relax the trust assumptions imposed on the quantum devices to the greatest feasible extent, assuring security against entirely uncharacterized devices. Mathematically, such definitions provide security in the broadest possible sense, their proofs relying only on the presence of a quantum channel over which potentially-corrupted devices are connected.

Progress in these areas has enabled the derivation of \textit{composable security}, which is closely related to device-independent efforts in its pursuit of the fewest trust assumptions necessary for a sound security definition. However, rather than being a property of a specific

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06

protocol, it is a standard for the combination of multiple protocols to yield similarly-secure resources—the formal analogue of connected classical networks whose components have not been independently tested.

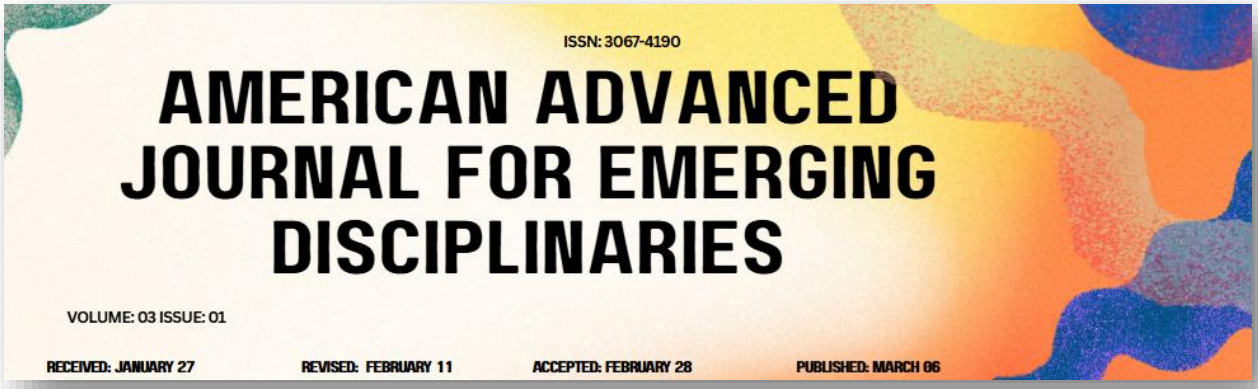


Fig 3: Beyond Theoretical Absolutes: Composable and Device-Independent Security Frameworks for Resilient Quantum Information Networks

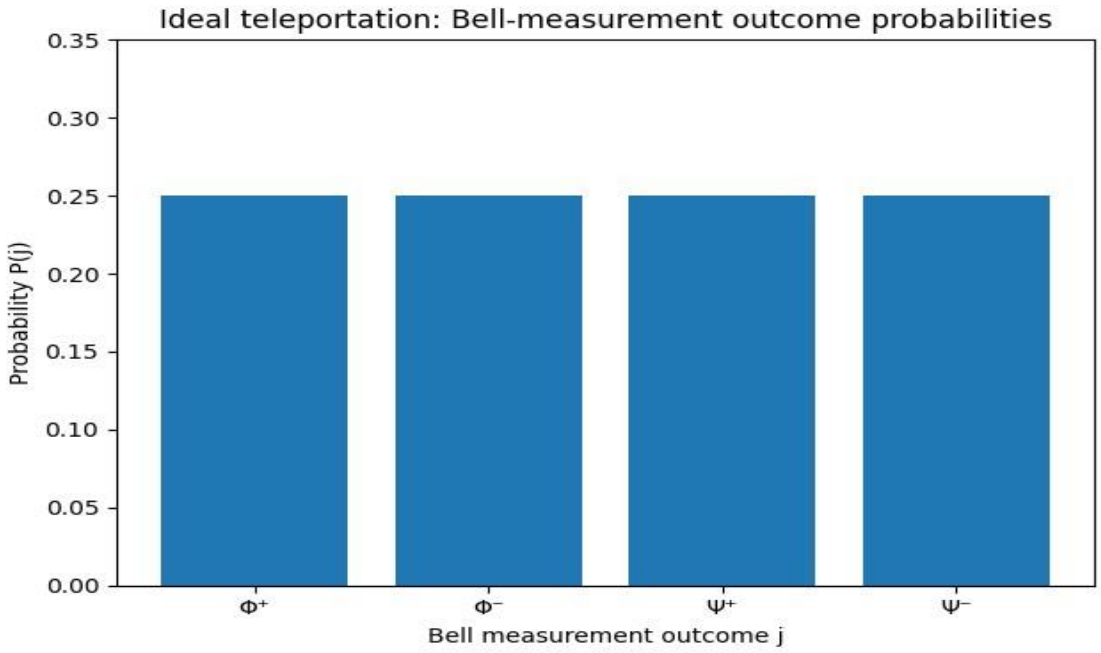
5.2. Device-Independent and Measurement-Device-Independent Protocols

Device-independent and measurement-device-independent approaches to security aim to achieve levels of security certification that can be implemented with the least amount of trust placed in the physical devices used for key distribution. Directly delivering a certified key without the assistance of a trusted quantum device is not achievable in the standard paradigm of quantum key distribution, even in the presence of a malicious eavesdropper. Losses and noise in real-life experimental implementations necessitate additional reconciliation and privacy amplification procedures that involve Alice and Bob relying on a central authority that accepts a quantum device of untrusted quality.

Moreover, whenever loss is substantial, it is unreasonable to place much trust in the security of the protocol, since the untrusted device of the setup can introduce additional information for the eavesdropper. In device-independent security, a source of entangled pair states can be placed at the center of control, Alice and Bob being spatially separated from it. In this case, the two sides only need to trust the pairs of correlations exposed by the source, while the devices in the two most distant locations can be assumed to be noisy. Thus the burden of trust is just put on the device that generates the quantum entanglement. These correlations can be accounted by any distribution of states and measurements satisfying the Bell inequalities.

In measurement-device-independent key distribution, the experimental implementations consider sources of quantum states that are relied upon for security. Only the measurement devices are replaced by those that are known to have been attacked. No other requirement is made about the amount of trust in the entangled pairs of states, thus both loss and noise can be asymptotically large, the limit now being set by the available capacity for reconciliation. In the experiments the commutation relation of the quantum measurement devices is also weakened, Alice and Bob allowing for different definitions of the probabilities of error for their protocol.

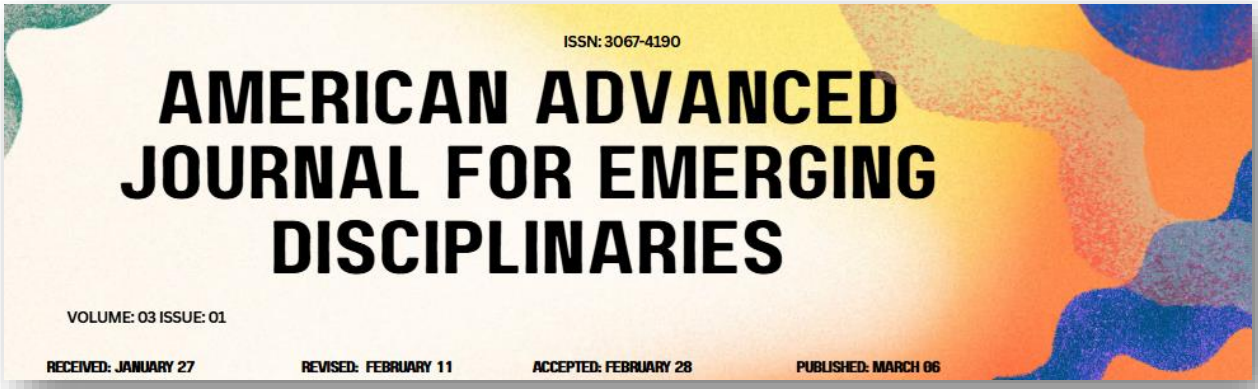
ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06



6. Experimental Realizations and Practical Deployments

Quantum networks have been demonstrated with nodes separated by a few tens of kilometers, but these have not yet reached the stage of a deployable, scalable quantum network. Here, current experimental realizations of quantum communication systems, some of which constitute the building blocks of a quantum network, are reviewed and gaps that still need to be bridged to achieve proper quantum networks are highlighted. These building blocks comprise efficient quantum light sources, single-photon detectors with high efficiencies, low-noise multiplexing technologies, long-distance fiber channels, free-space channels over metropolitan and long-haul distances, and the integration of quantum communication systems with the presently existing telecom infrastructure. All these elements have been realized in one way or another, but difficulties in terms of speed, costs, or scalability are still present.

Quantum communication systems operate on the same principles as classical telecommunication networks. However, these elements are not yet available at a sufficient level of maturity and scalability to support large-scale implementations of end-to-end quantum



networks. The quantum communication community, in its progress toward a full-fledged quantum internet, is therefore following the same path that classical telecommunication systems did a few decades ago. A first set of testimony in this direction is given by the development roadmaps of the major government-funded quantum communication initiatives in the US, EU, and China. These require not only the implementation of quantum channels —two trusted laboratories connected by a quantum channel that ensures a secret key distribution—is not sufficient for a scalable, operational system; two trusted nodes in a quantum network cannot be considered an operational end-to-end quantum communication system. Indeed, these are steps that can be pursued simultaneously: full end-to-end quantum systems for ideal cases are being implemented while the building blocks for full-scale quantum networks are being developed and tested.

Equation 3) Quantum teleportation: full algebra and the correction table

Teleportation: Alice measures in the Bell basis, gets outcome j with probability $P(j)$, and Bob applies $\mathcal{D}_j$.

Step-by-step teleportation derivation (standard, matches $\mathcal{D}_j$)

Step 1 (state to send):

$$|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1.$$

Step 2 (shared entanglement): assume Alice and Bob share

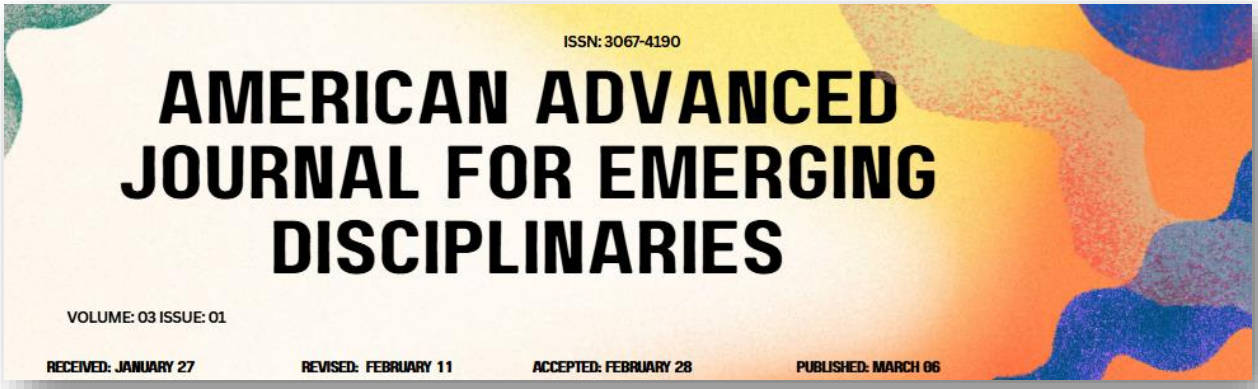
$$|\Phi^+\rangle_{BC} = \frac{|00\rangle_{BC} + |11\rangle_{BC}}{\sqrt{2}}.$$

(Alice holds B, Bob holds C.)

Step 3 (total 3-qubit state):

$$|\psi\rangle_A \otimes |\Phi^+\rangle_{BC} = (\alpha|0\rangle_A + \beta|1\rangle_A) \otimes \frac{|00\rangle_{BC} + |11\rangle_{BC}}{\sqrt{2}}.$$

Step 4 (expand):



$$= \frac{1}{\sqrt{2}}(\alpha|0\rangle_A|00\rangle_{BC} + \alpha|0\rangle_A|11\rangle_{BC} + \beta|1\rangle_A|00\rangle_{BC} + \beta|1\rangle_A|11\rangle_{BC}).$$

Step 5 (rewrite AB in Bell basis): using identities

$$\left|00\right\rangle = \frac{|\Phi^+\rangle+|\Phi^-\rangle}{\sqrt{2}}, \quad \left|11\right\rangle = \frac{|\Phi^+\rangle-|\Phi^-\rangle}{\sqrt{2}}, \left|01\right\rangle = \frac{|\Psi^+\rangle+|\Psi^-\rangle}{\sqrt{2}}, \quad \left|10\right\rangle = \frac{|\Psi^+\rangle-|\Psi^-\rangle}{\sqrt{2}},$$

you obtain (after grouping terms):

$|\psi\rangle_A|\Phi^+\rangle_{BC} = \frac{1}{2}(|\Phi^+\rangle_{AB}(\alpha|0\rangle + \beta|1\rangle)_C + |\Phi^-\rangle_{AB}(\alpha|0\rangle - \beta|1\rangle)_C + |\Psi^+\rangle_{AB}(\beta|0\rangle + \alpha|1\rangle)_C + |\Psi^-\rangle_{AB}(\beta|0\rangle - \alpha|1\rangle)_C)$.

Step 6 (measurement + correction):

- If Alice measures AB as $|\Phi^+\rangle$: Bob already has $|\psi\rangle \rightarrow$ apply I.
- If $|\Phi^-\rangle$: Bob has $Z|\psi\rangle \rightarrow$ apply Z.
- If $|\Psi^+\rangle$: Bob has $X|\psi\rangle \rightarrow$ apply X.
- If $|\Psi^-\rangle$: Bob has $XZ|\psi\rangle$ (equiv. Y up to global phase) $\rightarrow$ apply XZ.

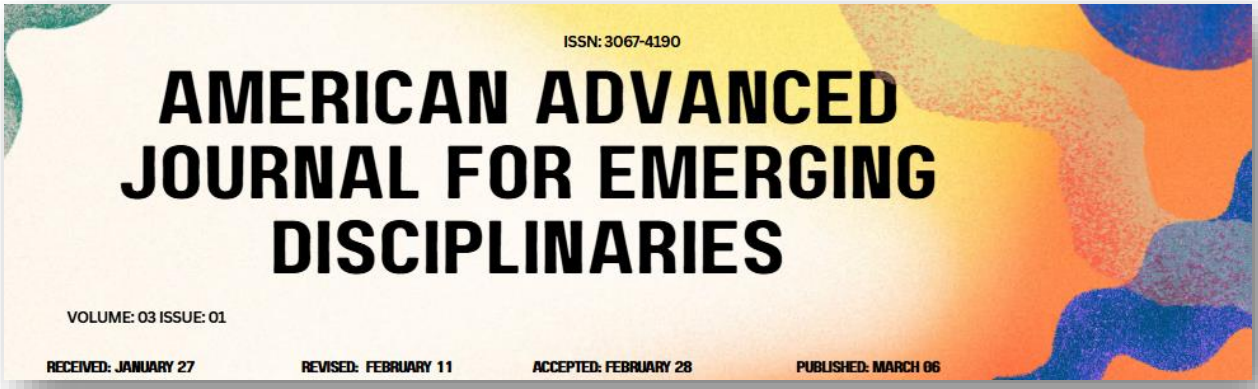
So the "operation $\mathcal{D}_j$" the article mentions is precisely a Pauli correction chosen by j.

Step 7 (probabilities): because each Bell component has amplitude $1/2$, in the *ideal* case

$$P(j) = \frac{1}{4} \quad \text{for each } j \in \{\Phi^+, \Phi^-, \Psi^+, \Psi^-\},$$

6.1. Photonic Implementations and Fiber Networks

On the experimental side, progress has been impressive, capturing many standard ingredients of quantum communication and networking. Multiphoton entangled sources have been built, with increasing numbers of sources and photons. Multiplexed detectors with good efficiency are available, as are detectors for time bins. The current record for the distance-integrated key rate in QKD is 3.5 × 1010 km−2, involving two space links and three ground



stations. Prototypes exist for primitive photonic repeaters, combining entanglement swapping with quantum relays. Quantum transmitters based on liquid crystals, including multiplexed devices, allow all spatial degrees of freedom—spatial, temporal, spectral, polarization—of photons to be prepared and manipulated.

In optical fiber links, the distance record is ≥830 km, achieved with full system testing. Channels can be multiplexed in time with short time slots, in frequency, and in the wavelength-division multiplexing of existing telecoms technology. Low-loss space links are being explored. Integration with existing telecoms for long-haul transmission is under development, and combinations of free-space transmission and optical-fiber links are realized in the NEXT experiment. Nevertheless, a substantial practical gap remains to be bridged before a quantum network with distributed entanglement can be realized.

7. Conclusion

Although quantum communication research has undergone impressive growth over the past three decades, these developments remain prescient and synthesis is essential. The literature on quantum communication protocols covers myriad tasks like key distribution, state transfer, teleportation, and entanglement swapping across ever-expanding distances; yet practical considerations have often been sidelined. The quantum internet will be a multi-layer network connecting quantum computers, memory nodes, and sensors using entanglement. Its implementation will thus require not just a new physical layer but also dedicated routing and

ISSN: 3067-4190
AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 11 ACCEPTED: FEBRUARY 28 PUBLISHED: MARCH 06

control planes that build on existing technology while accommodating emerging requirements.

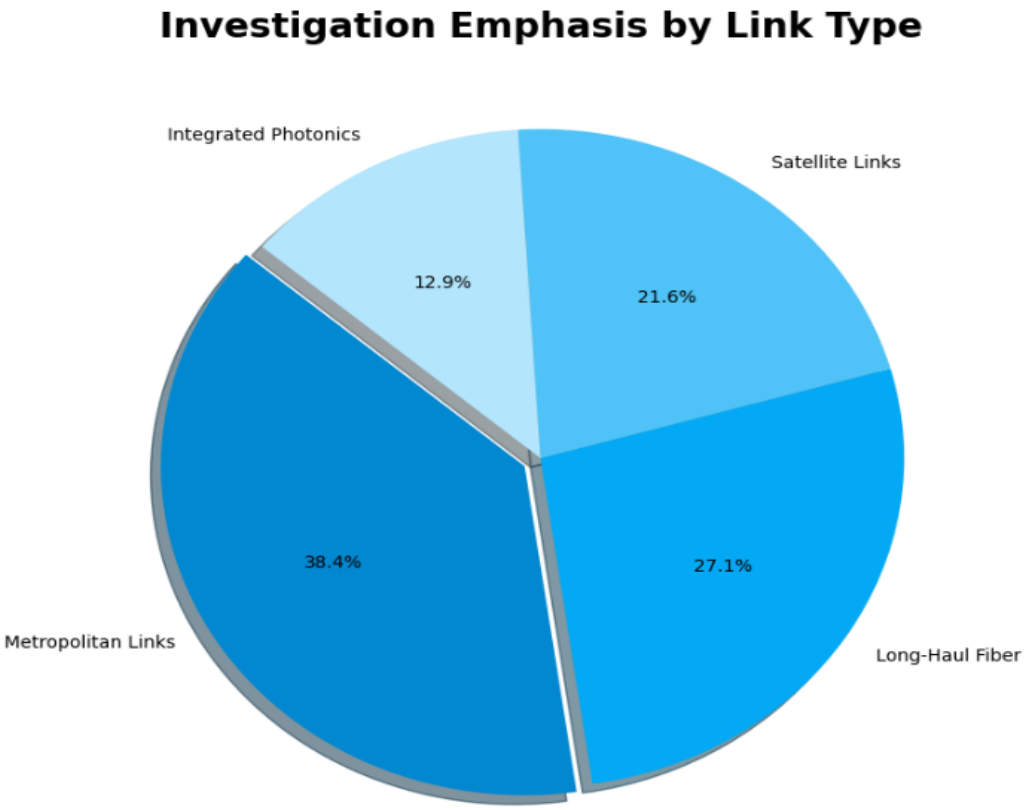
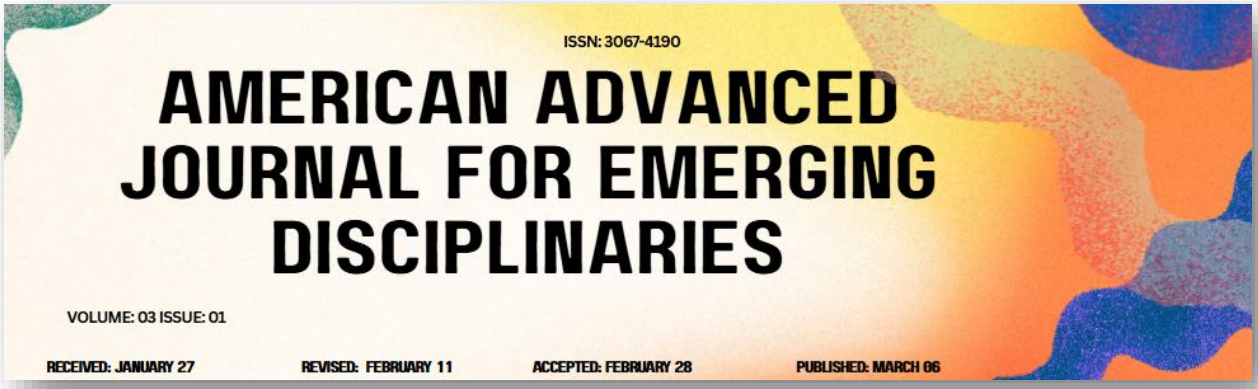


Fig 4: Investigation Emphasis by Link Type

As a result, the resulting synthesis identifies the core tasks already studied, maps the protocols employed, and assesses their performance under realistic conditions. Privacy concerns—arguably the most prominent cybersecurity problem of the present day—are also addressed, including security definitions and threat models. Recent architectural concepts are examined, with emphasis on interoperability and routing; the investigation focuses especially on composable-layer models capable of supporting metropolitan, long-haul, and satellite links. Ongoing experimental activity in integrated photonics and quantum telecommunications is reviewed, along with the scalability of current results and their relevance for prototypes. Finally,



conclusions highlight remaining challenges and define lines of inquiry for shaping future quantum networks.

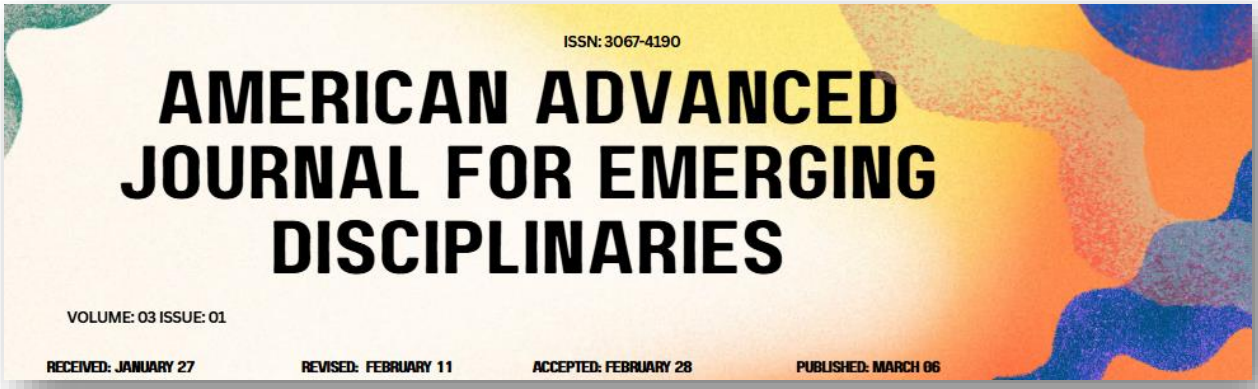
7.1. Summary and Future Directions in Quantum Communication

Research on quantum communication protocols and the quantum internet addresses the design and performance analysis of key quantum communication protocols and the architecture of the quantum internet. Milestones include the first elementary quantum communication protocols, initial formal sketching of quantum internet architectural layers and a first quantum routing protocol for entanglement connections. Quantum communication directly exploits distributed Quantum Mechanics to allow connected parties not only to share quantum states, but also to perform any of the tasks listed before. The protocols further allow a very general resource for communication, Networked Quantum Information (NQI). Such information can at least be used to perform teleportation, transfer of a general state, entanglement swapping, and Quantum Key Distribution (QKD). Thus, all tasks commonly considered in Quantum Communication are built in.

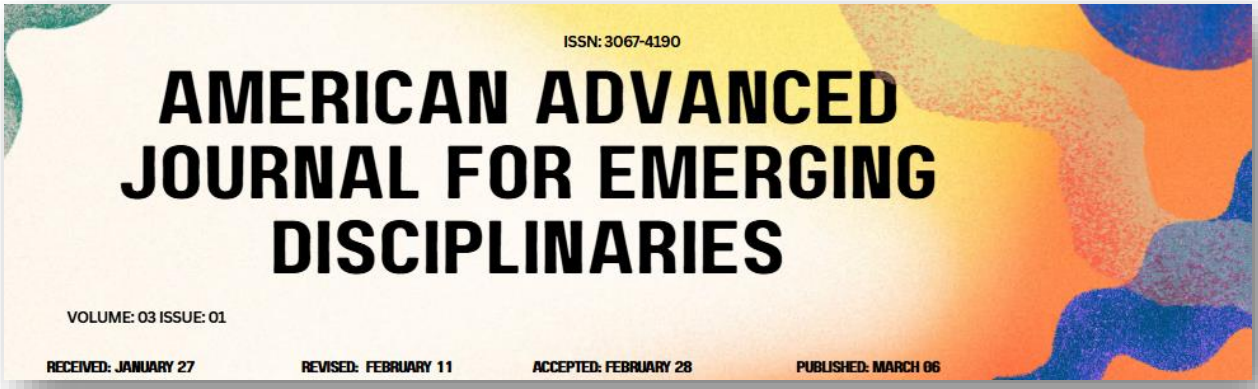
Quantum communication might sometimes outperform its classical development and sometimes fall short. For example, QKD guarantees provably secure keys—using the encapsulation theorem, consisting of a secret, but insecure classical channel. QKD-secure keys can allow secure but untrusted, and probably higher bit rate, teleportation. The proposed techniques and study shed some light on Quantum Communication and QKD from a different perspective, and open opportunities for future research. The Quantum Internet will initially consist of metropolitan networks, linked long-distance networks, and space segments; all networks at this stage are for research purposes only, and will have very limited user communities. Industrial deployment might be fully complete in some ten to twenty years from now.

References

[1] Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412), eaam9288.
[2] Kimble, H. J. (2008). The quantum internet. Nature, 453(7198), 1023–1030.
[3] Van Meter, R. (2014). Quantum networking. Wiley.



[4] Pirandola, S., Andersen, U. L., Banchi, L., et al. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236.
[5] Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. Nature Communications, 8, 15043.
[6] Bennett, C. H., Brassard, G., Crépeau, 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.
[7] Briegel, H. J., Dür, W., Cirac, J. I., & Zoller, P. (1998). Quantum repeaters. Physical Review Letters, 81(26), 5932–5935.
[8] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195.
[9] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., et al. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301–1350.
[10] Acín, A., Pironio, S., Vértesi, T., et al. (2012). Randomness versus nonlocality and entanglement. Physical Review Letters, 108(10), 100402.
[11] Pironio, S., Acín, A., Massar, S., et al. (2010). Random numbers certified by Bell's theorem. Nature, 464(7291), 1021–1024.
[12] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661–663.
[13] Lo, H. K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503.
[14] Pirandola, S., & Braunstein, S. L. (2016). Unite to build a quantum internet. Nature, 532(7598), 169–171.
[15] Pant, M., Krovi, H., Englund, D., et al. (2019). Routing entanglement in the quantum internet. npj Quantum Information, 5, 25.
[16] Kozlowski, W., Wehner, S., & Dahlberg, A. (2021). Architectural principles for a quantum internet. Quantum Science and Technology, 6(4), 044001.
[17] Dahlberg, A., & Wehner, S. (2019). Transforming graph states using single-qubit operations. Philosophical Transactions of the Royal Society A, 376(2123), 20170325.
[18] Murta, G., Van Meter, R., Caleffi, M., & Benjamin, S. C. (2020). Towards a quantum internet. IEEE Communications Surveys & Tutorials, 22(4), 2991–3031.
[19] Caleffi, M., Van Meter, R., & Zorzi, M. (2018). Classical control and management of quantum networks. IEEE Network, 32(6), 58–64.
[20] Gyongyosi, L., Imre, S., & Nguyen, H. V. (2018). A survey on quantum channel capacities. IEEE Communications Surveys & Tutorials, 20(2), 1149–1205.



[21] Takeoka, M., Guha, S., & Wilde, M. M. (2014). Fundamental rate-loss tradeoff for optical quantum key distribution. Nature Communications, 5, 5235.
[22] Wilde, M. M. (2017). Quantum information theory (2nd ed.). Cambridge University Press.
[23] Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information. Cambridge University Press.
[24] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.
[25] Sangouard, N., Simon, C., de Riedmatten, H., & Gisin, N. (2011). Quantum repeaters based on atomic ensembles. Reviews of Modern Physics, 83(1), 33–80.
[26] Humphreys, P. C., Kalb, N., Morits, J. P. J., et al. (2018). Deterministic delivery of remote entanglement. Nature, 558(7709), 268–273.
[27] Yin, J., Cao, Y., Li, Y. H., et al. (2017). Satellite-based entanglement distribution over 1200 kilometers. Science, 356(6343), 1140–1144.
[28] Wang, S., Chen, W., Yin, Z. Q., et al. (2020). Field and long-distance demonstration of a wide area quantum key distribution network. Optics Express, 28(3), 4164–4176.
[29] Calderaro, L., Agnesi, C., Dequal, D., et al. (2018). Towards quantum communication from global navigation satellite system. Quantum Science and Technology, 4(1), 015012.
[30] Azuma, K., Tamaki, K., & Lo, H. K. (2015). All-photonic quantum repeaters. Nature Communications, 6, 6787.
[31] Pirandola, S. (2019). End-to-end capacities of a quantum communication network. Communications Physics, 2, 51.
[32] Dahlberg, A., Skrzypczyk, P., Coopmans, T., et al. (2019). A link layer protocol for quantum networks. Proceedings of the ACM SIGCOMM Conference, 159–173.
[33] Cuquet, M., & Calsamiglia, J. (2012). Entanglement percolation in quantum networks. Physical Review Letters, 108(19), 190504.
[34] Van Meter, R., Satoh, T., Ladd, T. D., et al. (2016). Path selection for quantum repeater networks. Networking Science, 3(1–4), 82–95.
[35] Elkouss, D., & Wehner, S. (2021). Quantum network protocols. Annual Review of Condensed Matter Physics, 12, 301–329.