Quantum Internet—Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions

Amoldeep Singh, Kapal Dev, *Member, IEEE*, Harun Siljak, *Senior Member, IEEE*, Hem Dutt Joshi, *Member, IEEE*, and Maurizio Magarini, *Member, IEEE*

Abstract—The advanced notebooks, mobile phones, and Internet applications in today's world that we use are all entrenched in classical communication bits of zeros and ones. Classical Internet has laid its foundation originating from the amalgamation of mathematics and Claude Shannon's theory of information. However, today's Internet technology is a playground for eavesdroppers. This poses a serious challenge to various applications that rely on classical Internet technology, and it has motivated the researchers to switch to new technologies that are fundamentally more secure. By exploring the quantum effects, researchers paved the way into quantum networks that provide security, privacy, and range of capabilities such as quantum computation, communication, and metrology. The realization of Quantum Internet (QI) requires quantum communication between various remote nodes through quantum channels guarded by quantum cryptographic protocols. Such networks rely upon quantum bits (qubits) that can simultaneously take the value of zeros and ones. Due to the extraordinary properties of qubits such as superposition, entanglement, and teleportation, it gives an edge to quantum networks over traditional networks in many ways. At the same time, transmitting qubits over long distances is a formidable task and extensive research is going on satellite-based quantum communication, which will deliver breakthroughs for physically realizing QI in near future. In this paper, QI functionalities, technologies, applications and open challenges have been extensively surveyed to help readers gain a basic understanding of the infrastructure required for the development of the global QI.

Index Terms—Quantum mechanics, information theory, quantum computation, quantum communication and networking.

I. OUTLINE

QUANTUM Internet (QI) is trending Internet technology that facilitates quantum communication through quantum bits (qubits) among remote quantum devices or nodes. Such a technology will work in synergy with classical Internet to overcome the limitations posed by traditional interconnect technologies, as was highlighted in [1]. This novel technology stems from the laws of quantum mechanics, where one of the laws states that it is impossible to measure a property of a system without changing its state. Consequently, qubits cannot be copied and any attempt to do so will be detected, thus making the communication more secure and private [2]. The properties of qubits give an edge to QI over the traditional Internet in many ways [3].

Qubits also exhibit quantum *entanglement* [4], where qubits at remote nodes are correlated with each other. This correlation is stronger than ever possible in the classical domain. Entanglement is inherently private, as it is not possible, because of no-cloning [5], for a third qubit to be entangled with either of the two entangled qubits. Therefore, this quantum effect could open up a different galaxy of applications with world-changing potential [6], [7], [8], [9], [10], [11], [12], [13]. As qubits are prone to environmental losses, transmitting qubits over long distances is a challenging task due to *decoherence* [14]. Therefore, extensive research is going on to achieve long-haul quantum communication [15], [16]. To mitigate this noise, various techniques are employed, such as Quantum Error-Correcting (QEC) codes [17] and fault-tolerant techniques [18], [19], [20].

In the modern era, where the Internet plays a vital role in everyday life [21], providing secure communication and data privacy is of prime importance, ensuring no eavesdropping between two communicating parties [22]. On the technical side, some of the contemporary cryptographic techniques might be broken in the future, with the advent of quantum computers. New potential in cryptography emerges with advances in *quantum cryptography* that exploits quantum mechanical principle of *no-cloning*. These features play a vital role in providing secrecy and integrity to the data
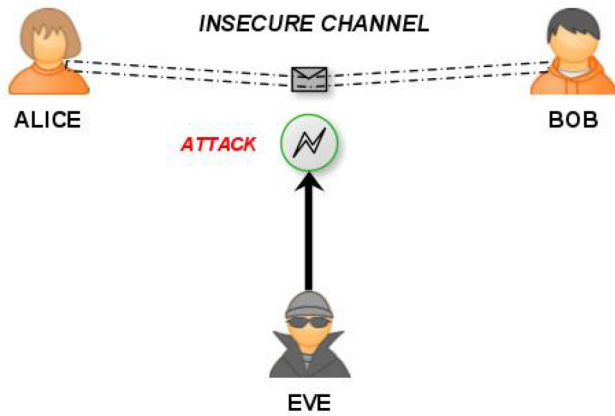
Fig. 1. Communication between Alice and Bob intercepted by *Eve*. Here, channel is insecure which means that information is not encrypted by a *cipher*, thus vulnerable to attacks by *Eve*.

Fig. 2. Vision of future quantum Internet working in synergy with classical Internet.

to be communicated, thus making messages unintelligible to any unauthorized party. If a malevolent third party, such as *Eve*, as shown in Fig. 1, eavesdrops on this key distribution, privacy of the communication will be compromised. This problem is addressed by the best-known application of quantum networking, i.e., Quantum Key Distribution (QKD), which provides secure access to computers on the cloud [23] utilizing various protocols. QKD networks are commercially available [24], [25], and are studied and deployed covering metropolitan distances [26], [27], [28], [29]. Long distance QKD networks with trusted nodes are also currently possible [26], [30]. Ultra-secure QKD protocols are developed based on well-accepted laws that govern quantum physics for sharing secret keys among two parties [9]. Further advances in the field ask for the significant interdisciplinary effort by research groups working on this novel technology to make it widespread [31], [32].

A. Quantum Race

A tremendous amount of effort is put together by scientists to realize global QI. As a result, infrastructures to realize this technology are extensively studied and new solutions are proposed. For instance, manufacturing of quantum computers is speeding up; various tech giants such as IBM, Google, Intel, and Alibaba have already started working on it. A 50-qubits processor has been built and tested by IBM in November 2017 [33]. Google has announced a 72-qubit processor [34] and recently, towards the end of 2019, the company has claimed to have entered a new era of incredible computational power by achieving "quantum supremacy," i.e., solving a computational problem that has not had a classical computing solution obtainable in a reasonable time span [35]. Intel and Alibaba are actively working on technologies to develop double-digit-qubits processors. In this quantum computing race, future quantum computers will come into force having disruptive potential to tackle complex problems such as understanding photosynthesis, improvising catalysts for formulating renewable fuels [36], [37], and complex Artificial Intelligence (AI) systems [38].
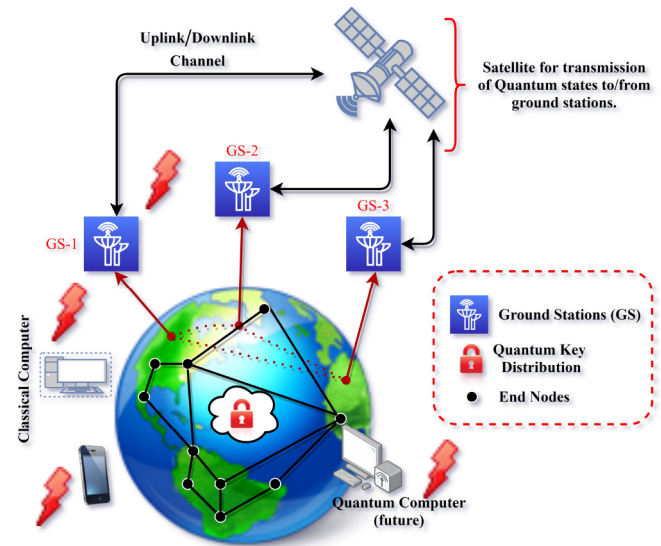
In the interim, European countries are also actively involved in building QI and, to boost the research, the European Commission has launched a ten-year €1-billion leading project [39]. In 2018, the European Union has announced its first grant of €132-million as an initiative in the quantum flagship for the following three years to speed up the quantum research [40]. Stephanie Wehner's group at the Delft University of Technology in the Netherlands has a strong vision for QI technology. This team is working to assemble the first authentic quantum network, which is planned to link four urban areas in the Netherlands [41]. They are coordinating in a large venture called Quantum Internet Alliance (QIA) and together with other scientists are trying to reach their goal to develop a blueprint for a pan-European entanglement-based QI [41]. This blueprint will set the stage for a strong European QI industry. Outside Europe, the U.S. government has earmarked nearly 1.3 billion U.S. dollars in funding for quantum research via its National Quantum Initiative Act, set to run from 2019 to 2023 [42]. In the year 2017, a research group from China has successfully demonstrated and observed a satellite-based distribution of entangled photon pairs to two separate ground stations on the earth, and with the successful launch of the Micius satellite, they have already set the first step to realize QI as a global network [43].

It is envisioned that a future QI will somewhat look like as seen in Fig. 2. It will have a network of remote nodes interconnected with each other with the help of multiparty entanglement and quantum teleportation using fiber-based or free space channels. The quantum effects of quantum mechanics will make this network secure using various QKD protocols. QEC codes will be required to encode the qubits carrying the information that will protect them from decoherence and environmental effects. With advancements in multi qubit processors, full scale quantum computers will come into force and, along with existing classical infrastructure, will revolutionize the world with inherently secure global QI.

TABLE I
COMPARISON OF THIS SURVEY WITH OTHER RELATED SURVEYS

Topics	Basics of Quantum Mechanics	Qubit Technologies	Quantum entanglement	Quantum Teleportation	Quantum Repeaters	Quantum Channels	Quantum Memories	QKD	End Nodes	Quantum error correction
Laszlo Gyongyosi and Sandor Imre (2019) [44]	√						√			√
Stephanie Wehner (2018) et al. [2]			√	√	√	√	√	√	√	√
Robert Bedington (2017) et al. [52]			√	√	√		√			√
Valerio Scarani et al. (2009) [50]			√	√	√	√	√			√
Angela Sara Cacciapuoti et al. (2020) [47]	√		√	√	√	√	√			√
Stefano Pirandola et al. (2015) [46]		√	√	√	√		√			
Gerardo Adesso and Fabrizio Illuminati (2007) [51]	√		√	√	√		√			
Hoi-Kwong Lo et al. (2014) [54]			√	√			√			√
Laszlo Gyongyosi et al. (2018) [48]	√		√			√	√			√
Feihu Xu et al. (2020) [49]			√		√	√	√	√	√	√
Stefano Pirandola et al. (2020) [55]			√			√	√	√	√	√
Zunaira Babar et al. (2018) [56]	√		√							√
Nedasadat Hosseinidehaj et al. (2019) [53]	√		√			√	√	√	√	√
This Survey	√	√	√	√	√	√	√	√	√	√

B. Motivation and Contribution

There are some specific surveys and review papers available that include the research work accomplished in particular aspects of QI and underlying technologies, but no generalized reviews. A brief comparison of this survey with other published surveys on quantum networking is presented in Table I. It is worth noting that several published surveys are specific to certain concepts such as quantum computing [44], quantum cryptography [45], quantum teleportation [46], [47], quantum channel capacities [48], quantum key distribution [49], [50], quantum entanglement [51], and satellite based quantum communication [52], [53]. Motivated by this, we have adopted a generalized approach targeting the wide audience to appreciate the advantages of quantum communication over the classical one, with the following contributions.

- The basic concepts of quantum mechanics that are required to have an in-depth knowledge of quantum communication are put forth.
- We provide enough tutorial content by highlighting the functionalities of QI, followed by possible applications it can offer, and by underlining the challenges it can face with.
- We cover all the components of QI explicitly so that even the readers without quantum related background can easily understand the preliminaries governing this novel technology.

- We bring all the components of QI together, which are required to build the global quantum networks, by outlining their historical developments with communication perspective.

The rest of the paper structure is detailed as shown in Fig. 3. Section II starts with the preliminaries of quantum mechanics that are required to understand the basic concepts needed for quantum computation and communication. In Section III, different technologies adopted to represent qubits are listed. This is followed by reviewing the functionalities of QI in Section IV, which includes quantum teleportation, quantum repeaters, quantum channels, quantum memories, QKD, and end nodes. In Section V, some of the applications that have been discovered theoretically by researchers are listed and reviewed. After that, in Section VI, challenges faced in realizing QI are analysed, such as decoherence, imperfections faced by quantum teleportation process, entanglement generation, and distribution of quantum states. Finally, in Section VII, future perspectives are discussed followed by concluding remarks and research directions for the realization of the global QI.

II. PRELIMINARIES

In this section, we study the basics of quantum mechanics with an emphasis on qubits. We discuss the mathematics behind single qubit and multi qubit systems, state vector

Fig. 3. Structure of the paper.

representations on the Bloch sphere, and the basic quantum gates.

A. Quantum Mechanics

Quantum mechanics is a discipline with a continuously increasing importance in today's world applied with colossal success in many fields of science and technology including physics, chemistry, AI, life sciences, and military applications. It is formulated as a mathematical framework, or set of rules, for the development of physical hypotheses by exploiting the properties of single quantum systems involving qubits. For harnessing the power of quantum mechanics in various applications, the study of the qubit and of the single quantum system is of utter importance. It has the potential to offer secure communications [57] that can make them cryptographically as secure as the One-Time-Pad (OTP) [58], unlike today's classical communication and cryptography with its vulnerabilities. For better understanding the quantum effects of quantum mechanics, certain theorems [59] were postulated by physicists to get a clear view of properties of qubits.

1) State Space and Superposition Principle: An isolated or closed system of qubits is associated with complex Hilbert space, also known as the *state space* of the system. A unit vector completely describes the state vector of a system in its state space. A qubit is the simplest quantum mechanical system that can be represented geometrically by a Bloch sphere, as depicted in Fig. 4. Any *pure* quantum state $|\psi\rangle$ can be represented by a point on the surface of the Bloch sphere with spherical coordinates of θ as polar angle, i.e., angle that a line makes with Z-axis, and ϕ as an azimuthal angle, i.e., angle that line makes with X-axis [60]:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \tag{1}$$

where "$|\cdot\rangle$" is called a "ket-vector" in *Dirac notation*, which physically represents the pure quantum state of the qubit. The angle ϕ represents the *phase* of a quantum state $|\psi\rangle$. Every individual state in the Bloch sphere is represented by a two-dimensional (2D) vector, where $|0\rangle$ and $|1\rangle$ are its basis vectors that are orthogonal to each other. States that can be represented
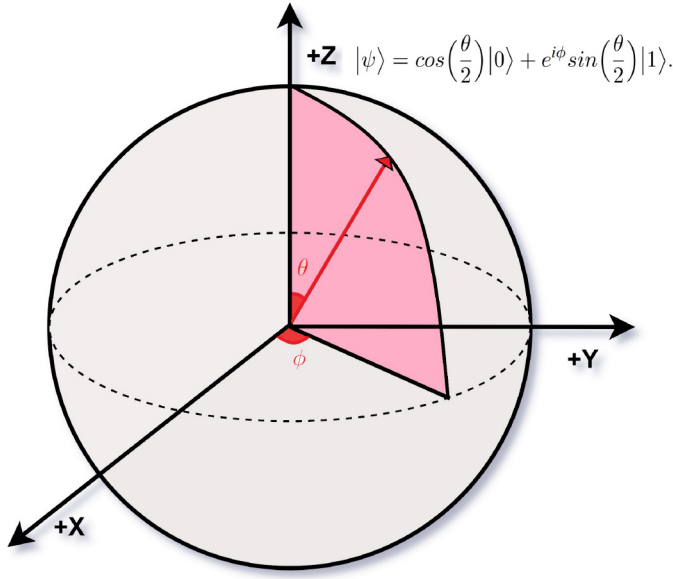
Fig. 4.   Bloch sphere: Geometrical representation of pure quantum state of a qubit. Here any state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be shown by a point on the surface of the sphere, where $\alpha = \cos(\frac{\theta}{2})$ and $\beta = e^{i\phi}\sin(\frac{\theta}{2})$.

by a "ket-vector" are known as *pure quantum states*. In comparison, *mixed states* are mixtures of pure states, resulting in probabilistic results when measured. It is a system with weak state or whose state is not fully defined, written in infinitely many different ways as probable outcomes of well-defined pure states [47], [61]. The pure state, given in equation (1), upon measurement results in either state $|0\rangle$ or $|1\rangle$, as depicted by *Copenhagen interpretation* [62].

While in classical communication, the transmission of information takes place in the form of bits taking either "0" or "1" value, the quantum communication on the other hand uses qubits that can be in a *superposition* of the two basis states simultaneously taking the value of "0" and "1" [63]. The result of measurement of such states is not definite $|0\rangle$ or definite $|1\rangle$. The principle of superposition can be best understood by visualizing the polarization state of a photon. At 45 degree of polarization, a photon is simultaneously vertically and horizontally polarized, representing both states at the same time [3]. A famous thought experiment paradigm of superposition principle is *Shrödinger's cat*, where the cat is, as colloquially interpreted, simultaneously dead and alive as a result of random event that may or may not occur [64].

2) Measurement of Quantum State: As discussed above, a qubit upon measurement will collapse it into one of the basis states [4]. This property of qubits is very well utilized in keeping the communications secure as any measurement of quantum state by *Eve* will affect its state irreversibly. In (1), the coefficients of $|0\rangle$ and $|1\rangle$ represent the probability amplitudes and their squares represent the probabilities of getting "0" and "1" upon measurement. The value of probability amplitudes of the quantum states greatly affects the outcome of measurement and these can be manipulated by quantum gates that will be discussed in Section II-D. Measurements can also be understood with the help of the Bloch sphere, as earlier discussed. If

the measurement is performed along the Z-axis, the result will be "0" or "1." If it is performed along the Y-axis, the result will be $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}i|1\rangle$ or $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}i|1\rangle$. The positive X-axis is pointing towards the reader, the state is $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ and any measurement performed in this direction will result in any one of these states.

3) Quantum No-Cloning: This theorem, which was first formulated by Wooters, Zurek and Deiks in 1982 [5], states that the quantum state of any particle carrying a qubit in a quantum channel cannot be either copied, amplified or cloned, thus making it a reliable and secure form of communication. Any attempt to clone it will be detected, further activating the QKD protocols [65]. However, at the same time, no-cloning prevents qubits to be sent over long distances by amplification or sending copies of qubits, as it is done in classical communication, for efficient detection of bits without any loss of information. For this purpose, *quantum repeaters* are studied to solve the problem of long distance communication of qubits, which is the core functionality required for full-scale QI.

B. Single Qubit System

In classical digital communication systems, the information is encoded in the form of binary bits. The bit represents a logical state with one of two possible values, i.e., "1" or "0". On the other hand, in quantum communication, instead of bits, qubits are employed to carry quantum information from source to destination. A qubit can be imagined as a *two-way system; direction of polarization of a photon, the up or down spin of an electron, or two energy levels of an electron orbiting an atom.* For instance, the electron can exist in either "ground" or "excited" state in an atom, represented by a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|0\rangle$ and $|1\rangle$ corresponds to ground state and excited state, respectively. By directing light on the atom at the right time and the right intensity, it is possible to move the electron from the $|0\rangle$ state to the $|1\rangle$ state and the other way around. Manipulating the time interval of the light, an electron, at first, in the state $|0\rangle$ can now be moved somewhere between $|0\rangle$ and $|1\rangle$, into $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ state, i.e., superposition of basis states. The variables α and β are complex numbers representing probability amplitudes, which means that $|\alpha|^2$ is the probability of getting $|\psi\rangle = 0$ as a result of the measurement on qubit $|\psi\rangle$ and $|\beta|^2$ is the probability of getting $|\psi\rangle = 1$ as a result of the measurement on qubit $|\psi\rangle$. It must be satisfied that,

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

A classical bit is like a coin resulting in definite outputs of heads or tails. Supposing, a qubit with $\alpha = \beta = \frac{1}{\sqrt{2}}$, will be in the state:

$$|\pm\rangle = \frac{1}{\sqrt{2}}|0\rangle \pm \frac{1}{\sqrt{2}}|1\rangle, \tag{3}$$

which gives a result 0 with 0.5 probability and result 1 with 0.5 probability, when measured over the time. This state often plays a vital role in quantum communication and is denoted by $|+\rangle$ and $|-\rangle$. Despite qubit theoretically having the capacity of carrying an infinite amount of information, all quantum states

collapse to a single state of 0 and 1 upon measurement and the reason for this characteristic is still unknown.

C. Multiple Qubits

In Section II-B, it was seen that a single qubit system is 2D but, in the real world, more number of qubits are required for complex computations to gain full advantage of quantum postulates. Hence, there is also a need to study multiple qubit systems. For instance, a two-qubit system will have four computational basis states denoted by $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. The quantum state for a pair of qubits is represented by state vectors having their respective amplitude coefficients as

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle. \quad (4)$$

Similar to the condition that has been discussed for a single qubit, the measurement result of (4) occurs with probability a_{00}^2 for $|00\rangle$, a_{01}^2 for $|01\rangle$, a_{10}^2 for $|10\rangle$, and a_{11}^2 for $|11\rangle$. If $x =$ 00, 01, 10, 11, then normalization condition is $\sum_x |a_x|^2 = 1$. Thus, it can be seen that with the addition of single qubit, the computational basis states are increased exponentially thereby giving space for complex computations that were beyond reach with classical resources.

1) Bell States or EPR Pairs: EPR is the name which came from famous paradox raised by three scientists Einstein, Podolsky, and Rosen in their famous paper *"Can a quantum mechanical description of physical reality be considered complete?"*, where unintuitive properties of Bell states were pointed out [66]. In a two qubit mechanical system, Bell states are mathematically expressed as:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle, \quad (5)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle, \quad (6)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle, \quad (7)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle. \quad (8)$$

The two particles in these Bell states are termed *EPR pairs* and are responsible for entanglement generation and distribution in the case of quantum teleportation, which is the key functionality of QI. *EPR pairs* are generated by various schemes (Section III-A) and are sent to Alice and Bob so that any measurement at Alice's qubit is the same as performed on Bob's qubit, which is justified because they share entangled qubits of an EPR pair. A Bell state has the property that when the first qubit state is measured, it results in two outcomes, i.e., 0 with $\frac{1}{2}$ probability and 1 with $\frac{1}{2}$ probability leaving the post-measurement state to be $|00\rangle$ and $|11\rangle$, respectively. Due to this, if the second qubit is measured, it results in the same outcome as the first qubit. This explains the interesting *correlation* between these two qubits. Even if some local operations are applied to the first or second qubit, these *correlations* still exited because of entanglement. EPR's paradox was improvised by John Bell in [67], where it is stated that these measurement correlations in the Bell state are much stronger than anything possible in classical systems. This
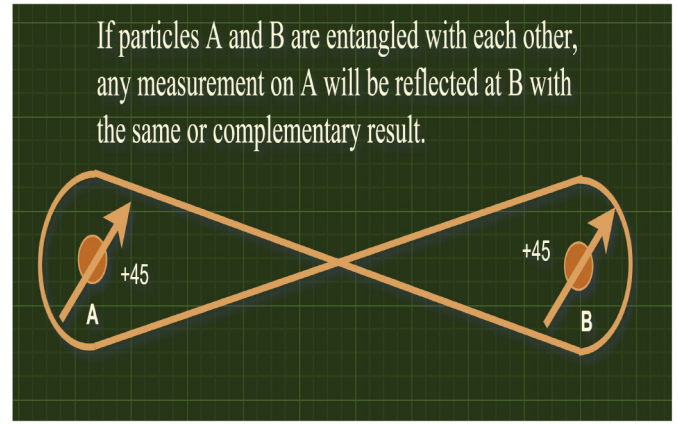

Fig. 5. Entanglement: Two particles **A** and **B** are correlated with each other even if they are a long distance apart. If any measurement is done at **A** having spin $+45$, then the same is reflected at **B**. This happens due to the weird phenomena of quantum entanglement.

enables processing of the information that goes well beyond what is possible in the classical world.

2) Entanglement: Quantum entanglement, shown in Fig. 5, is the phenomenon of correlation between two pairs of qubits that are separated by a physical distance, such that any random measurement on entangled qubits will generate the same set of random outcomes [68]. The concept of *quantum entanglement*, which is governed by laws of quantum mechanics, is the core functionality for many applications and does not have any counterpart in *classical communication*. As discussed in the Section II-C1, an EPR pair is a maximally entangled pair of qubits that are in a superposition. Independently measuring these qubits results in a random distribution of "1" and "0" in equal probability. This means that the state of entangled qubits is instantaneously fixed when the other pair of an entangled qubit is measured. Entanglement does not allow any exchange of information between remote nodes, rather it allows obtaining only mutual information. For information exchange, qubits can be transmitted between remote nodes without actually sending them from source to destination by the phenomenon of quantum *teleportation* [47], [69], which is fundamental for quantum networks [70]. An unknown quantum state can also be transmitted through quantum teleportation from source to a destination over long distances with the aid of EPR pair and local operations.

The concept of *entanglement* was first recognised by Einstein *et al.* in 1935 [66] and the phenomena of entanglement was originally given by Schrödinger in the same year [64]. It was also termed as *spooky action at a distance* by Einstein. After that, Bohm investigated the two quantum particles, that were entangled to each other, are now termed qubits [71]. Later on, Bell in his research [67] come up with a theorem to experimentally test the question of the locality and reality of entanglement. This development motivated various researchers to create entangled particles in labs [72], [73], [74]. A series of experiments practised in 2015 covered all the experimental loopholes that were present before [75], [76], [77]. Using entanglement for communication in technical applications is not clear, because entanglement

itself does not allow information transmission. However, it can help to build a virtual secure channel or a cryptographic channel [9]. Systems with multiple particles involved are represented by 2^n-Dimensional state space. It can be seen that, with the addition of a single qubit, the computational basis states are increased exponentially, thereby giving space for complex computations which are impossible in classical communication systems. A system of this type is described by the Greenberger–Horne–Zeilinger (GHZ) theorem [78], which is different from Bell's theorem [67] in the context of deterministic nature of the predicted outcomes. The application of the GHZ theorem is that multi-particle entanglement can be used for QEC [79]. These ways high-dimensional entangled EPR pairs are developed and proved advantageous in quantum theory [80].

D. Quantum Gates

Quantum computations rely on quantum gates for changing or manipulating the states of qubits. A quantum computer is built using quantum circuits that contain various gates and wires to manipulate the information stored in qubits. Using these quantum gates, quantum circuits can be built that can entangle and teleport qubits from Alice to Bob. In this section, some of the famous quantum gates are discussed, which are the building blocks of various quantum circuits required to build a full-fledged quantum computer.

1) Single Qubit Quantum Gates: Single qubit operation in quantum domain is simply defined by any rotation about the axis of the Bloch sphere as shown in Fig. 4. These rotations can be defined by Pauli matrices [81]. Certain transforms are defined for $180°$ rotations and are given by:

$$Pauli - X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{9}$$

which is represented as transformation along X-axis. Similarly, for transformations along Y-axis and Z-axis, the matrix representation is given by:

$$Pauli - Y \equiv \begin{bmatrix} 0 & -i \\ i & 0, \end{bmatrix}, \tag{10}$$

and

$$Pauli - Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{11}$$

respectively. Equation (9) is the matrix representation of quantum NOT-Gate. *Pauli*-X can be manipulated with a $90°$ ($\pi/2$) rotation along Y-axis after $180°$ (π) rotation about the Z-axis yielding a Hadamard gate transform represented by the following matrix:

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{12}$$

2) Multiple Qubits Gate: In practice, more than one qubit is involved in computations. Hence, studying manipulations on multiple qubits is important to understand the insights. A *controlled*-NOT (CNOT) gate is the widely used multi-qubit logic gate, which has *target* qubit and *control* qubit as the inputs of the CNOT gate. If the *control* qubit is kept one,

TABLE II
TRUTH TABLE FOR CNOT-GATE

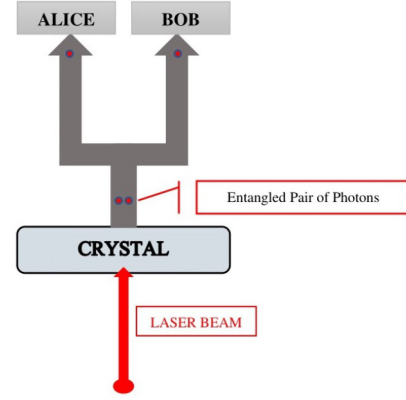| Input		Output	
Control Qubit	Target Qubit	Control Qubit	Target Qubit
0	0	0	0
0	1	0	1
1	1	1	0
1	0	1	1

Fig. 6. Parametric Down Conversion: Generation of entanglement by incident of laser beam to a crystal.

target qubit is inverted at the output; if the *control* qubit is kept zero, the *target* qubit retains its original state. To understand the operation, a truth table is shown in Table II and its matrix transform is:

$$CNOT_{Gate} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{13}$$

III. ENABLING TECHNOLOGIES

This section starts with a brief introduction to quantum entanglement and the schemes adopted for its generation and distribution. The technologies adopted for representing the qubits toward quantum computation and networking are studied. All the schemes and the choices for the selection of qubits are summarized in Table III.

A. Entanglement Generation and Distribution

Entanglement is a counter-intuitive form of correlation that has no correspondence in the classical domain, as discussed earlier. Random results can be obtained by individually measuring any qubit forming an EPR pair and the two independent measurements result in an outcome that is either directly or complementary related. In particular, for exchange of information between two remote nodes through quantum teleportation, entanglement generation and distribution are the key ingredient in this process [82]. Some schemes adopted for generation and distribution of EPR pairs between Alice and Bob, which are long distance apart, are discussed in what follows.

1) Spontaneous Parametric Down Conversion: In this scheme, which is depicted in Fig. 6, photons are employed for

TABLE III
CHOICES FOR QUBIT TECHNOLOGY SELECTION

| Design questions	Design choices		
	Entanglement generation		
Entities in entanglement	Photon-Photon: Spontaneous Parametric Down Conversion	Photon-Atom: Single atom excitation	Atom-Atom: Two atoms excitation
Technical overhead vs. success rate	more overhead, high success rate: deterministic interface	less overhead, non-deterministic: heralded interface	
Features	Qubit technologies		
Reusing existing semiconductor production	Solid State Approach		
Cheap production at current scale	Superconducting approach		
Low cost of running	Photonic approach		
High connectivity	Ion trap approach		
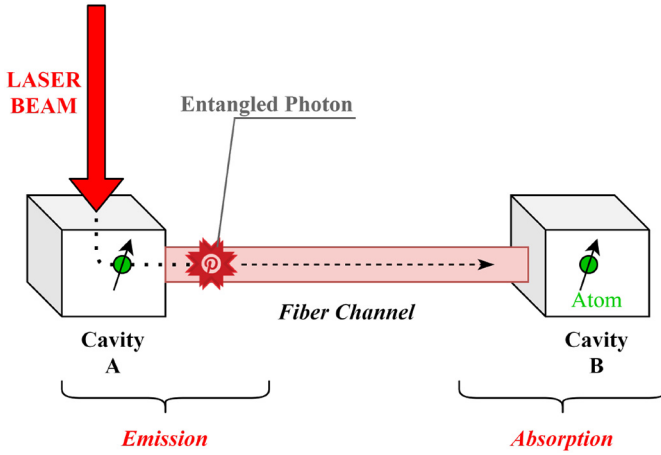
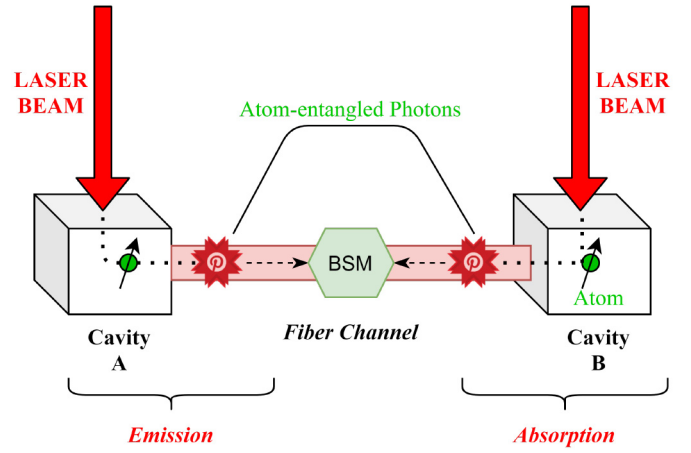Fig. 7. Entanglement generation by single atom excitation.

Fig. 8. Entanglement generation by two atoms simultaneous excitation by laser pulse.

entanglement generation and distribution between two remote nodes by the incidence of the laser beam on a crystal. The use of photons is advantageous as they can travel at high speed and can cover a long distance in fiber channels with the least amount of attenuation. Thus, photons are promising candidates for the entanglement creation [83], [84]. The photons are also associated with moderate amount of decoherence and noise as they least interact with the environment [47]. In the optical parametric down conversion method, a laser beam is incident on a birefringent crystal, which converts photon beams into pair of correlated photons with the help of non-linear effects of crystal [85]. The entangled photons are vertically and horizontally polarized and individually transported to Alice and Bob through a quantum channel, so that any measurement at Alice is reflected at Bob irrespective of the distance between them.

2) Single Atom Excitation by Laser Beam: A different scheme, as shown in Fig. 7, can be employed for entanglement generation and distribution. In this, atoms coupled firmly with an optical cavity are excited by a laser source, resulting in the radiation of atom-entangled photons that departs from the cavity C_A and travels through quantum channel reaching another cavity C_B, where the photons are absorbed coherently, thus mapping the polarization of photon onto the state of

remote atoms. In this way, two atoms are remotely entangled by photons [86], [87].

3) Two Atoms Simultaneous Excitation by Laser Beam: In this scheme, two atoms are simultaneously excited by the incidence of a laser beam on cavities C_A and C_B resulting in radiation of two atom-entangled photons. These atom-entangled photons depart from C_A and C_B, as shown in Fig. 8, and travel along the quantum channel where the Bell State Measurement (BSM) takes place. BSM is a scheme that is utilized for the generation of maximally entangled Bell states based on Hong-Ou-Mandel (HOM) interference, where two photons interact with each other at a beamsplitter (BS) [88]. It performs a joint quantum measurement on the state of these atom-entangled photons resulting in entanglement swapping operation [89], discussed in Section IV-B, distributing entanglement between remote atoms [90], [91], [92].

B. Qubit Technologies

1) Cavity Quantum Electrodynamics: Cavity quantum electrodynamics (cQED) refers to qubit technology where coherent interaction takes place between matter qubits such as quantum dot systems, trapped ions, and quantized field of optical or microwave resonator. Coherency is achieved by using a low-loss cavity, which is used to enhance the electric

field associated with a single photon, such that the rabi frequency corresponding to atom-field interaction is faster than the decay rate of the field in the cavity [70]. It investigates the coupling properties of atoms with photon modes in cavities. Armour *et al.* [93], Irish and Schwab [94] have recently proposed the idea of cQED using nano-mechanical resonators [93], [94]. The cQED has many applications in Quantum Information Processing (QIP) such as atom-atom, atom-photon, and photon-photon entanglement [95], [96].

2) Photonic Qubits: Photonic qubits have played a very important role in QIP as they can be controlled by traditional optical components and experience the least amount of *decoherence* in their path, which is the phenomenon of loss of quantum information due to the fragile nature of photons in noisy environments. As it is one of the most challenging and disrupting aspect of quantum communication, it will be detailed in Section VI-A. This is the first qubit technology that was realised for generation and distribution of quantum entanglement [74], [97], [98] and has been used for experimental realization of quantum cryptography [99]. They are the first candidates to accomplish the task of quantum teleportation [46], [100], [101], [102], [103], [104]. As QI requires long-distance communication, photonic qubits can achieve this with very little decoherence. If free space is considered as a communicating channel, the birefringence is weak and the absorption of photons is small at optical frequencies as compared to fiber channels [105]. Also, this technology is particularly attractive as photons can be instantly connected to various quantum communication applications such as distributed quantum computation [106].

3) Trapped Ions: The trapped ion is another promising approach for scalable QIP [107], [108]. It offers excellent features such as coherence [109] and effective implementation of entangling gates with least amount of cross-talk [110]. This approach depends basically on the idea proposed by Cirac and Zoller in [111]. Experiments using trapped-ions qubit show single-qubit and multi-qubit operations having fidelity significantly higher than the minimum threshold needed during fault-tolerant quantum computing [112], [113], [114]. Using this technique, a fully programmable five-qubit quantum computer was built [115]. Although the ion trap approach can hold a large number of qubits, their role in quantum computing is radically restricted by the number of entanglement operations that can be executed within the time limits of coherence [116]. Consequently, the improvement of mechanisms for achieving high-speed and high-fidelity entangling gates is necessary for accomplishing large-scale computation on trapped ion platforms [117].

4) Solid State Approach: Solid-state qubits are formed by electron spins [118] followed by superconducting circuits [119] having the transition frequencies in the range of Gigahertz (GHz) thus making them compatible with traditional off-the-shelf Radio Frequency (RF) and microwave components. The solid-state quantum memories, along with photonic qubits, provide excellent solutions that comprise semiconductor quantum dots [118], [120] or rare-earth-doped crystals [121]. This approach has the advantage of meeting scalability requirements in QIP. A large number of solid-state

systems has been built, starting from the 1990s up to recently, that can achieve quantum computation with required scalability. Big tech giants like Google, Intel, and IBM are pursuing this technology and due to the demonstration of the best performance of superconducting qubits, they have already invested into building supreme quantum processors. The most extensive demonstration is the Sycamore processor, built by Google, that has 53 operational qubits [122] and is considered as a breakthrough in the development of technology to realize QI on a large scale [123].

5) Superconducting Approach: Superconducting circuits comprise of Josephson junctions, interconnects, and passive elements, i.e., inductors and capacitors, with good isolation [124]. These circuits operate at milliKelvin (mK) temperatures. Some materials used in such circuits are aluminium (Al), titanium nitride (TiN), and niobium (Nb), substrates of silicon (Si) and sapphire (Al_2O_3), which are compatible with CMOS manufacturing technology [125]. This approach provides lithographic scalability, compatibility with off-the-shelf microwave components, and nanosecond-level operability. These features have all been fused, thus placing superconducting qubit technology at the forefront of the development of emerging quantum processors. This technology also features high fidelity teleportation [126] with single-qubit gate fidelities exceeding 99.9% and two-qubit gate fidelities exceeding 99.5% [119].

IV. QUANTUM INTERNET FUNCTIONALITIES

Quantum Internet is a system that consists of various functionalities required for communicating information among remote nodes of a network. In this section, we will focus on various functionalities of QI like quantum teleportation, quantum channels, quantum repeaters, quantum memories, QKD, and end nodes.

A. Quantum Teleportation

Quantum teleportation comprises a system for transmitting qubits inside a network of quantum communication without physically transferring the particle storing the qubit. The concept of teleporting qubits has started with the seminal work presented in *"Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels"* [69]. It was proved experimentally by Anton Zeilinger group in 1997 for the first time through the successful transmission of quantum optical states [100]. At the same time, group of Sandu Popescu successfully experimented with the photonic teleportation in 1998 [103]. The teleportation distance of 55 m was achieved under laboratory conditions by Swiss researcher Nicolas Gisin and his team in 2003 [127] and later verified it in 2007 by using Swisscom's commercial telecommunication network based on fiber-optics [128]. Later in 2004, researchers from Innsbruck and USA succeeded in teleporting atomic states for the first time [129] followed by an Austrian group led by Anton Zeilinger who achieved a distance of 600 m through a fiber-optic across Danube [130]. This distance was improved to 1.3 km in [75]. Significant experimental progresses in quantum teleportation networks have improved the beeline distance to 8.2 km [15] and 100 km [131]. A larger distance - 144 km
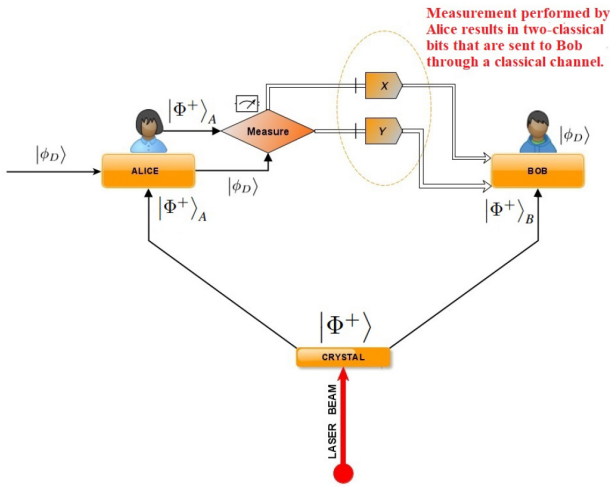
Fig. 9. Quantum Teleportation: Alice holds $|\Phi^+\rangle_A$ and Bob holds $|\Phi^+\rangle_B$ state of the pair. Measurement of Bell state and data qubit as a pair $|\phi_D\rangle$ $|\Phi^+\rangle_A$ is done by Alice and the result of the measurement is stored in classical bits **X** and **Y** as shown above. Manipulating **X** and **Y** at Bob, the original state of $|\phi_D\rangle$ is recovered.

between the islands of La Palma and Tenerife - of teleportation was further achieved by a team of Anton Zeilinger in 2012 using a free space channel [132]. With the advancements in satellite technology, teleportation over a distance of more than 1200 km has been successfully realized with the launch of the Micius satellite by Jian-Wei Pan and his team from China [16].

A large portion of the examinations has been confined to the teleportation of single-body quantum states, i.e., quantum teleportation of two-level states [69], multidimensional states [82], continuous variable teleportation [133], and discrete variable teleportation [134]. Teleportation through noisy channels of bipartite entangled states is studied in [135]. Quantum teleportation of a two-qubit entangled state is discussed in [136] and [137]. It is facilitated by quantum entanglement. Quantum teleportation is realized, as shown in Fig. 9, with two parallel links required for communication.

1) Quantum channel link, for generating entangled EPR pair and distributing it between source and destination nodes.
2) Classical channel link, for transmitting two classical bits from a source node to a destination node for sending the measurement result of source qubit.

Quantum teleportation is not straightforward for application, which renders efficient communication and fidelity of the system [47]. However, at the same time, it involves imperfections in its process imposed by photon loss in environment-*decoherence* or are the result of a sequence of operations that are applied for the processing of teleportation [138]. Thus, the technology opted for quantum teleportation plays a strong part in improving the system fidelity and reducing decoherence [47].

The process of teleportation begins with source node Alice in possession of an unknown data qubit $|\phi_D\rangle = \alpha|0\rangle + \beta|1\rangle$, and an EPR pair shared between Alice and Bob. Let us assume the bell pair to be $|\Phi^+\rangle$, as shown in (5). Bell pair qubit which

Alice holds is denoted by $|\Phi^+\rangle_A$ and the other pair of qubit held by Bob is $|\Phi^+\rangle_B$, as shown in Fig. 9. The procedure of teleportation between Alice and Bob is as follows.

1) Bell state $|\Phi^+\rangle$ is prepared by Alice and Bob such that each of them holds the qubit of this EPR pair. Alice holds $|\Phi^+\rangle_A$ and Bob holds $|\Phi^+\rangle_B$ state of the pair.
2) Simultaneously, the state to be teleported, i.e., $|\phi_D\rangle$, is acquired by Alice.
3) Measurement of Bell state and data qubit as a pair $|\phi_D\rangle|\Phi^+\rangle_A$ is performed by Alice and the result of measurement, stored in two classical bits, is sent to destination Bob through classical link.
4) Bob manipulates the received classical bits and apply corrections in X or Z direction accordingly.
5) At last, Bob's qubit state $|\Phi^+\rangle_B$ now holds the same quantum state as Alice's $|\phi_D\rangle$. This completes the process of teleportation of the data qubit between end nodes of Alice and Bob.

In the process of measurement, the entanglement of EPR pair is destroyed, therefore it should be noted here that for teleportation of another data qubit, another EPR pair should be generated and distributed. Thus, it can be seen that quantum entanglement is an important quantum effect, as it is fundamental pre-requisite for transmission of particle storing the qubit. It is vital to look at the technologies to generate and distribute the qubits, which are discussed in Section III-B. In view that Alice and Bob represent remote nodes, the entanglement generation taking place at one side must be complemented by way of the entanglement distribution capability, moving entangled qubit to the destination side. Considering this, it is highly likely for the adoption of photons as entanglement providers [91]. The reason for this choice lays in the advantages offered by photons for entanglement distribution [98], along with least interaction with the environment, smooth control with basic optical components as well as high-speed low-loss transmission to far off nodes.

1) Mathematical Details: For the state of clarity, lets analyse the mathematical details of quantum teleportation process. The input is data qubit state $|\phi_D\rangle$, that is to be teleported from Alice to Bob. EPR pairs of Bell state $|\Phi^+\rangle$ is required to be in possession of both Alice and Bob.

- Global state of Alice and Bob is represented by $|\psi_D\rangle$, which is the tensor product of $|\phi_D\rangle$ and $|\Phi^+\rangle$ given by:

$$|\psi_D\rangle = |\phi_D\rangle \otimes |\Phi^+\rangle. \tag{14}$$

Thus, we get

$$|\psi_D\rangle = \alpha|0\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta|1\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{15}$$

Now, (15) becomes

$$|\psi_D\rangle = \frac{(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)}{\sqrt{2}}. \tag{16}$$

- Alice then applies the CNOT operation to the pair of qubits that she has, that maps $|10\rangle$ into $|11\rangle$ and vice

versa, the result of which is:

$$|\psi_D\rangle = \frac{(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)}{\sqrt{2}}. \quad (17)$$

- Alice then applies Hadamard gate operation to $|\phi_D\rangle$, that maps $|0\rangle$ into $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $|1\rangle$ into $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, resulting in:

$$\begin{aligned}|\psi_D\rangle = (&\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle \\ &+ \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle)/2.\end{aligned} \quad (18)$$

- Rearranging (18) gives

$$\begin{aligned}|\psi_D\rangle = (&|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) \\ &+ |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle))/2.\end{aligned} \quad (19)$$

- Alice then applies the join measurement on the pair of qubits at her possession and has 25% probability of getting each of the combinations $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
- The measurement result of Alice instantaneously affects the state of the Bob's qubit regardless of the distance between them as the pairs are entangled.
- Bob can recover the original state of qubit $|\Phi_D\rangle$ after manipulating the classical bits, received through classical link, having the information of Alice's measurement.
- If the result of Alice's measurement is $|00\rangle$, then the state of Bob's qubit is $\alpha|0\rangle + \beta|1\rangle$ as depicted from (19). Thus, Bob's qubit follows the original quantum state $|\Phi_D\rangle$ and there is no need for any further operation. If Alice's joint measurement is $|01\rangle$, the measurement result of Bob is $\alpha|1\rangle + \beta|0\rangle$. So, Bob recovers the original quantum state $|\Phi_D\rangle = \alpha|0\rangle + \beta|1\rangle$ by applying Pauli-X gate operation. Similarly, for Alice's measurement of $|10\rangle$ and $|11\rangle$, Bob again recovers the original state by applying certain gate operations, which successfully completes the process of teleportation of qubits between Alice and Bob.
- After all this, it can be concluded that teleportation process obeys the speed of light, thus preserving the theory of relativity.

2) Teleportation Using Quantum Switch: Quantum teleportation, as discussed earlier, is the core functionality of QI that exploits the unmatched property of quantum mechanics, i.e., *quantum entanglement*. Entanglement generation and distribution is accomplished between Alice and Bob through quantum and classical channels. Since entanglement distribution is limited by noise and decoherence, it further degrades the efficiency of teleported information. Hence, there is a need to efficiently use the resources that are available by exploiting the laws of quantum mechanics and distribute the entangled information through noisy channels with the help of superposition of causal orders of available channels [139]. This is achieved through *quantum switch* [140], which uses superposition principle and permits quantum particles to propagate concurrently among more than one space-time trajectories [141], [142]. The usual assumption is that quantum information, which is stored in quantum particles is sent through well defined orders of channels as described by the
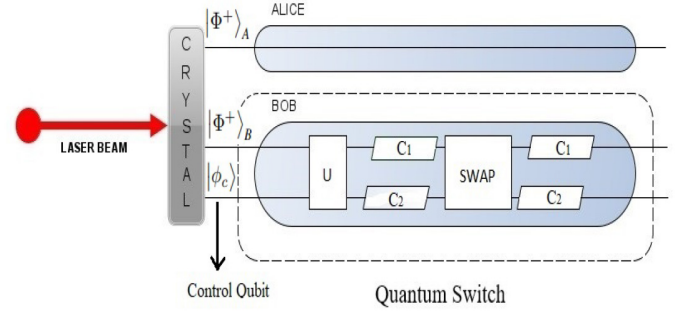

Fig. 10. Entanglement Distribution using quantum switch: Alice holds $|\Phi^+\rangle_A$ and Bob holds $|\Phi^+\rangle_B$ state of an EPR pair. A control qubit $|\phi_c\rangle$ is also there at Bob which decides the order of channel to be traversed. This operation is performed by U gate, that directs qubit $|\Phi^+\rangle_B$ at Bob through upper or lower line on the basis of the state of control qubit $|\phi_c\rangle$. SWAP gate enables the entanglement-carrier $|\Phi^+\rangle_B$ through it to the other side of the switch, distributing entanglement between Alice and Bob.

classical theory of Shannon in [143]. But, the particles can traverse through superposition of multiple channels at the same time, which means that the relative order is indefinite [144]. The quantum switch is a novel device that controls the order in which channels are traversed with the help of a *control qubit.* This new resource can be advantageous for problems faced in fields of quantum computation [145], QIP [140], non-local games [146], and communication complexity [147]. Let us assume that we have two channels in the entanglement distribution process, i.e., C_1 and C_2. If a message *"M"* travels from Alice to Bob through these channels, it can traverse either C_1 followed by C_2, or C_2 followed by C_1. But, knowing the property of quantum superposition of channels, it is not possible to determine the order in which the channel is traversed, which means that superposition of both the channels exist, i.e., message *"M"* traverses the channel C_1 and C_2 in superposition of orders $C_1 \rightarrow C_2$ and $C_2 \rightarrow C_1$. For this task, a control bit $|\phi_c\rangle$ is assigned, as shown in Fig. 10. If $|\phi_c\rangle$ is initialized to $|\phi_c\rangle = |0\rangle$, the quantum switch enables message "M" to traverse path $C_1 \rightarrow C_2$ and if $|\phi_c\rangle$ is initialized to $|\phi_c\rangle = |1\rangle$, the quantum switch enables message *"M"* to traverse path $C_2 \rightarrow C_1$. Interestingly, if control bit is initialized with superposition of basis states $|0\rangle$ and $|1\rangle$ in state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, then quantum switch enables the message *"M"* to traverse the superposition of orders $C_1 \rightarrow C_2$ and $C_2 \rightarrow C_1$. This operation of traversing the particular order of channel is performed by a U gate as seen in Fig. 10, directing qubit $|\Phi^+\rangle_B$ at Bob on the basis of state of control qubit $|\phi_c\rangle$ as mentioned earlier. The SWAP gate is implemented with Polarization Beam Splitter (PBS) and Half-Wave Plates (HWPs), which helps to switch between the polarization states of $|\phi_c\rangle$, i.e., horizontal and vertical polarization. The theoretical analysis of employing a quantum switch and advantages it offers, is discussed in [139], [142], [148], [149], and experimentally detailed in [150], [151]. Therefore, a quantum switch is the core functionality of the quantum Web and is a key fixing in the quantum teleportation process.

B. Quantum Repeaters

A quantum repeater is another functionality of QI that is employed in between the remote nodes, to transmit quantum
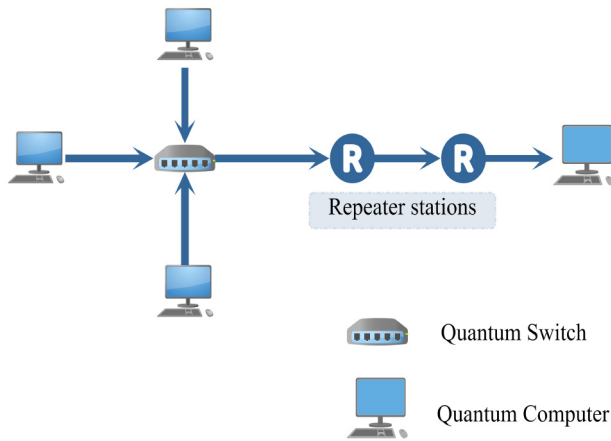
Fig. 11. Repeater Stations: These stations are employed at short distances so that entanglement can be established between intermediary nodes and ultimately between end nodes which are long distance apart. Here, *quantum switch* is also employed to transmit information between end nodes, traversing channels in superposition of different orders.

information to long distance as shown in Fig. 11. They generate maximally entangled pairs between two far away end nodes by bifurcating the network into segments, establishing the long distance entanglement between end points. In long distance communication, most of the information carrying photons gets lost because of channel attenuation or other environmental factors. This exponential problem of photon loss was addressed by Jurgen Briegel in 1998 by introducing the model of a quantum repeater [152]. In the classical domain, the issue is resolved by employing classical repeaters that copy the information after regular intervals for amplification. However, in the case of quantum communication, due to the no-cloning theorem [153], information carried in qubits cannot be copied or amplified since classical repeaters are not suitable for this communication. Hence, the quantum repeater model proposed by Briegel is employed to transmit qubits from Alice to Bob without any loss of information [152].

The evolution of quantum repeaters is classified into three distinct generations [154]. In the **first generation** of quantum repeaters, intermediate stations are placed as shown in Fig. 11, in such a way that links are short distance apart and probability for establishing entanglement among repeater stations is high. Due to a the feature of *entanglement swapping* [154], discussed in Section IV-B2, all these stations are interconnected in terms of entanglement from Alice to Bob [69], [89], thus entangling the far away end nodes.

Each repeater station must be capable of receiving, processing, and transmitting classical and quantum information. For this, some specific protocols are employed, considering the following points.

- Firstly, entanglement must be established between adjacent nodes.
- Next, *entanglement swapping* must take place at the repeater stations such that qubits at the end nodes are instantaneously entangled.
- After that, error correction takes place, where few strongly entangled states are generated from weakly entangled states by a process known as *entanglement distillation* or *purification* [155]. Multiple copies of weakly

entangled states are used by Alice and Bob for distillation. By combining all these states, and applying local operation using quantum gates, pure Bell pairs can be generated [156]. So, a two-way classical communication is required to acknowledge both nodes about successful purification.

One limitation of first generation quantum repeaters is that they require two-way classical communication for entanglement purification step, which creates a performance bottleneck as the distance of communication is increased. Thus, there is a need to move towards schemes that require only one-way communication and no classical signals are required for acknowledgement of success rate. Therefore, the **second generation** of quantum repeaters employ QEC (one-way classical communication) for the purpose of entanglement purification [18], [157], [158]. With this scheme, the waiting time for receiving the acknowledgement of purification is not needed, thus qubits can be used for entangling the link again without waiting [154]. In [157], researchers used Calderbank-Steane-Shor (CSS) encoding for significant improvements in speed of entanglement generation between nodes. The second generation quantum repeaters using heralded entanglement generation still needs two-way signalling to reduce loss errors. Therefore, in the **third generation** of quantum repeaters, this two-way signalling is replaced by one-way signalling using certain loss-tolerant codes [18], [19], [20], [159]. In [18], quantum information is encoded in matter qubits that are transferred to photons and are sent through the channel from the transmitter to the receiver [19]. At the receiver, these quantum states are transferred to matter qubits before carrying out the error correction. The matter qubits are not required to serve as quantum memories as in first and second generations. In 2014, this scheme was termed as fully fault-tolerant [20]. Matter qubits may be too demanding for use in quantum repeaters, and thus, all optical quantum repeaters were developed by taking a time reversal of the DLCZ-like (discussed later in this section) quantum repeater protocol [159].

A lot of research is going on in this field with single quantum systems [160], [161], [162]. Significant theoretical as well as experimental progress on repeater protocols with repeater elements has taken place [154], [163], [164]. The majority of implementations follows encoding, where information is encoded in discrete variables and protocols based on this have been existed and been improved upon since two decades [154], [163]. But, repeaters with continuous variable (Section VII-D) protocols has been a state of subject recently and the first protocol was published in 2017, 2018 [165], [166].

There are certain conditions that are required for the design of quantum repeaters, although the losses surge exponentially with the distance of communication. Supposing, the distance of communication between Alice and Bob is *D*. The idea is to create an entanglement between two pairs, each covering the distance of *D/2*. Entanglement between these two pairs is created by entanglement swapping between another two pairs covering the distance *D/4* and so on. This process is repeated unless entanglement is created between all the intermediary nodes, ultimately entangling the qubits at the far away end
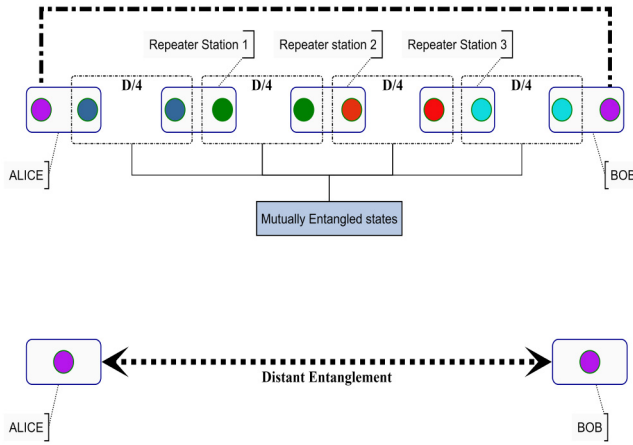
Fig. 12. Quantum Repeaters: Entanglement is generated between distant nodes by employing intermediary repeater stations which have qubits that are mutually entangled to each other. Thus, after performing *Entanglement swapping* operation , Alice and Bob qubits are entangled. In this way, long distance communication would be possible which is the main requirement of QI.

nodes, as shown in Fig. 12. The quantum repeater stations improve the photonic qubit transfer rate [154]. End nodes can also be used as quantum repeaters, thus posing similar requirements on protocols for its realization. The construction of maximally entangled states over long distances is achieved according to special protocols as described in [84], [152]. The most famous protocol is **DLCZ protocol** named after authors Duan *et al.* [167]. Particularly, adopting atomic ensembles as quantum memories and linear optical techniques, as compared to single atoms, makes it easier to maintain strong coupling between the photons and memories that prove advantageous in long-distance communication of quantum information [168]. The idea behind the functionality of the DLCZ protocol is a photon having spontaneous Raman emission, generating a simultaneous joint spin excitation in the atomic ensemble. The connection between the atomic excitation in each ensemble and emitted photons forms the foundation for the generation of entanglement for each intermediary link, done via a single-photon detection [169]. The spin excitations can be effectively reconverted into photons through associative interference effect. This correlation between emitted photons and atomic excitations in each ensemble, forms the crux of the entanglement swapping operation. Due to these advantages offered by atomic ensembles, DLCZ protocol is experimented successfully in [169], [170], [171], [172], [173], [174]. Many researchers motivated by the features of atomic ensembles and the experimental results, started improvising DLCZ protocol and came out with exciting results. Thus, knowing the basics of DLCZ protocol gives insights about how this protocol can be improved further for quantum repeater purposes. The physics behind this protocol and the entanglement creation between long distant ensembles is thoroughly discussed in [164]. In an ensemble of three-level systems with two ground states g_1 and g_2 and excited state e, the transition of g_1-e is first incidented with an off-resonant laser pulse resulting in the spontaneous emission of a Raman photon on the e-g_2 transition. This photon which is generated on a condition that energy of g_2 is higher than that of g_1, is termed

as *Stokes* photon. These photons, transmitted through optical fibers, are responsible for entanglement creation between two remote ensemble locations using DLCZ protocol.

States having minimum entanglement are termed as noisy, so after entanglement distillation, they are turned to purified states having maximum entanglement. Realizing QI with QKD and trusted repeater networks, requires the use of quantum satellites such as Micius [43], which bolster free-space quantum channels covering longer distances. The vacuum in outer space provides noiseless communication thus improving fidelity for such quantum-satellites based quantum systems. The misfortunes over longer distances, including those brought about by climatic diffraction, are significantly less. All things considered, the advancement of quantum repeaters for a quantum Web requires complex quantum innovation.

1) Workflow: The working principle of the first generation of quantum repeaters can be best understood with the help of a simplified example where the sender Alice and the destination Bob perform quantum cryptography with received entangled photons. As of now, these two end nodes are distant apart and photon losses occurring in channels deteriorated the photon rate. So, they have to keep the noise as minimised, in the channel, as possible. To achieve that, they use quantum repeater that can be expressed mathematically as

$$S_1 \Longleftrightarrow S_2 \langle b^m \rangle S_3 \Longleftrightarrow S_4, \qquad (20)$$

where "$\Longleftrightarrow$" corresponds to entanglement and "$\langle b^m \rangle$" corresponds to joint BSM for performing entanglement swapping discussed in what follows.

2) Entanglement Swapping: In this process, the projection of the state of two particles is made onto an entangled state, for obtaining an overall entanglement. It is done by performing special BSM, which does not essentially require an immediate cooperation between the two particles, such a measurement will automatically collapse the state of the remaining two particles into an entangled state. Entanglement swapping is nothing but the quantum teleportation of entanglement of quantum states. Multiple teleportation procedures are performed by multiple repeater stations, thus forming a quantum channel for transmission of quantum information between end nodes, that are thousands of kilometers apart physically [69], [89], [175].

C. Quantum Channels

The QI is an inherently secure network that will be implemented along with classical Internet, where end nodes will be connected via classical and quantum channels. A continuous quantum channel is created until all the end nodes are connected as shown in Fig. 2. The classical information as well as quantum information can be sent through quantum channels. As seen in teleportation of data qubit $|\phi_D\rangle$, EPR pairs that are generated, are distributed to Alice and Bob through a quantum channel. Now, this channel can be a free space channel for sending quantum information to long distances or can be fiber based channels, which can be used to send quantum information to relatively shorter distances. How efficiently an entanglement can be distributed depends upon the capacity of a channel and entanglement distribution process, which

is mainly limited by the photon loss in channel that scales exponentially in a usual scenario. The communication channel capacity defines the ability of the channel to deliver the information from Alice to Bob in a faithful and recoverable way.

The steps of quantum communication through quantum channels differ from the communication through classical channels in many ways. In quantum channel, communication of quantum information takes place in three different phases.

- **Channel encoding phase**, where sender Alice encodes or prepares the quantum state to be sent to the destination Bob, so that the information encoded compensates for the noise in channel [176], [177].
- Next Phase is **quantum evolution phase**, where quantum information is put on the quantum channel, which maps the information to the receiver Bob.
- Final phase is **decoding phase**, which includes quantum information to be decoded by destination Bob. Here received quantum state, containing the exact information, can be a superposed state or a state possessing some noise. This state is then measured by Bob taking into account the error correcting procedures.

1) Free Space Channels: The free-space optical channel was first utilized for QKD in [178], [179] by the Los Alamos National Laboratory (LANL). Some QKD experiments were demonstrated that were capable to operate in daylight conditions [180], [181]. Another project sponsored by U.S. government has reportedly performed a QKD experiment with an aircraft flying at 10,000 feet to ground station using free-space channel [182]. The Free space channel link has been demonstrated in various experiments [48], [182]. DARPA sponsored QKD network using free space link has been demonstrated in [183]. Quantum communication has been demonstrated by the Zeilinger group between two peaks in the Canary Islands, separated by 144 km [132], [184]. The free-space optical quantum channel has all the earmarks of being very promising for long-distance quantum communication [185]. The information-carrying photons are quick and vigorous, and are prone to environmental loss. The advantage of using free space channel is that, most of the photon loss mechanism occurs lower than 10-30 km of atmosphere, leaving behind most of path as vacuum with negligible loss of photons and decoherence. Only dispersion effect is present once light leaves the atmosphere [186]. Thus, free-space optical channel keeps the quantum information in photons intact and increases the system fidelity and channel capacity. Therefore, high information capacity photons are required for this purpose, i.e., orbital angular momentum (OAM) modal basis of photons [187]. QKD protocols encoding by OAM modes were verified experimentally in the laboratory conditions [188], [189]. The effect of atmospheric turbulence on OAM modes are discussed in [190]. Some research groups have developed the ways to mitigate atmospheric turbulence in free space with certain techniques such as, using adaptive optics post-processing [191], [192], robust states [193], and optimal encoding scheme [194].

Until the launch of Micius satellite by China [43], entanglement distribution was only possible with distances not more

TABLE IV
FEATURES OF FREE-SPACE AND FIBER-BASED CHANNELS FOR QUANTUM COMMUNICATION

Free-Space Channels	Fiber-Based Channels
It uses free space as a mode of communication.	It consists of core and cladding that carries light photons.
It suffers from loss due to environmental effects such as beam diffraction, pointing error, atmospheric turbulence, and absorption but is resistant to such losses after entering vacuum.	It suffers from absorption and coupling losses but has negligible loss due to environmental factors.
Supports satellite communication where it can act as Up-link or Down-link channel.	Supports ground to ground long distance communication.
High Fidelity	Low Fidelity

than 100 km [131]. But with this launch, it became possible to achieve entanglement distribution between two far away ground stations located on earth with distances greater than 1000 km through terrestrial free space channels [195]. Much of the system fidelity depends on the quantum channel loss, which comprises of beam diffraction, pointing error, atmospheric turbulence, absorption, beam divergence [196]. Thus, satellite based entanglement distribution puts more stringent requirements for link efficiencies than any classical satellite to ground communications. Taking into account all these losses, the attenuation of the link should not be greater than 60 dB for ground-to-satellite quantum communication to be successful [197]. These losses leads to beam broadening which results in loss of photons limiting the photons received by receiver end. Typically losses are in the order of 30-40 dB [196]. So, various techniques are heralded to achieve efficient long distance communications [192], [193], [194].

2) Fiber Based Channels: Besides free space links, which play a vital role in long-haul quantum communication, optical fiber links are more attractive because of their technological maturity owing to traditional Internet technology. The qualitative features of both these channels are mentioned in Table IV. Here qubits carrying information are transmitted from Alice to Bob through optical modes in fibers. A standard single-mode fiber (SMF) consists of a core and a cladding that carries the light. Total internal reflection guides the light along the core of the fiber because of the difference in index of refraction. These waveguides are fabricated directly in silicon [198] or in conductors such as aluminum [199]. There are different types of fibers available for propagation of quantum states; SMFs, multi-mode fibers (MMFs), few-mode fibers, multi-core fibers (MCFs) etc. Among all, SMFs have a smaller core that keeps the light more tightly, therefore better suited for high-precision environments of quantum experiments [200]. In one such experiment, entanglement is created at a distance of 300 km through optical fiber channel [25].

Fiber-based channels have an advantage that environmental factors are not significant inside fiber channels, thus preserving the coherence of photons. Instead, it suffers from polarization-preservation and optical attenuation problems that limits the distance of communication to a few hundreds of kilometres [201], [202], [203].

D. Quantum Memories

Quantum memories are an integral part of quantum communication system, which is required by intermediary devices to store and process the qubits for sending and receiving photons with high fidelity [204]. Quantum computing includes a tool for the synchronization of the processes within a quantum computer [205]. In addition, quantum memories are employed with quantum repeaters for extending the range of quantum communication [152]. Quantum memories were also studied in the strategic report on quantum information processing and communication, which proved to be helpful in European integrated project Qubit Applications (QAP). This had a sub-project involving seven research groups devoted to the development of quantum memories [206]. For achieving the scalability required for large-scale long-distance quantum communication, quantum memories are employed for converting qubits between light and matter. They also control the storage of qubits and retrieve them with stationary matter systems [167], [206]. Quantum memories are also required for timely operations for perfect timing and synchronization [70], [164], [206], [207]. As discussed earlier, communication between distant nodes storing matter qubits, engages quantum memories for the transfer of quantum information between these nodes with entanglement distribution [173], in free space or fiber based channels [82]. For this, atomic ensembles were proved to be best contender for quantum memory, with good amount of experimental progress [172], [208]. Quantum memories having cold neutral atoms are discussed in [209], [210], having doped crystals in [211], enabling the storage and retrieval functionality of single-photon entanglement extending to high-dimensional entanglement [212] and continuous-variable entanglement [213]. As a result, transfer efficiency of all these implementations lies between 15% and 25% [214]. High fidelity entanglement transfer is a major challenge for network scalability inspite of various implementations of efficient quantum memories for polarization qubits [215], [216].

E. Quantum Key Distribution

Every field in today's modern era, whether it is military applications, financial institutions, private multinational companies or government agencies etc, rely upon a full-fledged Internet to accomplish the day to day tasks and share gigabytes of data over the Internet. The security of this data is fundamental, as any eavesdropping attack on private/public channels, will be a serious attack on the privacy as shown in Fig. 1. The security of systems using traditional cryptographic protocols is based upon the complexity in solving mathematical problems such as factorization of large integers or discrete logarithmic problem, and believing that the hackers computing performance is inadequate. Cryptography is classified into symmetric, asymmetric and hybrid cryptography where some type of keys are used for encryption and decryption of messages. If the same key is used for encryption and decryption of messages, such systems are known as *private key cryptosystems* [217]. On the other hand, *public key cryptosystems* use public key for encryption and private/secret key for decryption [218]. The idea of public key cryptosystem was put forth by Diffie and Hellman in 1976 [219]. The first implementation was done by Rivest, Shamir, and Adleman (RSA) in 1978 [220]. Since public key cryptosystems are slow, hybrid schemes are employed that combine private key and public key methods offering considerable speed advantages [221]. In public key cryptosystems, without the knowledge of the secret key a message cannot be decoded, thus enhancing the security of the systems. Unfortunately, private key cryptosystems suffers from *key distribution problem*, i.e., distributing the keys in a secure manner. QKD provides excellent privacy against hacks, and provides solution to key distribution problems using quantum cryptography [65] with the following objectives.

- First, sender Alice and Bob shares a secret/private key with each other, without *Eve* having no knowledge of it.
- Next, this key is distributed from Alice to Bob through an inherently secure quantum channel. The security of this key depends upon the fact that any attempt of hacking or spying by *Eve* will disturb the state of the key qubits, thus exposing his/her attempt. Hence, it is impossible for *Eve* to copy the information without being detected.
- Alice and Bob must be capable of *authenticating* the message, in order to prevent it from *Eve* taking the position of either Alice or Bob. This task can be accomplished by quantum authentication protocols such as [222], [223], [224]. If such level of authentication can be achieved, QKD can provide provable security against unlimited attacks, that is nearly impossible with classical key exchange cryptographic protocols.

The first experiment to demonstrate QKD was performed in 1989, covering distance of 32 cm [225]. This distance had to be increased practically for achieving QKD over long distance using optical fiber channels or free space channels. But, with increased distance, fiber and atmospheric losses increases, resulting in decrease of photon count and key rate significantly due to decoherence effect [226], [227]. No-cloning theorem [5] also restricts sending several copies of information, thus limiting the practically achieved distance of QKD to few hundreds of km [203]. Therefore, researchers are focused on exploring satellite to ground QKD so that two remote nodes or network of nodes achieves QKD for long distance without significant absorption and turbulence [228]. Following this, in 2004, an experiment was conducted in free space that reported a successful survival of entanglement of photons with noisy atmosphere of 13 km from ground [229]. This distance was further improved from 100 km to upto 500 km with various satellite based successful QKD experiments [131], [132], [230], [231]. With the launch of Micius satellite, breakthrough has been achieved with QKD covering much greater distance of 1200 km [43]. Using same satellites, a secure key has been generated between two ground stations located in China and Europe that are 7600 km apart [232]. In addition, already existing fiber links of 2000 km, i.e., that between Beijing to Shanghai, are integrated with free space QKD links using Micius. A quantum communication distance of 4600 km was reported between ground stations [233]. These experiments provide significant breakthrough in realizing global space-based QI.

1) Key Protocols: For providing security and integrity of data, QKD systems operate in two stages. In the **first stage**, a random bit sequence, known as "key," is generated, which can be a result of certain binary operation performed on the data to be transmitted. In the **second stage**, the generated quantum "key" is sent to destination in a secure manner over classical channel where it can be decoded using the same private "key". A cryptographic protocol used in classical systems is OTP, which is provably secure in quantum technology [234]. No algorithm will be able to acquire the knowledge of the "key", as it is generated quantum randomly. Some of these protocols are discussed below.

- **OTP**: OTP is one of the oldest classical cryptographic techniques that dates back to 1882, it was invented by Frank Miller [235]. It is a simple and highly effective private key cryptosystem. Security of the OTP cannot be compromised without the knowledge of a *pre-shared* key, which is known only to Alice and Bob (private key). If the information is intercepted by *Eve*, then Alice and Bob will get to know about the spying, as a result the information will be declared *invalid*. The data is encrypted by a binary operation on *data* and *key* bits. The result of this operation is sent to Bob, who then decodes the information using the same binary operation on the received data bits, thus retrieving the original information with the help of a pre-shared private key having the following features.

  1) The key generated must be used only once. It cannot be reused and should be in its original form. Not even one part of this key must be reused as it will compromise the security of the system.
  2) The length of the key must be at least as long as the data to be sent, so that even if *Eve* attacks the channel she does not succeed.
  3) The key must be shared to Alice and Bob in a secret manner, so that only Alice and Bob must be in a possession of this key.

  Since the OTP requires the length of the key to be at least as long as the amount of data to be transmitted, it becomes impractical to be used in several cases. Hence, there is a need to explore and exploit the property of entanglement, to generate a quantum vernam cipher [236] and other protocols for enhancing the security [237].

- **BB84 Protocol**: This protocol is one of the popular methods used for quantum cryptography. It was formulated by two physicists, Charles H. Bennett and Gilles Brassard, at IBM in 1984 [65]. Though original idea was proposed by Wiesner in 1970's, but the research could not be published in the same year as it was published a decade later in 1983 [238]. In this protocol, back to back photons carrying qubits are sent to Bob, who tries to perform a measurement on the arrived photons carrying qubits. Some of the photons are lost due to decoherence and never arrive while some of those are not detected. Out of all the detected photons, some of the bits are utilized to form the *key*, the rest are utilized to expose the *Eve* and gather information about spying. Alice encodes the information with her own *basis*, about
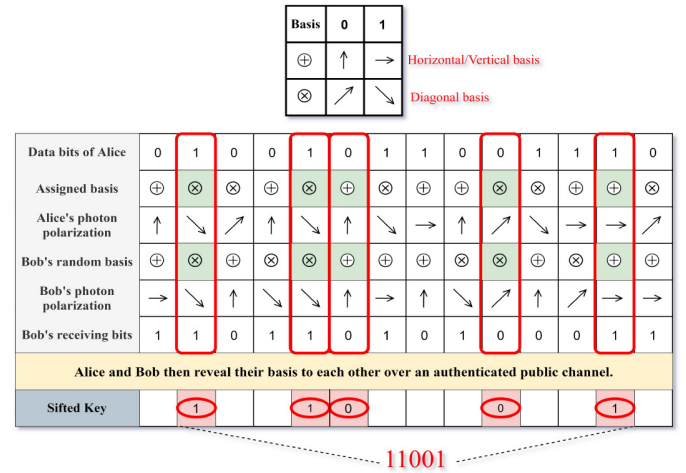

Fig. 13.   BB84 protocol.

which only Bob is familiar with. If this information is decoded using a different basis, other than the Alice's one, then the measurement will *disturb* the state of the photons carrying the qubits. In this context, *Eve* measuring the information with different basis *alters* the state of qubits, thus revealing its presence, resulting in Bob to discard those bits. BB84 protocol is based on the communication of a series of single qubits sent from Alice to Bob, that are stored in photons represented by their polarization states. Usually, the transmission between Alice and Bob takes place through quantum channels but fiber-optic channels can also be used. Alice can use the *vertical/horizontal* or *diagonal* basis of polarization for encoding the information, i.e., $|\uparrow\rangle$ for vertical basis, $|\rightarrow\rangle$ for horizontal basis, $|\nearrow\rangle$ and $|\searrow\rangle$ for diagonal basis. Let the states $|\uparrow\rangle = |0\rangle$ and $|\rightarrow\rangle = |1\rangle$ be represented by $\oplus$. The states $|\nearrow\rangle = |0\rangle$ and $|\searrow\rangle = |1\rangle$ are represented by $\otimes$. The protocol runs as follows.

1) The quantum states are encoded using the data bits of Alice with the assigned basis (e.g., $\oplus$ and $\otimes$) and random classical bits (0 or 1). Alice sends the encoded quantum states to Bob through any channel that is usually vulnerable to attack by *Eve* for spying. The data encoded is in the form $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\nearrow\rangle$, $|\searrow\rangle$.
2) Bob then uses a random basis for measurement of qubits received with basis $\oplus$ and $\otimes$ as shown in Fig. 13. This is the last quantum operation carried out in this protocol.
3) Bob then acknowledges to Alice for the qubits that he has received via a public channel.
4) Alice and Bob discloses the basis used to encode the data qubits via a public channel. When both choose the same basis, the corresponding measured bits are kept and this data will form the *key*. If they choose a different basis then the bits will be *rejected* and this process is well known as *sifting*.
5) Next, the presence of *Eve* is checked by revealing a random number of bits encoded by Alice. If the detected bits by Bob are the same, then there is no
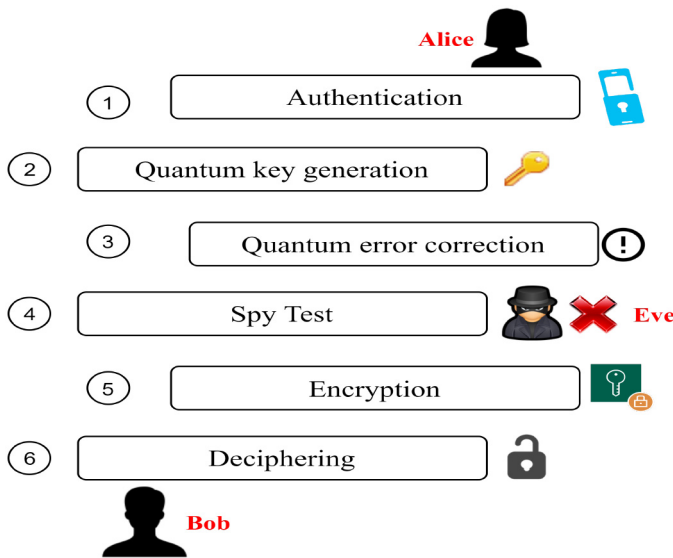
Fig. 14.   An example of Ekert protocol: This entanglement-based QKD protocol runs in 6 steps.

interference by *Eve* and the remaining error free bits are termed as *encryption keys*.

In 2007, results from polling stations in Swiss parliamentary elections, in the canton of Geneva were transferred, using this protocol, to Bern over hundreds of kilometres and nobody could hack the system till date. In this way, a secure communication is possible in any distributed network exploiting the realms of quantum mechanics. It is used in satellite based communications theoretically and experimentally as shown in [184], [186], [195] and [230]. This reach can possibly be extended using *relays*, that may or may not be trusted [239]. In future QI, QKD will play a very important role in making the Internet hack-proof as it is the main requirement in today's digital era. But every solution comes with some shortcomings and BB84 protocol is no different. The biggest disadvantage is its limited distance upto which it can work efficiently. It can cover only up to hundreds of km through fiber-based or free space atmospheric channels.

- **Ekert Protocol**: This protocol which takes into consideration the entanglement of photons carrying qubits, was proposed in 1991 by Artur Ekert [9]. The first implementation of this protocol was achieved by Anton Zeilinger and his group in 1999 over a short distance of 360 m [240]. By the same team, the first money transfer via quantum cryptography was demonstrated in 2004 [241]. This protocol runs in 6 steps as shown in Fig. 14.
  1) First, an authenticated channel must be set up, which can be classical or quantum in nature, between Alice and Bob and they have to make sure there is no chance for *Eve* to take position of any one of them. This channel is open to interceptions.
  2) Next, an EPR pair of entangled photons is sent to Alice and Bob, whose measurement results in values of 0 or 1. Alice and Bob filter those bits that shows clear correlations (important bits) from those

without clear correlations (unessential bits). For this, need of classical channel is a necessity.
  3) Then, privacy amplification procedure [242] is employed for correcting the measurement errors.
  4) The network security depends upon whether the states are maximally entangled or not, otherwise decoherence becomes an obstacle in the communication. *Eve's* hacking attempt can be detected with Bell's inequality [243]. If this inequality is not violated, then it can be believed that there is an eavesdropping attack, or the information communicated has some technical issues. As a result, any successful attack by *Eve* can be detected immediately and the system functionality is checked.
  5) The quantum key, taking into consideration the relevant bits, is used for a symmetrical procedure such as OTP and sent over the regular Internet.
  6) After that, Bob receives the data that are encrypted in a ciphertext and deciphers it with the self generated private key. This completes the Ekert protocol resulting in the generation of a secure key.

2) Security of QKD: Quantum key distribution relies upon protocols and the specified steps of operations to be performed between Alice and Bob. It is generally a two-step process. In the first step, Alice and Bob takes some correlated data, e.g., *X* or *Y*, that can be quantum or classical in nature. Then, in the next step, Alice and Bob exchange some information through classical or quantum channel, resulting in an output *X'* and *Y'*. This output is generally a pair of secret keys that are only shared between Alice and Bob. If uncorrelated data inputs are used, then a protocol might not be able to produce the desired output, i.e., *secret keys*. For any protocol to be secure, depending on its input, it should be able to judge the situation and abort the generation of keys in case of tampered inputs. This explains that a QKD protocol must be *robust* enough so that it does not compromise the security of the system.

The protocols discussed in Section IV-E1 are provably secure. The proof remains in the observation that after *information reconciliation* [244] and *privacy amplification* [245] are performed, the key rates obtained turn out to be coinciding with the achievable qubit transmission rate over noisy communication channels [246]. So, it can be concluded that the OTP, BB84, Ekert protocol, and EPR protocols [245] are secure as long as *Eve* attacks on the transmission of one qubit at a time. If *Eve* performs simultaneous attacks where she obstructs and stores large blocks of the qubits to be communicated, then it will compromise the security of the system. But then again, QEC codes plays an important role in maintaining the security of these systems [17].

There can be a case when Alice and Bob share imperfect keys and they both have upper bound on *Eve*. Therefore, keys cannot be correlated, thereby compromising the security which results in *Eve* intercepting the channel and gaining access to private data. To enhance the security, *information reconciliation* followed by *privacy amplification* [247], [248] steps increases the correlation of the private keys and minimizes the *Eve's* chances of accessing the information, achieving desired level of security.

The quantum realm inherits the features of secure communication such as no-cloning theorem. Hence, QKD protocols governed by the laws of quantum mechanics while sharing the keys between Alice and Bob on private or public channel, are inherently hack-proof. An *eavesdropper* can attack any communication between Alice and Bob in different manner. She can attack either quantum or classical channel and compromise the security. Another case can be taken where *Eve* likely to gain the information, tries to measure the intercepted photons before sending the photons Bob. *Eve* is still unaware of the basis measure each bit of photons with wrong basis having 50% probability. Hence, this wrong measurement changes the state of the information carrying photons, before Bob receives it. This measurement will affect the ability of Bob to measure the bits correctly because the state of the photons has already been changed by *Eve*. Even if Bob uses the basis shared by Alice to measure the photons, he will still measure the photons correctly with 50% probability. Therefore, every time a photon qubit is measured by *Eve* before sending it to Bob, Bob will be left with 75% probability that he will measure the bits correctly and 25% chances that he will measure the bits wrongly. Therefore, it can be seen that a considerable amount of error is introduced by *Eve* by attacking the quantum channel. Hence, there is 25% probability that *Eve's* extracted key is incorrect, and eavesdropping can also be exposed by Alice and Bob. Therefore, a private key will be generated or an eavesdropping will be detected. So, to overcome this obstruction, *Eve* has the option of copying the qubit, and sending the original bit to Bob while keeping the copy to herself.

The qubit which is kept by *Eve* can be measured later on when Alice and Bob discloses their basis of measurements. But this idea is not practical in quantum realms because of the property of no-cloning. Hence, any attempt to copy the qubit will be detected keeping the security of QKD protocols intact [249]. But in such protocols, it is possible that *Eve* pretends to be, Bob to Alice, and pretends to be, Alice to Bob. Therefore, proper *authentication* protocols are required such as [222], [223], [224], [250], [251], [252] to guard against such an attack. Also, QEC codes [17] are there to mitigate various types of attacks by *Eve*, making the communication system secure and sound. The amount of information *Eve* can gain is reduced significantly using these codes and also noise is compensated in channels.

F. End Nodes

End nodes are the most basic and the most important requirement of quantum networks. All the components of practical QI need *end nodes* for long-haul communication to take place. These nodes can be future quantum computers, quantum memories, quantum repeaters, and classical computers working in synergy with future quantum computers. Fidelity can be improved with the help of multiple qubits employed at the end nodes making it a small scale quantum computer for communication purposes. These nodes have different set of functionalities ranging from QKD to distributed quantum computing. An end node type and its corresponding functionality is presented in Table V. Quantum computers were

TABLE V
END NODE COMPLEXITY PERSPECTIVES

End-node type	End-node functionality
Single qubit operation	QKD
Single qubit + memory	Access to connected quantum computers
Multiple qubits (today's scale)	Emerging distributed computing
Full-scale (future) quantum computer	Distributed quantum computing

first introduced way back in 1980's by Feynman in [253], there it was proposed that it is possible for one quantum device to work in synergy with other quantum devices that are more efficient than any classical computer. A quantum Turing machine was suggested by Benioff back in 1982 [254]. Deutsch formulated the first quantum algorithm based on quantum Turing machines in [255], [256]. With all these advancements, the first implementation of real quantum computer was done in 1993 [257]. Also in 1994, Shor in his pioneer research developed a prime factorization algorithm that can factor composite numbers or take discrete logarithms in time polynomial [258]. Therefore, with such a huge computation power, various encryption and security protocols such as RSA [220] and Diffie-Hellman key exchange [259] are at risk. This sets stringent requirements of ultra secure Internet technology.

For the realization of QI to become a reality, the end nodes must have a robust storage of quantum states, until the maximal entanglement is established between the end nodes [2]. For this, entanglement generators must be employed in physical layer of QI functionalities [47]. Quantum repeater stations along with quantum memories are also realized at the end nodes for achieving long haul quantum communications [206]. If all these robust end node types are intermingled efficaciously, the peak stage of the QI may become a reality soon.

V. POSSIBLE APPLICATIONS

Quantum Internet is a diverse field with a possibility of a whole bunch of applications [47]. As this technology is still in its infancy, it is not possible to predict the exact area of applications that it can offer. But, as this technology is developing, many applications are already predicted and proved with relevant literature. Some of them are discussed below like secure communication, blind computing, clock synchronization, longer baseline of telescopes, and Internet of things.

A. Secure Communication

Secure communication is the first and foremost requirement in modern everyday life [260]. There are numerous applications which depends on transfer of data from one node to another using Internet like online banking, stock exchange trading, online shopping, military applications, national security, IoT, etc. QI with various QKD protocols will maintain the security and privacy of the information exchanged over

the Internet [261]. Traditional classical communication in today's world uses various encryption protocols, such as Diffie-Hellman key exchange [259] and RSA protocols [262], in e-commerce websites. These protocols can be cracked with future full-scale quantum computers, putting all the security systems at a risk. But, with QI and security protocols such as, QKD [244], Quantum Secret Sharing (QSS) [263], Quantum Secure Direct Communication (QSDC) [264], quantum teleportation [69], and quantum dense coding [265], any attempt to hack the system will be detected on-site preserving the privacy of systems. QKD has been researched widely, and successfully applied to a distance covering from few hundreds of kilometers [266], [267], [268] to thousands of km with the launch of Micius satellite by scientists from China [43].

QKD can be non-deterministic and deterministic. Non-deterministic QKD can be observed in the BB84 protocol [65] and in BBM92 protocol [23]. In case of QSDC, some secret information is sent securely through a quantum channel directly, without any initial generation of keys [264], [269], [270]. Other protocols based on QSDC are quantum signature [271], quantum dialog [272], [273] and quantum direct secret sharing [274]. The QSDC scheme is also supported by a block transmission technique formulated in [264]. High-dimensional entanglement based QSDC protocol is formulated in [275], [276], [277], multipartite entanglement based protocols are discussed in [278], [279] and hyper-entanglement based protocol is developed in [280], that explains the security of QSDC based quantum communication systems.

As IoT plays an important role in our lives due to wide area of applications [281], [282], [283], thus protecting data involved in wide IoT applications is most important aspect which can be possible with inherently secure QI. The security that relies on the actual encryption primitives is at risk of being compromised by the upcoming quantum computers that are already in development. Quantum attacks [284] that includes *individual, collective or general* attacks using future quantum computation capabilities [49], affect public-key cryptosystems [285]. All these cryptosystems based upon the prime factorization of integers, the elliptic-curve problem of discrete logarithm or the problem of discrete logarithm [258], are vulnerable to quantum attacks by sufficiently powerful quantum computers. Also, Grover's algorithm [286] can be used for attacks on symmetric ciphers by roughly a quadratic factor [287]. Security of IoT will benefit from quantum cryptography as it works on the principles of quantum theorems. It can be applied both in wireless and optical communication, both of which are requirements in security and integrity of IoT systems. Post-quantum IoT cryptosystems has been surveyed in [288] and it can improve the safety of many related fields, that rely heavily on resource-constrained and battery-dependent IoT devices. Post-quantum cryptography refers to cryptographic protocols that are resistant to quantum attacks [284]. It can impact various applications of IoT, that requires critical security, such as defense and public safety [289], industrial IoT railways [290] or smart healthcare [291]. Therefore, the transition from classical primitives to quantum primitives is essential to ensure the overall security of data on the way.

B. Blind Computing

Blind Quantum Computation (BQC) is another application of QI that is related to the security of a user. In this way his privacy is not leaked to a quantum computer, which is involved in computation [292]. The technology to build a quantum computer is moving at a fast pace, but only a few centers in the world may use it because of its superiority and cost. Just like today's supercomputer rental system, users may receive limited access rights. Suppose a user, Alice, wants to have limited access to a mainframe quantum computer, and shares her sensitive information, for computation. The result of this computation is sent back to Alice through the classical channel. In this case, if Alice want the result of computation without revealing her sensitive information, she has to use a BQC protocol. It allows any user to interact with a mainframe quantum computer without revealing her sensitive information to any person (say Bob) having access to mainframe quantum computer [293], [294]. Lately, e-payments, in almost every field, has become the mainstream because of e-commerce websites. However, their security is compromised by emergence of quantum computers in market. Recently, based on BQC, e-payment security evaluation system is employed for evaluating security of network transactions, that guarantees security [295].

BQC was originally proposed by Chaum in 1983 [296] and was first formulated by Childs in 2001 [297], where encryption was secured with OTP using circuit model such that server with full-fleged quantum computer keeps the information private and learns nothing about it. The protocol proposed by Arrighi and Salvail in 2006 [292], requires Alice to prepare and measure the multi-qubit entangled state. In addition, it is sensitive to cheating, which means that, if full-fledged quantum computer does not mind getting caught, he can obtain information. In such a protocol, it was required a constant-sized quantum computer having access to a quantum memory for Alice [298]. A protocol using one-way model [299] was formulated in 2009 by Broadbent *et al.* in [300], where Alice only needs a classical computer and a small scale quantum device that will use randomly rotated single-qubit states for its computation. Hence, this protocol is unconditionally secure and Alice's input and output are kept secret. The security of this protocol is experimentally demonstrated in an optical system [301]. This research has inspired many other researchers to implement more robust blind quantum computation protocols. Hence, QI in future will deploy costly and powerful quantum computers on the cloud, majorly owned by big tech companies. However, in addition to providing security and privacy to the user data, BQC would also check whether the computation is executed by a quantum processor, and is not a fraud.

C. Clock Synchronization

An important issue in many practical applications of modern technologies is accurate timekeeping and synchronization of clocks all over the world [302]. Due to accurate synchronization of clocks, all the scientific applications dependant upon time synchronization, shows minimal errors. These applications include quantum positioning system [303],

synchronization of electric power generators feeding into national power grids, synchronous data transfers and financial transactions, long baseline of telescopes and distributed quantum computation. But, these navigation systems, such as GPS, suffers from security threat known as spoofing [304], [305]. Therefore, a scheme of distributing high precision time data through quantum Micius satellite securely is reported in [7]. It is based on two-way QKD using free-space channel.

As high-phase coherent lasers are developing, optical atomic clocks, operated by several atoms, have reached the Standard Quantum Limit (SQL) with considerable stability. SQL is set by the number of available atoms and interrogation time [306], [307], [308]. Beyond SQL, significant improvements can be achieved in clock performance by preparing atoms in a quantum-related state [6]. For clock synchronization, entanglement techniques are required which connects distant quantum nodes with clocks to be connected in a quantum network [70], [309], [310]. A distributed network of quantum confined clocks, separated by long distances, can be treated as a ultimate clock, where all members in different countries can merge their resources together and coherently achieve higher clock stability. In this way they can distribute this international time scale to everyone in real time. The distributed architecture permits each member of the network to profit from the stability of the local clock signal without losing sovereignty or negotiating to security.

Quantum algorithms are required for addressing the problem of Quantum Clock Synchronization (QCS). It is required to minimise the difference of time, i.e., δ, between two spatially separated clocks with least communication resources. The δ can be calculated accurately and is dependent upon the stability of clock frequency and the uncertainty of the delivery time of messages sent between the two clocks separated by long distance. Presently, protocols are being developed to measure the δ with greater accuracies. Some protocols shows accuracies better than 100 ns for clocks separated by more than 8000 km [311]. With advancements in these protocols such as Ticking Qubit Handshake (TQH), as discussed in [311], this accuracy can be increased to 100 ps. It allows clock synchronization that is not dependent upon uncertainties in delivery time of message between the clocks.

D. Longer Baseline of Telescope

In modern world, astronomy totally depends on very long baseline interferometry between telescope having greater resolving power than a single telescope. Infrared and optical interferometer arrays used in today's world [312], [313] have photons incoming at different telescopes, that must be substantially gathered together for measuring the interference. Due to fluctuations in phase and photon loss in transmission, the baseline can only be limited to a few hundreds, at most. Sufficient sensitivity and improved resolution of telescopes will have many impact on various scientific applications based on space such as; measuring star distance or imaging of planets outside the solar system. Quantum communication using quantum repeaters can reliably send quantum states of qubits over noisy communication channels with [152], that allows the teleportation of quantum states over long distances with least amount of error. Using this technology, the baseline of telescope arrays can be extended as compared to conventional telescopes arrays. If a single pair of telescopes is used, that has a fixed baseline, they would not reconstruct the original distribution of source brightness effectively. Instead of this, if an array of telescopes with different baselines is used, it will acquire much more information than usual [314]. Thus, quantum communication can be applied to extend the baseline of telescopes to exponentially increase the amount of information gathered using traditional schemes.

VI. OPEN PROBLEMS AND CHALLENGES

Here, we present the open problems and challenges that are faced in the process of realization of the quantum networks. We start with the problem of decoherence followed by the effects of decoherence in quantum teleportation, entanglement, design complexity and the issue of collapse of the quantum states when measured.

A. Decoherence

Quantum communication takes place when wave functions of quantum states travel from Alice to Bob through free space or fiber based channels [315]. In physics, two waves are said to be *coherent*, if they maintain fixed phase relationship to each other or changes, according to the laws of physics, with time. Due to environmental effects and fragility of photons carrying the qubits, the interaction of the quantum states with the environment causes loss of photons, and hence the phase relationships are lost. This phenomenon of loss of quantum information in the environment with time is known as *decoherence*. Due to decoherence, quantum states lose their properties and enter the world of classical physics. For preserving the quantum state of photons carrying the information, they must be perfectly-isolated from the environment. However, this isolation is not practical and is hard to achieve considering the current quantum technologies. Decoherence is irreversible and it affects the whole communication process including quantum teleportation process or entanglement generation and distribution process. Reliability of a teleportation system is measured with quantum fidelity which is considered as the fundamental figure of merit, and larger the imperfections introduced by decoherence, the lower is the fidelity. Thus, decoherence degrades the fidelity of teleportation [47], and due to this phenomenon, the quantum states that were pure in nature are converted into mixed states [316].

Decoherence is quantified by *decoherence times*, i.e., time for which the qubits can be entangled without any loss of information. So, the computation must be completed before the qubits loose information. It depends upon the technology used for qubits. Qubits realized with superconducting circuits, exhibits 100 micro-seconds of decoherence time [317], and a much larger decoherence time has been reported with trapped ions [318]. Reliability of a teleportation system is measured with quantum fidelity which is considered as the fundamental figure of merit, and larger the imperfections introduced

by decoherence, the lower is the fidelity. Therefore, classical or QEC techniques are extensively adopted to preserve the quantum information against decoherence and imperfections [319]. Usually, the problem of decoherence is overcome by entanglement distillation [167], [319], [320], which requires an additional level of qubit processing.

B. Imperfect Quantum Teleportation

Imperfections are present in all communication modes, and quantum communication is not an exception. These imperfections result from decoherence, as discussed in Section VI-A. Quantum communication suffers from environmental interactions and loss of photons carrying qubits. Decoherence also affects the quantum teleportation process as well as entanglement generation and distribution process. However, other operations that are applied to quantum states of quantum teleportation process, further introduce imperfections in the teleported qubit [63]. These quantum imperfections are multiplicative in nature, therefore, it can be considered that this phenomenon is more reminiscent of the classical fading effect, rather than the classical additive noise caused by the Brownian motion of electrons [321].

A lot of research is going on to accurately model the quantum-domain of imperfections, that are capable of taking into consideration the different effects of imperfections on the quantum teleportation process [47].

C. Entanglement of Nodes Across the Network

One of the biggest challenge for QI is generation and distribution of entanglement between different nodes across the network. It is the central element to the quantum mechanics and is the most interesting phenomena that has no counterpart in classical communication [70]. An EPR pair generated by striking laser beam to a crystal (see Section III-A), is responsible for entanglement generation and distribution in the quantum teleportation process which is the key functionality of QI. The major challenge that is involved in entanglement distribution is to extend entanglement to nodes that are at a long distance apart as well as storing the states of qubits at the nodes and regularly updating them using quantum codes. This purpose is solved by employing quantum repeaters [322], but despite of all these schemes, extensive research is required in quantum repeaters, quantum memories, QEC codes and entanglement purification and distillation [156], so that multi-party entanglement is free of imperfections and decoherence. Although the physics community has conducted in-depth research on the long-distance entanglement distribution in the past 20 years, and the entanglement distribution rate increases with distance, it still poses a key problem in realization of QI.

D. Design Complexity

Unlike classical communication where data in packets is sent along with copies of the same, just in case the data is lost or attacked, it is impossible in quantum communication to copy or amplify qubits because of the properties of no-cloning theorem [47] and the postulate of measurement of quantum state. This put some stringent design challenges, that

increases the complexity of the design of network functionalities in QI. If we talk about classical error-correcting codes, they cannot be directly applied to quantum communication, because re-transmission of qubits is not possible. Therefore, QEC codes are required and network functionalities have to be designed accordingly making the system complex. Such design complexity is present in every layer of QI design starting from functionality layer of error correcting to the layer of medium access control and route discovery, to the layer-4 protocols such as TCP/IP [2], [323].

A corollary of no-cloning theorem is no-broadcasting theorem [47], where quantum information cannot be transmitted to more than one recipients. Therefore, the link layer must be thoughtfully redesigned to take care of design complexity [63].

E. Measurement of Quantum States

As discussed in Section II-A1, a qubit can be in superposition of the two basis states and measuring the quantum state of qubit will collapse it into one of the basis states [324]. This means that prior to measurement, what amount of information can be stored and transmitted by a qubit is still unknown. The problem of measurement is best illustrated by "paradox" of Schrödinger's cat [64]. A cat can be alive or dead both at the same time due to superposition. Upon measurement, the answers is always a living cat or a dead cat. How a probabilistic result landed into a definite result is still a debatable issue and lots of hidden information is there behind this paradox.

VII. FUTURE DIRECTIONS

Here, we present some future perspectives of QI technology to make this vision a reality.

A. Evolution of Quantum Processors

Quantum computer with great computation capabilities will be required in future QI technologies, for performing complex computations. They can solve the problems that are practically impossible with state-of-the-art supercomputers. The quantum network is becoming powerful and efficient because of the increase in the number of qubits at the end nodes. To meet these requirements, quantum processors with double-digit qubits are evolving, that will shape the future of quantum networking. This technological development would help boost the economies of the world, as various cloud operators will make fortunes, with BQC protocols maintaining user privacy. Also, quantum computers will be linked to each other through pure entanglement, and communication will take place using quantum teleportation. The QI might also assist quantum computer networking to reach even greater performance capacities.

B. Implementation of Trusted Repeater Network

The repeater network plays an important role in modern networking and therefore, a lot of theoretical and practical research have been established [152], [174], [325], [326], even if they are still at a developing stage [327], [328]. Implementing repeater networks requires number of intermediary nodes that are entangled to each other so that entanglement

is generated between two far away end nodes with the phenomena of *entanglement swapping* as discussed in Section IV-B2. Each pair of adjacent repeater nodes exchange the encrypted keys using QKD which allows the far away end nodes to generate their own keys with a assumption that nodes should be trusted. But, until recently in Bristol work [329], trust-free nodes are also proved scalable in a city wide quantum network utilizing entanglement-based QKD. Thus, trusted nodes assumption can be avoided in three ways, firstly by use of entanglement-based QKD [330], measurement-device independent QKD [331], [332], [333], multi-path communication techniques such as quantum network coding [334] and by use of quantum repeaters [152]. But still, trusted repeater is a hot topic of research that will be implemented along with trust-free nodes to overcome distance limitations between QKD nodes.

C. Quantum Error Correcting Codes

The future QI technologies will require advanced QEC codes that works on the basis of encoding qubits carrying quantum information in a unique way that mitigates the influence of noise, decoherence and other environmental factors [17]. After that, quantum information is decoded to retrieve the original quantum state [56]. The Decoherence Free Subspace (DFS) stores data in multiple qubits instead of storing data in a single qubit, which selects specific aspects of the system that are less affected by one or more important environmental factors [335]. In this way, DFS stores data in a subspace of the Hilbert space related to quantum systems that are least influenced by the interaction of its system with the surrounding environment [336], [337]. But, identifying DFS for complex quantum systems is extremely difficult [337], which requires more advanced DFS techniques such as Dynamic Decoupling (DD) [338], [339], where radio-frequency pulses are applied as external interaction to manipulate the non-unitary component of quantum system [339]. Nevertheless, the robust design of the sequence provided by the DD technique suppresses the imperfections in the experiments upto a greater extent [336]. This implies that more advanced techniques are required and further research is needed in QEC codes.

D. Exploring Interface Between DV and CV

Discrete Variable (DV) and Continuous Variable (CV) describes the states where quantum states can be represented in the quantum communications [4], [340]. In DV states, data are represented by discrete features such as the polarization of single photons [69], which can be detected by single-photon detectors. Also, the information is represented by finite number of basis states, such as "qubit" which is the standard unit of DV quantum states. Alternative to this approach are the CV quantum states that were introduced in [23], [341]. Here the information is encoded onto the optical field defined by quadrature variables that constitutes infinite dimensional hilbert space and is useful for quantum information carriers such as lasers [342]. CV states can be detected by highly efficient homodyne or heterodyne detectors having faster transmission rates than single-photon detectors [343]. Therefore, an extensive research in theoretical and experimental domains is needed at the interface of CV and DV states, that will extract the best features from both these technologies to exploit the best of both.

E. Integrating Qubits With Other Technologies

Many powerful computers that are built use different synergies of systems such as bits, neurons, and qubits for computation. Summit supercomputer that has been built by IBM, has a peak performance of 200,000 teraflops, and is the world's most powerful machine that is built on the "bits + neurons" platform. This supercomputer can solve complex computation problems and tasks related to AI. Conclusively, supercomputers based upon "bits + neurons" scheme expedite technologically suitable workloads and deliver novel scientific insights. Neurons can also be combined with qubits, and together they can build a quantum computer with neuron-inspired machine learning algorithms to derive a quantum advantage over classical computation [344]. Qubits along with bits can be another combination based on which quantum processors can be developed [345], that has capabilities well beyond the reach of classical computations. Therefore, exploring possible synergies of "bits + qubits + neurons" will shape the future of computing. With this, the capabilities of "bits + qubits + neurons" must be extensively researched and will remain a topic of active research in coming years. However, some advanced computing systems and use cases are already operating at the intersection between the pairs of these computing methods.

F. Exploration of Solid-State Memories

Solid-state qubits are formed by electron spins [118] followed by superconducting circuits [119], comprising of Josephson junctions, interconnects, and passive elements, that are designed to behave as a quantum mechanical two-stage system with good isolation. Solid state quantum memories are more advantageous and attractive as they can maintain its coherence even at cryogenic temperatures. For example, crystalline-solid spin ensembles formed by implanting defects in lattice; such as implanting Nitrogen-Vacancy (NV) centers into diamonds, or by rare-earth-doped crystals, can be proved coherent for hours at cryogenic temperatures. Hence, comprehensive efforts are needed to explore the union of superconducting processors and solid-state quantum memories to enhance the performance of transmission and generation of microwave photons. Accordingly, steps must be taken to investigate on-chip teleportation between a superconducting qubit and NV in a local quantum memory. If these integrations are successful, this hybrid technology would become the most encouraging design to be scaled up into a comprehensive quantum network. Therefore, employing such hybrid quantum computers as end nodes in quantum networking, the next 5-10 years could see the implementation of a hybrid-technology QI globally.

G. Quantum-Classical Synergy

A future QI will soon be developed owing to the launch of various quantum satellites paving the way for

long-distance entanglement and QKD with eavesdropping detection. Quantum communication links will require already mature fiber channels for the exchange of classical data required for the quantum teleportation process [233]. QKD also requires classical channels for information reconciliation and privacy amplification, to achieve higher key rates and reduced latencies over noisy communication channels [246]. A fully secure QKD based channels will ultimately connect classical devices such as mobiles, tablets, smart wearables, satellites, smart vehicles with utmost security. A secure quantum cloud will exist, that will take care of user privacy and its data through BQC. Thus, future QI will work in synergy with the classical Internet giving rise to a universe of applications with excellent security.

VIII. Conclusion

In this survey, we have discussed the quantum Internet and its technological advances that cover the basic concepts to understand this novel technology. We have introduced the readers to the basic physics underlying this technology and the unmatched security and privacy that it offers due to laws of inherently secure quantum mechanics. The future quantum Internet will bring security based on various quantum key distribution algorithms and will enable networking of classical and quantum nodes that are located remotely. The most important and challenging requirement for quantum Internet is quantum teleportation based on entanglement generation and distribution between a network of far-away nodes. For this, quantum repeaters are employed that generate entanglement between far-away nodes with the help of entanglement swapping among pairwise intermediary nodes, where the quantum information is stored in local quantum memories. The quantum information is fragile, which means that environmental effects such as decoherence, where quantum information is lost with time, will negatively impact quantum communication. Due to decoherence, quantum states lose their properties and enters the world of classical physics. Therefore, realization of the quantum Internet technology will come with lots of design challenges and complexities. Consequently, multidisciplinary efforts will be required that will pave the way for the realization of a full-fledged quantum Internet. A breakthrough has been achieved since the launch of the quantum satellites that have achieved QKD between two far-away ground stations, which has motivated various research groups to speed up the efforts to build a full-blown quantum Internet in near future.

References

[1] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[2] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, Oct. 2018, Art. no. eaam9288.

[3] R. Van Meter, "Quantum networking and Internetworking," *IEEE Netw.*, vol. 26, no. 4, pp. 59–64, Jul./Aug. 2012.

[4] M. A. Nielsen, I. Chuang, and L. K. Grover, "Quantum computation and quantum information," *Amer. J. Phys.*, vol. 70, no. 5, pp. 558–559, May 2002.

[5] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[6] P. Komar *et al.*, "A quantum network of clocks," *Nat. Phys.*, vol. 10, no. 8, pp. 582–587, 2014.

[7] H. Dai *et al.*, "Towards satellite-based quantum-secure time transfer," *Nat. Phys.*, vol. 16, no. 8, pp. 848–852, May 2020.

[8] T. B. Bahder, "Quantum positioning system," in *Proc. 36th Annu. Precise Time Time Interval Syst. Appl. Meeting*, Dec. 2004, pp. 53–76.

[9] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, p. 661, Aug. 1991.

[10] C. Crépeau, D. Gottesman, and A. Smith, "Secure multi-party quantum computation," in *Proc. 34th Annu. ACM Symp. Theory Comput.*, May 2002, pp. 643–652.

[11] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation," *Phys. Rev. A*, vol. 96, no. 1, 2017, Art. no. 012303.

[12] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced measurements: Beating the standard quantum limit," *Science*, vol. 306, no. 5700, pp. 1330–1336, 2004.

[13] D. Gottesman, T. Jennewein, and S. Croke, "Longer-baseline telescopes using quantum repeaters," *Phys. Rev. Lett.*, vol. 109, no. 7, 2012, Art. no. 070503.

[14] H. E. Brandt, "Qubit devices and the issue of quantum decoherence," *Progr. Quantum Electron.*, vol. 22, nos. 5–6, pp. 257–370, 1999.

[15] R. Valivarthi *et al.*, "Quantum teleportation across a metropolitan fibre network," *Nat. Photon.*, vol. 10, no. 10, pp. 676–680, 2016.

[16] J.-G. Ren *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, 2017.

[17] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, no. 2, p. 900, Feb. 1997.

[18] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. Hollenberg, "Surface code quantum communication," *Phys. Rev. Lett.*, vol. 104, no. 18, 2010, Art. no. 180503.

[19] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories," *Nat. Photon.*, vol. 6, no. 11, pp. 777–781, 2012.

[20] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Ultrafast and fault-tolerant quantum communication across long distances," *Phys. Rev. Lett.*, vol. 112, no. 25, 2014, Art. no. 250501.

[21] N. Promwongsa *et al.*, "A comprehensive survey of the tactile Internet: State-of-the-art and research directions," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 472–523, 1st Quart., 2021.

[22] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an Internet of Secure Things: A survey on issues and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1372–1391, 2nd Quart., 2020.

[23] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, p. 3121, 1992.

[24] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *NPJ Quantum Inf.*, vol. 2, no. 1, pp. 1–12, 2016.

[25] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, "Entanglement distribution over 300 km of fiber," *Opt. Exp.*, vol. 21, no. 20, pp. 23241–23249, 2013.

[26] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075001.

[27] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network ," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011.

[28] D. Stucki *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, 2011, Art. no. 123001.

[29] S. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Exp.*, vol. 22, no. 18, pp. 21739–21756, 2014.

[30] R. Courtland, "China's 2,000-km quantum link is almost complete [news]," *IEEE Spectr.*, vol. 53, no. 11, pp. 11–12, Nov. 2016.

[31] M. Caleffi, D. Chandra, D. Cuomo, S. Hassanpour, and A. S. Cacciapuoti, "The rise of the quantum Internet," *Computer*, vol. 53, no. 6, pp. 67–72, Jun. 2020.

[32] S. Pirandola and S. L. Braunstein, "Physics: Unite to build a quantum Internet," *Nat. News*, vol. 532, no. 7598, pp. 169–171, Apr. 2016.

[33] D. Castelvecchi, "IBM's quantum cloud computer goes commercial," *Nat. News*, vol. 543, no. 7644, p. 159, Mar. 2017.

[34] J. Kelly, Z. Chen, B. Chiaro, B. Foxen, J. Martinis, and Quantum Hardware Team, "Operating and characterizing of a 72 superconducting qubit processor 'Bristlecone': Part 1," in *Proc. APS Meeting Abstracts*, vol. 2019, Jan. 2019, Art. no. A42.002.

[35] J. Preskill, "Quantum computing and the entanglement frontier," 2012. [Online]. Available: arXiv:1203.5813.

[36] Y. Cao *et al.*, "Quantum chemistry in the age of quantum computing," *Chem. Rev.*, vol. 119, no. 19, pp. 10856–10915, 2019.

[37] K. Bourzac, "4 tough chemistry problems that quantum computers will solve [News]," *IEEE Spectr.*, vol. 54, no. 11, pp. 7–9, Nov. 2017.

[38] D. Gil and W. M. J. Green, "1.4 the future of computing: Bits + neurons + qubits," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Apr. 2020, pp. 30–39.

[39] E. Gibney, "Billion-euro boost for quantum tech: Third European Union flagship project will be similar in size and ambition to graphene and human-brain initiatives," *Nature*, vol. 532, no. 7600, pp. 426–427, 2016.

[40] E. Cartlidge, *Europe's Euro1 Billion Quantum Flagship Announces Grants*, Amer. Assoc. Adv. Sci., Washington, DC, USA, Nov. 2018.

[41] (2018). *Quantum Internet Alliance*. [Online]. Available: https://quantum-internet.team

[42] C. Monroe, M. G. Raymer, and J. Taylor, "The U.S. National Quantum Initiative: From act to action" *Science*, vol. 364, no. 6439, pp. 440–442, 2019.

[43] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[44] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Comput. Sci. Rev.*, vol. 31, pp. 51–71, Feb. 2019.

[45] S. Pirandola and S. Mancini, "Quantum teleportation with continuous variables: A survey," *Laser Phys.*, vol. 16, pp. 1418–1438, Oct. 2006.

[46] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nat. Photon.*, vol. 9, no. 10, pp. 641–652, Sep. 2015.

[47] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum Internet," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3808–3833, Jun. 2020.

[48] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1149–1205, 2nd Quart., 2018.

[49] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Modern Phys.*, vol. 92, no. 2, 2020, Art. no. 025002.

[50] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, p. 1301, Sep. 2009.

[51] G. Adesso and F. Illuminati, "Entanglement in continuous-variable systems: Recent advances and current perspectives," *J. Phys. A Math. Theor.*, vol. 40, no. 28, p. 7821, 2007.

[52] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *NPJ Quantum Inf.*, vol. 3, no. 1, pp. 1–13, 2017.

[53] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 1st Quart., 2019.

[54] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, no. 8, pp. 595–604, Jul. 2014.

[55] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, Jun. 2020.

[56] Z. Babar *et al.*, "Duality of quantum and classical error correction codes: Design principles and examples," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 970–1010, 1st Quart., 2018.

[57] J.-Y. Hu *et al.*, "Experimental quantum secure direct communication with single photons," *Light Sci. Appl.*, vol. 5, no. 9, 2016, Art. no. e16144.

[58] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *J. Amer. Inst. Electr. Eng.*, vol. 45, no. 2, pp. 109–115, Feb. 1926.

[59] Y. Kanamori, S.-M. Yoo, W. Pan, and F. T. Sheldon, "A short survey on quantum computers," *Int. J. Comput. Appl.*, vol. 28, no. 3, pp. 227–233, 2006.

[60] A. K. Pati, "Minimum classical bit for remote preparation and measurement of a qubit," *Phys. Rev. A*, vol. 63, no. 1, Dec. 2000, Art. no. 014302.

[61] L. E. Ballentine, "States, pure and mixed, and their representations," in *Compendium Quantum Physics*. Heidelberg, Germany: Springer, 2009, pp. 744–746.

[62] H. Wimmel, *Quantum Physics and Observed Reality: A Critical Interpretation of Quantum Mechanics*. Singapore: World Sci., 1992.

[63] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum Internet: Networking challenges in distributed quantum computing," *IEEE Netw.*, vol. 31, no. 1, pp. 137–143, Jan./Feb. 2020.

[64] E. Schrödinger, "Die gegenwärtige situation in der quantenmechanik," *Naturwissenschaften*, vol. 23, no. 49, pp. 823–828, Dec. 1935.

[65] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. Int. Conf. Comput. Syst. Signal Process.*, Dec. 1984, pp. 175–179.

[66] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.*, vol. 47, no. 10, p. 777, May 1935.

[67] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Phys. Physique Fizika*, vol. 1, no. 3, pp. 195–200, Nov. 1964.

[68] E. Hagley *et al.*, "Generation of Einstein-Podolsky-Rosen pairs of atoms," *Phys. Rev. Lett.*, vol. 79, no. 1, pp. 1–5, Jul. 1997.

[69] 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," *Phys. Rev. Lett.*, vol. 70, no. 13, p. 1895, Mar. 1993.

[70] H. J. Kimble, "The quantum Internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[71] D. Bohm, "A suggested interpretation of the quantum theory in terms of 'hidden' variables. I," *Phys. Rev.*, vol. 85, no. 2, p. 166, Jan. 1952.

[72] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories," *Phys. Rev. Lett.*, vol. 28, no. 14, pp. 938–941, Apr. 1972.

[73] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of Bell's inequalities using time-varying analyzers," *Phys. Rev. Lett.*, vol. 49, no. 25, p. 1804, Dec. 1982.

[74] Z. Ou and L. Mandel, "Violation of Bell's inequality and classical probability in a two-photon correlation experiment," *Phys. Rev. Lett.*, vol. 61, no. 1, p. 50, Jul. 1988.

[75] B. Hensen *et al.*, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, no. 7575, pp. 682–686, 2015.

[76] M. Giustina *et al.*, "Significant-loophole-free test of Bell's theorem with entangled photons," *Phys. Rev. Lett.*, vol. 115, no. 25, Dec. 2015, Art. no. 250401.

[77] L. K. Shalm *et al.*, "Strong loophole-free test of local realism," *Phys. Rev. Lett.*, vol. 115, no. 25, Dec. 2015, Art. no. 250402.

[78] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*. Dordrecht, The Netherlands: Springer, 1989, pp. 69–72.

[79] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, Oct. 1995, Art. no. R2493.

[80] M. Erhard, M. Krenn, and A. Zeilinger, "Advances in high-dimensional quantum entanglement," *Nat. Rev. Phys.*, vol. 2, no. 7, pp. 365–381, Jun. 2020.

[81] R. Van Meter, *Quantum Networking*. London, U.K.: Wiley, 2014.

[82] S. Stenholm and P. J. Bardroff, "Teleportation of N-dimensional states," *Phys. Rev. A*, vol. 58, no. 6, p. 4373, Dec. 1998.

[83] C. Cabrillo, J. I. Cirac, P. Garcia-Fernandez, and P. Zoller, "Creation of entangled states of distant atoms by interference," *Phys. Rev. A*, vol. 59, no. 2, p. 1025, Feb. 1999.

[84] S. Bose, P. Knight, M. Plenio, and V. Vedral, "Proposal for teleportation of an atomic state via cavity decay," *Phys. Rev. Lett.*, vol. 83, no. 24, p. 5158, Dec. 1999.

[85] M. H. Rubin, D. N. Klyshko, Y. Shih, and A. Sergienko, "Theory of two-photon entanglement in type-II optical parametric down-conversion," *Phys. Rev. A*, vol. 50, no. 6, p. 5122, Dec. 1994.

[86] S. Ritter *et al.*, "An elementary quantum network of single atoms in optical cavities," *Nature*, vol. 484, no. 7393, pp. 195–200, Apr. 2012.

[87] S. Welte, B. Hacker, S. Daiss, S. Ritter, and G. Rempe, "Photon-mediated quantum gate between two neutral atoms in an optical cavity," *Phys. Rev. X*, vol. 8, no. 1, Feb. 2018, Art. no. 011018.

[88] C.-K. Hong, Z.-Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Phys. Rev. Lett.*, vol. 59, no. 18, p. 2044, Nov. 1987.

[89] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "'Event-ready-detectors Bell' experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, no. 26, pp. 4287–4290, Dec. 1993.

[90] C. Ferrari and B. Braunecker, "Entanglement, which-way measurements, and a quantum erasure," *Amer. J. Phys.*, vol. 78, no. 8, pp. 792–795, 2010.

[91] T. Northup and R. Blatt, "Quantum information transfer using photons," *Nat. Photon.*, vol. 8, no. 5, p. 356, Apr. 2014.

[92] M. Caleffi, "Optimal routing for quantum networks," *IEEE Access*, vol. 5, pp. 22299–22312, 2017.

[93] A. Armour, M. Blencowe, and K. Schwab, "Entanglement and decoherence of a micromechanical resonator via coupling to a cooper-pair box," *Phys. Rev. Lett.*, vol. 88, Mar. 2002, Art. no. 148301.

[94] E. K. Irish and K. Schwab, "Quantum measurement of a coupled nanomechanical resonator—Cooper-pair box system," *Phys. Rev. B*, vol. 68, no. 15, Oct. 2003, Art. no. 155311.

[95] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, "Decoherence, continuous observation, and quantum computing: A cavity QED model," *Phys. Rev. Lett.*, vol. 75, no. 21, p. 3788, Nov. 1995.

[96] S. Van Enk, J. Cirac, and P. Zoller, "Purifying two-bit quantum gates and joint measurements in cavity QED," *Phys. Rev. Lett.*, vol. 79, no. 25, p. 5178, Dec. 1997.

[97] Y. Shih and C. O. Alley, "New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion," *Phys. Rev. Lett.*, vol. 61, no. 26, p. 2921, Dec. 1988.

[98] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, no. 24, p. 4337, Dec. 1995.

[99] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.*, vol. 74, no. 1, p. 145, Mar. 2002.

[100] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, pp. 575–579, 1997.

[101] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Phys. Rev. Lett.*, vol. 80, no. 18, p. 3891, May 1998.

[102] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, "Experimental demonstration of four-photon entanglement and high-fidelity teleportation," *Phys. Rev. Lett.*, vol. 86, no. 20, p. 4435, May 2001.

[103] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 80, no. 6, p. 1121, Feb. 1998.

[104] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional quantum teleportation," *Science*, vol. 282, no. 5389, pp. 706–709, 1998.

[105] H.-S. Zhong *et al.*, "Quantum computational advantage using photons," *Science*, vol. 370, no. 6523, pp. 1460–1463, 2020.

[106] D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem," *IET Quantum Commun.*, vol. 1, no. 1, pp. 3–8, May 2020.

[107] D. Nigg *et al.*, "Quantum computations on a topologically encoded qubit," *Science*, vol. 345, no. 6194, pp. 302–305, 2014.

[108] E. P. Gale, Z. Mehdi, L. M. Oberg, A. K. Ratcliffe, S. A. Haine, and J. J. Hope, "Optimized fast gates for quantum computing with trapped ions," *Phys. Rev. A*, vol. 101, May 2020, Art. no. 052328.

[109] C. Monroe and J. Kim, "Scaling the ion trap quantum processor," *Science*, vol. 339, no. 6124, pp. 1164–1169, Mar. 2013.

[110] Y. Lu *et al.*, "Dark-state cooling of a trapped ion using microwave coupling," *Phys. Rev. A*, vol. 92, no. 2, 2015, Art. no. 023420.

[111] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Phys. Rev. Lett.*, vol. 74, no. 20, p. 4091, May 1995.

[112] T. Harty *et al.*, "High-fidelity preparation, gates, memory, and read-out of a trapped-ion quantum bit," *Phys. Rev. Lett.*, vol. 113, no. 22, Nov. 2014, Art. no. 220501.

[113] J. P. Gaebler *et al.*, "High-fidelity universal gate set for 9_{Be+} ion qubits," *Phys. Rev. Lett.*, vol. 117, no. 6, Aug. 2016, Art. no. 60505.

[114] C. Ballance, T. Harty, N. Linke, M. Sepiol, and D. Lucas, "High-fidelity quantum logic gates using trapped-ion hyperfine qubits," *Phys. Rev. Lett.*, vol. 117, no. 6, Aug. 2016, Art. no. 060504.

[115] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Demonstration of a small programmable quantum computer with atomic qubits," *Nature*, vol. 536, no. 7614, pp. 63–66, Aug. 2016.

[116] D. P. D. Vincenzo, "Quantum computation," *Science*, vol. 270, no. 5234, pp. 255–261, Oct. 1995.

[117] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, pp. 45–53, Mar. 2010.

[118] D. Loss and D. P. D. Vincenzo, "Quantum computation with quantum dots," *Phys. Rev. A*, vol. 57, no. 1, p. 120, Jan. 1998.

[119] M. Kjaergaard *et al.*, "Superconducting qubits: Current state of play," *Annu. Rev. Condens. Mat. Phys.*, vol. 11, no. 1, pp. 369–395, 2020.

[120] W. Gao *et al.*, "Quantum teleportation from a propagating photon to a solid-state spin qubit," *Nat. Commun.*, vol. 4, no. 1, pp. 1–8, 2013.

[121] F. Bussières *et al.*, "Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory," *Nat. Photon.*, vol. 8, no. 10, pp. 775–778, Sep. 2014.

[122] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019.

[123] W. D. Oliver, "Quantum computing takes flight," *Nature*, vol. 574, no. 7779, pp. 487–488, Oct. 2019.

[124] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver, "A quantum engineer's guide to superconducting qubits," *Appl. Phys. Rev.*, vol. 6, no. 2, Jun. 2019, Art. no. 021318.

[125] D.-R. W. Yost *et al.*, "Solid-state qubits integrated with superconducting through-silicon vias," *NPJ Quantum Inf.*, vol. 6, no. 1, pp. 1–7, Jul. 2020.

[126] L. Steffen *et al.*, "Deterministic quantum teleportation with feed-forward in a solid state system," *Nature*, vol. 500, no. 7462, pp. 319–322, Aug. 2013.

[127] I. Marcikic, H. De Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, "Long-distance teleportation of qubits at telecommunication wavelengths," *Nature*, vol. 421, no. 6922, pp. 509–513, Jan. 2003.

[128] O. Landry, J. A. W. van Houwelingen, A. Beveratos, H. Zbinden, and N. Gisin, "Quantum teleportation over the Swisscom telecommunication network," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 24, no. 2, pp. 398–403, 2007.

[129] M. Barrett *et al.*, "Deterministic quantum teleportation of atomic qubits," *Nature*, vol. 429, no. 6993, pp. 737–739, Jun. 2004.

[130] R. Ursin *et al.*, "Quantum teleportation across the Danube," *Nature*, vol. 430, no. 7002, p. 849, Aug. 2004.

[131] J. Yin *et al.*, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," *Nature*, vol. 488, no. 7410, pp. 185–188, Aug. 2012.

[132] R. Ursin *et al.*, "Entanglement-based quantum communication over 144 km," *Nat. Phys.*, vol. 3, no. 7, pp. 481–486, Jun. 2007.

[133] S. L. Braunstein and H. J. Kimble, "Teleportation of continuous quantum variables," *Phys. Rev. Lett.*, vol. 80, no. 4, p. 869, 1998.

[134] V. Gorbachev and A. Trubilko, "Quantum teleportation of Einstein-Podolsky-Rosen pair with the help of crossroads three particle state," *Zhurnal Ehksperimental'noj Teoreticheskoj Fiziki*, vol. 118, no. 5, pp. 1036–1040, 2000.

[135] J. Lee and M. Kim, "Entanglement teleportation via werner states," *Phys. Rev. Lett.*, vol. 84, no. 18, p. 4236, May 2000.

[136] M. Ikram, S.-Y. Zhu, and M. S. Zubairy, "Quantum teleportation of an entangled state," *Phys. Rev. A*, vol. 62, no. 2, Jul. 2000, Art. no. 022307.

[137] B.-S. Shi, Y.-K. Jiang, and G.-C. Guo, "Probabilistic teleportation of two-particle entangled state," *Phys. Lett. A*, vol. 268, no. 3, pp. 161–164, Apr. 2000.

[138] Z. He, Z. Xiong, and Y. Zhang, "Influence of intrinsic decoherence on quantum teleportation via two-qubit Heisenberg XYZ chain," *Phys. Lett. A*, vol. 354, nos. 1–2, pp. 79–83, 2006.

[139] S. Salek, D. Ebler, and G. Chiribella, "Quantum communication in a superposition of causal orders," Sep. 2018. [Online]. Available: arXiv:1809.06655.

[140] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, "Quantum computations without definite causal structure," *Phys. Rev. A*, vol. 88, no. 2, Aug. 2013, Art. no. 022318.

[141] M. Caleffi and A. S. Cacciapuoti, "Quantum switch for the quantum Internet: Noiseless communications through noisy channels," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 575–588, Mar. 2020.

[142] G. Chiribella and H. Kristjánsson, "Quantum Shannon theory with superpositions of trajectories," *Proc. Royal Soc. A*, vol. 475, no. 2225, May 2019, Art. no. 20180903.

[143] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[144] G. Chiribella, "Perfect discrimination of no-signalling channels via quantum superposition of causal structures," *Phys. Rev. A*, vol. 86, no. 4, 2012, Art. no. 040301.

[145] A. Feix, M. Araújo, and Č. Brukner, "Quantum superposition of the order of parties as a communication resource," *Phys. Rev. A*, vol. 92, no. 5, 2015, Art. no. 052326.

[146] O. Oreshkov, F. Costa, and Č. Brukner, "Quantum correlations with no causal order," *Nat. Commun.*, vol. 3, no. 1, pp. 1–8, Oct. 2012.

[147] P. A. Guérin, A. Feix, M. Araújo, and Č. Brukner, "Exponential communication complexity advantage from quantum superposition of the direction of communication," *Phys. Rev. Lett.*, vol. 117, no. 10, 2016, Art. no. 100502.

[148] P. A. Guérin, G. Rubino, and Č. Brukner, "Communication through quantum-controlled noise," *Phys. Rev. A*, vol. 99, no. 6, Jun. 2019, Art. no. 062317.

[149] G. Chiribella *et al.*, "Indefinite causal order enables perfect quantum communication with zero capacity channels," *New J. Phys.*, vol. 23, Mar. 2021, Art. no. 033039.

[150] K. Goswami *et al.*, "Indefinite causal order in a quantum switch," *Phys. Rev. Lett.*, vol. 121, no. 9, Aug. 2018, Art. no. 090503.

[151] Y. Guo *et al.*, "Experimental transmission of quantum information using a superposition of causal orders," *Phys. Rev. Lett.*, vol. 124, no. 3, Jan. 2020, Art. no. 030502.

[152] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The Role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, no. 26, p. 5932, Dec. 1998.

[153] D. Dieks, "Communication by EPR devices," *Phys. Lett. A*, vol. 92, no. 6, pp. 271–272, Nov. 1982.

[154] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 78–90, May/Jun. 2015.

[155] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, no. 5, pp. 722–725, Jan. 1996.

[156] X.-M. Hu *et al.*, "Long-distance entanglement purification for quantum communication," *Phys. Rev. Lett.*, vol. 126, Jan. 2021, Art. no. 010503.

[157] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum repeater with encoding," *Phys. Rev. A*, vol. 79, Mar. 2009, Art. no. 032325.

[158] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, "From quantum multiplexing to high-performance quantum networking," *Nat. Photon.*, vol. 4, no. 11, pp. 792–796, Aug. 2010.

[159] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nat. Commun.*, vol. 6, no. 1, pp. 1–7, Apr. 2015.

[160] F. Rozpedek *et al.*, "Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission," *Phys. Rev. A*, vol. 99, no. 5, May 2019, Art. no. 052330.

[161] S. Santra, S. Muralidharan, M. Lichtman, L. Jiang, C. Monroe, and V. S. Malinovsky, "Quantum repeaters based on two species trapped ions," *New J. Phys.*, vol. 21, no. 7, Jul. 2019, Art. no. 073002.

[162] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon, "Light-matter entanglement over 50 km of optical fibre," *NPJ Quantum Inf.*, vol. 5, no. 1, pp. 1–5, Aug. 2019.

[163] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," *Sci. Rep.*, vol. 6, no. 1, pp. 1–10, Feb. 2016.

[164] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Modern Phys.*, vol. 83, no. 1, p. 33, Mar. 2011.

[165] J. Dias and T. C. Ralph, "Quantum repeaters using continuous-variable teleportation," *Phys. Rev. A*, vol. 95, no. 2, Feb. 2017, Art. no. 022312.

[166] F. Furrer and W. J. Munro, "Repeaters for continuous-variable quantum communication," *Phys. Rev. A*, vol. 98, no. 3, Sep. 2018, Art. no. 032335.

[167] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, Nov. 2001.

[168] C. Chou, S. Polyakov, A. Kuzmich, and H. Kimble, "Single-photon generation from stored excitation in an atomic ensemble," *Phys. Rev. Lett.*, vol. 92, no. 21, May 2004, Art. no. 213601.

[169] C. H. van der Wal *et al.*, "Atomic memory for correlated photon states," *Science*, vol. 301, no. 5630, pp. 196–200, Jul. 2003.

[170] A. Kuzmich *et al.*, "Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles," *Nature*, vol. 423, no. 6941, pp. 731–734, Jun. 2003.

[171] D. Matsukevich and A. Kuzmich, "Quantum state transfer between matter and light," *Science*, vol. 306, no. 5696, pp. 663–666, Oct. 2004.

[172] C.-W. Chou, H. de Riedmatten, D. Felinto, S. V. Polyakov, S. J. Van Enk, and H. J. Kimble, "Measurement-induced entanglement for excitation stored in remote atomic ensembles," *Nature*, vol. 438, no. 7069, pp. 828–832, Dec. 2005.

[173] C.-W. Chou *et al.*, "Functional quantum nodes for entanglement distribution over scalable quantum networks," *Science*, vol. 316, no. 5829, pp. 1316–1320, Jun. 2007.

[174] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, "Experimental demonstration of a BDCZ quantum repeater node," *Nature*, vol. 454, no. 7208, pp. 1098–1101, Aug. 2008.

[175] V. Vedral and M. B. Plenio, "Entanglement measures and purification procedures," *Phys. Rev. A*, vol. 57, no. 3, p. 1619, Mar. 1998.

[176] T. Shang, X.-J. Zhao, and J.-W. Liu, "Quantum network coding based on controlled teleportation," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 865–868, May 2014.

[177] H. V. Nguyen *et al.*, "Towards the quantum Internet: Generalised quantum network coding for large-scale quantum communication networks," *IEEE Access*, vol. 5, pp. 17288–17308, 2017.

[178] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New J. Phys.*, vol. 4, no. 1, p. 43, Jan. 2002.

[179] C. Kurtsiefer *et al.*, "A step towards global key distribution," *Nature*, vol. 419, no. 6906, p. 450, Oct. 2002.

[180] D. M. Benton, P. M. Gorman, P. R. Tapster, and D. M. Taylor, "A compact free space quantum key distribution system capable of daylight operation," *Opt. Commun.*, vol. 283, no. 11, pp. 2465–2471, Jun. 2010.

[181] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045007.

[182] A. Tunick, T. Moore, K. Deacon, and R. Meyers, "Review of representative free-space quantum communications experiments," in *Proc. Quantum Commun. Quantum Imag. VIII*, vol. 7815, Aug. 2010, Art. no. 781512.

[183] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," in *Proc. Quantum Inf. Comput. III*, vol. 5815, May 2005, pp. 138–149.

[184] A. Fedrizzi *et al.*, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nat. Phys.*, vol. 5, no. 6, pp. 389–392, May 2009.

[185] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A Communication theory perspective," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2231–2258, 4th Quart., 2014.

[186] P. Villoresi *et al.*, "Experimental verification of the feasibility of a quantum channel between space and earth," *New J. Phys.*, vol. 10, no. 3, Mar. 2008, Art. no. 033038.

[187] L. Allen, M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, "Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes," *Phys. Rev. A*, vol. 45, no. 11, p. 8185, Jun. 1992.

[188] M. Mafu *et al.*, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," *Phys. Rev. A*, vol. 88, no. 3, Sep. 2013, Art. no. 032305.

[189] G. Vallone *et al.*, "Free-space quantum key distribution by rotation-invariant twisted photons," *Phys. Rev. Lett.*, vol. 113, no. 6, Aug. 2014, Art. no. 060503.

[190] S. K. Goyal, F. S. Roux, T. Konrad, A. Forbes, and A. H. Ibrahim, "The effect of turbulence on entanglement-based free-space quantum key distribution with photonic orbital angular momentum," *J. Opt.*, vol. 18, no. 6, Apr. 2016, Art. no. 064002.

[191] S. Zhao, J. Leach, L. Gong, J. Ding, and B. Zheng, "Aberration corrections for free-space optical communications in atmosphere turbulence using orbital angular momentum states," *Opt. Exp.*, vol. 20, no. 1, pp. 452–461, Dec. 2012.

[192] A. E. Willner *et al.*, "Optical communications using orbital angular momentum beams," *Adv. Opt. Photon.*, vol. 7, no. 1, pp. 66–106, Mar. 2015.

[193] T. Brünner and F. S. Roux, "Robust entangled qutrit states in atmospheric turbulence," *New J. Phys.*, vol. 15, no. 6, Jun. 2013, Art. no. 063005.

[194] J. R. G. Alonso and T. A. Brun, "Protecting orbital-angular-momentum photons from decoherence in a turbulent atmosphere," *Phys. Rev. A*, vol. 88, no. 2, Aug. 2013, Art. no. 022326.

[195] M. Aspelmeyer *et al.*, "Long-distance free-space distribution of quantum entanglement," *Science*, vol. 301, no. 5633, pp. 621–623, Aug. 2003.

[196] M. Krenn, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, "Quantum communication with photons," in *Optics in Our Time*, vol. 18. Cham, Switzerland: Springer, 2016, p. 455.

[197] V. Sharma and S. Banerjee, "Analysis of atmospheric effects on satellite-based quantum communication: A comparative study," *Quantum Inf. Process.*, vol. 18, no. 3, p. 67, Jan. 2019.

[198] J. Ballato *et al.*, "Silicon optical fiber," *Opt. Exp.*, vol. 16, no. 23, pp. 18675–18683, Oct. 2008.

[199] A. Dhar, S. Das, H. S. Maiti, and R. Sen, "Fabrication of high aluminium containing rare-earth doped fiber without core–clad interface defects," *Opt. Commun.*, vol. 283, no. 11, pp. 2344–2349, Jun. 2010.

[200] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, "High-dimensional quantum communication: Benefits, progress, and future challenges," *Adv. Quantum Technol.*, vol. 2, no. 12, Oct. 2019, Art. no. 1900038.

[201] H. Takesue *et al.*, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nat. Photon.*, vol. 1, no. 6, pp. 343–348, Jun. 2007.

[202] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.*, vol. 6, no. 1, pp. 1–9, Jan. 2016.

[203] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, 2016, Art. no. 190501.

[204] L. Ma, O. Slattery, and X. Tang, "Optical quantum memory and its applications in quantum communication systems," *J. Res. Nat. Inst. Stand. Technol.*, vol. 125, Jan. 2020, Art. no. 125002.

[205] P. Botsinis *et al.*, "Quantum search algorithms for wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1209–1242, 2nd Quart., 2019.

[206] C. Simon *et al.*, "Quantum memories," *Eur. Phys. J. D*, vol. 58, no. 1, pp. 1–22, Apr. 2010.

[207] L.-M. Duan and C. Monroe, "Colloquium: Quantum networks with trapped ions," *Rev. Modern Phys.*, vol. 82, no. 2, p. 1209, Apr. 2010.

[208] B. Julsgaard, A. Kozhekin, and E. S. Polzik, "Experimental long-lived entanglement of two macroscopic objects," *Nature*, vol. 413, no. 6854, pp. 400–403, Sep. 2001.

[209] D.-S. Ding, "Raman quantum memory of photonic polarized entanglement," in *Broad Bandwidth and High Dimensional Quantum Memory Based on Atomic Ensembles*. Singapore: Springer, Dec. 2018, pp. 91–107.

[210] K. S. Choi, H. Deng, J. Laurat, and H. Kimble, "Mapping photonic entanglement into and out of a quantum memory," *Nature*, vol. 452, no. 7183, pp. 67–71, Mar. 2008.

[211] I. Usmani, C. Clausen, F. Bussières, N. Sangouard, M. Afzelius, and N. Gisin, "Heralded quantum entanglement between two crystals," *Nat. Photon.*, vol. 6, no. 4, pp. 234–237, Mar. 2012.

[212] Z.-Q. Zhou *et al.*, "Quantum storage of three-dimensional orbital-angular-momentum entanglement in a crystal," *Phys. Rev. Lett.*, vol. 115, no. 7, Aug. 2015, Art. no. 070502.

[213] K. Jensen *et al.*, "Quantum memory for entangled continuous-variable states," *Nat. Phys.*, vol. 7, no. 1, pp. 13–16, Nov. 2011.

[214] Z. Yan *et al.*, "Establishing and storing of deterministic quantum entanglement among three distant atomic ensembles," *Nat. Commun.*, vol. 8, no. 1, pp. 1–8, 2017.

[215] P. Vernaz-Gris, K. Huang, M. Cao, A. S. Sheremet, and J. Laurat, "Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble," *Nat. Commun.*, vol. 9, no. 1, pp. 1–6, Jan. 2018.

[216] Y. Wang *et al.*, "Efficient quantum memory for single-photon polarization qubits," *Nat. Photon.*, vol. 13, no. 5, pp. 346–351, Mar. 2019.

[217] T. Rao and K.-H. Nam, "Private-key algebraic-coded cryptosystems," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Dec. 1986, pp. 35–48.

[218] T. Okamoto, K. Tanaka, and S. Uchiyama, "Quantum public-key cryptosystems," in *Proc. Annu. Int. Cryptol. Conf.*, Aug. 2000, pp. 147–165.

[219] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[220] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[221] A. W. Dent, "Hybrid cryptography," IACR, Lyon, France, Rep. 2004/210, Jun. 2004.

[222] G. Zeng and G. Guo, "Quantum authentication protocol," Jan. 2000. [Online]. Available: arXiv:quant-ph/0001046.

[223] H. N. Barnum, "Quantum secure identification using entanglement and catalysis," May 1999. [Online]. Available: arXiv:quant-ph/9910072.

[224] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, "Quantum identification system," *Phys. Rev. A*, vol. 60, no. 1, pp. 149–156, Jul. 1999.

[225] C. H. Bennett and G. Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working!" *ACM SIGACT News*, vol. 20, no. 4, pp. 78–80, 1989.

[226] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "KaaS: Key as a service over quantum key distribution integrated optical networks," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 152–159, May 2019.

[227] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Multi-tenant provisioning for quantum key distribution networks with heuristics and reinforcement learning: A comparative study," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 2, pp. 946–957, Jun. 2020.

[228] J. G. Rarity, P. Tapster, P. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.*, vol. 4, no. 1, p. 82, Jan. 2002.

[229] C.-Z. Peng *et al.*, "Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication," *Phys. Rev. Lett.*, vol. 94, no. 15, Apr. 2005, Art. no. 150501.

[230] J.-Y. Wang *et al.*, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nat. Photon.*, vol. 7, no. 5, pp. 387–393, Apr. 2013.

[231] S. Nauerth *et al.*, "Air-to-ground quantum communication," *Nat. Photon.*, vol. 7, no. 5, pp. 382–386, Mar. 2013.

[232] S.-K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, Jan. 2018, Art. no. 030501.

[233] Y.-A. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, Jan. 2021.

[234] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[235] S. M. Bellovin, "Frank Miller: Inventor of the one-time pad," *Cryptologia*, vol. 35, no. 3, pp. 203–222, Jul. 2011.

[236] D. W. Leung, "Quantum Vernam cipher," *Quantum Inf. Comput.*, vol. 2, no. 1, pp. 14–34, Dec. 2002.

[237] H. Murray, J. Horgan, J. F. Santos, D. Malone, and H. Siljak, "Implementing a quantum coin scheme," in *Proc. 31st Irish Signals Syst. Conf. (ISSC)*, Aug. 2020, pp. 1–7.

[238] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[239] J. Yin *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, Jun. 2020.

[240] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, "Observation of three-photon greenberger-horne-zeilinger entanglement," *Phys. Rev. Lett.*, vol. 82, no. 7, p. 1345, Feb. 1999.

[241] T. Beth, J. Müller-Quade, and R. Steinwandt, "Cryptanalysis of a practical quantum key distribution with polarization-entangled photons," *Quantum Inf. Comput.*, vol. 5, no. 3, pp. 181–186, May 2005.

[242] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Phys. Rev. Lett.*, vol. 77, no. 13, p. 2818, Sep. 1996.

[243] A. Aspect, "Bell's inequality test: More ideal than ever," *Nature*, vol. 398, no. 6724, pp. 189–190, Mar. 1999.

[244] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Workshop Theory Appl. Cryptogr. Techn.*, Jul. 1993, pp. 410–423.

[245] S. J. Lomonaco, "A quick glance at quantum cryptography," *Cryptologia*, vol. 23, no. 1, pp. 1–41, Jun. 1999.

[246] M. Mehic, M. Niemiec, H. Siljak, and M. Voznak, "Error reconciliation in quantum key distribution protocols," in *Reversible Computation: Extending Horizons of Computing: Selected Results of the COST Action IC1405*. Cham, Switzerland: Springer Nature, 2020, pp. 222–236.

[247] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[248] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, no. 2, pp. 210–229, Apr. 1988.

[249] A. I. Nurhadi and N. R. Syambas, "Quantum key distribution (QKD) protocols: A survey," in *Proc. 4th Int. Conf. Wireless Telemat. (ICWT)*, Nov. 2018, pp. 1–5.

[250] X. Li and H. Barnum, "Quantum authentication using entangled states," *Int. J. Found. Comput. Sci.*, vol. 15, no. 4, pp. 609–617, 2004.

[251] J. G. Jensen and R. Schack, "Quantum authentication and key distribution using catalysis," Jun. 2000. [Online]. Available: arXiv:quant-ph/0003104

[252] D. Ljunggren, M. Bourennane, and A. Karlsson, "Authority-based user authentication in quantum key distribution," *Phys. Rev. A*, vol. 62, no. 2, Jul. 2000, Art. no. 022305.

[253] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, nos. 6–7, pp. 467–488, 1982.

[254] P. Benioff, "Quantum mechanical models of turing machines that dissipate no energy," *Phys. Rev. Lett.*, vol. 48, no. 23, p. 1581, 1982.

[255] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proc. Royal Soc. London A, Math. Phys. Sci.*, vol. 400, no. 1818, pp. 97–117, 1985.

[256] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proc. Royal Soc. London A, Math. Phys. Sci.*, vol. 439, no. 1907, pp. 553–558, 1992.

[257] S. Lloyd, "A potentially realizable quantum computer," *Science*, vol. 261, no. 5128, pp. 1569–1571, 1993.

[258] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999.

[259] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," in *Proc. 3rd ACM Conf. Comput. Commun. Security*, 1996, pp. 31–37.

[260] T. Wang, Z. Zheng, M. H. Rehmani, S. Yao, and Z. Huo, "Privacy preservation in big data from the communication perspective—A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 753–778, 1st Quart., 2019.

[261] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[262] H. Sedlak, "The RSA cryptography processor," in *Proc. Workshop Theory Appl. Cryptogr. Techn.*, Dec. 1987, pp. 95–105.

[263] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, p. 1829, Mar. 1999.

[264] G.-L. Long and X.-S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A*, vol. 65, no. 3, Feb. 2002, Art. no. 032302.

[265] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, p. 2881, Nov. 1992.

[266] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photon.*, vol. 9, no. 3, pp. 163–168, Feb. 2015.

[267] J.-P. Chen *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, no. 7, Feb. 2020, Art. no. 070501.

[268] X.-T. Fang *et al.*, "Surpassing the rate-transmittance linear bound of quantum key distribution," Aug. 2019. [Online]. Available: arXiv:1908.01271.

[269] G.-L. Long, F.-G. Deng, C. Wang, X.-H. Li, K. Wen, and W.-Y. Wang, "Quantum secure direct communication and deterministic secure quantum communication," *Front. Phys. China*, vol. 2, no. 3, pp. 251–272, 2007.

[270] Z.-C. Zhu, A.-Q. Hu, and A.-M. Fu, "Cryptanalysis and improvement of the controlled quantum secure direct communication by using four particle cluster states," *Int. J. Theor. Phys.*, vol. 53, no. 5, pp. 1495–1501, Dec. 2014.

[271] C. S. Yoon, M. S. Kang, J. I. Lim, and H. J. Yang, "Quantum signature scheme based on a quantum search algorithm," *Physica Scripta*, vol. 90, no. 1, Dec. 2014, Art. no. 015103.

[272] G. Gao, "Two quantum dialogue protocols without information leakage," *Opt. Commun.*, vol. 283, no. 10, pp. 2288–2293, 2010.

[273] C. Zheng and G. Long, "Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs," *Sci. China Phys. Mech. Astron.*, vol. 57, no. 7, pp. 1238–1243, Jul. 2014.

[274] Z.-J. Zhang, "Multiparty quantum secret sharing of secure direct communication," *Phys. Lett. A*, vol. 342, nos. 1–2, pp. 60–66, Jul. 2005.

[275] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Phys. Rev. A*, vol. 71, no. 4, Apr. 2005, Art. no. 044305.

[276] S. Jin, G. Yan-Xiao, X. Ping, Z. Shi-Ning, and Z. You-Bang, "Quantum secure direct communication by using three-dimensional hyperentanglement," *Commun. Theor. Phys.*, vol. 56, no. 5, p. 831, Nov. 2011.

[277] A. Meslouhi and Y. Hassouni, "A quantum secure direct communication protocol using entangled modified spin coherent states," *Quantum Inf. Process.*, vol. 12, no. 7, pp. 2603–2621, Mar. 2013.

[278] C. Wang, F. G. Deng, and G. L. Long, "Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state," *Opt. Commun.*, vol. 253, nos. 1–3, pp. 15–20, Sep. 2005.

[279] Z.-W. Sun, R.-G. Du, and D.-Y. Long, "Quantum secure direct communication with two-photon four-qubit cluster states," *Int. J. Theor. Phys.*, vol. 51, no. 6, pp. 1946–1952, Jan. 2012.

[280] W. Tie-Jun, L. Tao, D. Fang-Fang, and D. Fu-Guo, "High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement," *Chin. Phys. Lett.*, vol. 28, no. 4, Feb. 2011, Art. no. 040305.

[281] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[282] M. Suárez-Albela, P. Fraga-Lamas, T. M. Fernández-Caramés, A. Dapena, and M. González-López, "Home automation system based on intelligent transducer enablers," *Sensors*, vol. 16, no. 10, p. 1595, Sep. 2016.

[283] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas, and C. J. Escudero, "A plug-and-play human-centered virtual TEDS architecture for the Web of things," *Sensors*, vol. 18, no. 7, p. 2052, Jun. 2018.

[284] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemp. Phys.*, vol. 57, no. 3, pp. 366–387, Mar. 2016.

[285] C. F. Kerry and P. D. Gallagher, *Digital Signature Standard (DSS)*, FIPS Standard 186-4, Jul. 2013.

[286] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219.

[287] M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channels and the cost of randomizing quantum information," Mar. 2000. [Online]. Available: arXiv:quant-ph/0003101.

[288] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: A Survey on quantum-resistant cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020.

[289] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, "A review on Internet of Things for defense and public safety," *Sensors*, vol. 16, no. 10, p. 1644, Oct. 2016.

[290] P. Fraga-Lamas, T. M. Fernández-Caramés, and L. Castedo, "Towards the Internet of Smart Trains: A review on Industrial IoT-connected railways," *Sensors*, vol. 17, no. 6, p. 1457, Jun. 2017.

[291] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[292] P. Arrighi and L. Salvail, "Blind quantum computation," *Int. J. Quantum Inf.*, vol. 4, no. 5, pp. 883–898, 2006.

[293] T. Morimae and K. Fujii, "Blind quantum computation protocol in which alice only makes measurements," *Phys. Rev. A*, vol. 87, no. 5, May 2013, Art. no. 050301.

[294] M. Abadi, J. Feigenbaum, and J. Kilian, "On hiding information from an oracle," *J. Comput. Syst. Sci.*, vol. 39, no. 1, pp. 21–50, Aug. 1989.

[295] D.-Q. Cai *et al.*, "Implementation of an E-payment security evaluation system based on quantum blind computing," *Int. J. Theor. Phys.*, vol. 59, pp. 2757–2772, Jul. 2020.

[296] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*. Boston, MA, USA: Springer, 1983, pp. 199–203.

[297] A. M. Childs, "Secure assisted quantum computation," Jul. 2001. [Online]. Available: arXiv:quant-ph/0111046.

[298] A. C.-C. Yao, "Interactive proofs for quantum computations," in *Proc. Int. Symp. Algorithms Comput.*, Apr. 2003, p. 1.

[299] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Phys. Rev. Lett.*, vol. 86, no. 22, p. 5188, May 2001.

[300] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal Blind Quantum Computation," in *Proc. 50th Annu. IEEE Symp. Found. Comput. Sci.*, 2009, pp. 517–526.

[301] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of blind quantum computing," *Science*, vol. 335, no. 6066, pp. 303–308, 2012.

[302] J. C. Corbett *et al.*, "Spanner: Google's globally distributed database," *ACM Trans. Comput. Syst.*, vol. 31, no. 3, pp. 1–22, Aug. 2013.

[303] S. Duan, S. Cong, and Y. Song, "A survey on quantum positioning system," *Int. J. Model. Simulat.*, vol. 41, no. 4, pp. 265–283, Mar. 2020.

[304] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satellite Div. Inst. Navigation (ION GNSS)*, Sep. 2008, pp. 2314–2325.

[305] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security J.*, vol. 25, no. 2, pp. 19–27, 2003.

[306] B. Bloom *et al.*, "An optical lattice clock with accuracy and stability at the 10^{-18} level," *Nature*, vol. 506, no. 7486, pp. 71–75, 2014.

[307] N. Hinkley *et al.*, "An atomic clock with 10^{-18} instability," *Science*, vol. 341, no. 6151, pp. 1215–1218, 2013.

[308] T. Nicholson *et al.*, "Comparison of two independent Sr optical clocks with 1×10^{-17} stability at 10^3s," *Phys. Rev. Lett.*, vol. 109, no. 23, Dec. 2012, Art. no. 230801.

[309] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network," *Phys. Rev. Lett.*, vol. 78, no. 16, p. 3221, Apr. 1997.

[310] S. Perseguers, G. Lapeyre, Jr., D. Cavalcanti, M. Lewenstein, and A. Acín, "Distribution of entanglement in large-scale quantum networks," *Rep. Progr. Phys.*, vol. 76, no. 9, Sep. 2013, Art. no. 096001.

[311] I. L. Chuang, "Quantum algorithm for distributed clock synchronization," *Phys. Rev. Lett.*, vol. 85, no. 9, p. 2006, Aug. 2000.

[312] J. D. Monnier, "Optical interferometry in astronomy," *Rep. Progr. Phys.*, vol. 66, no. 5, p. 789, Apr. 2003.

[313] P. Lawson, *Principles of Long Baseline Stellar Interferometry*, Jet Propulsion Lab., Pasadena, CA, USA, 2000.

[314] F. Zernike, "The concept of degree of coherence and its application to optical problems," *Physica*, vol. 5, no. 8, pp. 785–795, Aug. 1938.

[315] G. Vallone *et al.*, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, no. 4, Jul. 2015, Art. no. 040502.

[316] D. A. Lidar and T. A. Brun, *Quantum Error Correction*. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[317] R. Van Meter and S. J. Devitt, "The path to scalable distributed quantum computing," *Computer*, vol. 49, no. 9, pp. 31–42, Sep. 2016.

[318] P. T. Fisk, "Trapped-ion and trapped-atom microwave frequency standards," *Rep. Progr. Phys.*, vol. 60, no. 8, p. 761, Aug. 1997.

[319] D. Chandra *et al.*, "Quantum topological error correction codes: The Classical-to-quantum isomorphism perspective," *IEEE Access*, vol. 6, pp. 13729–13757, 2017.

[320] P. Kurpiers *et al.*, "Deterministic quantum state transfer and remote entanglement using microwave photons," *Nature*, vol. 558, no. 7709, pp. 264–267, 2018.

[321] J. Williamson, "Brownian motion of electrons," *J. Phys. A, Gen. Phys.*, vol. 1, no. 6, p. 629, Nov. 1968.

[322] R. Van Meter and J. Touch, "Designing quantum repeater networks," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 64–71, Aug. 2013.

[323] V. G. Cerf and R. E. Icahn, "A protocol for packet network intercommunication," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 2, pp. 71–82, May 2005.

[324] G. Fürnkranz, *The Quantum Internet: Ultrafast and Safe from Hackers*. Cham, Switzerland: Springer Nature, 2020.

[325] D. Collins, N. Gisin, and H. De Riedmatten, "Quantum relays for long distance quantum cryptography," *J. Modern Opt.*, vol. 52, no. 5, pp. 735–753, Feb. 2005.

[326] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Phys. Rev. A*, vol. 59, no. 1, p. 169, Jan. 1999.

[327] R. Alléaume *et al.*, "Using quantum key distribution for cryptographic purposes: A survey," *Theor. Comput. Sci.*, vol. 560, pp. 62–81, Dec. 2014.

[328] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks," *J. Comput. Security*, vol. 18, no. 1, pp. 61–87, 2010.

[329] S. K. Joshi *et al.*, "A trusted node-free eight-user metropolitan quantum communication network," *Sci. Adv.*, vol. 6, no. 36, Sep. 2020, Art. no. eaba0959.

[330] X. Liu *et al.*, "An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution," *APL Photon.*, vol. 5, no. 7, Jun. 2020, Art. no. 076104.

[331] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[332] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, no. 1, Mar. 2016, Art. no. 011024.

[333] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, "Measurement-device-independent quantum key distribution over asymmetric channel and unstable channel," *Sci. Rep.*, vol. 8, no. 1, pp. 1–7, Dec. 2018.

[334] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, "Quantum network coding," in *Proc. Annu. Symp. Theor. Aspects Comput. Sci.*, 2007, pp. 610–621.

[335] D. A. Lidar, I. L. Chuang, and K. B. Whaley, "Decoherence-free subspaces for quantum computation," *Phys. Rev. Lett.*, vol. 81, no. 12, p. 2594, Sep. 1998.

[336] D. Suter and G. A. Álvarez, "Colloquium: Protecting quantum information against environmental noise," *Rev. Modern Phys.*, vol. 88, no. 4, Oct. 2016, Art. no. 041001.

[337] C. P. Koch, "Controlling open quantum systems: Tools, achievements, and limitations," *J. Phys. Condens. Mat.*, vol. 28, no. 21, May 2016, Art. no. 213001.

[338] L. Viola, E. Knill, and S. Lloyd, "Dynamical decoupling of open quantum systems," *Phys. Rev. Lett.*, vol. 82, no. 12, p. 2417, Mar. 1999.

[339] L. Viola and S. Lloyd, "Dynamical suppression of decoherence in two-state quantum systems," *Phys. Rev. A*, vol. 58, no. 4, p. 2733, 1998.

[340] S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," *Rev. Modern Phys.*, vol. 77, no. 2, p. 513, Jun. 2005.

[341] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, no. 1, Dec. 1999, Art. no. 010303.

[342] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," Apr. 2002. [Online]. Available: arXiv:quant-ph/0204127.

[343] C. Croal *et al.*, "Free-space quantum signatures using heterodyne measurements," *Phys. Rev. Lett.*, vol. 117, no. 10, Sep. 2016, Art. no. 100503.

[344] V. Havlíček *et al.*, "Supervised learning with quantum-enhanced feature spaces," *Nature*, vol. 567, no. 7747, pp. 209–212, 2019.

[345] A. Peruzzo *et al.*, "A variational eigenvalue solver on a photonic quantum processor," *Nat. Commun.*, vol. 5, p. 4213, Jul. 2014.

Amoldeep Singh received the M.E. degree in electronics (VLSI design) from Punjab Engineering College, Chandigarh, India. He is a Research Scholar with the Electronics and Communication Department, Thapar Institute of Engineering and Technology, Patiala, India. He is an exchange student with Politecnico di Milano, Milan, Italy, and is associated with Erasmus KA-107 project. His research interests includes quantum communication, quantum networking, VLSI interconnects, and optical interconnects.

Kapal Dev (Member, IEEE) received the B.E. and M.E. degrees in Electronics and the Ph.D. degree in Telecommunication Engineering from Politecnico di Milano, Italy, and the Postdoctoral degree in Fusion of 5G and Blockchain.

He is currently working as a Senior Research Associate with the Institute of Intelligent Systems, University of Johannesburg, South Africa. He is a Senior Researcher with Munster Technological University, Ireland. He was a Postdoctoral Research Fellow with the CONNECT Centre, School of Computer Science and Statistics, Trinity College Dublin. He worked as a 5G Junior Consultant and an Engineer with Altran Italia S.p.A, Milan, Italy, on 5G use cases. He worked as a Lecturer with Indus University, Karachi, in 2014. He is also working for OCEANS Network as the Head of Projects to manage OCEANS project processes and functions to improve efficiency, consistency, and best practice integration. He is very active in leading (as Principle Investigator) Erasmus + International Credit Mobility (ICM) and Capacity Building for Higher Education and H2020 Co-Fund projects. Received a few Million Euros funding and few are in review as well as in the writing phase. His research interests include blockchain, 6G networks, and artificial intelligence.

Dr. Dev was awarded the Ph.D. degree by Politecnico di Milano, under the prestigious fellowship of Erasmus Mundus funded by European Commission. He is a Evaluator of MSCA co-fund schemes, Elsevier book proposals and top scientific journals and conferences, including IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE INTERNET OF THINGS, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, *Future Generation Computer Systems*, *Computer Networks* (COMNET), TETT, IEEE VTC, and WF-IoT. He is also serving as the Guest Editor in *Computer Communications* (I.F: 2.8), COMNET (I.F 3.11), the Lead Chair in one of CCNC 2021 workshops, and editing a book for CRC Press. He is also serving as an Associate Editor in *Wireless Networks*, *IET Quantum Communication*, *IET Networks*, and a Review Editor in *Frontiers in Communications and Networks*. He is the TPC Member of IEEE BCA 2020 in conjunction with AICCSA 2020, ICBC 2021, DICG co-located with Middleware 2020 and FTNCT 2020. He is a member of the ACM and actively involved with various working groups and committees of IEEE and ACM related to 5G and beyond, blockchain and artificial intelligence.

Harun Siljak (Senior Member, IEEE) received the bachelor's and master's degrees in automatic control and electronics from the University of Sarajevo in 2010 and 2012, respectively, and the Ph.D. degree in electrical and electronics engineering from the International Burch University, Sarajevo, in 2015. He is an Assistant Professor with the School of Engineering, Trinity College Dublin. During his earlier Marie Curie fellowship at TCD, he merged complex systems science and reversible computation in a new toolbox for wireless communications, mainly for control and optimisation of large antenna arrays. The tools developed during the project found their application in quantum computation and communications, as well as molecular and neuronal communications. He serves as an Associate Editor for the *EURASIP Journal on Wireless Communications and Networking*, and the Science Communication Officer for the Western Balkans Chapter of Marie Curie Alumni Association and MAT-DYN-NET COST Action.

Hem Dutt Joshi (Member, IEEE) received the B.Tech. degree in ECE from Barkatullah University, Bhopal, India, in 1999, the M.E. degree in CCN from MITS, Gwalior, in 2004, and the Ph.D. degree from JUET, Guna, India, in 2012, where he worked as an Assistant Professor from 2006 to 2013. He is currently working as an Associate Professor with the Department of ECE, TIET, Patiala. He also worked as a Visiting Research Fellow with CONNECT, Science Foundation Ireland Research Centre for Future Networks, Trinity College Dublin, Ireland, in 2019. He is involved very extensively in research regarding high data rate wireless communication systems and signal processing. He has more than 15 years of teaching and research experience. His research interests include wireless communication, OFDM system, MIMO–OFDM, signal processing for wireless communication, and 5G communication system.

Maurizio Magarini (Member, IEEE) received the M.Sc. and Ph.D. degrees in electronic engineering from the Politecnico di Milano, Milan, Italy, in 1994 and 1999, respectively. He worked as a Research Associate with the Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, from 1999 to 2001. From 2001 to 2018, he was an Assistant Professor with Politecnico di Milano, where he has been an Associate Professor since June 2018. From August 2008 to January 2009, he spent a sabbatical leave with Bell Labs, Alcatel–Lucent, Holmdel, NJ, USA. He has been involved in several European and National research projects. He has authored and coauthored more than 100 journal and conference papers. His research interests are in the broad area of communication and information theory. Topics include synchronization, channel estimation, equalization, and coding applied to wireless and optical communication systems. His most recent research activities have focused on molecular communications, massive MIMO, study of waveforms for 5G cellular systems, wireless sensor networks for mission critical applications, and wireless networks using UAVs, and high-altitude platforms. In 1994, he was granted the TELECOM Italia (currently, TIM) Scholarship Award for his M.Sc. Thesis. He was a co-recipient of four best paper awards. He is an Associate Editor for IEEE ACCESS and *IET Electronics Letters* and a Member of the Editorial Board of *Nano Communication Networks* (Elsevier) and *Telecom* (MDPI).