An Overview of Quantum Teleportation

Travis S. Humble

Abstract

Quantum teleportation is a communication protocol for the exchange of information between remotely separated parties. We survey some prominent applications of quantum teleportation that show potential for collecting and analyzing information. In addition to a background review of the underlying principles, we highlight the use of quantum teleportation in quantum key distribution, long-distance quantum communication networks, and quantum computing. The latter applications are significant as they show promise for cracking conventional public-key encryption systems and providing alternate key distribution systems that are secure against attack.

Introduction

Quantum information science (QIS) formulates a theory of information using the principals of quantum physics, an effort driven by the insight that physical systems encoding information are ultimately governed by the laws of quantum mechanics. But more importantly, adopting a quantum paradigm (instead of a classical one) provides unique opportunities in communication, cryptography, and computation [1]. Examples illustrating the uniqueness of QIS include: theoretically secure quantum key distribution schemes for encrypting classical information [2, 3], the creation of quantum communication channels for nonlocal sharing of secret quantum information [3], and the ability of a quantum computer to more efficiently execute algorithms, e.g., for factoring large numbers [5] and querying unsorted databases [6].

These emerging quantum capabilities are of specific interest. For example, the advent of a quantum computer would enable a dramatic speed up in factorizing large numbers. However, many public-key (asymmetric) encryption systems, e.g., RSA, rely on factorization as a computationally intractable problem to guarantee the security of the key. Consequently, a quantum computer poises a risk to the encryption and information security of many communication networks. An equally important example is quantum key distribution (QKD), which is a quantum-based protocol for securely distributing a one-time pad of random numbers between two parties. While QKD provides a secure alternative for publicly encrypting messages, it is also a means available to any technologically sophisticated adversary. These two considerations alone have made QIS an active interest.

The above breakthroughs are expected to revolutionize the ways information is collected and analyzed in the future. In this article, we survey some of the novel opportunities afforded by QIS with an emphasis on applications of the quantum teleportation protocol [2]. In its bare form, quantum teleportation is a method for communicating quantum information, i.e., information encoded into the quantum-mechanical state of a physical system. When a quantum bit, or qubit, of information is teleported between two locations, it does not pass through the intervening space. Instead, quantum teleportation uses two communication channels to transfer information. Remarkably, neither communication channel can individually identify the transmitted information. One of these channels is a classical communication channel that connects the sender with a remotely located recipient. The other channel is a quantum communication channel that is established between the sender and recipient when they share a pair of entangled particles. As described in more detail below, entangled particles are uniquely characterized by their ability to demonstrate perfect correlations between their individual properties.

In the quantum teleportation protocol, the sender make a measurement on her particle and then conveys to the recipient the minimal amount of classical information that characterizes the measurement outcome. With the classical information in hand, the recipient performs a correcting operation to account for quantum-mechanical uncertainty and, subsequently, recovers the teleported information. Perhaps the most intriguing aspect of quantum teleportation comes from the observation that at not time during the protocol does the teleported information exist in the space between the two parties. The classical information that is transferred is cannot by itself identify the teleportation information. Similarly, in absence of the classical measurement information, the recipients particle appears to exist in a statistically random state.

The ability to teleport information (a feat realized experimentally [7]) underlies a variety of applications in quantum communication and quantum computation. Our survey highlights the most prominent of these applications and some of the supporting quantum technologies. However, our account is not exhaustive; the relatively young field of QIS is undergoing a period of rapid expansion. In addition, we omit most references to the pragmatic issue of how these quantum information protocols may be best implemented, especially in regards to potential physical systems. Though the latter issue is perhaps the most daunting challenge facing applications of QIS at the moment, our goal is to highlight the opportunities that others are diligently working to realize.

Quantum Teleportation

The novelty of quantum teleportation arises from the properties of entangled particles. Entanglement is a feature of quantum mechanics whereby two or more quantum systems show correlations in their measured properties, even though the individual systems appear to behave randomly. Mathematically, entanglement implies that the joint state of a two-particle system is not factorizable. Using bra-ket notation, an example of entanglement is given by the two-particle state

$$\left|\varphi_{12}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_1\right\rangle\left|\downarrow_2\right\rangle + \left|\downarrow_1\right\rangle\left|\uparrow_2\right\rangle\right), \tag{1}$$

where subscripts 1 and 2 label the particles and the orthonormal ket vectors, $\left|\uparrow\right\rangle$ and $\left|\downarrow\right\rangle$, span the two-dimensional Hilbert space of each subsystem. For example, the arrows could label the “up” and “down” spins of an electron or the horizontal and vertical polarizations of a photon. In either case, correlations inherent to the entangled state are readily observed by noting that when system 1 is measured in the up $(\uparrow)$ state, system 2 will always be in the down $(\downarrow)$ state and vice versa. Quantum mechanics does not allow us to predetermine which of these two results will be observed, but we are assured that the measured results of the individual systems will always be perfectly correlated. What makes entanglement a powerful resource for information processing is that these correlations are guaranteed even when the two systems are remote from one another. In contrast, an unentangled state cannot show nonlocal correlations.

In its simplest form, quantum teleportation considers two parties, conventionally named Alice and Bob, to share a pair of particles in the entangled state (1). Alice wishes to teleport a qubit of information to Bob that is encoded in the state of a third particle as

$$\left|\psi_3\right\rangle = a\left|\uparrow_3\right\rangle + b\left|\downarrow_3\right\rangle. \tag{2}$$

e.g., if the particle is a photon, the polarization vector could be *a*(horizontal) + *b*(vertical). The complex coefficients *a* and *b* satisfy normalization $|a|^2 + |b|^2 = 1$ and are presumed to be unknown to Alice. For Alice to convey a complete description of the state (2) would generally require an infinite number of classical bits to specify the (arbitrary) complex-valued coefficients *a* and *b*. Of course, in Alice's efforts to discover this information, she would necessarily destroy the state of the particle. But, by using quantum teleportation, Alice can completely transfer the qubit to Bob at a significantly reduced communication cost (2 bits).

To demonstrate, we rewrite the composite three-particle state $\left|\Psi_{123}\right\rangle = \left|\varphi_{12}\right\rangle\left|\psi_3\right\rangle$ using the following set of orthogonal (Bell) states [8]

$$\left|\varphi_{23}^{(\pm)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_2\right\rangle\left|\downarrow_3\right\rangle \pm \left|\downarrow_2\right\rangle\left|\uparrow_3\right\rangle\right) \tag{3}$$

$$\left|\psi_{23}^{(\pm)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_2\right\rangle\left|\uparrow_3\right\rangle \pm \left|\downarrow_2\right\rangle\left|\downarrow_3\right\rangle\right).$$

These four states, widely used by Bell, form a complete basis set for the two-particle Hilbert space of particles 2 and 3. In addition, the Bell states are maximally entangled, in that they maximize the entropy of the individual particles while minimizing the entropy of the pair. Using the Bell basis, we express the three-particle state as

$$\left|\Psi_{123}\right\rangle = \frac{1}{2}\Big[\left(a\left|\uparrow_1\right\rangle - b\left|\downarrow_1\right\rangle\right)\left|\varphi_{23}^{(+)}\right\rangle + \left(a\left|\uparrow_1\right\rangle + b\left|\downarrow_1\right\rangle\right)\left|\varphi_{23}^{(-)}\right\rangle \tag{4}$$

$$+\left(b\left|\uparrow_1\right\rangle - a\left|\downarrow_1\right\rangle\right)\left|\psi_{23}^{(+)}\right\rangle + \left(b\left|\uparrow_1\right\rangle + a\left|\downarrow_1\right\rangle\right)\left|\psi_{23}^{(-)}\right\rangle\Big].$$

According to Eq. (4), if Alice projects (measures) particles 2 and 3 into any one of the Bell states, then the subsequent state of particle 1 is unitarily related to the original qubit, *regardless of where the first particle may be located.* It is this nonlocal aspect of information transfer that led the original authors to term this protocol quantum teleportation [3].

For example, a projection into the state $\left|\varphi_{23}^{(-)}\right\rangle$, denoted by $\left\langle\varphi_{23}^{(-)}\middle|\Psi_{123}\right\rangle$, yields the normalized state of particle 1 as $\left|\psi_1\right\rangle = a\left|\uparrow_1\right\rangle - b\left|\downarrow_1\right\rangle$. The original qubit is then recovered when Bob applies to particle 1 the local unitary transformation

$$U_a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{5}$$

Recovery of the original qubit following projections into the remaining three Bell states, $\left|\varphi_{12}^{(+)}\right\rangle$, $\left|\psi_{12}^{(+)}\right\rangle$, and $\left|\psi_{12}^{(-)}\right\rangle$, respectively requires the unitary operators

$$U_b = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U_c = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad U_d = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{6}$$

In the case of polarization-encoded qubits, all of these unitary transformation can be carried out using polarization rotators and quarter waveplates.

The four possible measurement outcomes (labeled *a*, *b*, *c*, and *d*) are equally probable, and the result of Alice's Bell-state measurement must be relayed to Bob in order for him to recover the unknown qubit; if Bob does not apply the correct local transformation, he cannot infer any information about the teleported qubit [3]. This step necessitates 2 bits of classical information to be transferred across the classical channel. Unsurprisingly, since the protocol requires the use of a classical channel, quantum teleportation cannot be used for faster-than-light signaling. Figure 1 is a schematic of the described protocol.

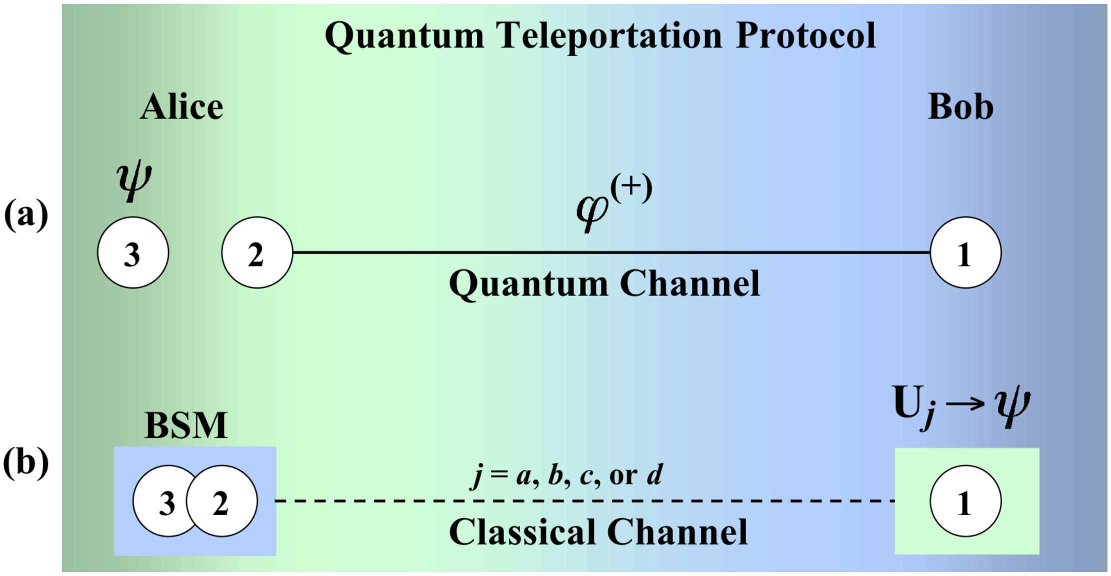

Figure 1. A schematic demonstration of the quantum teleportation protocol, where the circles represent particles, the solid line represents the quantum communication channel (entanglement), and the dashed line represents the classical communication channel. (a) Initially, Alice and Bob share some entanglement via particles 1 and 2. Alice has a third particle in which a quantum state ψ is encoded. (b) Alice subjects particles 2 and 3 to a Bell-state measurement (BSM), which generates two bit of classical information j, that distinguish between the four possible measurement outcomes. Alice communicates this information to Bob using a classical channel, whereupon Bob uses his knowledge of j to apply the appropriate unitary operator U_j and ensure his particle now encodes the state ψ.

In addition to the classical communication cost, Alice and Bob also incur a cost in using a pair of entangled particles to execute the teleportation protocol. The latter cost has been quantified by Bennett *et al.* as 1 ebit, where an ebit is the amount of entanglement between a pair of maximally entangled particles [9]. Moreover, the aggregate cost of 2 classical bits and 1 ebit has been shown to be the minimal number of each resource type necessary for teleporting a qubit. Finally, we note that Alice must destructively measure the state of particles 2 and 3, and that she does not retain a copy of the unknown qubit for herself. This outcome is consistent with another well-known feature of quantum mechanics, the fact that quantum information cannot be copied [10].

One notable aspect of quantum teleportation is that the qubit of information is never accessible except by Alice and Bob. Following Alice's Bell-state measurement, particles 2 and 3 are destroyed and Alice retains no information about the qubit. Before receiving the appropriate message from Alice, particle 1 is related to the original qubit in a random way that provides Bob with no useful information. During this intervening period, which is necessarily as long as it takes for Alice to communicate the measurement outcome to Bob, the qubit of information is not accessible to anyone. It is only by combining the information transferred across both the quantum and classical communication channels that a qubit is successfully teleported. This interpretation has led to teleportation being called the "quantum one-time pad," a reference to the theoretically secure means of classically encrypting a message [11].

Remote State Preparation

In the foregoing discussion, teleportation of a qubit was shown to require 2 classical bits and 1 ebit. When the qubit is unknown to both parties, these resources have been shown as both sufficient and necessary for teleportation. However, it is possible that Alice has foreknowledge of the qubit she wishes to teleport, in which case the classical communication cost can be reduced to 1 classical bit. This economical variant of the teleportation protocol has been termed remote state preparation [12].

The simplest example of remote state preparation is when Alice wishes to teleport a state of the form

$$\left|\psi_j\right\rangle = \left(\left|\uparrow_j\right\rangle + e^{i\delta}\left|\downarrow_j\right\rangle\right)\big/\sqrt{2}\,, \qquad (7)$$

where δ is a real-valued phase. We denote by $\left|\overline{\psi}_j\right\rangle$ the state that is orthogonal to Eq. (7), i.e.,

$$\left|\overline{\psi}_j\right\rangle = \left(\left|\uparrow_j\right\rangle - e^{i\delta}\left|\downarrow_j\right\rangle\right)\big/\sqrt{2}\,. \qquad (8)$$

Alice and Bob share a pair of entangled particles whose state is given by $\left|\varphi_{12}^{(-)}\right\rangle$, cf. Eq. (3). Alice projects her member of the pair (particle 2) into the state $\left|\overline{\psi}_2\right\rangle$, in which case particle 1 is left in the intended state, i.e.,

$$\left\langle\overline{\psi}_2\middle|\varphi_{12}^{(-)}\right\rangle = \frac{e^{i(\pi-\delta)}}{\sqrt{2}}\left|\psi_1\right\rangle. \tag{9}$$

Yet, a successful projection occurs only 1/2 of the time; the remaining measurements are projections into the orthogonal outcome, i.e., $\left\langle\psi_2\middle|\varphi_{12}^{(-)}\right\rangle = e^{-i\delta}\left|\overline{\psi}_1\right\rangle\big/\sqrt{2}$. It is possible for Bob to correct for this "failure" when the state is known to be of the form (7), provided Alice notifies him that a failure has occurred. As Alice needs to communicate to Bob only which of two possible outcomes she recorded, the subsequent communication cost is 1 classical bit plus 1 ebit [12].

Remotely preparing qubits of a more general form, e.g., as given by Eq. (2), is also possible, though probabilistic in practice. That is to say, the protocol succeeds when the orthogonal complement to ψ is projected onto the entangled pair, resulting in the state $\left|\psi_1\right\rangle$, but fails otherwise. In the case of failure, Bob is generally unable to recover the intended state because the necessary inversion operation cannot be implemented by any physical means (see Ref. [12] for elaboration on this point). Thus, this scheme, which is probabilistic but exact, requires Alice to make more than one attempt at remote state preparation. In addition, Alice and Bob will need a bookkeeping scheme to identify those outcomes that are deemed successful. Remarkably, Bennett et al. have shown that it is possible to recover the minimal cost of 1 classical bit and 1 ebit per qubit, provided one takes the asymptotic limit, i.e., in the limit that many states are remotely prepared, [12].

Entanglement Distribution and Quantum Repeaters

An essential component of the quantum teleportation protocol is that Alice and Bob share a pair of entangled particles. But the distribution of entangled particles over long distances is currently very challenging experimentally. Part of the challenge is that the physical system encoding a qubit is always embedded in a surrounding environment. Interactions between the system of interest and the environment act as sources of noise that can destroy the encoded information. The influences of noise may manifest as bit errors or phase errors in the state of particle, or through the complete destruction of the particle altogether.

For example, when photons are used to encode quantum information, e.g., using the polarization state, subsequent transmission through a fiber optic cable makes the photons susceptible to depolarizing effects (bit and phase errors) and absorption (destruction). The probability for these errors to occur scales exponentially with the length of the fiber and places a significant limit on the distances over which polarization-entangled photons can be reliably transmitted [13]. Quantum information encoded into other physical systems (notably atomic and molecular structures) is similarly hampered by forms of decoherence induced by the surrounding environment.

A means of circumventing these forms of noise, while achieving entanglement distribution, is to use a variation of the quantum teleportation protocol called entanglement swapping [2, 14]. In this scenario, particle 3 (the original message qubit) is initially entangled with a fourth particle. The composite state of the four-particle system $\left|\Psi_{1234}\right\rangle = \left|\varphi_{12}\right\rangle\left|\varphi_{34}\right\rangle$ may be rewritten as

$$\left|\Psi_{1234}\right\rangle = \frac{1}{2}\Big[\left|\varphi_{14}^{(+)}\right\rangle\left|\varphi_{23}^{(+)}\right\rangle - \left|\varphi_{14}^{(-)}\right\rangle\left|\varphi_{23}^{(-)}\right\rangle + \left|\psi_{14}^{(+)}\right\rangle\left|\psi_{23}^{(+)}\right\rangle - \left|\psi_{14}^{(-)}\right\rangle\left|\psi_{23}^{(-)}\right\rangle\Big], \tag{10}$$

where pairs of subscripts denote which particles are entangled. Now, if Alice projects particles 2 and 3 into a Bell-state, the state of particles 1 and 4 will be subsequently entangled, as portrayed by Fig. 2.

The four possible measurement outcomes from Eq. (10) correspond with the four possible Bell states; the measurement needs to be communicated to both ends of the newly formed quantum channel so that the parties are aware of which entangled state they share. This step also verifies to the parties that entanglement swapping occurred. But what is perhaps the most remarkable feature of entanglement swapping is that particles 1 and 4 are never required to be in physical contact with one another. In particular, the distance by which the particles are physically separated can be exceedingly great.

Entanglement swapping provides a means for preparing quantum communications channels over arbitrary distances through the use of a quantum repeater [15, 16, 17]. Suppose Alice and Bob are separated by a distance L, which is divided into N piece-wise segments connected by N - 1 nodes, as shown in Fig. 3(a). Let each node in the transmission line also be a source of entangled particle pairs. In a quantum repeater setup, both Alice and node 1 transmit a particle to the middle of the first segment. Upon meeting in the middle of the segment, entanglement swapping is performed on the transmitted particles, cf. Fig. 3(b). Consequently, Alice's remaining particle is entangled with the other particle originating from node 1, which can then be moved a distance $L/2N$ along the second segment of the transmission line. Thus, this process extends the original quantum channel over a distance of $3L/2$.

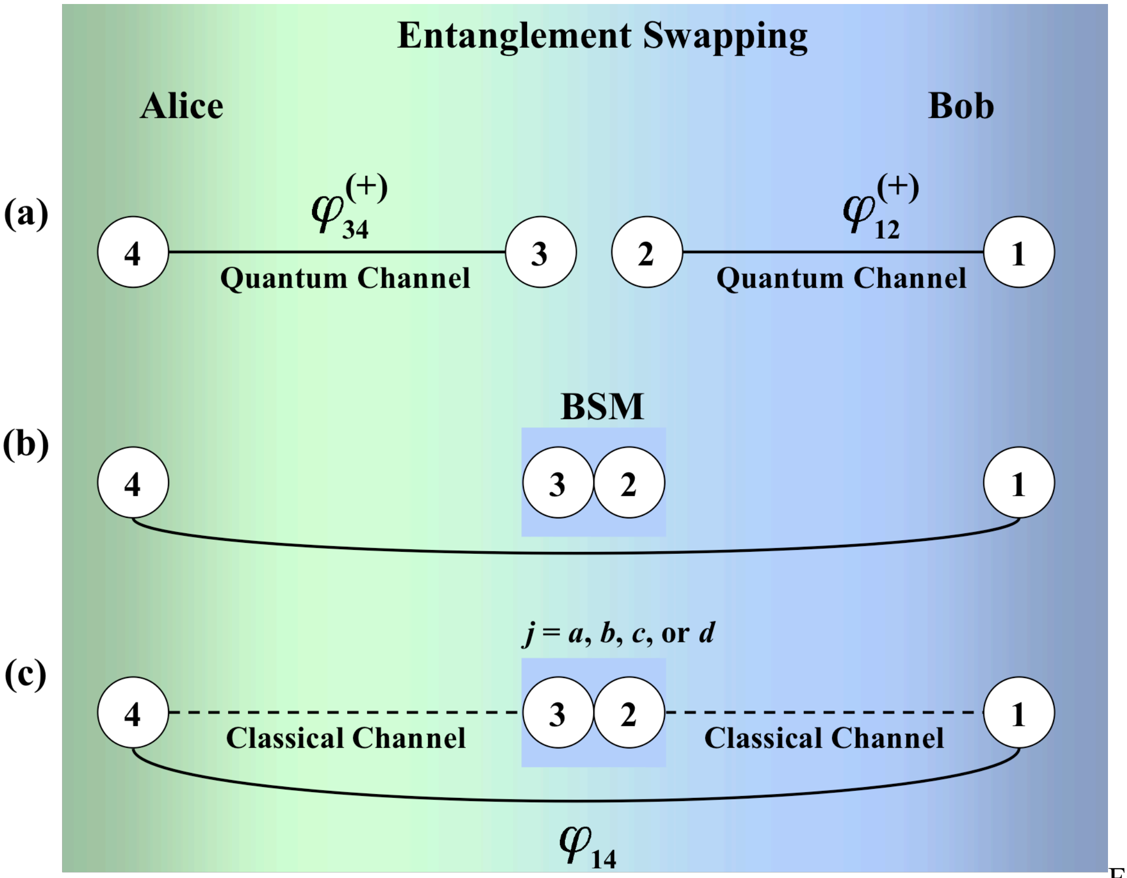

Figure 2. Entanglement swapping between Alice and Bob. (a) Initially, both parties posses a pair of entangled particles. (b) Bringing together a member from each pair, a Bell-state measurement (BSM) is performed. (c) Transmission of the BSM outcome *j* to both Alice and Bob verifies entanglement swapping occurred and notifies the parties which entangled state they share.

The above procedure can be repeated in a stepwise manner along successive segments with each swapping operation increasing the distance over which the quantum channel extends by an amount L/N. Ultimately, after $N - 1$ such actions, Alice and Bob share a quantum channel across the whole distance. (More efficient strategies are also possible, e.g., by preparing quantum channels across each segment in parallel [16].)

Even though any one particle only traverses a distance $L/(2N)$ in the scheme presented above, there is still a finite probability that the transmitted particles will be affected by noise, which will reduce entanglement of the final particle pair. Without any means to correct for these errors, the segmented transmission line presented above does not offer any advantage over direct distribution of the entanglement. This is because the transmission probabilities across each segment decreases as $\exp\left(-L/NL_0\right)$, where L_0 is a characteristic length scale. When multiplied by the number of segments N, we see no advantage over the original scheme of direct distribution.

But, if the errors accrued across a segment are not too great, it is possible to correct for them using *entanglement purification* [9]. Entanglement purification reduces an ensemble of nonmaximally entangled states into a single, maximally entangled state. In practical terms, this amounts to sending multiple particles across each (noisy) segment, after which entanglement purification is performed. The number of nonmaximally entangled states required by the purification protocol depends on the desired level of output entanglement. Note that for a state to be "purified", however, a minimal amount of entanglement must belong to each member of the ensemble. This effectively places a bound on the acceptable noise level, which in turn restricts the maximal distance of each segment. But, more importantly, by using entanglement swapping and purification in concert, a reliable quantum channel can be established between Alice and Bob over arbitrary distance.

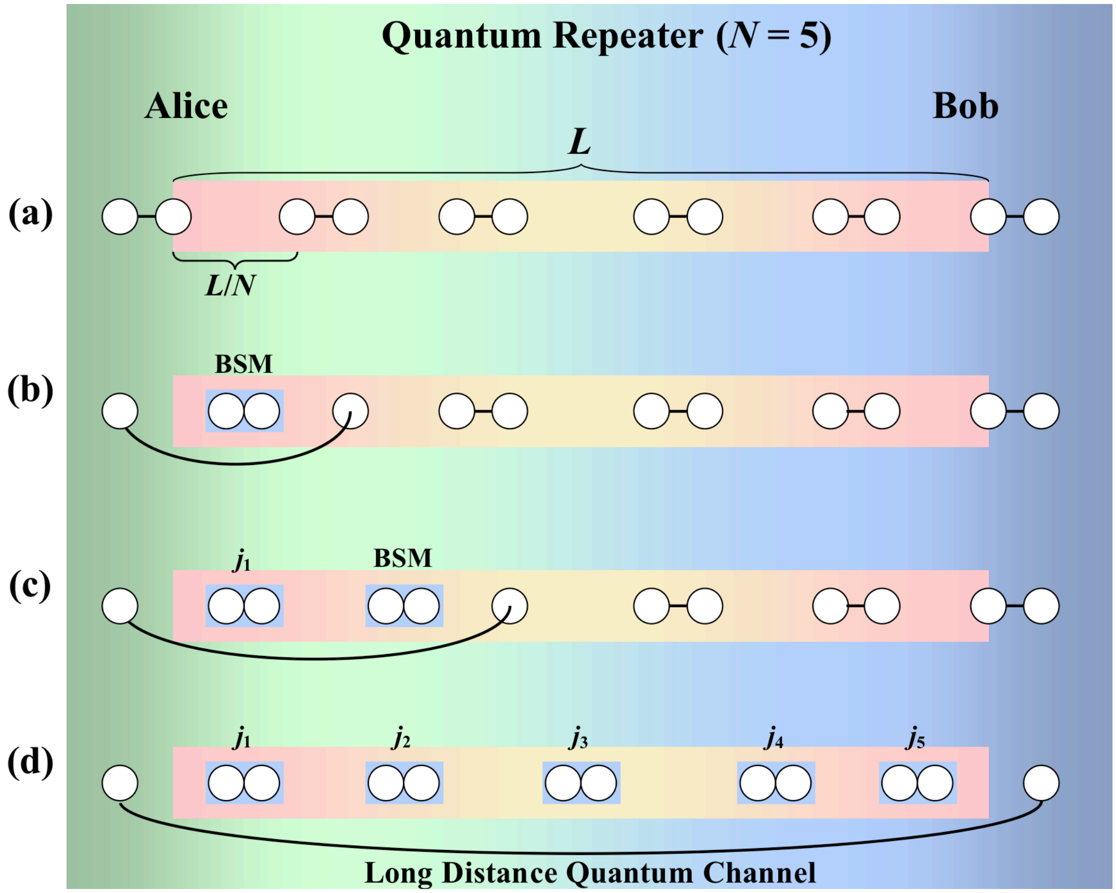

Figure 3. A quantum repeater for entanglement distribution. (a) The transmission distance L is divided into N segments (here $N = 5$) with the intervening N-1 nodes as sources of entangled particles. (b) Midway the first segment, a Bell-state measurement (BSM, blue box) swaps entanglement using one of the particles from node 1 and one of Alice's particles. The measurement outcome j_1 labels the newly formed quantum channel. (c) Repeated applications of the BSM extend the quantum channel further along the transmission line. (d) After N BSM's, Alice and Bob share a long distance quantum channel determined by the string of outcomes j. Entanglement purification requires that steps (b) and (c) are repeated many times.

Presently, implementations of a quantum repeater face a significant technical challenge due to the resources required by entanglement purification, i.e., the ensemble of minimally entangled states spanning each segment. In general, the number of states required depends on the degree of desired fidelity, as well as the amount of minimal entanglement initially available; typical numbers are on the order of 10's of pairs spanning each segment [16, 17]. Unfortunately, current state-of-the-art techniques for generating entangled states (photonic implementations are perhaps the most advanced) are unable to reliably prepare so many distantly separated entangled states simultaneously.

The problem of generating a sufficient number of entangled states would be alleviated to some extent if a quantum memory device was developed, i.e., a device capable of storing quantum information in a noise-free environment. Previously prepared entangled states could then be stored while others were being generated. To date, only preliminary forms of such a device exist [18], but, as we shall see in the next section, the development of robust quantum memory could underlie future secure forms of encrypted communication.

Finally, we present a note on the security of a quantum repeater in the even that Alice and Bob must rely on a third party to operate the intermediary entanglement swapping nodes. In this scenario, Alice and Bob must verify that their quantum communication channel has not been compromised by some man-in-the middle attack. To do so, Alice and Bob will test the entanglement of states prepared using the quantum repeater in order to quantity the amount of entanglement present. Maximally entangled states (1 ebit) are only obtainable in the absence of an eavesdropping attack. This testing procedure requires that both parties sample from an ensemble of entangled states prepared using the quantum repeater. The sampling procedure for both parties consists of randomly choosing between two measurement bases. These choices will later be announced openly to determine instances of when Alice and Bob made different bases choices. By comparing the measurements obtained in the latter cases, a measure of the entanglement in the down-selected sample of states can be obtained using, e.g., Bell's inequality [8]. Effectively, Alice and Bob are ensuring that correlations between their data exist and that these correlations are inherently quantum mechanical. As we will see below, this same verification step is required to test the security of QKD protocols. Of course, this technique of testing entanglement can also be used for diagnosing between which nodes the eavesdropper is located.

Entanglement-based Quantum Key Distribution

Quantum communication channels are useful not only for teleporting unknown quantum states, but also for generating strings of random bits between distant parties. This has lead to the development of quantum key distribution (QKD). In QKD, one exploits uncertainty inherent to the quantum-mechanical measurement in order to circumvent eavesdropping in the distribution of a cryptographic key. When both parties share the secret key, it can be used by them to encrypt a (classical) message.

The original QKD protocol was proposed by Bennett and Brassard in 1984 (BB84) and uses single, unentangled particles [2]. In the BB84 protocol, Alice sends Bob a particle whose state she randomly chooses to belong either to the set $|\uparrow\rangle$ and $|\downarrow\rangle$, or $|\rightarrow\rangle$ and $|\leftarrow\rangle$. (The two bases must be maximally conjugate in the sense that $|\langle\uparrow|\rightarrow\rangle|^2 = |\langle\downarrow|\rightarrow\rangle|^2 = 1/2$, etc.) Similarly, Bob randomly chooses to measure the state of the received particle in one of the two bases. After Bob performs his measurements on a sample of the transmitted particles, he announces to Alice (and anyone else who may be listening) what sequence of bases he used for his measurements. Alice confirms to Bob which of his measurements coincided with her preparations, and the corresponding measurement results (which are not communicated openly but are known to both Alice and Bob) comprise the raw key. In the next stage, classical cryptographic methodology takes over with the use of error correction and privacy amplification to strengthen the security of the trusted, sifted key [11].

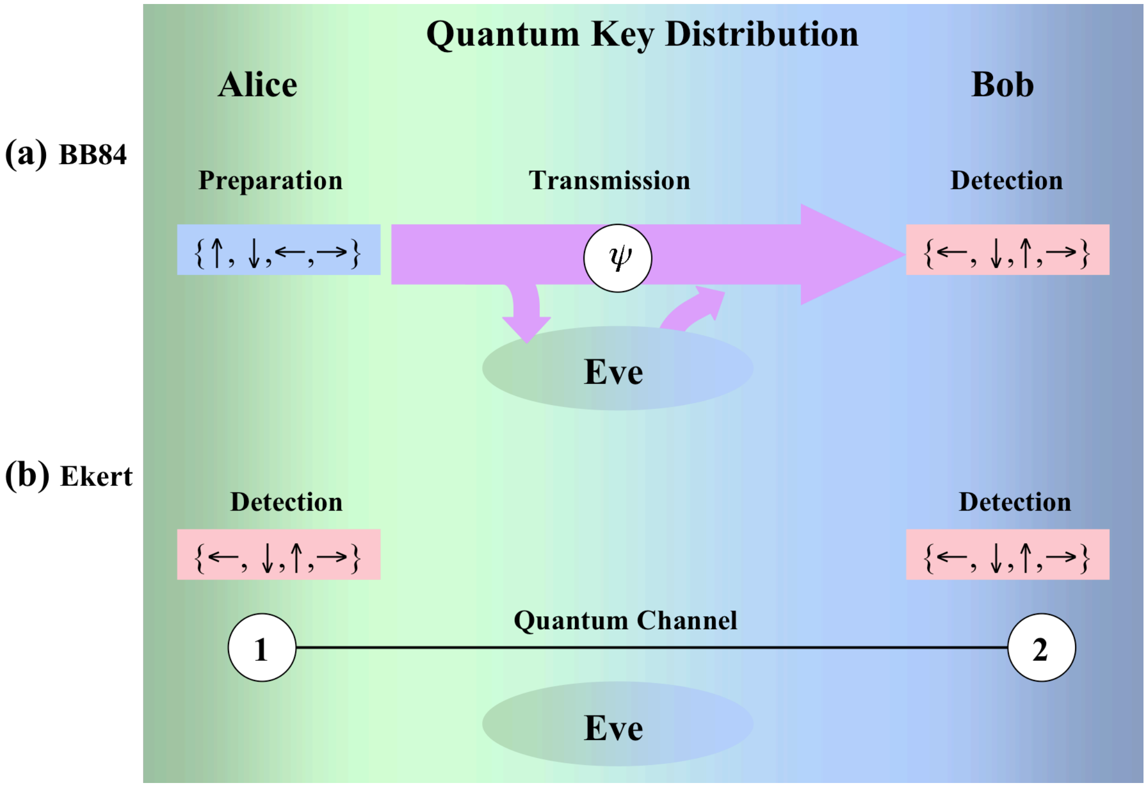

Figure 4. Two schemes for quantum key distribution. (a) BB84 protocol: Alice transmits randomly prepared states while Bob detects each particle in a randomly chosen basis. Alice and Bob compare the generated bit values over an open channel to create a secret key. Eve's access to the particle during transmission may compromise the security of the key because she could potentially carry out some form of eavesdropping attack, e.g., an intercept-resend attack. (b) Entanglement-based protocol: Alice and Bob use shared entangled particles to generate a random string. They verify the expected nonlocal and reconcile their strings over an open channel. To circumvent any form eavesdropping by Eve, the entangled particles can be securely distributed ahead of time and stored until a key needs to be generated.

In BB84, the classical communication channel over which Alice and Bob communicate need only be authentic, not confidential, such that any eavesdropper Eve may listen to their conversation but not modify it. BB84-QKD is provably secure under ideal circumstances, i.e., the sources and detectors are working ideally [19], but under more realistic conditions, including noisy transmission channels and imperfect detectors, QKD is only known to withstand certain attacks. For example, it has been shown that if Eve attempts to intercept and resend the photons that Alice transmits to Bob, then Eve's interceptions can be identified by an increased bit error rate in the sifted key (a consequence of the no-cloning theorem) [11]. Hence, Alice and Bob monitor the extent of Eve’s intrusion through an accompanying increase in the (quantum) bit error rate; they reject the sifted key in the event the bit error rate is too large (~11% or more [19]), or they perform privacy amplification techniques to increase the secrecy of the sifted key. However, the possibility that Eve might gain some vital information of the shared key using more sophisticated attacks has not been ruled out [20, 21].

An alternative, entanglement-based strategy for quantum key distribution closely mimics the original BB84 protocol. In this implementation of QKD, first put forward by Ekert [3], Alice and Bob share a pair of entangled particles. Both parties measure their particles using randomly and independently chosen bases. After completing a sequence of measurements, Alice and Bob announce their respective bases (but not the measured values). For those measurements where their chosen bases are different, Alice and Bob then openly share their measurement results. With this data, both are able to compute a suitable form of Bell’s inequality to test the nonlocality of the particles observed behavior [8, 22]. If violated, Bell’s inequality assures the security of the quantum communication channel, since only quantum-mechanically entangled particles remain correlated when subjected to this combined random measurement apparatus. The other, unannounced measurements can be used to build the raw key from which a sifted key is generated by means of error correction and privacy amplification (as in the BB84 protocol). If Bell’s inequality is not violated, then Alice and Bob should not trust that their remaining measurements were derived from the intended entangled particles. This is because, in addition to sources of noise, the failure to violate Bell’s inequality signals the presence of an eavesdropper and a loss of confidentiality.

Despite strongly similarities between BB84 and the Ekert protocol, there are some benefits to entanglement-based QKD that lie in the use of nonlocality to ensure privacy.

Foremost is the fact that no information about the secret key exists until Alice and Bob measure an entangled particle pair. Accordingly, the distribution of entangled particles does not commit the users to communication with each other. In contrast, the BB84 protocol requires that Alice initially prepare and track the quantum state of each particle sent to Bob. This operational restriction means that whomever distributes the particles has the information necessary to discern the raw key that Bob generates with his choice of basis. Since generation and distribution of the entangled particles in the Ekert protocol could occur by means of third parties (quantum repeaters), the former restriction does not apply. Of course, such generated and distributed particles would need to be tested to ensure entanglement between Alice and Bob.

An appealing scenario for the use of entanglement-based QKD arises when quantum memory devices are available. It should then be possible for Alice and Bob to store distributed, entangled particles for future use. For example, Alice and Bob could distribute entanglement in a trusted (local) environment, after which they part ways. At some later time, the shared entanglement resources could be used to perform QKD provided a classical (authentic) two-way communication channel was available. This procedure would side step Eve's potential attacks on entanglement distribution, including those denial-of-service attacks in which the particles are (intentionally) destroyed. Of course, if the quantum memory entanglement stores become depleted, Alice and Bob must replenish them. Because the distribution of entangled particles does not commit the recipients to communication, one can envision secure couriers that independently provide renewed quantum memories to the Alice and Bob.

Quantum Networks and Quantum Computers

Quantum teleportation has expanded the repertoire of quantum information science by enabling a host of teleportation-based quantum technologies. In addition to straightforward teleportation, our survey has included applications to remote-state preparation [12], entanglement distribution and quantum repeaters [15, 16], quantum memories [18], and entanglement-based quantum key distribution [3]. These applications are themselves the foundations for developing quantum computers, quantum key distribution systems, and long-distance quantum communication networks [1, 23]. The latter are multi-faceted, integrated systems composed of many interconnected components and protocols. We will describe briefly some aspects of their continuing development. A more comprehensive review can be found in Ref. [1].

Quantum networks consist of multiple interconnected nodes between which qubits of information are transmitted. Transmission of information between nodes is done either by directly sending the encoded particle or by using variations of quantum teleportation. Individual nodes in a network may be quantum memory or entanglement sources, or nodes may be used together to carry out steps in a communication protocol, e.g., a quantum repeater. The connectivity of the nodes determines the geometry of the quantum network and is a basic feature in the design of network function. Entanglement-based QKD is a simple example of a quantum network where two parties directly interact. More elaborate networks consisting of multiple users and indirect communication pathways are also possible. An essential component of a given quantum network is an accompanying network of classical communication channels to satisfy the communication cost incurred, e.g., as in the teleportation protocol. Quantum networks, especially those based on faint laser pulses, have recently been implemented outside of the laboratory. In particular, simple quantum networks set up for QKD have become the first quantum technology to reach the market [24] and to be implemented on a large (metropolitan) scale [25, 26]. Future quantum networks will utilize entanglement sources, quantum teleportation, and quantum repeaters.

Quantum computers are, in many regards, specialized quantum networks for executing quantum algorithms [27]. The development of quantum computers has attracted attention because of the enormous speed up that quantum algorithms can bring to certain problems, e.g., factoring numbers [5]. Although proposed architectures vary, quantum computers are typically composed of a sequence of computational gates (unitary transformations) that transform an input qubit to an output qubit. Ultimately, the calculation terminates when a measurement on the transformed qubit(s) is carried out and a classical bit value is obtained. Confidence in the measurement is built by repeating the procedure a desired number of times. The global effort currently underway seeks to identify those physical systems best suited for the development of a quantum computer. Several proposals show promise, but outstanding technical issues remain with each [28].

The capabilities that quantum networks and quantum computers portend are significant: communication networks for securely transmitting information, both classical and quantum, and sufficient computational power for pragmatic brute-force cryptanalysis. Though many practical issues remain unresolved in their development, the theory leading to their inception can be viewed as a demonstration of the capabilities of quantum information science [29].

References

1. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, New York, 2000).
2. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE Press, New York, 1984).
3. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **61**, 661 (1991).
4. C. H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, and W. K. Wooters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett. **70**, 1895 (1993).
5. P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM* (IEEE Press, New York).
6. L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the 28th Annual Symposium on the Theory of Computing* (ACM Press, New York, 1996).
7. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," Nature **390**, 575 (1997).
8. J. S. Bell, "On the problem of hidden variables in quantum mechanics," Rev. Mod. Phys. **38**, 447 (1966).
9. C. H. Bennett, H,. J. Bernstein, S. Popescu, and B. Schumaker, "Concentrating partial entanglement by local operations," Phys. Rev. A **53**, 2046 (1996).
10. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802 (1982).
11. N. Gisin, G. Ribordy, W. Dür, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145 (2002).
12. C. H. Bennett, D. P. Divincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, "Remote state preparation," Phys. Rev. Lett. **87**, 077902 (2001).
13. With optical fibers, the current limit on transmission distance is on the order of 100 km. Although free-space, i.e., atmospheric, transmission pathways do not suffer from depolarizing or absorption noise, there is a significantly greater background noise, especially during daytime hours.
14. M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "'Even-ready-detectors' Bell experiment via entanglement swapping," Phys. Rev. Lett. **71**, 4287 (1993).
15. 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. **81**, 5932 (1998).
16. W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," Phys. Rev. A. **59**, 169 (1999).
17. W. Dür, "Quantum communication over long distances using quantum repeaters," Thesis, University of Innsbruck, Austria (1998).

18. C. Langer *et al*. "Long-lived qubit memory using atomic ions," Phys. Rev. Lett. **95**, 060502 (2005); in this example, a qubit was reliably stored in an atomic superposition state for up to 10 seconds.
19. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441 (2000).
20. H. E. Brandt, "Quantum-cryptographic entangling probe," Phys. Rev. A **71**, 042312 (2005).
21. J. H. Shapiro and F. N. C. Wong, "Attacking quantum key distribution with single-photon two-qubit quantum logic," Phys. Rev. A **73**, 012315 (2006).
22. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiments to test local hidden-variable theories," Phys. Rev. Lett. **23**, 880 (1969).
23. D. Gottesman and I. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," Nature **402**, 390 (1999).
24. The two most prominent examples are MagiQ (www.magiqtech.com) and id Quantique (www.idquantique.com). Both specialize in optical implementations of quantum cryptography.
25. C. Elliot, D. Pearson, and G. Troxel, "Quantum cryptography in practice," *SIGCOMM 2003* (ACM Press, New York, 2003)
26. C. Elliot, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," Proc. of SPIE **5815**, 138 (2005).
27. V. Vedral, A. Barenco, and A. Ekert, "Quantum networks for elementary arithmetic operations," Phys. Rev. A **54**, 147 (1996).
28. See the "Quantum computation roadmap," commissioned by ARDA and available at www.qist.lanl.gov, for a list of proposals and a survey of current efforts in quantum computation and quantum networks.

29. TSH gratefully acknowledges support from the IC Postdoctoral Research Fellowship.