Inside Quantum Repeaters

William J. Munro, Koji Azuma, Kiyoshi Tamaki, and Kae Nemoto

(Invited Paper)

***Abstract*—Most quantum communication tasks need to rely on the transmission of quantum signals over long distances. Unfortunately, transmission of such signals is most often limited by losses in the channel, the same issue that affects classical communication. Simple signal amplification provides an elegant solution for the classical world, but this is not possible in the quantum world, as the no-cloning theorem forbids such an operation and, thus, an alternative approach, a quantum repeater, is needed. Quantum repeaters enable one to create a known maximally entangled state between the end points of the network by first segmenting the network into pieces, creating entanglement between the segments, and then, connecting those entanglement to create the required long range entanglement. Quantum teleportation then allows an unknown quantum message to be transmitted between them using the long-range entangled state. This form of quantum communication will be at the heart of the future quantum Internet. In this review, we will detail various approaches to quantum repeaters, and discuss their expected performance and limitations.**

***Index Terms*—Quantum communication, repeaters and networks.**

I. Introduction

THE development of technologies based on the principles of quantum mechanics is likely to be one of the foundations upon which the 21 century society relies [1]–[3]. What form these technologies will take is still unknown, but it is already well known that the principles of superposition and entanglement allow tasks to be undertaken that are either extremely hard or impossible to be achieved in the classical world. Such tasks include for instance secure communication [4], the prime factorisation of large integers [5] and the simulation of complex quantum systems [6]. The full potential and range of applications are however still unknown. Broadly the field of quantum information processing (the field associated with these quantum principles) can be broken into a number of areas including:

1) Quantum measurement, metrology and sensing [7], [8],
2) Quantum communication [9]–[12],
3) Quantum computation and simulation [6], [13]–[15].

All these areas have seen significant advances in recent years with many technologies being developed. Even commercially available ones exist [16]. We will now turn our attention to quantum communication as the focus of this review paper, beginning with a brief discussion of what quantum communication is. Quantum communication is a way to transmit signals (either quantum or classical) over distances using the principles of quantum mechanics. Such signals could be used for tasks ranging from cryptography to large-scale distributed quantum computation [17]–[19]. One of the technologically most advanced is quantum key distribution (QKD) [4], [9], a task where one establishes a secret key between the two remote parties (Alice and Bob in this case) using simple light pulses. A number of field tests have already been demonstrated [20]–[23]. For most other applications one needs to generate entangled links between the various parties and these can be used in a number of ways. The simplest is to use the entangled resource to teleport a quantum state from Alice to Bob [24]. but these entangled links could also be used to generate multipartite entangled states for quantum secret sharing [25], distributed quantum sensing, metrology or computing activities, etc. If these parties are far beyond the attenuation length of the channel between themselves, then one will not efficiently be able to establish the entangled links. In such a situation quantum repeaters are likely to be needed [26], [27] and work by dividing the long-distance link into a number of segments with a repeater at each node [27]. As the links are a shorter distance apart, the entangled links can be obtained with much higher probability and hence by connecting all the links together with entanglement swapping [24], [28] we can generate the required long-range entanglement.

This review is organised as follows. We begin in Section II with an overview of quantum communication via exemplifying QKD and quantum teleportation. Here it will be shown that it is essential for quantum communication to distribute entanglement between two remote parties Alice and Bob, and then in Section III we introduce three generic entanglement distribution schemes. These schemes suffer from photon loss in the optical fibres, which naturally limits the communication distance. A solution is to use quantum repeaters and thus in Section IV we detail the basic concepts of how quantum repeaters work and the components required. Such components include the previously described mechanisms for entanglement distribution (see Section III) plus schemes for entanglement purification (see Section IV-A) and entanglement swapping (see Section IV-B). This is followed in Section V by how these components can be combined to create longer-range entanglement links. We also identify key limitations in this basic design. In Section VI, we show how these limitations can be overcome. As a result, the communication rate is dramatically increased and the requirements on the memory time become less demanding, now associated only with the communication time between adjacent nodes. Section VII further shows that a quantum repeater network can

Manuscript received August 12, 2014; revised November 4, 2014 and December 30, 2014; accepted January 6, 2014.

W. J. Munro, K. Azuma, and K. Tamaki are with the NTT Basic Research Laboratories, NTT Corporation, Atsugi 243-0198, Japan (e-mail: bill.munro@me.com; azuma.koji@lab.ntt.co.jp; tamaki.kiyoshi@lab.ntt.co.jp).

K. Nemoto is with the National Institute of Informatics, Tokyo 101-8430, Japan (e-mail: nemoto@nii.ac.jp).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSTQE.2015.2392076

1077-260X © 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

be established without the use of quantum memories at all, while Section VIII briefly introduced how a complex network could be achieved.

II. Quantum Communication

Let us introduce the concept behind quantum communication. The main role of quantum communication is to transmit quantum signals over distances [9]–[12]. More specifically it enables a party called Alice to send a distant party called Bob any quantum state of the form $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with complex numbers α and β (satisfying $|\alpha|^2 + |\beta|^2 = 1$), where $\{|i\rangle\}_{i=0,1}$ are orthonormal basis states that might, for example, be the ground state $|g\rangle$ and an excited state $|e\rangle$ of a matter system or the horizontally polarised state $|H\rangle$ and vertically polarised state $|V\rangle$ of a single-photon system. Since Alice's state $|\psi\rangle_A$ should be transferred to Bob through the ideal quantum channel, the ideal channel could be described by the identity map $I^{A\to B} = |0\rangle_{B\,A}\langle 0| + |1\rangle_{B\,A}\langle 1|$ because $I^{A\to B}|\psi\rangle_A = |\psi\rangle_B$. Hence, one might think that the ultimate goal for realising quantum communication is to give Alice and Bob a device to work as the identity map $I^{A\to B}$)]. However, interestingly, this is not the only solution. In particular, quantum communication is also possible if the distant parties, Alice and Bob, share an entangled pair called a Bell state $|\Phi^+\rangle_{AB} = (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)/\sqrt{2}$. In this section, we illustrate this approach through providing representative quantum communication operations, i.e., quantum teleportation [24] and QKD [4], [9]. As a result, the Bell state is regarded as a resource for quantum communication.

A. Quantum Teleportation

Quantum teleportation [24] is an important primitive quantum communication operation [12] which is based on Alice and Bob's pre-established Bell state $|\Phi^+\rangle_{AB}$. Then by using this Bell state and classical communication Alice can transmit any state of the form $|\psi\rangle = \alpha|0\rangle_{A'} + \beta|1\rangle_{A'}$ to Bob.

The scheme begins with Alice's Bell measurement on the systems A' and A giving a result corresponding to one of the four Bell states $|\Phi^\pm\rangle_{A'A} = (|0\rangle_{A'}|0\rangle_A \pm |1\rangle_{A'}|1\rangle_A)/\sqrt{2}$ and $|\Psi^\pm\rangle_{A'A} = (|0\rangle_{A'}|1\rangle_A \pm |1\rangle_{A'}|0\rangle_A)/\sqrt{2}$. If a measurement outcome corresponding to state $|\Phi^+\rangle_{A'A}$ is obtained, Bob's state is $|\psi\rangle_B$ (from ${}_{A'A}\langle\Phi^+||\psi\rangle_{A'}|\Phi^+\rangle_{AB} = |\psi\rangle_B/2$), which is the state Alice wants to transfer. Similarly for a measurement outcome corresponding to state $|\Phi^-\rangle_{A'A}$, Bob's state is $Z_B|\psi\rangle_B$ as ${}_{A'A}\langle\Phi^-| = {}_{A'A}\langle\Phi^+|Z_A$ and $Z_A|\Phi^+\rangle_{AB} = Z_B|\Phi^+\rangle_{AB}$, where Z is a sign flip defined by $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. For a measurement outcome corresponding to state $|\Psi^+\rangle_{A'A}$ ($|\Psi^-\rangle_{A'A}$), Bob's state is $X_B|\psi\rangle_B$ ($Z_B X_B|\psi\rangle_B$), where X is a bit flip defined as $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. Hence, if Alice sends the measurement outcome to Bob over a classical channel, by applying one of unitary operations $\{I_B, Z_B, X_B, Z_B X_B\}$ depending on Alice's measurement outcome, Bob can always obtain the state $|\psi\rangle_B$ originally held by Alice. Therefore, Alice can send her quantum signal $|\psi\rangle_{A'}$ to Bob just by using the Bell state $|\Phi^+\rangle_{AB}$ and classical communication.

Since quantum teleportation requires classical communication from Alice to Bob, Bob's system B should work as a quantum memory to keep a quantum state until at least the end of the classical communication. This is important as it inherently implies that quantum teleportation requires the use of a quantum memory.

B. Quantum Key Distribution

Suppose that Alice and Bob have systems AB in the Bell state $|\Phi^+\rangle_{AB}$, and they make Z-basis measurements (i.e., measurement in the basis of $\{|i\rangle\}_{i=0,1}$) on the systems AB. Then, since the Bell state is a pure state, nobody (except for Alice and Bob who actually obtained the measurement outcomes) can predict the measurement outcomes. That is, their bits are perfectly secure. In addition, from the definition of the Bell state $|\Phi^+\rangle_{AB} = (|00\rangle_{AB} \pm |11\rangle_{AB})/\sqrt{2}$, the Z-basis measurement outcomes are always random and perfectly correlated. Hence, the Z-basis measurement outcomes on systems AB in the Bell state $|\Phi^+\rangle_{AB}$ can serve as a secret bit [29], [30]. This allows Alice to send any 1-bit information to Bob in an information-theoretically secure manner, by invoking the one-time pad (based on a public channel between Alice and Bob). Therefore, a Bell pair is a resource for transmitting 1 bit in a secure manner.

Usually, Alice and Bob need to possess quantum memories to share the Bell state $|\Phi^+\rangle_{AB}$ [for instance, owing to the probabilistic nature of the entanglement generation or of quantum purification needed under the existence of noises (see Section IV-A)]. However, interestingly, the secure key from this protocol can be shown [31] to be equivalent to that from a QKD protocol *without quantum memories*, e.g., where Alice and Bob simply perform measurements on the incoming pulses distributed from a third party or Alice sends pulses over a quantum channel to Bob who performs measurements on the pulses (see Section III)]. This is so because Alice and Bob's quantum memories to be prepared in the Bell state $|\Phi^+\rangle_{AB}$ can be regarded as fictitious qubits in the QKD protocol. Therefore, QKD protocols usually do not require Alice and Bob to have quantum memories, which is in a striking contrast to the quantum teleportation that needs quantum memories.

III. Entanglement Distribution

As was seen in the previous section, the resource for many quantum communication schemes is entanglement between remote parties, Alice and Bob. Thus we will begin with explaining how to supply Alice and Bob with entanglement in practice, i.e., entanglement generation schemes. It can be achieved in quite a number of ways [10], [11], [24], [26], [27], [32]–[44] using many different types of physical systems, for instance, using single atoms (or artificial atoms) within cavities or ensembles of atoms in a vapor. Nonetheless, they still share a number of core attributes that allow us to characterise them into three basic themes. These are depicted in Fig. 1 and use single photons as the communication medium. However note that, in general, entangled-photon or continuous variable sources [35] can be used in many cases. Let us consider the three representative approaches in order.

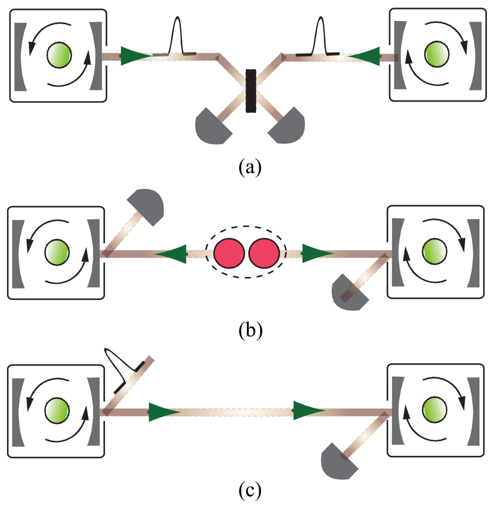

Fig. 1. Schematic illustration of three schemes to generate entanglement between two spatially separated nodes. The first (a) is based on the emission or reflection of a photon from each individual cavity and their interference at a polarising beamsplitter in the mid point between the nodes. Detection of a photon in each mode heralds the creation of the entangled link. The second scheme (b) is based on sending half of a Bell state to each repeater node where the photon is entangled with the qubit in the associated cavity. The measurement of each photon then transfers the original photonic Bell-state entanglement to the repeater nodes, as well heralding photon loss. The third scheme (c) is based on a single photon initially starting at one of the nodes where it interacts with the qubit in the cavity present there to entangle with it. The photon is then transmitted over an optical fiber to the adjacent repeater where it interacts and entangles itself with the qubit in that cavity. The measurement of the photon then projects the two remote qubits into an entangled state, provided the photon was measured.

In the first case (see Fig. 1(a)), a single photon (p) is entangled with an atom (a) in a cavity, by either the atom emitting a photon or a photon being reflected off the cavity mirror, creating a state of the form $[|g\rangle_a|H\rangle_p + |e\rangle_a|V\rangle_p]/\sqrt{2}$ [45]–[53]. With two atoms a_1a_2 in separate cavities being entangled to their respective single photons p_1p_2, we have a combined state of the form

$$|\Psi_1\rangle = \frac{1}{2}[|g\rangle_{a_1}|H\rangle_{p_1} + |e\rangle_{a_1}|V\rangle_{p_1}] [|H\rangle_{p_2}|g\rangle_{a_2} + |V\rangle_{p_2}|e\rangle_{a_2}]. \quad (1)$$

Interfering the two photons on a polarising beamsplitter, and post-selecting situations where we have one photon in each output mode, our combined state can be represented by $[|g\rangle_{a_1}|H\rangle_{p_1}|H\rangle_{p_2}|g\rangle_{a_2} + |e\rangle_{a_1}|V\rangle_{p_2}|V\rangle_{p_1}|e\rangle_{a_2}]/\sqrt{2}$. Measuring the photons in the basis of diagonal state $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and anti-diagonal state $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$, we have

$$|\Psi_2\rangle = \begin{cases} |\Phi^+\rangle_{a_1a_2}, & \text{for } D, D \text{ or } A, A \\ |\Phi^-\rangle_{a_1a_2}, & \text{for } D, A \text{ or } A, D \end{cases} \quad (2)$$

with $|\Phi^\pm\rangle_{a_1a_2} := \frac{1}{\sqrt{2}}[|g\rangle_{a_1}|g\rangle_{a_2} \pm |e\rangle_{a_1}|e\rangle_2]$. We immediately observe that depending on the parity of the measurement result associated with the detection of a polarization-encoded photon at each port after the PBS, we have one of two Bell states with 25% probability each [54]. The measurement results need to be sent to both end nodes indicating which Bell state they have generated or that no coincidence result occurred. In this last situation, the photons "bunch" and so no photons are detected in one of the modes (no coincidence counts). In this case our entanglement generation operation has failed and a classical message must be sent indicating we must try again.

The second entanglement distribution scheme depicted in Fig. 1(b) is based on an optical Bell state (say $[|H\rangle_{p_1}|H\rangle_{p_2} + |V\rangle_{p_1}|V\rangle_{p_2}]/\sqrt{2}$) [55] being sent to the adjacent nodes from a node between them, where the qubits (atoms or vapors) in the end nodes have been prepared in the equal superposition state $|+\rangle_{a_i} = [|g\rangle_{a_i} + |e\rangle_{a_i}]/\sqrt{2}$. A controlled-phase operation can be performed between each qubit and its associated photon giving

$$|\Psi_3\rangle = \frac{1}{2}|\Phi^+\rangle_{a_1a_2} \otimes [|H\rangle_{p_1}|H\rangle_{p_2} + |V\rangle_{p_1}|V\rangle_{p_2}] + \frac{1}{2}|\Psi^+\rangle_{a_1a_2} \otimes [|H\rangle_{p_1}|H\rangle_{p_2} - |V\rangle_{p_1}|V\rangle_{p_2}] \quad (3)$$

where $|\Psi^\pm\rangle_{a_1a_2} = [|g\rangle_{a_1}|e\rangle_{a_2} \pm |e\rangle_{a_1}|g\rangle_{a_2}]/\sqrt{2}$. Measuring both photons individually in the basis of states $|D\rangle$ and $|A\rangle$ results in a Bell state, depending on the parity similarly to Eq. (2). A classical message is sent between the nodes indicating which parity result was obtained. In the ideal case, this scheme succeeds with 100% probability and thus has an advantage compared to the previous scheme. It does however require a source of optical Bell states (as well as a controlled-phase operation between a photon and an atom).

The third entanglement distribution depicted in Fig. 1(c) is based on a single photon being transmitted between the nodes [34], [44], [50], [51], [53], [56], [57]. In this case consider that the left-hand-side node has prepared a qubit in the state $|+\rangle_{a_1}$ along with a single photon as $|D\rangle_{p_1}$. A controlled-phase operation is then performed between them followed by the photon being sent over the channel to its adjacent node. In the right-hand-side node, the photon interacts with its qubit which was prepared in the state $|+\rangle_{a_2}$. The resulting three-qubit state has the form

$$|\Psi_4\rangle = \frac{1}{\sqrt{2}}|\Phi^+\rangle_{a_1a_2} \otimes |D\rangle_{p_1} + \frac{1}{\sqrt{2}}|\Psi^+\rangle_{a_1a_2} \otimes |A\rangle_{p_1}.$$

Now measuring the single photon in the basis of states $|D\rangle$ and $|A\rangle$ we project the distant qubits into the state $|\Phi^+\rangle_{a_1a_2}$ for an event of detecting D and $|\Psi^+\rangle_{a_1a_2}$ for A. For the event of detecting A, the second node can perform a local correction operation to transform $|\Psi^+\rangle_{a_1a_2}$ to $|\Phi^+\rangle_{a_1a_2}$. In principle this scheme succeeds deterministically.

So far, our considerations have been highly idealised in the sense that we have not considered channel loss, nor imperfect sources and detectors. As these can be considered as loss events, and as we are conditioning our entanglement generation on a photon click that occurs only when single photons have not been lost, their effect is to simply lower the probability of success. For the three entanglement distribution examples given above, we can express the probability of success of the entanglement generation as

$$p_s = e^{-L/L_0} p_{\text{local}}, \quad (4)$$

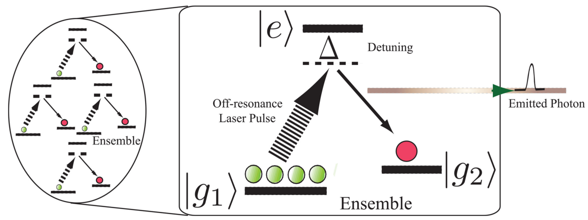

Fig. 2. An energy level diagram of an ensemble of three-level Λ system. Each Λ system has non-degenerate ground states $|g_1\rangle$ and $|g_2\rangle$ and an excited state $|e\rangle$. The system initially begins with all atoms in their corresponding $|g_1\rangle$. An off-resonance classical laser pulse drives the $|g_1\rangle \leftrightarrow |e\rangle$ transition and a photon can be emitted from the $|e\rangle - |g_2\rangle$ transition: $|g_1\rangle|0\rangle_p \rightarrow |g_2\rangle|1\rangle_p$ (where the subscript p indicating a photonic mode). For a weak pulse on a single atom we have $|g_1\rangle|0\rangle_p \rightsquigarrow |g_1\rangle|0\rangle_p + \epsilon|g_2\rangle|1\rangle_p$ and thus for the ensemble $|0\rangle_{\rm ens}|0\rangle_p \rightsquigarrow |0\rangle_{\rm ens}|0\rangle_p + \epsilon|1\rangle_{\rm ens}|1\rangle_p$.

where $p_{\rm local}$ is the probability of the success of the local devices assumed in the respective protocol, and L is the length of the fiber (connecting Alice and Bob) with the attenuation length L_0. In particular, $p_{\rm local} = p^2_{\rm source}p^2_{\rm cou}p^2_{\rm det}/2$ for the first scheme, $p_{\rm local} = p_{\rm ent}p^2_{\rm cou}p^2_{\rm det}$ for the second scheme, and $p_{\rm local} = p_{\rm source}p^2_{\rm cou}p_{\rm det}$ for the third scheme, where $p_{\rm source}$ is the probability for a single-photon emission from a source, $p_{\rm cou}$ is the probability of coupling a photon to the qubit, $p_{\rm det}$ is the probability of detecting a photon with a detector, and $p_{\rm ent}$ is the probability of an entangled-photon-pair emission from a source. In the case of the application to QKD, the qubit can be regarded as a virtual one, and thus, we can assume $p_{\rm cou} = 1$. But e^{-L/L_0} is a shared exponential factor as can be seen in Eq. (4), which makes long-distance quantum communication inefficient.

A. An Example: The DLCZ Entanglement Distribution Scheme

It is now instructive to examine a specific example of one of these entanglement distribution protocols. One of the earliest was developed by Duan, Lukin, Cirac and Zoller [33], which is called the DLCZ protocol. This protocol is based on atomic ensembles. The ensemble is formed from a collection of three-level atoms in a Λ configuration (see Fig. 2) all prepared in their ground states $|g_1\rangle_i$. Our qubit in the ensemble is represented by the collective ground state $|0\rangle_{\rm ens} = |g_1\rangle_1|g_1\rangle_2|g_1\rangle_3\ldots|g_1\rangle_N$ and the first excited state $|1\rangle_{\rm ens} = S^\dagger|0\rangle_{\rm ens}$ where $S^\dagger = \sum_{i=1}^N |g_2\rangle_i\langle g_1|/\sqrt{N}$ with another state $|g_2\rangle$. The ensemble is driven by an off-resonance laser pulse inducing potential Raman transitions from $|g_1\rangle_i$ into $|g_2\rangle_i$ and photon emission from the $|e\rangle - |g_2\rangle$ transition in each Λ system. The interaction with this weak pulse (mean photon number $\bar{n} \ll 1$) for the whole ensemble gives

$$|\Psi_1\rangle = \sqrt{1-|\lambda|^2}(|0\rangle_{\rm ens}|0\rangle_p + \lambda|1\rangle_{\rm ens}|1\rangle_p + \lambda^2|2\rangle_{\rm ens}|2\rangle_p\ldots), \quad (5)$$

where $|1\rangle_p$ is a single forward propagating Stokes photon and $|\lambda| \ll 1$. Such a state is analogous to $[|g\rangle|H\rangle + |e\rangle|V\rangle]/\sqrt{2}$ (but where instead of polarization states, number states are used) and thus we can use an entanglement distribution scheme like the form of Fig. 1(a) to entangle the remote ensembles. After the 50/50 beamsplitter on optical modes, each of which is entangled with an atomic ensemble, our system can be described by

$$|\Psi_2\rangle \sim (1-|\lambda|^2)[|0\rangle_{{\rm ens}_1}|0\rangle_{{\rm ens}_2}|0\rangle_{p_1}|0\rangle_{p_2} + \lambda(|\Psi^+\rangle_{{\rm ens}_1{\rm ens}_2}|1\rangle_{p_1}|0\rangle_{p_2} + |\Psi^-\rangle_{{\rm ens}_1{\rm ens}_2}|0\rangle_{p_1}|1\rangle_{p_2}) + O(\lambda^2)] \quad (6)$$

where $|\Psi^\pm\rangle_{{\rm ens}_1{\rm ens}_2} = [|1\rangle_{{\rm ens}_1}|0\rangle_{{\rm ens}_2} \pm |0\rangle_{{\rm ens}_1}|1\rangle_{{\rm ens}_2}]/\sqrt{2}$ with $1, 2$ labelling the two separate ensembles. Now by detecting a single photon at either detector, we project our ensembles into the entangled state $|\Psi^\pm\rangle_{{\rm ens}_1{\rm ens}_2}$ with probability $\sim |\lambda|^2$ depending on which detector clicked. Further when we include channel and detected losses, our resulting state $\rho = |\Psi^\pm\rangle_{{\rm ens}_1{\rm ens}_2}\langle\Psi^\pm| + O(\lambda^2)$ conditioned on a single photon detection event at either detector occurs with probability $p_{\rm s} \sim |\lambda|^2 e^{-L/2L_0}p_{\rm det}p_{\rm cou}$. As $|\lambda| \ll 1$ and generally $L \gg L_0$, the probability for generating the entangled link is quite small, but with many attempts, an entangled link can be generated. The success probability of this protocol has a better scaling for distance L than those of the three examples in the previous section by $e^{-L/2L_0}$ [33] (but note that two pairs of $|\Psi^\pm\rangle_{{\rm ens}_1{\rm ens}_2}$ are needed for applications [33]).

IV. The Components in Quantum Repeaters

The entanglement distribution schemes described in Section III showed that the probability of success for generating a single entangled link scales exponentially with e^{-L/L_0}. This necessitates the use of quantum repeaters to allow long-distance communication with finite resources and reasonable rates. In a quantum repeater protocol there are three primary operations required to create the long-range Bell state that can be used for quantum communication tasks such as QKD or teleportation. These operations are:

1) Entanglement distribution: the process for creating entangled links between network nodes.
2) Entanglement purification: the process where we create a more highly entangled state from a number of lower quality ones.
3) Entanglement swapping: the process in which a Bell-state measurement is performed within a node on two qubits which are halves of separate Bell states. The Bell measurement allows us to provide a longer entangled link connecting adjacent repeater nodes.

The first operation has already been described in the previous section, but now entanglement is needed only between shorter-range adjacent nodes and thus the success probability for generating the entangled link depends on the distance of the adjacent nodes, rather than the total communication distance. The remaining two operations (entanglement purification and entanglement swapping) need to be considered independently as they can be quite different in nature and the operational details will show us the limitations each has. We will consider entanglement purification next.

A. Quantum Purification

A significant problem with the Bell states one generates from an entanglement distribution scheme between the two remote nodes is that they are not perfect. While losses can be overcome by attempting to generate the entangled links many times, other errors will occur in such systems. The matter qubits are known to experience dephasing even if they are long-lived. Further our state preparation and detection may not be perfect (e.g., we may not measure exactly in the basis of states $|D\rangle$ and $|A\rangle$). Such errors cannot generally be overcome by repetition (which can be taken as a countermeasure against the loss), and instead decrease the quality (fidelity) of the entangled link. If a dephasing error occurs with probability $1-F$, then our resulting state (expressed as a density matrix) is given by

$$\rho = F|\Phi^+\rangle_m\langle\Phi^+| + (1-F)|\Phi^-\rangle_m\langle\Phi^-|, \tag{7}$$

where F serves also as the fidelity of the resulting state. Other types of errors associated with imperfect local operations will further decrease this fidelity, inducing errors corresponding to the other three Bell-state elements. This is likely to lead to a mixture of a Bell state and the maximally mixed state

$$\rho_w = \frac{1-F}{3}\mathrm{I}_4 + \frac{4F-1}{3}|\Phi^+\rangle_m\langle\Phi^+|, \tag{8}$$

which is known as Werner state [58].

The decrease in the fidelity of the entangled link means information present in the state has been lost. Once information has been lost there is not a simple way to recover it. However as we are trying to generate a known Bell state, we can distill from multiple imperfect copies a Bell state with higher fidelity by a process known as quantum purification [10], [42], [44], [59]–[61]. The original purification scheme was proposed by Bennett *et al.* [10] and is depicted in Fig. 3(a). It requires that two copies of the state have already been established between the remote repeater nodes (the two Bell states do not have to be identical in practice, but for simplicity of explanation here we will assume they are). Within each node a CNOT is applied between the qubit of one Bell pair and the qubit for the second Bell pair. The qubits from the second Bell pair are then measured out in the computational basis $\{|g\rangle, |e\rangle\}$. The measurement results are then transmitted over a classical channel between the nodes. The resulting state is only kept if the measurement results were the same (e.g., g, g or e, e). In such a case the purification is successful and a higher-fidelity state should be obtained as long as the initial fidelity of the state was greater than about 50% and our local operations (CNOT and the projective measurement) are accurate enough. If the measurement results were not the same (e.g., g, e or e, g), the purification protocol has failed and one needs to start over again with fresh entangled states. This makes the purification protocol inherently probabilistic in nature, but it is heralded. One knows whether or not it is successful only after the classical measurement results are exchanged between the nodes. This is likely to be significant performance bottleneck.

As an example of purification, let us consider the "recurrence method" protocol. Consider two copies of our Werner state ρ_w shared between Alice and Bob which we represent as $\rho_{w_{1,2}} \otimes \rho_{w_{3,4}}$, where the labels i, j indicate the qubits of that entangled pair. Qubits 1 and 3 are in the left-hand node while 2 and 4 are in the right-hand node. We apply CNOT gates between qubits (1&3) and (2&4) followed by a measurement on qubits (3&4) in the computational basis. The resulting state can be expressed

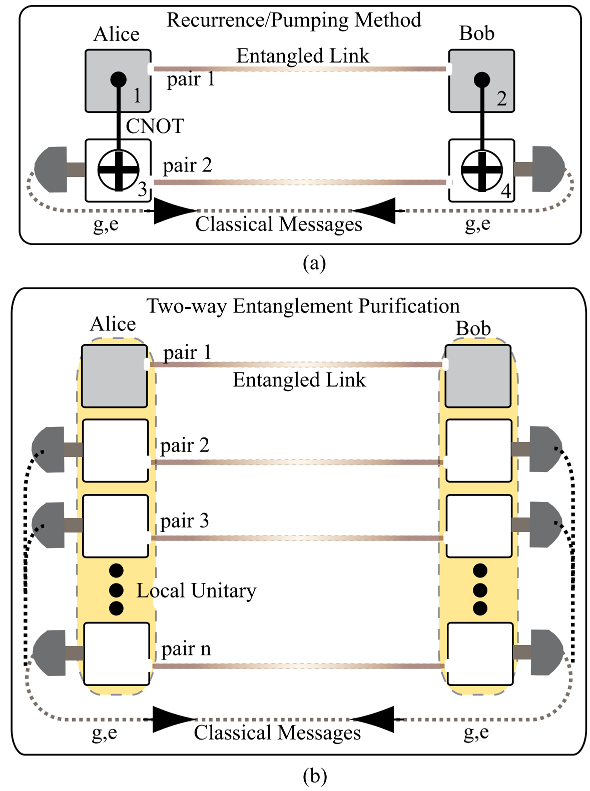

Fig. 3. (a) Schematic illustration of an entanglement purification scheme using two imperfect Bell pairs and local operations including CNOT gates and projective measurements. (b) Schematic illustration of a generalised entanglement purification scheme using n imperfect Bell pairs, local operations and classical communication.

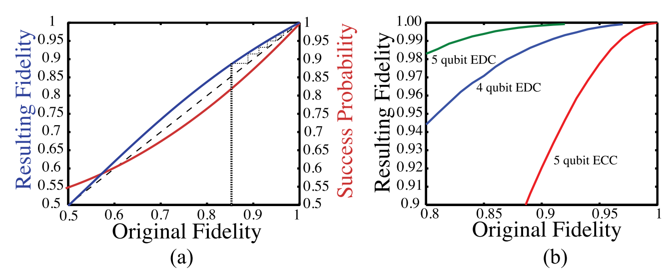

Fig. 4. (a) Plot of the fidelity of the purified Werner state and its probability of success versus its initial fidelity of 2 imperfect Bell pairs. The dotted lines shows the increase in fidelity achievable by performing multiple rounds of purification. (b) Entanglement purification using the 4-qubit and 5-qubit EDC and the 5-qubit error correction code (ECC) [62]. The success probabilities for these protocols can be found in [63] and [64].

as

$$\rho_w = \frac{1-F_p}{3}\mathrm{I}_4 + \frac{4F_p-1}{3}\left|\Phi^+\rangle_m\langle\Phi^+\right|, \tag{9}$$

where the new fidelity of the state is given by [10]

$$F_p = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2} \tag{10}$$

with the probability of the successful purification's heralded operation being $P = F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2$. These two quantities are plotted in Fig. 4(a) for two initial Werner states with fidelity F.

What can be clearly seen is that it takes many rounds of purification to obtain a Werner state with fidelity above 99% when one starts with low fidelity pairs (e.g., $F = 85\%$). In the original protocol, for simplicity, extra depolarisation to convert the resulting state to the Werner form is assumed, but the protocol works without such depolarisation [59] giving better performance.

The examples we have illustrated above have assumed that the Bell pairs used in the purification have the same fidelity. This may be rather demanding on resources since at every purification step we require two identical states resulting from the previous successful purification round and the total number of initial Bell pairs required will grow exponentially with the number of purification steps. This constraint can be relaxed and many of the purification protocols will work even if the pairs are not identical [27], [43]. In such a case, one may not be able to generate an arbitrarily high fidelity Bell state. However the pairs one has obtained may be good enough. A scheme which uses non-identical pairs is known as entanglement pumping [27]. Consider that we already have an original Werner state with fidelity F_1 and that our second pair coming directly from the entanglement distribution is a Werner state with fidelity F. After successful purification our state has a fidelity (11), as shown bottom of the page. This can be iterated a number of times to achieve to pump our original F_1 pair to even higher fidelities. But it is generally not possible to obtain a maximally entangled state with arbitrary small error, because there exists a fixed point beyond which no improvement is possible, depending on the fidelity F. If the purification fails during any step the entire process must start again from new pairs with fidelity F_1.

There is also no reason one has to be restricted to the recurrence method and the entanglement pumping that are examples of the two-way error-detection codes (EDC) (which succeed only in a probabilistic way). Instead one can use one-way quantum EDC or quantum error correction codes (ECC) [42], [44], [63], [64] which we schematically illustrate in Fig. 3(b). These use multiple pairs (rather than 2) at the same time and EDC in principle increase the fidelities much faster [63], [64] if the initial entangled pairs have a high fidelity. This is shown in Fig. 4(b) using the 4-qubit and 5-qubit EDC's as well as the 5 qubit ECC [64], [74]. For instance, the 5 qubit EDC can purify 5 imperfect pairs with a fidelity of 0.85 into one with a fidelity above 99% in a single round with a success probability of 0.44. Significantly more resources and communication time are required if one uses the recurrence method or the entanglement pumping (see Fig 3(a)).

Finally the schemes we have detailed here so far have assumed perfect local operations (CNOT gates and measurements). In any realistic system this will not be perfect and their effect can be twofold: heralded errors (e.g., when probabilistic gates fail) and unheralded ones (e.g., measurements error, imperfect gates etc.). In the first case, this is just like the purification failed and we need to start again. For the second case, we do not know whether the error occurred and thus the fidelity of our Bell state will be limited.

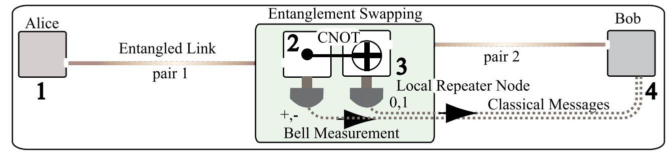

Fig. 5. Schematic illustration of an entanglement swapping scheme using a local Bell measurement. The Bell-state measurement can be performed using a CNOT gate operation between qubits 2 and 3 (2 as the control and 3 as the target) followed by measurements on those qubits (qubit 3 in the basis $\{|0\rangle, |1\rangle\}$ and qubit 2 in the basis $\{|+\rangle, |-\rangle\}$ with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$). A correction information is then sent to Bob.

B. Entanglement Swapping

Given that we now have a mechanism to establish high-fidelity pairs between adjacent repeater nodes (e.g., entanglement distribution followed by purification), we now need a mechanism to extend the range of the entanglement. This can be achieved with an operation known as entanglement swapping [27], [28], [38]—an operation that is effectively a Bell-state measurement on a node that is linked to neighbouring nodes with entangled links (see Fig. 5). Consider that we have two pairs in the form $|\Phi^+\rangle_{m_{12}} \otimes |\Phi^+\rangle_{m_{34}}$, where the labels 1, 2, 3, 4 indicate the locations of the qubits. Performing a Bell-state measurement between qubits 2 and 3 projects qubits 1 and 4 into the state $|\Phi^+\rangle_{m_{14}}$ up to a Pauli correction operation $\{I, Z, X, ZX\}$ depending on the Bell measurement result. The result of the measurement needs to be sent to qubit 4 (or qubit 1 but not both) so the correction operation can be performed. Further the message heralds the success or failure of the swapping operation if necessary.

The previous example used ideal Bell states in the entanglement swapping protocol. However because of channel noise and imperfection of local devices, we will instead have mixed states. Modelling these as a Werner state ρ_w with fidelity F, the resulting state after the Bell-state measurement (and correction operations) is also a Werner state $\rho_{w_{14}}(F')$ with $F' = F^2 + (1-F)^2/3$. This fidelity is depicted in Fig. 6 and clearly shows that the fidelity of the longer-range state has decreased compared with the fidelity of the two initial entangled links. In fact, with a good approximation $F' = F^2$ for $F \sim 1$, if one is performing entanglement swapping on multiple links (say n links), the resulting fidelity will drop by $F' = F^n$. This means purification will need to be performed on longer-range links.

C. Entanglement Swapping in the DLCZ Scheme

Previously we have shown in Section III-A how entanglement distribution can be achieved using the DLCZ approach. How-

$$F_2 = \frac{F_1 F + \frac{1}{9}(1-F_1)(1-F)}{F_1 F + \frac{1}{3}F_1(1-F) + \frac{1}{3}F(1-F_1) + \frac{5}{9}(1-F_1)(1-F)} \tag{11}$$

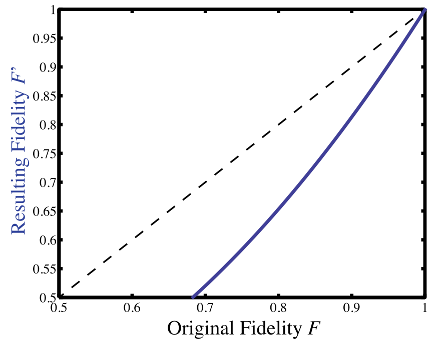

Fig. 6. Plot of the fidelity F' of the Werner state after one round of entanglement swapping versus its initial fidelity F. The dashed curve is the $F' = F$ line.

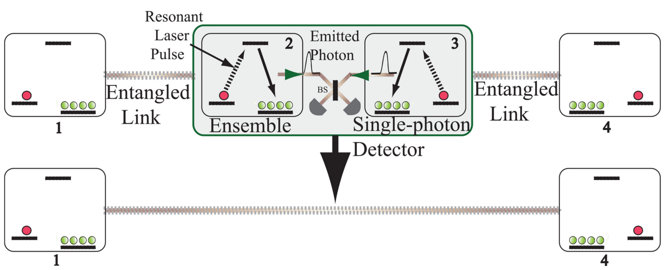

Fig. 7. Schematic illustration of the DLCZ entanglement swapping scheme based on single-photon emission from the collective mode of the ensembles and a linear-optical Bell-state measurement [33]. The single photons are emitted using resonant laser pulses.

ever there is no simple and direct way to achieve our Bell-state measurement (or CNOT gate) between the qubits encoded into the ensembles. Fortunately, we can transform the atomic excitation into a photonic one coherently and thus can in principle use it to perform a probabilistic (but heralded) linear-optical Bell-state measurement (see Fig. 7). This is achieved as follows: By exciting with a resonant laser pulse the $|g_2\rangle \leftrightarrow |e\rangle$ transition to take the photonic excitation stored in the one half of the entangled ensembles, we convert it to a photon. In this case we have

$$|\Psi^+\rangle_{\mathrm{ens}_1\mathrm{ens}_2} \rightarrow \frac{1}{\sqrt{2}}[|1\rangle_{\mathrm{ens}_1}|0\rangle_{p_1} + |0\rangle_{\mathrm{ens}_1}|1\rangle_{p_1}]|0\rangle_{\mathrm{ens}_2}, \quad (12)$$

where our entanglement is now between the first ensemble and the photon emitted from the second one. Now using this process, in Fig. 7 the central node obtains two optical modes emitted by two ensembles. Making these photons interfere with a 50/50 beamsplitter we have

$$\begin{aligned}|\Psi\rangle = &\frac{1}{2}|1\rangle_{\mathrm{ens}_1}|1\rangle_{\mathrm{ens}_4}|0\rangle_{p_2}|0\rangle_{p_3}\\ &+ \frac{1}{2\sqrt{2}}\left[|1\rangle_{\mathrm{ens}_1}|0\rangle_{\mathrm{ens}_4} + |0\rangle_{\mathrm{ens}_1}|1\rangle_{\mathrm{ens}_4}\right]|1\rangle_{p_2}|0\rangle_{p_3}\\ &+ \frac{1}{2\sqrt{2}}\left[|1\rangle_{\mathrm{ens}_1}|0\rangle_{\mathrm{ens}_4} - |0\rangle_{\mathrm{ens}_1}|1\rangle_{\mathrm{ens}_4}\right]|0\rangle_{p_2}|1\rangle_{p_3}\\ &+ \frac{1}{2\sqrt{2}}|0\rangle_{\mathrm{ens}_1}|0\rangle_{\mathrm{ens}_4}\left[|2\rangle_{p_2}|0\rangle_{p_3} - |0\rangle_{p_2}|2\rangle_{p_3}\right] \quad (13)\end{aligned}$$

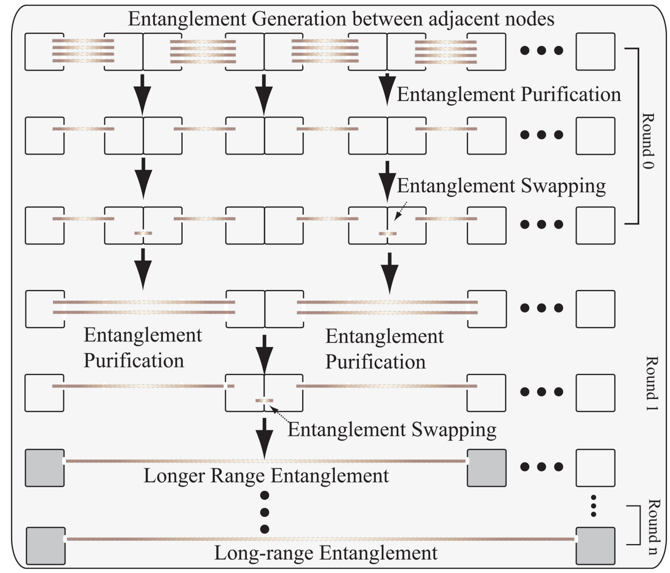

Fig. 8. Quantum repeater scheme for generating long-range entanglement. It begins by splitting the network into a number of segments and placing repeater stations at these nodes. Multiple entangled pairs are then generated between adjacent nodes. These links are then purified and entanglement swapping is performed to create a link twice as long as the original one. These new links are then purified and entanglement swapping is performed again to create a link four times as long. This continues until entanglement is generated between the end repeater nodes (Alice and Bob).

and hence by measuring a single photon (with a probability of $p_{\mathrm{det}}p_{\mathrm{cou}}[2 - p_{\mathrm{det}}p_{\mathrm{cou}}]/4$) at either detector, the two remote ensembles are projected into either entangled state $\frac{1}{2-p_{\mathrm{det}}p_{\mathrm{cou}}}|\Psi^\pm\rangle_{\mathrm{ens}_1\mathrm{ens}_4}\langle\Psi^\pm| + \frac{1-p_{\mathrm{det}}p_{\mathrm{cou}}}{2-p_{\mathrm{det}}p_{\mathrm{cou}}}|0\rangle_{\mathrm{ens}_1}|0\rangle_{\mathrm{ens}_4}\langle 0|_{\mathrm{ens}_1}\langle 0|_{\mathrm{ens}_4}$ depending on which detector clicked. For near unity coupling and detection efficiency our state is thus $\sim |\Psi^\pm\rangle_{\mathrm{ens}_1\mathrm{ens}_4}$. As this entanglement swapping operation is probabilistic in nature, a classical message needs to be sent to the nodes containing ensembles 1 and 4 indicating whether it succeeded or not. In the case of failure, we must start over again from the entanglement distribution step.

V. Quantum Repeater: First Generation

Now that we have described the fundamental components needed for quantum repeaters, it is insightful to illustrate how they are combined together (see Fig. 8) and the quantum repeaters perform. Let us consider this in general before moving to specific approaches. Our task begins by the creation of a number of entangled links between adjacent repeater nodes. Once enough links have been generated entanglement purification is performed if necessary (either once or a number of times) to give the required high-fidelity link. Then two neighbouring high-fidelity links are then connected by the entanglement swapping protocol to give a link twice as long as the original one (this finishes round 0). Round 1 begins with purification of the entanglement at this longer range, followed by entanglement swapping to create even longer links (this step is likely to involve round 0 & 1 being done again). This continues until one generates the entanglement one requires between the Alice and Bob's nodes with the required fidelity. If the purification or entanglement swapping fails at any step, we must start over that part again from round 0.

A. Performance With Classical Losses Alone

While the quantum repeater protocol for generating long-range entanglement may seem quite straightforward in nature, its behaviour is quite complex due to the various probabilistic elements inherent in the scheme. It is hence insightful to examine the performance of these repeater networks by initially restricting our attention to the DLCZ protocol. The DLCZ protocol can overcome the effect of the photon loss with the use of atomic-ensemble quantum memories. The protocol has a feature that it does not explicitly use entanglement purification, i.e., it is composed only of entanglement generation and swapping. Under the assumption that photon losses are the only sources of error the required time to successfully generate a Bell state $|\Psi^+\rangle_{AB}$ for a network of total distance $L_{\rm tot}$ divided in 2^n segments is estimated [26] to be

$$T_{\rm tot} = \frac{L_{\rm tot}}{2^n c}\frac{f_0}{P_0}\frac{f_1}{P_1}\cdots\frac{f_n}{P_n}\frac{1}{P_s}. \tag{14}$$

Here, $L_{\rm tot}/(2^n cP_0)$ is the time associated with an attempt to create an entangled link between adjacent repeater nodes (each of which has two memories) with success probability P_0. These two parts give the average time for generating a successful link between the adjacent nodes. The terms P_i are the probability for the entanglement swapping to be successful at the ith round while the terms f_i takes into account that for the entanglement swapping to occur, one requires two neighbouring links. If the average time to generate one link is T, then one on average only needs to wait $T/2$ for the success in the second link [26] and so $f_i \sim 3/2$ is a good approximation. Finally P_s is the successful post-selection probability at the end. As mentioned above, if our only errors are associated with channel losses, then with $|\lambda| \ll 1$,

$$\begin{aligned} T_{\rm tot} &\sim \left(\frac{3}{2p_{\rm det}p_{\rm cou}}\right)^{n+1}\frac{L_{\rm tot}}{c|\lambda|^2 e^{-L/(2L_0)}} \\ &\sim O(L_{\rm tot}e^{L_{\rm tot}/(2^{n+1}L_0)}), \end{aligned} \tag{15}$$

which is the polynomial scaling with $L_{\rm tot}$ (remembering $L = L_{\rm tot}/2^n$ is just the distance between adjacent nodes).

It is very important now to contrast this with the situation of not using the repeater approach at all, but instead just using the entanglement distribution scheme over the total distance $L_{\rm tot}$. In this case the average time to generate the entangled link is

$$T_{\rm tot} \sim \frac{L_{\rm tot}e^{L_{\rm tot}/2L_0}}{c|\lambda|^2 p_{\rm det}p_{\rm cou}}, \tag{16}$$

which is scaling exponentially with $L_{\rm tot}$ compared with polynomial in $L_{\rm tot}$ for the basic repeater scheme above.

B. Performance With Finite-Coherence-Time Quantum Memories

Our simple example above showed how the basic time to generate an entangled link between Alice and Bob could scale polynomially with $L_{\rm tot}$. This was unfortunately a highly idealised situation and we have to include other imperfections both in entanglement distribution and entanglement swapping steps. Imperfection in entanglement distribution for instance will result in a mixed state with fidelity $F < 1$. As we have 2^n links, the fidelity of the resulting entangled link between Alice and Bob could scale as $F^{2^n} = F^{L_{\rm tot}/L}$ and thus decrease exponentially as $L_{\rm tot}$ increases. This loss in fidelity must be recovered and hence a form of purification is necessary. Purification is a natural solution but is highly non-ideal: First we need to generate multiple entangled links between repeater nodes and second our generation time could scale as $O(L_{\rm tot}/c)$ rather than $O(L/c)$. The reason is that if purification is performed between Alice and Bob's nodes (or some fixed factor of the distance between them), which is actually required in the nested purification protocol [27], then the time to generate the entangled links scale as multiples of the round-trip time over the end-to-end path due to the classical signalling required to herald the purification successful operation. However, practical matter qubits (quantum memories in effect) [65] usually degrade exponentially with this round-trip communication time, i.e., again exponentially with $L_{\rm tot}/c$. In fact, most quantum memories lose coherence with time due to dephasing which we can represent by the fidelity to a Bell state,

$$F_{\rm dephasing} = \frac{1 + \exp\left[-2t/T_2\right]}{2}, \tag{17}$$

where t is the time from the qubits initialisation and T_2 is the dephasing time of the memory. Therefore, if our signalling time is scaling at $O(L_{\rm tot}/c)$, then the loss in fidelity due to dephasing will be exponential in nature unless T_2 also scales with $L_{\rm tot}$.

A similar argument holds even for the case of the use of probabilistic entanglement swapping as in the DLCZ protocol. In fact, if the entanglement swapping works only probabilistically, the time for the classical signalling required to herald the successful entanglement swapping scales as $L_{\rm tot}/c$ [66]. Therefore, even in this case, due to the dephasing, the loss in fidelity will be exponential with the communication distance $L_{\rm tot}$. It thus seems that we need to change the repeater protocols a little [65] or else an exponential scaling reappears in repeater schemes.

VI. Quantum Repeater: Second Generation

As previously mentioned, conventional two-way messaging needed by probabilistic entanglement purification/swapping creates a significant performance bottleneck, due to having to wait for the classical signals (indicating whether the purification/swapping operation was successful or not) to propagate between the two involved nodes. Moreover, it could cause a worse problem regarding the scaling of the communication resources if we consider the finite coherence time of practical matter qubits. A simple way for overcoming these difficulties is to replace the probabilistic operations with deterministic ones. For instance, as for the entanglement swapping, we could assume the use of a deterministic Bell measurement for matter qubits, because there actually exist various matter qubits that allow a 2-qubit gate to be performed faithfully and efficiently. To overcome the difficulty on entanglement purification, we

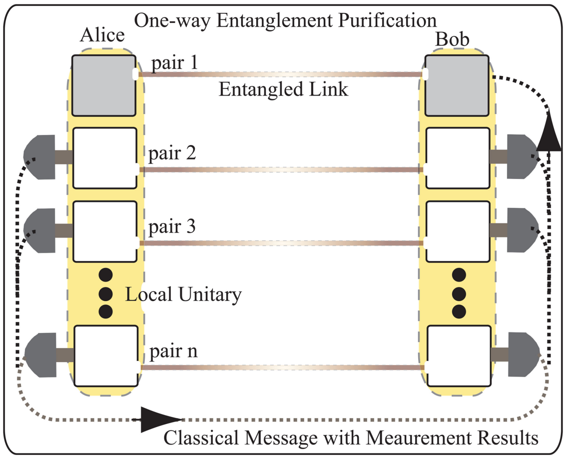

Fig. 9. Schematic illustration of an entanglement purification scheme using error correction codes on n imperfect pre-established Bell pairs. On the left-hand side node, we perform the circuit for the error-correction encoding on the n qubits and measure all but the first qubit in the appropriate basis. At the same time (not necessary however) the right-hand side node performs the decoding circuit and measures its appropriate qubits. As soon as the measurements are complete Alice and Bob's qubits are now available for use (as this purification is deterministic). The classical signal from Alice to Bob just carries Alice's measurement result allowing Bob to interpret which Bell state has been generated and the correction operation (either a bit flip or sign flip) to get $|\Psi^+\rangle$. In many cases this correction is classically tracked in the Pauli frame (the Pauli frame indicates whether an X, Z or both corrections need to be performed at some time [67]). We should also note that it is not necessary to measure out all but one of the qubits involved in the entangled links. Instead the logical qubit can be maintained by the use of ancilla qubits within that node with the syndrome being measured with the help of the ancilla qubits. Entanglement swapping could then be performed on the logical qubits enabling a much more error resilient system.

need to move to one-way schemes where no classical signals are needed to indicate whether the schemes succeed or not. We could use error correction codes to perform such purification [42], [44], [63], [64], [75], as shown in Fig. 9. The use of error correction does however put significant constraints on the quality of entangled links that can be used. In Fig. 4 we plotted the resulting fidelity for purification using the 5 qubit error correction code [64] assuming perfect local gates. For initial fidelities $F > 0.88$ a net increase in the fidelity is seen after purification, but for $F < 0.88$ the resulting purified entangled state decreases in fidelity. Thus for a particular error correction code there is a minimum fidelity of the required entangled links. This is a significant constraint. However its advantage is that we do not need to wait for the classical messaging between the nodes before the qubits in the entangled links can be used again. This in turn has a major impact on the lifetimes required for the quantum memories. In fact, they only need to be good enough compared to the time required to generate the adjacent entangled links and not multiples of the signalling time between the end nodes of the network.

With error correction, as well as deterministic 2-qubit gates for the deterministic entanglement swapping, enabling the coherence times of our quantum memories to scale only with time scales associated with the signalling time between adjacent repeater nodes, we need to return to the generation of these primitive entangled links and determine how we can minimise the time associated with these. As discussed in Section III, the creation of an entangled link between nodes is inherently

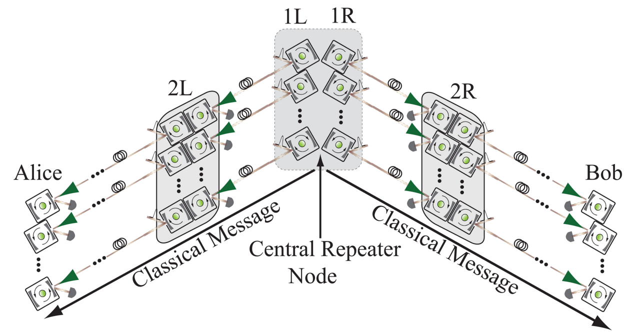

Fig. 10. Schematic illustration of the arrangement of a quantum repeater protocol in a butterfly design that reduces the requirements on all the quantum memories to those associated with the round trip between adjacent repeater nodes rather than the round trip over the entire network.

probabilistic in nature due to the effect of loss. With a success probability p_{s} (scaling as $\exp[-L/L_0]$), we need to perform [44]

$$m = \frac{\log_e \epsilon}{\log_e (1 - p_{\mathrm{s}})} \sim -\frac{\log_e \epsilon}{p_{\mathrm{s}}} \tag{18}$$

trials to generate a single link with maximum failure rate ϵ (typically $\epsilon \leq 10^{-2}$). To minimise the time to generate the links (and hence the memory times) they should be done in a parallel fashion using multiplexing [44].

With a mechanism to deterministically generate an entangled link in a single round trip time (the time for the single photon to propagate between adjacent nodes and a return classical message heralding success) with the multiplexing and using error correction for purification, we can now design a repeater scheme where the memory storage times are kept to a minimum. We depict one potential arrangement in Fig. 10 based on a butterfly design [44]. The generation of the entangled link between Alice and Bob begins by the central node (1L-1R) establishing links to both the left-hand 2L and the right-hand 2R adjacent nodes. Once the entangled links (1L-2L, 1R-2R) have been established (at least as far as the adjacent nodes know), the adjacent nodes (2L, 2R) can then establish entanglement to their next neighbour (3L, 3R). At the same time a classical message from these nodes is sent back to the node that established the entanglement with it. The central node now knows that it has entanglement to both its left and right adjacent nodes. On the links to the left hand adjacent node 2L, the error correction encoding circuit can be performed including the measurement. A similar operation can be performed on the qubits associated with links to the right hand adjacent node (2R). Entanglement swapping is then performed between the pairs of the remaining qubits - one associated with the links to the left (1L) and the other to the right (1R). The classical messages with the error correction results are then shipped along the channel to Alice and Bob (which ever is closer) as well as the results from the entanglement swapping. An error corrected link has thus been created between non-adjacent nodes and the qubits in the central node are free to initiate a new entangled link. They have only been in use for the round-trip time associated with sending signals to the adjacent nodes. This in turns means those qubits only require a coherence time long enough compared to $T \sim L/c$ rather than $T \sim L_{\mathrm{tot}}/c$

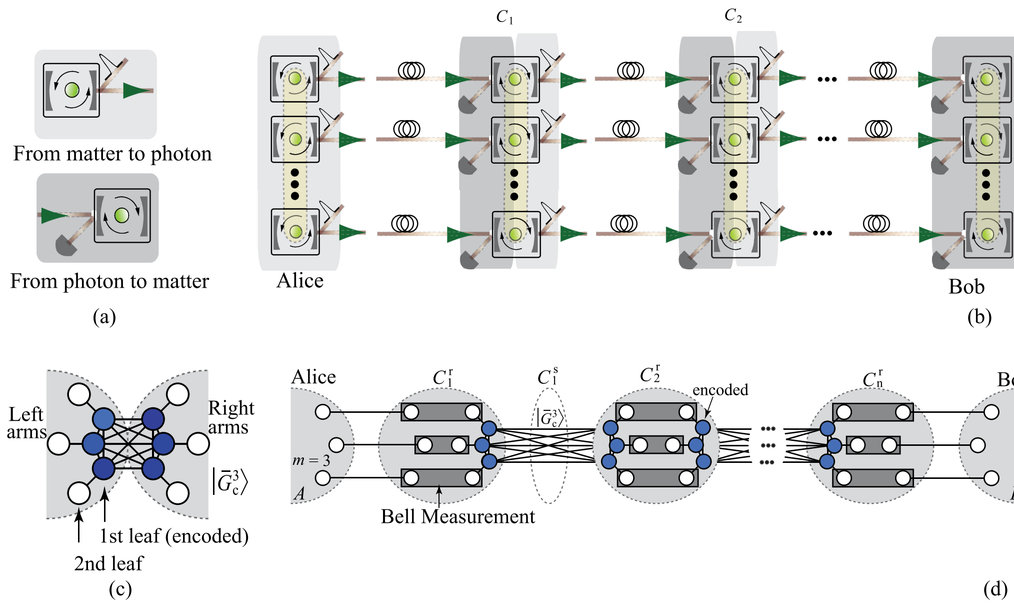

Fig. 11. Third Generation quantum repeaters. (a) Schematic illustrations showing the transfer of quantum information between a single photon and a matter qubit, with detection heralding loss events. (b) shows the basic protocol transferring quantum information from Alice to Bob. It begins first with Alice preparing matter qubits in an encoded qubit state based on a redundant quantum parity code [57]. She transfers the encoded qubit state of matter qubits into photons, using the transfer mechanism of (a), and sends the photons to adjacent node C_1. On receiving the photons, adjacent node C_i $(i = 1, \ldots, n)$ transfers the state of photons into matter qubits, again using the mechanism of (a) where the photon detectors announce which photons are lost. Then the matter qubits perform error-correcting operations followed by re-encoding. The encoded qubit state is again transferred into freshly prepared photons, with the mechanism of (a). The node C_i sends the photons into the adjacent node C_{i+1}. These steps are repeated until Bob receives the photons and performs the error correction operations. In (c) and (d) an all photonic quantum repeater is illustrated, which works without the need for matter qubits at all. The basic component shown in (c) is a cluster state $|G_c^m\rangle$ that has m left and right arms, each of which is composed of 1st-leaf encoded qubit and 2nd-leaf qubit. An edge represents the past application of the controlled-phase gate to qubits in $|D\rangle$ [67]. In (d) we illustrate how the cluster states can be used in the repeater protocol. It begins with Alice (Bob) sending m single photons entangled with her (his) local qubits to the adjacent receiver node C_1^r (C_{n+1}^r). Every source node C_i^s prepares $|\bar{G}_c^m\rangle$, and the left (right) arms are sent to the left-hand (right-hand) adjacent receiver node C_i^r (C_{i+1}^r). Now on receiving the single photons, C_i^r performs linear-optics-based Bell measurements [68] on the m pairs of the 2nd-leaf qubits of the left and right arms. If the Bell measurement succeeds, C_i^r applies the X-basis measurements to the 1st-leaf qubits on the successful arms while performing Z-basis measurements on all the other 1st-leaf qubits. However if all the m Bell measurements or one of the measurements on the 1st-leaf qubits fails, the receiver node considers that this trial fails. The receiver nodes announce all the measurement outcomes to Alice and Bob, and the protocol succeeds in which no receiver node judges this trial as failure.

for the first generation schemes (remembering $L_{\rm tot} = L \times 2^n$). The approach also increases the rate at which end to end Bell pairs can be generated between Alice and Bob. For this butterfly approach with $L \sim 40$ km, a rate of nearly 5 kHz [44] could be achieved over 1000 km compared with 1 Hz in first generation schemes. This raises an interesting question about whether or not we have reached a fundamental performance limit given a certain node separation.

VII. Quantum Repeater: Third Generation

As we saw in the previous section, the second generation repeater schemes are ultimately limited in their performance by the requirement that a classical message needs to be sent to herald the successful entanglement distribution operation between adjacent nodes. While this message is being sent the qubits in those nodes are not available for further processing. If we could remove such messaging, then we would significantly improve the performance of the repeater network.

To remove the return classical messaging we need to encode our quantum signal to be sent between the repeater nodes so that it is tolerant to loss [57], [69]–[71]. In this case, we could send our quantum information encoded in matter qubits into photons equipped with a loss-tolerant code [57], send over the channel to the neighbouring repeater node where the information is transferred to matter qubits [see Fig. 11(a)] and loss events heralded. Error correction is then performed and the information encoded back to the full loss-tolerant code. It is then transferred back to photons and sent to the next adjacent node [see Fig. 11(b)]. This continues until Bob receives the quantum message. It is important to mention that loss-tolerant codes only tolerate loss less than 50%, but this is enough to allow repeater nodes to be spaced further apart than conventionally thought (50% loss corresponds to $\sim$15 km travel for a single photon being transmitted over conventional telecom fiber). Next in the scheme of [57] the repeater nodes are only used for refreshing the loss-tolerant code, and so the matter qubits at that nodes are *no longer* required to be long-lived quantum memories. As all the components of the repeater system just transmit quantum information from the sender to the receiver, the repetition rate is now just determined by that of the slowest one. Further this protocol by Munro *et al.* was generalised by Muralidharan *et al.* [71] to be fully fault tolerant, meaning communication is possible over arbitrarily long distances.

As implied above, to achieve polynomial-scaling quantum repeaters with matter qubits, the matter qubits should effectively

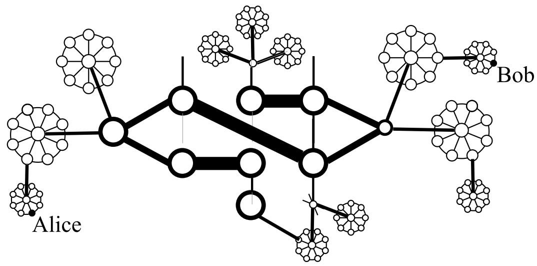

Fig. 12. Schematic illustration of an arbitrary quantum network (or a connected set of networks—a quantum internet) where Alice and Bob want to communicate over a complex topology network where they do not know the exact route between them. The thicker the connecting lines between the nodes are, the more capacity those links have. Such capacity can be achieved by having more resources available at those nodes.

satisfy all Divincenzo's criteria [72]. On the other hand, most matter quantum memories to be used in quantum repeaters can be transformed [26], [73] into a single-photon source. Hence, matter qubits may be too demanding to accomplish quantum repeaters, and thus, it is fundamental to consider whether quantum repeaters are possible without any matter qubit, i.e., in an all optical way with single-photon sources, detectors, linear optical elements, and local active feedforward techniques alone. Recently Azuma *et al.* [70] developed all optical quantum repeaters by taking a time reversal of the DLCZ-like quantum repeater protocol. The time reversal means that in a synchronised fashion, every "source" repeater node first generates a photonic complete-like cluster state to simulate the entanglement swapping, and then performs the entanglement generation by sending the halves of the cluster state to the adjacent "receiver" repeater nodes. This is followed by *adaptive* Z-basis or X-basis measurements at receiver repeater nodes to complete the entanglement swapping (see Fig. 11(d). It is important to emphasise here that all these steps, including the preparation of the cluster state, can be accomplished with the optical devices alone, and no matter based quantum memory is needed. Further as this protocol is the time reversal of a quantum repeater scheme with polynomial scaling, its required resources increase just polynomially with the communication distance. In addition, the repetition rate of the protocol is limited by the local operations within the repeaters and thus a high rate is possible, similar to Munro *et al.* protocol [57].

VIII. Networks

Our considerations so far have been about sending quantum information between Alice and Bob down a linear network. In reality, Alice and Bob are likely to be members of a complex quantum network where they may not even know the exact topology of the network (see Fig. 12 for instance). If one needs to establish entanglement between all the repeater nodes on the route between Alice and Bob at the same time, then Alice and Bob will need to map out the topology of the required part of the network they need. However if one is directly transmitting the quantum information, then a telephone (or internet) exchange like approach can be used and routing around broken nodes can be easily achieved. Alice would need to know Bob's quantum telephone (internet) number but not the exact route. Alice would forward her message to a local exchange who could forward it to region exchange etc who in turn will get it to Bob. This kind of quantum telephone exchange model is ideal for the third generation repeater approaches as the transmission of the quantum information in encoded form is naturally suited to being routed.

IX. Concluding Discussion

The development of quantum technologies is likely to enable abilities for the processing of information that far exceed what we can do today. Quantum communication is going to be at the core of these developments—especially if a quantum enabled internet is to arise. To enable such developments—whether for the secure distribution of classical key material, teleporting quantum states, or a fully distributed quantum computer we need to be able to send quantum based information over long distances. This will necessitate the development of quantum repeaters to overcome losses associated with the use of optical fibres. In this review, we have outlined the developments of quantum repeaters highlighting the core components required. Such components include schemes to distribute entanglement between adjacent nodes, schemes to take several imperfect Bell pairs shared between two repeater nodes and purify them to one of higher quality and schemes to perform entanglement swapping to allow the range of entanglement to be extended.

We show how the first generation of repeaters will only enable entanglement links to be generated between Alice and Bob with a rate that scales as multiples of the time for classical signalling to be communicated between these end points. We have then shown how to improve this scaling to the signalling time between adjacent nodes when purification is performed using error correction techniques. This significantly reduces the coherence requirements of the quantum memories within every repeater node at the expense of requiring better gates within the nodes. Furthermore, we then show an approach where quantum memories can be removed all together and where the communication rate is now limited by the time to perform the local operations within the repeater nodes, rather than any time associated with signalling between nodes.

Acknowledgment

The author would like to thank G. Knee for helpful discussions. This research is in part executed under the Project UQCC by the National Institute of Information and Communications Technology (NICT).

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge, U.K.: Cambridge Univ. Press, 2000.
[2] T. P. Spiller and W. J. Munro, "Towards a quantum information technology industry," *J. Phys., Condens. Matter*, vol. 18, pp. V1–V10, 2006.
[3] J. P. Dowling and G. J. Milburn. (2002). Quantum technology: The second quantum revolution. [Online]. Available: http://arxiv.org/abs/quant-ph/0206091
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.
[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Sci. Stat. Comput.*, vol. 26, pp. 1484–1509, 1997.

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

[7] C. M. Caves, "Quantum limits on noise in linear amplifiers," *Phys. Rev. D*, vol. 26, p. 1817, 1982.

[8] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced measurements: Beating the standard quantum limit," *Science*, vol. 306, pp. 1330–1336, 2004.

[9] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Bangalore, India, 1984, pp. 175–179.

[10] C. H. Bennett *et al.*, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, pp. 722–726, 1996.

[11] S. Enk, J. I. Cirac, and P. Zoller, "Photonic channels for quantum communication," *Science*, vol. 279, pp. 205–208, 1998.

[12] N. Gisin and R. Thew, "Quantum communication," *Nature Photon.*, vol. 1, pp. 165–171, 2007.

[13] D. Deutsch, "Quantum-theory, the church-turing principle and the universal quantum computer," *Proc. Roy. Soc. London A*, vol. 400, pp. 97–117, 1985.

[14] S. Lloyd, "Universal quantum simulators," *Science*, vol. 273, pp. 1073–1078, 1996.

[15] T. D. Ladd *et al.*, "Quantum Comput.," *Nature*, vol. 464, pp. 45–53, 2010.

[16] [Online]. Available: http://www.idquantique.com/, [Online]. Available: http://magiqtech.com, [Online]. Available: http://quintessencelabs.com/, [Online]. Available: http://www.sequrenet.com

[17] L. K. Grover. (1997). Quantum telecomputation. [Online]. Available: http://arXiv.org/quant-ph/9704012

[18] J. I. Cirac, A. Ekert, S. Huelga, and C. Macchiavello, "Distributed quantum computation over noisy channels," *Phys. Rev. A*, vol. 59, p. 4249, 1999.

[19] R. Van Meter, W. Munro, K. Nemoto, and K. Itoh, "Arithmetic on a distributed-memory quantum multicomputer," *ACM J. Emerging Technol. Comput. Syst.*, vol. 3, pp. 2–23, 2009.

[20] Will Knight, Quantum cryptography network gets wireless link, New Scientist, Jun. 7, 2005.

[21] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, pp. 075001-1–075001-37 2009.

[22] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Exp.*, vol. 19, pp. 10387–10409, 2011.

[23] I. Gerhardt *et al.*, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Commun.*, vol. 2, pp. 1895–1899, 2011.

[24] C. H. Bennett *et al.*, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, p. 1895, 1993.

[25] R. Cleve, D. Gottesman, and H. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, p. 648, 1999.

[26] N. Sangouard, C. Simon, N. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, pp. 33–80, 2011.

[27] 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, pp. 5932–5935, 1998.

[28] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "Event-ready-detectors—Bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, p. 4287, 1993.

[29] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, p. 661, 1991.

[30] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, p. 557, 1992.

[31] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, p. 441, 2000.

[32] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Phys. Rev. A*, vol. 59, pp. 169–181, 1999.

[33] 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, pp. 413–418, 2001.

[34] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, "Fault-tolerant quantum communication based on solid-state photon emitters," *Phys. Rev. Lett.*, vol. 96, p. 070504, 2006.

[35] P. Van Loock *et al.*, "Hybrid quantum repeater using bright coherent light," *Phys. Rev. Lett.*, vol. 96, p. 240501, 2006.

[36] B. Zhao *et al.*, "Robust creation of entanglement between remote memory qubits," *Phys. Rev. Lett.*, vol. 98, p. 240502, 2007.

[37] Z. Yuan *et al.*, "Experimental demonstration of a BDCZ quantum repeater node," *Nature*, vol. 454, pp. 1098–1101, 2008.

[38] A. M. Goebel *et al.*, "Multistage Entanglement Swapping," *Phys. Rev. Lett.*, vol. 101, p. 080403, 2008.

[39] C. Simon *et al.*, "Quantum repeaters with photon pair sources and multimode memories," *Phys. Rev. Lett.*, vol. 98, p. 190503, 2007.

[40] N. Sangouard, R. Dubessy, and C. Simon, "Quantum repeaters based on single trapped ions," *Phys. Rev. A*, vol. 79, p. 042340, 2009.

[41] W. J. Munro, R. Van Meter, S. G. R. Louis, and K. Nemoto, "High-bandwidth hybrid quantum repeater," *Phys. Rev. Lett.*, vol. 101, p. 040502, 2008.

[42] L. Jiang *et al.*, "Quantum repeater with encoding," *Phys. Rev. A*, vol. 79, p. 032325, 2009.

[43] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto, "System design for a long-line quantum repeater," *IEEE/ACM Trans. Netw.*, vol. 17, no. 3, pp. 1002–1013, Jun. 2009.

[44] W. J. Munro *et al.*, "From quantum multiplexing to high-performance quantum networking," *Nature Photon.* vol. 4, pp. 792–796, 2010.

[45] A. Stute *et al.*, "Quantum-state transfer from an ion to a photon," *Nature Photon.*, vol. 7, pp. 219–222, 2013.

[46] J. Volz, R. Gehr, G. Dubois, J. Est-ve, and J. Reichel, "Measurement of the internal state of a single atom without energy exchange," *Nature*, vol. 475, pp. 210–213, 2011.

[47] K. De Greve *et al.*, "Quantum-dot spin-photon entanglement via frequency downconversion to telecom wave-length," *Nature*, vol. 491, pp. 421–425, 2012.

[48] W. B. Gao, P. Fallahi, E. Togan, J. Miguel-Sanchez, and A. Imamoglu, "Observation of entanglement between a quantum dot spin and a single photon," *Nature*, vol. 491, p. 426, 2012.

[49] J. R. Schaibley *et al.*, "Demonstration of quantum entanglement between a single electron spin confined to an InAs quantum dot and a photon," *Phys. Rev. Lett.*, vol. 110, p. 167401, 2013.

[50] E. Waks and J. Vuckovic, "Dipole induced transparency in drop-filter cavity-waveguide systems," *Phys. Rev. Lett.*, vol. 96, p. 153601, 2006.

[51] C. Y. Hu, A. Young, J. L. O'Brien, W. J. Munro, and J. G. Rarity, "Giant optical faraday rotation induced by a single-electron spin in a quantum dot: applications to entangling remote spins via a single photon," *Phys. Rev. B*, vol. 78, p. 085307, 2008.

[52] C. Santori, D. Fattal, and Y. Yamamoto, *Single-Photon Devices and Applications*. New York, NY, USA: Wiley, 2010.

[53] K. Nemoto *et al.*, "Photonic architecture for scalable quantum information processing in diamond," *Phys. Rev. X*, vol. 4, p. 031022, 2014.

[54] S. L. Braunstein and A. Mann, "Measurement of the Bell operator and quantum teleportation," *Phys. Rev. A*, vol. 51, p. R1727, 1995.

[55] C. Jones, K. De Greve, and Y. Yamamoto, "A high-speed optical link to 955 entangle quantum dots," arXiv:1310.4609, 2013.

[56] L. Childress, J. M. Taylor, A. S. Srensen, and M. D. Lukin, "Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters," *Phys. Rev. A*, vol. 72, p. 052330 2005.

[57] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories," *Nature Photon.*, vol. 6, pp. 777–781, 2012.

[58] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," *Phys. Rev. A*, vol. 40, pp. 4277–4281, 1989.

[59] D. Deutsch *et al.*, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Phys. Rev. Lett.*, vol. 77, p. 2818, 1996.

[60] J.-W. Pan, S. Simon, C. Brukner, and A. Zeilinger, "Entanglement purification for quantum communication," *Nature*, vol. 410, pp. 1067–1070, 2001.

[61] W. Dür and H. J. Briegel, "Entanglement purification and quantum error correction," *Rep. Prog. Phys.* vol. 70, pp. 1381–1424, 2007.

[62] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Rep. Prog. Phys.*, vol. 76, pp. 076001-1–076001-35, 2013

[63] H. Aschauer, Ph.D. dissertation, Quantum communication in noisy environments, Physics Department, Ludwig maximilians universitat, Munich, Germany, 2004.

[64] A. M. Stephens, J. Huang, K. Nemoto, and W. J. Munro, "Hybrid-system approach to fault-tolerant quantum communication," *Phys. Rev. A*, vol. 87, p. 052333, 2013.

[65] L. Hartmann, B. Kraus, H.-J. Briegel, and W. Dur, "On the role of memory errors in quantum repeaters," *Phys. Rev. A*, vol. 75, p. 032310, 2007.

[66] M. Razavi, M. Piani, and N. Lütkenhaus, "Quantum repeaters with imperfect memories: Cost and scalability," *Phys. Rev. A*, vol. 80, p. 032301, 2009

[67] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Phys. Rev. Lett.*, vol. 86, pp. 5188–5191, 2000.

[68] P Kok *et al.*, “Linear optical quantum computing with photonic qubits,” *Rev. Mod. Phys.*, vol. 79, pp. 135–174 2007.

[69] A. G. Fowler *et al.*, “Surface code quantum communication,” *Phys. Rev. Lett.*, vol. 104, p. 180503, 2010.

[70] K. Azuma, K. Tamaki, and H. K. Lo, All photonic quantum repeaters. (2013). [Online]. Available: http://arxiv.org/abs/1309.7207

[71] 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, p. 250501, 2014.

[72] D. P. DiVincenzo, The physical implementation of quantum computation. (2000). [Online]. Available: http://arxiv.org/abs/quant-ph/0002077

[73] C. Simon *et al.*, “Quantum memories,” *Eur. Phys. J. D*, vol. 58, pp. 1–22, 2010.

[74] R. Laflamme, C. Miquel, J. Paz, and W. Zurek, Perfect Quantum Error Correction Code, quant-ph/9602019, 1996.

[75] E. Knill and R. Laflamme, “Theory of quantum error-correcting codes,” *Phys. Rev. A*, vol. 55, p. 900, 1997.

William J. Munro received the Graduation degree with a Ph.D. degree in quantum optics from the University of Waikato, Hamilton, New Zealand, in 1995. He is currently the Group Leader of the newly formed Theoretical Quantum Physics Research Group, NTT Basic Research Laboratories, Atsugi, Japan. He was with the University of Queensland, Australia and HP Laboratories, Bristol, U.K. In 2010, he joined the NTT Basic Research Laboratories. His current research interests include practical implementations for quantum technology.

Koji Azuma received the bachelor’s degree from Osaka University, Osaka, Japan, the master’s degree from the University of Tokyo, Tokyo, Japan, and the Ph. D degree in physics from Osaka University in 2010. He is currently a Researcher at the Theoretical Quantum Physics Research Group, NTT Basic Research Laboratories, Atsugi, Japan. In April 2010, he got his present position. His research interests include quantum information theory and the realization of quantum communication and computation.

Kiyoshi Tamaki received the Ph.D. degree from the Graduate University for Advanced Studies (SOKENDAI), Hayama, Japan, in 2004. After receiving the Ph.D degree, he was with the Perimeter Institute for Theoretical Physics, Canada, and the University of Toronto, Canada. In January 2006, he joined the NTT Basic Research Laboratories, Atsugi, Japan, where he is currently a Researcher at the Theoretical Quantum Physics Research Group. His main research interests include theory of quantum information processing, especially security proofs of practical QKD.

Kae Nemoto received the Ph.D. degree in theoretical physics from Ochanomizu University, Tokyo, Tokyo, Japan. She spent several years as a Postdoctoral Research Fellow with the University of Queensland and the University of Wales in U.K. Since 2003, she has been a Faculty Member at the National Institute of Informatics, Tokyo, where she is currently a Professor. Her current research interests include the implementation of quantum information devices, hybrid quantum systems, quantum networks, and complex systems. She is a Fellow of the IOP, London.