Quantum Repeater with Encoding

Quantum Repeater with Encoding

Liang Jiang[1], J. M. Taylor[2], Kae Nemoto[3], W. J. Munro[3,4], Rodney Van Meter[3,5], and M. D. Lukin[1]
[1]*Department of Physics, Harvard University, Cambridge, MA 02138, USA*
[2]*Department of Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[3]*National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*
[4]*Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS34 8QZ, UK and*
[5]*Faculty of Environment and Information Studies, Keio University 5322 Endo, Fujisawa, Kanagawa 252-8520, Japans*
(Dated: December 21, 2008)

We propose a new approach to implement quantum repeaters for long distance quantum communication. Our protocol generates a backbone of encoded Bell pairs and uses the procedure of classical error correction during simultaneous entanglement connection. We illustrate that the repeater protocol with simple Calderbank-Shor-Steane (CSS) encoding can significantly extend the communication distance, while still maintaining a fast key generation rate.

PACS numbers: PACS number

I. INTRODUCTION

Quantum key distribution generates a shared string of bits between two distant locations (a key) whose security is ensured by quantum mechanics rather than computational complexity [1]. Recently, quantum communication over 150 km has been demonstrated [2], but the key generation rate decreases exponentially with the distance due to the fiber attenuation. Quantum repeaters can resolve the fiber attenuation problem, reducing the exponential scaling to polynomial scaling by introducing repeater stations to store intermediate quantum states [3, 4, 5]. Dynamic programming-based search algorithm can optimize the key generation rate and the final-state fidelity of the quantum repeaters [6]. Using additional local resources (i.e., more quantum bits per station), the key generation rate can be further improved by multiplexing different available pairs [7] and banding pairs according to their fidelities [8]. However, since all these protocols use entanglement purification that requires two-way classical communication, the time to purify pairs increases with the distance and all these protocols are relatively slow. Thus, the finite coherence time of quantum memory ultimately limits the communication distance [9]. As illustrated in Fig. 1, the estimated key generation rate sharply decreases as soon as the memory error becomes dominant.

Here we propose a new, fast quantum repeater protocol in which the communication distance is *not* limited by the memory coherence time. Our protocol encodes logical qubits with small CSS codes [10], applies entanglement connection at the encoded level, and uses classical error correction to boost the fidelity of entanglement connection. We eliminate the time-consuming entanglement purification operation over long distances and also avoid the resource-consuming procedure of quantum error correction. We find that the new repeater protocol with small CSS codes can extend the communication distance ($10^3 \sim 10^6$ km) and maintain an efficient key generation rate (above 100 bits/sec) using finite local resources ($30 \sim 150$ qubits/station) that scale logarithmically with distance.

In Sec. II, we describe the idealized quantum repeater protocol to overcome the fiber attenuation problem, emphasizing the possibility of simultaneous entanglement connection and pointing out three other major imperfections (entanglement infidelity, operational errors, and memory errors) that still needs to be suppressed. In Sec. III, we consider an example of quantum repeater with repetition code to suppress the bit-flip errors. In Sec. IV, we provide the general protocol for quantum repeater with CSS code that can suppress both bit-flip and dephasing errors. In Sec. V, we compute the final fidelity achievable with our protocol, which in principle can be arbitrarily close to unity using large and efficient CSS code. In Sec. VI, we calculate the maximum number of connections depending on the code and the imperfections, and we also estimate the key generation rate. In Sec. VII, we discuss potential improvements and other applications.

II. FAST QUANTUM COMMUNICATION WITH IDEAL OPERATIONS

We start by describing an idealized quantum repeater protocol, where fiber attenuation is the only problem to be overcome. As illustrated in Fig. 2, there are L repeater stations, and the separation between the neighboring stations is of the order of the fiber attenuation length. The Bell pairs $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ between neighboring repeater stations are independently generated and verified. Then *entanglement connection* (swapping) [12, 13] is applied to connect these Bell pairs into a long Bell pair. Each intermediate repeater station measures the two local qubits in the Bell basis (called *Bell measurement*, see the inset of Fig. 2) and announces 2 classical bits of information, which uniquely specify the four possible measurement outcomes and enables the determination of the *Pauli frame* for the remaining qubits

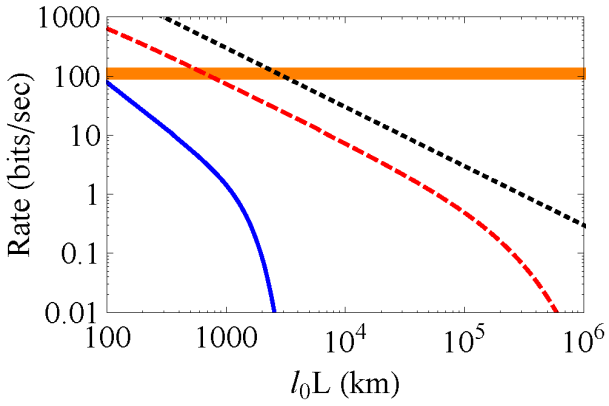

FIG. 1: Comparison between the conventional and new repeater protocols, in terms of the generation rate of Bell pairs or secret bit pairs (i.e., the sustained bandwidth of the repeater channel). The memory coherence time is assumed to be $t_{coh} = 10$ sec, and the nearest neighbor spacing is $l_0 = 10$ km. (i) The blue curve is the BDCZ protocol (with the maximum number of qubits per station increasing logarithmically with distance, see scheme C in Ref. [11]). The sharp decrease in rate is attributed to blinded connection and purification [9] when the memory error becomes dominant (i.e., time $\gtrsim 0.01\tau_{coh} = 0.1$ sec). (ii) The red dashed curve is the parallel protocol (with the number of qubits per station increasing at least linearly with distance, see scheme B in Ref. [11]). (iii) The black dotted reference curve is the inverse of the classical communication time between the final stations. Since all conventional repeater protocols rely on two-way classical communication, their rates always stay below the reference curve unless parallel or multiplexed [8] repeater channels are used. (iv) The orange horizontal thick line is our new repeater protocol with encoding (with the number of qubits per station increasing logarithmically or poly-logarithmically with distance). Since our protocol runs in the one-way communication mode, the rate is independent of the communication distance, and can reach above the black dashed curve. Our protocol is much more efficient over long distances than conventional protocols.

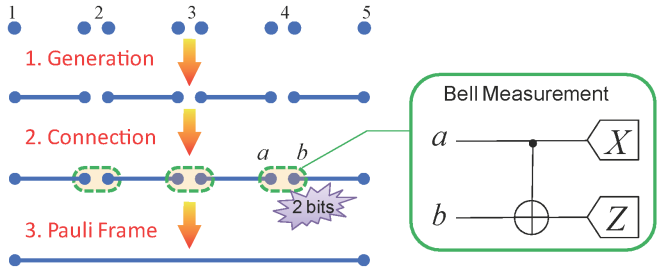

FIG. 2: Idealized quantum repeater. There are $L = 5$ repeater stations. Each intermediate station has two physical qubits. **Step 1. (Generation)** Bell pairs between neighboring repeater stations are generated. **Step 2. (Connection)** The qubits at the intermediate stations are measured in the Bell basis (see the inset). **Step 3. (Pauli Frame)** The Pauli frame for qubits at the outermost stations is determined, based on the outputs of intermediate Bell measurements. Finally, one remote Bell pair between the outermost stations is created.

(i.e., the choice of local Pauli operators that adjust the long Bell pair to $|\Phi^+\rangle$ [14]). This is a deterministic process requiring local operation and (one-way) classical communication.

The entanglement connection can be applied *simultaneously* [1] for all intermediate stations, because the quantum circuit for Bell measurement does not depend on the Pauli frame. It is the interpretation of the measurement outcome that depends on the Pauli frame. Fortunately, we can wait until we collect all $2(L-2)$ announced classical bits from intermediate stations, and decide the Pauli frame for the final distant Bell pair. In addition, without compromising the security for quantum key distribution, the two final (outermost) stations can measure their qubits in random X and Z basis and announce their choices of the basis even before receiving classical bits from intermediate stations. Half of the time, they will find that they choose the same basis (in the Pauli frame) and obtain strongly correlated measurement outcomes that can be used for secret keys [15]. Thanks to the *simultaneous entanglement connection*, the idealized quantum repeater can be very fast and the *cycle time* τ_c is just the total time for entanglement generation and connection between neighboring repeater stations.

In practice, however, there are three major imperfections besides the fiber attenuation. (1) The generated entangled state ρ between neighboring repeater stations is not the perfect Bell state $|\Phi^+\rangle$, characterized by the entanglement fidelity

$$F_0 = \langle\Phi^+|\,\rho\,|\Phi^+\rangle \leq 1. \tag{1}$$

(2) The local operations for entanglement connection have errors [3, 4, 5, 6]. For example, the local two-qubit unitary operation U_{ij} would be

$$U_{ij}\rho U_{ij}^\dagger \to (1-\beta)\,U_{ij}\rho U_{ij}^\dagger + \frac{\beta}{4}\,\mathrm{Tr}_{ij}\,[\rho]\otimes I_{ij}, \tag{2}$$

where β is the gate error probability, $\mathrm{Tr}_{ij}\,[\rho]$ is the partial trace over the subsystem i and j, and I_{ij} is the identity operator for the subsystem i and j. The projective measurement of state $|0\rangle$ would be

$$P_0 = (1-\delta)\,|0\rangle\langle 0| + \delta\,|1\rangle\langle 1|\,, \tag{3}$$

where δ is the measurement error probability. (3) The quantum memory decoheres with rate γ. We model the memory error probability for storage time τ_c as $\mu = 1 -$

[1] We use the rest frame of the repeater stations.

$e^{-\gamma\tau_c} \approx \gamma\tau_c$. The action of the memory error on the ith qubit would be

$$\rho \to (1-\mu)\,\rho + \frac{\mu}{2}\,\mathrm{Tr}_i\left[\rho\right] \otimes I_i, \tag{4}$$

where $\mathrm{Tr}_i\left[\rho\right]$ is the partial trace over the subsystem i, and I_i is the identity operator for the subsystem i.

In the following two sections, we will present the new repeater protocol. Our new repeater protocol replaces the physical qubits (in Fig. 2) with encoded qubits (in Fig. 3), generates the encoded Bell pairs between neighboring stations, connects the encoded Bell pairs at intermediate stations simultaneously, and determines the Pauli frame for the encoded Bell pair shared by the final stations. In Sec. III we provide an illustrative example of quantum repeater with 3-qubit repetition code that can fix only bit-flip errors. In Sec. IV we propose our new protocol with CSS codes that can fix all imperfections listed above.

III. QUANTUM REPEATER WITH REPETITION CODE

To illustrate the idea, we first consider an example that uses the 3-qubit repetition code to encode one logical qubit

$$\left|\tilde{0}\right\rangle = |000\rangle \quad \text{and} \quad \left|\tilde{1}\right\rangle = |111\rangle\,, \tag{5}$$

which can fix one bit-flip error. Although it cannot fix all the errors given in Sec. II, this example illustrates all other key elements of the new repeater protocol and it can be easily generalized to the CSS encodes that can fix all the errors as discussed in Sec. IV.

First, we generate the encoded Bell pair $\left|\tilde{\Phi}^+\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|\tilde{0}\right\rangle_1\left|\tilde{0}\right\rangle_2 + \left|\tilde{1}\right\rangle_1\left|\tilde{1}\right\rangle_2\right)$ between neighboring stations 1 and 2, as illustrated in the upper-left panel of Fig. 3. We need at least six qubits from each station: three for memory qubits (blue dots) and three for ancillary qubits (gray dots). There are three steps: (i) We locally prepare the encoded state $\frac{1}{\sqrt{2}}\left(\left|\tilde{0}\right\rangle_1 + \left|\tilde{1}\right\rangle_1\right)$ and $\left|\tilde{0}\right\rangle_2$ and store them in the memory qubits (in blue squared boxes); (ii) we generate three copies of the physical Bell pairs $\left(\frac{|0\rangle_1|0\rangle_2+|1\rangle_1|1\rangle_2}{\sqrt{2}}\right)^{\otimes 3}$ between ancillar qubits (gray lines); (iii) we use the entanglement resources of 3 physical Bell pairs to implement 3 *teleportation-based CNOT gates* [16, 17, 18], applied *transversally* between the memory qubits storing the encoded states $\frac{1}{\sqrt{2}}\left(\left|\tilde{0}\right\rangle_1 + \left|\tilde{1}\right\rangle_1\right)$ and $\left|\tilde{0}\right\rangle_2$:

$$\frac{1}{\sqrt{2}}\left(|000\rangle_1 + |111\rangle_1\right) \otimes |000\rangle_2 \tag{6}$$

$$\to \frac{1}{\sqrt{2}}\left(|000\rangle_1|000\rangle_2 + |111\rangle_1|111\rangle_2\right), \tag{7}$$

which gives us exactly the desired encoded Bell pair $\left|\tilde{\Phi}^+\right\rangle_{12}$. Similarly, we can generate encoded Bell pairs $\left|\tilde{\Phi}^+\right\rangle_{j,j+1}$ between neighboring stations j and $j+1$, for $j = 2, \cdots, L-1$.

Then we connect the encoded Bell pairs $\left|\tilde{\Phi}^+\right\rangle_{12}$ and $\left|\tilde{\Phi}^+\right\rangle_{23}$ to obtain the longer encoded Bell pair $\left|\tilde{\Phi}^+\right\rangle_{13}$. The idea is to perform the encoded Bell measurement over the two encoding blocks at station 2. We use $2a$ and $2b$ to refer to the left and the right encoding blocks at station 2, respectively. As shown in Fig. 3 (see step 2 and the lower-left panel), we apply three pairwise CNOT gates between the two encoding blocks $\{a_i\}$ and $\{b_i\}$ at station 2. To see the possible outcomes of this procedure, we rewrite the initial state in terms of Bell states between stations 1 and 3,

$$\begin{aligned}
&\left|\tilde{\Phi}^+\right\rangle_{1,2a} \otimes \left|\tilde{\Phi}^+\right\rangle_{2b,3} \\
=&\frac{1}{2}\left(\begin{array}{l}\left|\tilde{\Phi}^+\right\rangle_{13} \otimes \left|\tilde{\Phi}^+\right\rangle_{2a,2b} + \left|\tilde{\Phi}^-\right\rangle_{13} \otimes \left|\tilde{\Phi}^-\right\rangle_{2a,2b} \\ + \left|\tilde{\Psi}^+\right\rangle_{13} \otimes \left|\tilde{\Psi}^+\right\rangle_{2a,2b} + \left|\tilde{\Psi}^-\right\rangle_{13} \otimes \left|\tilde{\Psi}^-\right\rangle_{2a,2b}\end{array}\right) \\
\to&\frac{1}{2}\left(\begin{array}{l}\left|\tilde{\Phi}^+\right\rangle_{13} \otimes \left|\tilde{+}\right\rangle_{2a}\left|\tilde{0}\right\rangle_{2b} + \left|\tilde{\Phi}^-\right\rangle_{13} \otimes \left|\tilde{-}\right\rangle_{2a}\left|\tilde{0}\right\rangle_{2b} \\ + \left|\tilde{\Psi}^+\right\rangle_{13} \otimes \left|\tilde{-}\right\rangle_{2a}\left|\tilde{0}\right\rangle_{2b} + \left|\tilde{\Psi}^-\right\rangle_{13} \otimes \left|\tilde{-}\right\rangle_{2a}\left|\tilde{1}\right\rangle_{2b}\end{array}\right),
\end{aligned}$$

where $\left|\tilde{\Phi}^\pm\right\rangle_{13} = \frac{1}{\sqrt{2}}\left(\left|\tilde{0}\right\rangle_1\left|\tilde{0}\right\rangle_3 \pm \left|\tilde{1}\right\rangle_1\left|\tilde{1}\right\rangle_3\right)$, $\left|\tilde{\Psi}^\pm\right\rangle_{13} = \frac{1}{\sqrt{2}}\left(\left|\tilde{0}\right\rangle_1\left|\tilde{1}\right\rangle_2 \pm \left|\tilde{1}\right\rangle_1\left|\tilde{0}\right\rangle_2\right)$, $\left|\tilde{\pm}\right\rangle_{2a} = \frac{1}{\sqrt{2}}\left(\left|\tilde{0}\right\rangle_{2a} \pm \left|\tilde{1}\right\rangle_{2a}\right)$. To complete the encoded Bell measurement, we projectively measure the logical qubits of these two encoding blocks as follows: (1) The logical qubit for $2a$ should be measured in the $\{\left|\tilde{\pm}\right\rangle\}$ basis, which can be achieved by measuring the physical qubits $\{a_i\}$ in the $\{|\pm\rangle\}$ basis. Since $\left|\tilde{+}\right\rangle = \frac{1}{2}\left(|+++\rangle + |+--\rangle + |-+-\rangle + |--+\rangle\right)$ and $\left|\tilde{-}\right\rangle = \frac{1}{2}\left(|---\rangle + |-++\rangle + |+-+\rangle + |++-\rangle\right)$, there will be an odd number of $|+\rangle$ outputs if the encoded qubit is in state $\left|\tilde{+}\right\rangle$, and an even number of $|+\rangle$ outputs if the encoded qubit is in state $\left|\tilde{-}\right\rangle$. (2) The logical qubit for $2b$ should be measured in the $\{\left|\tilde{0}\right\rangle, \left|\tilde{1}\right\rangle\}$ basis, which can be achieved by measuring the physical qubits $\{b_i\}$ in the $\{|0\rangle, |1\rangle\}$ basis. There should be three $|0\rangle$ outputs for state $\left|\tilde{0}\right\rangle$, and three $|1\rangle$ outputs for state $\left|\tilde{1}\right\rangle$. The pairwise CNOT gates and projective measurement of physical qubits are summarized in the lower-left panel of Fig. 3.

We now show the suppression of bit-flip errors due to the repetition code [Eq. (5)]. If one of the physical qubits in $2b$ is bit-flipped, the measurement outcomes for $2b$ will contain two correct outputs and one erroneous output. Choosing the majority output, we can identify and correct the erroneous output, and still obtain the logical bit encoded in $2b$ correctly. We emphasize that only classical error correction is used. If there is one physical qubit in $2a$ that suffers from a bit-flip error, this error will not affect the outputs for $2a$, as bit-flip errors commute with

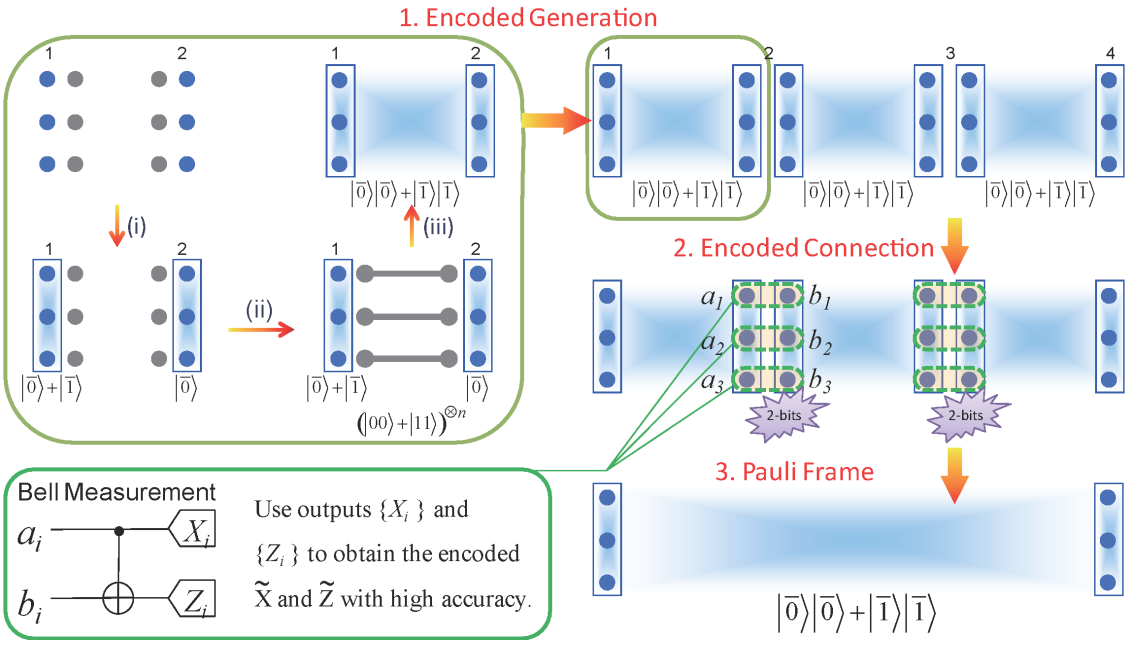

FIG. 3: Repeater protocol with encoding. Each repeater station has $2n$ memory qubits (blue dots) and $O(n)$ auxiliary qubits (gray dots). Here $n = 3$. **Step 1. (Encoded Generation)** Between two neighboring stations (upper-left panel): (i) memory qubits are fault-tolerantly prepared in the encoded states $|\tilde{0}\rangle$ or $|\tilde{+}\rangle = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle + |\tilde{1}\rangle)$, (ii) purified physical Bell pairs are generated between auxiliary qubits (connected gray dots), (iii) an encoded Bell pair $\left|\tilde{\Phi}^{+}\right\rangle_{AB} = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle_A|\tilde{0}\rangle_B + |\tilde{1}\rangle_A|\tilde{1}\rangle_B)$ between neighboring stations is created using encoded CNOT gate (achieved by n pairwise, teleportation-based CNOT gates [16, 17, 18]). **Step 2. (Encoded Connection)** Encoded Bell measurements are simultaneously applied to all intermediate repeater stations, via pairwise CNOT gates between qubits a_i and b_i followed by measurement of the physical qubits (the lower-left panel). Using classical error correction, the outcomes for the encoded Bell measurement can be obtained with a very small effective logical error probability $Q \sim q^{t+1}$ [Eq. (11)]. The outcome is announced as 2 classical bits (purple star) at each intermediate repeater station. **Step 3. (Pauli Frame)** According to the outcomes of intermediate encoded Bell measurements, the Pauli frame [14] can be determined for qubits at the outermost stations. Finally, one encoded Bell pair between the final (outermost) stations is created.

the operators to be measured; this error may affect one corresponding physical qubit in $2b$, which can be identified and corrected using the majority. Therefore, we can obtain the logical outcomes for both $2a$ and $2b$, and the suppressed effective logical error probability can be

$$Q = \binom{3}{2} q_b^2 + \binom{3}{3} q_b^3 \approx 6q_b^2 \ll q_b, \tag{8}$$

where $q_b \leq 4\beta + 2\delta + \mu$ is the effective error probability for each b_i to give the wrong output (Appendix. A).

To complete the entanglement connection, station 2 announces the outcomes for its two logical qubits from the encoded Bell measurement, which contains *two* classical bits of information and determines the Pauli frame for the encoded Bell pair shared between stations 1 and 3. Note that the detailed outputs of physical qubits are only important to obtain the logical outcomes, but not needed for communication among stations. Similarly, we can perform entanglement connection for all the intermediate stations. Furthermore, these entanglement connections can still be applied simultaneously for all intermediate striations, as described in Sec. II. The final stations share the encoded Bell pair $\left|\tilde{\Phi}^{+}\right\rangle_{1L} = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle_1|\tilde{0}\rangle_L + |\tilde{1}\rangle_1|\tilde{1}\rangle_L)$, whose Pauli frame is determined by the $2(L-2)$ announced classical bits from all intermediate stations.

IV. QUANTUM REPEATER WITH CSS CODE

In this section, we will generalize the repeater protocol from the 3-qubit repetition code to any $[[n, k, 2t+1]]$ *CSS code* [10], which encodes k logical qubits with n physical qubits and fixes up to t (bit-flip and dephasing) errors. For simplicity, we will focus on the CSS codes with $k = 1$, which includes the well studied $[[5, 1, 3]]$, $[[7, 1, 3]]$ (Steane), and $[[9, 1, 3]]$ (Shor) codes. Extension of the protocol to $k > 1$ is straightforward. The CSS code can be regarded as a combination of two classical error correcting codes C^X and C^Z, which fix dephasing errors and bit-blip errors, respectively. The error syndromes for the code C^X (or C^Z) can be obtained if we have the outputs for the n physical qubits measured in the X (or Z) basis.

The relevant properties of the CSS codes are summarized as follows: (1) The measurement of logical operator $\tilde{X}$ (or $\tilde{Z}$) can be obtained from projective measurement of physical qubits in the X (or Z) basis. (2) The outputs from measurements of physical qubit in the X (or Z) basis should comply with the rules of the classical error correcting code C^X (or C^Z), which can fix up to t^X (or t^Z) errors in the n output bits. (For example, the 3-qubit repetition cod can fix up to $t^Z = 1$ bit-flip error as discussed in Sec. III.) Suppose each output bit has an (uncorrelated) effective error probability $q \sim \beta + \delta + \mu$, after fixing up to t errors the remaining error probability for the logical outcome is $O\left(q^{t+1}\right)$, assuming $t = \min\left\{t^X, t^Z\right\}$. (3) The encoded CNOT gate can be implemented by n pairwise CNOT gates between two encoding blocks [10]. Such pairwise CNOT gates do not propagate errors within each encoding block, and it can be be used for preparation of encoded Bell pairs.

We find that each repeater station needs approximately $6n$ physical qubits (see Appendix B for details), including $2n$ memory qubits to store the two encoded qubits that are entangled with the neighboring stations, and approximately $4n$ ancillary qubits for the fault-tolerant preparation of the encoded qubits and generation of non-local encoded Bell pairs between neighboring repeater stations. There are three steps for each cycle of the new repeater protocol:

1. Generate encoded Bell pairs between two neighboring stations (see the upper-left panel of Fig. 3): (i) We initialize the memory qubits in logical states $\left|\tilde{0}\right\rangle$ and $\frac{1}{\sqrt{2}}\left(\left|\tilde{0}\right\rangle + \left|\tilde{1}\right\rangle\right)$ at each station *fault-tolerantly* (with errors effectively uncorrelated among physical qubits from the same encoding block) [2]. (ii) We use entanglement purification to obtain purified Bell pairs between two neighboring stations [11]. Each purified Bell pair can be immediately used for a *teleportation-based CNOT gate* [16, 17, 18]. (iii) According to the property (3) of the CSS code, we need n teleportation-based CNOT gates to implement the encoded CNOT gate and obtain the encoded Bell pair $\left|\tilde{\Phi}^+\right\rangle_{j,j+1} = \frac{1}{\sqrt{2}}\left(\left|\tilde{0}\right\rangle_j \left|\tilde{0}\right\rangle_{j+1} + \left|\tilde{1}\right\rangle_j \left|\tilde{1}\right\rangle_{j+1}\right)$ between neighboring stations j and $j+1$.

2. Connect the encoded Bell pairs, performing encoded Bell measurement at all intermediate stations simultaneously (see step 2 of Fig. 3). At each intermediate station, we first apply the pairwise CNOT gates between qubits a_i and b_i, with a_i from the control block and b_i from the target block, for $i = 1, \cdots, n$ (as shown in the lower-left panel in Fig. 3). Then we projectively measure the physical qubits in the X basis for a_i and in the Z basis for b_i. According to the property (2) of the CSS code, we can use the classical error correcting code C^X (or C^Z) to fix up to t errors in $\{a_i\}$ (or $\{b_i\}$), leaving only $O\left(q^{t+1}\right)$ for the logical error probability. Thus, the outcomes for the encoded $\tilde{X}$ and $\tilde{Z}$ operators of the encoded Bell measurement can be obtained with high accuracy of $O\left(q^{t+1}\right)$. Similar to the idealized repeater, each intermediate repeater station announces 2 classical bits of information of the encoded Bell measurement.

3. According to the $2(L-2)$ announced classical bits from all intermediate repeater stations, choose the Pauli frame at the final repeater stations for the shared encoded Bell pair.

V. ERROR ESTIMATE

In order to calibrate the encoded Bell pair obtained from the new repeater protocol, we need to generalize the definition of entanglement fidelity, because the encoding enables us to correct small errors that deviate from the logical subspace. We define the *entanglement fidelity* as

$$F = \left\langle \tilde{\Phi}^+ \right| \mathcal{R}\left[\rho_{\text{fina,Bell}}\right] \left| \tilde{\Phi}^+ \right\rangle, \tag{9}$$

where $\mathcal{R}$ represents the (ideal) recovery operation with quantum error correction [19]. The entanglement fidelity F can calibrate the security for the protocol and bound the maximum information leaked from the final stations [3]. F can also be practically obtained from the correlation measurement between the final repeater station (Appendix C).

We emphasize that the property of fault-tolerance can be maintained throughout the entire repeater protocol (fault-tolerant initialization, transverse CNOT gate, and encoded qubit measurement), so the errors for individual physical qubits are effectively uncorrelated. With some calculation (see Appendix. A), we estimate that the effective error probability (per physical qubit) is

$$q = 4\beta + 2\delta + \mu, \tag{10}$$

Note that q does not explicitly depend on F_0, because for level-m purified Bell pairs (see Appendix D) the operational errors (β and δ) dominate the super-exponentially suppressed infidelity approximately $(1-F_0)^{2^{m/2}}$. Then the *effective logical error probability* for each encoding block (caused by more than t errors from the encoded block) is

$$Q = \sum_{j=t+1}^{n} \binom{n}{j} q^j (1-q)^{n-j} \approx \binom{n}{t+1} q^{t+1}, \tag{11}$$

[2] We can achieve fault-tolerant preparation of the logical state $\left|\tilde{0}\right\rangle$ (or $\left|\tilde{+}\right\rangle$) by two approaches. One approach uses several copies of the logical states to distill a purified logical state with negligible contribution from initial correlated errors [28]. Alternatively, we may start with $|0\rangle^{\otimes n}$ (or $|+\rangle^{\otimes n}$), projectively measure the x-stabilizers using fault-tolerant circuit, and update the stabilizers during entanglement connection. See Appendix B for details.

[3] According to Ref. [31], if the two final stations share a Bell pair with fidelity $F = 1 - 2^{-s}$, then Eve's mutual information with the key is at most $2^{-c} + 2^{O(-2s)}$ where $c = s - \log_2(2 + s + 1/\ln 2)$.

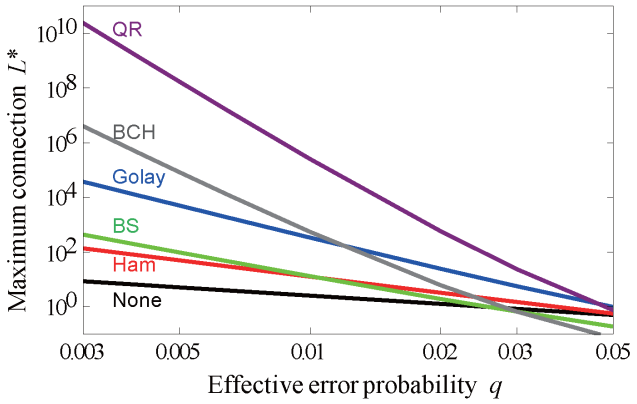

FIG. 4: From Eqs. (11,13), the maximum number of connections L^* is estimated as a function of the effective error probability q, assuming $F^* = 0.95$, for various CSS codes [20] listed in Table I. For $q < 0.03$, L^* scales as $1/q^{t+1}$.

where the approximation requires small q. Since any logical error from the repeater stations will affect the final encoded Bell pair, the entanglement fidelity is

$$F = (1-Q)^{2L}, \tag{12}$$

with infidelity $1 - F \approx 2LQ$ for small Q.

For large codes, we may evaluate Eq. (11) under the assumptions $n \gg t \gg 1$. Approximating the combinatorial function in this limit yields $Q \approx \frac{1}{\sqrt{2\pi t}} \left(\frac{e^{1+1/2n} nq}{t+1} \right)^{t+1}$, which indicates that for large codes with $n \propto t$, Q can be arbitrarily small when $q \lesssim q_c \approx \lim_{n,t\to\infty} \frac{t+1}{e^{1+1/2n} n}$. Numerically, we can evaluate the complete sum in Eq. (11) and we find $q_c \approx 5\%$, which corresponds to $\sim 1\%$ per-gate error rates. In addition, CSS codes with $n \lesssim 19t$ exist for arbitrarily large t (according to the Gilbert-Varsharov bound, see Eq. (30) in Ref. [21]). Therefore, our new repeater protocol with encoding provides a scalable approach for long distance quantum communication.

VI. EXAMPLE IMPLEMENTATIONS

We now consider the implementation of the new repeater protocol. Given the effective error probability q and the *target fidelity* F^*, we can use Eq. (12) to calculate the *maximum number of connections*

$$L^* = \frac{\ln F^*}{\ln (1-Q)}. \tag{13}$$

This provides a unitless distance scale over which Bell pairs with fidelity F^* can be created. According to Eqs. (11,13), we can estimate L^* as a function of q, which is plotted in Fig. 4 assuming $F^* = 0.95$ for various CSS codes. Since L^* scales as $q^{-(t+1)}$ for $q \lesssim 3\%$, we can significantly increase L^* by considering efficient quantum codes with large t. For example, given $q = 0.3\%$, we estimate the maximum number of connections $L^* \approx 9$, 1.4×10^2, and 3.7×10^4 for cases of no encoding, $[[7,1,3]]$ Hamming code, and $[[23,1,7]]$ Golay code, respectively. If we choose the nearest neighbor spacing to be $l_0 = 10$ km (about half the fiber attenuation length), the corresponding maximum distances will be 90 km, 1.4×10^3 km, and 3.7×10^5 km. The new protocol can easily reach and go beyond intercontinental distances. In Table I, we summarize the local resources and maximum communication distance for the new protocol with different encoding.

Name	Code $[[n,k,2t+1]]$	Resources (qubits/station)	Distance (km)
No encoding	–	4	180
Repetition-3	$[3,1,3]$	18	1.0×10^4
Repetition-5	$[5,1,5]$	30	1.0×10^6
Hamming	$[[7,1,3]]$	42	1.4×10^3
Bacon-Shor	$[[25,1,5]]$	150	4.3×10^3
Golay	$[[23,1,7]]$	138	3.7×10^5
BCH	$[[127,29,15]]$	–	4.0×10^7
QR	$[[103,1,19]]$	–	2.4×10^{11}

TABLE I: Local resources, and maximum communication distance for the new repeater protocol. In the case of no encoding, each station has 2 qubits for entanglement connection, and 2 additional qubits for entanglement purification to obtain high-fidelity purified Bell pairs. For repetition codes (with single square bracket), only one type of errors (bit-flip or dephasing) can be suppressed. For other CSS codes (with double square brackets), both bit-flip and dephasing errors can be suppressed. The local resources are estimated to be $6n$ qubits for each station (Appendix B). The distance is estimated from Eqs. (11,13), assuming parameters $q = 0.3\%$, $F^* = 0.95$ and $l_0 = 10$ km.

Besides maximum distances, we also estimate the key generation rate, which is the inverse of the cycle time for the new protocol. For fast local operations (systems such as ion traps [22, 23] and NV centers [24, 25] can achieve almost MHz rate for local operations), the cycle time is dominated by creating purified Bell pairs between neighboring stations

$$\tau_c \approx \kappa \frac{l_0}{v} \frac{e^{l_0/l_{att}}}{\eta^2}. \tag{14}$$

We find that $\tau_c \approx 0.9\kappa$ ms, given the parameters of $l_0 = 10$ km, the fiber attenuation length $l_{att} \approx 20$ km, the signal propagation speed $v \approx 2 \times 10^5$ km/s, and the overall efficiency for collecting and detecting single photon $\eta \approx 0.3$. The dimensionless prefactor κ is the time overhead to ensure that n purified Bell pairs are obtained between neighboring stations. Since there are approximately $4n$ ancillary qubits for entanglement generation at each station, the rate to generate unpurified Bell pairs also increases with n. Thus, κ is not sensitive to the choice of n. As detailed in Appendix D, we estimate

$\kappa \approx 8$ for $\beta = \delta = 10^{-3}$ and $F_0 = 0.95$ with depolarizing error, and the purified pair has fidelity 0.9984 after three levels of purification. Therefore, for the parameters considered here, approximately $6n$ qubits at each station can achieve $\tau_c \approx 7$ ms, which is sufficient for quantum key generation rate of 100 bits/sec over long distances.

VII. DISCUSSION

Our new repeater protocol is significantly faster than the standard repeater protocols over long distances [3, 4, 5, 6], because the time-consuming procedure of entanglement purification of distant Bell pairs is now replaced by local encoding with simple CSS code and classical error correction. The new protocol runs in the one-way communication mode, so the key generation rate is independent of the communication distance, and only limited by the cycle time for encoded Bell pair generation and entanglement connection. The key generation rate can be further improved by having higher efficiency η, improved fidelity F_0, smaller separation between stations l_0, and more qubits per repeater station. In addition, the rate can also be increased by using CSS codes with $k > 1$ (e.g., the $[[127, 29, 15]]$ BCH code mentioned in Fig. 4), along with a small modification to the protocol that each intermediate station sends $2k$ classical bits associated with k Bell measurements.

Asymptotically, CSS codes with $n \lesssim 19t$ exist for arbitrarily large t [obtained from the Gilbert-Varsharov bound, see Eq. (30) in Ref. [21]]. Thus, the effective logical error probability Q [Eq. (11)] can be arbitrarily small for $q \lesssim 5\%$, and $n \propto t \sim \ln L$ is a small number increasing only logarithmically with L. In practice, however, it is still challenging to initialize large CSS encoding block fault-tolerantly with imperfect local operations. To avoid complicated initialization, we may construct larger CSS codes by concatenating smaller codes with r nesting levels, and the code size scales polynomially with the code distance, $n \propto t^r \sim (\ln L)^r$. Alternatively, we may consider the Bacon-Shor code [26]; the encoding block scales quadratically with the code distance $n = (2t+1)^2 \sim \ln^2 L$, and the initialization can be reduced to the preparation of $(2t+1)$-qubit GHZ states.

If the imperfections are dominated by the dephasing errors, we may use the $[2t+1, 1, 2t+1]$ repetition code [e.g., use the $(2t+1)$-qubit GHZ states $|+\cdots+\rangle \pm |-\cdots-\rangle$ with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ to encode one logical qubit]. The repetition code has the advantage of small encoding block and efficient initialization (see Table I). For example, given $q = 0.3\%$ and $F^* = 0.95$, we estimate $L^* \approx 1.0 \times 10^3$ and 1.0×10^5 for 3-qubit and 5-qubit repetition codes, respectively. Such simple repetition encoding can be useful for quantum networks as well [27].

Our repeater protocol can also generate high fidelity entanglement over long distances. For example, $F^* = 0.999$ and $L^* \approx 730$ can be achieved with $q = 0.3\%$ and the $[[23, 1, 7]]$ Golay code. Such high fidelity entanglement might be useful for applications such as quantum state teleportation and distributed quantum computation [18]. Since quantum circuits for state-teleportation or teleportation-based CNOT gate only use Clifford group operations, the generated entanglement can be immediately used in these circuits without waiting for the classical information of the Pauli frame. The adjustment of the Pauli frame has to be postponed until the classical information is received [4].

Suppose good quantum memory (with coherence time longer than the communication time) is available at the final stations, real distant Bell pairs (rather than just strings of secret bits for quantum key distribution) can be generated. For on-demand generation of distant Bell pairs, the time delay $(l_0 L/c)$ associated with the classical communication to specify the Pauli frame is inevitable, and the total time to create one Bell pair on-demand is $\tau_c + l_0 L/c$. For offline generation of distant Bell pairs that are stored in good quantum memory for later use, we have to assume that there are enough qubits at the final stations to store all Bell pair generated, while the number of qubits at each intermediate station remains unchanged. Up to the time delay $(l_0 L/c)$ for the first Bell pair , our quantum repeater channel can create distant Bell pairs at the rate $1/\tau_c$, again corresponding to the flat curve in Fig. 1.

VIII. CONCLUSION

In summary, we have proposed a new, fast quantum repeater protocol for quantum key distribution over intercontinental distances. Our protocol fault-tolerantly generates a backbone of Bell pairs with CSS encoding, and uses simple procedure of classical error correction during connection. Our protocol using simple CSS code can provide secure quantum communication over thousands or even millions of kilometers, with 0.3% effective error probability per physical qubit and 0.95 target fidelity for the final Bell pair (see Table I). The quantum key generation rate can be above 100 bits/sec, only limited by the Bell pair generation between neighboring stations.

We would thank Hans Briegel, Ignacio Cirac, Wolfgang Dür, John Preskill, Anders Sørensen, Sébastien Perseguers, Frank Verstraete, Karl Vollbrecht for stimulating discussions. L.J. and J.M.T. thank NII for the hospitality, where part of this research was done. K.N. and W.J.M. acknowledge support in part by MEXT, NICT, HP and QAP.

[4] Good quantum memory with coherence time longer than the communication time might be needed.

APPENDIX A: EFFECTIVE ERROR PROBABILITY

For our quantum repeater protocol, we introduce the effective error probability q, which estimates the odds for obtaining a wrong output of each physical qubit during entanglement connection. The effective error probability combines various imperfections from entanglement generation and entanglement connection. In the following, we will derive the effective error probability q in terms of various error parameters β, δ, and μ as detailed in Sec. II.

First of all, we observe that all relevant operations (local CNOT gates, teleportation-based CNOT gates, and measurements in Z or X basis) never mix bit-flip errors and phase errors. For example, CNOT gates never convert bit-flip errors into phase errors. Measurements in the Z basis are only sensitive to bit-flip errors, but not to phase errors. Therefore, we can use two probabilities (b, p) to characterize the bit-flip and phase errors, respectively.

We will calculate these two probabilities for the physical qubits from the operational step 1(i,ii,iii) and step 2 as illustrated in Fig. 3. For state distillation [step 1(i)], it is possible to have $(b', p') = (\beta/4 + \mu/2, \beta/2 + \mu/2)$ for each physical qubit of the encoding block. For entanglement purification [step 1(ii)], it is possible to have $(b'', p'') = (\beta/2, \beta/4)$ for each physical qubit of the physical Bell pairs. For teleportation-based CNOT gates [16, 17, 18] [step 1(iii)], the control and target qubits accumulate errors from the input qubits, with $(b_c''', p_c''') = (b' + \beta/2, 2p' + 2p'' + \beta + \delta)$ for the control, and $(b_t''', p_t''') = (2b' + 2b'' + \beta + \delta, b' + \beta/2)$ for the target. Finally, after entanglement connection [step 2], the accumulated probability for obtaining a wrong output is

$$q_b = b_c''' + b_t''' + \beta/2 + \delta = \frac{15}{4}\beta + 2\delta + \mu \tag{A1}$$

for measurements in the Z basis, and is

$$q_p = p_c''' + p_t''' + \beta/2 + \delta = 4\beta + 2\delta + \mu \tag{A2}$$

for measurements in the X basis. For simplicity, we may just use

$$q = \max\{q_b, q_p\} = 4\beta + 2\delta + \mu \tag{A3}$$

to estimate the effective error probability.

APPENDIX B: FAULT-TOLERANT INITIALIZATION OF THE CSS CODE

We now consider two possible approaches to fault-tolerant preparation of the logical states $|\tilde{0}\rangle$ (and $|\tilde{+}\rangle = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle + |\tilde{1}\rangle)$) of the CSS code, using local operations within each repeater station. Both approaches use the technique of state distillation [28].

To facilitate the discussion, we first briefly review the stabilizer formulism for the CSS code [10, 29]. The error syndromes for the code C^X can be obtained by measuring the operators $\{g_j^X\}_{j=1,\cdots,m_X}$, and the syndromes for the code C^Z can be obtained by measuring the operators $\{g_{j'}^Z\}_{j=1,\cdots,m_Z}$. The operators g_j^X and $g_{j'}^Z$ commute $[g_j^X, g_{j'}^Z] = 0$ for all j and j'. The operators $\{g_j^X\}$ and $\{g_{j'}^Z\}$ are called the stabilizer generators. The logical information are stored in the subspace with $+1$ eigenvalues for all stabilizer generators $\{g_j^X\}$ and $\{g_{j'}^Z\}$. (E.g., the 3-qubit repetition code is a CSS code with stabilizer generators $\{g_1^Z, g_2^Z\} = \{Z_1Z_2, Z_2Z_3\}$; any logical state $|\phi\rangle = \alpha|\tilde{0}\rangle + \beta|\tilde{1}\rangle$ satisfies the condition $Z_1Z_2|\phi\rangle = |\phi\rangle$ and $Z_2Z_3|\phi\rangle = |\phi\rangle$.) Note that the stabilizer generator g_j^Z is a product of Z operators, and $g_{j'}^X$ is a product of X operators. In addition, the logical operator $\tilde{X}$ (or $\tilde{Z}$) for the CSS code can also be expressed as a product of X (or Z) operators. (E.g., the 3-qubit repetition code has logical operators $\tilde{X} = X_1X_2X_3$ and $\tilde{Z} = Z_1Z_2Z_3$.)

1. First Approach

In the first approach, we generate several copies of the logical states $|\tilde{0}\rangle$, which are not fault-tolerant as the errors might be correlated among qubits within each encoding block. For example, one quantum gate (with error probability ε) may induce errors in the multiple physical qubits; that is the probability for multi-qubit errors can occurs at the order of $O(\varepsilon)$. To suppress such multi-qubit errors, we use the state distillation circuits (i.e., generalization of the entanglement purification circuits) to suppress both the X and Z errors. After each round of distillation, the correlated errors will be suppressed from $O(\varepsilon^l)$ to $O(\varepsilon^{l+2} + \varepsilon^{2l})$. The distillation operation does not introduce any new correlated errors. Thus after sufficiently many rounds of distillation, the correlated errors can be suppressed. Meanwhile the uncorrelated errors from the distillation operations are also suppressed by the following distillation operations. Therefore, after sufficiently many rounds of distillation, the probability for uncorrelated errors will reach a steady value, of the order of $\beta + \delta$ for each physical qubit.

2. Second Approach

In the second approach, we try to avoid correlated errors from the beginning. The idea is that we start with n physical qubits initialized in the product state $|0\rangle^{\otimes n}$, and projectively measure the stabilizers, which can be achieved fault-tolerantly using the GHZ states (as described in the next paragraph). We obtain a set of binary numbers associated with the stabilizer measurements. In principle, we can perform error correction to the encoding block to restore it to the $+1$ co-eigenstates for the stabilizers. Alternatively, we may keep track of the values for

the stabilizers, and take them into account throughout the entanglement generation and entanglement connection (as detailed below). Finally, we use several copies of the encoding block with uncorrelated error to perform just one round of state distillation to suppress the error probability per physical qubits to $\sim \beta + \delta$.

To achieve fault-tolerant measurement of the stabilizer, we use l-qubit GHZ states (with $l \leq n$) that can be initialized fault-tolerantly [10]. According to the standard form of the stabilizer code (see Ref. [10], page 470), the error in the value for each stabilizer is equivalent to the error of one physical qubit. We further improve the reliability of the stabilizer measurement by repeating it several times [30].

Since we have included the -1 eigenstates for the stabilizers, we need to generalize the encoded CNOT operation by keeping track of the stabilizers as well as the logical qubits. Suppose the encoding block for the control qubit has eigenvalues $(\mathbf{x}_1, \mathbf{z}_1)$ associated with the X and Z stabilizers, and the block for the target qubit has eigenvalues $(\mathbf{x}_2, \mathbf{z}_2)$. The outputs have eigenvalues $(\mathbf{x}_1, \mathbf{z}_1\mathbf{z}_2)$ for the control block and $(\mathbf{x}_1\mathbf{x}_2, \mathbf{z}_2)$ for the target block. Consequently, when we apply the generalized encoded CNOT operation to entanglement generation, there is additional classical communication to exchange the information of stabilizers between neighboring stations, so that both stations can update the eigenvalues of the stabilizers for their encoding blocks. When we apply the generalized encoded CNOT operation to entanglement connection, the classical error correction need to take into account the eigenvalues of the stabilizers to correct errors. Apart the these modifications, the remaining operations remain the same.

3. Estimate Local Resources for Second Approach

We now estimate the minimum number of qubits needed for each repeater station, which is required by the fault-tolerant preparation of the encoding block with small error probability. (For simplicity, we assume that local operational time is much faster than the communication time and can be safely neglected.) We focus on the second scheme of fault-tolerant preparation, which first uses the GHZ states to projectively measure the stabilizers and then apply state distillation to suppress individual qubit errors. We emphasize again that both operations of stabilizer measurement and state distillation can be performed fault-tolerantly.

The local resources are split into two categories: the memory qubits to store two encoding blocks ($2n$ qubits), and the ancillary qubits to assist fault-tolerant preparation. The ancillary qubits should fault-tolerantly prepare of the GHZ state (using n_{GHZ} qubits), and store additional two encoding blocks ($2n$ qubits) for the 2-level state distillation. Altogether, there are $4n+n_{GHZ}$ qubits for each station.

We now detail the procedure of prepare the distilled state in the storage block b, using two-level state distillation with two additional blocks $a1$ and $a2$. First, we obtain a level-1 distilled encoding block in b (by projectively preparing the encoded state for $a1$ and b, and using $a1$ to successfully purify b). Then we obtain another level-1 distilled encoding block in $a2$ (by projectively preparing the encoded state for $a1$ and $a2$, and using $a1$ to successfully purify $a2$). Finally, we obtain the level-2 distilled encoding block in b (by using $a2$ to successfully purify b). Generally, we can obtain a level-l distilled block by using l additional blocks (i.e., l n qubits).

APPENDIX C: ENTANGLEMENT FIDELITY AND CORRELATION

There are two major sources that will reduce the entanglement fidelity for the final encoded Bell pairs. First, the errors from the Bell measurement from intermediate stations will lead to the wrong choice of the Pauli frame, and the probability that all $L-2$ Bell measurements are error-free is $(1-Q)^{2(L-2)}$. In addition, unsuccessful local error correction for the final encoded Bell pair will also reduce the generalized fidelity, and the probability to have a successful error correction is approximately $(1-Q)^2$. Therefore, we estimate that the entanglement fidelity to be $F \approx (1-Q)^{2L-2} \gtrsim (1-Q)^{2L}$.

These two sources also affect the correlation of the secret keys. If the secret keys are obtained from the measurement in the X or Z basis, only half of the $2(L-2)$ classical bits from intermediate repeater stations are relevant while the other half do not affect the keys at all. And the probability for successful classical error correction to infer the encoded logical qubit is of the order of $(1-Q)^2$. Therefore, the correlation is approximately $C \approx (1-Q)^L \approx \sqrt{F}$.

APPENDIX D: TIME OVERHEAD AND FAILURE PROBABILITY FOR ENTANGLEMENT PURIFICATION

We now consider the process of generating n purified Bell pairs between neighboring stations. We will calculate the failure probability P_{fail} for obtaining at least n purified Bell pairs using N_0 unpurified Bell pairs. The failure probability should also depend on the fidelity of unpurified Bell pairs (F_0) and the error probability for local operations (β and δ). Generally, the more unpurified Bell pairs N_0, and the smaller failure probability P_{fail}. For a given P_{fail}, we can estimate the N_0 and consequently the cycle time τ_c that determines the key generation rate.

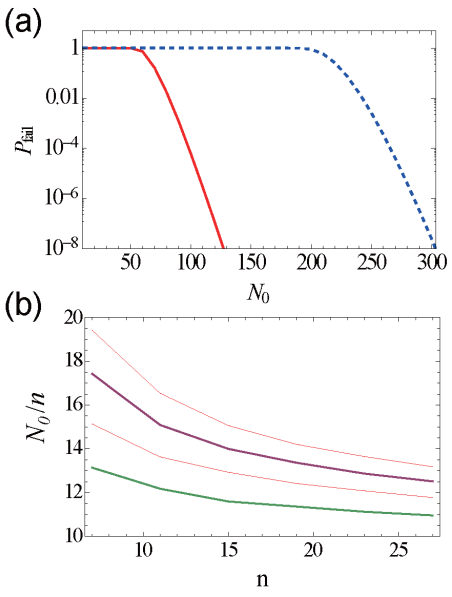

FIG. 5: Failure probability and unpurified Bell pairs. (a) The failure probability P_{fail} decreases exponentially with the number of unpurified Bell pairs N_0 (when N_0 surpasses certain threshold), for $n = 7$ (red solid line) and $n = 23$ (blue dashed line). (b) For fixed P_{fail}, the ratio $N_0/n \sim 15$ for a wide range of n. The four curves from lower left to the upper right correspond to $P_{fail} = 10^{-3}, 10^{-5}, 10^{-7}$ and 10^{-9}, respectively. For both plots, we assume unpurified Bell pairs with fidelity $F_0 = 0.95$ due to depolarizing error. The operational error probabilities are $\beta = \delta = 10^{-3}$. After three levels of purifications, the fidelity of the Bell pair can be 0.9984.

1. Failure Probability

In order to obtain the failure probability, we first calculate the number distribution for purified Bell pairs obtained from N_0 unpurified Bell pairs.

We distinguish the purified Bell pairs according their level of purification. A level-$(i+1)$ pair is obtained from a successful purification using two level-i pairs. Level-0 pairs are the same as unpurified Bell pairs. Level-l pairs are directly used for non-local CNOT gates.

We introduce the number distribution $\left\{p_m^{(i)}\right\}_{m=0,1,2,\cdots}$ for level-i pairs obtained from N_0 unpurified Bell pairs, with $i = 0, 1, \cdots, l$. The number distribution for level-0 pairs is

$$p_m^{(0)} = \delta_{m,N_0}. \tag{D1}$$

As two level-i pairs are needed for one level-$(i+1)$ pair, we define

$$\tilde{p}_k^{(i)} = p_{2k}^{(i)} + p_{2k+1}^{(i)}, \tag{D2}$$

which can be used to calculate the number distribution for level-$(i+1)$ pairs

$$p_m^{(i+1)} = \sum_{j=m} \begin{pmatrix} j \\ m \end{pmatrix} r_i^m \left(1 - r_i\right)^{j-m} \tilde{p}_j^{(i)}, \tag{D3}$$

where r_i is the success probability for obtaining a level-$(i+1)$ pair from two level-i pairs. Thus, the failure probability is

$$P_{fail} = \sum_{j=0}^{n-1} p_j^{(l)}. \tag{D4}$$

For example, given $\beta = \delta = 10^{-3}$ and $F_0 = 0.95$ with depolarizing error, the fidelity for level-3 purified pair can be 0.9984. In Fig. 5(a), we plot the failure probability that decreases exponentially when N_0 surpasses certain threshold. In Fig. 5(b), we plot N_0/n as a function of n, requiring fixed failure probability P_{fail} ($10^{-3}, 10^{-5}$, 10^{-7} or 10^{-9}). We note that $N_0/n \approx 15$ is sufficient to ensure $P_{fail} < 10^{-5}$ a wide range of n.

2. Time Overhead and Key Generate Rate

We now estimate the time needed to obtain n purified Bell pairs between two neighboring repeater stations. Each attempt of entanglement generation takes time l_0/v, with success probability $\eta^2 e^{-l_0/l_{att}}$. Since there are n_{EnG} $(= 2n + n_{GHZ})$ qubits available at each station, the generation rate of unpurified Bell pairs is

$$R = \frac{v}{l_0} \eta^2 e^{-l_0/l_{att}} n_{EnG}, \tag{D5}$$

where the spacing between nearest stations is $l_0 = 10$ km, the fiber attenuation length is $l_{att} = 20$ km, the signal propagation speed is $v = 2 \times 10^5$ km/s, and the overall efficiency for collecting and detecting single photon is $\eta \approx 0.3$. We have $R = n_{EnG} 1.1 \times 10^3 \, \text{sec}^{-1}$.

We can estimate the time to obtain N_0 unpurified Bell pairs $\tau_0 = N_0/R$. Since each station need to connect with both neighboring stations, the total cycle time is twice as long:

$$\tau_c = 2N_0/R = \kappa \frac{l_0}{v} \frac{e^{l_0/l_{att}}}{\eta^2}, \tag{D6}$$

with

$$\kappa = \frac{2N_0}{n_{EnG}} \approx \frac{2N_0}{4n} \approx 8, \tag{D7}$$

where the last equality assumes $n_{EnG} \approx 4n$ (i.e., $n_{GHZ} \approx 2n$) and $N_0/n \approx 15$ to ensure $P_{fail} < 10^{-5}$ [see Fig. 5(b)]. Therefore, for the parameters considered here, approximately $6n$ qubits at each station can achieve $\tau_c \approx 7$ ms, which is sufficient for quantum key generation rate of 100 bits/sec over long distances.

[1] N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, et al., Nature Phys. **3**, 481 (2007).

[3] H. J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[4] L. Childress, J. M. Taylor, A. S. Sorensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).

[5] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).

[6] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, Proc. Natl. Acad. Sci. U. S. A. **104**, 17291 (2007).

[7] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, Phys. Rev. Lett. **98**, 060502 (2007).

[8] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto, e-print arXiv: **0705.4128** (2007).

[9] L. Hartmann, B. Kraus, H. J. Briegel, and W. Dur, Phys. Rev. A **75**, 032310 (2007).

[10] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, U.K; New York, 2000).

[11] W. Dur, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[12] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[13] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[14] E. Knill, Nature (London) **434**, 39 (2005).

[15] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[16] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).

[17] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000).

[18] L. Jiang, J. M. Taylor, A. S. Sorensen, and M. D. Lukin, Phys. Rev. A **76**, 062323 (2007).

[19] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[20] A. M. Steane, Phys. Rev. A **68**, 042322 (2003).

[21] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[22] D. Leibfried, M. D. Barrett, T. Schaetz, J. Britton, J. Chiaverini, W. M. Itano, J. D. Jost, C. Langer, and D. J. Wineland, Science **304**, 1476 (2004).

[23] M. Riebe, H. Haffner, C. F. Roos, W. Hansel, J. Benhelm, G. P. T. Lancaster, T. W. Korber, C. Becher, F. Schmidt-Kaler, D. F. V. James, et al., Nature (London) **429**, 734 (2004).

[24] F. Jelezko, T. Gaebel, I. Popa, M. Domhan, A. Gruber, and J. Wrachtrup, Phys. Rev. Lett. **93**, 130501 (2004).

[25] M. V. G. Dutt, L. Childress, L. Jiang, E. Togan, J. Maze, F. Jelezko, A. S. Zibrov, P. R. Hemmer, and M. D. Lukin, Science **316**, 1312 (2007).

[26] D. Bacon, Phys. Rev. A **73**, 012340 (2006).

[27] S. Perseguers, L. Jiang, N. Schuch, F. Verstraete, M. D. Lukin, J. I. Cirac, and K. G. H. Vollbrecht, Phys. Rev. A **78**, 062324 (2008).

[28] A. M. Steane, Nature (London) **399**, 124 (1999).

[29] D. Gottesman, Ph.D. thesis, Caltech (1997).

[30] P. Aliferis, D. Gottesman, and J. Preskill, Quantum Inf. Comput. **6**, 97 (2006).

[31] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).