Proceedings Paper:
Rey-Domínguez, J. and Razavi, M. (2025) Quantum key distribution over an encoded repeater chain with sequential swapping. In: 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC). 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), 31 Mar - 02 Apr 2025, Nara, Japan. Institute of Electrical and Electronics Engineers (IEEE) , pp. 323-330. ISBN 979-8-3315-3160-7

https://doi.org/10.1109/qcnc64685.2025.00058

Quantum key distribution over an encoded repeater chain with sequential swapping

Javier Rey-Domínguez
School of Electrical and Electronic Engineering
University of Leeds
Leeds, United Kingdom
j.reydominguez@leeds.ac.uk

Mohsen Razavi
School of Electrical and Electronic Engineering
University of Leeds
Leeds, United Kingdom
m.razavi@leeds.ac.uk

***Abstract*—Most current proposals for entanglement distribution networks assume a connection-oriented approach, where resources along a path may be reserved before the start of the session. This strategy, however, does not match the common practice in the existing infrastructure for the Internet, which relies on connectionless packet switching. In our work, we study how a hop-by-hop teleportation can be used to perform entanglement distribution across a network without any prior resource reservation. Specifically, we investigate the attainable secret key generation rate between two users employing this protocol in a repeater chain setup. We analyze this scenario for deterministic quantum repeaters with and without encoding, where we consider a three-qubit repetition code for error detection in the former case. Typical models for the operational errors in these protocols are considered. Our results suggest that the usage of quantum error detection schemes will enable trust-free secret key distribution at distances of interest.**

***Index Terms*—Quantum repeaters, quantum communications, quantum networks, quantum key distribution, quantum cryptography.**

I. Introduction

With certain applications of quantum communications, such as quantum key distribution (QKD) [1]–[3], reaching commercial maturity [4], [5], the interest in the construction of early quantum networks is on the rise. Several examples of such networks have already been deployed [6]–[13]. Nevertheless, most of them rely on trusted nodes, operate only over small to medium distances and/or are *ad hoc* solutions for specific applications (e.g. QKD). In the future, it is expected that a global network of trust-free, general-purpose quantum networks will be deployed in order to offer users around the globe access to useful quantum technologies. Importantly, many challenges have to be solved first in order to realize such a network of networks, often referred to as the quantum Internet [14]–[18].

A key challenge is that of enabling quantum communications at arbitrarily long distances, which has motivated the proposal of different quantum repeater schemes [19]–[21] over the years. Among these, the so-called one-way repeaters [22], [23], which reliably transmit quantum states by using quantum error correction codes, may be able to achieve the highest performance. However, the quantum circuitry required to prepare these codes is out of reach for today's technology. What is more, these schemes often require repeater nodes to be positioned at short distances from each other, which is hard to integrate into the current infrastructure for terrestrial communications. Therefore, early quantum networks will probably make use of repeaters based on entanglement distribution [19], [24], [25], although this will not be without implementation challenges either. Nonetheless, much of the literature concerning networking protocols for these repeaters assumes that resources along a communications path must be allocated to the users beforehand. While this connection-oriented strategy, reminiscent of the classical circuit switching paradigm [26], [27], might offer the best performance for a pair of users, it is not immediately compatible with the connectionless, packet-switched approach used in the Internet and most modern networks [26], [27].

To address the above issue, repeater schemes [28]–[31] in which entanglement is distributed using sequential entanglement swapping [32], [33] have been proposed lately. These solutions appear to be more compatible with the current Internet protocols, as distribution can be achieved without the necessity of establishing any dedicated "virtual circuit". Nonetheless, they suffer from increased waiting times, which decreases the quality of the shared entanglement due to the effects of memory decoherence. This, together with other common sources of error in entanglement distribution schemes, highlights the necessity of error handling mechanisms to be integrated within the protocols. Despite this, most studies so far have focused on probabilistic repeaters [19], [24], and ignored the problem of error propagation. The work in [28] considers entanglement distillation as an error correction mechanism, but this strategy is probabilistic and might face scalability issues not captured in the small topology considered in their work.

In our work, we propose instead a sequential entanglement swapping scheme in which encoded quantum repeaters [25] are employed for *error detection*. We analyze the performance of our scheme in a repeater chain setup running a QKD session, as it has been shown that error detection is sufficient to obtain good secret key rates in similar contexts [34]. For reference, we also study two versions of the sequential scheme without any encoding, where the swapping operation is implemented, in the first case, through a probabilistic, optical Bell state measurement (BSM), and, in the other, through a deterministic, gate-based circuit. We consider typical models for the respective circuits' operational errors and for the mem-

ory decoherence due to waiting times. Our findings suggest that sequential protocols for entanglement distribution based on error detection might soon be compatible with the current infrastructure for the Internet. What is more, intercontinental distances could be achieved in the long-term, given operational errors can be kept under control.

The outline of the paper is the following. We describe the proposed sequential swapping protocol in Section II, both for the unencoded and encoded repeater chains, and model the sources of error that we take into account for our simulations. Then, we go over the analysis of the secret key rate in this setup in Section III. We present our numerical results in Section IV and, lastly, we summarize our work in Section V.

II. Description of the Proposed Setup

In order to measure the potential performance of a sequential entanglement distribution scheme with error detection, we consider here the problem of distributing a secret key, using an entanglement-based QKD protocol [35], over a repeater chain. That is, given two users Alice and Bob (A and B) away from each other at a total distance L, we consider that N_r intermediate nodes are used, each of them connected to two neighboring nodes through quantum and classical channels (in practice, these could be integrated in the same physical channel) of equal length

$$L_0 = \frac{L}{N_r + 1}, \tag{1}$$

as shown in Fig. 1.

For the sake of clarity, we refer to a node as being *downstream* (*upstream*) with respect to another when it is closer to the destination (source). For instance, in Fig. 1 the source A and the node R_2 are the upstream and downstream neighbors of node R_1, respectively.

We assume that each node is capable of distributing entanglement to its neighbors by using a *meet-in-the-middle* scheme [36]–[39]. In this scheme, two participating nodes locally generate entanglement between some quantum memories (which we call communication qubits) and photons. Then, simultaneously, they send the photons through the shared quantum channel, where some intermediate devices, assumed to be equidistant to both nodes, perform a Bell state measurement (BSM). If the BSM is successful, the quantum memories are assumed to be projected into an entangled state, and the intermediate device transmits a success message to the nodes. Otherwise, the nodes simply make subsequent attempts until success. The probability of success for a single attempt can be computed as

$$p_{\text{gen}} = p_{\text{cou}}^2 p_{\text{BSM}} 10^{-\alpha_{\text{ch}} L_0/10}, \tag{2}$$

where p_{cou} is the coupling efficiency of the communication qubits with the optical fibers, and of the fibers with the device implementing the BSM, including any frequency conversion needed along the way; p_{BSM} denotes the success probability of the BSM given that both photons have been received; and α_{ch} is the attenuation constant of the fiber.

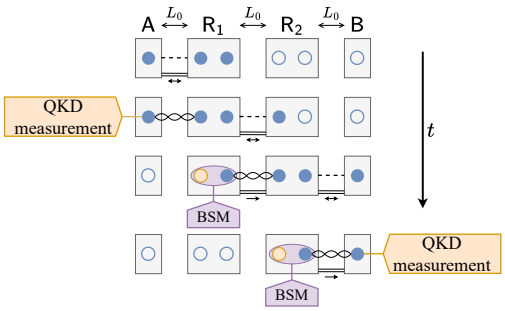

Fig. 1. Operational scheme for the sequential exchange of a single secret key bit over an unencoded repeater chain with $N_r = 2$ repeaters and $N_{\text{comm}} = 1$ communication qubit per node per channel. Filled blue circles represent qubits in use (generating or storing entanglement), empty blue circles represent inactive qubits, and orange circles represent qubits whose state is correlated to the result of the QKD measurement. Dashed lines represent attempts of entanglement generation. Twisted lines represent entanglement. Double solid lines represent classical communications, with the arrows below them indicating its direction.

In order to reduce the waiting time of the entanglement generation procedure, we consider that each node possesses two sets of N_{comm} communication qubits, where all the qubits within each set can be used all at once to generate entanglement with a neighboring node. We assume that rounds of entanglement generation attempts are made concurrently for all communication qubits in these sets, which can be achieved for instance through multiplexing techniques. Moreover, we assume that the generation procedure is only activated on-demand, and hence an initialization signal must be exchanged between nodes to initiate it.

As for the strategy used to distribute the secret key, we consider that the users run an end-to-end session of BBM92 [35], i.e., the entanglement-based alternative to BB84 [40]. In the general setup for this scheme, Alice and Bob use shared pairs of end-to-end entangled qubits and perform single-qubit measurements of their local qubits in either the $\mathcal{Z}$ or $\mathcal{X}$ bases. Then, they discuss the basis they have chosen for each round (each entangled pair) over a classical channel, and discard the measurement results from rounds where their basis choice was different. The results of a subset of the remaining rounds are used to perform parameter estimation to possibly detect the action of an eavesdropper. Finally, the leftover results can be used to distill the shared secret key.

In the following subsections, we give a detailed description of the protocol run by the nodes to distribute entanglement and, eventually, obtain a secret key. Specifically, we describe the considered strategy in Section II-A, and later identify the most relevant sources of error and how we model them in Section II-B.

A. QKD over the sequential repeater chain

Here, we first illustrate the proposed scheme to distribute a single secret bit between two users using two repeater nodes without encoding. As a first step, Alice (A) starts the entanglement generation procedure with R_1. Once a pair of

communication qubits in these nodes are entangled, she immediately performs her QKD measurement in a random basis $\mathcal{Z}$ or $\mathcal{X}$. Simultaneously, R_1 initiates entanglement generation with R_2. Importantly, this can happen at the same time because the meet-in-the-middle generation scheme notifies both nodes of successful generation at the same time. Note that, after Alice's measurement, the state of the upstream communication qubit in node R_1 is correlated with Alice's result but the entanglement itself has been consumed, and therefore Alice is free to use her communication qubit for any other task without affecting the distribution of the secret bit.

Later, when nodes R_1 and R_2 obtain an entangled pair, node R_1 performs a BSM on both of its quantum memories. In the case of the probabilistic repeater chain, the state of both memories is translated into a pair of photons which are interfered at a local, optical BSM. Instead, the gate-based quantum repeaters perform the BSM deterministically through a quantum circuit. In both cases, the results are forwarded through classical signals to R_2. This effectively teleports the state of the upstream communication qubit in R_1 to R_2, up to a Pauli frame adjustment described by the measurement result.

Moreover, node R_2 also begins generating entanglement with Bob (B) as soon as it receives the successful heralding signal, canceling the procedure if a message heralding the failure of the BSM is received. When this final entanglement is achieved, R_2 performs another BSM and repeats R_1's procedure, forwarding any necessary Pauli adjustment and teleporting the state of its upstream communication qubit onto Bob's quantum memory. Concurrently, Bob immediately performs his own QKD measurement on his local qubit. Finally, when he receives the result of the intermediate BSMs (assuming they have all been successful), he performs the necessary adjustments to his result. Crucially, these adjustments can be applied classically, during the sifting stage, by taking into consideration the basis Bob has selected for his measurement. Sifted key bits will then be used in the rest of the QKD protocol.

Moving on to the encoded repeater chain, we consider here repeaters using a typical setup for three-qubit repetition codes [25], [34]. That is, two neighboring nodes can each apply local operations to three quantum memories (which we call memory qubits) and three entangled communication qubits, followed by measurements of the latter, to get a joint entangled state in the memory qubits which we call encoded entanglement. A node sharing encoded entanglement with two neighbors can then locally employ an encoded swapping circuit consisting of three gate-based BSMs to measure his own memory qubits, projecting the two other nodes into an extended encoded entangled state up to an adjustment described by some classical information that the node must transmit through the network. The user nodes may decode the end-to-end encoded entanglement to obtain a single, high quality entangled pair of memory qubits.

With this in mind, we describe our proposed strategy for the distribution of a single secret bit, where we assume that each communication qubit in the nodes is paired with a memory qubit onto which the encoding circuit may be applied. Firstly, Alice (A) uses the communication qubits to generate entanglement with the first repeater, R_1. Once three communication qubits are entangled, she prepares the corresponding memory qubits in the necessary state and applies the encoding and decoding circuits back to back. Moreover, she also performs the QKD measurement over the decoded memory qubit. She classically transmits the results of the encoding procedure to R_1. At the same time as Alice, node R_1 initiates entanglement generation towards the next hop and uses its own encoding circuit, projecting its memory qubits onto a joint state that is correlated to the bit obtained by Alice's measurement. When the results of Alice's measurement arrive to R_1, the repeater can discern if any error has occurred and, if that is the case, choose to drop the distribution attempt, i.e., to stop generating entanglement towards the next hop. The reason for this choice is the insight shown by some studies that most of the secret key rate in QKD over encoded repeater networks comes from rounds with no errors, and so dropping erroneous transmissions early liberates the resources for rounds that have a higher chance of success [34]. If no errors have been detected, the repeater simply completes the entanglement generation procedure, following it up with the application of the encoding and swapping circuits. Any classical information obtained will be forwarded to the next hop, who then behaves similarly. Once Bob is reached, he will immediately use the encoding, decoding and QKD measurements as Alice did, and then classically adjust the result of his QKD bit according to all intermediate measurements.

The complete secret key procedure is executed by repeating the above strategy for as many times as needed. The rounds where a probabilistic BSM has failed or the encoded swapping has detected an error can then be discarded in the sifting stage after some discussion between Alice and Bob.

B. Imperfections and error models

Depending on the underlying hardware used for the entanglement generation scheme, the communication qubits may not be perfectly entangled after a heralding success signal is received. We will assume in general that, after entanglement generation, all communication qubits are left in a Werner state of fidelity F_0 with respect to the Bell state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, which corresponds to a quantum state of the form:

$$W_{F_0} = F_0 \, |\Phi^+\rangle\langle\Phi^+| + \frac{1 - F_0}{3} \left(\mathbb{I} - |\Phi^+\rangle\langle\Phi^+| \right). \quad (3)$$

Moreover, after some time delay τ of being stored in a quantum memory, a state may suffer from quantum decoherence. We model quantum memories as a probabilistic depolarization channel, that is, for a state with density matrix ρ stored for a time τ, each qubit i decoheres independently according to the following transformation:

$$\rho \to e^{-\tau/T_{\text{coh}}} \rho + \left(1 - e^{-\tau/T_{\text{coh}}} \right) \text{Tr}_{\mathsf{i}}(\rho) \otimes \frac{\mathbb{I}_{\mathsf{i}}}{2}, \quad (4)$$

where Tr_{i} denotes the partial trace over qubit i and $\mathbb{I}_{\mathsf{i}}/2$ denotes the maximally mixed state in i.

Another possible source of error is the quantum circuits themselves. All circuits considered for our simulations use exclusively single-qubit and two-qubit gates. In particular, we consider that each gate-based BSM, both the one in the deterministic repeater chain and the three in the encoded swapping for the encoded chain, consists of a single CNOT gate and two single-qubit measurements; the local entanglement to be prepared in the memory qubits before encoding is obtained with the circuit in Ref. [41]; the decoding circuit is the one described in Ref. [34]; and any other operations necessary for the encoded repeater setup follow the design in Ref. [25].

We assume that all single-qubit gates are ideal, since low error rates compared to more complex gates can be achieved in practice. On the other hand, we define β as the probability that the qubits involved in some two-qubit gate with unitary operator go through a quantum depolarizing channel rather than the desired operation being applied. That is, for a gate with ideal unitary operator $\mathrm{U_{ij}}$ being applied to two qubits i and j, the overall quantum state described by density operator ρ undergoes the following transformation:

$$\rho \to (1-\beta)\mathrm{U_{ij}}\rho\mathrm{U_{ij}^{\dagger}} + \beta\,\mathrm{Tr_{ij}}(\rho)\otimes\frac{\mathbb{I}_{\mathrm{ij}}}{4}, \tag{5}$$

where $\mathrm{Tr_{ij}}$ denotes the partial trace over qubits i and j, and $\mathbb{I}_{\mathrm{ij}}/4$ denotes the maximally mixed state in ij.

As for the operation of the optical BSM-mediated swapping in the probabilistic repeater chain, we assume that this operation introduces no errors and has a probability of success p_{BSM}.

Finally, we model single-qubit measurements such that they have a probability δ of returning the wrong result. That is, the POVM in the $\mathcal{Z}$ and $\mathcal{X}$ basis are defined, respectively, as:

$$\begin{cases}\mathrm{P}_0 = (1-\delta)\,|0\rangle\langle 0| + \delta\,|1\rangle\langle 1|\,,\\ \mathrm{P}_1 = (1-\delta)\,|1\rangle\langle 1| + \delta\,|0\rangle\langle 0|\,,\end{cases}\quad\begin{cases}\mathrm{P}_+ = (1-\delta)\,|+\rangle\langle +| + \delta\,|-\rangle\langle -|\,,\\ \mathrm{P}_- = (1-\delta)\,|-\rangle\langle -| + \delta\,|+\rangle\langle +|\,.\end{cases} \tag{6}$$

III. Error and rate analysis

In this section we go over the analysis of the secret key rate for our systems of interest. Specifically, we obtain the secret key rate in the asymptotic regime as the following product:

$$\mathrm{SKR} = R r_{\infty}, \tag{7}$$

where R is the repetition rate, that is, the entanglement distribution rate, and r_{∞} denotes the secret fraction in the asymptotic regime, which can be derived from the security proofs of BBM92 [40], [41] by computing:

$$r_{\infty} = p_{\mathrm{EE}}\max\{0, 1-\mathrm{h}_2(e_{\mathcal{Z}})-\mathrm{h}_2(e_{\mathcal{X}})\}, \tag{8}$$

where p_{EE} denotes the probability of obtaining an end-to-end state (i.e. no BSM has failed in the probabilistic chain, nor has any error been detected in the encoded chain); $\mathrm{h}_2(p) = -p\log_2(p) - (1-p)\log_2(1-p)$; and $e_{\mathcal{Z}}$ ($e_{\mathcal{X}}$) denotes the error rate in the $\mathcal{Z}$ ($\mathcal{X}$) basis.

In terms of repetition rate, we have considered that Alice restarts the entanglement distribution procedure as soon as possible, building up a pipeline of sequential teleportations along the chain. Nevertheless, we observe that whenever a repeater node is generating entanglement downstream, some quantum memories are needed to store the state which is to be teleported. Therefore, the entanglement generation procedure in the upstream direction must run with a reduced subset of quantum memories. While this resource limitation is negligible when considering a large number of quantum memories, it can lead to a staggered pipeline in the more memory-constrained scenarios. For the sake of simplicity, we consider only this latter case, in which each repeater node distributes entanglement in one direction exclusively, hence halving the repetition rate, whose average we compute as:

$$R = \frac{1}{2\,\mathrm{E}\{\tau_{\mathrm{hop}}\}}, \tag{9}$$

where τ_{hop} is the waiting time at each hop, that is, the delay before generating an entangled pair in the unencoded repeater chains, or before generating three entangled pairs when employing encoded repeaters.

Since we are considering an on-demand meet-in-the-middle scheme, which must be initiated by some classical messages sent downstream, the waiting time of the entanglement generation can be computed as:

$$\tau_{\mathrm{hop}} = \frac{L_0}{c}(G_{\mathrm{attempts}}+1), \tag{10}$$

with G_{attempts} being the number of entanglement generation rounds that are necessary to generate the desired entanglement, and c corresponding to the speed of light in fiber, which we take to be the typical value of $c = 200\,000\,\mathrm{km/s}$.

In the case of the repeater chain without encoding, that is, when we only require one entangled pair, we can model G_{attempts} with a geometric distribution characterized by the probability of generating (at least one) entangled pair in a generation round. Therefore, for both deterministic and probabilistic repeaters, its expected value is:

$$\begin{aligned}\mathrm{E}\{G_{\mathrm{attempts}}\}\Big|_{\mathrm{Det}} &= \mathrm{E}\{G_{\mathrm{attempts}}\}\Big|_{\mathrm{Prob}}\\ &= \frac{1}{1-(1-p_{\mathrm{gen}})^{N_{\mathrm{comm}}}}.\end{aligned} \tag{11}$$

Similarly, the number of entanglement generation rounds needed to share the necessary entanglement for encoded repeaters can be expressed as the third order statistic of a set of N_{comm} realizations of a geometric distribution, which has the following average:

$$\begin{aligned}\mathrm{E}\{G_{\mathrm{attempts}}\}\Big|_{\mathrm{Enc}} &= \frac{(N_{\mathrm{comm}}-2)(N_{\mathrm{comm}}-1)}{2-2(1-p_{\mathrm{gen}})^{N_{\mathrm{comm}}}}\\ &\quad - \frac{(N_{\mathrm{comm}}-2)N_{\mathrm{comm}}}{1-(1-p_{\mathrm{gen}})^{N_{\mathrm{comm}}-1}}\\ &\quad + \frac{(N_{\mathrm{comm}}-1)N_{\mathrm{comm}}}{2-2(1-p_{\mathrm{gen}})^{N_{\mathrm{comm}}-2}}.\end{aligned} \tag{12}$$

Finally, we compute the error rates in Eq. (8) by taking into account the error models described in Section II-B. That is, we ignore any disturbance that may be caused by the action of a potential eavesdropper, and worry only about the error rates due to legitimate operation. Then, we can express:

$$\begin{aligned} e_{\mathcal{Z}} &= \mathrm{Tr}\{\mathrm{P}_0^{(\mathsf{A})}\mathrm{P}_1^{(\mathsf{B})}\rho_{\mathrm{EE}}\} + \mathrm{Tr}\{\mathrm{P}_1^{(\mathsf{A})}\mathrm{P}_0^{(\mathsf{B})}\rho_{\mathrm{EE}}\}, \\ e_{\mathcal{X}} &= \mathrm{Tr}\{\mathrm{P}_+^{(\mathsf{A})}\mathrm{P}_-^{(\mathsf{B})}\rho_{\mathrm{EE}}\} + \mathrm{Tr}\{\mathrm{P}_-^{(\mathsf{A})}\mathrm{P}_+^{(\mathsf{B})}\rho_{\mathrm{EE}}\}, \end{aligned} \tag{13}$$

where ρ_{EE} is the end-to-end distributed entangled state right before the QKD measurements in each setup (provided the distribution was successful), and $\mathrm{P}_{\psi}^{(\mathsf{Q})}$ is the POVM element corresponding to measuring state $|\psi\rangle$ in system Q.

In order to obtain ρ_{EE}, we go over the evolution of the quantum state step by step. Firstly, we define ρ_0 as the initial entangled state (after encoding in the case of encoded repeaters) after a single hop. That is [34]:

$$\begin{aligned} \rho_0\Big|_{\mathrm{Det}} &= \rho_0\Big|_{\mathrm{Prob}} = W_{F_0}, \\ \rho_0\Big|_{\mathrm{Enc}} &= \frac{\mathrm{Tr}_{\mathsf{comm}}\left\{\mathrm{M}_{\mathrm{Enc}}\xi_{\mathrm{Enc}}\left(\rho_{\mathsf{mem}}\otimes W_{F_0}^{\otimes 3}\right)\right\}}{p_{\mathrm{Enc}}}, \end{aligned} \tag{14}$$

where $\mathrm{Tr}_{\mathsf{comm}}$ denotes tracing out the communication qubits; $\mathrm{M}_{\mathrm{Enc}}$ denotes the measurement operator that corresponds to the resulting state requiring no adjustment; ξ_{Enc} denotes the transformation of the encoding circuit according to the described error models; ρ_{mem} corresponds to the joint state of the memory qubits following the preparation analyzed in [41]; and

$$p_{\mathrm{Enc}} = \mathrm{Tr}\left\{\mathrm{M}_{\mathrm{Enc}}\xi_{\mathrm{Enc}}\left(\rho_{\mathsf{mem}}\otimes W_{F_0}^{\otimes 3}\right)\right\}. \tag{15}$$

Importantly, it is sufficient to consider the case where no adjustment is necessary because we are considering that all adjustments are applied in the classical domain, without introducing any errors.

To analyze the swapping operation, we first make the observation that the transformation of the optical BSM can be modeled as the ideal operation, i.e. $\beta = \delta = 0$, of the gate-based BSM, provided it was successful. Considering that, we express the quantum state after i sequential swaps along the repeater chain as:

$$\rho_i = \frac{\mathrm{Tr}_{\mathsf{i}}\left\{\mathrm{M}_{\mathrm{Swap}}\xi_{\mathrm{Swap}}\left(\mathrm{D}_{\tau_{\mathrm{hop}}}(\rho_{i-1})\otimes\rho_0\right)\right\}}{p_i}, \tag{16}$$

for $i \leq N_r$, where Tr_{i} denotes tracing out the quantum memories in node $\mathsf{R_i}$ (where the swapping takes place); $\mathrm{M}_{\mathrm{Swap}}$ denotes the measurement operator in which no Pauli frame adjustments are required and, in the case of the encoded chain, no errors were detected; ξ_{Swap} corresponds to the transformation implemented by the swapping quantum circuit; $\mathrm{D}_{\tau_{\mathrm{hop}}}$ corresponds to the memory decoherence of the quantum memories in repeater node $\mathsf{R_i}$ after a delay τ_{hop}; and

$$p_i = \mathrm{Tr}\left\{\mathrm{M}_{\mathrm{Swap}}\xi_{\mathrm{Swap}}\left(\mathrm{D}_{\tau_{\mathrm{hop}}}(\rho_{i-1}),\rho_0\right)\right\}. \tag{17}$$

Once again, we restrict our analysis to the case where no Pauli frame adjustments are needed, since these adjustments are applied ideally. Moreover, for the encoded chain, we consider solely the measurements without errors, since our error detection strategy drops any round in which a different result is read.

p_{cou}	p_{BSM}	α_{ch}	N_{comm}	F_0	β	δ	T_{coh}
0.81	0.5	$0.2\,\mathrm{dB/km}$	6	0.99	0.001	0.001	2 s

TABLE I
PARAMETERS CONSIDERED IN THE SIMULATIONS.

Finally, the end-to-end state can be obtained directly in the case of the unencoded chains, and after the decoding stage. Specifically, we have that:

$$\begin{aligned} \rho_{\mathrm{EE}}\Big|_{\mathrm{Det}} &= \rho_{N_r}\Big|_{\mathrm{Det}}, \\ \rho_{\mathrm{EE}}\Big|_{\mathrm{Prob}} &= \rho_{N_r}\Big|_{\mathrm{Prob}}, \\ \rho_{\mathrm{EE}}\Big|_{\mathrm{Enc}} &= \frac{\mathrm{Tr}_{\mathsf{red}}\left\{\mathrm{M}_{\mathrm{Dcd}}\xi_{\mathrm{Dcd}}\left(\rho_{N_r}\big|_{\mathrm{Enc}}\right)\right\}}{p_{\mathrm{Dcd}}}, \end{aligned} \tag{18}$$

where $\mathrm{Tr}_{\mathsf{red}}$ denotes tracing out the quantum memories storing any redundant entanglement in both end nodes; $\mathrm{M}_{\mathrm{Dcd}}$ denotes the measurement operator in which no errors were detected; ξ_{Dcd} corresponds to the transformation implemented by the decoding quantum circuit; and

$$p_{\mathrm{Dcd}} = \mathrm{Tr}\left\{\mathrm{M}_{\mathrm{Dcd}}\xi_{\mathrm{Dcd}}\left(\rho_{N_r}\Big|_{\mathrm{Enc}}\right)\right\}. \tag{19}$$

Finally, the probability of obtaining an end-to-end entangled state can be obtained for each strategy as:

$$\begin{aligned} p_{\mathrm{EE}}\Big|_{\mathrm{Det}} &= 1, \\ p_{\mathrm{EE}}\Big|_{\mathrm{Prob}} &= \left(p_{\mathrm{BSM}}\right)^{N_r}, \\ p_{\mathrm{EE}}\Big|_{\mathrm{Det}} &= p_{\mathrm{Dcd}}\prod_{i=1}^{N_r}(16p_i), \end{aligned} \tag{20}$$

where the factor 16 comes from the fact that there are 16 measurement results at the swapping stage which detect no errors (but which may require Pauli frame adjustments).

IV. RESULTS

In order to examine the viability of the proposed strategies in the near-to-mid term, we consider a set of parameters as shown in Table I for our numerical calculations. Specifically, we investigate first whether these protocols are compatible with the current infrastructure for classical networks, which often relies on optical fiber links with lengths in the upper range of tens of kilometers, or even upwards of $100\,\mathrm{km}$. Then, we fix a practical value for L_0 and observe how the secret key rate changes with distance, with a special interest in the maximum range at which key distribution is possible.

Given the aforementioned structure, we start by plotting the secret key rate against L_0 for a fixed total distance of $L = 800\,\mathrm{km}$ in Fig. 2. For reference, we also plot the capacity bound for the repeaterless channel, commonly known as the PLOB bound [42], adjusted to a clock rate (repetition rate)

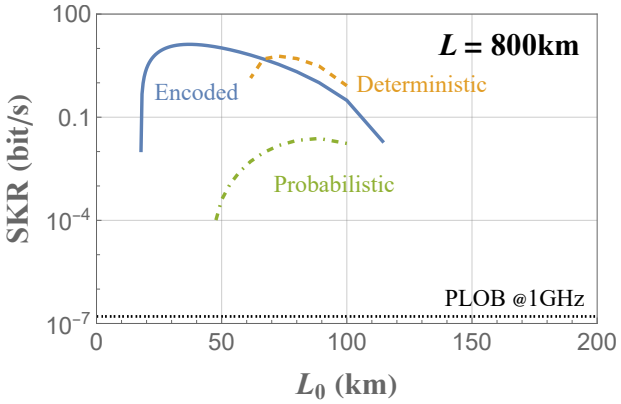

Fig. 2. Secret key rate against the distance between repeaters, L_0, for a total distance between users $L = 800\,\mathrm{km}$. Solid blue line: encoded repeater chain using three-qubit repetition code. Dashed yellow line: unencoded repeater chain with deterministic, gate-based swapping. Dot-dashed green line: unencoded repeater chain with probabilistic, optical-BSM-based swapping. Dotted black line: PLOB bound, given a repetition rate of 1 GHz.

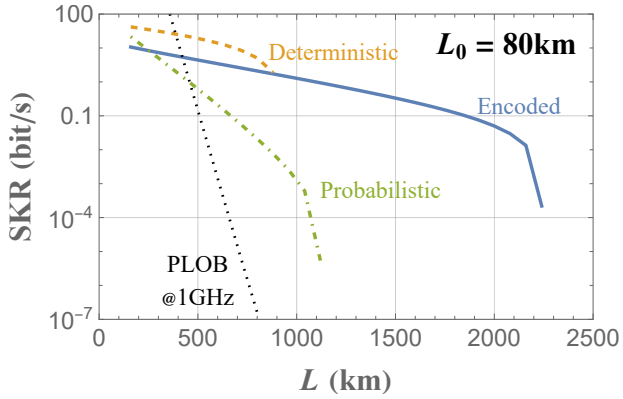

Fig. 3. Achievable secret key rate against the total distance between users, L, in km, for a distance between neighbouring stations of $L_0 = 80\,\mathrm{km}$. Solid blue line: encoded repeater chain using three-qubit repetition code. Dashed yellow line: unencoded repeater chain with gate-based swapping. Dot-dashed green line: unencoded repeater chain with probabilistic swapping. Dotted black line: PLOB bound, given a repetition rate of 1 GHz.

of 1 GHz. As we can see in Fig. 2, the variation of the key rate is not monotonic with L_0. Even though each additional node decreases the average waiting time (and therefore the memory decoherence), any non-ideal implementation will also introduce operational errors. This results in having an optimum value for L_0. It is interesting to note that, for our chosen parameters, the optimal point is found at a larger hop length for the unencoded repeater chains. The reason is that, as expected, any additional swap with these types of repeaters results in the unmitigated propagation and compounding of errors and, in the specific case of deterministic repeaters, also in the introduction of additional noise, which makes them more likely to suffer from heavier diminishing returns. Importantly, however, we notice that the optimal hop length in both unencoded chains is achieved around a similar point of about $80\,\mathrm{km}$, which could indeed be compatible with existing infrastructure. In fact, while the encoded case behaves best at shorter intervals, it is still capable of distilling secret key and convincingly surpassing the PLOB bound for values of L_0 below $110\,\mathrm{km}$, which suggests that encoded repeaters could also be potentially suited for integration in real-life networks in the near future.

Having checked the issue of physical compatibility with the underlying topology, we now move on to check the achievable range of the repeater chains for a practical hop length. In particular, we fix this value to $L_0 = 80\,\mathrm{km}$, which we have found to be close to optimal in the scenario without any coding, and compute the secret key rate against the total distance between users. The results are displayed in Fig. 3.

First of all, we see that the PLOB bound is beaten by all three repeater chains considered, confirming the fact that we are effectively increasing the capacity of the channel with quantum repeaters. Moreover, we see that the unencoded chain with gate-based swapping, labeled as *Deterministic* in Figs. 2 and 3, offers the best performance at short ranges. The reason is that, unlike the encoded chain, only one entangled pair of communication qubits needs to be generated at each hop, therefore reducing the waiting time in the generation procedure and increasing the overall repetition rate of both unencoded strategies. What is more, the SKR attained by the chain of probabilistic repeaters rapidly falls as the distance grows, due to a large number of failure points. Despite this, probabilistic repeaters are capable of distributing a secret key up to about $1100\,\mathrm{km}$, which convincingly surpasses the range of deterministic unencoded repeaters, which only reach distances of around $900\,\mathrm{km}$. This illustrates the advantage of the former strategy, which more heavily relies on the repeat until success paradigm, allowing a lower repetition rate in exchange for a setup which introduces no errors, and thus produces higher-quality entanglement in the rounds where it does not fail.

Finally, we focus on the encoded repeater chain. As mentioned, the requirement of three entangled pairs per hop increases the hop delay and makes this strategy worse in short range but, in exchange, the improved resilience to errors allows this setup to distribute keys up to distances close to $2200\,\mathrm{km}$. For reference, this is more than double what is currently the limit for twin-field QKD protocols [43], and could be sufficient for large scale quantum key distribution at a transnational, or even continental scale. Therefore, it is possible that, if integrated with satellite technology or strategically-placed trusted nodes, a network relying on encoded repeaters following sequential swapping could reach ranges at intercontinental scale.

V. Conclusion

We described strategies for sequential swapping over repeater chains based on three repeater schemes. Specifically, we considered repeaters without encoding where the entanglement swapping was implemented through probabilistic optical BSMs and deterministic gate-based BSMs, as well as encoded

repeaters which employ simple repetition codes for error detection. Then, we investigated the performance of these strategies for QKD applications, assuming the usage of a BBM92 protocol for the purpose of illustration. We analyzed the attainable secret key rates under these scenarios considering typical error models in repeater systems. Preliminary results showed that encoded repeater networks based on the proposed strategies could be compatible with current optical infrastructure. Furthermore, we show that long-range quantum communications could be achieved with relatively few resources if quantum circuits with sufficiently low operational errors can be implemented. This will pave the way for future generations of quantum networks.

ACKNOWLEDGMENTS

We thank Koji Azuma for insightful discussions. We acknowledge support from the European Union's Horizon Europe Framework Programme under the Marie Sklodowska Curie Grant No. 101072637, Project Quantum-Safe Internet (QSI) and the UKRI EPSRC grant No. EP/X028313/1.

DATA AVAILABILITY STATEMENT

All data that support the findings of this study are included within the article (and any supplementary files).

REFERENCES

[1] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, pp. 595–604, Aug 2014.

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, p. 025002, May 2020.

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, pp. 1012–1236, Dec. 2020.

[4] A. Pljonkin and P. K. Singh, "The review of the commercial quantum key distribution system," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 795–799, 2018.

[5] E. Parker, *Commercial and Military Applications and Timelines for Quantum Technology*. Santa Monica, CA: RAND Corporation, 2021.

[6] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," in *Quantum Information and Computation III* (E. J. Donkor, A. R. Pirich, and H. E. Brandt, eds.), vol. 5815, pp. 138 – 149, International Society for Optics and Photonics, SPIE, 2005.

[7] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The secoqc quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, p. 075001, July 2009.

[8] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks," *J. Comput. Secur.*, vol. 18, p. 61–87, Jan. 2010.

[9] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express*, vol. 19, pp. 10387–10409, May 2011.

[10] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," *npj Quantum Information*, vol. 5, p. 101, Nov. 2019.

[11] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Željko Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, "A trusted node–free eight-user metropolitan quantum communication network," *Science Advances*, vol. 6, no. 36, p. eaba0959, 2020.

[12] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, pp. 214–219, Jan. 2021.

[13] M. Alshowkan, B. P. Williams, P. G. Evans, N. S. Rao, E. M. Simmerman, H.-H. Lu, N. B. Lingaraju, A. M. Weiner, C. E. Marvinney, Y.-Y. Pai, B. J. Lawrie, N. A. Peters, and J. M. Lukens, "Reconfigurable quantum local area network over deployed fiber," *PRX Quantum*, vol. 2, p. 040304, Oct. 2021.

[14] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, p. eaam9288, Oct. 2018.

[15] W. Kozlowski and S. Wehner, "Towards large-scale quantum networks," in *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication*, NANOCOM '19, (New York, NY, USA), Association for Computing Machinery, Sept. 2019.

[16] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, "Quantum internet protocol stack: A comprehensive survey," *Computer Networks*, vol. 213, p. 109092, Aug. 2022.

[17] W. Kozlowski, S. Wehner, R. V. Meter, B. Rijsman, A. S. Cacciapuoti, M. Caleffi, and S. Nagayama, "RFC 9340: Architectural Principles for a Quantum Internet," Tech. Rep. 9340, Internet Engineering Task Force, Mar. 2023.

[18] Y. Li, H. Zhang, C. Zhang, T. Huang, and F. R. Yu, "A survey of quantum internet protocols from a layered perspective," *IEEE Communications Surveys & Tutorials*, pp. 1–1, Feb. 2024.

[19] 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, Dec. 1998.

[20] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 78–90, Sept. 2015.

[21] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," *Scientific Reports*, vol. 6, p. 20463, Feb. 2016.

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

[23] 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, June 2014.

[24] 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, Nov. 2001.

[25] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum repeater with encoding," *Phys. Rev. A*, vol. 79, p. 032325, Mar. 2009.

[26] L. L. Peterson and B. S. Davie, *Computer networks : a systems approach*. Boston: Morgan Kaufmann Publishers, fourth ed., 2007.

[27] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*. Boston: Pearson, 7th ed., 2017.

[28] L. Aparicio and R. V. Meter, "Multiplexing schemes for quantum repeater networks," in *Quantum Communications and Quantum Imaging IX* (R. E. Meyers, Y. Shih, and K. S. Deacon, eds.), vol. 8163, p. 816308, International Society for Optics and Photonics, SPIE, 2011.
[29] H. Zhang, Y. Li, C. Zhang, and T. Huang, "Hybrid packet switching assisted by classical frame for entanglement-based quantum networks," Oct. 2023.
[30] Z. Xiao, J. Li, K. Xue, Z. Li, N. Yu, Q. Sun, and J. Lu, "A connectionless entanglement distribution protocol design in quantum networks," *IEEE Network*, pp. 1–1, Oct. 2023.
[31] M. G. de Andrade, E. A. V. Milligen, L. Bacciottini, A. Chandra, S. Pouryousef, N. K. Panigrahy, G. Vardoyan, and D. Towsley, "On the analysis of quantum repeater chains with sequential swaps," May 2024.
[32] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar. 1993.
[33] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""event-ready-detectors" bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, pp. 4287–4290, Dec. 1993.
[34] Y. Jing, D. Alsina, and M. Razavi, "Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective postselection tool," *Phys. Rev. Appl.*, vol. 14, p. 064037, Dec. 2020.
[35] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992.
[36] C. Simon and W. T. M. Irvine, "Robust long-distance entanglement and a loophole-free bell test with ions and photons," *Phys. Rev. Lett.*, vol. 91, p. 110405, Sept. 2003.
[37] X.-L. Feng, Z.-M. Zhang, X.-D. Li, S.-Q. Gong, and Z.-Z. Xu, "Entangling distant atoms by interference of polarized photons," *Phys. Rev. Lett.*, vol. 90, p. 217902, May 2003.
[38] L.-M. Duan and H. J. Kimble, "Efficient engineering of multiatom entanglement through single-photon detections," *Phys. Rev. Lett.*, vol. 90, p. 253601, June 2003.
[39] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, "Design and analysis of communication protocols for quantum repeater networks," *New Journal of Physics*, vol. 18, p. 083015, Aug. 2016.
[40] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sept. 2009.
[41] S. Bratzik, H. Kampermann, and D. Bruß, "Secret key rates for an encoded quantum repeater," *Phys. Rev. A*, vol. 89, p. 032335, Mar 2014.
[42] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, p. 15043, Apr 2017.
[43] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, p. 210801, May 2023.