Optimistic Entanglement Purification in Quantum Networks

Mohammad Mobayenjarihani*, Gayane Vardoyan†, Don Towsley*
*Manning College of Information and Computer Sciences, University of Massachusetts, Amherst
†QuTech and Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology
mobayen@cs.umass.edu, g.s.vardoyan@tudelft.nl, towsley@cs.umass.edu

***Abstract*—Noise and photon loss encountered on quantum channels pose a major challenge for reliable entanglement generation in quantum networks. In near-term networks, heralding is required to inform endpoints of successfully generated entanglement. If after heralding, entanglement fidelity is too low, entanglement purification can be utilized to probabilistically increase fidelity. Traditionally, purification protocols proceed as follows: generate heralded EPR pairs, execute a series of quantum operations on two or more pairs between two nodes, and classically communicate results to check for success. Purification may require several rounds while qubits are stored in memories, vulnerable to decoherence. In this work, we explore the notion of optimistic purification in a single link setup, wherein classical communication required for heralding and purification is delayed, possibly to the end of the process. Optimism reduces the overall time EPR pairs are stored in memory. While this is beneficial for fidelity, it can result in lower rates due to the continued execution of protocols with sparser heralding and purification outcome updates. We apply optimism to the entanglement pumping scheme, ground- and satellite-based EPR generation sources, and current state-of-the-art purification circuits. We evaluate sensitivity performance to a number of parameters including link length, EPR source rate and fidelity, and memory coherence time. We observe that our optimistic protocols are able to increase fidelity, while the traditional approach becomes detrimental to it for long distances. We study the trade-off between rate and fidelity under entanglement-based QKD, and find that optimistic schemes can yield higher rates compared to non-optimistic counterparts, with most advantages seen in scenarios with low initial fidelity and short coherence times.**

I. Introduction

Certain features of quantum mechanics, such as superposition, entanglement, and interference, have the potential to equip us with applications that are not achievable in the classical world. Examples of quantum-enabled advantages include exponential and polynomial algorithmic speedups [1] and provably secure communication [2]. Besides being able to provide the latter, quantum networks [3] can also support distributed quantum computation [4], clock synchronization [5], and quantum sensing [6]. An essential requirement for distributed quantum applications is entanglement of sufficiently high quality shared between nodes. Consequently, one of the main goals of a quantum network is to reliably distribute this resource across a potentially large distance.

A maximally entangled bipartite state (also known as an Einstein-Podolsky-Rosen (EPR) [7] or Bell pair) is a pair of qubits that are entangled such that if we measure the quantum state of one, then we know the exact state of the other. One can use photons to generate and distribute EPR pairs but due to exponential photon loss in optical fiber, the generation of an EPR pair over a long distance poses a significant challenge. Further, due to the No-Cloning Theorem [8], one cannot copy or amplify quantum information at intermediate stations. A solution is to use quantum repeaters [9, 10] that assist with long-distance entanglement generation via entanglement swapping [11, 12].

Fig. 1. Purification example. Two nodes, with three quantum memories each, begin with three imperfect entangled states (red curves, dashed). After purification is carried out (successfully in the example), the nodes are left with a higher-quality single entangled state (red curve, solid).

Imperfect memories, decoherence, and gate noise preclude the distribution of perfect entanglement within a quantum network. In reality, what nodes receive are low quality EPR pairs. Entanglement quality is crucial for distributed quantum applications, *e.g.*, quantum key distribution (QKD) [2, 13], Blind Quantum Computation (BQC) [14], as it can determine not only performance measures specific to such an application, but also the feasibility of carrying it out at all. It is therefore necessary to take heed of and increase this quality when possible. One measure of entanglement quality is *fidelity*, which quantifies the closeness of a given quantum state to some desired state. In quantum networks, a commonly sought-after goal is the distribution of high-fidelity entanglement, where fidelity is computed in reference to one of the four Bell pairs. One way to increase fidelity is through purification [15], which involves the application of local gates and measurements on both ends of a shared entangled state, followed by classical information exchange to communicate success or failure of this probabilistic process. Figure 1 illustrates the method at a high level.

Heralded entanglement purification (HEP) is a necessary mechanism for first-generation quantum networks [16], and yet, practical execution workflows for such protocols still

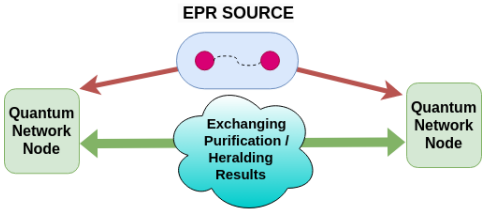


Fig. 2. The setup is comprised of an entanglement source situated between two quantum network nodes. The nodes, capable of performing purification, are equipped with quantum memories that can store entangled states.

require more study. Our work investigates the advantages and limitations of purification for two nodes connected by a single quantum link – a building block for quantum networks – as a means of improving our understanding of how such workflows could be designed and realized on a fully fledged network. Figure 2 illustrates the setting we consider: two nodes are connected via a classical channel used for heralding entanglement and exchanging purification results. Equidistant from both nodes is an entanglement generation source that distributes sub-unit fidelity entanglement. Nodes are equipped with imperfect quantum memories and noisy quantum gates.

Purification can be performed by two nodes that share at least two heralded entangled pairs: one, which we denote as the *main* pair, is kept, while others, often called *sacrificial* pairs, are eventually measured[1] [10, 15, 17, 18]. The traditional way of carrying out purification involves each node performing local operations on its qubits and measuring all sacrificial pairs. Then, based on measurement results, which are exchanged over a classical channel, purification is deemed either successful or unsuccessful. Upon success, the parties may perform further purification on the purified entangled state(s), or allow an application to consume the entanglement. In case of failure, the nodes are forced to discard the main pair and begin the entire process anew. In this paper, we refer to the traditional method as the *baseline protocol (BASE)*.

Classical communication – a required part of purification, is a potentially significant cause of fidelity degradation – the main entangled pairs must remain in noisy storage while awaiting confirmation. If a purification scheme has several rounds (*e.g.*, the pumping scheme [10]), or each purification circuit includes several measurements, then all results must be checked [19], and this further increases the storage time of a pair. Checking purification results costs time at least equal to the data propagation delay on a link. This makes traditional purification impractical for longer distances when the nodes involved are equipped with noisy quantum memories.

A characteristic property of the purification schemes that we study is the reduced wait time of stored entanglement via curtailment of overall classical communication. This reduced storage time in turn impacts the fidelity of entangled pairs by the time they are ready to be consumed by an application. An example of such a scheme is one that foregoes a number of classical communication rounds, continuing on to further purification steps without checking for purification success/failure. This idea was introduced by Hartmann *et al.* in [20]. The authors applied their idea to heralded EPR pairs in the pumping scheme [21], and showed that nodes can be optimistic with respect to purification results, checking purification outcomes only at the end. In this work, we refer to their scheme as the *heralded-optimistic protocol (HOPT)* .

In this work, we further increase optimism, by applying it not only to purification results but also to heralding signals. Intuitively, our optimistic protocol (OPT) can yield even higher fidelities since entanglement spends even less time in quantum memory. Similar to the work in [21], we apply our optimistic approach to the pumping scheme, in ground- and satellite-based setups [22], and show that for large distances and short memory coherence times, our approach increases fidelity while HOPT and BASE can harm fidelity. Nevertheless, a heightened degree of optimism can decrease the overall rate, since more entanglement will be spent on failed purification procedures. Thus, a trade-off exists between rate and fidelity. We study this rate-fidelity trade-off with the secret key rate (SKR) of the BB84 protocol [2, 13]. We evaluate the SKR on the pumping scheme [10], for a range of hardware parameters including the link's entanglement generation rate, the initial fidelity of generated entanglement, and quantum memory coherence time. We also study the effect of distance between nodes on the secret key rate. We also evaluate a current state-of-the-art purification circuit [19] that includes multiple purification checkpoints. We observe that in harsh environments – lower initial (pre-purification) fidelity and short coherence time – optimistic schemes are advantageous for the SKR. In scenarios with higher coherence times, one may switch to the baseline or the heralded-optimistic protocol, and in the case of high initial fidelity, purification may not be necessary at all.

The remainder of this paper is structured as follows: in Section II we discuss related work in purification schemes. In Section III we provide the necessary background in quantum networking. In Section IV, we explain our optimistic approach and methodology. In Section V, we evaluate our optimistic approach on a number of different purification schemes. Finally, in Section VI, we conclude our work and discuss challenges and future directions.

II. Related Work

Entanglement purification was introduced by Bennett *et al.* in [15]. They developed a circuit to improve the fidelity of one Werner state [23] (see Section III for a definition of this state) by sacrificing another state of the same form. In this work, the authors did not evaluate purification performance in terms of rate and fidelity in quantum networks. Further, the effects of memory coherence and entanglement storage time on state fidelity and secret key rate were not considered. Deutsch *et al.* [17] improved previous work by proposing a protocol – often referred to as DEJMPS – which converges faster and requires fewer resources. The scheme does not restrict the initial states to be Werner – in this relaxation, a state can be

[1]More generally, $n \to k$ purification, with $n > k$ initial and k resulting states, is also possible.

any linear combination of Bell basis states. In [17], there is no evaluation of the effect of memory noise on final fidelity. Dür *et al.* [10] proposed the pumping scheme (see Section IV) and the application of purification in quantum repeaters [10, 24]; however, they did not consider quantum memory storage noise in their analysis.

Hartmann *et al.* studied the effect of memory noise on quantum repeaters with purification in [20]. Their noise model accounts for noisy two-qubit gates and dephasing in quantum memories. They proposed nodes perform DEJMPS purification and entanglement swapping without checking results or applying corrections until the very end in a quantum network – a manner of operation they dubbed *blind mode*. In this work, we show that this methodology can exacerbate state fidelity when distances are large and memory coherence times are short. In [21], the authors analyzed the scalability of blind repeaters, while still *heralding* EPR pair generation. In our work, we show that we can also be optimistic about *heralding* signals, thereby improving performance in terms of fidelity and SKR.

All the aforementioned papers apply sub-optimal purification circuits. Nickerson *et. al* introduced the STRINGENT protocol, which outperforms previous protocols in terms of fidelity improvement and quantum state consumption [25]. The effects of waiting times (arising from delays due to classical communication of heralding and purification results) on quantum states were not evaluated, however. Krastanov *et. al* applied a genetic algorithm to optimize purification circuits with respect to resource consumption and output fidelity [19]. The algorithm takes the initial state fidelity and the maximum allowed number of operations as input parameters. In their work, circuit performance evaluation did not consider the effect of classical communication-induced waiting time and storage noise on output fidelity and rate. As the results in [19] are the current state-of-the-art in purification, we apply our optimistic scheme to these circuits and evaluate output fidelity and overall rate, while also incorporating storage noise and classical communication time overhead.

III. Quantum Networking Background

In this section, we provide necessary quantum background for this paper. We begin by introducing EPR pairs, fidelity, quantum channels, the secret key fraction of BB84, quantum repeaters, and purification in more detail. We also explain the entanglement generation setup that we use throughout this work.

A. EPR Pairs

EPR pairs (also known as Bell states [26]) are the following two-qubit quantum states: $|\phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and $|\psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$. A common objective for nodes in a quantum network is to be in possession of one qubit of a Bell state, *e.g.*, $|\phi^{+}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, with the other qubit belonging to another node with whom an application is jointly being carried out.

B. Fidelity and Noise Model

Fidelity is a quantity that measures the closeness of two quantum states. Given a density matrix ρ of a non-maximally entangled bipartite state, the fidelity $F \in [0, 1]$ with reference to $|\phi^{+}\rangle$ is given by[2]

$$F(\rho) = \left\langle \phi^{+} \right| \rho \left| \phi^{+} \right\rangle, \tag{1}$$

clearly, higher values are desirable.

In the real world, quantum gates and quantum memories are imperfect and may inadvertently apply noise to qubits, decreasing their fidelities. In this work, we consider the effect of noisy two-qubit gates on qubits, where noise is modeled by a depolarization channel for quantum gates. Namely, upon application of a two-qubit quantum gate U on the density matrix ρ of an n-qubit system, the transformation is successful with probability p_g, and the two qubits undergoing the transformation are depolarized with probability $1 - p_g$:

$$\rho' = p_g U \rho U^{\dagger} + (1 - p_g) Tr_{i,j}(\rho) \otimes \frac{I}{4}, \tag{2}$$

where ρ' is the resulting density matrix, $Tr_{i,j}$ is a partial trace over qubits i and j that are affected by U, and I is the identity matrix. In this work, we assume that controlled gates (*e.g.*, CNOT and CZ) depolarize both control and target qubits, while single-qubit gates are assumed to be ideal.

Similar to quantum gates, measuring a qubit introduces errors in the output state. Measurement can project an arbitrary state to the correct state with probability p_m or to the wrong state with probability $1 - p_m$. An example is an imperfect projection onto the $|0\rangle$ state:

$$\rho' = p_m \left|0\rangle\langle 0\right| \rho \left|0\rangle\langle 0\right| + (1 - p_m) \left|1\rangle\langle 1\right| \rho \left|1\rangle\langle 1\right|, \tag{3}$$

where ρ and ρ' are the density matrices of the pre- and post-measurement states, respectively.

We also account for the time-dependent noise affecting qubits stored in quantum memories. We assume that this noise is described by two types of errors: amplitude damping and dephasing. Amplitude damping is associated with the parameter T_1, which characterizes how rapidly a state loses its excitation, and dephasing is associated with the parameter T_2 which describes how rapidly a state loses its phase information [27, 28]. The amplitude damping channel acts as follows on the density matrix ρ:

$$\begin{aligned} &\rho \mapsto E_0 \rho E_0^{\dagger} + E_1 \rho E_1^{\dagger}, \\ &E_0 = \left|0\rangle\langle 0\right| + \sqrt{1 - \lambda} \left|1\rangle\langle 1\right|, \\ &E_1 = \sqrt{\lambda} \left|0\rangle\langle 1\right|, \end{aligned} \tag{4}$$

where $\lambda = 1 - e^{-t/T_1}$ and t is the time that the qubit is stored in memory. The stored qubit then goes through a dephasing

[2]We note that another widely accepted definition of fidelity employs a square root.

channel that acts as follows:

$$\rho \mapsto (1-p_z)\rho + p_z Z\rho Z \tag{5}$$
$$p_z = \frac{1}{2}\left(1 - e^{-t/T_2} e^{t/(2T_1)}\right),$$

where Z is the Pauli Z gate and t is the time that the qubit spends in the memory. The composition of amplitude and phase damping as described above is thought to be a generally effective way to model state evolution in quantum memories (see discussion in [29] and references therein).

Another error that can occur is photon loss, one of the main obstacles in a quantum network. The probability of successfully transmitting a photon over optical fiber depends on the fiber transmissivity η_f. The latter decreases exponentially with distance (or link length) l. The probability of transmitting a photon over distance l is

$$\eta_f = 10^{(-\alpha_f \times l)/10}, \tag{6}$$

where α_f is the fiber attenuation coefficient [28].

C. Secret Key Fraction

A direct application of EPR pairs is entanglement-based QKD such as entanglement-based BB84 and the E91 protocol [13]. The secret key rate of BB84 is an increasing function of entanglement rate and fidelity. Recall that purification sacrifices EPR pairs to increase a target state's fidelity. This has the effect of reducing the entanglement generation rate, thus manifesting a rate-fidelity trade-off problem that makes it difficult to decide whether purification is beneficial. Fidelity influences the secret key rate via the secret key fraction, SKF_{BB84}, given by

$$SKF_{BB84} = \max(1 - h(\theta_x) - h(\theta_z), 0) \tag{7}$$
$$\text{where } \theta_x = Tr(\rho X \otimes X), \quad \theta_z = Tr(\rho Z \otimes Z),$$

X, Z are the Pauli X and Z operators, respectively; Tr is the matrix trace, and $h(p) = -p\log(p) - (1-p)\log(1-p)$ is the binary entropy [30]. The secret key rate (SKR) is the production of SKF_{BB84} and the rate of EPR pairs with the density matrix of ρ. We later study the rate-fidelity trade-off of different purification schemes via secret key rate.

D. EPR Pair Generation Model and Purification

Figure 3 illustrates the entanglement generation setup considered in this work: a source located between two network nodes distributes entanglement, with polarization encoding used on the photons of each state [9]. An implementation of this abstracted EPR pair generation scheme is introduced in [31]. In this scheme, each node has an atom in a cavity. We label photons p_1 and p_2 and atoms a_1 and a_2, where each subscript represents the node to which these resources belong. The source distributes states of the form

$$\left|\phi^+\right\rangle_{p_1p_2} = (|00\rangle_{p_1p_2} + |11\rangle_{p_1p_2})/\sqrt{2},$$

where horizontal polarization for p_i is represented by $|0\rangle_{p_i}$ and vertical polarization by $|1\rangle_{p_i}$. Here, we assume each attempt

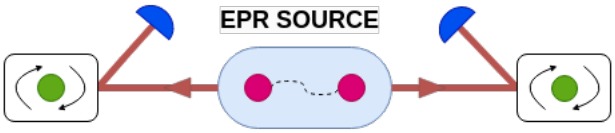


Fig. 3. EPR pair generation setup. The source in the middle sends half of an EPR pair to each quantum network node. Each node entangles its photon with an atom in a cavity and measures the photon, or, in case of failure, heralds photon loss to the other node.

to generate a $\left|\phi^+\right\rangle_{p_1p_2}$ state is successful at the source. Each photon p_i is then transmitted to atom a_i located at node i. Each atom begins in a superposition of the ground and excited states:

$$|+\rangle_{a_i} = (|0\rangle_{a_i} + |1\rangle_{a_i})/\sqrt{2}, \tag{8}$$

where $|0\rangle_{a_i}$ represents the ground state and $|1\rangle_{a_i}$ the excited state. After receiving a photon, each node applies a CZ operation on the photon and the atom, bringing the overall state to

$$|\psi\rangle = 1/2\left|\phi^+\right\rangle_{a_1a_2} \otimes [|00\rangle_{p_1p_2} + |11\rangle_{p_1p_2}] + \tag{9}$$
$$1/2\left|\psi^+\right\rangle_{a_1a_2} \otimes [|00\rangle_{p_1p_2} - |11\rangle_{p_1p_2}].$$

Both nodes then measure their photons in the diagonal basis (*i.e*, $\{|+\rangle, |-\rangle\}$ basis), and apply corrections on the resulting EPR pair based on the measurement results.

In this last stage, upon photon measurement, a node applies the Pauli X gate on its atomic qubit if and only if it observed $|+\rangle$ as the outcome. Once an EPR pair is established, it may be consumed directly by an application, *i.e.*, without any purification; we say in this case that the nodes have performed *direct sharing* of entanglement.

In the introduction, we described purification at a high level; here we elaborate more. As previously mentioned, the purpose of purification is to increase the fidelity of a shared entangled pair between two nodes in a quantum network. Bennett *et al.* introduced the first purification scheme in [15], sometimes called the BBPSSW protocol. In this proposal, one Werner state, *i.e.*, a state that can be expressed as

$$\rho = \frac{4F_0 - 1}{3}\left|\phi^+\right\rangle\!\!\left\langle\phi^+\right| + \frac{1-F_0}{3} I_4, \tag{10}$$

with F_0 its initial fidelity [23], is sacrificed to increase the fidelity of another. In this work, we assume our entanglement generation mechanism generates Werner states as in see (10). Since noisy gates and noisy quantum state storage may result in a mixed state that is not Werner, it is often more accurate to relax the Werner assumption and allow input states to be a linear combination of Bell states.

For such states, the DEJMPS protocol introduced in [17] outperforms BBPSSW. DEJMPS can be applied successively to the same EPR pair to further increase its fidelity. Such a procedure can be carried out by the pumping scheme introduced by Dür *et al.* in [10]. The method increases a

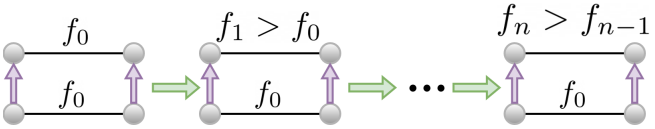


Fig. 4. An illustration of the entanglement pumping purification scheme with $n+1$ purification steps. The nodes begin with two EPR pairs with equal fidelity f_0, and pump the main EPR pair (top) with sacrificial EPR pairs (bottom) until purification stops yielding significant benefits.

main EPR pair's fidelity by consecutively purifying it with another sacrificial EPR pair. In this work, we refer to each purification of the main EPR pair by a sacrificial EPR pair as a *purification step*; Figure 4 illustrates this process that includes $n+1$ purification steps. Note that with the pumping scheme, the fidelity of the main EPR pair ceases to improve after a number of steps that depend on the sacrificial pair fidelity. Finally, as before, nodes exchange purification results via a classical channel to determine if purification was successful or not. If any purification round fails, the entire process must be restarted.

Although the aforementioned purification techniques increase entanglement fidelity, they are not optimized to use as few EPR pairs as possible or to yield the highest fidelity improvement. Optimization techniques can be applied to purification schemes to address these shortcomings. Krastanov *et al.* applied a genetic algorithm to optimize purification circuits in [19]. For the noise model in their generated circuits, they considered imperfect measurement projection as in (3) and depolarization in controlled gates as in (2). Some of these circuits include several projective measurements and require the nodes to classically communicate results as part of the protocol. In our work, we evaluate our optimistic protocol on the traditional pumping scheme, as well as on an optimized circuit from [19].

E. Satellite Setup

While optical fiber transmissivity decreases exponentially with link length, in free space, this decrease follows a polynomial trend. Consequently, the use of satellites [22, 32] and photon transmission through free space have gained significant attention as emerging technologies that appear to make EPR pair distribution over long distances more feasible. Nevertheless, due to longer propagation delays for classical messages, EPR pair distribution with satellite technology potentially introduces longer waiting times for stored quantum states. Stored entangled pairs thus suffer more decoherence, suggesting that such an entanglement generation setting could benefit from a reduction of overall classical communication.

Figure 5 illustrates our satellite setup. We assume two ground stations on Earth are separated by distance d on the order of hundreds of kilometers. The satellite orbits at height h and is equidistant from each ground station, at distance l_o. The satellite generates EPR pairs and sends half of each state toward each ground station. Photons travel a distance l_o through free space of polynomially-decreasing transmissivity, and, once they reach the atmosphere, are subjected to a

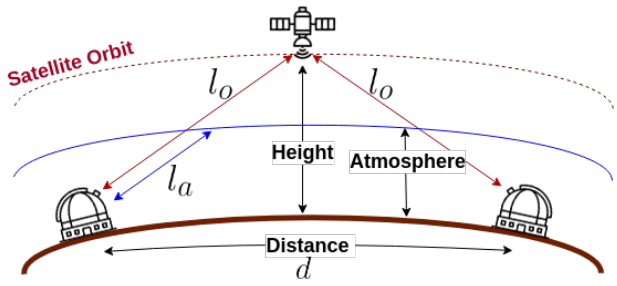


Fig. 5. Satellite setup for generating EPR pairs over long distances.

further decrease in transmissivity – this time exponential with atmosphere attenuation coefficient α_a – for the remaining distance to the ground station, l_a. In this setup, we consider optical links with circular apertures of diameters d_s and d_g for the satellite and ground station, respectively, that operate at wavelength λ. The upper bound for transmissivity between the satellite and the ground station is approximated by

$$\begin{aligned} \eta_o &= \min((\pi d_s^2/4)(\pi d_g^2/4)/(\lambda l_o)^2, 1), \\ \eta_a &= \exp(-\alpha_a l_a), \\ \eta_s &= \eta_o \eta_a, \end{aligned} \tag{11}$$

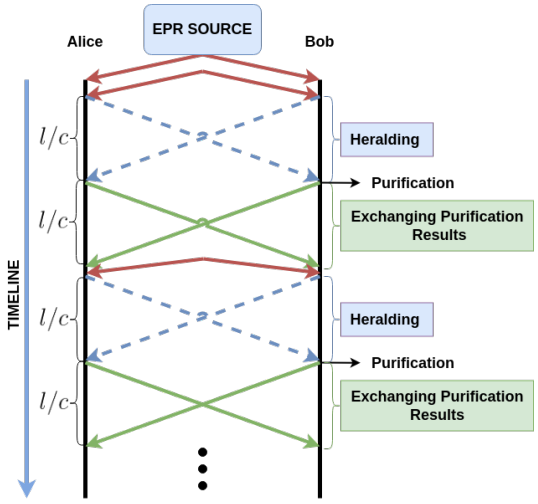
where η_o and η_a are channel transmissivities corresponding to free space and the atmosphere, respectively, and η_s is the overall transmissivity [33, 34].

IV. Purification Protocols

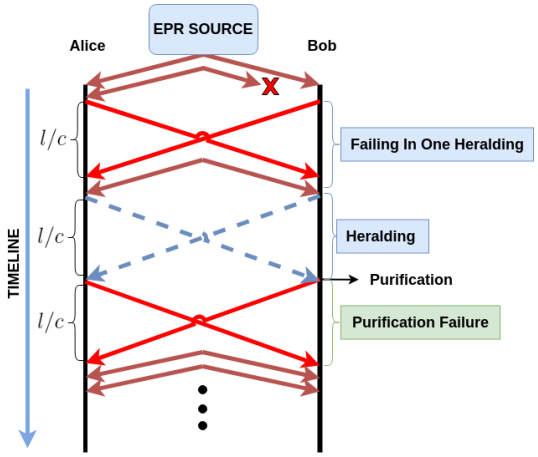
In this section, we first discuss the traditional way of carrying out purification via the pumping scheme. Recall that we refer to this method as the *baseline protocol (BASE)*. We then introduce our *optimistic protocol (OPT)* and finally introduce the *heralded-optimistic protocol (HOPT)* scheme briefly discussed in Sections I and II. Throughout this section, we assume the time it takes for the EPR source to send out a new pair of photons to Alice and Bob is negligible compared to the propagation delay.

A. Baseline Protocol (BASE)

In quantum networks, heralding signals inform nodes of entanglement generation success or failure, and in case of the former, may also be used to provide information about necessary correction operations. Purification, being a probabilistic procedure, also requires classical information exchanges between participating nodes. Figure 6 exemplifies the sequence and timing of events for *baseline* entanglement pumping. Figure 6(a) depicts a successful purification procedure, while Figure 6(b) depicts a purification scenario where failure occurs in heralding and later in purification. In Figure 6, nodes Alice and Bob, each equipped with two quantum memories, are separated by l km. An EPR pair source in the middle of the link sends half of the pair to Alice and the other half to Bob. Alice and Bob both know the rate of the EPR source and have synchronized clocks that tell them when they should expect to receive photons. Thus, upon each clock tick, any party that has

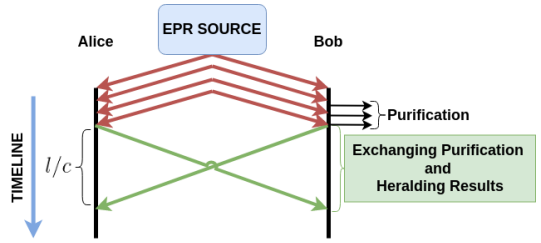


(a) Example execution without failures.

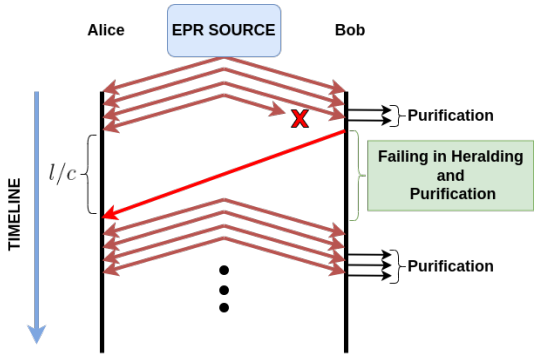


(b) Example with EPR pair generation and purification failures.

Fig. 6. Baseline purification protocol event sequence and timing.



(a) Example execution without failures.



(b) Example with entanglement generation failure. Bob informs Alice, and the process restarts.

Fig. 7. Optimistic purification scheme event sequence and timing.

not received their portion of the EPR pair informs the other party of the failure. At the beginning of protocol, once they receive two EPR pairs, they send heralding signals, which take at least l/c seconds to transmit, where c is the speed of light in optical fiber – 200,000 km/s. Then they perform purification and send the results through a classical channel while waiting for the purification results.

In the following, we go through the timeline presented in Figure 6: The nodes (i) receive their portion of the main entangled pair from the midpoint source, (ii) receive their portion of an auxiliary (sacrificial) entangled pair, (iii) herald entanglement generation success/failure. These steps are repeated until both pairs are successfully received. Next, the nodes (iv) execute a set of quantum gates and measurements on both sides, and (v) exchange measurement results via classical messages. The nodes then compare results, and if purification succeeds, they repeat the process from step (ii) until a desired number of purification steps is achieved. If the results indicate that purification failed, the nodes discard the main pair and restart from step (i). If on the other hand, either party receives no photon, then a failure signal is sent. As soon as two EPR pairs are established, the nodes initiate purification as outlined above.

B. Optimistic Protocol (OPT)

The main idea behind the optimistic protocol is to proceed with all purification steps without waiting for any heralding or consistency checks until the very end. Figure 7 illustrates the optimistic protocol timeline, where Alice and Bob are equipped with the same hardware as in the baseline setup. Panel 7(a) depicts a scenario where all entanglement generation attempts and purification steps are successful, while panel 7(b), presents a scenario in which Bob does not receive his portion of an EPR pair, and the procedure is restarted.

In the following, we go through the timeline of Figure 7: (i) Alice and Bob receive their portion of the main and sacrificial EPR pairs from a midpoint source and each node that receives her/his portion does not wait for the heralding signal and will continue to execute required quantum gates for purification. A node that does not receive one or both photons will inform the other party of failure, causing all pairs to be discarded, and the process to restart. Upon success, the nodes go to step (ii), where they execute local quantum gates and measurements to carry out purification, then they exchange purification results but they do not wait to receive them from the other end. The nodes then (iii) receive the next sacrificial EPR pair and perform another round of purification without waiting for any heralding signals or purification results. As previously, if a node detects entanglement generation failure or purification

failure, it informs its partner, taking the process back to step (i). The nodes repeat step (iii) until a desired number of purification steps are completed. Finally, the nodes (iv) check the final purification measurement outcomes to verify whether the purification steps were successful, going back to step (i) in case a failure occurs. Note that in a setup where the propagation delay is larger than the time takes for the EPR source to send out a new pair of photons to Alice and Bob, end nodes do not check the results at the very end of a purification procedure, but they check the purification/heralding results in time when they are waiting to receive a new EPR pair and determine the next action based on the purification/heralding results.

C. Heralded Optimistic Protocol (HOPT)

We now introduce the *heralded-optimistic protocol (HOPT)* which lies between the optimistic and baseline approaches. In this protocol, Alice and Bob wait only for each others' heralding signals – they are optimistic about purification results and exchange them only at the very end of the process. This protocol was first introduced by Hartmann *et al.* [20], and its distance scalability was later studied in [21].

In this work, we modify the original HOPT protocol such that end-nodes do not wait until the end of the whole purification procedure to exchange the purification results, instead they can exchange the purification results as soon as they measure their qubits. This modification allows Alice and Bob to be informed of purification failures earlier than the original protocol [20] that checks at the very end, thereby preventing them from wasting EPR pairs on a failed purification. Because of early notice of purification failure, this modification improves the overall rate compared to the original protocol. We compare our proposed OPT with the improved HOPT.

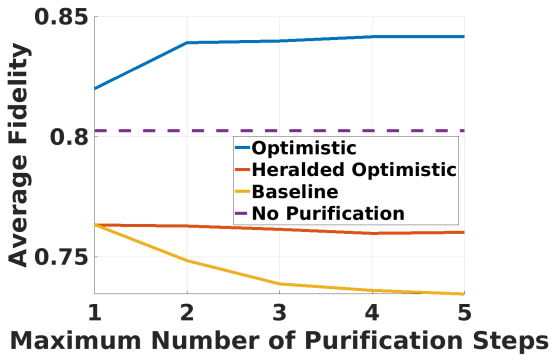
V. Evaluation

In this section, we compare OPT to BASE, HOPT, and sharing EPR pairs with no purification (NOP). We begin with the pumping scheme of [18] for ground- and satellite-based settings, then continue with current state-of-the-art purification circuits of [19] for ground-based EPR generation. For entanglement pumping, we calculate the average rate and fidelity as a function of the total number of purification steps for a fixed hardware parameter set. Additionally, we examine the effect of different memory coherence times and EPR source rates on fidelity. We evaluate the circuit of [19] in a similar manner. Last, we evaluate the QKD performance of different protocols for ground- and satellite-based EPR generation schemes. To do so, we calculate the SKR for ground- and satellite-based setups for all protocols and show that, the optimistic protocol yields the highest SKR when memory coherence times and initial fidelities are low.

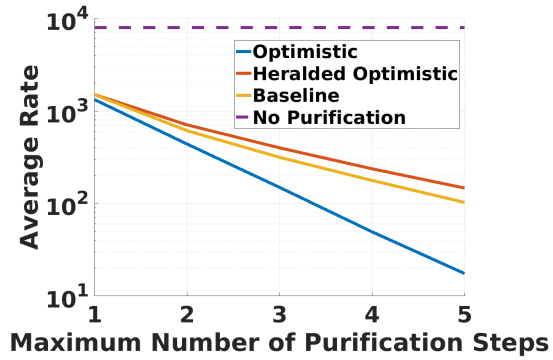
A. Simulation Setup

We evaluate each protocol for different combinations of memory coherence time (T_2), distance (d) between two nodes, initial fidelity (F_0), and EPR source rate (μ). For all cases, we utilize the Monte Carlo method. In our simulations, one simulation iteration starts with no shared entanglement and ends when the protocol successfully purifies a state.

For each combination of values, we perform 10,000 iterations, except for the QKD evaluation on circuits from [19] where we perform 50,000 iterations. Using these simulations, we calculate average fidelity and average rate of resulting en-



(a) Fidelity for different protocols



(b) Rate for different protocols

Fig. 8. Fidelity and rate as functions of purification steps for different purification protocols and direct sharing with no purification, implementing entanglement pumping in ground-based setup. For the EPR source rate (μ) of 1 GHz, the distance (d) of 20 km, and the initial fidelity (F_0) of 0.9.

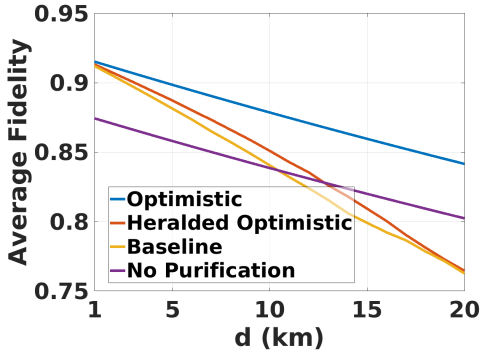


Fig. 9. Fidelity comparison for different protocols for distances (d) from 1 km up to 20 km in ground-based setup. For each data point, we plot the highest fidelity over five successive purification steps. EPR source rate (μ), initial fidelity (F_0), and memory coherence time (T_2) are set to 1 GHz, 0.9, and 1 ms, respectively.

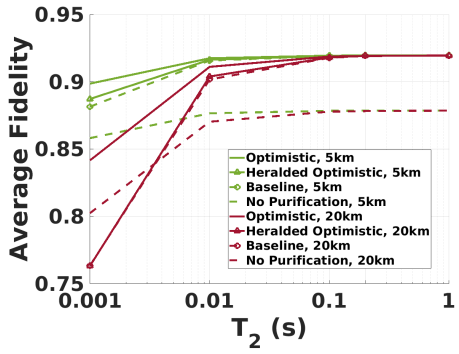


Fig. 10. The effect of memory coherence time (T_2) on average fidelity for entanglement pumping in ground-based setup. Initial fidelity (F_0) and EPR source rate (μ) are set to 0.9 and 1 GHz, respectively. Here, all schemes' fidelities converge for $T_2 \geq 0.1$ s.

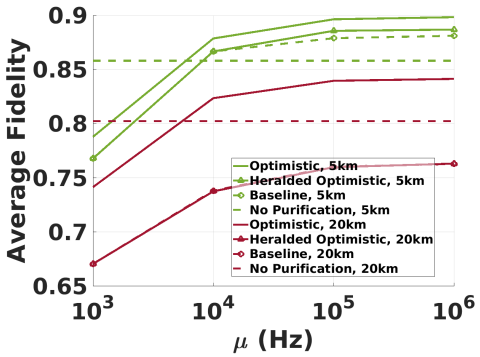
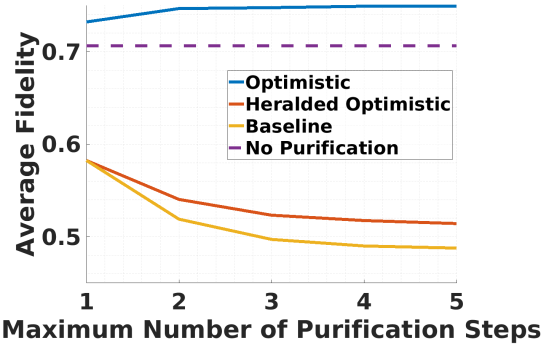
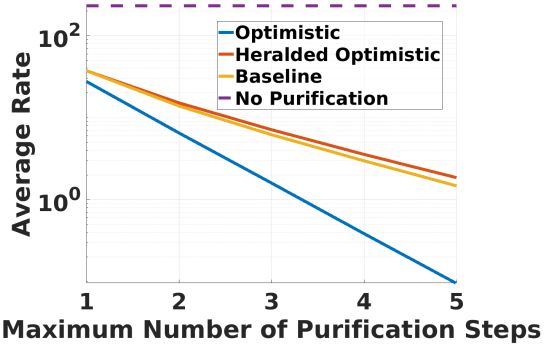


Fig. 11. The effect of EPR source rate (μ) on the average output fidelity in ground-based setup. Initial fidelity (F_0) and memory coherence time (T_2) are set to 0.9 and 1 ms, respectively. Average fidelity increases with rate; the improvement becomes negligible beyond 10^6 Hz.



(a) Fidelity for satellite-based setup



(b) Rate for satellite-based setup

Fig. 12. Fidelity and rate comparison for different protocols implementing entanglement pumping, versus direct sharing without purification in satellite-based setup. Initial fidelity (F_0), EPR source rate (μ), memory coherence time (T_2), and distance (d) are set to 0.9, 1 GHz, 10 ms, and 500 km, respectively.

tanglement, as well as the average SKR. For each simulation, we ascertain that the confidence interval is less than three percent of the average value. For all simulations, the noise parameters for gates, measurements, and memories are the same. For controlled gates, we assume depolarization with parameter $p_g = 0.99$, as per [19] (see (2)). We assume imperfect measurement projection with parameter $p_m = 0.99$, as per [19] (see (3)). For memory noise, we assume amplitude damping (T_1) and dephasing (T_2) (see (4) and (5)). Since in our evaluation, we do not store qubits in memory for a long time (at most, in the regime of milliseconds) and T_1 for amplitude damping is typically on the order of minutes – *e.g.*, [27] reports a T_1 of at least six minutes for Nitrogen-Vacancy (NV) center in diamond carbon atoms – it is not a significant source of noise for a stored qubit. However, we include it in our simulation, setting T_1 to six minutes. On the other hand, T_2 is on the order of milliseconds, and up to seconds as observed in experiments [27, 35]. For T_2, we evaluate our scheme from 0.001s up to 1s, increasing at a logarithmic scale. We set the fiber attenuation coefficient α_f to 0.2 as in [28]. We select initial fidelity F_0 from the range 0.75 to 0.90. μ is selected from the range 1 KHz to 1 GHz [32, 36]. Inter-node distance, d, varies from 1 km up to 20 km.

For the satellite setup, the distance between ground stations d is at most 500 km and the satellite height is set to 400 km, matching the average altitude of the international space station [37]. The atmosphere extinction attenuation, α_a, is set to 0.028125 [33]. Sender and receiver hardware parameters are set to a wavelength $\lambda = 737$ nm, a satellite optical link aperture $d_s = 0.2$ m, and a ground station optical link aperture $d_g = 2$ m [33].

B. Pumping Scheme

In this section, we evaluate the effect of the number of purification steps on average fidelity and rate. Then we study the effect of distance (d) on average fidelity. Next, we study the effect of coherence time (T_2) and EPR source rate (μ) on average fidelity. We compare OPT with HOPT, BASE, and NOP in a ground-based setup. For all cases, we do at most five steps of purification in the pumping scheme as going further does not improve fidelity significantly. We limit the number of memories to two for each node, the required number of memories for each step of the pumping scheme. We set $F_0 = 0.9$, $\mu = 1$ GHz, $T_2 = 0.001$ s, and $d = 20$ km; and plot the results for fidelity and rate in Figure 8(a) and Figure 8(b) respectively. We observe in Figuer 8(a) that OPT outperforms

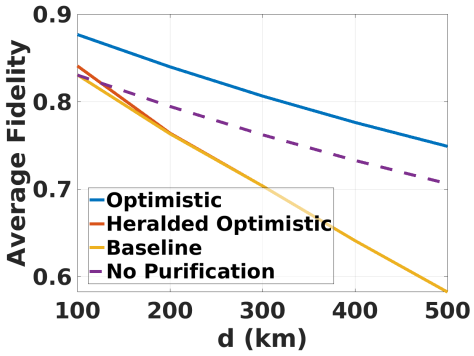


Fig. 13. Fidelity comparison for different protocols implementing entanglement pumping in satellite-based setup, for distance (d) from 100 km up to 500 km. For each data point of purification protocols, we plot the highest fidelity over five purification steps. We set initial fidelity (F_0) to 0.9, EPR source rate (μ) to 1 GHz, and memory coherence time (T_2) to 10 ms.

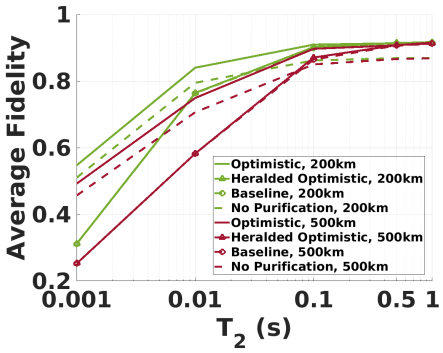


Fig. 14. The effect of memory coherence time (T_2) on the average fidelity in the satellite-based setup. The initial fidelity (F_0) and the EPR source rate (μ) are set to 0.9 and 1 GHz, respectively. Increasing T_2 causes purification protocols to converge to the same fidelity.

all other protocols, while BASE and HOPT yield fidelities lower than NOP. We also observe in Figure 8(b) that OPT yields a lower rate compared to other protocols, however, the higher rates of HOPT and BASE do not compensate for their lower fidelity. Next, we study the effect of d on average output fidelity. We plot the highest fidelity achieved over five steps of purification in Figure 9, note that for OPT, step five always has the highest fidelity, while for BASE or HOPT this may not be the case (see Figure 8(a)). NOP is also included in the plot. We find that OPT outperforms other protocols, and by increasing d, the difference between OPT and other purification protocols increases. Furthermore, an increase in d leads to a longer waiting time, which results in a decrease in the fidelity of both BASE and HOPT, causing them to fall below the fidelity of NOP. Moreover, for larger d, the difference between HOPT and BASE decreases as they perform fewer purification steps and when they decrease to one step their performance becomes the same.

We next analyze the effect of T_2 on the average fidelity of all protocols for $F_0 = 0.9$, $d = 5, 20$ km, and $\mu = 1$ GHz. To investigate the impact of T_2, we compare average

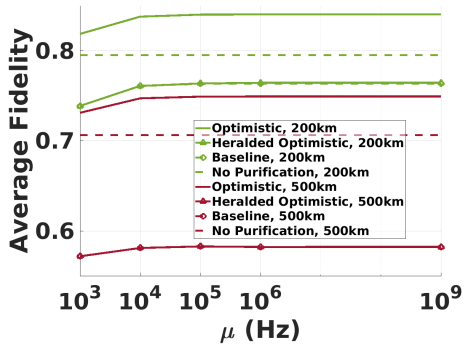
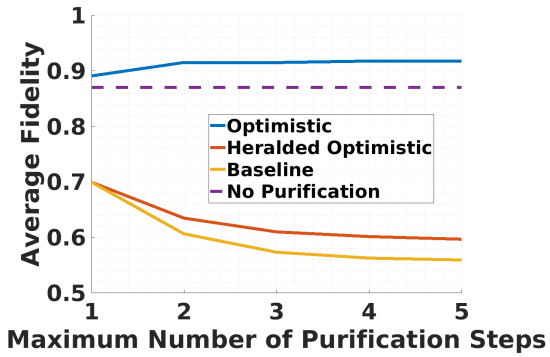
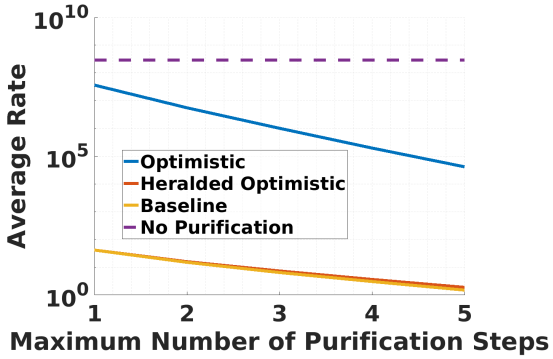


Fig. 15. The effect of EPR source rate (μ) on the average fidelity in satellite-based setup for the initial fidelity (F_0) of 0.9 and the memory coherence time (T_2) of 10 ms.



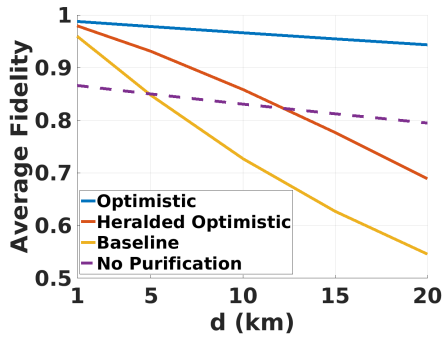
(a) Fidelity for satellite-based setup



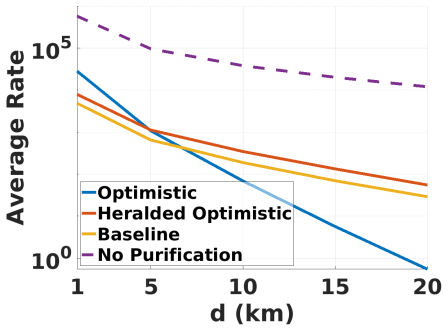
(b) Rate for satellite-based setup

Fig. 16. Fidelity and rate comparison for different protocols without waiting for final confirmation in satellite-based setup. Initial fidelity (F_0), EPR source rate (μ), memory coherence time (T_2), and distance (d) are set to 0.9, 1 GHz, 10 ms, and 500 km, respectively.

output fidelity across all protocols for different values of this parameter. We plot the highest average fidelity that is achieved over the number of purification steps as a function of T_2 for all protocols in Figure 10. We observe that by increasing T_2, all purification protocols converge to the same output fidelity. The distance between nodes plays a role in the convergence behavior: for 5 km, the difference between different protocol fidelities is negligible for T_2 larger than 0.01 s, and for 20



(a) Fidelity for optimized purification circuit.



(b) EPR rate for optimized purification.

Fig. 17. Final fidelity and rate for optimized purification circuit in ground-based setup. For initial fidelity (F_0) of 0.9, a memory coherence time (T_2) of 1ms, and an EPR source rate (μ) of 1 GHz.

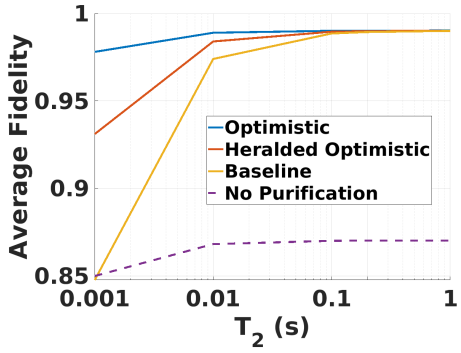


Fig. 18. The effect of memory coherence time (T_2) on the average fidelity in the optimized circuit for ground-based setup. Initial fidelity (F_0), distance (d), and EPR source rate (μ) are set to 0.9, 5 km, and 1 GHz, respectively. Increasing T_2 causes protocols to converge to the same fidelity.

km, when T_2 is larger than 0.1 s.

EPR source rate, μ, also affects output fidelity, and consequently the selection of a purification protocol. We study the effect of μ on average fidelity for $F_0 = 0.9$, $d = 5, 20$ km, and $T_2 = 1$ ms and plot it in Figure 11. As μ decreases, each qubit spends more time in memory and therefore is subjected to decoherence for a longer period. By increasing μ, output fidelity increases; however, when the rate surpasses 1 MHz, output fidelity improvement is negligible for all protocols.

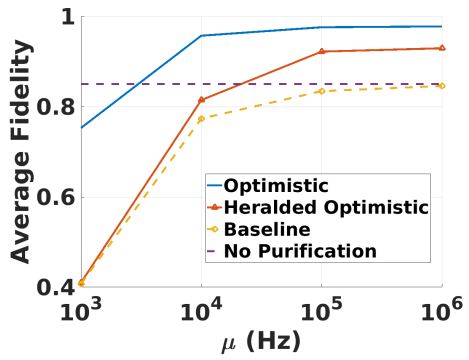


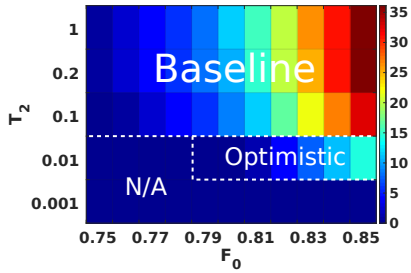
Fig. 19. The effect of source rate on output fidelity for the optimized circuit in ground-based setup. Initial fidelity (F_0), distance (d), and memory coherence time (T_2) are set to 0.9, 5 km, and 1 ms, respectively.

C. Satellite-based EPR Generation Setup

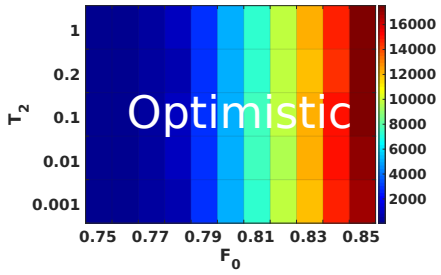
In this section, we evaluate the performance of all purification protocols, implementing a pumping scheme, in a satellite-based setup. Similar to the ground-based setup, the maximum number of purification steps is five, as beyond five steps the fidelity does not improve significantly. We restrict each node to have a maximum of two memories, the minimum number of memories for each step of the pumping scheme. Since the distances between two end nodes are significantly larger compared to the ground-based setup, memory decoherence becomes more severe. Consequently, having a memory with a coherence time of 1 ms significantly reduces overall fidelity due to the large waiting time induced by classical communication; we therefore set the coherence time to 10 ms for fidelity and rate evaluation. We plot the average fidelity as a function of number of purification steps in Figure 12(a) for $F_0 = 0.9$, $\mu = 1$ GHz, $d = 500$ km, and $T_2 = 10$ ms. We observe that OPT provides the highest average fidelity, while HOPT and BASE yield lower fidelities compared to NOP. For the same parameters, we plot the average entanglement rate as a function of number of purification steps in Figure 12(b). We observe that the average entanglement rate under OPT is lower than other protocols; however, the average entanglement rates of HOPT and BASE are lower than NOP. This brings up the rate-fidelity trade-off problem, which we study in Section V-E.

Next, we explore the effect of inter node distance d on average fidelity in Figure 13. We observe that OPT exhibits superior performance compared to the other protocols, and as d increases, the performance gap widens. In addition, an increase in d leads to a longer EPR pairs storage time in noisy memories, which results in a decrease in the performance of BASE and HOPT, causing them to fall below that of NOP.

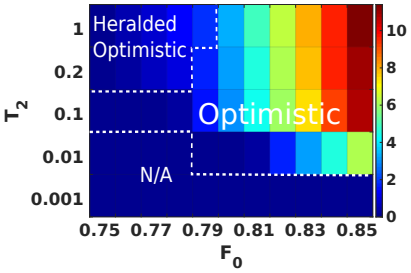
We then analyze the effect of T_2 and μ on the average fidelities of all protocols. To study the effect of T_2, we fix μ to 1 GHz and F_0 to 0.9 for distances of 200 and 500 km. We plot average fidelity as a function of T_2 in Figure 14. We observe that OPT yields the highest fidelity, but that, as



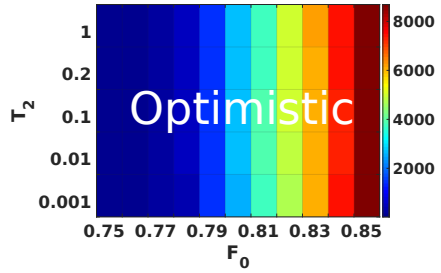
(a) Ground-based setup with 1 KHz EPR source rate (μ) and $d = 20$ km.



(b) Ground-based setup with 1 MHz EPR source rate (μ) and $d = 20$ km.



(c) Satellite-based setup with 1 KHz EPR source rate (μ) and $d = 500$ km.



(d) Satellite-based setup with 1 MHz EPR source rate (μ) and $d = 500$ km.

Fig. 20. Heatmaps for BB84 SKR using the pumping scheme, as a function of T_2 and F_0 for various rates and EPR pair generation setups. We demarcate different regions with dashed lines and label each region to show the best protocol for QKD in that region. The 'N/A' label indicates values of (F_0, T_2) where no positive SKR can be achieved.

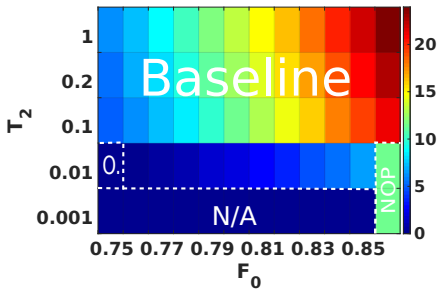
T_2 increases, all purification protocols converge to the same fidelity value and once $T_2 = 0.5\,s$ the difference is negligible. For evaluating the effect μ on the average fidelity, we set $F_0 = 0.9$ and $T_2 = 10$ ms. We plot average fidelity as a function of μ in Figure 15, where we observe that increasing μ improves average fidelity and that after $\mu = 1$ MHz this improvement is negligible.

Our analysis shows a significant decrease in final average fidelities in the satellite scenario due to large classical communication latencies. For example in Figure 12(a), we observe that OPT only increases fidelity to ~ 0.75, which is not suitable for many applications. Some applications such as QKD [2, 13, 30], allow end nodes to measure their qubits as soon as they receive or purify them and continue to receive EPR pairs and/or purify them; and at the meantime, exchange the heralding and purification results to see whether purification was successful or not to filter out failed EPR pairs. We calculate fidelity and the rate with the modification in which end nodes measure their qubits before the final confirmation. We show fidelity and rate as a function of number of purification steps for the same hardware parameters set previously in Figure 16(a) and Figure 16(b), respectively. We observe that average fidelity increases due to the decrease in waiting time. This reduction in wait time also improves the overall rates of all protocols and amplifies OPT's rate to surpass those of BASE and HOPT.

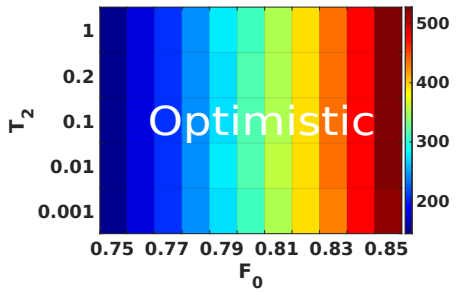
D. Optimized Purification Circuit

We now evaluate the benefit of optimism in the context of a circuit generated by a genetic algorithm introduced in [19]. To do so, we remove amplitude-damping noise in quantum memories since the genetic algorithm of [19] does not support this noise model. However, as discussed previously, we do not expect this to have a significant impact on results since qubits are stored in memories for relatively short periods of time, on the order of milliseconds. For evaluation, we use the genetic algorithm to produce an optimized circuit similar to the original L17 circuit of [19] that has the same performance in terms of fidelity improvement and average number of consumed EPR pairs. The circuit has 17 operations and requires nine EPR pairs and three quantum memories. We selected L17 as the basis of our design since it outperforms the STRINGENT protocol [25]. To evaluate fidelity and rate, we set $\mu = 1$ GHz and $T_2 = 0.001$ s, the same as the ground-based pumping scheme evaluation. Average fidelity and average rate as a function of d can be found in Figure 17(a) and Figure 17(b), respectively. We find that the OPT outperforms other protocols in terms of fidelity. Further, BASE and HOPT yield lower fidelities than NOP for longer distances. OPT achieves higher rates than the other protocols for $d < 4.3$ km.

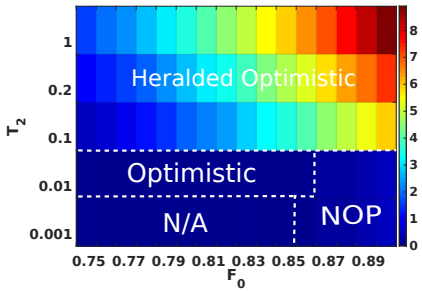
Next, we evaluate the effect of T_2 and μ on average fidelity for a 5 km link. We plot average fidelity as a function of T_2 in Figure 18 for $F_0 = 0.9$ and $\mu = 1$ GHz. As T_2 increases, the fidelity difference between OPT and other protocols decreases, becoming negligible for $T_2 > 0.1$ s. We also study the effect of μ on the average fidelity in Figure 19. We observe that by increasing μ, average fidelity improves, and when μ surpasses 1 MHz, this improvement is negligible.



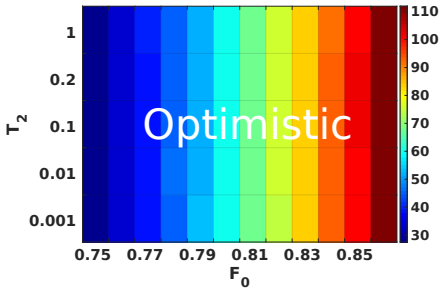
(a) Ground-based setup with 1 KHz EPR source rate (μ) and $d = 20$ km.



(b) Ground-based setup with 1 MHz EPR source rate (μ) and $d = 20$ km.



(c) Satellite-based setup with 1 KHz EPR source rate (μ) and $d = 500$ km.



(d) Satellite-based setup with 1 MHz EPR source rate (μ) and $d = 500$ km.

Fig. 21. Heatmaps for BB84 for an optimized purification circuit as a function of T_2 and F_0 for various rates and EPR pair generation setups. We demarcate different regions with dashed lines and label them to indicate the protocol with the highest QKD SKR for each region. 'NOP' indicates generating secret keys without any purification and 'O.' stands for optimistic. We indicate the regions where SKR is zero with 'N/A' label.

E. Secret Key Rate Evaluation

In this section, we study the rate-fidelity trade-off for all protocols by evaluating their performance in the context of BB84's SKR [30]. In previous descriptions (see Figures 6 and 7), all protocols wait for the final confirmation and purification results, and users do not receive new EPR pairs while waiting. In the case of QKD, we make the modification that end nodes measure the EPR pair of a purification procedure prior to the final confirmation so that the measurement output can be sent along with purification and heralding results; this way, their memories are free and able to receive new EPR pairs, allowing the generation of the next secret key bit to proceed. This modification for QKD yields the greatest benefit where distances between end nodes are large, such as a satellite setting. Similar to previous sections, we study the effect T_2, d, F_0, and μ on the secret key rate in ground-based and satellite-based scenarios. We evaluate QKD performance for the pumping scheme and the optimized purification circuit of [19]. In our simulations, we set d to 20 and 500 km for ground- and satellite-based settings, respectively. We set μ equal to 1 KHz and 1 MHz for both scenarios (for the evaluation of 10 KHz and 100 KHz of pumping scheme see Appendix A). In all cases, we consider a range of values for T_2 and initial fidelity F_0. We display the maximum SKR across all protocols for each combination of F_0 (x-axis) and T_2 (y-axis). We partition different regions of the heatmap with dashed lines to indicate which protocol achieved the maximum SKR for each (F_0, T_2) pair.

For entanglement pumping, presented in Figure 20, our study indicates that at $T_2 = 0.01$, F_0 in the range of 0.79 to 0.85, and $\mu = 1$ KHz, OPT outperforms other variants. Increasing T_2 and F_0 improves the performance of BASE and HOPT (see Figure 20(a) for ground-based setup and Figure 20(c) for satellite-based setup). By increasing μ to 1 MHz, the OPT approach outperforms other approaches for all (F_0, T_2) (see Figure 20(b) for ground-based setup and Figure 20(d) for satellite-based setup).

For the purification circuit of [19], we modified the fitness function of the genetic algorithm to generate a new circuit optimized to the SKR of BB84 (the original algorithm's fitness function aims at maximizing the output fidelity). Moreover, we consider storage noise while generating the circuit. We generate a circuit that uses three memories with T_2 of 0.01, requires five EPR pairs of initial fidelity 0.75, and has at its disposal a 1 KHz EPR source. Figure 21 presents the performance of the circuit for all three purification protocols. Similar to the pumping scheme, we observe that OPT outperforms other protocols when F_0 and T_2 are low(see Figures 21(a) and 21(c) for ground-based and satellite-based setups respectively). It is worth mentioning that our generated circuit outperforms the pumping protocol, in that it is capable of achieving a positive SKR using OPT, in cases where F_0 and T_2 are so low that the pumping protocol can not yield a key. For example, Figure 21(a), for $T_2 = 0.01$ and $F_0 = 0.75$, shows that the

optimized circuit utilizing our optimistic protocol can generate a secret key, while pumping cannot generate any secret key (see SKR for $T_2 = 0.01$ and $F_0 \leq 0.78$ in Figure 20(a)). Similar to the pumping scheme, by increasing the EPR source rate to 1 MHz, the optimistic protocol outperforms other protocols for all (F_0, T_2) (see Figures 21(b) and 21(d) for ground- and satellite-based setups respectively).

VI. Conclusion and Future Directions

In this work, we proposed optimism in purification circuits. Our study showed that being optimistic about heralding signals and purification results can be advantageous to fidelity and, in some hardware parameter regimes, to overall purified EPR rate in classic purification schemes (*e.g.*, entanglement pumping) and optimized purification circuits of [19], compared to baseline (*i.e.*, herald all EPR pairs, check every purification result) and heralded-optimistic (*i.e.*, herald EPR pairs, exchange purification results only while heralding) approaches. We study the effects of memory and gate noise; EPR source rate, and node distance on the performance of our proposed optimistic protocol and compare it to the aforementioned protocols. As part of a future direction, we aim to evaluate our proposed scheme on real hardware such as NV centers in diamond [27, 28, 38]. Moreover, we aim to test our approach on a quantum repeater chain and analyze the effect of different parameters on the output fidelity and overall end-to-end EPR rate. The optimistic approach can also be applied to GHZ state [39] distribution schemes. In [40] authors proposed a procedure to distribute a quadripartite GHZ state between four end nodes. This involves generating four Bell pairs and applying purification, then applying a procedure called fusion (for an optimized version of GHZ distribution and fusion see [41]) to generate the desired quadripartite GHZ. We expect that for such a task, the optimistic approach would benefit both fidelity and rate.

Acknowledgment

This research was supported in part by the NSF grant CNS-1955744, NSF-ERC Center for Quantum Networks grant EEC-1941583, and MURI ARO Grant W911NF2110325.

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, Dec. 1984*, 1984, pp. 175–179.

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

[4] V. S. Denchev and G. Pandurangan, "Distributed quantum computing: A new frontier in distributed systems or science fiction?" *ACM SIGACT News*, vol. 39, no. 3, pp. 77–95, 2008.

[5] E. O. Ilo-Okeke, L. Tessler, J. P. Dowling, and T. Byrnes, "Remote quantum clock synchronization without synchronized clocks," *npj Quantum Information*, vol. 4, no. 1, pp. 1–5, 2018.

[6] Z. Zhang and Q. Zhuang, "Distributed quantum sensing," *Quantum Science and Technology*, vol. 6, no. 4, p. 043001, 2021.

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

[8] J. L. Park, "The concept of transition in quantum mechanics," *Foundations of physics*, vol. 1, no. 1, pp. 23–33, 1970.

[9] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 78–90, 2015.

[10] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Physical Review A*, 1999.

[11] 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," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

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

[13] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[14] P. Arrighi and L. Salvail, "Blind quantum computation," *International Journal of Quantum Information*, vol. 4, no. 05, pp. 883–898, 2006.

[15] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical review letters*, vol. 76, no. 5, p. 722, 1996.

[16] 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, no. 1, p. 20463, 2016.

[17] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Physical review letters*, 1996.

[18] W. Dür and H. J. Briegel, "Entanglement purification and quantum error correction," *Reports on Progress in Physics*, vol. 70, no. 8, p. 1381, 2007.

[19] S. Krastanov, V. V. Albert, and L. Jiang, "Optimized entanglement purification," *Quantum*, vol. 3, p. 123, 2019.

[20] L. Hartmann, B. Kraus, H.-J. Briegel, and W. Dür, "Role of memory errors in quantum repeaters," *Physical Review A*, vol. 75, no. 3, p. 032310, 2007.

[21] M. Razavi, M. Piani, and N. Lütkenhaus, "Quantum repeaters with imperfect memories: Cost and scalability," *Physical Review A*, vol. 80, no. 3, p. 032301, 2009.

[22] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[23] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," *Physical Review A*, vol. 40, no. 8, p. 4277, 1989.

[24] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[25] N. H. Nickerson, Y. Li, and S. C. Benjamin, "Topological quantum computing with a very noisy network and local error rates approaching one percent," *Nature communications*, vol. 4, no. 1, p. 1756, 2013.

[26] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.

[27] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpędek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho *et al.*, "A link layer protocol for quantum networks," in *Proceedings of the ACM Special Interest Group on Data Communication*, 2019, pp. 159–173.

[28] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk *et al.*, "Netsquid, a network simulator for quantum information using discrete events," *Communications Physics*, 2021.

[29] T. Coopmans, "Tools for the design of quantum repeater networks," Ph.D. dissertation, 2021.

[30] G. Murta, F. Rozpędek, J. Ribeiro, D. Elkouss, and S. Wehner, "Key rates for quantum key distribution protocols with asymmetric noise," *Physical Review A*, vol. 101, no. 6, p. 062321, 2020.

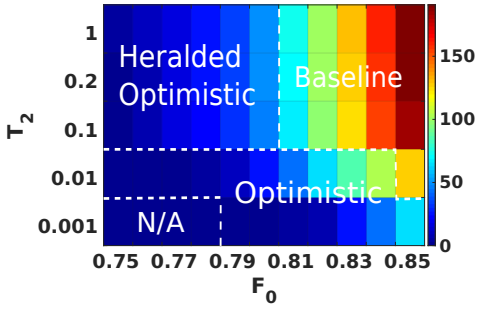
[31] P. Dhara, S. J. Johnson, C. N. Gagatsos, P. G. Kwiat, and S. Guha, "Heralded multiplexed high-efficiency cascaded source of dual-rail entangled photon pairs using spontaneous parametric down-conversion," *Physical Review Applied*, vol. 17, no. 3, p. 034071, 2022.

[32] S. Khatri, A. J. Brady, R. A. Desporte, M. P. Bart, and J. P. Dowling, "Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet," *npj Quantum Information*, vol. 7, no. 1, pp. 1–15, 2021.

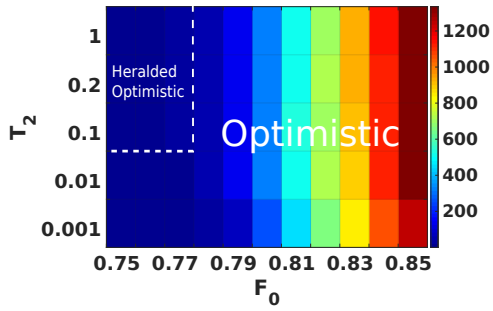
[33] N. K. Panigrahy, P. Dhara, D. Towsley, S. Guha, and L. Tassiulas, "Optimal entanglement distribution using satellite based quantum networks," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2022, pp. 1–6.
[34] J. Shapiro, S. Guha, and B. Erkmen, "Ultimate channel capacity of free-space optical communications," *Journal of Optical Networking*, vol. 4, no. 8, pp. 501–516, 2005.
[35] M. Pompili, S. L. Hermans, S. Baier, H. K. Beukers, P. C. Humphreys, R. N. Schouten, R. F. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse *et al.*, "Realization of a multinode quantum network of remote solid-state qubits," *Science*, vol. 372, no. 6539, pp. 259–264, 2021.
[36] Y. Cao, Y.-H. Li, W.-J. Zou, Z.-P. Li, Q. Shen, S.-K. Liao, J.-G. Ren, J. Yin, Y.-A. Chen, C.-Z. Peng *et al.*, "Bell test over extremely high-loss channels: towards distributing entangled photon pairs between earth and the moon," *Physical review letters*, vol. 120, no. 14, p. 140405, 2018.
[37] G. H. Kitmacher, *Reference guide to the international space station*, 2006, no. NASA/SP-2006-557.
[38] L. Childress and R. Hanson, "Diamond nv centers for quantum computing and quantum networks," *MRS bulletin*, vol. 38, no. 2, pp. 134–138, 2013.
[39] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," in *Bell's theorem, quantum theory and conceptions of the universe*. Springer, 1989, pp. 69–72.
[40] N. H. Nickerson, Y. Li, and S. C. Benjamin, "Topological quantum computing with a very noisy network and local error rates approaching one percent," *Nature communications*, vol. 4, no. 1, pp. 1–5, 2013.
[41] S. de Bone, R. Ouyang, K. Goodenough, and D. Elkouss, "Protocols for creating and distilling multipartite GHZ states with Bell pairs," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–10, 2020.

APPENDIX A

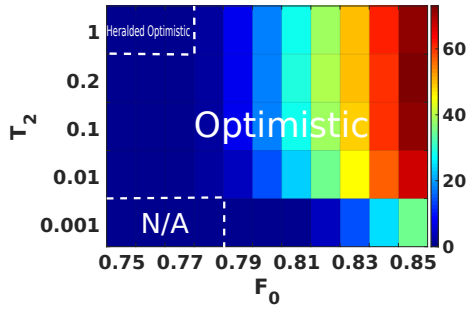
In this appendix, we plot the SKR for purification protocols with an EPR source rate (μ) of 10 and 100 KHz using a pumping scheme for ground-based and satellite-based setups. The results are shown in Figure 22 in the form of a heatmap plot (see Section V-E). We observe that by increasing μ, OPT outperforms other protocols in more regions. The reason behind this improvement is that with a higher μ, OPT can receive more EPR pairs. In contrast, HOPT and BASE cannot, because they have to wait for more confirmation throughout the process (HOPT for heralding, and BASE for heralding and purification confirmation), preventing them from receiving and performing operations on EPR pairs.



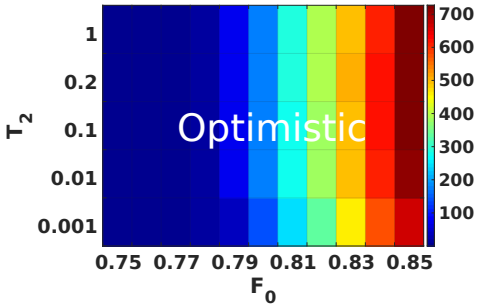
(a) Ground-based setup with 10 KHz EPR source rate (μ) and $d = 20$ km.



(b) Ground-based setup with 100 KHz EPR source rate (μ) and $d = 20$ km.



(c) Satellite-based setup with 10 KHz EPR source rate (μ) and $d = 500$ km.



(d) Satellite-based setup with 100 KHz EPR source rate (μ) and $d = 500$ km.

Fig. 22. Heatmaps for BB84 SKR using the pumping scheme, as a function of T_2 and F_0 for various rates and EPR pair generation setups. We demarcate different regions with dashed lines and label each region to show the best protocol for QKD in that region. The 'N/A' label indicates values of (F_0, T_2) where no positive SKR can be achieved.