Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission

Filip Rozpędek,[1,2,*,†] Raja Yehia,[1,3,†] Kenneth Goodenough,[1,2,†] Maximilian Ruf,[1,2] Peter C. Humphreys,[1,2]
Ronald Hanson,[1,2] Stephanie Wehner,[1,2] and David Elkouss[1]

[1] *QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[2] *Kavli Institute of Nanoscience, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[3] *Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris 6, F-75005 Paris, France*

(Received 28 September 2018; revised manuscript received 4 February 2019; published 22 May 2019)

Quantum channels enable the implementation of communication tasks inaccessible to their classical counterparts. The most famous example is the distribution of secret key. However, in the absence of quantum repeaters, the rate at which these tasks can be performed is dictated by the losses in the quantum channel. In practice, channel losses have limited the reach of quantum protocols to short distances. Quantum repeaters have the potential to significantly increase the rates and reach beyond the limits of direct transmission. However, no experimental implementation has overcome the direct transmission threshold. Here, we propose three quantum repeater schemes and assess their ability to generate secret key when implemented on a setup using nitrogen-vacancy (NV) centers in diamond with near-term experimental parameters. We find that one of these schemes—the so-called single-photon scheme, requiring no quantum storage—has the ability to surpass the capacity—the highest secret-key rate achievable with direct transmission—by a factor of 7 for a distance of approximately 9.2 km with near-term parameters, establishing it as a prime candidate for the first experimental realization of a quantum repeater.

DOI: 10.1103/PhysRevA.99.052330

I. INTRODUCTION

There exist communication tasks for which quantum resources allow for qualitative advantages. Examples of such tasks include clock synchronization [1–4], distributed computation [5], anonymous information transmission [6,7], and the distribution of secret key [8,9]. While some of these tasks have been implemented over short distances, their implementation over long distances remains a formidable challenge.

One of the main hurdles for long-distance quantum communication is the *loss* of photons, whether it is through fiber or free space. Unfortunately, the no-cloning theorem [10] makes the amplification of the transmitted quantum states impossible. For tasks such as the generation of a shared secret key or entanglement, this limits the corresponding generation rate to scale at best linearly in the transmissivity η of the fiber joining two distant parties [11–13].

Luckily, while quantum mechanics prevents us from overcoming the effects of losses through amplification, it is possible to do so using repeater stations [14–16]. Formally, we call a quantum repeater a device that allows for better performance than can be achieved over the direct communication channel alone [17]. This performance is measured differently for different tasks, such as secret-key generation or transmission of quantum information. Consequently, the optimal performance that can be achieved over the direct channel without using repeaters, called the channel capacity, is also different for these two tasks. Here we will assess our proposed repeater schemes for the task of secret-key generation, as it is easier to realize experimentally. Our formal definition of a repeater—as opposed to a relative definition with respect to some setup of reference—endows the demonstration of a quantum repeater with a fundamental meaning that cannot be affected by future technological developments in the field.

However, a successful experimental implementation of a quantum repeater has not yet been demonstrated. This is mainly due to the additional noise introduced by such a quantum repeater. While the implementation of a single quantum repeater does not necessarily imply that that setup can be scaled up to a larger number of repeater nodes (due to the effects of noise and decoherence), the first demonstration of a functioning quantum repeater will form an important step toward practical quantum communication and the quantum internet [18].

A multitude of quantum repeater schemes have been put forward [15,19–29], each with their own strengths and weaknesses. It should be noted here that most of the earlier repeater proposals aim at overcoming transmission losses using heralded entanglement generation and compensate for noise arising in quantum memories using two-way entanglement distillation. However, some of the schemes, e.g., those in Refs. [24–26], introduce error correction to overcome operational errors while those in Refs. [27–29] use error correction also for dealing with losses. Although *a priori* it is not clear which of those schemes will perform best with current or near-term experimental parameters, it is clear that operating on large number of qubits in each repeater node, necessary for the implementation of error correction, is a significant experimental challenge. Therefore, it is not expected that the first realizations of quantum repeaters will be based on large

[*] f.d.rozpedek@tudelft.nl.

[†] These authors contributed equally to this work.

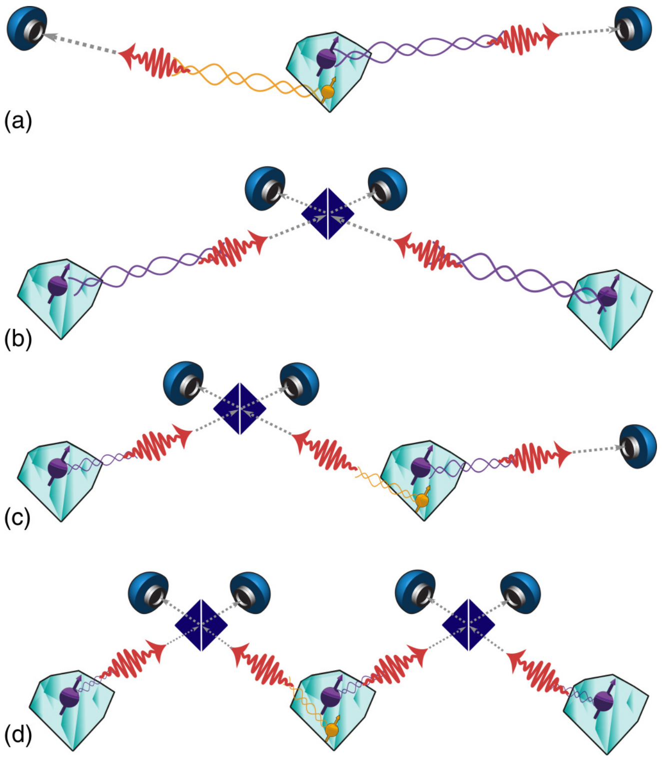

FIG. 1. Schematic overview of the four quantum repeater schemes assessed in this paper. From top to bottom: the Single Sequential Quantum Repeater (SiSQuaRe) scheme (a), the single-photon scheme (b), the Single-Photon with Additional Detection Setup (SPADS) scheme (c), and the Single-Photon Over Two Links (SPOTL) scheme (d). The purple particles represent NV electron spins capable of emitting photons (red wiggly arrows) while the yellow particles represent carbon ^{13}C nuclear spins. Dark blue squares depict the beam splitters used to erase the which-way information of the photons, followed by blue photon detectors. For more details on the different proposals, see Sec. II.

error-correction schemes. Hence, here we will focus on simple schemes without encoding, leaving out also entanglement distillation. We will discuss entanglement distillation in the context of our findings in the discussion at the end of the article.

In this work, we propose three such schemes and together with the fourth scheme analyzed before [17,30], we assess their performance for generating secret key. We consider their implementation based on nitrogen-vacancy centers in diamond (NV centers), a system which has properties making it an excellent candidate for long-distance quantum communication applications [31–40].

The four considered schemes are the following: the "single sequential quantum repeater node" (first proposed and studied in Ref. [30], then further analyzed in Ref. [17]), the single-photon scheme (proposed originally in the context of remote entanglement generation [41], also studied in the context of secret-key generation without quantum memories [42]), and two schemes which are a combination of the first two. See Fig. 1 for a schematic overview of the repeater proposals considered in this work.

We compare the *secret-key rate* of each of these schemes to the highest theoretically achievable secret-key rate using direct transmission, the *secret-key capacity of the pure-loss channel* [13]. We show that one of these schemes, the *single-photon scheme*, can surpass the secret-key capacity by a factor of 7 for a distance of ≈9.2 km with near-term parameters. This shows the viability of this scheme for the first experimental implementation of a quantum repeater.

In Sec. II, we discuss and detail the different repeater proposals that will be assessed in this work. In Sec. III, we expand on how the different components of the repeater proposals would be implemented experimentally. Section IV details how to calculate the secret-key rate achieved with the quantum repeater proposals from the modeled components. In Sec. V, we discuss how to assess the performance of a quantum repeater. The comparison of the different repeater proposals is performed in Sec. VI, which allows us to conclude with our results in Sec. VII. The numerical results of this article were produced with a PYTHON script and a MATHEMATICA script, which are available upon request.

II. QUANTUM REPEATER SCHEMES

In the following section, we present the quantum repeater schemes that will be assessed in this work. All these schemes use NV-center-based setups which involve memory nodes consisting of an electron spin qubit acting as an optical interface and possibly an additional carbon ^{13}C nuclear spin qubit acting as a long-lived quantum memory. Specifically, the optical interface of the electron spin allows for the generation of spin-photon entanglement, where the photonic qubits can then be transmitted over large distances. The carbon nuclear spin acts as a long-lived memory but can be accessed only through the interaction with the electron spin. Here, we briefly go over all the proposed schemes, consider why they are interesting from an experimental perspective, and discuss their advantages and disadvantages.

A. Single sequential quantum repeater (SiSQuaRe) scheme

The first scheme that we discuss here was proposed and analyzed in Ref. [30] and further studied in Ref. [17]. The scheme involves a node holding two quantum memories in the middle of Alice and Bob (see Fig. 2). This middle node tries to send a photonic qubit, encoded in the time-bin degree of freedom, that is entangled with one of the quantum memories,

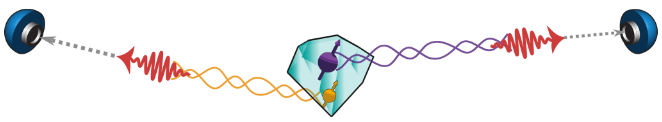

FIG. 2. Schematic overview of the SiSQuaRe scheme. The NV center in the middle first attempts to generate an entangled photon-electron pair, after which it tries to send the photon through the fiber to Alice. Alice then directly measures the photon, using either a BB84 or a six-state measurement. Then after the state of the electron spin is swapped to the carbon ^{13}C nuclear spin, the same is attempted on Bob's side. After both Alice and Bob measured a photon, a Bell-state measurement is performed on the two quantum states held by the middle node. Alice and Bob can use their measurement outcomes together with the outcome of the Bell-state measurement to generate a single raw bit of key.

through a fiber to Alice. This is attempted repeatedly until the photon successfully arrives, after which Alice performs a BB84 [8] or a six-state measurement [43,44]. By performing such a measurement, the quantum memory will be steered into a specific state depending on the measurement outcome. Now the same is attempted on Bob's side. After Bob has measured a photon, the middle node performs a Bell-state measurement on both quantum memories. Using the classical information of the outcome of the Bell-state measurement, Alice and Bob can generate a single raw bit. In our model, the middle node has only one photonic interface (corresponding to the NV electron spin) and hence has to send the photon sequentially first to Alice and then to Bob.

While trying to send a photon to Bob, the state stored in the middle node will decohere. A possible way to compensate for the effects of decoherence is to introduce a so-called *cut-off* [17]. The cut-off is a limit on the number of attempts we allow the middle node to try and send a photon to Bob. If the cut-off is reached, the stored state is discarded, and the middle node attempts again to send a photon to Alice. Since the scheme starts from scratch, we are effectively trading off the generation time versus the quality of our state. By optimizing over the cut-off, it is possible to considerably increase the distance over which secret key can be generated [17].

Setup and scheme

We will now describe the exact procedure of this scheme, when Alice and Bob use a nitrogen-vacancy center in diamond as quantum memories and as a photon source. The scheme that we study is the following:

(1) The quantum repeater attempts to generate an entangled qubit-qubit state between a photon and its electron spin, and sends the photon to Alice through a fiber.

(2) The first step is repeated until a photon arrives at Alice's side, after which she performs a BB84 or a six-state measurement. The electron state is swapped to the carbon spin.

(3) The quantum repeater attempts to do the same on Bob's side while the state in the carbon spin is kept stored. This state will decohere during the next steps.

(4) Repeat until a photon arrives at Bob's side, who will perform a BB84 or a six-state measurement. If the number of attempts n reaches the cut-off n^*, restart from step 1.

(5) The quantum repeater performs a Bell-state measurement and communicates the result to Bob.

(6) All the previous steps are repeated until sufficient data have been generated.

B. The single-photon scheme

Cabrillo *et al.* [41] devised a procedure that allows for the heralded generation of entanglement between a separated pair of matter qubits (their proposal discusses specific implementation with single atoms, but the scheme can also be applied to other platforms such as NV centers or quantum dots) using linear optics. For the atomic ensemble platform, this scheme also forms a building block of the DLCZ quantum repeater scheme, named after the authors Duan, Lukin, Cirac, and Zoller [20]. Here, we will refer to this scheme as a single-photon scheme as the entanglement generation is heralded by a detection of only a single photon. This requirement of successful transmission of only a single photon from one node makes it possible for this scheme to qualify as a quantum repeater (see below for more details).

The basic setup of the single-photon scheme consists of placing a beam splitter and two detectors between Alice and Bob, with both parties simultaneously sending a photonic quantum state toward the beam splitter. The transmitted quantum state is entangled with a quantum memory, and the state space of the photon is spanned by the two states corresponding to the presence and absence of a photon. Immediately after transmitting their photons through the fiber, both Alice and Bob measure their quantum memories in a BB84 or six-state basis (see the discussion of which quantum key distribution protocol is optimal for each scheme in Sec. IV B and in Sec. VI A). Note that this is equivalent to preparing a specific state of the photonic qubit and therefore is closely linked to the measurement-device-independent quantum key distribution (MDI QKD) [45] as discussed in Appendix I. However, preparing specific states that involve the superposition of the presence and absence of a photon on its own is generally experimentally challenging. The NV implementation allows us to achieve this task precisely by preparing spin-photon entanglement and then measuring the spin qubit. Afterward, by conditioning on the click of a single detector only, Alice and Bob can use the information of which detector clicked to generate a single raw bit of key; see Appendix E and Ref. [41] for more information.

The main motivation of this scheme is that, informally, we only need one photon to travel half the distance between the two parties to get an entangled state. This thus effectively reduces the effects of losses, and in the ideal scenario the secret-key rate would scale with the square root of the total transmissivity η, as opposed to linear scaling in η (which is the optimal scaling without a quantum repeater [46]).

However, one problem that one faces when implementing this scheme is that the fiber induces a phase shift on the transmitted photons. This shift can change over time, e.g., due to fluctuations in the temperature and vibrations of the fiber. The uncertainty of the phase shift induces dephasing noise on the state, reducing the quality of the state.

To overcome this problem, a two-photon scheme was proposed by Barrett and Kok [47], which does not place such a high requirement on the optical stability of the setup. Specifically, in the Barrett and Kok scheme the problem of optical phase fluctuations is overcome by requiring two consecutive clicks and performing additional spin-flip operations on both of the remote memories. The Barrett and Kok scheme has seen implementation in many experiments [48–51]. However, the requirement of two consecutive clicks implies that a setup using only the Barrett and Kok scheme with two memory nodes will never be able to satisfy the demands of a quantum repeater. Specifically, the probability of getting two consecutive clicks will not be higher than the transmissivity of the fiber between the two parties and therefore will not surpass the secret-key capacity.

In the single-photon scheme, on the other hand, the dephasing caused by the unknown optical phase shift is overcome by using active *phase stabilization* of the fiber to reduce the fluctuations in the induced phase. This technique has been

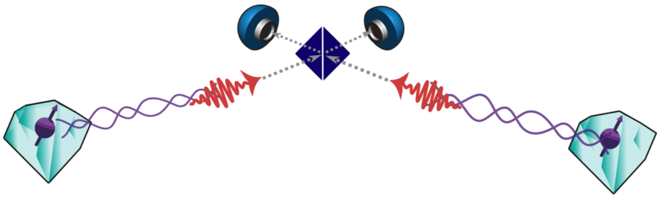

FIG. 3. Schematic overview of the single-photon scheme. Alice and Bob simultaneously transmit a photonic state from their NV centers toward a balanced beam splitter in the center. This photonic qubit, corresponding to the presence and absence of a photon, is initially entangled with the NV electron spin. If only one of the detectors (which can be seen at the top of the figure) registers a click, Alice and Bob can use the information of which detector clicked to generate a single raw bit of key.

used in the experimental implementations of the single-photon scheme for remote entanglement generation using quantum dots [52,53], NV centers [31], and atomic ensembles [54]. For experimental details relating to NV implementation, we refer the reader to Sec. III. This phase-stabilization technique effectively reduces the uncertainty in the phase, allowing us to significantly mitigate the resulting dephasing noise; see Appendix A for mathematical details.

In contrast to the Barrett and Kok scheme, the single-photon scheme cannot produce a perfect maximally entangled state, even in the case of perfect operations and perfect phase stabilization. This is because losses in the channel result in a significant probability of having both nodes emitting a photon which can also lead to a single click in one of the detectors, yet the memories will be projected onto a product state. As we discuss below, this noise can be traded versus the probability of success of the scheme by reducing the weight of the photon-presence term in the generated spin-photon entangled state. This is discussed in more detail below and the full analysis is presented in Appendix E.

The single-photon scheme with phase stabilization is a promising candidate for a near-term quantum repeater with NV centers. We note here that recently other QKD schemes that use the MDI framework have been proposed. These schemes, similar to our proposal, use single-photon detection events to overcome the linear scaling of the secret-key rate with η [42,55,56]. In these proposals, in contrast to our single-photon scheme, no quantum memories are used, but instead Alice and Bob send phase-randomized optical pulses to the middle heralding station.

1. Setup and scheme

In the setup of the single-photon scheme, Alice and Bob are separated by a fiber where in the center there is a beam splitter with two detectors (see Fig. 3). They will both create entanglement between a photonic qubit and a stored spin and send the photonic qubit to the beam splitter.

Alice and Bob thus perform the following:

(1) Alice and Bob both prepare a state $|\psi\rangle = \sin\theta\,|\downarrow\rangle\,|0\rangle + \cos\theta\,|\uparrow\rangle\,|1\rangle$ where $|\downarrow\rangle\,/\,|\uparrow\rangle$ refers to the dark or bright state of the electron-spin qubit, $|0\rangle\,/\,|1\rangle$ indicates the absence or presence of a photon, and θ is a tunable parameter.

(2) Alice and Bob attempt to both separately send the photonic qubit to the beam splitter.

(3) Alice and Bob both perform a six-state measurement on their memories.

(4) The previous steps are repeated until only one of the detectors between the parties clicks.

(5) The information of which detector clicked gets sent to Alice and Bob for classical correction.

(6) All the previous step are repeated until sufficient data have been generated.

The parameter θ can be chosen by preparing a nonuniform superposition of the dark and bright state of the electron spin $|\psi\rangle = \sin\theta\,|\downarrow\rangle + \cos\theta\,|\uparrow\rangle$ via coherent microwave pulses. This is done before applying the optical pulse to the electron which entangles it with the presence and absence of a photon. The parameter θ can then be tuned in such a way as to maximize the secret-key rate. In the next section, we will briefly expand on some of the issues arising when losses and imperfect detectors are present. We defer the full explanation and calculations until Appendix E.

2. Realistic setup

In any realistic implementation of the single-photon scheme, a large number of attempts is needed before a photon detection event is observed. Furthermore, a single detector registering a click does not necessarily mean that the state of the memories is projected onto the maximally entangled state. This is due to multiple reasons, such as losing photons in the fiber or in some other loss process between the emission and detection, arrival of the emitted photons outside of the detection time window and the fact that *dark counts* generate clicks at the detectors. Photon loss in the fiber effectively acts as amplitude damping on the state of the photon when using the presence or absence state space [13,57]. Dark counts are clicks in the detectors, caused by thermal excitations. These clicks introduce noise, since it is impossible to distinguish between clicks caused by thermal excitations and the photons traveling through the fiber if they arrive in the same time window. All these sources of loss and noise acting on the photonic qubits are discussed in detail in Appendix A. Finally, we note that we assume here the application of non-number resolving detectors. This can lead to additional noise in the low-loss regime, since the event in which two photons got emitted cannot be distinguished from the single-photon emission events even if no photons got lost. However, in any realistic loss regime this is not a problem, since the probability of two such photons arriving at the heralding station is quadratically suppressed with respect to events where only one photon arrives. In the realistic regime, almost all the noise coming from the impossibility of distinguishing two-photon from single-photon emission events is the result of photon loss. Namely, if a two-photon emission event occurs and the detector registers a click, then with dominant probability it is due to only a single photon arriving, while the other one being lost. Hence the use of photon-number-resolving detectors would not give any visible benefit with respect to the use of the non-number-resolving ones. For a detailed calculation of the effects of losses and dark counts for the single-photon scheme, see Appendix E.

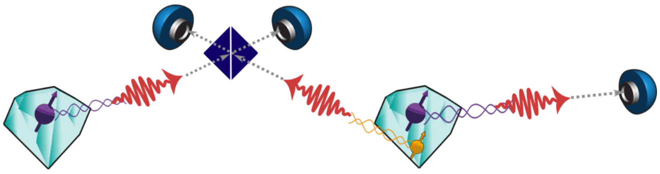

FIG. 4. Schematic overview of the SPADS scheme. First, the two NV centers run the single-photon scheme, such that Alice measures her electron spin directly after every attempt. After success, the middle node swaps its state to the carbon spin. Then the middle node generates electron-photon entangled pairs where the photonic qubit is encoded in the time-bin degree of freedom and sent to Bob. This is attempted until Bob successfully measures the photon or until the cut-off is reached. If the cut-off is reached, the scheme gets restarted; otherwise the middle node performs an entanglement swapping on its two memories and communicates the classical outcome to Alice and Bob, who can correct their measurement outcomes to obtain a bit of raw key.

C. Single photon with additional detection setup (SPADS) scheme

The third scheme that we consider here is the single-photon with additional detection setup (SPADS) scheme, which is effectively a combination of the single-photon scheme and the SiSQuaRe scheme as shown in Fig. 4. If the middle node is positioned at two thirds of the total distance away from Alice, the rate of this setup would scale, ideally, with the cube root of the transmissivity η.

This scheme runs as follows:

(1) Alice and the repeater run the single-photon scheme until success; however, only Alice performs her spin measurement immediately after each spin-photon entanglement generation attempt. This measurement is either in a six-state or BB84 basis.

(2) The repeater swaps the state of the electron spin onto the carbon spin.

(3) The repeater runs the second part of the SiSQuaRe scheme with Bob. This means it generates spin-photon entanglement between an electron and the time-bin-encoded photonic qubit. Afterward, it sends the photonic qubit to Bob. This is repeated until Bob successfully measures his photon in a six-state or BB84 basis or until the cut-off n^* is reached, in which case the scheme is restarted with step 1.

(4) After Bob has received the photon and communicated this to the repeater, the repeater performs a Bell-state measurement on its two quantum memories and communicates the classical result to Bob.

(5) All the previous steps are repeated until sufficient data have been generated.

The motivation for introducing this scheme is twofold. First, we note that by using this scheme we divide the total distance between Alice and Bob into three segments: two segments corresponding to the single-photon subscheme and the third segment over which the time-bin-encoded photons are sent. This gives us one additional independent segment with respect to the single-photon or the SiSQuaRe scheme on their own. Hence, for distances where no cut-off is required, we expect the scaling of the secret-key rate with the transmissivity to be better than the ideal square root scaling of the previous two schemes. Furthermore, dividing the total distance into more segments should also allow us to reach larger distances before dark counts become significant. When considering the resources necessary to run this scheme, we note that the additional third node needs to be equipped only with a photon detection setup.

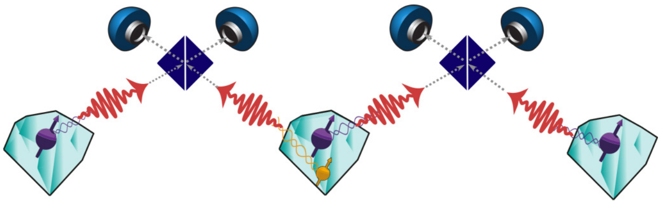

FIG. 5. Schematic overview of the setup for the SPOTL scheme. This scheme is a combination of the SiSQuaRe and single-photon scheme. Instead of sending photons directly through the fiber as in the SiSQuaRe scheme, entanglement is established between the middle node and Alice or Bob using the single-photon scheme.

Second, we note that the SPADS scheme can also be naturally compared to the scenario in which an NV center is used as a single-photon source for direct transmission between Alice and Bob. Both the setup for the SPADS scheme and such direct transmission involve Alice using an NV for emission and Bob having only a detector setup. Hence, the SPADS scheme corresponds to inserting a new NV node (the repeater) between Alice and Bob without changing their local experimental setups at all. This motivates us to compare the achievable secret-key rate of the SPADS scheme and direct transmission. We perform this comparison on a separate plot in Sec. VI.

D. Single photon over two links (SPOTL) scheme

The final scheme that we study here is the single-photon over two links (SPOTL) scheme, and it is another combination of the single-photon and SiSQuaRe schemes. A node is placed between Alice and Bob which tries to sequentially generate entanglement with their quantum memories by using the single-photon scheme (see Fig. 5). The motivation for this scheme is that, while using relatively simple components and without imposing stricter requirements on the memories than in the previous schemes, its secret-key rate would ideally scale with the fourth root of the transmissivity η.

1. Setup and scheme

The setup that we study is the following:

(1) Alice and the repeater run the single-photon scheme until success with the tunable parameter $\theta = \theta_A$. However, only Alice performs her spin measurement immediately after each spin-photon entanglement generation attempt. This measurement is in a six-state basis.

(2) The repeater swaps the state of the electron spin onto the carbon spin.

(3) Bob and the repeater run the single-photon scheme until success or until the cut-off n^* is reached, in which case the scheme is restarted with step 1. The tunable parameter is set here to $\theta = \theta_B$. Again, only Bob performs his spin measurement immediately after each spin-photon entanglement generation attempt and this measurement is in a six-state basis.

(4) The quantum repeater performs a Bell-state measurement and communicates the result to Bob.

(5) All the previous steps are repeated until sufficient data have been generated.

We note that for larger distances the optimal cut-off becomes smaller. Then, since we lose the independence of the attempts on both sides, the scaling of the secret-key rate with distance is expected to drop to $\sqrt{\eta}$, which is the same as for the single-photon scheme. However, the total distance between Alice and Bob is now split into four segments. Alice and Bob thus send photons over only one fourth of the total distance. Thus, this scheme should be able to generate key over much larger distances than the previous ones, as the dark counts will start becoming significant for larger distances only.

III. NV IMPLEMENTATION

Having proposed different quantum repeater schemes, we now move on to describe their experimental implementation based on nitrogen-vacancy centers in diamond [58]. This defect center is a prime candidate for a repeater node due to its packaged combination of a bright optical interface featuring spin-conserving optical transitions that enable high-fidelity single-shot readout [59] and individually addressable, weakly coupled ^{13}C memory qubits that can be used to store quantum states in a robust fashion [33,60]. Moreover, second-long coherence times of an NV electron spin have been achieved recently by means of dynamical decoupling sequences [32].

By applying selective optical pulses and coherent microwave rotations, we first generate spin-photon entanglement at an NV center node [50]. To generate entanglement between two distant NV electron spins, these emitted photons are then overlapped on a central beam splitter to remove their which-path information. Subsequent detection of a single photon heralds the generation of a spin-spin entangled state [50]. For all schemes based on single-photon entanglement generation, we need to employ active phase-stabilization techniques to compensate for phase shifts of the transmitted photons, which will reduce the entangled state fidelity, as introduced in Sec. II B. These fluctuations arise from both mechanical vibrations and temperature-induced changes in optical path length, as well as phase fluctuations of the lasers used during spin-photon entanglement generation. This problem can be mitigated by using light reflected off the diamond surface to probe the phase of an effectively formed interferometer between the two NV nodes and the central beam splitter, and by feeding the acquired error signal back to a fiber stretcher that changes the relative optical path length [31].

The electron spin state can be swapped to a surrounding ^{13}C nuclear spin to free up the single optical NV interface per node for a subsequent entangling round; a weak (approx. few kHz), always-on, distance-dependent magnetic hyperfine interaction between the electron and ^{13}C spin forms the basis of a dynamical decoupling based universal set of nuclear gates that allow for high-fidelity control of individual nuclear spins [33,34,37,38]. Crucially, the so-formed memory can retain coherence for thousands of remote entangling attempts despite stochastic electron spin reset operations, quasistatic noise, and microwave control infidelities during the subsequent probabilistic entanglement generation attempts [38,61] (see Appendix B for details).

In the NV node containing both the electron and carbon nuclear spin, it is also possible to perform a deterministic Bell-state measurement on the two spins. Specifically, a combination of two nuclear-electron spin gates and two sequential electron spin state measurements reads out the combined nuclear-electron spin state in the Z and X bases, enabling us to discriminate all four Bell states [62].

For an NV center in free space, only ≈3% of photons are emitted in the *zero-phonon line* (ZPL) that can be used for secret-key generation. This poses a key challenge for a repeater implementation, since this means that the probability of successfully detecting an emitted photon is low. Therefore, we consider a setup in which the NV center is embedded in an optical cavity with a high ratio of quality factor Q to mode volume V to enhance this probability via the Purcell effect in the weak coupling regime [63]. This directly translates into a lower optical excited state lifetime that is beneficial to shorten the time window during which we detect ZPL photons after the beam splitter, reducing the impact of dark counts on the entangled state. Additionally, a cavity introduces a preferential mode into which the ZPL photons are emitted that can be picked up efficiently. This leads to a higher expected collection efficiency than the noncavity case [40]. Enhancement of the ZPL has been successfully implemented for different cavity architectures, including photonic crystal cavities [64–71], microring resonators [72], whispering-gallery-mode resonators [73,74] and open, tunable cavities [75–77]. However, cavity-assisted entanglement generation has not yet been demonstrated for these systems, limited predominantly by broad optical lines of surface-proximal NV centers. Therefore, we focus on the open, tunable microcavity approach [78], since it has the potential for incorporating micron-scale diamond slabs inside the cavity, while allowing us to keep high Q/V values and providing *in situ* spatial and spectral tunability [79]. In these diamond slabs, an NV center can be microns away from surfaces, potentially allowing us to maintain bulk-like optical and spin properties as needed for the considered repeater protocols.

IV. CALCULATION OF THE SECRET-KEY RATE

With the modeling of each of the components of the different setups in hand, the performance of each setup can be estimated. The performance of a setup is assessed in this paper by its ability to generate a secret key between two parties, Alice and Bob. We note here that the ability of a quantum repeater to generate a secret key can be measured in two different ways—in its *throughput* and its *secret-key rate*. The throughput is equal to the amount of secret key generated per unit time, while the secret-key rate equals the amount of secret key generated per *channel use*. In this paper, we will focus on the secret-key rate only. This is because it allows us to make concrete information-theoretical statements about our ability to generate secret key. Moreover, we note that the secret-key rate is also more universal in the sense that it can be easily converted into the throughput by multiplying it with the repetition rate of our scheme (number of attempts we can perform in a unit time). It must be also

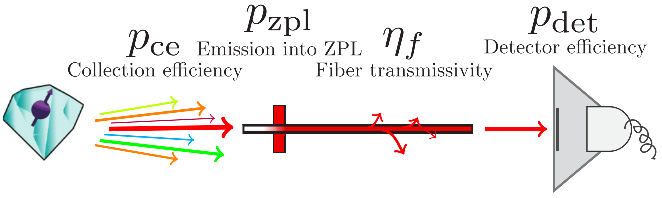

FIG. 6. The model of photon-loss processes occurring in our repeater setups. The parameter $p_{\rm ce}$ is the photon-collection efficiency, which includes the probability that the photon is successfully coupled into the fiber. Only photons emitted at the zero-phonon line (ZPL) can be used for quantum information processing. All non-ZPL photons are filtered out, such that a fraction $p_{\rm zpl}$ of the photons remains. The photons are then transmitted through a fiber with transmissivity η_f. Such successful transmissions are registered by the detector with probability $p_{\rm det}$. Additionally, a significant fraction of photons can arrive in the detector outside of the detection time window $t_{\rm w}$. Such photons will effectively also get discarded. Here we describe the total efficiency of our apparatus by a single parameter, $p_{\rm app} = p_{\rm ce}p_{\rm zpl}p_{\rm det}$.

noted here that demonstrating repeater schemes that achieve higher throughput than the currently available QKD systems based on direct transmission will be a great challenge. This is because the sources of photonic states used within those QKD systems operate at the GHz repetition rates, while the performance of the repeater schemes will be limited by many additional factors such as transmission latency and time of local operations at the memory nodes. These issues are not captured by the secret-key rate directly. Nevertheless, as mentioned before, the universality of the secret-key rate allows for the interconversion between the two quantities. We further discuss the differences between the throughput and secret-key rate in Sec. VI E.

The secret-key rate R is equal to

$$R = \frac{Yr}{N_{\rm modes}}, \tag{1}$$

where Y and r are the yield and secret-key fraction, respectively. The yield Y is defined as the average number of raw bits generated per channel use and the secret-key fraction r is defined as the amount of secret key that can be extracted from a single raw bit (in the limit of asymptotically many rounds). Here $N_{\rm modes}$ is the number of optical modes needed to run the scheme. Time-bin encoding requires two modes while the single-photon scheme uses only one mode. Hence, $N_{\rm modes} = 2$ for all the schemes that use time-bin encoding in at least one of the arms of the setup. For the schemes that use only the single-photon subschemes as their building blocks, we have that $N_{\rm modes} = 1$.

In the remainder of this section, we will briefly detail how to calculate the yield and secret-key fraction, from which we can estimate the secret-key rate of each scheme.

A. Yield

The yield depends not only on the used scheme but also on the losses in the system. We model the general emission and transmission of photons through fibers from NV centers in diamond as in Fig. 6. That is, with probability $p_{\rm ce}$ spin-photon entanglement is generated and the photon is coupled into a fiber. The photons that successfully got coupled into the fiber might not be useful for quantum information processing since they are not coherent. Thus, we filter out those photons that are not emitted at the zero-phonon line, reducing the number of photons by a further factor of $p_{\rm zpl}$. Then, over the length of the fiber, a photon gets lost with probability $1 - \eta_f = 1 - e^{-\frac{L}{L_0}}$, where L_0 is the attenuation length and η_f is the transmissivity. After exiting the fiber, the photon gets registered as a click by the detector with probability $p_{\rm det}$. Finally, the photon gets accepted as a successful click if the click happens within the time window $t_{\rm w}$ of the detector (see Appendix A for more details).

The yield can then be calculated as the reciprocal of the expected number of channel uses needed to get one single raw bit,

$$Y = \frac{1}{\mathbb{E}[N]}, \tag{2}$$

with N being the random variable that models the number of channel uses needed for generating a single raw bit.

1. Yield of the single-photon scheme

The yield of the single-photon scheme is relatively easy to calculate, since the single condition heralding the success of the scheme is a single click in one of the detectors in the heralding station. Therefore, the yield Y is simply the probability that an individual attempt will result in a single click in one of the detectors. This probability will depend on the losses in the system, dark counts and the angle θ. A full calculation of the yield is given in Appendix E.

2. Yield of the SiSQuaRe, SPADS, and SPOTL schemes

The SiSQuaRe, SPADS, and SPOTL schemes require two conditions for the heralding of the successful generation of a raw bit, namely the scheme needs to succeed both on Alice's and Bob's sides independently. In this case, we are going to take a very conservative perspective and assume the total number of channel uses to be the sum of the required channel uses on Alice's and Bob's side of the memory repeater node,

$$\mathbb{E}[N] = \mathbb{E}[N_A + N_B]. \tag{3}$$

Moreover, every time Bob reaches n^* attempts, both parties start the scheme over again. The cut-off increases the average number of channel uses, thus decreasing the yield. Denoting by p_A and p_B the probability that a single attempt of the subscheme on Alice's and Bob's side respectively succeeds, we find (see Appendix C for the derivation)

$$\mathbb{E}[N_A + N_B] = \frac{1}{p_A[1-(1-p_B)^{n^*}]} + \frac{1}{p_B}. \tag{4}$$

B. Secret-key fraction

The secret-key fraction is the fraction of key that can be extracted from a single raw state. It is a function of the average quantum bit error rates in the X, Y, and Z basis [80,81] (QBER), and depends on the protocol (such as the BB84 [8] or six-state protocol [43,44]) and classical postprocessing used (such as the advantage distillation postprocessing [81]) .

Here we consider the entanglement-based version of the BB84 and six-state protocols. That is, Alice and Bob both perform measurements on their local qubits which share quantum correlations. We note that both the BB84 and the six-state protocol can in principle be run either in a symmetric or asymmetric way. Symmetric means that the probabilities of performing measurements in all the used bases are the same, while for asymmetric protocols they can be different. We note in the asymptotic regime, which is the regime that we consider here, it is possible to set this probability bias to approach unity and still maintain security [82]. Unfortunately, for technical reasons, within our model it is not possible to run an asymmetric six-state protocol when time-bin-encoded photons are used [17].

Moreover, as we mentioned above, it is also possible to apply different types of classical postprocessing of the raw key generated through the BB84 or the six-state protocol. In particular, here we consider two types of postprocessing: the standard one-way error correction and a more involved two-way error correction protocol called advantage distillation, which can tolerate much more errors. Specifically, here we consider the advantage distillation protocol proposed in Ref. [81], as this advantage distillation protocol has high efficiency (in particular, in the scenario of no noise, the efficiency of this protocol equals unity). Hence, in our model, we effectively consider two protocols for generating a secret key: BB84 with standard one-way error correction and a six-state method with advantage distillation. We refer the reader to Appendix G for the mathematical expressions for the secret-key fraction for all the considered protocols.

Now we can state explicitly which QKD protocols will be considered for each scheme, which in turn depends on the type of measurements that Alice and Bob perform in that scheme. There are two physical implementations of measurements that Alice and Bob perform, depending on the scheme under consideration. That is, they either measure a quantum state of a spin or of a time-bin-encoded photons. Since the fully asymmetric six-state protocol with advantage distillation has higher efficiency than both symmetric and asymmetric BB84 protocol with one-way error correction, we will use this six-state protocol for both the single-photon and SPOTL scheme. The SiSQuaRe and SPADS schemes involve direct measurement on time-bin-encoded photons. Hence, for these schemes, we consider the maximum of the amount of key that can be obtained using the fully asymmetric BB84 protocol and the symmetric six-state protocol with advantage distillation (which can tolerate more noise, but has three times lower efficiency than the fully asymmetric BB84 protocol).

To estimate the QBER, we model all the noisy and lossy processes that take place during the protocol run. From this, we calculate the qubit error rates and yield, from which we can retrieve the secret-key fraction. We invite the interested reader to read about the details of these calculations in Appendices E and F. The derivation of the QBER and the yield for the SiSQuaRe scheme is performed in Ref. [17]. Moreover, in this work we introduce certain refinements to the model which we discuss in Appendix D. With the QBER in hand, we can calculate the resulting secret-key fraction for the considered protocols as presented in Appendix G.

We note here that we consider only the secret-key rate in the asymptotic limit and that we thus do not have to deal with nonasymptotic statistics.

V. ASSESSING THE PERFORMANCE OF QUANTUM REPEATER SCHEMES

In this section, we will detail four benchmarks that will be used to assess the performance of quantum repeaters. The usage of such benchmarks for repeater assessment has been done in Refs. [17,30], and achieving a rate greater than such benchmarks can be seen as milestones toward the construction of a quantum repeater.

The considered benchmarks are defined with respect to the efficiencies of processes involving photon loss when emitting photons at NV centers, transmitting them through an optical fiber and detecting them at the end of the fiber as described in Sec. IV A and as shown in Fig. 6.

Having this picture in mind, we can now proceed to present the considered benchmarks. The first three of these benchmarks are inspired by fundamental limits on the maximum achievable secret-key rate if Alice and Bob are connected by quantum channels which model quantum key distribution over optical fiber without the use of a (possible) quantum repeater.

The first of these benchmarks we consider here is also the most stringent one, the so-called *capacity of the pure-loss channel*. The capacity of the pure-loss channel is the maximum achievable secret-key rate over a channel modeling a fiber of transmissivity η_f, and is given by [13]

$$-\log_2(1-\eta_f). \tag{5}$$

This is the maximum secret-key rate achievable, meaning that even if Alice and Bob had perfect unbounded quantum computers and memories, they could not generate secret key at a larger rate. If, by using a quantum repeater setup, a higher rate can be achieved than $-\log_2(1-\eta_f)$, we are certain our quantum repeater setup allowed us to do something that would be impossible with direct transmission. Surpassing the secret-key capacity has been widely used as a defining feature of a quantum repeater [11–13,17,23,30,83–88]. Unfortunately, and as could be expected, surpassing the capacity is experimentally challenging. This motivates the introduction of other, easier to surpass, benchmarks. These benchmarks are still based on (upper bounds on) the secret-key capacity of quantum channels which model realistic implementations of quantum communications over fibers.

The second benchmark is built on the idea of including the losses of the apparatus into the transmissivity of the fiber. The resultant channel with all those losses included we call here *the extended channel*. The benchmark is thus equal to

$$-\log_2(1-\eta_f p_{\mathrm{app}}). \tag{6}$$

Here p_{app} describes all the intrinsic losses of the devices used, that is, the collection efficiency p_{ce} at the emitting diamond, the probability that the emitted photon is within the zero-phonon line p_{zpl} (which is necessary for generating quantum correlations), and photon detection efficiency p_{det}, so that $p_{\mathrm{app}} = p_{\mathrm{ce}} p_{\mathrm{zpl}} p_{\mathrm{det}}$.

The third benchmark we consider is the so-called *thermal channel bound*, which takes into account the effects of dark counts. The secret-key capacity of the thermal channel has been studied extensively [13,86–92]. We consider the following bound on the secret-key capacity of the thermal channel,

$$-\log_2[(1-\eta_f p_{\rm app})(\eta_f p_{\rm app})^{\overline{n}}] - g(\overline{n}), \tag{7}$$

if $\overline{n} \leqslant \frac{\eta_f p_{\rm app}}{1-\eta_f p_{\rm app}}$, and otherwise zero [13]. Here $\overline{n}$ is the average number of thermal photons per channel use and is equal to $t_{\rm w}$, the time window of the detector, times the average number of dark counts per second; see Ref. [17] for more details. The function $g(x)$ is defined as $g(x) \equiv (x+1)\log_2(x+1) - x\log_2(x)$. We note here that the time window of the detector $t_{\rm w}$ is not fixed in our model but is optimized over for every distance in order to achieve the highest possible secret-key rate. Hence, in this benchmark we fix $t_{\rm w} = 5$ ns which is the shortest duration of the time window that we consider in our secret-key rate optimization.

Finally, the secret-key rate achieved with *direct transmission using the same devices* can be seen as the fourth benchmark. Specifically, here we mean the secret-key rate achieved when Alice uses her electron spin to generate spin-photon entanglement and sends the time-bin-encoded photon to Bob. She then measures her electron spin while Bob measures the arriving photon. However, to take a conservative view, we will only use this direct transmission benchmark for the SPADS scheme. This is motivated by the fact that for both the SPADS scheme and the direction transmission scheme, the experimental setups on Alice's and Bob's side are the same, ensuring that the two rates can be compared fairly. We note that similarly as in the modeled secret-key rates achievable with our proposed repeater schemes, also for this direct transmission benchmark we optimize over the time window $t_{\rm w}$ for each distance.

The secret-key capacity stated in Eq. (5) is the main benchmark that we consider. Surpassing it establishes the considered scheme as a quantum repeater. The two expressions in Eqs. (6) and (7) and the achieved rate with direct transmission are additional benchmarks, which guide the way toward implementation of a quantum repeater. We define all the considered benchmarks for the channel with the same fiber attenuation length L_0 as the channel used for the corresponding achievable secret-key rate.

VI. NUMERICAL RESULTS

We now have a full model of the rate of the presented quantum repeater protocols as a function of the underlying experimental parameters. In this section, we will first state all the parameters required by our model and then present the results and conclusions drawn from the numerical implementation of this model. In particular, in Sec. VI A, we will first provide a deeper insight into the benefits of using the six-state protocol and advantage distillation in specific schemes. In Sec. VI B, we determine the optimal positioning of the repeater nodes for our schemes and investigate the dependence of the secret-key rate achievable with those schemes on the photon emission angle θ and the cut-off n^* for the appropriate schemes. In Sec. VI C, we then use the insights acquired in the previous section to compare the achievable secret-key rates for all the proposed repeater schemes with the secret-key capacity and other proposed benchmarks. In particular, we show that the single-photon scheme significantly outperforms the secret-key capacity and hence can be used to demonstrate a quantum repeater. Finally, in Sec. VI D, we determine the duration of the experiment that would allow us to demonstrate such a quantum repeater with the single-photon scheme.

The parameters that we will use are either parameters that have been achieved in an experiment or correspond to expected parameters when the NV center is embedded in an optical Fabry-Perot microcavity. The parameters we will use are listed in Table I.

To be now more specific, the photon collection efficiency $p_{\rm ce}$ and the probability of emitting into the zero-phonon line $p_{\rm zpl}$ are the two crucial parameters relying on the implementation of the optical cavity. The quoted value of $p_{\rm ce}$ has not been experimentally demonstrated yet, while the value of $p_{\rm zpl}$ has not been demonstrated in the context of quantum

TABLE I. Parameters used for the nitrogen-vacancy center setups considered in this paper.

Parameter	Notation	Value
Dephasing of ^{13}C due to interaction	a_0	1/2000 per attempt [38,61]
Dephasing of ^{13}C with time	a_1	1/3 per second [60]
Depolarizing of ^{13}C due to interaction	b_0	1/5000 per attempt [38]
Depolarizing of ^{13}C with time	b_1	1/3 per second [60]
Memory-photon entanglement preparation time	$t_{\rm prep}$	6 μs [48]
Depolarizing parameter for the measurement of the electron spin	F_m	0.95 [31]
Depolarizing parameter for two qubit gates in quantum memories	F_g	0.98 [33]
Dephasing parameter for the memory-photon state preparation	$F_{\rm prep}$	0.99 [48]
Collection efficiency	$p_{\rm ce}$	0.49 [40,48]
Emission into the zero-phonon line	$p_{\rm zpl}$	0.46 [77]
Detector efficiency	$p_{\rm det}$	0.8 [48]
Dark count rate	d	10 per second [48]
Characteristic time of the NV emission	τ	6.48 ns [77,93]
Detection window offset	$t_{\rm w}^{\rm offset}$	1.28 ns [48]
Attenuation length	L_0	0.542 km [48]
Refractive index of the fiber	$n_{\rm ri}$	1.44 [94]
Optical phase uncertainty of the spin-spin entangled state	$\Delta\phi$	14.3°[31]

communication. All the other independent parameters in the above list that are not related to the setup with a cavity have been demonstrated in experiments relevant for remote entanglement generation. The parameters that have not been discussed in the main text are discussed in the Appendices.

A. Comparing BB84 and six-state advantage distillation protocols

We first investigate here when the BB84 or six-state advantage distillation protocol performs better. It was shown in Ref. [17] that in the SiSQuaRe scheme there is a trade-off—for the low-noise regime (small distances) the fully asymmetric BB84 protocol is preferable, while in the high-noise regime (large distances) the problem of noise can be overcome by using a six-state protocol supplemented with advantage distillation. This technique allows us to increase the secret-key fraction at the expense of reducing the yield by a factor of three, since a six-state protocol in which Alice and Bob perform measurements on photonic qubits does not allow for the (fully) asymmetric protocol within our model. Numerically, we find that for the SPADS and SPOTL scheme advantage distillation is *necessary* to generate nonzero secret keys at any distance. This is due to the fact that there is a significant amount of noise in these schemes. Thus, for the SPADS (SPOTL) scheme the (a)symmetric six-state protocol with advantage distillation is optimal.

To provide more insight into the performance of those different QKD schemes for different parameter regimes, we plot the achievable secret-key fraction for the SPADS and SPOTL schemes as a function of the depolarizing parameter due to imperfect electron spin measurement F_m in Fig. 7 (see Appendix B for the discussion of the corresponding noise model). Noise due to imperfect measurements is one of the significant noise sources in our setup, since the SPADS scheme involves three and the SPOTL scheme four single-qubit measurements on the memory qubits. The data have been plotted for a fixed distance of $12.5L_0$, where $L_0 = 0.542$ km is the attenuation length of the fiber. Moreover, since on this plot we aim at maximizing only the secret-key fraction over the tunable parameters, we set the cut-off n^* to one and the detection time window t_w to 5 ns (the smallest detection time window we use) for both schemes. Furthermore, within the single-photon subscheme, the heralding station is always placed exactly in the middle between the two memory nodes. We also consider the positioning of the memory repeater node to be two-thirds away from Alice for the SPADS scheme and in the middle for the SPOTL scheme, as discussed in the next section. For the SPOTL scheme, we also assume $\theta_A = \theta_B$, which we will justify in the next section.

We see that for the current experimental value of $F_m = 0.95$ both schemes can generate keys only if the advantage distillation postprocessing is used. As F_m increases, we observe that for the SPADS scheme first the six-state protocol without advantage distillation and then the BB84 protocol start generating keys. For the SPOTL scheme, the value of F_m at which the six-state protocol without advantage distillation starts generating keys is much larger than the corresponding value of F_m for any of the studied protocols for the SPADS scheme. This is because the SPOTL scheme involves more noisy processes than the SPADS scheme. This also provides an approximate quantification of the benefit of using advantage distillation. Specifically, looking at the SPOTL scheme, it can be observed that while at the current experimental value of $F_m = 0.95$, advantage distillation allows for generating keys, but at a higher value of the depolarizing parameter $F_m = 0.97$, still no key can be generated with standard one-way postprocessing. Moreover, we see that utilizing advantage distillation for the SPADS scheme allows for the generation of keys, even with very noisy measurements when $F_m = 0.91$. We also observe two distinct scalings of the secret-key fraction with F_m in the regime where a nonzero amount of keys is generated. These two scalings depend on whether we use symmetric or asymmetric protocols. Specifically, for the SPADS scheme, the symmetric six-state protocol is used. Therefore, the corresponding two curves have a slope that is approximately three times smaller than the other three curves corresponding to the protocols that run in the fully asymmetric mode.

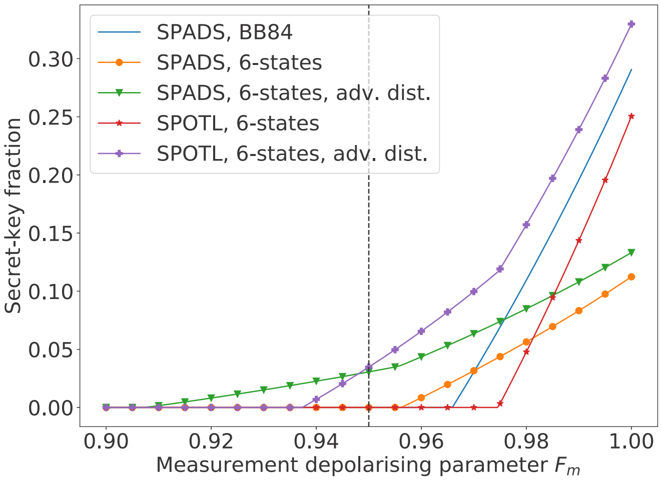

FIG. 7. Secret-key fraction as a function of the depolarizing parameter due to noisy measurement F_m for the total distance of $12.5L_0$. We see that for the current experimental value of $F_m = 0.95$ (marked with a dashed black vertical line) both schemes can generate keys only if the advantage distillation postprocessing is used. As F_m increases, the protocols that do not utilize advantage distillation also start generating keys. We also see that the curves can be divided into two groups in terms of their slope in the regime where they generate nonzero amounts of keys. Those two groups correspond to the scenarios where a fully asymmetric (bigger slope) or a symmetric (smaller slope) protocol is used. For all the plotted protocols, the cut-off n^* is set to one and $t_w = 5$ ns (the smallest detection time window we use) to maximize the secret-key fraction. Moreover, for each value of F_m, we optimize the secret-key fraction over the angle θ. For the SPOTL scheme, we assume $\theta_A = \theta_B$. For the SPADS scheme, we position the repeater node 2/3 of the total distance away from Alice and in the middle between Alice and Bob for the SPOTL scheme.

B. Optimal settings

We see that the above described repeater schemes include several tunable parameters. These parameters are the cut-off n^* for Bob's number of attempts until restart, the angle θ in the single-photon scheme, and the positioning of the

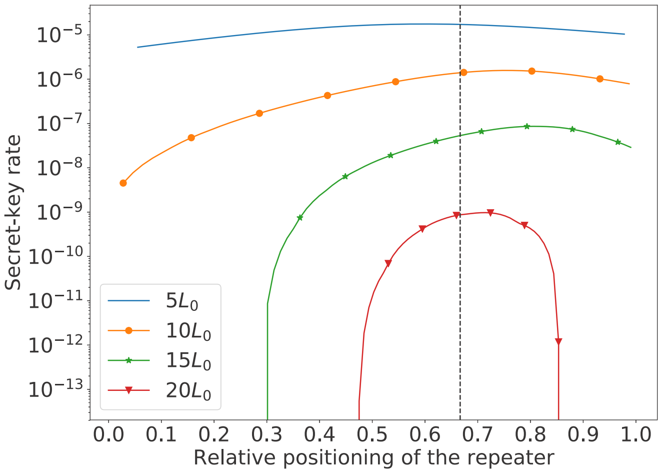

FIG. 8. Secret-key rate as a function of the relative positioning of the repeater for few different total distances for the SPADS scheme. The total distances are expressed in terms of the fiber attenuation length $L_0 = 0.542$ km. We see that positioning the repeater two-thirds of the distance away from Alice (marked by the vertical black dashed line) is a good positioning for all the distances. For each total distance considered and each positioning, the secret-key rate is optimized over the cut-off n^*, the angle θ, and the time window of the detector t_w.

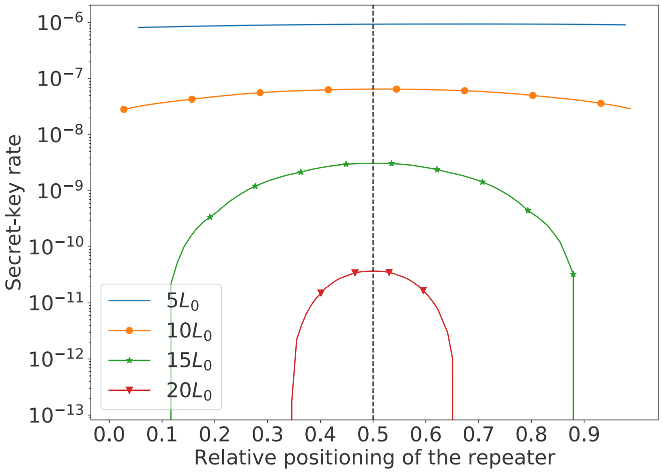

FIG. 9. Secret-key rate as a function of the relative positioning of the repeater for few different total distances for the SPOTL scheme. The total distances are expressed in terms of the fiber attenuation length $L_0 = 0.542$ km. We see that positioning the repeater in the middle between Alice and Bob (marked by the vertical black dashed line) is a good positioning for all the distances. For each total distance considered and each positioning, the secret-key rate is optimized over the cut-off n^*, the angles θ_A and θ_B, and the time window of the detector t_w.

repeater. These parameters can be optimized to maximize the secret-key rate. Here we will approach this optimization in a consistent way: We gradually restrict the parameter space by making specific observations based on numerical evidence.

The first claim that we will make is in relation to the *optimal positioning of the repeater.* In Ref. [17], we have conjectured that for the SiSQuaRe scheme the middle positioning of the repeater is optimal. For the single-photon scheme, we want the probability of transmitting the photons from each of the two nodes to the beam-splitter heralding station to be equal. This effectively sets the target state between the electron spins to be the maximally entangled state. Hence, if we restrict ourselves to the case where the emission angles θ of both Alice and Bob are the same, then it is natural to position the heralding station symmetrically in the middle between them. Hence, the only nonobvious optimal positioning is for the SPADS and SPOTL scheme.

For the SPADS scheme, positioning the repeater at two-thirds of the relative distance away from Alice could intuitively be expected to be optimal. This is because the single-photon scheme runs on two segments: Alice–beam splitter, beam splitter–repeater, while the one half of the SiSQuaRe scheme runs only over a single segment between the repeater and Bob. By segment, we mean here a distance over which we need to be able to independently transmit a photon. In Fig. 8, we show the secret-key rate as a function of the relative positioning of the repeater for a set of different total distances. We see there that despite the fact that positioning the repeater at two-thirds is not always optimal, it is a good enough positioning for all distances for our purposes. For each data point on the plot, we independently optimize over the cut-off n^*, the angle θ of the single-photon subscheme, and the duration of the detector time window t_w.

The SPOTL scheme has the same symmetry as the SiSQuaRe scheme, in the sense that the part of the scheme performed on Alice's side is exactly the same as on Bob's side. This symmetry is only broken by the sequential nature of the scheme. Since we have already observed that the middle positioning is optimal for the SiSQuaRe scheme, we expect to see the same behavior for the SPOTL scheme. Indeed, we confirm this expectation numerically in Fig. 9. Here for each data point we independently optimize over the cut-off n^*, the angle θ_A (θ_B) of the single-photon subscheme on Alice's (Bob's) side, and the duration of the detection time window.

To conclude, we will always place the heralding station within the single-photon (sub)protocol exactly in the middle between the two corresponding memory nodes. Moreover, we will also always place the memory repeater node in the middle for the SPOTL scheme and two-thirds of the distance away from Alice for the SPADS scheme.

Having established the optimal positioning of the repeater, we look into the relation between θ_A and θ_B for the SPOTL scheme. We observe that the relative error resulting from optimizing the secret-key rate over a single angle $\theta_A = \theta_B$ rather than two independent ones is smaller than 1% for all distances. Hence, from now on we will restrict ourselves to optimizing only over one angle θ for the SPOTL scheme.

Having resolved the issues of the optimal positioning of the repeater for all schemes and reducing the number of angles to optimize over for the SPOTL scheme to one, we now investigate how our secret-key rate depends on the remaining parameters. These parameters are the angle θ, the cut-off n^*, and the duration of the detection time window t_w. The optimal time window follows a simple behavior for all schemes: For short distances, the probability of getting a dark count p_d is negligible compared to the probability of detecting the signal photon. Hence, for those distances we can use a time window of 30 ns

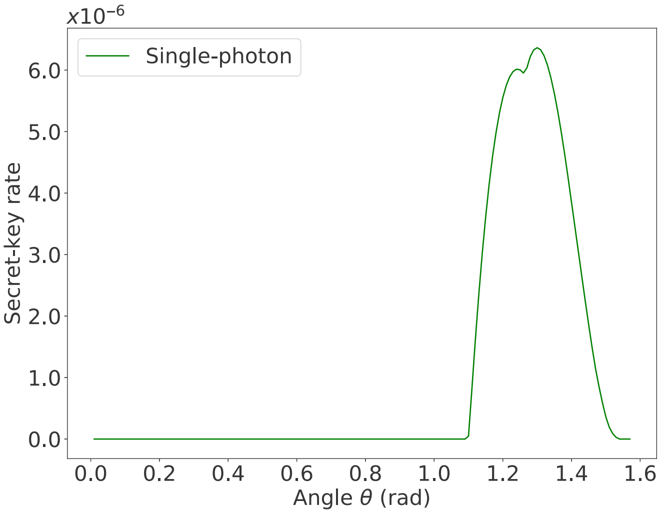

FIG. 10. Secret-key rate as a function of the θ angle for the single-photon scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that there is a relatively large range of angles for which a nonzero amount of keys can be generated. For each value of θ, the secret-key rate is optimized over the time window t_w. The kink on the plot is a consequence of the fact that the six-state protocol with advantage distillation involves optimization over two subprotocols.

to make sure that almost all the emitted photons which are not polluted by the photons from the optical excitation pulse arrive inside the detection time window. We always need to sacrifice the photons arriving within the time t_w^{offset} after the optical pulse has been applied to filter out the photons from that pulse; see Appendix A for details. Then, for larger distances where p_d starts to become comparable with the probability of detecting the signal photon, the duration of the time window is gradually reduced. This reduces the effect of dark counts at the expense of having more photons arriving outside of the time window. See Appendix A for the modeling of the losses resulting from photons arriving outside of the time window.

The dependence of the secret-key rate on the angle θ, the tunable parameter that Alice and Bob choose in their starting state $|\psi\rangle = \sin\theta\,|\downarrow\rangle\,|0\rangle + \cos\theta\,|\uparrow\rangle\,|1\rangle$ in the single-photon scheme, is more complex. We observe that the optimal value of θ is closer to $\frac{\pi}{2}$ for schemes that involve more noisy processes. Informally, this means that Alice and Bob send fewer photons toward the beam splitter to overcome the noise coming from events in which both nodes emit a photon. At $\frac{\pi}{2}$, however, no photons are emitted and the rate drops down to zero. We illustrate this in Figs. 10, 11, and 12. We see that for the SPADS and SPOTL scheme, there is only a restricted regime of the angle θ for which one can generate a nonzero amount of keys. In particular, the SPOTL scheme requires a larger number of noisy operations and therefore cannot tolerate much noise arising from the effect of photon loss in the single-photon subscheme. This means that there is only a small range of θ that allows for production of secret key. The single-photon scheme involves fewer operations and can tolerate more noise, and so lower values of the parameter θ still allow for the generation of keys.

We also investigate the dependence of the rate on the cut-off. Both the SPADS and SPOTL scheme require a lower cut-off than the SiSQuaRe scheme; see Figs. 13 and 14. This is caused by the fact that each of them involves more noisy operations, and hence less noise tolerance is possible.

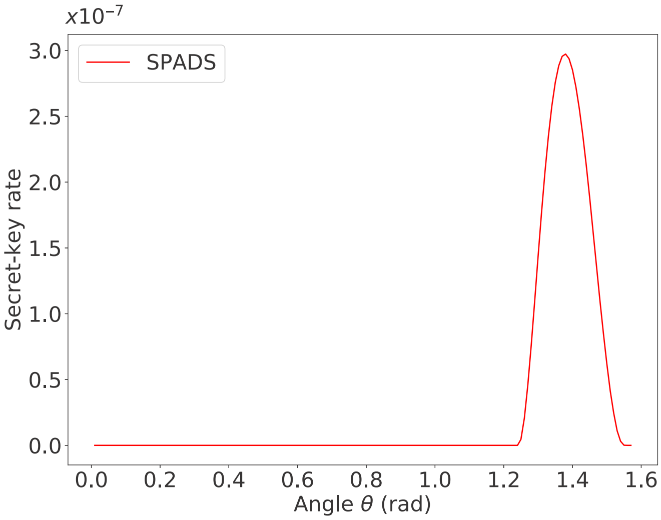

FIG. 11. Secret-key rate as a function of the θ angle for the SPADS scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that due to more noisy processes the range of θ that allows us to generate keys is much more restricted than for the single-photon scheme. For each value of θ, the secret-key rate is optimized over the cut-off n^* and the time window t_w.

C. Achieved secret-key rates of the quantum repeater proposals

Now we are ready to present the main results, the secret-key rate for all the considered schemes as a function of the

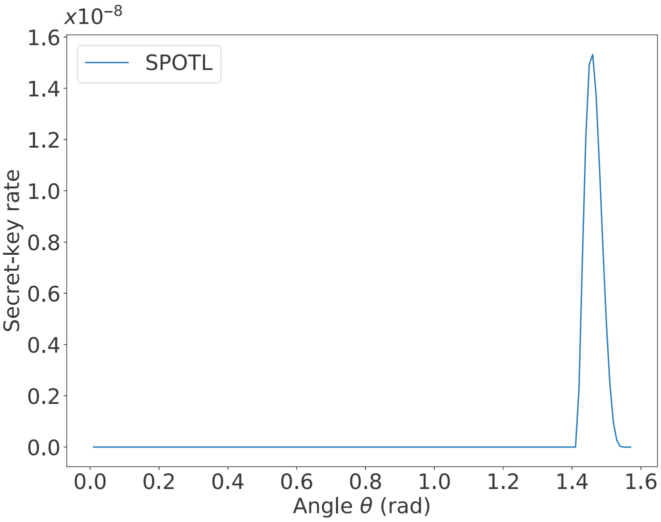

FIG. 12. Secret-key rate as a function of the angle $\theta = \theta_A = \theta_B$ for the SPOTL scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that, due to the increased amount of noisy processes, this scheme requires θ to be in a much narrower regime than for the single-photon and SPADS schemes, as can be seen by comparing the plot with the plots in Figs. 10 and 11. This corresponds to the overwhelming dominance of the dark state of the spin (no emission of the photon) in order to avoid any extra noise coming from the photon loss. For each value of θ, the secret-key rate is optimized over the cut-off n^* and the time window t_w.

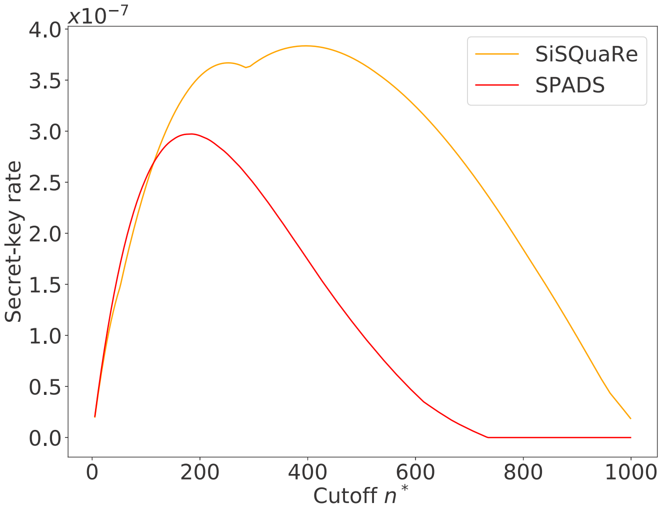

FIG. 13. Secret-key rate as a function of the cut-off for the SiSQuaRe and SPADS scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that the SPADS scheme requires a lower cut-off than the SiSQuaRe scheme because it involves more noisy operations. For each value of the cut-off n^*, we optimize the secret-key rate over the time window t_w and for the SPADS scheme also over the θ angle. The kink for the SiSQuaRe scheme arises because of the optimization over the fully asymmetric one-way BB84 protocol and symmetric six-state protocol with advantage distillation, which itself involves optimization over two subprotocols.

total distance when optimized over θ, the cut-off n^*, and the duration of the time window t_w. We compare the rates to the benchmarks from Sec. V.

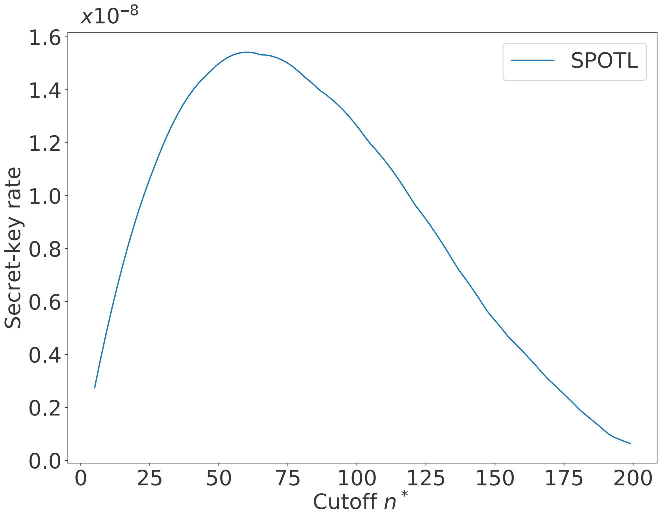

FIG. 14. Secret-key rate as a function of the cut-off for the SPOTL scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that due to the large number of noisy operations, this scheme requires a low cut-off in order to be able to generate keys. For each value of the cut-off n^*, we optimize the secret-key rate over the time window t_w and the θ angle.

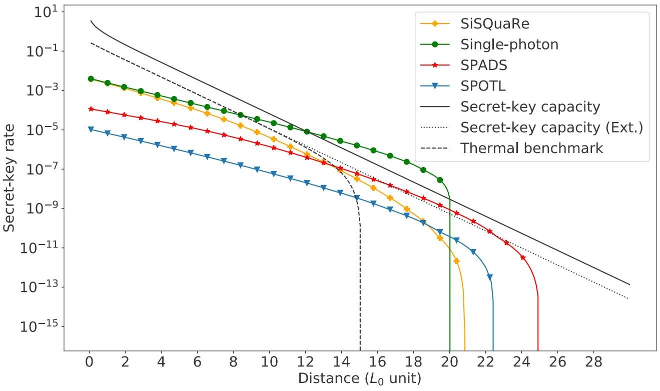

FIG. 15. Rate of all studied quantum repeater schemes as a function of the distance between Alice and Bob, expressed in the units of $L_0 = 0.542$ km. We also plot the different benchmarks from Sec. V. We see that the single-photon scheme outperforms the secret-key capacity. For the achievable rates, the secret-key rate is optimized over the cut-off n^*, the angle θ, and the time window t_w independently for each distance.

In Fig. 15, we plot the rate of all four of the quantum repeater schemes as a function of the distance between Alice and Bob. We observe that already for realistic near-term parameters, the single-photon scheme can outperform the secret-key capacity of the pure-loss channel by a factor of 7 for a distance of ≈9.2 km.

We have also investigated what improvements would need to be done in order for the SPADS and SPOTL schemes to also overcome the secret-key capacity. An example scenario in which the SPADS scheme outperforms this repeaterless bound includes better phase stabilization such that $\Delta\phi = 5^\circ$ and reduction of the decoherence effects in the carbon spin during subsequent entanglement generation attempts such that $a_0 = 1/8000$ and $b_0 = 1/20\,000$. Further improvement of these effective coherence times to $a_0 = 1/20\,000$ and $b_0 = 1/50\,000$ allows the SPOTL scheme to also overcome the secret-key capacity. We note that maintaining coherence of the carbon-spin memory qubit for such a large number of subsequent remote entanglement-generation attempts is expected to be possible using the method of decoherence-protected subspaces [38,61].

As mentioned before, the SPADS scheme can be naturally compared against the benchmark of the direct transmission using NV as a source. The results are depicted in Fig. 16. We see that the SPADS scheme easily overcomes the NV-based direct transmission and the thermal benchmark for larger distances, for which these benchmarks drop to zero.

In Fig. 15, we observe that for the SPOTL scheme, the total distance over which key can be generated, is significantly smaller than for the SPADS scheme. This is despite the fact that the full distance is divided into four segments. The rather weak performance of this scheme is because it involves a larger number of noisy operations. As a result, the scheme can tolerate little noise from the single-photon subscheme, requiring the angle θ to be close to $\frac{\pi}{2}$, as can be seen in Fig. 12. Hence, the probability of photon emission becomes greatly diminished and so the distance after which dark counts start becoming significant is much smaller than for the SPADS scheme. To overcome this problem, one would need to reduce the amount of noise in the system. One of the main sources of noise is the imperfect single-qubit measurement. Hence, we illustrate the achievable rates for the scenario with the boosted

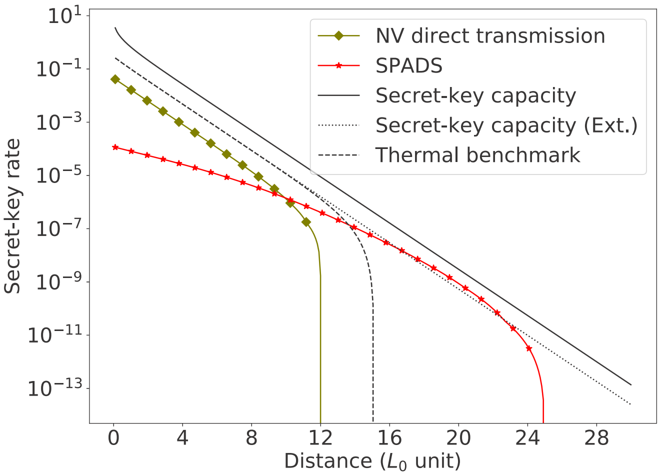

FIG. 16. Comparison of the SPADS scheme with the rate achievable using the direct transmission, with NV being the photon source. The secret-key rates for those schemes are plotted as a function of the distance between Alice and Bob, expressed in the units of $L_0 = 0.542$ km. We also plot the different benchmarks. We see that the SPADS scheme easily overcomes the direct transmission and the thermal benchmark (see Sec. V). For the secret-key rate achievable with the SPADS scheme, we perform optimization over the cut-off n^*, the angle θ, and the time window t_w independently for each distance. Similarly, we also optimize the secret-key rate achievable with direct transmission over the time window t_w.

measurement depolarizing parameter $F_m = 0.98$ in Fig. 17. Additionally, in this plot we also consider the application of probabilistic frequency conversion to the telecom wavelength at which $L_0 = 22$ km. Frequency conversion has already been achieved experimentally in the single-photon regime with success probability of 30% [95]. This is also the success probability that we consider here. The corresponding benchmarks have also been plotted for the new channel with $L_0 = 22$ km.

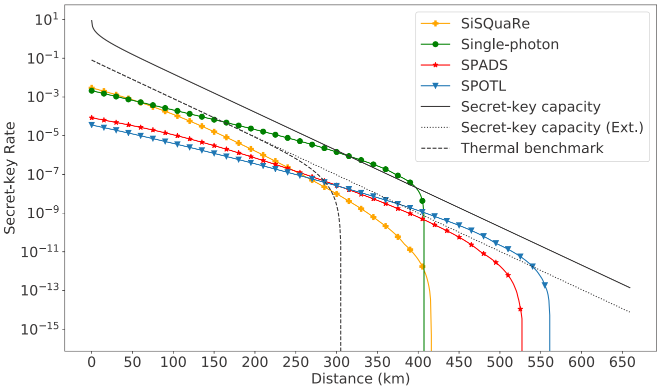

FIG. 17. Secret-key rate as a function of distance in units of km for transmission at telecom channel with $L_0 = 22$ km, along with the benchmarks from Sec. V. We consider an improved measurement depolarizing parameter of $F_m = 0.98$. The frequency conversion efficiency is assumed to be 0.3. We observe that the SPOTL scheme allows for the generation of secret key over a distance of more than 550 km. For the achievable rates, the secret-key rate is optimized over the cut-off n^*, the angle θ, and the time window t_w independently for each distance.

We see in Fig. 17 that with the improved measurement and using frequency conversion, the SPOTL scheme allows us now to generate secret key over more than 550 km. We also see that under those conditions the single-photon scheme can also overcome the secret-key capacity of the telecom channel.

D. Runtime of the experiment

While the theoretical capability of an experimental setup to surpass the secret-key capacity is a necessary requirement to claim a working quantum repeater, it does not necessarily mean that this can be experimentally verified in practice. Indeed, if a quantum repeater proposal only surpasses the secret-key capacity by a narrow margin at a large distance, the running time of an experiment could be too long for practical purposes. In this section, we will discuss an experiment which can validate a quantum repeater setup and calculate the running time of such an experiment, where we demonstrate that the single-photon scheme could be validated to be a quantum repeater within 12 h.

A straightforward way of validating a quantum repeater would consist of first generating secret key, calculating the achieved (finite-size) secret-key rate, and then comparing the rate with the secret-key capacity. However, this requires a large number of raw bits to be generated, partially due to the loose bounds on finite-size secret-key generation. What we propose here is an experiment where the QBER and yield are separately estimated to be within a certain confidence interval. Then, if with the (worst-case) values of the yield and the QBER the corresponding asymptotic secret-key rate still confidently beats the benchmarks, one could claim that, in the asymptotic regime, the setup would qualify as a quantum repeater.

As we show in Appendix H, it is possible to run the single-photon scheme over a distance of $17L_0 \approx 9.2$ km for approximately 12 h to find with high confidence ($\geqslant 1$–1.5×10^{-4}) that the scheme beats the capacity [see Eq. (5)] at that distance by a factor of at least 3.

E. Discussion and future outlook

It is worth noting that our figure of merit—the secret-key rate—is weakly impacted by the latency of transmission, which grows linearly with distance for the SiSQuaRe, SPADS, and SPOTL schemes. Its only effect on the secret-key rate is the resulting decoherence time in the quantum memories while the memory nodes await the success or failure signals. This decoherence due to the waiting time is negligible in comparison to the noise due to interaction, arising from subsequent entanglement generation attempts. On the other hand, this latency would clearly be very visible in low throughput of these schemes. A single-photon scheme, on the other hand, has an advantage of the repetition rate being limited only by the local processing of the memory nodes, which would result in a higher throughput. We observe this fact in the modest expected duration of the experiment, even in the high-loss regime needed for overcoming the secret-key capacity. It is worth noting that while the single-photon scheme maintains constant latency for QKD, there exist schemes where such constant latency can be maintained also for remote entanglement generation; see, e.g., Ref. [96]. It is hence clear that there are certain important properties of an efficient quantum repeater scheme that are not captured by the secret-key rate. However, achieving high throughputs for arbitrary distances would require almost all the components to be efficient in terms of rates and memories to be of high quality in terms of operational and long-storage fidelities. It is clear that demonstrating all these features together in a single experiment is still a future goal. The advantage of the secret-key rate is that overcoming the secret-key capacity would form a crucial step toward an implementation of an efficient and practical, long-distance quantum repeater architecture whose validity would carry an information-theoretic significance and will therefore be totally independent of any hardware-based reference scenario.

In our model, we have identified a significant amount of noise arising in the system. As a result, we find that it is not always beneficial to just divide the fixed distance into more elementary links. Hence, it is a natural question whether this noise could be eliminated, e.g., using entanglement distillation. In fact, for the noise arising due to photon loss in the single-photon scheme, not only does there exist an efficient distillation procedure [97,98], but it has also already been demonstrated in the NV platform [33]. Moreover, in the ideal case of noiseless operations and storage, a scheme based on generating two entangled states through the single-photon scheme and then distilling them as demonstrated in Ref. [33] should effectively also be able to overcome the secret-key capacity [35] and provide a significant boost by completely removing the noise due to photon loss. Furthermore, an implementation of such a distillation-based remote entanglement-generation scheme would alleviate the requirement of the optical phase stabilisation of the system. Therefore, this distillation-based scheme could be a natural fifth candidate for a proof of principle repeater. Nevertheless, we believe that the fidelities of quantum operations and the effective coherence times of the memories used in this paper might need to be improved before this distillation would prove useful.

VII. CONCLUSIONS

We analyzed four experimentally relevant quantum repeater schemes on their ability to generate secret key. More specifically, the schemes were assessed by contrasting their achievable secret-key rate with the secret-key capacity of the channel corresponding to direct transmission. The secret-key rates have been estimated using near-term experimental parameters for the NV center platform. The majority of these parameters have already been demonstrated across multiple experiments. A remaining challenging element of our proposed schemes is the implementation of optical cavities. These cavities would enable the enhancement of both the photon emission probability into the zero-phonon line and the photon collection efficiency to the desired level.

With these near-term experimental parameters, our assessment shows the viability of one of the schemes, the single-photon scheme, for the first experimental demonstration of a quantum repeater. In fact, the single-photon scheme achieves a secret-key rate more than seven times greater than the secret-key capacity. We also estimated the duration of an experiment to conclude that a rate larger than the secret-key capacity is achievable. The duration of the experiment would be approximately 12 h.

Finally, we show that a scheme based on concatenating the single-photon scheme twice (i.e., the SPOTL scheme), has the capability to generate secret key at large distances. However, this requires converting the frequency of the emitted photons to the telecom wavelength and modestly improving the fidelity at which measurements can be performed.

ACKNOWLEDGMENTS

The authors would like to thank Koji Azuma, Tim Coopmans, Axel Dahlberg, Suzanne van Dam, Roeland ter Hoeven, Norbert Kalb, Victoria Lipinska, Marco Lucamarini, Gláucia Murta, Matteo Pompili, and Jérémy Ribeiro for helpful discussions and feedback. This work was supported by the Dutch Technology Foundation (STW), the Netherlands Organization for Scientific Research (NWO) through a VICI grant (R.H.), a VIDI grant (S.W.), the European Research Council through a Starting Grant (R.H. and S.W.), the Ammodo KNAW award (R.H.) and the QIA project (funded by European Union's Horizon 2020, Grant Agreement No. 820445).

APPENDIX A: LOSSES AND NOISE ON THE PHOTONIC QUBITS

In this Appendix, we describe how the losses and noise affect our photonic qubits. In particular, we first recall how the two types of encoding result in the losses acting as different quantum channels on the states. Then, we study the effects of a finite detector time window. More specifically, we first show that the arrival of a photon outside the time window is equivalent to all the other loss processes, and second we calculate the probability of registering a dark count within the time window. We also show how to model the noise arising from those dark counts for the SiSQuaRe and SPADS schemes. Finally, we calculate the dephasing induced by the unknown phase shift for the single-photon scheme.

1. Effects of losses for the different encodings

The physical process of probabilistically losing photons corresponds to different quantum channels depending on the qubit encoding. In our repeater schemes, we use two types of encoding: time-bin and presence or absence of a photon. For a time-bin-encoded qubit in the ideal scenario of no loss, we always expect to obtain a click in one of the detectors. Hence, loss of a photon resulting in a no-click event raises an erasure flag which carries the failure information. Therefore, it is clear that for this encoding the physical photon loss process corresponds to an erasure channel with the erasure probability given by one minus the corresponding transmissivity,

$$D(\rho) = \eta\rho + (1-\eta)|\perp\rangle\langle\perp|. \tag{A1}$$

Here $|\perp\rangle$ is the loss flag, corresponding to the nondetection of a photon. Since we are only interested in the quantum state of the system for the successful events when a detection event has occurred, we effectively postselect on the nonerasure events. For presence or absence encoding, the situation is different since now there is no flag available that could explicitly tell us whether a photon got lost or not. In fact, for this encoding the photon loss results in an amplitude-damping channel applied to the photonic qubit. Here, the damping parameter equals one minus the transmissivity of the channel [99].

2. Effects of the detector time window

The detector only registers clicks that fall within a certain time window. It is *a priori* not clear what kind of noisy or lossy channel should be used to model the loss of information due to nondetection of photons arriving outside of the time window. This is because in a typical loss process we have a probabilistic leakage of information to the environment. In the scenario considered here, the situation is slightly different as effectively no leakage occurs, but rather certain part of the incoming signal effectively gets discarded. Here we will show that despite this qualitative difference, within our model this process can effectively be modeled as any other loss process.

Now, let us provide a brief description of the physics of this process. First, the detection time window is chosen such that the probability of detecting a photon from the optical excitation pulse used to entangle the electron spin with the photonic qubit is negligible [48]. For that reason, the detection time window is opened after a fixed offset $t_{\rm w}^{\rm offset}$ with respect to the beginning of the decay of the optical excited state of the electron spin. We note that for the considered enhancement of the ZPL emission using the optical cavity, we predict the characteristic time of the NV emission τ to be approximately half of the corresponding value of τ if no cavity is used [48,77,93]. Therefore, here we consider the scenario where the duration of the optical excitation pulse is made twice shorter with respect to the one used in Ref. [48]. This will allow us to filter out the unwanted photons from the excitation pulse by setting $t_{\rm w}^{\rm offset}$ to half of the offset used in Ref. [48].

Second, we note that the detection time window cannot last too long; specifically, it needs to be chosen such that there is a good trade-off between detecting coherent and noncoherent (i.e., dark counts) photons. In this subsection, we will discuss the effects of photons arriving outside of this time window and the effects of registering dark counts within this time window.

a. Losses from the detector time window

The NV center emits a photon through an exponential decay process with characteristic time τ. Therefore the probability of detecting a photon during a time window starting at $t_{\rm w}^{\rm offset}$ and lasting for $t_{\rm w}$ is

$$\begin{aligned} p_{\rm in}(t_{\rm w}) &= \frac{1}{\tau}\int_{t_{\rm w}^{\rm offset}}^{t_{\rm w}^{\rm offset}+t_{\rm w}} dt\,\exp\left(-\frac{t}{\tau}\right) \\ &= \exp\left(-\frac{t_{\rm w}^{\rm offset}}{\tau}\right) - \exp\left(-\frac{t_{\rm w}^{\rm offset}+t_{\rm w}}{\tau}\right). \end{aligned} \tag{A2}$$

Clearly the process of a photon arriving outside of the time window is qualitatively different from the loss process where the photons get lost to the environment. In the remainder of this section, we will now look at the difference between these two phenomena in more detail.

The emission process of the NV center is a coherent process over time. Consider a generic scenario in which we divide the emission time into two intervals, denoted by "in" and "out," respectively. Coherent emission then means that the state of the photon emitted by the electron spin in state $|\uparrow\rangle$ will be

$$|\psi\rangle = \sqrt{p_{\rm in}}\,|1\rangle_{\rm in}\,|0\rangle_{\rm out} + \sqrt{1-p_{\rm in}}\,|0\rangle_{\rm in}\,|1\rangle_{\rm out}\,. \tag{A3}$$

Now let us come back to our specific model, in which the "in" mode corresponds to the interval $[t_{\rm w}^{\rm offset}, t_{\rm w}^{\rm offset}+t_{\rm w}]$ and the "out" mode to all the times $t \geqslant 0$ lying outside of this interval ($t = 0$ is the earliest possible emission time). Here, the emission into the "in" mode occurs with probability $p_{\rm in}(t_{\rm w})$. Hence, the spin-photon state resulting from the emission by the $\alpha\,|\downarrow\rangle + \beta\,|\uparrow\rangle$ spin state is

$$\begin{aligned} |\psi\rangle = {}& \alpha\,|\downarrow\rangle\,|0\rangle_{\rm in}\,|0\rangle_{\rm out} + \beta\,|\uparrow\rangle\,[\sqrt{p_{\rm in}(t_{\rm w})}\,|1\rangle_{\rm in}\,|0\rangle_{\rm out} \\ &+ \sqrt{1-p_{\rm in}(t_{\rm w})}\,|0\rangle_{\rm in}\,|1\rangle_{\rm out}]. \end{aligned} \tag{A4}$$

If the presence of absence encoding is used, such a photonic qubit is then transmitted to the detector. Since only the spin and the "in" mode of the photon will be measured, we can now trace out the "out" mode:

$$\begin{aligned} \rho = {}& [|\alpha|^2 + |\beta|^2 p_{\rm in}(t_{\rm w})]|\phi\rangle\langle\phi| \\ &+ |\beta|^2[1-p_{\rm in}(t_{\rm w})]|\uparrow\rangle\langle\uparrow| \otimes |0\rangle\langle 0|_{\rm in}, \end{aligned} \tag{A5}$$

where

$$|\phi\rangle = \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2 p_{\rm in}(t_{\rm w})}}[\alpha\,|\downarrow\rangle\,|0\rangle_{\rm in} + \beta\sqrt{p_{\rm in}(t_{\rm w})}\,|\uparrow\rangle\,|1\rangle_{\rm in}]. \tag{A6}$$

Note that this state can be obtained by passing the photonic qubit of the state

$$|\psi\rangle = \alpha\,|\downarrow\rangle\,|0\rangle + \beta\,|\uparrow\rangle\,|1\rangle \tag{A7}$$

through the amplitude-damping channel with the damping parameter given by $1 - p_{\rm in}(t_{\rm w})$. Hence, we can conclude that for the photon number encoding, the possibility of the photon arriving outside of the time window of the detector can be modeled in the same way as any other photon-loss process, namely an amplitude-damping channel applied to that photonic qubit.

In the case of time-bin encoding, we effectively have four photonic qubits, since now we have "in" and "out" modes for both the early (denoted by "e") and the late (denoted by "l") time window. We assume here that the slots do not overlap. That is, a photon emitted in the "out" mode of the early time window is always distinct from any photon in the late time window. This can be achieved by making the time gap between the "in" modes of the early and late window long enough. In this case, the emission process results in a state

$$\begin{aligned} |\psi\rangle = {}& \alpha\,|\downarrow\rangle\,[\sqrt{p_{\rm in}(t_{\rm w})}\,|1\rangle_{e,\rm in}\,|0\rangle_{e,\rm out}\,|0\rangle_{l,\rm in}\,|0\rangle_{l,\rm out} \\ &+ \sqrt{1-p_{\rm in}(t_{\rm w})}\,|0\rangle_{e,\rm in}\,|1\rangle_{e,\rm out}\,|0\rangle_{l,\rm in}\,|0\rangle_{l,\rm out}] \qquad \text{(A8)} \\ &+ \beta\,|\uparrow\rangle\,[\sqrt{p_{\rm in}(t_{\rm w})}\,|0\rangle_{e,\rm in}\,|0\rangle_{e,\rm out}\,|1\rangle_{l,\rm in}\,|0\rangle_{l,\rm out} \\ &+ \sqrt{1-p_{\rm in}(t_{\rm w})}\,|0\rangle_{e,\rm in}\,|0\rangle_{e,\rm out}\,|0\rangle_{l,\rm in}\,|1\rangle_{l,\rm out}]. \qquad \text{(A9)} \end{aligned}$$

Again, tracing out the "out" modes results in a state

$$\rho = p_{\text{in}}(t_{\text{w}})|\phi\rangle\langle\phi| + [1 - p_{\text{in}}(t_{\text{w}})][|\alpha|^2|\downarrow\rangle\langle\downarrow| + |\beta|^2|\uparrow\rangle\langle\uparrow|] \otimes|00\rangle\langle 00|_{e,l}, \tag{A10}$$

where

$$|\phi\rangle = \alpha\,|\downarrow\rangle\,|1\rangle_e\,|0\rangle_l + \beta\,|\uparrow\rangle\,|0\rangle_e\,|1\rangle_l = \alpha\,|\downarrow\rangle\,|e\rangle + \beta\,|\uparrow\rangle\,|l\rangle\,. \tag{A11}$$

Here $|00\rangle_{e,l}$ corresponds to the loss flag from which we see that for the time-bin encoding the possible arrival of a photon outside of the time window results in an erasure channel with the erasure probability given by $[1 - p_{\text{in}}(t_{\text{w}})]$. Hence, this process can be also modeled as any other loss process for this encoding.

We have just shown that for both photon presence or absence and time-bin encodings the process of the photon arriving outside of the time window can be modeled by the source which prepares photons in a coherent superposition of the "in" and "out" modes and the detector tracing out (losing) the "out" modes. We have also shown that those two elements combined together result effectively in a loss process corresponding to the same channel as any other loss process for that encoding (amplitude damping for photon presence or absence and erasure channel for time-bin encoding).

However, between the source and the detector, there are other lossy or noisy components resulting in other quantum channels that need to be applied before the tracing out of the "out" mode at the detector. Now we show that for all loss and noise processes that occur in our model, the tracing out of the "out" mode can be mathematically commuted through all those additional noise and/or lossy processes. This means that the tracing out can be applied directly after the source, such that the above described reductions to amplitude damping or erasure channel can be applied.

Consider the quantum channels acting on the photonic qubits of the form

$$\mathcal{N} = \sum_i p_i \mathcal{N}^i_{\text{in}} \otimes \mathcal{N}^i_{\text{out}}. \tag{A12}$$

Effectively, these are the channels that do not couple the "in" and "out" modes. Since in reality "in" and "out" modes correspond to different time modes, their coupling would require some kind of memory inside the channel. Hence, we can think of the above defined channels as channels without memory. Now it is clear that for a quantum state ρ that among its registers includes both the "in" and the "out" mode, we have that

$$\text{Tr}_{\text{out}}[\mathcal{N}(\rho)] = \text{Tr}_{\text{out}}\left[\sum_i p_i \mathcal{N}^i_{\text{in}} \otimes \mathcal{N}^i_{\text{out}}(\rho)\right] = \sum_i p_i \mathcal{N}^i_{\text{in}}(\rho_{\text{in}}). \tag{A13}$$

Now, first tracing out the "out" modes and then applying the channel $\mathcal{N}$ (only the "in" part can be applied now) also results in $\sum_i p_i \mathcal{N}^i_{\text{in}}(\rho_{\text{in}})$ at the output. Hence, the tracing out of the "out" modes commutes with all the channels that are of the form (A12), which correspond to channels without memory. Clearly, the noise and loss processes that occur before the detection, such as photon loss or dephasing due to uncertainty in the optical phase of the photon, belong to this class of channels. In particular, this means that for photon presence or absence the amplitude damping due to photon loss in the channel and that due to photon arrival outside of the time window can be both combined into one channel with the single damping parameter given by $1 - \eta p_{\text{in}}(t_{\text{w}})$ (η denotes the transmissivity due to the loss process, e.g., the transmissivity of the fiber). The same applies to time-bin encoding where we now have a single erasure channel with erasure probability $1 - \eta p_{\text{in}}(t_{\text{w}})$.

To conclude, the arrival of the photon outside of the time window can be modeled in the same way as any other loss process for both photon encodings used and therefore we can now redefine the detector efficiency $p'_{\text{det}} = p_{\text{det}} p_{\text{in}}(t_{\text{w}})$ and the total apparatus efficiency $p'_{\text{app}} = p_{\text{ce}} p_{\text{zpl}} p'_{\text{det}}$. We can then define $\eta_{\text{total}} = p'_{\text{app}}\eta_f$ as the total transmissivity, with probability η_{total} a photon will be successfully transmitted from the sender to the receiver.

b. Dark counts within the detector time window

Photon detectors are imperfect, and due to thermal excitations, they will register clicks that do not correspond to any incoming photons. These undesired clicks are called dark counts and can effectively be seen as a source of noise. The magnitude of this noise depends on the ratio between the probability of detecting the signal photon and measuring a dark count. Clearly, dark counts become a dominant source of noise when the probability of detecting the signal photon becomes comparable to the probability of a dark count click. The probability p_d of getting at least one dark count within the time window t_{w} of awaiting the signal photon is given by $p_d = 1 - \exp(-t_{\text{w}} d)$, where d is the dark count rate of the detector [17].

In the SiSQuaRe scheme, Alice and Bob perform measurements on time-bin-encoded photons. The same applies to Bob in the SPADS scheme. Since at least two detectors are required to perform this measurement, the presence of dark counts means that the outcome may lie outside of the qubit space. Moreover, this measurement needs to be trusted. In consequence, a squashing map needs to be used to process the multiclick events in a secure way. Here, as an approximation, we consider the squashing map for the polarization encoding [100] in the same way as described in Ref. [17]. Hence, this measurement can also be modeled as a perfect measurement preceded by a depolarizing channel with parameter α, which depends on whether the BB84 or six-state protocol is used. The parameter α is given by [17]

$$\alpha_{A/B,\ \text{BB84}} = \frac{p'_{\text{app}}\eta_B(1 - p_d)}{1 - (1 - p'_{\text{app}}\eta_{A/B})(1 - p_d)^2}, \tag{A14}$$

$$\alpha_{A/B,\ \text{six-state}} = \frac{p'_{\text{app}}\eta_{A/B}(1 - p_d)^5}{1 - (1 - p'_{\text{app}}\eta_{A/B})(1 - p_d)^6}. \tag{A15}$$

Here $\eta_{A/B}$ denotes the transmissivity of the fiber between the memory repeater node and Alice's and/or Bob's detector setup. Finally, we note that dark counts increase the probability of registering a successful measurement event. For the optical measurement schemes utilizing the squashing map, the probability of registering a click in at least one detector is given by [17]

$$p_{A/B,\,\mathrm{BB84}} = 1 - (1 - p'_{\mathrm{app}}\eta_{A/B})(1 - p_d)^2, \tag{A16}$$

$$p_{A/B,\,\text{six-state}} = 1 - (1 - p'_{\mathrm{app}}\eta_{A/B})(1 - p_d)^6. \tag{A17}$$

The effect of dark counts in the single-photon scheme, which carries over to the SPOTL scheme, is analyzed in Appendix E.

3. Noise due to optical phase uncertainty

Another important noise process affecting photonic qubits is related to the fact that for the photon presence or absence encoding the spin-photon entangled state will also depend on the optical phase of the apparatus used. Specifically, it will depend on the phase of the lasers used to generate the spin photon entanglement as well as the optical phase acquired by the photons during the transmission of the photonic qubit. Knowledge about this phase is crucial for being able to generate entanglement through the single-photon scheme. In any realistic setup, however, there would be a certain degree of the lack of knowledge about this phase acquired by the photons. Since in the end what matters is the knowledge about the relative phase between the two photons, we can model this source of noise as the lack of knowledge of the phase on only one of the incoming photonic qubits. This noise process can be effectively modeled as dephasing. In this section, we will show that the phase uncertainty induces dephasing with a parameter λ equal to

$$\lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2}, \tag{A18}$$

where $\Delta\phi$ is the uncertainty in the phase and $I_{0/1}$ is the Bessel function of order 0/1. Let us assume that for Alice, the local phase of the photonic qubit has a Gaussian-like distribution on a circle, with standard deviation $\Delta\phi$ as observed in Ref. [31]. This motivates us to model the distribution as a von Mises distribution [101]. The von Mises distribution reads

$$f(\phi) = \frac{e^{\kappa\cos(\phi-\mu)}}{2\pi I_0(\kappa)}. \tag{A19}$$

Here μ is the measure of location, i.e., it corresponds to the center of the distribution, κ is a measure of concentration and can be effectively seen as the inverse of the variance, and I_0 is the modified Bessel function of the first kind of order 0. One can then show [101] that

$$\int_{-\pi}^{\pi} d\phi f(\phi)e^{\pm i\phi} = \frac{I_1(\kappa)}{I_0(\kappa)}e^{\pm i\mu}. \tag{A20}$$

Since we are only interested in the noise arising from the lack of knowledge about the phase rather than the actual value of this phase, without loss of generality we can assume $\mu = 0$. Moreover, the experimental parameter that we use here is effectively the standard deviation of the distribution $\Delta\phi$ and therefore we can write $\kappa = \frac{1}{(\Delta\phi)^2}$.

Hence, let us write the spin-photon entangled state that depends on the optical phase ϕ:

$$|\psi^{\pm}(\phi)\rangle = \sin(\theta)\,|{\downarrow}0\rangle \pm e^{i\phi}\cos(\theta)\,|{\uparrow}1\rangle\,. \tag{A21}$$

Now, the lack of knowledge about this phase leads to a mixed state:

$$\begin{aligned}\int_{-\pi}^{\pi} & f(\phi)|\psi^{\pm}(\phi)\rangle\langle\psi^{\pm}(\phi)|d\phi \\ &= \sin^2(\theta)|{\downarrow}0\rangle\langle{\downarrow}0| + \cos^2(\theta)|{\uparrow}1\rangle\langle{\uparrow}1| \\ &\quad \pm \sin(\theta)\cos(\theta)\int_{-\pi}^{\pi} f(\phi)(e^{i\phi}\,|{\uparrow}1\rangle\,\langle{\downarrow}0| \\ &\quad + e^{-i\phi}\,|{\downarrow}0\rangle\,\langle{\uparrow}1|)d\phi.\end{aligned} \tag{A22}$$

Let us now try to map this state onto a dephased state:

$$\begin{aligned}\lambda&|\psi^{\pm}(0)\rangle\langle\psi^{\pm}(0)| + (1-\lambda)|\psi^{\mp}(0)\rangle\langle\psi^{\mp}(0)| \\ &= \sin^2(\theta)|{\downarrow}0\rangle\langle{\downarrow}0| + \cos^2(\theta)|{\uparrow}1\rangle\langle{\uparrow}1| \\ &\quad \pm \sin(\theta)\cos(\theta)(2\lambda-1)(|{\uparrow}1\rangle\,\langle{\downarrow}0| + |{\downarrow}0\rangle\,\langle{\uparrow}1|).\end{aligned} \tag{A23}$$

Hence, we observe that

$$2\lambda - 1 = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{I_0\left(\frac{1}{(\Delta\phi)^2}\right)}, \tag{A24}$$

$$\rightarrow \lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2}. \tag{A25}$$

APPENDIX B: NOISY PROCESSES IN NV-BASED QUANTUM MEMORIES

In our setups, we use ^{13}C nuclear spins in diamond as long-lived memory qubits next to a nitrogen vacancy (NV) electron spin taking the role of a communication qubit. In this Appendix, we will detail our model of the noisy processes in the NV.

The electron spin can be manipulated via microwave pulses and an optical pulse is used to create and send a photon entangled with it. This operation is noisy and can be modeled as having a dephasing noise of parameter F_{prep}. This means that, if the desired generated target state between the photon and the electron spin was $|\psi^+\rangle$, we actually have a mixture $F_{\mathrm{prep}}|\psi^+\rangle\langle\psi^+| + (1 - F_{\mathrm{prep}})(\mathbb{I}\otimes Z)|\psi^+\rangle\langle\psi^+|(\mathbb{I}\otimes Z)$.

Information can be stored via a swapping of the electron spin state to the long-living nuclear ^{13}C spin. Through this swap operation we also free the communication qubit to be used for consecutive remote entanglement generation attempts. Because of interaction with its environment, a quantum state stored in a ^{13}C spin quantum memory undergoes an evolution that we model with a dephasing and a depolarizing channel with noise parameters $\lambda_1 = (1 + e^{-an})/2$ and $\lambda_2 = e^{-bn}$, respectively. The form of the parameters a and b in general depends on the scheme. For the SiSQuaRe, SPADS, and SPOTL schemes, there are two distinct effects that cause this decoherence: one induced by the time it takes to generate entanglement between the middle node and Bob, and one induced by the always-on hyperfine coupling between the electron spin and the carbon spin inside the middle NV node. This coupling becomes an additional source of decoherence for the carbon spin during probabilistic attempts to generate remote entanglement using the electron spin [38,61]. We model the decoherence effect on the qubit stored in the carbon spin of the middle node by a dephasing channel with parameter λ_1,

$$\mathcal{D}^{\lambda_1}_{\text{dephase}}(\rho) = \lambda_1\rho + (1-\lambda_1)Z\rho Z, \tag{B1}$$

and depolarizing channel with parameter λ_2,

$$\mathcal{D}^{\lambda_2}_{\text{depol}}(\rho) = \lambda_2\rho + (1-\lambda_2)\frac{\mathbb{I}}{D}, \tag{B2}$$

where λ_1 and λ_2 quantify the noise. The parameters depend as follows on the number of attempts n,

$$\lambda_1 = F_{T_2} = \frac{1+e^{-an}}{2}, \tag{B3}$$

$$\lambda_2 = F_{T_1} = e^{-bn}, \tag{B4}$$

where a and b are given by

$$a = a_0 + a_1\left(L_s\frac{n_{ri}}{c} + t_{\text{prep}}\right), \tag{B5}$$

$$b = b_0 + b_1\left(L_s\frac{n_{ri}}{c} + t_{\text{prep}}\right). \tag{B6}$$

Here n_{ri} is the refractive index of the fiber, c is the speed of light in vacuum, t_{prep} is the time it takes to prepare for the emission of an entangled photon, and L_s is the distance the signal needs to travel before the repeater receives the information about failure or success of the attempt. Let L_B denote the distance between the memory repeater node and Bob. Then for the SiSQuaRe and SPADS schemes $L_s = 2L_B$, as in each attempt, first the quantum signal needs to travel to Bob, who then sends back to the middle node the classical information about success or failure. For the SPOTL scheme $L_s = L_B$, as in this case, both the quantum and the classical signals need to travel only half of the distance between the middle node and Bob since the signals are exchanged with the heralding station, which is located halfway between the middle memory node and Bob. The parameters a_0 and b_0 quantify the noise due to a single attempt at generating an entangled spin photon, induced by stochastic electron spin reset operations, quasistatic noise, and microwave control infidelities. The parameters a_1 and b_1 quantify the noise during storage per second.

Gates and measurements in the quantum memory are also imperfect. We model those imperfections via two depolarizing channels. The first one acts on a single qubit with depolarizing parameter $\lambda_2 = F_m$ corresponding to the measurement of the electron spin. The second one acts on two qubits with depolarizing parameter $\lambda_2 = F_g$ corresponding to applying a two-qubit gate to both the electron spin and the ^{13}C spin. This means that every time a measurement is done on a e^- qubit of a quantum state ρ, it is actually done on $\mathcal{D}^{F_m}_{\text{depol}}(\rho)$. Also a swapping operation between the e^- spin and the nuclear spin (done experimentally via two two-qubit gates; see main text) leads to an error modeled by a depolarizing channel of parameter $F_{\text{swap}} = F_g^2$. Following the same logic, a Bell state measurement will cause the state to undergo an evolution given by a depolarizing channel. Specifically, following the decomposition of the Bell measurement into elementary gates for the NV implementation as described in Sec. III, this evolution will consist of a depolarizing channel with parameter F_g^2 acting on both of the measured qubits and the depolarizing channel with parameter F_m^2 acting only on the electron spin qubit.

APPENDIX C: EXPECTATION OF THE NUMBER OF CHANNEL USES WITH A CUT-OFF

In this Appendix, we derive an analytical formula for the expectation value of the number of channel uses between Alice and Bob needed to generate one bit of raw key for the SiSQuaRe, SPADS, and SPOTL schemes,

$$\mathbb{E}[N] = \frac{1}{p_A[1-(1-p_B)^{n^*}]} + \frac{1}{p_B}. \tag{C1}$$

For these three schemes, we implement a cut-off which is used to prevent decoherence. Each time the number of channel uses between the repeater node and Bob reaches the cut-off n^*, the entire protocol restarts from the beginning. Here, we take a conservative view and define the number of channel uses N between Alice and Bob as the sum $N_A + N_B$, where N_A (N_B) corresponds to the number of channel uses between Alice (Bob) and the middle node. From the linearity of the expectation value, we have that

$$\mathbb{E}[N_A + N_B] = \mathbb{E}[N_A] + \mathbb{E}[N_B]. \tag{C2}$$

We denote by p_A and p_B the probability of a successful attempt on Alice's and Bob's side respectively. Bob's number of channel uses follows a geometric distribution with parameter $p = p_B$, so that $\mathbb{E}[N_B] = \frac{1}{p_B}$. Without the cut-off, Alice's number of channel uses would follow a geometric distribution with parameter $p = p_A$. However, the cut-off parameter adds additional channel uses on Alice side. Since the probability that Bob succeeds within n^* trials is $p_{\text{succ}} = 1-(1-p_B)^{n^*}$, we in fact have that Alice's number of channel uses follows a geometric distribution with parameter $p'_A = p_A p_{\text{succ}}$. Hence, it is straightforward to see that

$$\mathbb{E}[N_A + N_B] = \frac{1}{p'_A} + \frac{1}{p_B} \tag{C3}$$

$$= \frac{1}{p_A[1-(1-p_B)^{n^*}]} + \frac{1}{p_B}. \tag{C4}$$

APPENDIX D: SISQUARE SCHEME ANALYSIS

The analysis of the SiSQuare scheme has been performed in Ref. [17]. In this work, we use the estimates of the yield and QBER as derived in Ref. [17] with the following modifications:

(1) For the calculation of the yield, we now adopt a conservative perspective and calculate the number of channel uses as $\mathbb{E}[N_A + N_B]$, as derived in Appendix C, rather than $\mathbb{E}[\max(N_A, N_B)]$. Note that $\mathbb{E}[\max(N_A, N_B)] \leqslant \mathbb{E}[N_A + N_B] \leqslant 2\mathbb{E}[\max(N_A, N_B)]$.

(2) The total depolarizing parameter for gates and measurements F_{gm} defined in Ref. [17] is now decomposed into individual operations as described in Appendix B. That is, in this work depolarization due to imperfect operations on the memories is expressed in terms of depolarizing parameter due to imperfect measurement, F_m, and imperfect two-qubit gate, F_g. Since in the analysis of the SiSQuaRe scheme we only deal

with Bell diagonal states, the overall noise due to imperfect swap gate and the Bell measurement leads to $F_{\mathrm{gm}} = F_g^4 F_m^2$.

(3) In Ref. [17], we have assumed the duration of the detection time window to be fixed to 30 ns and assumed that all the emitted photons will fall into that time window. Here, similarly as for other schemes, we perform a more refined analysis in which we include the trade-off between the duration of the time window and the dark count probability as described in Appendix A.

APPENDIX E: SINGLE-PHOTON SCHEME ANALYSIS

In this Appendix, we provide a detailed analysis of the single-photon scheme between two remote NV-center nodes. This section is structured as follows. First, we describe the creation of the spin-photon entangled state followed by the action of the lossy channel on the photonic part of this state, including the noise due to the uncertainty in the phase of the state induced by the fiber. Second, we apply the optical Bell measurement. Then we evaluate the effect of dark counts, which introduce additional errors to the generated state. Finally, we calculate the yield of this scheme and extract the QBER from the resulting state.

1. Spin-photon entanglement and action of a lossy fiber on the photonic qubit

First, both Alice and Bob generate spin-photon entangled states, parameterized by θ. As we will later see, this parameter allows for trading off the quality of the final entangled state of the two spins with the yield of the generation process. The ideal spin-photon state would then be described as

$$|\psi^+\rangle = \sin(\theta)\,|{\downarrow}\rangle\,|0\rangle + \cos(\theta)\,|{\uparrow}\rangle\,|1\rangle\,. \tag{E1}$$

The preparation of the spin-photon entangled state is not ideal. That is, the spin-photon entangled state is not actually as described above, but rather of the form (see Appendix B)

$$\begin{aligned}\rho &= F_{\mathrm{prep}}|\psi^+\rangle\langle\psi^+| + (1-F_{\mathrm{prep}})(\mathbb{I}\otimes Z)|\psi^+\rangle\langle\psi^+|(\mathbb{I}\otimes Z)\\ &= F_{\mathrm{prep}}|\psi^+\rangle\langle\psi^+| + (1-F_{\mathrm{prep}})|\psi^-\rangle\langle\psi^-|.\end{aligned} \tag{E2}$$

Here,

$$|\psi^-\rangle = \sin(\theta)\,|{\downarrow}\rangle\,|0\rangle - \cos(\theta)\,|{\uparrow}\rangle\,|1\rangle\,. \tag{E3}$$

For the next step, we need to consider two additional noise processes that affect the photonic qubits before the optical Bell measurement is performed. The first one is the loss of the photonic qubit. This can happen at the emission, while filtering the photons that are not of the required ZPL frequency, in the lossy fiber, in the imperfect detectors, or due to the arrival outside of the time window in which detectors expect a click. All these losses can be combined into a single loss parameter

$$\eta = \eta_{\mathrm{total}} = p_{\mathrm{ce}}\,p_{\mathrm{zpl}}\sqrt{\eta_f}\,p'_{\mathrm{det}}, \tag{E4}$$

with $\eta_f = \exp(-\frac{L}{L_0})$, where L is the distance between the two remote NV-center nodes in the scheme (see Fig. 6 and Appendix A). Hence, a photon is successfully transmitted through the fiber and detected in the middle heralding station with probability η. Now we note that the action of the pure-loss channel on the qubit encoded in the presence or absence of a photon corresponds to the action of the amplitude-damping channel with the damping parameter $1-\eta$ [99].

The second process that effectively happens at the same time as loss is the dephasing noise arising from the optical instability of the apparatus as described in Appendix A. We note that the amplitude-damping and dephasing channel commute; hence, it does not matter in which order we apply the two noise processes corresponding to the loss of the photonic qubit and unknown drifts of the phase of the photonic qubit in our model. Here, we first apply the dephasing due to the lack of knowledge of the phase on Alice's photon and then amplitude damping on both photons due to all the loss processes.

Following the model in Appendix A, the lack of knowledge about the optical phase will effectively transform Alice's state to

$$\begin{aligned}\rho_A = {}&[F_{\mathrm{prep}}\lambda + (1-F_{\mathrm{prep}})(1-\lambda)]|\psi^+\rangle\langle\psi^+|\\ &+ [(1-F_{\mathrm{prep}})\lambda + F_{\mathrm{prep}}(1-\lambda)]|\psi^-\rangle\langle\psi^-|,\end{aligned} \tag{E5}$$

where

$$\lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2}. \tag{E6}$$

Now we can apply all the transmission losses modeled as the amplitude-damping channel. The action of this channel on the photonic part of the state ρ results in the state that we can describe as follows. First, let us introduce two new states:

$$\begin{aligned}|\psi_\eta^\pm\rangle = {}&\frac{1}{\sqrt{\sin^2(\theta) + \eta\cos^2(\theta)}}(\sin(\theta)\,|{\downarrow}\rangle\,|0\rangle\\ &\pm\sqrt{\eta}\cos(\theta)\,|{\uparrow}\rangle\,|1\rangle).\end{aligned} \tag{E7}$$

Then, after the losses and before the Bell measurement, the state of Alice can be written as

$$\begin{aligned}\rho'_A = {}&[\sin^2(\theta) + \eta\cos^2(\theta)]\\ &\times\big([F_{\mathrm{prep}}\lambda + (1-F_{\mathrm{prep}})(1-\lambda)]|\psi_\eta^+\rangle\langle\psi_\eta^+|\\ &+ [(1-F_{\mathrm{prep}})\lambda + F_{\mathrm{prep}}(1-\lambda)]|\psi_\eta^-\rangle\langle\psi_\eta^-|\big)\\ &+ (1-\eta)\cos^2(\theta)|{\uparrow}\rangle\langle{\uparrow}||0\rangle\langle 0|,\end{aligned} \tag{E8}$$

and for Bob as

$$\begin{aligned}\rho'_B = {}&[\sin^2(\theta) + \eta\cos^2(\theta)]\\ &\times[F_{\mathrm{prep}}|\psi_\eta^+\rangle\langle\psi_\eta^+| + (1-F_{\mathrm{prep}})|\psi_\eta^-\rangle\langle\psi_\eta^-|]\\ &+ (1-\eta)\cos^2(\theta)|{\uparrow}\rangle\langle{\uparrow}||0\rangle\langle 0|.\end{aligned} \tag{E9}$$

2. States after the Bell measurement

Now we need to perform a Bell measurement on the photonic qubits within the states ρ'_A and ρ'_B. Here we consider the scenario with non-photon-number-resolving detectors. Assuming for the moment the scenario without dark counts, we have at most two photons in the system. Hence, we can consider three possible outcomes of our optical measurement: left detector clicked, right detector clicked, and none of the detectors clicked. The measurement operators can be easily derived by noting that in our scenario without dark counts, each of the detectors can be triggered either by one or two photons and no cross clicks between detectors are possible due to the photon-bunching effect. Then we can apply the reverse of the beam splitter mode transformations to the projectors on the events with one or two photons in each of the detectors to obtain these projectors in terms of the input modes. Finally, we truncate the resulting projectors to the qubit space since in our scenario it is not possible for more than one photon to be present in each of the input modes of the beam splitter. In this way, we obtain the following measurement operators:

$$\begin{aligned} A_0 &= |\Psi^+\rangle\langle\Psi^+| + \frac{1}{\sqrt{2}}|11\rangle\langle 11|,\\ A_1 &= |\Psi^-\rangle\langle\Psi^-| + \frac{1}{\sqrt{2}}|11\rangle\langle 11|, \qquad \text{(E10)}\\ A_2 &= |00\rangle\langle 00|. \end{aligned}$$

These outcomes occur with the following probabilities:

$$p_0 = p_1 = \eta\cos^2(\theta)\left[1 - \frac{\eta}{2}\cos^2(\theta)\right], \qquad \text{(E11)}$$

$$p_2 = [1 - \eta\cos^2(\theta)]^2. \qquad \text{(E12)}$$

The postmeasurement state of the two spins for the outcome A_0 is

$$\rho_0 = \frac{2\sin^2(\theta)}{2 - \eta\cos^2(\theta)}(a|\Psi^+\rangle\langle\Psi^+| + b|\Psi^-\rangle\langle\Psi^-|) + \frac{\cos^2(\theta)(2-\eta)}{2 - \eta\cos^2(\theta)}|\uparrow\uparrow\rangle\langle\uparrow\uparrow|. \qquad \text{(E13)}$$

Here,

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|\downarrow\uparrow\rangle \pm |\uparrow\downarrow\rangle), \qquad \text{(E14)}$$

$$a = \lambda\left[F_{\text{prep}}^2 + (1 - F_{\text{prep}})^2\right] + 2F_{\text{prep}}(1 - F_{\text{prep}})(1 - \lambda), \qquad \text{(E15)}$$

$$b = (1 - \lambda)\left[F_{\text{prep}}^2 + (1 - F_{\text{prep}})^2\right] + 2F_{\text{prep}}(1 - F_{\text{prep}})\lambda. \qquad \text{(E16)}$$

For the outcome A_1, the postmeasurement state of the spins is the same up to a local Z gate which Bob can apply following the trigger of the A_1 outcome. The postmeasurement state of the spins for the outcome A_2, that is, when none of the detector clicked, is

$$\begin{aligned} \rho_2 = \frac{1}{[1 - \eta\cos^2(\theta)]^2}[&\sin^4(\theta)|\downarrow\downarrow\rangle\langle\downarrow\downarrow|\\ &+ (1-\eta)\cos^2(\theta)\sin^2(\theta)(|\downarrow\uparrow\rangle\langle\downarrow\uparrow| + |\uparrow\downarrow\rangle\langle\uparrow\downarrow|)\\ &+ (1-\eta)^2\cos^4(\theta)|\uparrow\uparrow\rangle\langle\uparrow\uparrow|]. \qquad \text{(E17)} \end{aligned}$$

This is a separable state and so events corresponding to outcome A_2 (that is, no click in any of the detectors) will be discarded as failure. However, dark counts on our detectors can make us draw wrong conclusions about which of the three outcomes we actually obtained.

The effect of dark counts can be seen as follows:

We measured A_2 (no actual detection) but one of the detectors had a dark count. This event will happen with probability $2p_2p_d(1 - p_d)$ and will make us accept the state ρ_2. Note that this is a classical state so application of the Z correction by Bob does not affect this state at all.

We measured A_1 or A_2 but we also got a dark count in the other detector. This event will happen with probability $(p_0 + p_1)p_d$. This will effectively lead us to rejection of the desired state ρ_0. Hence, effectively ρ_0 will only be accepted if we measured A_1 or A_2 but the other detector did not have a dark count, which will happen with probability $(p_0 + p_1)(1 - p_d)$.

3. The yield and QBER

Taking dark counts into account, we see that the yield of the single-photon scheme, which is just the probability of registering a click in only one of the detectors, will be

$$\begin{aligned} Y &= (p_0 + p_1)(1 - p_d) + 2p_2p_d(1 - p_d)\\ &= 2(1 - p_d)\left\{\eta\cos^2(\theta)\left[1 - \frac{\eta}{2}\cos^2(\theta)\right]\right.\\ &\quad \left. + [1 - \eta\cos^2(\theta)]^2 p_d\right\}. \qquad \text{(E18)} \end{aligned}$$

The effective accepted state after a click in one of the detectors will then be

$$\rho_{\text{out}} = \frac{1}{Y}[(p_0 + p_1)(1 - p_d)\rho_0 + 2p_2p_d(1 - p_d)\rho_2]. \qquad \text{(E19)}$$

Note that both Alice and Bob perform a measurement on their electron spins immediately after each of the spin-photon-entanglement generation events. This measurement causes an error modeled as a depolarizing channel of parameter F_m on each qubit, which means that after a successful run of the single-photon protocol, the effective state shared by Alice and Bob including the noise of their measurements will be given by

$$\begin{aligned} \rho_{AB} &= F_m^2\rho_{\text{out}} + (1 - F_m)\\ &\quad \times F_m\left[\frac{\mathbb{I}_{2,A}}{2} \otimes \text{Tr}_A[\rho_{\text{out}}] + \text{Tr}_B[\rho_{\text{out}}] \otimes \frac{\mathbb{I}_{2,B}}{2}\right]\\ &\quad + (1 - F_m)^2\,\frac{\mathbb{I}_{4,AB}}{4}. \qquad \text{(E20)} \end{aligned}$$

One can then extract the QBER for this state in all the three bases using the appropriate correlated/anticorrelated projectors such that

$$e_z = \text{Tr}[(|00\rangle\langle 00| + |11\rangle\langle 11|)\rho_{AB}], \qquad \text{(E21)}$$

$$\begin{aligned} e_{xy} &= \text{Tr}[(|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_{AB}]\\ &= \text{Tr}[(|0_y1_y\rangle\langle 0_y1_y| + |1_y0_y\rangle\langle 1_y0_y|)\rho_{AB}]. \qquad \text{(E22)} \end{aligned}$$

Here $|+\rangle$ and $|-\rangle$ denote the two eigenstates of X and $|0_y\rangle$ and $|1_y\rangle$ denote the two eigenstates of Y. We note that for our model of the single-photon scheme the QBER in X and Y bases are the same and therefore we denote both by a single symbol e_{xy}.

APPENDIX F: SPADS AND SPOTL SCHEMES ANALYSIS

In order to compute the quantum bit error rate (QBER) of the single-photon with additional detection setup (SPADS) scheme and the single-photon over two links (SPOTL) scheme, we derive step by step the quantum state shared between Alice and Bob. The following results have been found using MATHEMATICA. Finally, we also calculate the yield of the SPADS and SPOTL schemes.

1. Generation of elementary links

a. Single-photon scheme on Alice side

The application of the single-photon scheme on Alice's side leads Alice and the quantum repeater to share a state given in Eq. (E19). This state can be rewritten as

$$\rho_{\text{A-QR}^e} = A_1|\Psi^+\rangle\langle\Psi^+| + B_1|\Psi^-\rangle\langle\Psi^-| + C_1(|10\rangle\langle 10| + |01\rangle\langle 01|) + D_1|11\rangle\langle 11| + E_1|00\rangle\langle 00|, \quad \text{(F1)}$$

with $A_1 = A(\theta_A, Y_A)$, $B_1 = B(\theta_A, Y_A)$, $C_1 = C(\theta_A, Y_A)$, $D_1 = D(\theta_A, Y_A)$, and $E_1 = E(\theta_A, Y_A)$. Here, we have that

$$A(\theta, Y) = \frac{1}{Y} 2\cos^2(\theta)\sin^2(\theta)\eta(1-p_d) \times\{[F_{\text{prep}}^2 + (1-F_{\text{prep}})^2]\lambda + 2F_{\text{prep}}(1-F_{\text{prep}})(1-\lambda)\}, \quad \text{(F2)}$$

$$B(\theta, Y) = \frac{1}{Y} 2\cos^2(\theta)\sin^2(\theta)\eta(1-p_d) \times\{[F_{\text{prep}}^2 + (1-F_{\text{prep}})^2](1-\lambda) + 2F_{\text{prep}}(1-F_{\text{prep}})\lambda\}, \quad \text{(F3)}$$

$$C(\theta, Y) = \frac{2}{Y}\cos^2(\theta)\sin^2(\theta)p_d(1-p_d)(1-\eta), \quad \text{(F4)}$$

$$D(\theta, Y) = \frac{1}{Y}\cos^4(\theta)[2(1-\eta)\eta(1-p_d) + \eta^2(1-p_d) + 2(1-\eta)^2 p_d(1-p_d)], \quad \text{(F5)}$$

$$E(\theta, Y) = \frac{2}{Y}\sin^4(\theta)p_d(1-p_d). \quad \text{(F6)}$$

In the above Y denotes the yield or the probability of success of the single-photon scheme and is given by Eq. (E18). Subscript A indicates that in that expression for the yield and for each of the above defined coefficients we use $\theta = \theta_A$. Moreover, we have made here the following change of notation with respect to the Appendix E, $|\downarrow\rangle \rightarrow |0\rangle$ and $|\uparrow\rangle \rightarrow |1\rangle$.

b. SWAP gate in the middle node

In the next step, a SWAP gate is applied in the middle node to transfer the electron state to the nuclear spin of the NV center. This causes a depolarizing noise of parameter $F_{\text{swap}} = F_g^2$ (see Appendix A). The resulting state can then be written as

$$\rho_{\text{A-QR}^C} = F_{\text{swap}}\rho_{\text{A-QR}^e} + (1-F_{\text{swap}})\text{Tr}_{\text{QR}}[\rho_{\text{A-QR}^e}] \otimes \frac{\mathbb{I}_{2,\text{QR}}}{2}. \quad \text{(F7)}$$

c. The procedure on Bob's side

We now use the electron spin of the quantum repeater to generate the second quantum state. Here, the procedures for the SPADS and SPOTL schemes diverge.

In the procedure for the SPADS scheme, the quantum repeater generates a spin-photon entangled state where the photonic qubit is encoded in the time-bin degree of freedom. Since the spin-photon entangled state is imperfect, the electron and the photon share a state

$$\rho_{\text{QR}^e-B} = F_{\text{prep}}|\Psi^+\rangle\langle\Psi^+| + (1-F_{\text{prep}})|\Psi^-\rangle\langle\Psi^-|. \quad \text{(F8)}$$

Here, we use the following labeling for time-bin-encoded early and late modes of the photon: $|e\rangle = |1\rangle$, $|l\rangle = |0\rangle$. This photon is then sent toward Bob's detector. The lossy channel acts on such a time-bin-encoded qubit as an erasure channel and so the quantum spin-photon state of the successful events in which the photonic qubit successfully arrives at the detector is unaffected by the lossy channel.

For the SPOTL scheme, the repeater's electron spin and Bob's quantum memory generate a second state of the form given in Eq. (E19). We can rewrite this state as

$$\rho_{\text{QR}^e-B} = A_2|\Psi^+\rangle\langle\Psi^+| + B_2|\Psi^-\rangle\langle\Psi^-| + C_2(|10\rangle\langle 10| + |01\rangle\langle 01|) + D_2|11\rangle\langle 11| + E_2|00\rangle\langle 00|, \quad \text{(F9)}$$

with $A_2 = A(\theta_B, Y_B)$, $B_2 = B(\theta_B, Y_B)$, $C_2 = C(\theta_B, Y_B)$, $D_2 = D(\theta_B, Y_B)$, and $E_2 = E(\theta_B, Y_B)$.

d. Decoherence in the quantum memories

Decoherence of the carbon spin in the middle node can be modeled identically for both the SPADS and SPOTL scheme.

During the $n < n^*$ attempts to generate the state ρ_{QR^e-B}, the carbon spin in the middle node holding half of the state $\rho_{\text{A-QR}^C}$ will decohere. Using the decoherence model discussed in Appendix B, decoherence of the carbon spin will thus give us

$$\rho'_{\text{A-QR}^C} = F_{T_1}[F_{T_2}\rho_{\text{A-QR}^C} + (1-F_{T_2})(\mathbb{I}_2\otimes Z)\rho_{\text{A-QR}^C}(\mathbb{I}_2\otimes Z)^\dagger] + (1-F_{T_1})\text{Tr}_{\text{QR}}[\rho_{\text{A-QR}^C}] \otimes \frac{\mathbb{I}_{2,\text{QR}}}{2}. \quad \text{(F10)}$$

For key generation, Alice (SPADS and SPOTL schemes) and Bob (SPOTL scheme) can actually measure their electron spin(s) immediately after the generation of spin photon entanglement, preventing the effect of decoherence on these qubit(s).

2. Noise due to measurements

a. Measurement of the qubits of Alice and Bob

In the SPADS scheme, Alice performs a measurement on her electron spin immediately after each of the spin-photon entanglement generation events to prevent any decoherence with time of this qubit. This measurement causes an error modeled as a depolarizing channel of parameter F_m. Bob, on the other hand, performs a measurement on a photonic qubit that is encoded in the time-bin degree of freedom. His measurement utilizes the squashing map so that we can model the noise arising from this measurement as a depolarizing channel with parameter α_B as described in Appendix A. Hence, the total state just before the Bell measurement is given by

$$\rho_{A-QR-B} = F_m\alpha_B\rho'_{\text{A-QR}^c}\otimes\rho_{\text{QR}^e-B} + (1-F_m)\alpha_B\frac{\mathbb{I}_{2,A}}{2}\otimes\text{Tr}_A[\rho'_{\text{A-QR}^c}]\otimes\rho_{\text{QR}^e-B} + (1-\alpha_B)F_m\rho'_{\text{A-QR}^c}\otimes\text{Tr}_B[\rho_{\text{QR}^e-B}]\otimes\frac{\mathbb{I}_{2,B}}{2}$$
$$+(1-F_m)(1-\alpha_B)\text{Tr}_{AB}[\rho'_{\text{A-QR}^c}\otimes\rho_{\text{QR}^e-B}]\otimes\frac{\mathbb{I}_{4,AB}}{4}. \tag{F11}$$

For the SPOTL scheme, both Alice and Bob perform a measurement on their electron spins immediately after each of the spin-photon entanglement generation events. This measurement causes an error modeled as a depolarizing channel of parameter F_m on each qubit, which means that after both Alice and Bob succeeded in performing the single-photon scheme with the repeater, the total, four-qubit state just before the Bell-measurement and including the noise of the measurements of Alice and Bob will be given by

$$\rho_{A-QR-B} = F_m^2\rho'_{\text{A-QR}^c}\otimes\rho_{\text{QR}^e-B} + (1-F_m)F_m\left[\frac{\mathbb{I}_{2,A}}{2}\otimes\text{Tr}_A[\rho'_{\text{A-QR}^c}]\otimes\rho_{\text{QR}^e-B} + \rho'_{\text{A-QR}^c}\otimes\text{Tr}_B[\rho_{\text{QR}^e-B}]\otimes\frac{\mathbb{I}_{2,B}}{2}\right]$$
$$+(1-F_m)^2\text{Tr}_{AB}[\rho'_{\text{A-QR}^c}\otimes\rho_{\text{QR}^e-B}]\otimes\frac{\mathbb{I}_{4,AB}}{4}. \tag{F12}$$

b. Bell state measurement

Before the entanglement swapping, we have a total state ρ_{A-QR-B}. We now perform a Bell state measurement on the two qubits in the middle node. The error coming from this measurement is modeled by concatenation of depolarizing channels (see Appendix A), which means that the measurement is actually performed on

$$\rho_{\text{fin}} = F_g^2F_m^2\rho_{A-QR-B} + F_g^2(1-F_m^2)\text{Tr}_{QR^e}[\rho_{A-QR-B}]\otimes\frac{\mathbb{I}_{2,QR^e}}{2}$$
$$+(1-F_g^2)\text{Tr}_{QR}[\rho_{A-QR-B}]\otimes\frac{\mathbb{I}_{4,QR}}{4}. \tag{F13}$$

While $\rho'_{\text{A-QR}^c}$ is not Bell diagonal for the SPADS scheme, ρ_{QR^e-B} is, and so we find that taking into account the classical correction (which will be performed on the measured bit-value by Alice and Bob) the four cases corresponding to different measurement outcomes are equivalent. This means that if we model the correction to be applied to the quantum state rather than the classical bit, then the four postmeasurement bipartite states shared between Alice and Bob are exactly the same.

For the SPOTL scheme, both $\rho'_{\text{A-QR}^c}$ and ρ_{QR^e-B} are not Bell diagonal, which means that the resulting state of qubits of Alice and Bob after the Bell state measurement depends on the outcome of this Bell measurement and those four corresponding states are not equivalent under local unitary corrections. In fact, the two states corresponding to the $\Phi^\pm$ outcomes and the two states corresponding to the $\Psi^\pm$ outcomes are pairwise equivalent under local Pauli corrections. Hence, we will derive two different QBER corresponding to the following different resulting states shared between Alice and Bob,

$$\rho_{\Phi,AB} = (\mathbb{I}_A\otimes U_{\Phi^\pm,B})\text{Tr}_{QR}\left[\frac{(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I})\rho_{\text{fin}}(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I})^\dagger}{\text{Tr}(\rho_{\text{fin}}(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I}))}\right](\mathbb{I}\otimes U_{\Phi^\pm,B})^\dagger, \tag{F14}$$

$$\rho_{\Psi,AB} = (\mathbb{I}_A\otimes U_{\Psi^\pm,B})\text{Tr}_{QR}\left[\frac{(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I})\rho_{\text{fin}}(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I})^\dagger}{\text{Tr}(\rho_{\text{fin}}(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I}))}\right](\mathbb{I}\otimes U_{\Psi^\pm,B})^\dagger. \tag{F15}$$

Here $U_{\Phi^\pm,B}$ and $U_{\Psi^\pm,B}$ denote the four Pauli corrections implemented by Bob after the corresponding outcome of the Bell measurement. Note that for the SPADS scheme $\rho_{\Phi,AB} = \rho_{\Psi,AB}$.

3. The yield and QBER

a. Yield

For both SPADS and SPOTL scheme, we calculate the yield as the inverse of the number of channel uses required to generate one bit of raw key, $Y = 1/\mathbb{E}[N]$, where $\mathbb{E}[N]$ is given by Eq. (C1). For the SPOTL scheme in that formula, we use $p_{A/B} = Y_{A/B}$, where $Y_{A/B}$ denotes the yield of the single-photon scheme on Alice's or Bob's side given by Eq. (E18). For the SPADS scheme, p_A takes the same form as for the SPOTL scheme (but is now calculated for two thirds of the total distance between Alice and Bob rather than half), while p_B is the probability of registering a click in Bob's optical detection setup as in the SiSQuaRe scheme.

b. Extraction of the qubit error rates

By projecting these final corrected states onto the correct subspaces, we can obtain the qubit error rates e_z and e_{xy} (with our model we find that for both SPADS and SPOTL schemes the error rates in X and Y bases are the same). The state shared between Alice and Bob after the Pauli correction will always be the same for the SPADS scheme. Thus, there is only a single QBER e_z and e_{xy} independently of the outcome of the Bell measurement. For the SPOTL scheme that is not the case, there will be two set of QBER corresponding to the states $\rho_{\Phi,AB}$ and $\rho_{\Psi,AB}$:

$$e_{z,\Phi} = \mathrm{Tr}[(|00\rangle\langle 00| + |11\rangle\langle 11|)\rho_\Phi], \tag{F16}$$

$$e_{z,\Psi} = \mathrm{Tr}[(|00\rangle\langle 00| + |11\rangle\langle 11|)\rho_\Psi], \tag{F17}$$

$$\begin{aligned} e_{xy,\Phi} &= \mathrm{Tr}[(|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_\Phi] \\ &= \mathrm{Tr}[(|0_y 1_y\rangle\langle 0_y 1_y| + |1_y 0_y\rangle\langle 1_y 0_y|)\rho_\Phi], \end{aligned} \tag{F18}$$

$$\begin{aligned} e_{xy,\Psi} &= \mathrm{Tr}[(|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_\Psi] \\ &= \mathrm{Tr}[(|0_y 1_y\rangle\langle 0_y 1_y| + |1_y 0_y\rangle\langle 1_y 0_y|)\rho_\Psi]. \end{aligned} \tag{F19}$$

Again, for the SPADS scheme $e_{z,\Phi} = e_{z,\Psi} = e_z$ and $e_{xy,\Phi} = e_{xy,\Psi} = e_{xy}$.

c. Averaging the qubit error rates

We have now derived the qubit error rates as a function of the experimental parameters. For the SPOTL scheme, we now average the QBER over the two outcomes to get the final average QBER,

$$\langle e_z\rangle = \langle p_\Psi e_{z,\Psi} + p_\Phi e_{z,\Phi}\rangle, \tag{F20}$$

$$\langle e_{xy}\rangle = \langle p_\Psi e_{xy,\Psi} + p_\Phi e_{xy,\Phi}\rangle, \tag{F21}$$

where p_Ψ (p_Φ) is the probability of measuring one of the $|\Psi\rangle$ ($|\Phi\rangle$) states in the Bell measurement and $\langle\cdots\rangle$ is found by averaging the expression over the number of Bob's attempts n with the geometric distribution within the first n^* trials. For the SPADS scheme, $\langle e_z\rangle$ and $\langle e_{xy}\rangle$ can be averaged directly. The dependence on n arises from the decoherence terms F_{T_1} and F_{T_2}. Indeed, those terms correspond to the decoherence in the middle node during the attempts on Bob's side. Denoting by p_B the probability that in a single attempt Bob generates entanglement with the quantum repeater using the single-photon scheme for the SPOTL scheme and using direct transmission of the time-bin-encoded qubit from the repeater to Bob for the SPADS scheme, we have that the exponentials in those expressions can be averaged as follows [17]:

$$\langle e^{-cn}\rangle = \frac{p_B e^{-c}}{1-(1-p_B)^{n^*}}\,\frac{1-(1-p)^{n^*}e^{-cn^*}}{1-(1-p_B)e^{-c}}. \tag{F22}$$

APPENDIX G: SECRET-KEY FRACTION AND ADVANTAGE DISTILLATION

In this section, we review the formulas for the secret-key fraction for the QKD protocols used in our model as a function of the QBER.

1. One-way BB84 protocol

For the fully asymmetric BB84 protocol with standard one-way postprocessing, the secret-key fraction is given by [80,82]

$$r = 1 - h(e_x) - h(e_z), \tag{G1}$$

where $h(x)$ is the binary entropy function. Note that this formula is symmetric under the exchange of e_x and e_z; that is, the secret-key fraction is the same independent of whether we extract the key in the Z or X basis. As we will see later in this section, this is not the case for the six-state protocol with advantage distillation.

2. Six-state protocol with advantage distillation

Now we shall examine the six-state protocol with advantage distillation of Ref. [81]. For the purpose of this section, following the notation of Ref. [81], we shall denote the four Bell states as

$$|\psi(\mathsf{x},\mathsf{z})\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0+\mathsf{x}\rangle + (-1)^{\mathsf{z}}\,|1\rangle\,|1+\mathsf{x}\ (\mathrm{mod}\,2)\rangle), \tag{G2}$$

for $\mathsf{x},\mathsf{z}\in\{0,1\}$. We then write the Bell-diagonal state as

$$\rho_{AB} = \sum_{\mathsf{x},\mathsf{z}\in\{0,1\}} p_{\mathsf{xz}}\,|\psi(\mathsf{x},\mathsf{z})\rangle\,\langle\psi(\mathsf{x},\mathsf{z})|\,. \tag{G3}$$

The considered advantage distillation protocol is described in Ref. [81]. It is shown there that if the key is extracted in the Z basis, then the secret-key fraction for the fully asymmetric six-state protocol supplemented with this two-way postprocessing technique is given by

$$r_{\text{six-state}} = \max\left\{1 - H(P_{\mathsf{XZ}}) + \frac{P_{\tilde{\mathsf{X}}}(1)}{2}h\left[\frac{p_{00}p_{10}+p_{01}p_{11}}{(p_{00}+p_{01})(p_{10}+p_{11})}\right], \frac{P_{\tilde{\mathsf{X}}}(0)}{2}[1-H(P'_{\mathsf{XZ}})]\right\}, \tag{G4}$$

where

$$P_{\tilde{\mathsf{X}}}(0) = (p_{00}+p_{01})^2 + (p_{10}+p_{11})^2, \tag{G5}$$

$$P_{\tilde{\mathsf{X}}}(1) = 2(p_{00}+p_{01})(p_{10}+p_{11}), \tag{G6}$$

$$p'_{00} = \frac{p_{00}^2+p_{01}^2}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{G7}$$

$$p'_{10} = \frac{2p_{00}p_{01}}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{G8}$$

$$p'_{01} = \frac{p_{10}^2+p_{11}^2}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{G9}$$

$$p'_{11} = \frac{2p_{10}p_{11}}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{G10}$$

P_{XZ} (P'_{XZ}) is the probability distribution over the coefficients p_{xz} (p'_{xz}) and $H(P_{\mathsf{XZ}})$ $[H(P'_{\mathsf{XZ}})]$ is the Shannon entropy of this distribution.

Now let us have a look at how to link the Bell coefficients p_{xz} with our QBER e_z and e_{xy} (for all our schemes, the estimated QBER in the X basis is the same as in the Y basis). In this section, we assume the target state that Alice and Bob want to generate is $|\psi(0,0)\rangle$. Note that in the analysis in Appendices E and F it is the state $|\psi(1,0)\rangle$ that is a target, but of course the secret-key fraction analysis is independent of which Bell state is a target state as they are all the same up to local Pauli rotations. Hence, the relation between the Bell-diagonal coefficients and the QBER is

$$p_{10} + p_{11} = e_z, \tag{G11}$$

$$p_{01} + p_{11} = e_{xy}, \tag{G12}$$

$$p_{01} + p_{10} = e_{xy}, \tag{G13}$$

$$p_{00} + p_{01} + p_{10} + p_{11} = 1. \tag{G14}$$

Therefore,

$$\begin{aligned} p_{00} &= 1 - \frac{e_z}{2} - e_{xy}, \\ p_{01} &= e_{xy} - \frac{e_z}{2}, \\ p_{10} &= p_{11} = \frac{e_z}{2}. \end{aligned} \tag{G15}$$

And so,

$$P_{\bar{\mathsf{X}}}(0) = 1 - 2e_z + 2e_z^2, \tag{G16}$$

$$P_{\bar{\mathsf{X}}}(1) = 2(1 - e_z)e_z. \tag{G17}$$

It is important to note that for the above described advantage distillation, the amount of generated secret key depends on the basis in which they are extracted, as has been shown in Ref. [102]. Let us now have a look at the amount of keys that can be extracted in the X and Y bases. As has been shown in Ref. [102], the secret-key fraction in these cases is also given by Eq. (G4) but now the Bell coefficients depend on QBER in the following way:

$$\begin{aligned} p_{00} &= 1 - \frac{e_z}{2} - e_{xy}, \\ p_{10} &= e_{xy} - \frac{e_z}{2}, \\ p_{01} &= p_{11} = \frac{e_z}{2}. \end{aligned} \tag{G18}$$

And so,

$$\begin{aligned} P_{\bar{\mathsf{X}}}(0) &= 1 - 2e_{xy} + 2e_{xy}^2, \\ P_{\bar{\mathsf{X}}}(1) &= 2(1 - e_{xy})e_{xy}. \end{aligned} \tag{G19}$$

We note that we have assumed here that in the case of key extraction in Y basis, either Alice or Bob applies a local bit flip in the Y basis to the shared state, as the target state $|\psi(0,0)\rangle$ is anticorrelated in that basis.

In Ref. [102], it has been also observed that in the considered case of having the QBER in the X and Y bases being equal, the six-state protocol with advantage distillation allows us to extract more keys if they are extracted in the basis with higher QBER. This observation determines the basis that we use for extracting key for the single-photon and the SPOTL schemes that use fully asymmetric six-state protocol with advantage distillation. Specifically, for the single-photon scheme we observe higher QBER in the Z basis, while for the SPOTL scheme the QBER is higher in the X and Y bases. Therefore, these are the bases that we choose to use for extracting keys for those schemes.

For the SiSQuaRe and SPADS schemes, the symmetric six-state protocol is used. Hence, for those schemes we group the raw bits into three groups corresponding to three different key-extraction bases, and we extract the key separately for each of these bases. Finally, to obtain the final secret-key fraction, we note that for the symmetric six-state protocol we also need to include sifting; that is, only one third of all the raw bits were obtained by Alice and Bob measuring in the same basis (the raw bits for the protocol runs in which they measured in different bases are discarded). Hence, if we denote by r_i the secret-key fraction obtained from the group of raw bits in which both Alice and Bob measured in the basis i, the final secret-key fraction for the six-state protocol for those schemes is given by

$$r = \tfrac{1}{3}\left(\tfrac{1}{3}r_x + \tfrac{1}{3}r_y + \tfrac{1}{3}r_z\right). \tag{G20}$$

Clearly, in our case we have $r_x = r_y = r_{xy}$.

3. One-way six-state protocol

In Fig. 7, we have also plotted the secret-key fraction for the one-way six-state protocol. For the fully asymmetric protocol and the case in which the key is extracted in the Z-basis, it is given by [80]

$$\begin{aligned} r = 1 - e_z h\left[\frac{1 + (e_x - e_y)/e_z}{2}\right] \\ - (1 - e_z) h\left[\frac{1 - (e_x + e_y + e_z)/2}{1 - e_z}\right] - h(e_z). \end{aligned} \tag{G21}$$

Although this formula does not appear to be symmetric under the permutation of e_x, e_y, e_z, it is in fact invariant under this permutation [103]. This means that for the symmetric one-way six-state protocol, in our case the final secret-key fraction is given by the expression in Eq. (G21) multiplied by the sifting efficiency of one-third.

APPENDIX H: RUNTIME OF THE EXPERIMENT

In this section, we will detail how to perform an experiment that will be able to establish that a setup can surpass the capacity of a quantum channel modeling losses in a fiber [see Eq. (5)]. This experiment can validate a setup to qualify as a quantum repeater, without explicitly having to generate a secret key. We show then that, for the listed parameters in the main text, the single-photon scheme can be certified to be a quantum repeater within approximately 12 h.

The experiment is based on estimating the yield of the scheme and the individual QBER of the generated states. More specifically, here we will calculate the probability that, assuming our model is accurate and each individual run is independent and identically distributed, the observed estimates of the yield and the individual QBER are larger and smaller, respectively, than some fixed threshold values. If, with these threshold values for the yield and QBER, the calculated asymptotic secret key still surpasses the capacity, we can claim a working quantum repeater. The experiment consists of first performing n attempts at generating a state between Alice and Bob, from which the yield can be estimated by calculating the ratio of the successful attempts and n. Then, the QBER in each basis is estimated by Alice and Bob measuring in the same basis in each of the successful attempts.

Central to our calculation is the fact that, for n instances of a Bernoulli random variable with probability p, the probability that the number of observed successes $S(n)$ is smaller or equal than some value k is equal to

$$P[S(n) \leqslant k] = \sum_{i=0}^{k} \binom{n}{i} p^i (1-p)^{n-i}. \tag{H1}$$

Assuming the outcomes of our experiment are independent and identically distributed, the observed yield $\bar{Y}$ satisfies

$$\begin{aligned} P[\bar{Y} \leqslant (Y - t_Y)] &= P[n\bar{Y} \leqslant n(Y - t_Y)] \\ &= \sum_{i=0}^{\lfloor n(Y-t_Y) \rfloor} \binom{n}{i} Y^i (1-Y)^{n-i}, \end{aligned} \tag{H2}$$

where $Y - t_Y$ is the lower threshold. Let us make this more concrete with a specific calculation. For a distance of $17L_0$ the yield is equal to $\approx 5.6 \times 10^{-6}$. Setting the maximum deviation in the yield to $\bar{Y} = Y - t_Y$ with $t_Y = 2.0 \times 10^{-7}$ and the number of attempts to $n = 5 \times 10^9$ (which corresponds to approximately a runtime of 12 h, assuming a single attempt takes 8.5×10^{-6} s, corresponding to t_{prep} and a single-shot readout lasting 2.5×10^{-6} s), we find that

$$P[\bar{Y} \leqslant (Y - t_Y)] \leqslant 9.2 \times 10^{-10}. \tag{H3}$$

Similarly, for the individual errors $\{e_k\}_{k \in \{x,y,z\}}$ in the three bases, we have that

$$\begin{aligned} P[\bar{e}_k \geqslant (e_k + t_k)] &= P[m\bar{e}_k \geqslant m(e_k + t_k)] \\ &= \sum_{i=\lceil m(e_k+t_k) \rceil}^{m} \binom{m}{i} (e_k)^i (1 - e_k)^{m-i}. \end{aligned} \tag{H4}$$

Here we set $m = \lfloor \frac{n}{3}(Y - t_Y) \rfloor$, which is an estimate for the number of raw bits that Alice and Bob obtain from measurements in each of the three bases, for the total n attempts of the protocol. All the raw bits from those three sets are then compared to estimate the QBER in each of the three bases. Note that we gather the same amount of samples for each basis, even when an asymmetric protocol would be performed. Setting $t_i = t = 0.015$, $\forall i \in \{x, y, z\}$ and, as before, $n = 5 \times 10^9$, we find, at a distance of $17L_0$ where $e_z \approx 0.171$ and $e_y = e_x \approx 0.141$, that

$$P[\bar{e}_z \geqslant (e_z + t)] \leqslant 9.0 \times 10^{-5}, \tag{H5}$$

$$P[\bar{e}_y \geqslant (e_y + t)] = P[\bar{e}_x \geqslant (e_x + t)] \leqslant 2.7 \times 10^{-5}. \tag{H6}$$

Then, with probability at least

$$\begin{aligned} &\{1 - P[\bar{e}_x \geqslant (e_x + t)]\}\{1 - P[\bar{e}_y \geqslant (e_y + t)]\} \\ &\times \{1 - P[\bar{e}_z \geqslant (e_z + t)]\}\{1 - P[\bar{Y} \leqslant (Y - t_Y)]\} \\ &\geqslant 1 - 1.5 \times 10^{-4}, \end{aligned} \tag{H7}$$

none of the observed QBER and yield exceed their threshold conditions. The corresponding lowest secret-key rate for these parameters (with a yield of $Y - t_Y$ and QBER of $e_x + t_x$, $e_y + t_y$, $e_z + t_z$) is $\approx 1.97 \times 10^{-7}$, which we observe is greater than the secret-key capacity by a factor ≈ 3.29 [see Eq. (5)] at a distance of $17L_0$, since the secret-key capacity equals $-\log_2(1 - e^{-17}) \lesssim 5.97 \times 10^{-8}$.

Thus, with high probability we can establish that the single-photon scheme achieves a secret-key rate significantly greater than the corresponding secret-key capacity for a distance of $17L_0 \approx 9.2$ km within approximately 12 h.

APPENDIX I: MDI QKD

We note here that the single-photon scheme for generating keys is closely linked to the measurement-device-independent (MDI) QKD protocol [45]. In particular, it is an entanglement-based version of a scheme in which Alice and Bob prepare and send specific photonic qubit states to the heralding station in the middle, where the qubits are encoded in the presence or absence of the photon. We note that in the ideal case of the single-photon scheme, the spin-photon state is given in Eq. (E1). For the six-state protocol, the spin part of this state is then measured in the X, Y, or Z basis at random according to a fixed probability distribution (this probability distribution dictates whether we use symmetric or asymmetric protocol). Considering the probabilities of the individual measurement outcomes, this is equivalent to the scenario in which Alice and Bob choose one of the three set of states at random according to the same probability distribution and prepare each of the two states from that set with the probability equal to the corresponding measurement outcome probability. These sets do not form bases, as the two states within each set are not orthogonal. We will therefore refer to these sets here as "pseudobases." Depending on the chosen pseudobasis, they prepare one of the six states encoding the bit value of "0" or "1" in that pseudobasis. These states and the corresponding preparation probabilities are the following:

(1) pseudo-basis 1: $\{|0\rangle, |1\rangle\}$ with probabilities $\{\sin^2\theta, \cos^2\theta\}$,

(2) pseudo-basis 2: $\{\sin\theta\,|0\rangle + \cos\theta\,|1\rangle\,,\ \sin\theta\,|0\rangle - \cos\theta\,|1\rangle\}$ with probabilities $\{\frac{1}{2}, \frac{1}{2}\}$, and

(3) pseudo-basis 3: $\{\sin\theta\,|0\rangle + i\cos\theta\,|1\rangle\,,\ \sin\theta\,|0\rangle - i\cos\theta\,|1\rangle\}$ with probabilities $\{\frac{1}{2}, \frac{1}{2}\}$.

These states are then sent toward the beam-splitter station. The station performs the standard photonic Bell-state measurement and sends the outcome to both Alice and Bob. Alice and Bob discard all the runs for which the beam-splitter station measured A_2 [recall the measurement operators in Eq. (E10)]. They then exchange the classical information about their pseudobasis choice and keep only the data for the runs in which they both used the same basis. For those data, they apply the following postprocessing in order to obtain correlated raw bits:

(1) Pseudo-basis 1: For both outcomes A_0 and A_1, Bob flips the value of his bit.

(2) Pseudo-basis 2: For the outcome A_0, they do nothing, for the outcome A_1 Bob flips the value of his bit.

(3) Pseudo-basis 3: For the outcome A_0, they do nothing; for the outcome A_1, Bob flips the value of his bit.

In this way, Alice and Bob have generated their strings of raw bits.

We note here that the direct preparation of the six states from the three pseudobases described above in the photonic presence or absence degree of freedom is experimentally hard. This is related to the fact that linear optics does not allow us to easily perform the single-qubit rotations necessary to prepare these states. The use of memory-based NV centers offers a great advantage here, as in these schemes the rotations that allow us to obtain the required amplitudes of the photonic states are performed on the electron spins rather than the photons themselves. There has also been proposed an alternative scheme that also benefits from single-photon detection events in which Alice and Bob send coherent pulses to the heralding station [42,55].

[1] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, Phys. Rev. Lett. **85**, 2010 (2000).

[2] M. Krčo and P. Paul, Phys. Rev. A **66**, 024305 (2002).

[3] J. Preskill, arXiv:quant-ph/0010098.

[4] V. Giovannetti, S. Lloyd, and L. Maccone, Nature (London) **412**, 417 (2001).

[5] T. P. Spiller, K. Nemoto, S. L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn, New J. Phys. **8**, 30 (2006).

[6] M. Christandl and S. Wehner, in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, Berlin, 2005), pp. 217–235.

[7] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, Berlin, 2007), pp. 460–473.

[8] C. H. Bennett and G. Brassard, in *International Conference on Computer System and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

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

[10] J. L. Park, Found. Phys. **1**, 23 (1970).

[11] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun. **5**, 5235 (2014).

[12] M. Takeoka, S. Guha, and M. M. Wilde, IEEE Trans. Inf. Theory **60**, 4987 (2014).

[13] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).

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

[15] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[16] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, IEEE J. Sel. Top. Quantum Electron. **21**, 78 (2015).

[17] F. Rozpędek, K. D. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, Quantum Sci. Technol. **3**, 034002 (2018).

[18] H. J. Kimble, Nature (London) **453**, 1023 (2008).

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

[20] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).

[21] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **98**, 190503 (2007).

[22] N. Sangouard, C. Simon, B. Zhao, Y.-A. Chen, H. de Riedmatten, J.-W. Pan, and N. Gisin, Phys. Rev. A **77**, 062301 (2008).

[23] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, Phys. Rev. A **92**, 022357 (2015).

[24] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).

[25] W. Munro, K. Harrison, A. Stephens, S. Devitt, and K. Nemoto, Nat. Photon. **4**, 792 (2010).

[26] N. K. Bernardes and P. van Loock, Phys. Rev. A **86**, 052301 (2012).

[27] W. Munro, A. Stephens, S. Devitt, K. Harrison, and K. Nemoto, Nat. Photon. **6**, 777 (2012).

[28] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).

[29] K. Azuma, K. Tamaki, and H.-K. Lo, Nat. Commun. **6**, 6787 (2015).

[30] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, Appl. Phys. B **122**, 1 (2016).

[31] P. C. Humphreys, N. Kalb, J. P. Morits, R. N. Schouten, R. F. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, Nature (London) **558**, 268 (2018).

[32] M. H. Abobeih, J. Cramer, M. A. Bakker, N. Kalb, M. Markham, D. J. Twitchen, and T. H. Taminiau, Nat. Commun. **9**, 2552 (2018).

[33] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson, Science **356**, 928 (2017).

[34] T. H. Taminiau, J. Cramer, T. van der Sar, V. V. Dobrovitski, and R. Hanson, Nat. Nanotechnol. **9**, 171 (2014).

[35] S. B. van Dam, P. C. Humphreys, F. Rozpędek, S. Wehner, and R. Hanson, Quantum Sci. Technol. **2**, 034002 (2017).

[36] M. Blok, N. Kalb, A. Reiserer, T. Taminiau, and R. Hanson, Faraday Discuss. **184**, 173 (2015).

[37] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, Nat. Commun. **7**, 11526 (2016).

[38] A. Reiserer, N. Kalb, M. S. Blok, K. J. M. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, Phys. Rev. X **6**, 021040 (2016).

[39] W. Gao, A. Imamoglu, H. Bernien, and R. Hanson, Nat. Photon. **9**, 363 (2015).

[40] S. Bogdanovic, S. B. van Dam, C. Bonato, L. C. Coenen, A. Zwerver, B. Hensen, M. S. Liddy, T. Fink, A. Reiserer, M. Loncar, and R. Hanson, Appl. Phys. Lett. **110**, 171103 (2017).

[41] C. Cabrillo, J. I. Cirac, P. Garcia-Fernandez, and P. Zoller, Phys. Rev. A **59**, 1025 (1999).

[42] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature (London) **557**, 400 (2018).

[43] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[44] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[45] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[46] S. Pirandola, arXiv:1601.00966.

[47] S. D. Barrett and P. Kok, Phys. Rev. A **71**, 060310 (2005).
[48] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán *et al.*, Nature (London) **526**, 682 (2015).
[49] B. Hensen, N. Kalb, M. Blok, A. Dréau, A. Reiserer, R. Vermeulen, R. Schouten, M. Markham, D. Twitchen, K. Goodenough *et al.*, Sci. Rep. **6**, 30289 (2016).
[50] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. Blok, L. Robledo, T. Taminiau, M. Markham, D. Twitchen, L. Childress *et al.*, Nature (London) **497**, 86 (2013).
[51] P. Maunz, D. Moehring, S. Olmschenk, K. Younge, D. Matsukevich, and C. Monroe, Nat. Phys. **3**, 538 (2007).
[52] R. Stockill, M. J. Stanley, L. Huthmacher, E. Clarke, M. Hugues, A. J. Miller, C. Matthiesen, C. Le Gall, and M. Atatüre, Phys. Rev. Lett. **119**, 010503 (2017).
[53] A. Delteil, Z. Sun, W.-b. Gao, E. Togan, S. Faelt, and A. Imamoğlu, Nat. Phys. **12**, 218 (2016).
[54] C. W. Chou, H. de Riedmatten, D. Felinto, S. V. Polyakov, S. J. van Enk, and H. J. Kimble, Nature (London) **438**, 828 (2005).
[55] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, arXiv:1805.05511.
[56] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X **8**, 031043 (2018).
[57] J. S. Ivan, K. K. Sabapathy, and R. Simon, Phys. Rev. A **84**, 042311 (2011).
[58] M. W. Doherty, N. B. Manson, P. Delaney, F. Jelezko, J. Wrachtrup, and L. C. L. Hollenberg, Phys. Rep. **528**, 1 (2013).
[59] L. Robledo, L. Childress, H. Bernien, B. Hensen, P. F. A. Alkemade, and R. Hanson, Nature (London) **477**, 574 (2011).
[60] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham *et al.*, Science **336**, 1283 (2012).
[61] N. Kalb, P. C. Humphreys, J. J. Slim, and R. Hanson, Phys. Rev. A **97**, 062330 (2018).
[62] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen *et al.*, Science **345**, 532 (2014).
[63] E. M. Purcell, H. C. Torrey, and R. V. Pound, Phys. Rev. **69**, 37 (1946).
[64] D. Englund, B. Shields, K. Rivoire, F. Hatami, J. Vučković, H. Park, and M. D. Lukin, Nano Lett. **10**, 3922 (2010).
[65] J. Wolters, A. W. Schell, G. Kewes, N. Nüsse, M. Schoengen, H. Döscher, T. Hannappel, B. Löchel, M. Barth, and O. Benson, Appl. Phys. Lett. **97**, 141108 (2010).
[66] T. Van Der Sar, J. Hagemeier, W. Pfaff, E. C. Heeres, S. M. Thon, H. Kim, P. M. Petroff, T. H. Oosterkamp, D. Bouwmeester, and R. Hanson, Appl. Phys. Lett. **98**, 193103 (2011).
[67] A. Faraon, C. Santori, Z. Huang, V. M. Acosta, and R. G. Beausoleil, Phys. Rev. Lett. **109**, 033604 (2012).
[68] B. J. Hausmann, B. J. Shields, Q. Quan, Y. Chu, N. P. De Leon, R. Evans, M. J. Burek, A. S. Zibrov, M. Markham, D. J. Twitchen, H. Park, M. D. Lukin, and M. Loncar, Nano Lett. **13**, 5791 (2013).
[69] J. C. Lee, D. O. Bracher, S. Cui, K. Ohno, C. A. McLellan, X. Zhang, P. Andrich, B. Alemán, K. J. Russell, A. P. Magyar, I. Aharonovich, A. Bleszynski Jayich, D. Awschalom, and E. L. Hu, Appl. Phys. Lett. **105**, 261101 (2014).
[70] L. Li, T. Schröder, E. H. Chen, M. Walsh, I. Bayn, J. Goldstein, O. Gaathon, M. E. Trusheim, M. Lu, J. Mower, M. Cotlet, M. L. Markham, D. J. Twitchen, and D. Englund, Nat. Commun. **6**, 6173 (2015).
[71] J. Riedrich-Möller, S. Pezzagna, J. Meijer, C. Pauly, F. Mücklich, M. Markham, A. M. Edmonds, and C. Becher, Appl. Phys. Lett. **106**, 221103 (2015).
[72] A. Faraon, P. E. Barclay, C. Santori, K. M. C. Fu, and R. G. Beausoleil, Nat. Photon. **5**, 301 (2011).
[73] P. E. Barclay, K. M. C. Fu, C. Santori, A. Faraon, and R. G. Beausoleil, Phys. Rev. X **1**, 011007 (2011).
[74] M. Gould, E. R. Schmidgall, S. Dadgostar, F. Hatami, and K. M. C. Fu, Phys. Rev. Appl. **6**, 2 (2016).
[75] H. Kaupp, C. Deutsch, H. C. Chang, J. Reichel, T. W. Hänsch, and D. Hunger, Phys. Rev. A **88**, 053812 (2013).
[76] S. Johnson, P. R. Dolan, T. Grange, A. A. Trichet, G. Hornecker, Y. C. Chen, L. Weng, G. M. Hughes, A. A. Watt, A. Auffèves, and J. M. Smith, New J. Phys. **17**, 122003 (2015).
[77] D. Riedel, I. Söllner, B. J. Shields, S. Starosielec, P. Appel, E. Neu, P. Maletinsky, and R. J. Warburton, Phys. Rev. X **7**, 031040 (2017).
[78] D. Hunger, T. Steinmetz, Colombe, Y., C. Deutsch, T. W. Hänsch, and J. Reichel, New J. Phys. **12**, 065038 (2010).
[79] E. Janitz, M. Ruf, M. Dimock, A. Bourassa, J. Sankey, and L. Childress, Phys. Rev. A **92**, 043844 (2015).
[80] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[81] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, Phys. Rev. A **76**, 032312 (2007).
[82] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[83] A. Khalique and B. C. Sanders, J. Opt. Soc. Am. B **32**, 2382 (2015).
[84] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, Appl. Phys. B **122**, 1 (2016).
[85] M. Pant, H. Krovi, D. Englund, and S. Guha, Phys. Rev. A **95**, 012304 (2017).
[86] K. Goodenough, D. Elkouss, and S. Wehner, New J. Phys. **18**, 063005 (2016).
[87] E. Kaur and M. M. Wilde, Phys. Rev. A **96**, 062318 (2017).
[88] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka, New J. Phys. **20**, 063025 (2018).
[89] N. Davis, M. E. Shirokov, and M. M. Wilde, Phys. Rev. A **97**, 062310 (2018).
[90] C. Ottaviani, R. Laurenza, T. P. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, in *Quantum Information Science and Technology II* (International Society for Optics and Photonics, Edinburgh, 2016), Vol. 9996, p. 999609.
[91] R. Laurenza, S. L. Braunstein, and S. Pirandola, Sci. Rep. **8**, 15267 (2018).
[92] R. Laurenza, S. Tserkis, L. Banchi, S. L. Braunstein, T. C. Ralph, and S. Pirandola, arXiv:1808.00608 (2018).
[93] M. Fox, *Quantum Optics: An Introduction* (Oxford University Press, Oxford, UK, 2006), Vol. 15.
[94] R. Paschotta, *Encyclopedia of Laser Physics and Technology* (John Wiley & Sons, Hoboken, NJ, 2008).
[95] S. Zaske, A. Lenhard, C. A. Keßler, J. Kettler, C. Hepp, C. Arend, R. Albrecht, W.-M. Schulz, M. Jetter, P. Michler *et al.*, Phys. Rev. Lett. **109**, 147404 (2012).

[96] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, New J. Phys. **18**, 083015 (2016).

[97] E. T. Campbell and S. C. Benjamin, Phys. Rev. Lett. **101**, 130502 (2008).

[98] N. H. Nickerson, J. F. Fitzsimons, and S. C. Benjamin, Phys. Rev. X **4**, 041041 (2014).

[99] I. L. Chuang, D. W. Leung, and Y. Yamamoto, Phys. Rev. A **56**, 1114 (1997).

[100] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Phys. Rev. A **89**, 012325 (2014).

[101] S. R. Jammalamadaka and A. Sengupta, *Topics in Circular Statistics* (World Scientific, Singapore, 2001), Vol. 5.

[102] G. Murta, F. Rozpędek, J. Ribeiro, D. Elkouss, and S. Wehner (unpublished).

[103] R. Renner, arXiv:quant-ph/0512258.