PAPER • OPEN ACCESS

Finite-key analysis for memory-assisted decoy-state quantum key distribution

To cite this article: Guillermo Currás Lorenzo and Mohsen Razavi 2020 *New J. Phys.* **22** 103005

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
13 May 2020

REVISED
3 August 2020

ACCEPTED FOR PUBLICATION
21 August 2020

PUBLISHED
2 October 2020

PAPER

Finite-key analysis for memory-assisted decoy-state quantum key distribution

Guillermo Currás Lorenzo[1] and Mohsen Razavi

School of Electronic and Electrical Engineering, University of Leeds, Leeds, United Kingdom
[1] Author to whom any correspondence should be addressed.

E-mail: G.J.CurrasLorenzo@leeds.ac.uk

Keywords: quantum key distribution, quantum communications, quantum memories, quantum optics, quantum repeaters

Abstract

Memory-assisted quantum key distribution (MA-QKD) systems are among novel promising solutions that can improve the key-rate scaling with channel loss. By using a middle node with quantum storage and measurement functionalities, they offer the same key-rate scaling with distance as a single-node quantum repeater. However, the distance at which they can surpass the nominal key rate of repeaterless systems, in terms of bits per second, is typically long, owing to the efficiency and/or interaction time issues when one deals with quantum memories. This crossover distance can be a few hundred kilometres, for instance, when one relies on the exchange of infinitely many key bits for the key-rate analysis. In a realistic setup, however, we should account for the finite-key effects in our analysis. Here, we show that accounting for such effects would actually favour MA-QKD setups, by reducing the crossover distance to the regime where realistic implementations can take place. We demonstrate this by rigorously analysing a decoy-state version of MA-QKD, in the finite-key regime, using memory parameters already achievable experimentally. This provides us with a better understanding of the advantages and challenges of working with memory-based systems.

1. Introduction

Quantum key distribution (QKD) has made a lot of progress as part of the solution package for secure communications in the quantum era [1]. But, when it comes to long distances, quantum technologies still have a long way to go before they can replicate the same functionalities that public-key cryptography offers. In terrestrial networks, such as the infrastructure that today's Internet is based on, the biggest challenge to overcome is perhaps the exponential growth of loss in optical fibres [2]. This makes it extremely difficult to perform QKD at long distances without trusted middle nodes. Quantum repeaters are potential solutions, but none of their theoretical architectures can currently be implemented experimentally to the full effect [3]. For instance, probabilistic quantum repeaters [4–6] would require quantum memory (QM) modules with high coupling efficiencies to light and with coherence times exceeding the transmission delays, which are hard to achieve together [7]. That said, even if the current QMs are not sufficiently advanced for quantum repeaters, they may still be used to offer key-rate improvements in some of the existing QKD systems. Working on such memory-assisted QKD (MA-QKD) systems paves the way for future scalable quantum repeaters. This work studies the secret key rate for decoy-state MA-QKD systems in the practical regime where only a finite block of data is exchanged among QKD users.

MA-QKD setups [7, 8] are based on the measurement-device-independent QKD (MDI-QKD) protocol [9], in which Alice and Bob send BB84-encoded pulses to a middle node, Charlie, who performs a Bell-state measurement (BSM). In MDI-QKD, a raw key bit can be generated if both pulses survive the channel loss in the same round and the BSM is successful. In MA-QKD, however, Charlie employs two QMs to store the quantum state of the users' pulses, and only performs the BSM when both memories have been loaded. This will allow the pulses that arrive in different rounds to be combined to produce a key bit. Thus, the key-rate scaling is improved from η^2 in MDI-QKD to η in MA-QKD [7], where η is the transmittance of

the channel between Alice/Bob and Charlie. Together with the recently introduced twin-field QKD (TF-QKD) [10], MA-QKD is a strong contender to beat the current rate versus distance records in QKD. Such an advantage has recently been demonstrated experimentally using silicon vacancy centres [11].

Offering advantage in a realistic setup that relies on imperfect QMs is not without its own challenges. For instance, photon-memory coupling can introduce additional loss in the setup. Some memories have also a long photon-memory interaction time that requires users to employ a low source repetition rate. The better scaling with channel loss can only offset these effects after a certain distance, which we refer to as the crossover distance. If this distance happens to be long, it would then be difficult to experimentally implement a stable system that benefits from such an advantage. Other effects, such as decoherence in the QMs, also need to be taken into account when evaluating system performance [7] and they typically exacerbate the situation. Additionally, in realistic setups, we should consider the effect of using weak laser pulses by the users in conjunction with finite-key effects. In this work, we develop a security analysis that accounts for all the above, and, in particular, quantify the interplay between the crossover distance and other parameters of the system.

Several analyses of MA-QKD have already been carried out, under varying assumptions and for different implementations of QMs. However, most of them [8, 12, 13] assume single-photon sources, which are difficult to attain in practice. In many QKD experiments, attenuated laser sources are used, instead. The multi-photon components in the signals generated by these sources introduce security loopholes, and they need to be dealt with [14]. The decoy-state method [15] is often used to bound the leaked information from these multi-photon signals, thus closing the loophole. This method involves the statistical estimation of channel probabilities, based on data collected from the use of different laser intensities. This statistical characterisation of the channel would only be perfect if one could collect an infinite amount of data by using the channel infinitely many times. In practice, a QKD experiment will run for a fixed amount of time, and a finite-size dataset will be generated [16]. By using statistical analyses based on concentration inequalities, it has been shown that a bound on the leaked information can be computed [16, 17], thus a secret key can still be distilled, with a failure probability that can be made arbitrarily small. However, as the total number of signals exchanged (the block size) gets smaller, the obtainable secret key rate is reduced. In fact, if the block size is too small, no secret key rate may be obtained at all.

In this paper, we provide the first analysis of a decoy-state MA-QKD setup that accounts for the statistical fluctuations that arise from generating a finite-size key. Previous work [7] on MA-QKD has only considered the asymptotic limit in which the users exchange an infinite number of signals, and under simplified assumptions on the loading of QMs with attenuated laser sources. In our finite-key analysis, we compare MA-QKD performance with that of a no-memory MDI-QKD system, by using parameters from state-of-the-art experiments on quantum memories [12]. We find that MA-QKD is inherently more resistant to finite-key effects, and it experiences a lower reduction in secret key rate than MDI-QKD. In particular, we see that once these effects are considered, the distance from which MA-QKD offers an advantage is reduced. This would make it easier for experimentalists to implement a decoy-state MA-QKD setup that outperforms, in terms of secret key rate versus distance, the equivalent decoy-state BB84 or MDI-QKD setups.

In terms of key rate, MA-QKD may not outperform the recently introduced TF-QKD, at least with state-of-the-art quantum memories. However, one should be careful when comparing systems that have different requirements. For instance, the single-photon interference of TF-QKD demands phase stability over long channels, which is experimentally difficult, and which MA-QKD does not need. We believe that comparing MA-QKD with MDI-QKD is the fairest when it comes to the requirements of each system. We note that there exists some recent work on memory assisted TF-QKD [18], which specifies under what circumstances adding quantum memories to TF-QKD setups can be advantageous. Moreover, we believe that MA-QKD is of special interest as the very first step towards building memory-based quantum repeaters. Unlike TF-QKD, or other no-memory systems, these offer a scalable solution for long distance quantum communications. Any practical progress with quantum repeaters would be based on fully understanding and implementing MA-QKD as the simplest memory-based repeater system. Our findings for MA-QKD systems suggest that memory-based quantum repeaters may also be resilient to finite-key effects, at least when users access them with decoy-state sources.

The rest of the paper is organised as follows. In section 2, we describe the analysed setup, placing an emphasis on the QM modules, and the different parameters that are used for modelling them. In section 3, we explain how different system parameters affect the secret-key rate. In section 4, we compare the secret key rate achievable in decoy-state MA-QKD and decoy-state MDI-QKD with examples from warm vapour and cold atomic ensembles. Section 5 concludes the paper with our interpretation of the results.

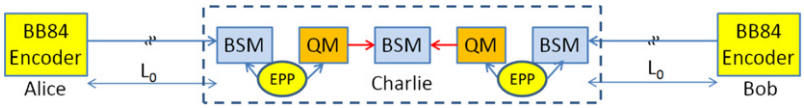

Figure 1. The schematic of an MA-QKD system. The two users Alice and Bob use decoy-state BB84 encoders to generate polarisation/phase encoded signals. Charlie, in the middle, uses EPP sources to teleport the state sent by the users to the corresponding memories. When both memories are loaded, their states are converted back to photons and combined in the middle BSM. For an example of the BSM module, see figure 4 of appendix A.

2. System description

In this section, we describe our MA-QKD setup and the assumptions we make on different devices and components of the system.

Figure 1 shows the schematic of the MA-QKD setup considered in this work. Here, in each round, Alice and Bob each send decoy-state BB84 states in their chosen basis. Charlie verifies the receipt of the transmitted signal by generating an entangled photon pair (EPP) on each side to effectively teleport the state of the users to a local photon on his site. The side BSMs in figure 1 would herald the success of such an event, in which case the remaining photon of the EPP source will be written to the corresponding QM. That is, its photonic state is transferred to the memory, and will be kept there until the state of the other user is also successfully received and teleported to its respective QM. At this point, the two QMs will be read, i.e., their states will be transferred to photons on which the middle BSM is performed. At the end of the protocol, Charlie announces his measurement results, and Alice and Bob would follow with conventional steps for sifting and post-processing of their key bits.

Note that the teleportation scheme used here to herald and transfer the state of photons is not an ideal one. In an ideal teleportation setting, the users have to send ideal single photons, whereas here they are using weak laser pulses. The effect of the multi-photon components has then to be taken into account. We analyse the memory-loading procedure for weak laser pulses in appendix A. In this scheme, we are also delaying the writing of the second photon of the EPP until we learn about the success of teleportation. While there is a chance that the transfer of this photonic state to the QM may fail, this delayed writing process has the advantage that the QM initialisation is not necessary in each round [12], but only when a writing procedure has been attempted. This helps with maximising the repetition rate of the protocol, especially when the initialisation phase is time consuming. We account for the failure in transferring a local single photon to the memory by the memory writing efficiency parameter.

Finally, while, in practice, an ideal EPP source as assumed here may not be realistic, it would help us obtain the key features of our finite-key analysis without overly complicating the calculations. The former issue can be managed by techniques introduced in reference [12], where they propose a quasi-EPP scheme based on single-photon sources, instead. It is also possible to create a photon-QM entangled pair in certain QMs [13, 19]. In all cases, we should be careful with the possible multiple excitations we may locally create at Charlie's node to not violate the conditions for the proper operation of MA-QKD systems [12, 20]. Under above considerations, we believe that the main result from our paper, i.e., the resilience of the decoy-state MA-QKD to finite-key effects, should still hold.

In the following, we describe the key components of our system in more detail.

2.1. Quantum memories

We model QMs using a few relevant parameters to our setup, while keeping our model as general as possible:

- The writing efficiency, denoted as η_w, is the probability of successfully transferring a single-photon state to the QM. We refer to this process by the term 'loading'.
- The reading efficiency, denoted as η_{r}, is the probability to transfer the qubit state stored in the QM back to a single photon. We assume that, at time t after loading, $\eta_{\mathrm{r}}(t) = \eta_{\mathrm{r}0}\exp[-t/T_1]$, where $\eta_{\mathrm{r}0}$ denotes the reading efficiency at time $t = 0$ and T_1 is the decay time constant of the QM.
- The QM decoherence time constant is denoted by T_2. We consider two decoherence processes: dephasing and depolarisation. In the case of dephasing, for an initial state $\rho(0)$ of the QM, the state at a time t after loading will be $$\rho(t) = p(t)\rho(0) + [1 - p(t)]\sigma_z\rho(0)\sigma_z, \quad (1)$$

where $p(t) = [1 + \exp(-t/T_2)]/2$. Dephasing will only affect X-basis states. For a depolarisation process, we assume

$$\rho(t) = p(t)\rho(0) + \frac{1-p(t)}{3}[\sigma_z\rho(0)\sigma_z + \sigma_x\rho(0)\sigma_x + \sigma_y\rho(0)\sigma_y]. \quad (2)$$

In both cases, we treat the QM state as a qubit for which σ_x, σ_y, and σ_z are its corresponding Pauli operators.

- We denote the interaction time with single photons as τ_{int}, for both reading and writing procedures. We denote the initialisation time of the QM as τ_{init}. Because of our delayed-writing assumption, a writing procedure will always be followed by a reading procedure, and the QM only needs to be initialised after reading.
- The writing time is denoted as τ_w, and the reading time is denoted as τ_{r}. For our delayed writing procedure, we assume $\tau_w = \tau_{\text{int}}$ and $\tau_{\text{r}} = \tau_{\text{int}} + \tau_{\text{init}}$. We effectively neglect the required time for measurement in both cases.
- We denote as τ_{p} the pulse duration of both the user sources and the EPP sources, which are assumed to have matching pulse shapes. We assume $\tau_{\text{p}} = \tau_w$ to maximize the writing efficiency into the memory. The MA-QKD system is to be run at a repetition rate of $R_{\text{s}} = 1/\tau_{\text{p}}$.

2.2. Channel and source model

Similarly, we present our assumptions on the channel and the users sources:

- We assume that the user sources produce phase-randomised coherent states, and that the intensity of the pulse can be perfectly tuned in each round. The users select a random intensity, in terms of mean number of photons, from the set $\{z, w_1, w_2, v\}$ with probability $\{p_z, p_{w_1}, p_{w_2}, p_v\}$. Emissions with the z intensity will be encoded in the Z basis, and they will be used to generate the raw key. Emissions with any other intensity will be encoded in the X basis, and they will be used to estimate the single-photon counts and their corresponding phase-error rate. We will refer to z as the signal intensity, and to $\{w_1, w_2, v\}$ as the decoy intensities. Our model can work with either polarisation or phase encoding. We denote the source repetition rate as R_{s}.
- We assume non-resolving detectors with efficiency η_{d} and a dark count rate γ_{dc}. The latter includes intrinsic effects as well as background photons in the channel. The dark count probability per detector per round of the protocol is $p_{\text{dc}} = \gamma_{\text{dc}}\tau_{\text{p}}$.
- We denote the total length of the channel separating Alice and Bob by L. We assume that the central node is located exactly halfway between the users. We denote the attenuation length of the channel by L_{att}. The transmission coefficient for each leg of the channel is given by $\eta_{\text{ch}} = \exp(\frac{-L}{2L_{\text{att}}})$.
- We consider the effect of setup misalignment between the user sources and the measurement devices in the central node. The standard way to model misalignment in QKD is by a misalignment probability e_{mis}, and previous analyses of MA-QKD have also modelled it that way [7]. However, as explained in appendix A, such a model is not directly applicable when considering the indirect loading of QMs with weak laser pulses. Here, we model misalignment by assuming that the encoding modes, e.g., horizontal and vertical polarisations, have been rotated from their ideal settings by a random angle θ. We then average over θ to find parameters of interest.
- In our setup, we allow for the usage of frequency converters to match the frequency of the telecom signals sent by the users with that of the EPP source. The EPP source, in one leg, should generate a beam that interacts with the QM. For a degenerate EPP source, this would typically require us to downconvert the frequency of the other beam to the telecom band. One can, in principle, design a non-degenerate EPP source, but we should then be careful with the extent of multiple excitations in the source [20]. We account for the efficiency of frequency converters by including additional loss in our setup.

3. Key-rate analysis

In this section, we find the secret key generation rate for our decoy-state MA-QKD setup, in both the asymptotic and finite-key regimes. We assume the nominal mode of operation in which no eavesdropper is present, and the system is only affected by device imperfections. Also, for simplicity, we assume that the sources used by Alice and Bob, and the channels connecting them to the middle node are identical.

3.1. Asymptotic case

In this subsection, we calculate the key rate obtainable in the limit that the users exchange an infinite number of signals. In this regime, we can assume that the signal intensity is used with probability $p_z \simeq 1$,

and that the decoy-state analysis provides a perfect estimate of the single-photon channel probabilities. Under these assumptions, the secret key rate is lower bounded by [7]

$$R \geqslant R_{\mathrm{s}} \left[Q_{11}^{Z} \left(1 - h(e_{\mathrm{ph}})\right) - f Q_Z h(e_Z) \right], \tag{3}$$

where Q_Z is the probability of generating a sifted key bit per round of the protocol, and e_Z is the error rate of the sifted key. Also, Q_{11}^{Z} is the single-photon contribution to Q_Z, and e_{ph} is the phase-error rate of these single-photon components.

Our objective here is to calculate what Alice and Bob would observe in a nominal experiment for directly measurable parameters Q_Z and e_Z, and their corresponding estimation for Q_{11}^{Z} and e_{ph} after using the decoy state method. For this, we mainly use the method introduced in [7], but we adjust it as needed to account for the specific components of our model. In particular, in the case of weak laser pulses at the source, we need to pay special attention to the modelling of misalignment in the channel. We also extend the results of [7] to depolarising channels.

Appendix A provides a detailed and self-contained description of our analysis. In short, we first obtain the exact expression for loading probability p_{load}^{μ} and loading error rate e_{load}^{μ} when Alice/Bob sends a phase-randomised coherent state with intensity μ under a generic model for channel misalignment. This parameter would then allow us to calculate the average number of rounds needed to load both memories, and the corresponding state of the memories after a heralded loading. We will then account for memory decoherence and decay processes and calculate the rate of success, and the corresponding error rate, for the middle BSM. Appendix A.2.1, provides the analytical form for all parameters needed in equation (3).

3.2. Finite-key regime

Now, we calculate the secret key rate in the more realistic scenario where the number of signals exchanged by the users is finite. In this regime, we still derive the secret key from the data points for which both users have used the Z basis, but we also need to take into account the rounds in which the users employ decoy intensities. In this case, we can no longer assume that the decoy-state analysis provides a perfect estimate of the single-photon statistics Q_{11}^{Z} and e_{ph}. Instead, we use a statistical analysis to bound them. Under our new assumptions, the total secret key length K satisfies

$$K \geqslant M_{11}^{Z}[1 - H(e_{\mathrm{ph}})] - M_Z H(e_Z), \tag{4}$$

where M_Z is the length of the sifted key, generated from the events in which both users selected the Z basis (i.e., the z intensity), and e_Z is its bit error rate; M_{11}^{Z} is the number of bits in this sifted key that originated from single-photon emissions, and e_{ph} is their phase-error rate.

In an experimental implementation of the protocol, the measurable observables available to us are the sets $\{M^{ab}\}$ and $\{E^{ab}\}$, where M^{ab} is the total number of measurement counts when Alice has used intensity a *and* Bob has used intensity b, while E^{ab} is the number of such events that result in error. The objective of Alice and Bob is to use this data to obtain statistical bounds on M_{11}^{Z} and e_{ph}.

The full description of our statistical analysis appears in appendix B. We use the idea in [21] to perform our statistical fluctuation analysis using X-basis data only. This would make our statistical estimation procedure more efficient. By applying tight multiplicative Chernoff bounds [16], we are then able to use the measured counts M^{ab} and E^{ab} to set linear constraints on the possible values that M_{11}^{Z} and e_{ph} could take. These constraints enable us to express the desired bounds on these quantities as the solution to two linear programs. We use the analytical estimation procedure introduced in [17] to solve these programs.

For our numerical simulations, we still need to make some assumptions on the obtained measurement results in a nominal experiment. For this purpose, we use the expected values for relevant parameters using the corresponding probability in the asymptotic regime, derived in the previous subsection. That is, we assume

$$M^{ab} = N Q^{ab} \quad \text{and} \quad E^{ab} = e_{ab} M^{ab}, \tag{5}$$

where N is the total number of rounds, i.e., the number of transmitted pulses by Alice/Bob, in the protocol, Q^{ab} is the probability of having a successful measurement originating from intensities a, for Alice, and b, for Bob, and e_{ab} is the probability that this measurement results in an error. Appendix A.2.2 provides the derivation and the analytical form for all these parameters.

In our finite-key analysis, we have only considered the effect of statistical fluctuations on parameter estimation. Thus, in our key rate formula in equation (4), we have neglected some of the less significant terms that usually appear in a rigorous finite-key analysis. The latter is to adhere to the universal composable framework [22, 23]; e.g., we direct the reader to equation (1) of [17]. We have neglected these terms for simplicity, as they are, in practice, only on the order of tens of bits, and because their effect is identical for the memory-assisted and no-memory systems, which the present work aims to compare.

Table 1. Parameter values of recently demonstrated warm vapour (WV) and cold atom (CA) ensembles [12], as well as silicon vacancy (SV) centres, used in the simulations in this work. For simplicity, in our simulations, we assume $T_2 = T_1$.

	WV [24]	CA [25]	SV [11]
Writing–reading efficiency, $\eta_w\eta_{r0}$	0.05	0.76	0.423
Decay time, T_1	120 μs	220 ms	200 μs
Interaction time, τ_{int}	1.43 ns	240 ns	142 ns
Repetition rate, R_s	518 MHz	4.2 MHz	7.04 MHz

Table 2. System parameter values used for the simulations in this work. For no-memory MDI-QKD, we assume that the channel misalignment, in their respective leg of the channel, flips the state sent by each user with probability e_{mis}. For MA-QKD, we assume that channel misalignment rotates the states sent by the users by an angle θ that follows a uniform distribution of width $2\sqrt{3e_{mis}}$; see equation (A23), and the explanation preceding it.

Attenuation length of the channel, L_{att}	22 km
Detector efficiency, η_d	93%
Detector dark count rate, γ_{dc}	1 count/s
Misalignment error probability, e_{mis}	0.5%
Conversion efficiency, η_c	0.5, 1

4. Numerical results

In this section, we use the results of section 3 to simulate the secret key rate that can be achieved with the decoy-state MA-QKD scheme in figure 1, in both the asymptotic and finite-key regimes. We use two types of memories for our analysis: warm vapour atomic ensembles, which often offer high bandwidth, hence high repetition rates, but a rather low coherence time; and cold atomic ensembles, which are often slower but benefit from longer coherence times. Table 1 summarises the relevant memory parameters used in our simulation based on the experimentally reported values in [24], for warm vapours, and [25], for cold atomic ensembles. In our simulations, we have assumed $T_1 = T_2$.

We compare the MA-QKD system with a no-memory MDI-QKD setup, run at a repetition rate of 1 GHz, as a reference point, and study how finite-key effects change the crossover distance under different circumstances. Appendix A.3 provides the analytical expressions used for simulating the MDI-QKD system. MDI-QKD is the closest no-QM system to MA-QKD, which enables us to make this comparison as fair as possible. They both offer measurement-device-independent features and they can both be run with minimal requirements on the source or channel phase stabilisation. The latter property is needed for advanced TF-QKD systems, whose rate-versus-distance scaling is similar to MA-QKD, but are expected to offer higher rates if properly implemented [26–28].

In all cases, we use the system parameters listed in table 2, which are attainable by today's technologies [29]. In all graphs, we optimise over the values of the intensities $\{z, w_1, w_2\}$, and assume a vacuum intensity of $v = 0.5 \times 10^{-3}$, since the optimal value $v = 0$ may be difficult to achieve in practice. We also optimise over their selection probabilities $\{p_z, p_{w_1}, p_{w_2}, p_v\}$. In our finite-key analysis, we assume a failure probability of $\varepsilon = 0.5 \times 10^{-11}$ for each of the concentration bounds used in section 2; the total failure probability of the estimation process is $20\varepsilon = 10^{-10}$.

In figure 2, we show the performance of the warm vapour memory in reference [24], for different values of the block size N, which represents the total number of signals sent by Alice (or Bob) in that run of the protocol. We can see that, at low distances, the key rate of MA-QKD is lower than that of MDI-QKD. This is partly due to the lower repetition rate for MA-QKD, but also due to the additional loss effects introduced by the QM's less-than-one writing and reading efficiencies. At longer distances, however, the improved key-rate scaling of MA-QKD with channel loss may overcome these effects. In figure 2(a), we can see that in the asymptotic regime (black curves), the MA-QKD protocol can only offer a small advantage over MDI-QKD from around 340 km to 430 km. However, once we use a finite block size N (colour curves), the crossover distance moves to the left to shorter channel lengths, and even approaches 100 km at $N = 10^{10}$. This suggests that in order to see the advantages of MA-QKD over no-QM MDI-QKD we only need to demonstrate such systems over much shorter distances than one may require in the asymptotic regime. With record distances for entanglement distribution between two QMs being around 50 km [30], one can hope that such a demonstration can take place in the near future.

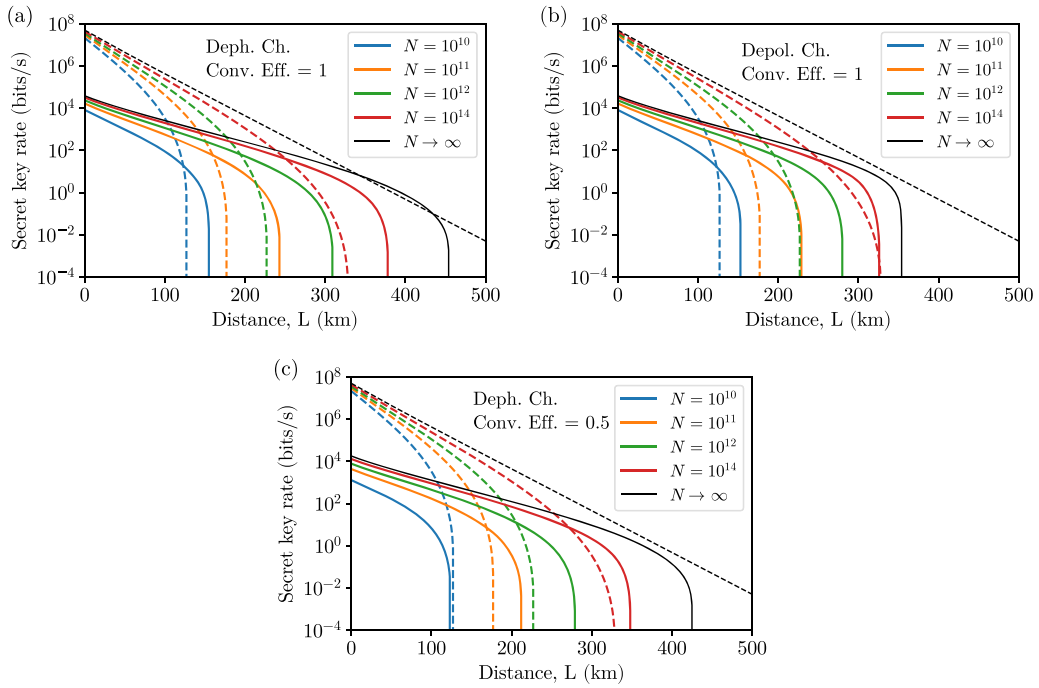

Figure 2. Secret key generation rate, in b/s, for an MA-QKD setup using warm vapour quantum memories [24] (solid lines), in comparison with no-memory MDI-QKD (dashed lines), for different values of the block size N. In (a) and (c) a dephasing channel is used to model memory decoherence, whereas, in (b), a depolarisation channel is used. The efficiency of the frequency converter is assumed ideal in (a) and (b), whereas, in (c), it is 50%.

While a slight shift to the left, due to finite-key effects, might be expected in figure 2, the considerable change in the crossover distance may come as a surprise. A naive thinking may suggest that in order to see the benefits in the finite-key setting, we need to have larger count numbers in MA-QKD, as compared to MDI-QKD, to reduce statistical errors in our parameter estimation. But, so long as, in the asymptotic case, the key rate for MDI-QKD is higher than that of MA-QKD, we may expect that the corresponding counts will also remain larger in the finite-key setting, hence no considerable change may be expected in the crossover distance. This argument, however, fails to give us an accurate picture of what is happening in the MA-QKD case. Below, we explain two key reasons for why the finite-key setting may benefit the MA-QKD setup, hence shifting the crossover distance to much shorter channel lengths.

- **Self-purification of multi-photon terms:** the MA-QKD system can by design get rid of some of the erroneous terms that would otherwise be present in the no-QM setup. Let us compare the two setups when Alice selects a non-vacuum intensity s, in the X basis, and Bob selects the vacuum intensity v. In no-QM MDI-QKD, there is a single BSM module, in which Alice's and Bob's emissions are directly combined. A successful BSM, in polarisation encoding, is declared if two detectors corresponding to different polarisations click. In the event that Bob sends a vacuum state, a successful BSM could happen because of the multi-photon terms in Alice's signal. This increases M^{sv} and E^{sv} counts, which add to the uncertainty in estimating e_{ph}. In MA-QKD, such counts are much lower. Charlie will declare that Bob's QM has been loaded when his corresponding side BSM is successful. For a vacuum input, such an event could only happen if one of the detectors clicks because of the dark count, assuming that the EPP source can only cause a click in one of the detectors. For low dark count rates, as we assume here, the measurement counts M^{sv}, as well as its corresponding terms in error will be close to zero in MA-QKD. Around the crossover distance, this makes the upper bound on e_{ph} lower for MA-QKD even if its corresponding value in the asymptotic case is higher than that of MDI-QKD. That is, MA-QKD enjoys less noisy statistics that helps us obtain tighter bounds on our parameters of interest.
- **Efficient use of decoy states:** in both MDI-QKD and MA-QKD, the secret key is extracted from events in which both users select the signal intensity z. The rounds in which they both employ the decoy intensities are used for parameter estimation only. The points that one user uses the Z basis and the other uses the X basis, are then somehow 'wasted' and will be sifted out. MA-QKD can help with better sifting efficiency. This is partly because of the main advantage of MA-QKD with respect to MDI-QKD in that the key rate scales with the transmissivity of one leg of the channel, rather than the

entire channel. To better understand this point, let us consider the effect of employing the vacuum intensity, v. Suppose that Alice and Bob are using either an MDI-QKD or an MA-QKD setup with a channel transmittance per leg of η, and that they use intensity z with probability $p_z \simeq 1$, as they do in the infinite key regime. Charlie will report a successful detection with probability Q_z. Now suppose that they use the same scheme as above, except that they now employ a (fictitious) finite-key scheme, in which they employ the vacuum intensity v with probability $p_v = p_z = 1/2$. The effect of this is equivalent to using a channel with transmittance per leg of $\eta/2$, since the effective transmittance of each user's link has been reduced by one half. Since MDI-QKD scales with η^2, Q_z will be reduced by a factor of 4. However, since MA-QKD scales with η, Q_z will only be reduced by a factor of 2. In reality, Alice and Bob will use additional decoy intensities other than the vacuum intensity. But since the decoy states will typically have larger vacuum components than the signal intensity z, they will have a similar effect as adding loss to the system, which MA-QKD tolerates better.

Another important factor in our finite-key comparison is the amount of time needed to collect data for a block size N. In the case of MDI-QKD, we can typically run the system at a high repetition rate on the order of GHz for very long periods of time. The stability of the memory-based system may, however, require us to stop collecting data after a certain period of time. It would be interesting to see how the two systems compare if, instead of the block size, one fixes the total data collection time T_{col}, instead. This corresponds to a block size of $N = R_s T_{\text{col}}$, for each system, and gives a considerable advantage to the faster system in collecting more data at an identical time. This would not make much a difference in the case of warm vapours as we can already run the system at sub-GHz rates. But, in the case of cold atomic ensembles or silicon vacancy centres, which represent slower memories, this would be interesting to study.

Figures 3(a)–(c) show the performance of MA-QKD using the cold atom QM reported in reference [25], with a repetition rate of 4.2 MHz, at different collection times. This means that, at an identical collection time, the MDI-QKD system can collect almost 250 times more data than the MA-QKD setup. It is interesting to see that, even under these harsher conditions, the MA-QKD system can offer a similar advantage as we saw in figure 2 over the no-QM MDI-QKD setup. As shown in figure 3(a), for a dephasing channel, in the asymptotic regime (black curves), the MA-QKD system can only offer a small advantage in the range from 300 km to 430 km. However, if the experiment is run for an hour (orange curves), MA-QKD can generate more key after 230 km, and, while MDI-QKD dies off at about 250 km, MA-QKD can generate a key up to 350 km. If the experiment is run for just a minute (blue curves), MA-QKD can offer an advantage after a distance of just 170 km. In figure 3(d), we show a similar graph for the silicon vacancy centres used in the recent MA-QKD experiment reported in [11]. This system has a slightly higher repetition rate, but a lower coherence time. The latter is the main reason why the cut-off distance is shorter in figure 3(d) compared with figure 3(a).

Note that it may not be possible to use a memory-based system continuously for a long period of time without applying certain calibrations or cooling techniques. This could reduce the time available for data collection, reducing the effective block size for an MA-QKD system. One key technique that may mitigate this problem in the setup considered in this work is the delayed writing procedure, in which we only attempt to interact with the memory if the corresponding side-BSM is successful. This means that the memory is kept in a ready-to-go initial state until we know a photon has survived the path loss, in which case its state is teleported to the memory. Given that at long distances the chance of the latter event is low, this suggests that the external interaction with the memory is not that frequent, and the time between any two such events can be used to bring the memory back to a solid initial state. In the case of memories reported in [24, 25], we also have the additional advantage that after reading the memory, it automatically goes back to its initial state. Nevertheless, it is easy in our analysis to consider the effect of possible interruptions in data collection by modifying the block size. For instance, for CA ensembles, we have verified that the advantage shown in figure 3(a) will remain even if we can only collect data a quarter of the experiment time.

Finally, we have looked at how different system parameters can affect the conclusion we draw above. In figures 2(b) and 3(b), we have used a depolarising channel to model the decoherence effect. In comparison to figures 2(a) and 3(a), where a dephasing model is used, we see that the warm vapour system, which has lower T_2 values, is more adversely affected than the cold atom system. We observe the same behaviour when we change the frequency converter efficiency from one to 0.5 as can be seen in figures 2(c) and 3(c). This can simply be a ramification of having noisier data in the case of warm vapours as compared to the cold atom case. This would result in less tight bounds on system parameters at the same block size or collection time, hence sharper drop in key rates. The overall effect would nevertheless suggest that MA-QKD systems can offer competitive performances in the finite-key regime irrespective of the memory or other relevant

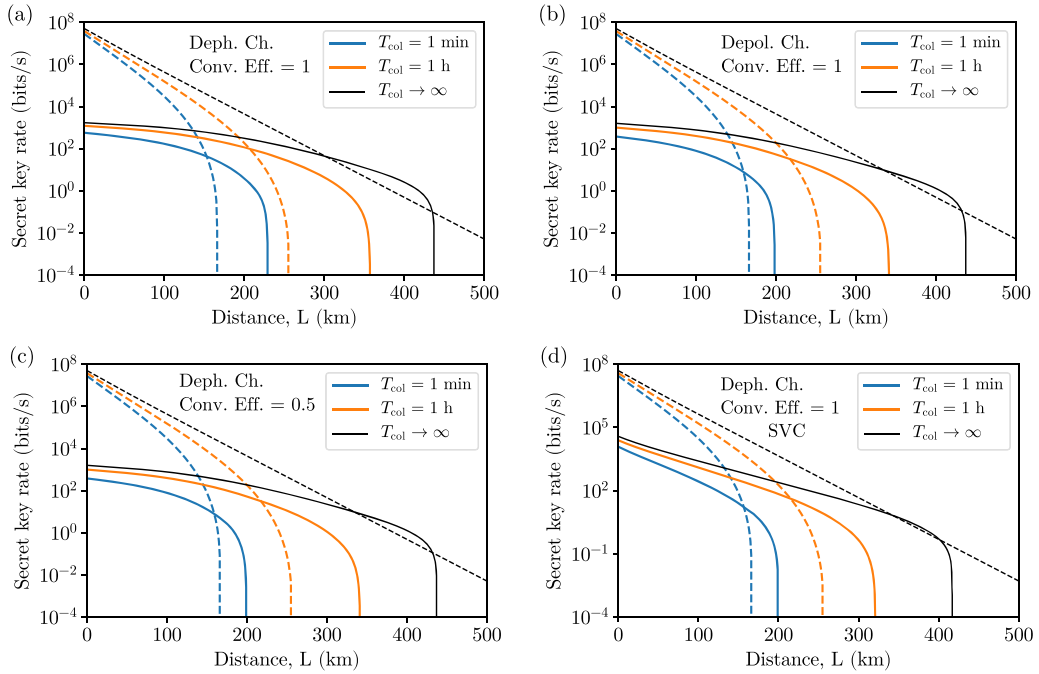

Figure 3. Secret key generation rate, in b/s, for an MA-QKD setup (solid lines) using (a)–(c) cold atom quantum memories, reported in [25], and (d) silicon vacancy centres, reported in [11], in comparison with no-memory MDI-QKD (dashed lines), if we collect data for 1 min (blue), 1 h (orange), or with no time limit (black). In (a), (c), and (d) a dephasing channel is used to model memory decoherence, whereas, in (b), a depolarisation channel is used. The efficiency of the frequency converter is assumed ideal in (a), (b), and (d), whereas, in (c), it is 50%.

system parameters. This would be an essential observation in the early demonstrations of memory-based systems and how we benchmark them against their rival counterparts.

5. Conclusions

By borrowing ideas from quantum repeaters, MA-QKD can improve the scaling of repeaterless QKD systems. However, the common imperfections in memory-based systems such as their coupling efficiency to photonic systems, or their finite coherence times, may make it difficult for them to offer any practical advantage as compared to their no-memory counterparts. In particular, previous analyses suggest that any advantage in the total key rate would often come only after a crossover distance that is still challenging to implement experimentally. In this work, we showed that once we considered the finite-key effects in the key rate analysis, the crossover distance in such systems was reduced to a point that an experimental implementation could be foreseen in the near future. This effect was attributed to two features of decoy-state MA-QKD systems. First is their ability to purify some of the errors that result from multi-photon terms in weak laser pulses, and the other relates to a more efficient sifting of signal and decoy states. It is essential, however, for MA-QKD systems to keep all sources of noise near the memory units low, as they otherwise would translate into erroneous measurements in the middle site. As such are the multiple excitation terms in the memories, or sources that drive them, or additional background noise that may enter the setup. All these issues are manageable with careful design and they are all precursors to implementing longer quantum communications links relying on QM units. In particular, we believe that the results of this work would be applicable to possible architectures for future quantum networks, in which end users are only equipped with simple equipment, such as decoy-state BB84 encoders, but the core of the network has advanced memory-based repeater chains [31].

We should note that there are no-memory QKD systems, such as TF-QKD [10], that offer a similar rate-vs-distance scaling as MA-QKD, and they have already been implemented at record distances [28]. An MA-QKD system may not be currently able to offer higher key rates or reach longer distances than those achieved by TF-QKD systems. But, it is important to recognise that the expertise and skills in both MA-QKD and TF-QKD would be required to implement scalable quantum repeater systems that go beyond the current rate-versus-distance records. In this respect, this work makes us one step closer to the final goal of implementing long-distance quantum communications systems.

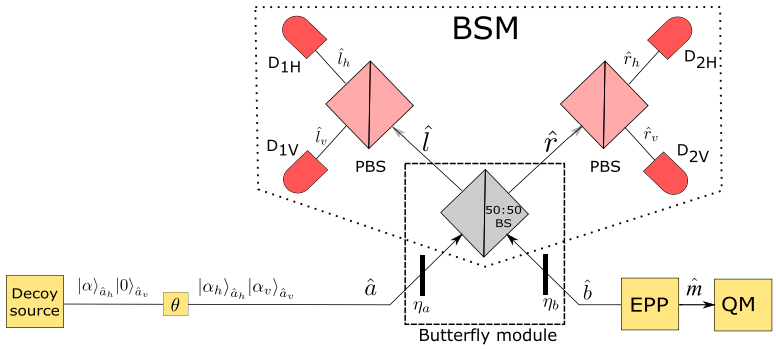

Figure 4. Loading of a QM with a Z-encoded weak coherent pulse, in a round with a misalignment angle of θ. The module in the dotted box represents a partial BSM on polarisation-encoded photons. We refer to the module in the dashed box as the butterfly module, in which η_a models the channel transmissivity and the quantum efficiency of a single-photon detector, whereas η_b captures the coupling and frequency conversion efficiencies as well as the quantum efficiency of a single-photon detector. The quantum efficiency of photodetectors in the BSM module is then assumed to be one.

Acknowledgments

We thank William Munro and Koji Azuma for valuable discussions. This work was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant No. 675662 (QCALL). All data generated can be reproduced by the equations and the methodology introduced in this paper.

Appendix A. Simulation model

In this appendix, we describe our simulation model, starting with our analysis of the indirect-loading of QMs with attenuated laser sources. Here, we assume that Charlie is honest, there is no eavesdropper, and we are only interested in finding the relevant parameters in a realistic setting.

Figure 4 shows a schematic view of our memory loading model for a single user, say Alice, in the polarisation encoding case. We model the loss in the channel, the measurement devices, and possible frequency converters as two beam splitters of transmissivity $\eta_a = \eta_{\rm ch}\eta_{\rm d}$ and $\eta_b = \eta_{\rm c}\eta_{\rm d}$ located at each input port of the 50:50 beam splitter of the BSM module. Here, $\eta_{\rm ch}$ models the transmissivity of the Alice–Charlie channel, $\eta_{\rm c}$ models the frequency conversion and/or coupling efficiency, and $\eta_{\rm d}$ represents the efficiency of the single-photon detectors. Note that by assuming the same efficiency $\eta_{\rm d}$ for all detectors, we are able to analyse its effects at the input ports of the BSM, simplifying our model. We do not need to consider the effect of the QM's writing efficiency, η_w, at the loading stage. Instead, we modify the reading efficiency $\eta_{\rm r}$ by an η_w factor, allowing us to analyse its effect at the reading stage. In figure 4, the EPP source is assumed to generate an ideal entangled state in the form $\frac{1}{\sqrt{2}}(|HH\rangle_{\hat{b}\hat{m}} + |VV\rangle_{\hat{b}\hat{m}})$, where $\hat{b}$ and $\hat{m}$, respectively, represent the two output modes of the EPP source heading towards the BSM module and the QM.

We also consider setup misalignment between the user sources and the central node, which, in polarisation encoding, we model as a random rotation of the horizontal and vertical modes. For simplicity, we assume that the rotation angle θ is independent and identically distributed between different rounds of the protocol, and for the two legs of the system. Also, we assume that polarisation maintenance schemes are in place, so that the reference frames at the user sources and the central node are the same on average. It is reasonable then to assume, as we do in this work, that the probability density function $f(\theta)$ is an even function of θ. One can use a similar formulation when other types of encoding, e.g. time-bin, are used.

In the following, in appendix A.1, we first find the post-measurement state of the loaded memory, the loading probability, and the its corresponding error rate under above considerations. The particular issue of misalignment turns out to complicate the analysis when we use weak laser pulses (WCPs) as compared to single-photon sources. Previous analyses of MA-QKD either assume no channel misalignment [8, 12] or model it as an error probability $e_{\rm mis}$ [7, 20], which is effectively given by $\int_{-\pi}^{\pi} f(\theta)\sin^2(\theta)\,{\rm d}\theta$. In our case, while the analysis is more cumbersome, the end result, in terms of the form of the post-measurement state of the QM, is similar to the single-photon case. This allows us to replicate most of the analysis in [7] in appendix A.2, and extend it to the case of depolarisation channels. In the last section of this appendix, we have summarised the key rate relationships used for the no-QM MDI-QKD as a reference point.

A.1. Memory loading

Here, we calculate the post-measurement state of the QM, its loading probability and error rate, in the two cases of Z and X bases.

A.1.1. Analysis for Z basis

Without loss of generality, let us consider the case that the user generates a horizontally polarised WCP of intensity μ. Ideally, the state generated is of the form $|\alpha\rangle_{\hat{a}_h}|0\rangle_{\hat{a}_v}$, where $\alpha=\sqrt{\mu}$ and $\hat{a}_h$ and $\hat{a}_v$ represent, respectively, the horizontal and vertical modes of the transmitted light in figure 4. In a particular round with a misalignment angle of θ, the misaligned state, at the input of the butterfly module, is given by

$$|\psi\rangle_{\hat{a}}^{\theta}=|\alpha_h\rangle_{\hat{a}_h}|\alpha_v\rangle_{\hat{a}_v}, \tag{A1}$$

where $\alpha_h=\alpha\cos\theta$ and $\alpha_v=\alpha\sin\theta$. Meanwhile, the joint state of the two output modes of the EPP source, i.e., $\hat{b}$ and $\hat{m}$, is given by

$$|\Phi^+\rangle_{\hat{b}\hat{m}}=\frac{1}{\sqrt{2}}(|HH\rangle_{\hat{b}\hat{m}}+|VV\rangle_{\hat{b}\hat{m}})=\frac{1}{\sqrt{2}}(|10H\rangle_{\hat{b}_h\hat{b}_v\hat{m}}+|01V\rangle_{\hat{b}_h\hat{b}_v\hat{m}}), \tag{A2}$$

where in the last equality, we have divided $\hat{b}$ into, respectively, horizontal and vertical modes $\hat{b}_h$ and $\hat{b}_v$. After reordering modes, and averaging over θ, the joint input state to the butterfly module is given by

$$\hat{\rho}_{\text{in}}=\int_{-\pi}^{\pi}f(\theta)\hat{\rho}_{\text{in}}^{\theta}\,\mathrm{d}\theta, \tag{A3}$$

where

$$\begin{aligned}\hat{\rho}_{\text{in}}^{\theta}=|\psi\rangle_{\hat{a}}^{\theta}\langle\psi|\otimes|\Phi^+\rangle_{\hat{b}\hat{m}}\langle\Phi^+|&=\frac{1}{2}|\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h}|1\rangle\langle 1|_{\hat{b}_h}|\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v}|0\rangle\langle 0|_{\hat{b}_v}|H\rangle\langle H|_{\hat{m}}\\&+\frac{1}{2}|\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h}|0\rangle\langle 0|_{\hat{b}_h}|\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v}|1\rangle\langle 1|_{\hat{b}_v}|V\rangle\langle V|_{\hat{m}}\\&+\frac{1}{2}|\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h}|1\rangle\langle 0|_{\hat{b}_h}|\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v}|0\rangle\langle 1|_{\hat{b}_v}|H\rangle\langle V|_{\hat{m}}\\&+\frac{1}{2}|\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h}|0\rangle\langle 1|_{\hat{b}_h}|\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v}|1\rangle\langle 0|_{\hat{b}_v}|V\rangle\langle H|_{\hat{m}},\end{aligned} \tag{A4}$$

and $|\psi\rangle\langle\psi|_{\hat{a}}$ is our shorthand notation for $|\psi\rangle_{\hat{a}\hat{a}}\langle\psi|$.

We are interested in the state projected to the QM after a successful loading, i.e., when exactly an H detector and a V detector click in the BSM module. To model this measurement process, we should find the output state of the butterfly module, with an input state as in equation (A3), and then find the post-measurement state for the desired measurement outcome. The key to calculate this is to realise that the horizontal and vertical modes will interact separately at the 50:50 beam splitter of the butterfly module, and will cause clicks in the horizontal and vertically polarised detectors, respectively. Thus, we can split the overall transformation $\hat{B}$ for the butterfly module in figure 4, and the overall POVM operator $\hat{M}$ in horizontal and vertical operators as follows:

$$\hat{B}=\hat{B}_h\otimes\hat{B}_v \tag{A5}$$

$$\hat{M}=\hat{M}_h\otimes\hat{M}_v. \tag{A6}$$

Here, the butterfly operators $\hat{B}_h$ and $\hat{B}_v$ in figure 4 only differ in their input and output modes: $\hat{B}_h$ will take modes $\hat{a}_h$ and $\hat{b}_h$ to modes $\hat{l}_h$ and $\hat{r}_h$, while $\hat{B}_v$ will take modes $\hat{a}_v$ and $\hat{b}_v$ to modes $\hat{l}_v$ and $\hat{r}_v$. The measurement operators (POVMs) are also identical for both the horizontal and vertical modes, and are given by

$$\hat{M}_x=(1-p_{\text{dc}})\left[\left(\hat{I}_{\hat{l}_x}-(1-p_{\text{dc}})|0\rangle\langle 0|_{\hat{l}_x}\right)\otimes|0\rangle\langle 0|_{\hat{r}_x}\right]+(1-p_{\text{dc}})\left[|0\rangle\langle 0|_{\hat{l}_x}\otimes\left(\hat{I}_{\hat{r}_x}-(1-p_{\text{dc}})|0\rangle\langle 0|_{\hat{r}_x}\right)\right], \tag{A7}$$

for $x\in\{h,v\}$, where $\hat{I}$ is the identity operator for the corresponding mode. $\hat{M}_x$ represents the event of getting a click in the x-polarised left detector and no click on the x-polarised right detector, or vice versa.

Using the above notation, the post-measurement state of the QM, after a successful loading, is given by

$$\hat{\rho}_{\hat{m}} = \frac{\mathrm{Tr}_{\hat{l}_h,\hat{l}_v,\hat{r}_h\hat{r}_v}\left[\hat{B}^\dagger\hat{\rho}_{\mathrm{in}}\hat{B}\hat{M}\right]}{\mathrm{Tr}\left[\hat{B}^\dagger\hat{\rho}_{\mathrm{in}}\hat{B}\hat{M}\right]} = \frac{1}{p^{\mu}_{\mathrm{load}}}\int_{-\pi}^{\pi} f(\theta)\mathrm{Tr}_{\hat{l}_h,\hat{l}_v,\hat{r}_h\hat{r}_v}\left[\hat{B}^\dagger\hat{\rho}^{\theta}_{\mathrm{in}}\hat{B}\hat{M}\right]\,\mathrm{d}\theta \tag{A8}$$

where

$$\mathrm{Tr}_{\hat{l}_h,\hat{l}_v,\hat{r}_h\hat{r}_v}\left[\hat{B}^\dagger\hat{\rho}^{\theta}_{\mathrm{in}}\hat{B}\hat{M}\right] = c_{HH}(\theta)|H\rangle\langle H| + c_{VV}(\theta)|V\rangle\langle V| + c_{HV}(\theta)|H\rangle\langle V| + c_{VH}(\theta)|V\rangle\langle H|, \tag{A9}$$

with

$$\begin{aligned}
c_{HH}(\theta) &= \frac{1}{2}\,\mathrm{Tr}\left[\hat{B}^\dagger_h|\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h}|1\rangle\langle 1|_{\hat{b}_h}\hat{B}_h\hat{M}_h\right]\,\mathrm{Tr}\left[\hat{B}^\dagger_v|\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v}|0\rangle\langle 0|_{\hat{b}_v}\hat{B}_v\hat{M}_v\right]\\
c_{VV}(\theta) &= \frac{1}{2}\,\mathrm{Tr}\left[\hat{B}^\dagger_h|\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h}|0\rangle\langle 0|_{\hat{b}_h}\hat{B}_h\hat{M}_h\right]\,\mathrm{Tr}\left[\hat{B}^\dagger_v|\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v}|1\rangle\langle 1|_{\hat{b}_v}\hat{B}_v\hat{M}_v\right]\\
c_{HV}(\theta) &= \frac{1}{2}\,\mathrm{Tr}\left[\hat{B}^\dagger_h|\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h}|1\rangle\langle 0|_{\hat{b}_h}\hat{B}_h\hat{M}_h\right]\,\mathrm{Tr}\left[\hat{B}^\dagger_v|\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v}|0\rangle\langle 1|_{\hat{b}_v}\hat{B}_v\hat{M}_v\right]\\
c_{VH}(\theta) &= \frac{1}{2}\,\mathrm{Tr}\left[\hat{B}^\dagger_h|\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h}|0\rangle\langle 1|_{\hat{b}_h}\hat{B}_h\hat{M}_h\right]\,\mathrm{Tr}\left[\hat{B}^\dagger_v|\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v}|1\rangle\langle 0|_{\hat{b}_v}\hat{B}_v\hat{M}_v\right],
\end{aligned} \tag{A10}$$

and

$$p^{\mu}_{\mathrm{load}} = \mathrm{Tr}\left[\hat{B}^\dagger\hat{\rho}_{\mathrm{in}}\hat{B}\hat{M}\right] = \int_{-\pi}^{\pi} f(\theta)[c_{HH}(\theta) + c_{VV}(\theta)]\,\mathrm{d}\theta \tag{A11}$$

is the probability of a successful loading for a WCP with intensity μ.

Every individual trace term in equation (A10) involves either horizontal or vertical modes, and is equivalent to the probability of having exactly one detector click in the corresponding polarisation. Such terms have already been calculated in table 3 of [31], which here we reuse, after making necessary adjustments, to obtain

$$\begin{aligned}
c_{HH}(\theta) &= \left(1-p_{\mathrm{dc}}\right)^2\left(1-\mathrm{e}^{-1/2\,\eta_a\,(\sin^2\theta)\mu}\left(1-p_{\mathrm{dc}}\right)\right)\\
&\quad\times\left(\left(\eta_b\,\left(\cos^2\,\theta\right)\mu\,\eta_a - 2\,\eta_b + 4\right)\mathrm{e}^{1/2\,\eta_a\,(\cos^2\theta)\mu} - 4\,(1-\eta_b)\left(1-p_{\mathrm{dc}}\right)\right)\mathrm{e}^{-1/2\,\eta_a\,\mu\,((\cos^2\theta)+1)},\\
c_{VV}(\theta) &= \left(1-p_{\mathrm{dc}}\right)^2\Big[\left(1-p_{\mathrm{dc}}\right)\left(\eta_b\,\cos^2\,\theta\mu\,\eta_a - \eta_b\,\eta_a\,\mu + 2\,\eta_b - 4\right)\mathrm{e}^{-1/2\,\eta_a\,\mu\,(\cos^2\theta+1)}\\
&\quad - 4\,(1-\eta_b)\left(1-p_{\mathrm{dc}}\right)\mathrm{e}^{1/2\,\eta_a\,\mu\,(\cos^2\theta-2)} - \left(\eta_b\,\cos^2\,\theta\mu\,\eta_a - \eta_b\,\eta_a\,\mu + 2\,\eta_b - 4\right)\mathrm{e}^{-1/2\,\eta_a\,\mu}\\
&\quad + 4\,\mathrm{e}^{-\eta_a\,\mu}\left(-1+p_{\mathrm{dc}}\right)^2(1-\eta_b)\Big],
\end{aligned} \tag{A12}$$

and

$$c_{HV}(\theta) = c_{VH}(\theta) = \frac{1}{4}\cos\,\theta\,\sin\,\theta(1-p_{\mathrm{dc}})^2(\eta_a\eta_b\mu\,\mathrm{e}^{-\eta_a\mu}). \tag{A13}$$

It is interesting that, in the above, the diagonal terms c_{HV} and c_{VH} are odd functions of θ. Under our assumption that $f(\theta)$ is an even function, we have that

$$\int_{-\pi}^{\pi} f(\theta)c_{HV}(\theta)\,\mathrm{d}\theta = \int_{-\pi}^{\pi} f(\theta)c_{VH}(\theta)\,\mathrm{d}\theta = 0, \tag{A14}$$

implying that these terms vanish when considering the average post-measurement state $\hat{\rho}_{\hat{m}}$ in equation (A8). Thus, $\hat{\rho}_{\hat{m}}$ can be expressed as

$$\rho_{\hat{m}} = e^{\mu}_{\mathrm{load}}|H\rangle\langle H| + (1-e^{\mu}_{\mathrm{load}})|V\rangle\langle V|, \tag{A15}$$

where

$$e^{\mu}_{\mathrm{load}} = \frac{1}{p^{\mu}_{\mathrm{load}}}\int_{-\pi}^{\pi} f(\theta)c_{HH}(\theta)\,\mathrm{d}\theta \tag{A16}$$

is the probability of loading the memory with the wrong state. In our case, when we send H-polarised light, a successful BSM in figure 4 suggests that the $\hat{b}$ mode is V-polarised. The state stored in the memory, for an EPP source with $|\Phi^+\rangle_{\hat{b}\hat{m}}$ as its initial state, is then also expected to be V-polarised. That is why the coefficient for $|H\rangle\langle H|$, in equation (A15), represents the loading error probability, in Z basis, for a WCP with intensity μ.

Due to the symmetry of the setup, if the user sends vertically polarised light, the loading probability p^{μ}_{load} would be the same, but the post-measurement state is given by $\rho_{\hat{m}} = (1-e^{\mu}_{\mathrm{load}})|H\rangle\langle H| + e^{\mu}_{\mathrm{load}}|V\rangle\langle V|$.

A.1.2. Analysis for X basis

Without loss of generality, let us assume that Alice generates the plus state given by

$$\left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\hat{a}_h}\left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\hat{a}_v}. \tag{A17}$$

In a particular round with a misalignment angle θ, the butterfly module will receive the state

$$|\psi\rangle_{\hat{a}}^{\theta}=\left|\frac{\alpha}{\sqrt{2}}(\sin\ \theta+\cos\ \theta)\right\rangle_{\hat{a}_h}\left|\frac{\alpha}{\sqrt{2}}(\sin\ \theta-\cos\ \theta)\right\rangle_{\hat{a}_v}, \tag{A18}$$

while the output state of the EPP source can be written as

$$|\Phi^{+}\rangle_{\hat{b}\hat{m}}=\frac{1}{\sqrt{2}}(|DD\rangle_{\hat{b}\hat{m}}+|AA\rangle_{\hat{b}\hat{m}})=\frac{1}{\sqrt{2}}\left((|10\rangle+|01\rangle)|D\rangle+(|10\rangle-|01\rangle)|A\rangle\right)_{\hat{b}_h\hat{b}_v\hat{m}}, \tag{A19}$$

where $|D\rangle=(|H\rangle+|V\rangle)/\sqrt{2}$ and $|A\rangle=(|H\rangle-|V\rangle)/\sqrt{2}$.

The analysis is similar to the one for the Z basis. After going through similar steps, we find that the probability to successfully load the memory is given by

$$\begin{aligned}p_{\text{load}}^{\mu}=\int_{-\pi}^{\pi}f(\theta)\frac{1}{2}\left(1-p_{\text{dc}}\right)^2\Big(&\left(1-p_{\text{dc}}\right)\left(\cos\ \theta\ \sin(\theta)\,\mu\eta_a\,\eta_b-1/2\,\eta_b\,\mu\eta_a+6\,\eta_b-8\right)\mathrm{e}^{-1/2\,\eta_a\,\mu\left(\cos\ \theta\ \sin(\theta)+3/2\right)}\\&-\left(1-p_{\text{dc}}\right)\left(\cos\ \theta\ \sin(\theta)\,\mu\eta_a\,\eta_b+1/2\,\eta_b\,\mu\eta_a-6\,\eta_b+8\right)\mathrm{e}^{1/4\,\eta_a\,\mu(2\ \cos(\theta)\sin(\theta)-3)}\\&+\left(\eta_b\,\mu\eta_a-4\,\eta_b+8\right)\mathrm{e}^{-1/2\,\eta_a\,\mu}+8\ \mathrm{e}^{-\eta_a\,\mu}\left(1-p_{\text{dc}}\right)^2\left(1-\eta_b\right)\Big)\ \mathrm{d}\theta,\end{aligned} \tag{A20}$$

and, under our assumption that $f(\theta)$ is even, the post-measurement state of the memory can be written as

$$\rho_{\hat{m}}=e_{\text{load}}^{\mu}|D\rangle\langle D|+(1-e_{\text{load}}^{\mu})|A\rangle\langle A|, \tag{A21}$$

where

$$\begin{aligned}e_{\text{load}}^{\mu}=\frac{1}{p_{\text{load}}^{\mu}}\int_{-\pi}^{\pi}f(\theta)\frac{1}{4}\left(-1+p_{\text{dc}}\right)^2&\\\times\Big(&\left(1-p_{\text{dc}}\right)\left(\cos(\theta)\sin(\theta)\,\mu\eta_a\,\eta_b-1/2\,\eta_b\,\mu\eta_a+6\,\eta_b-8\right)\mathrm{e}^{-1/2\,\eta_a\,\mu\left(\cos(\theta)\sin(\theta)+3/2\right)}\\&-\left(1-p_{\text{dc}}\right)\left(\cos(\theta)\sin(\theta)\,\mu\eta_a\,\eta_b+1/2\,\eta_b\,\mu\eta_a-6\,\eta_b+8\right)\mathrm{e}^{1/4\,\eta_a\,\mu(2\ \cos(\theta)\sin(\theta)-3)}\\&+\left(2\,\eta_b\,\mu\eta_a-2\left(\cos^2\ \theta\right)\mu\eta_a\,\eta_b-4\,\eta_b+8\right)\mathrm{e}^{-1/2\,\eta_a\,\mu}+8\ \mathrm{e}^{-\eta_a\,\mu}\left(1-p_{\text{dc}}\right)^2\left(1-\eta_b\right)\Big)\ \mathrm{d}\theta.\end{aligned} \tag{A22}$$

Finally, note that we calculate the integrals in and equations (A11), (A16), (A20) and (A22) numerically as a closed form expression for them could not be found. In our simulations, to compute p_{load}^{μ} and e_{load}^{μ}, we assume that $f(\theta)$ follows a uniform distribution over $[-\Theta,\Theta]$. To have a fair comparison with no-memory MDI-QKD, we choose $\Theta=\sqrt{3e_{\text{mis}}}$, where e_{mis} is the misalignment error probability in one leg of a symmetric MDI-QKD setup. This is motivated by the fact that

$$\frac{1}{2\sqrt{3e_{\text{mis}}}}\int_{-\sqrt{3e_{\text{mis}}}}^{\sqrt{3e_{\text{mis}}}}\sin^2\ \theta\ \mathrm{d}\theta\approx\frac{1}{2\sqrt{3e_{\text{mis}}}}\int_{-\sqrt{3e_{\text{mis}}}}^{\sqrt{3e_{\text{mis}}}}\theta^2\ \mathrm{d}\theta=e_{\text{mis}}, \tag{A23}$$

which implies that the chosen $f(\theta)$ would cause a misalignment error of approximately e_{mis} in the MDI-QKD setup.

A.2. Key rate simulation

In appendix A.1, we showed that the post-measurement QM state after a successful loading is a mixture of the desired and undesired states for the QM; see equations (A15) and (A21). In effect, it is as if the state of QM has flipped with a probability e_{load}^{μ}. This is similar to how misalignment acts on a single photon state, because of which we can think of the whole loading process as a channel with an effective misalignment of e_{load}^{μ}. This would also make it possible to use the methodology in reference [7] to calculate the required parameters of the key rate formula. In particular, the photonic states retrieved from the two QMs turn out to also have a similar form to a misaligned photon, although at a higher error rate to account for the dephasing/depolarisation process.

In the following, we explain how to simulate all terms in the key-rate formula, in both the asymptotic and finite-key regimes. Given that in MA-QKD, one of the memories will be read immediately after loading,

only one of the QMs would undergo the decay process. That implies that the middle BSM in figure 1 can be thought as an asymmetric MDI-QKD setup, with possibly different transmissivities η_l and η_r for, respectively, its left and right legs [7]. We can then use the yield and error rate formulas, summarised below, of asymmetric single-photon MDI-QKD for our rate calculation:

$$Y_{11}^{\mathrm{MDI}}(\eta_l,\eta_r)=(1-p_d)^2\left[\frac{\eta_l\eta_r}{2}+(2\eta_l+2\eta_r-3\eta_l\eta_r)p_d+4(1-\eta_l)(1-\eta_r)p_d^2\right], \tag{A24}$$

$$e_{11;X}^{\mathrm{MDI}}(\eta_l,\eta_r,e_d)Y_{11}^{\mathrm{MDI}}(\eta_l,\eta_r)=e_0Y_{11}^{\mathrm{MDI}}(\eta_l,\eta_r)-(e_0-e_d)(1-p_d)^2\eta_l\eta_r/2, \tag{A25}$$

$$e_{11;Z}^{\mathrm{MDI}}(\eta_l,\eta_r,e_d)Y_{11}^{\mathrm{MDI}}(\eta_l,\eta_r)=e_0Y_{11}^{\mathrm{MDI}}(\eta_l,\eta_r)-(e_0-e_d)(1-p_d)^2(1-2p_d)\eta_l\eta_r/2, \tag{A26}$$

where $e_0=1/2$ and e_d is the total misalignment probability in the asymmetric MDI-QKD setup, i.e., the probability that exactly one of the photons is misaligned.

A.2.1. Asymptotic regime

In this case, the key-rate formula is given by equation (3). In this regime, we assume that the signal intensity z, encoded in the Z-basis, is chosen with probability approaching one, and the parameter estimation provides perfect estimates of the single-photon terms Q_{11}^Z and e_{ph}. We only then need to simulate the values of Q_Z, e_Z, Q_{11}^Z and e_{ph} under nominal mode of operation. The procedure we use to calculate these terms is very similar to that of [7]. The main differences are our new model for the memory-loading with WCPs, developed earlier in this appendix, and the inclusion of the depolarising channel for memory decoherence.

To compute Q_Z, we divide it into two parts: (1) the probability of having the two memories loaded and available to read in a given round, denoted by P_{side}, and (2) the probability that the middle BSM is successful, given that the QMs are ready, denoted by P_{mid}. Then,

$$Q_Z=P_{\mathrm{side}}P_{\mathrm{mid}}. \tag{A27}$$

To find P_{side}, we first estimate the probability to load the QM with a Z-encoded WCP, given by p_{load}^z in equation (A11). Then, we compute the average number of rounds N_{L} that it takes to load both memories, substituting η_A and η_B by p_{load}^z in equation (C.3) of [7], to obtain

$$N_{\mathrm{L}}=\frac{3-2p_{\mathrm{load}}^z}{p_{\mathrm{load}}^z(2-p_{\mathrm{load}}^z)}. \tag{A28}$$

Then, we have that

$$P_{\mathrm{side}}=\frac{1}{N_{\mathrm{L}}+N_{\mathrm{r}}}, \tag{A29}$$

where N_{r} is the number of rounds it takes to read the memory, which we assume to be one.

The second term is given by

$$P_{\mathrm{mid}}=Y_{11}^{\mathrm{MDI}}(\eta_m,\eta_{m'}), \tag{A30}$$

where $\eta_m=\eta_w\eta_{\mathrm{r0}}\eta_{\mathrm{d}}$ is the effective reading efficiency of the QM loaded later, and $\eta_{m'}$ is the average effective reading efficiency of the QM loaded earlier, given by [7]

$$\eta_{m'}=\frac{(1+\mathrm{e}^{T/T_1}-p_{\mathrm{load}}^z)p_{\mathrm{load}}^z}{(2-p_{\mathrm{load}}^z)(\mathrm{e}^{T/T_1}+p_{\mathrm{load}}^z-1)}\eta_m, \tag{A31}$$

where T_1 is the time constant for the decay process of the QM.

The single-photon component Q_{11}^Z is given by

$$Q_{11}^Z=Q_Z\frac{(p_{\mathrm{load}}^{\mathrm{SP}})^2}{(p_{\mathrm{load}}^z)^2}z^2\ \mathrm{e}^{-2z}, \tag{A32}$$

where $p_{\mathrm{load}}^{\mathrm{SP}}$ is the probability to load the QM when a single photon is sent, given by [7]

$$p_{\mathrm{load}}^{\mathrm{SP}}=Y_{11}^{\mathrm{MDI}}(\eta_{\mathrm{ch}}\eta_{\mathrm{d}},\eta_{\mathrm{c}}\eta_{\mathrm{d}}). \tag{A33}$$

To find e_{ph}, we first calculate the misalignment-error probability for loading the QM with an X-basis single photon, which is given by [7]

$$e_{\mathrm{load}}^{X,\mathrm{SP}}=e_{11;X}^{\mathrm{MDI}}(\eta_{\mathrm{ch}}\eta_{\mathrm{d}},\eta_{\mathrm{c}}\eta_{\mathrm{d}},e_{\mathrm{mis}}). \tag{A34}$$

Then, we obtain

$$e_{\mathrm{ph}}=e_{11;X}^{\mathrm{MDI}}(\eta_m,\eta_m',\mathrm{E}\left\{e_{\mathrm{QM}}^{\mathrm{SP}}\right\}), \tag{A35}$$

where $\mathrm{E}\left\{e_{\mathrm{QM}}^{\mathrm{SP}}\right\}$ is the total misalignment probability, given by

$$\mathrm{E}\left\{e_{\mathrm{QM}}^{\mathrm{SP}}\right\} = 2e_{\mathrm{load}}^{X,\mathrm{SP}} + 2\beta\mathrm{E}\left\{e_{\mathrm{deph}}\right\} - 2e_{\mathrm{load}}^{X,\mathrm{SP}}e_{\mathrm{load}}^{X,\mathrm{SP}} - 4\beta\mathrm{E}\left\{e_{\mathrm{deph}}\right\}e_{\mathrm{load}}^{X,\mathrm{SP}}, \tag{A36}$$

with

$$\mathrm{E}\left\{e_{\mathrm{deph}}\right\} = 1 - \frac{p_{\mathrm{load}}^{z}}{1-(1-p_{\mathrm{load}}^{z})^{2}} - \frac{(p_{\mathrm{load}}^{z})^{2}(1-p_{\mathrm{load}}^{z}\ \mathrm{e}^{-T/T_2})}{[1-(1-p_{\mathrm{load}}^{z})\mathrm{e}^{-T/T_2}][1-(1-p_{\mathrm{load}}^{z})^{2}]}, \tag{A37}$$

in the case of dephasing memories, and by

$$\mathrm{E}\left\{e_{\mathrm{QM}}^{\mathrm{SP}}\right\} = 2e_{\mathrm{load}}^{X,\mathrm{SP}} + 2\beta\mathrm{E}\left\{e_{\mathrm{depol}}\right\} - 2e_{\mathrm{load}}^{X,\mathrm{SP}}e_{\mathrm{load}}^{X,\mathrm{SP}} - 4\beta\mathrm{E}\left\{e_{\mathrm{depol}}\right\}e_{\mathrm{load}}^{X,\mathrm{SP}}, \tag{A38}$$

with

$$\mathrm{E}\left\{e_{\mathrm{depol}}\right\} = \frac{2}{3}\mathrm{E}\left\{e_{\mathrm{deph}}\right\}, \tag{A39}$$

in the case of depolarising memories.

To calculate e_Z, we use

$$e_Z = e_{11;Z}^{\mathrm{MDI}}(\eta_m, \eta_m', \mathrm{E}\left\{e_{\mathrm{QM}}\right\}), \tag{A40}$$

where $\mathrm{E}\left\{e_{\mathrm{QM}}\right\}$ is the average total misalignment-error probability between the two QMs, which depends on the specific model used for decoherence. In the dephasing model, the Z-basis QM states will not be affected by the decoherence, therefore, the probability that exactly one state is misaligned is as follows

$$\mathrm{E}\left\{e_{\mathrm{QM}}\right\} = e_{\mathrm{QM}} = 2e_{\mathrm{load}}^{z}(1-e_{\mathrm{load}}^{z}), \tag{A41}$$

where e_{load}^{z} is given by equation (A16). For the depolarisation model, we have

$$\mathrm{E}\left\{e_{\mathrm{QM}}\right\} = 2e_{\mathrm{load}}^{z} + 2\beta\mathrm{E}\left\{e_{\mathrm{depol}}\right\} - 2e_{\mathrm{load}}^{z}e_{\mathrm{load}}^{z} - 4\beta\mathrm{E}\left\{e_{\mathrm{depol}}\right\}e_{\mathrm{load}}^{z}, \tag{A42}$$

where $\beta = 1 - 2e_{\mathrm{load}}^{z}$.

To derive equation (A42) and equations (A36) to (A39), we have used a similar analysis as in appendix D of reference [7].

A.2.2. Finite-key regime

In this case, we need to calculate the sets $\{M^{ab}\}$ and $\{E^{ab}\}$, where M^{ab} is the total number of measurement counts when Alice (Bob) has used intensity a (b), while E^{ab} is the number of such events that also result in an error. Note that intensity z is encoded in the Z basis and intensities $\{w_1, w_2, v\}$ are encoded in the X basis; we are only interested in estimating $\{M^{ab}\}$ and $\{E^{ab}\}$ when a, b are encoded in the same basis.

For our numerical simulations, we still need to make some assumptions on the obtained measurement results in a nominal experiment. For this purpose, we use the expected values for relevant parameters using the corresponding probability in the asymptotic regime. That is, we assume

$$M^{ab} = NQ^{ab} \quad \text{and} \quad E^{ab} = e_{ab}M^{ab}, \tag{A43}$$

where N is the total number of rounds, i.e., the number of transmitted pulses by Alice/Bob, in the protocol, Q^{ab} is the probability of having a successful measurement originating from intensities a, for Alice, and b, for Bob, and e_{ab} is the probability that this measurement results in an error.

To calculate Q_{ab}, we first compute the total gain Q_{tot}, using the same procedure as for Q_Z in the asymptotic case, with the difference that Q_{tot} is now a function of the average memory-loading probability given by

$$\bar{p}_{\mathrm{load}} = \sum_a p_a p_{\mathrm{load}}^{a}, \tag{A44}$$

where p_a is the probability of selecting intensity $a \in \{z, w_1, w_2, v\}$; and p_{load}^{a} is the probability of a successful loading when the user selects intensity a, given by either equations (A16) or (A22), depending on whether intensity a is encoded in the Z or X basis. Then, we have that

$$N_{\mathrm{L}} = \frac{3-2\bar{p}_{\mathrm{load}}}{\bar{p}_{\mathrm{load}}(2-\bar{p}_{\mathrm{load}})}, \tag{A45}$$

$$\eta_{m'} = \frac{(1+\mathrm{e}^{T/T_1}-\bar{p}_{\mathrm{load}})\bar{p}_{\mathrm{load}}}{(2-\bar{p}_{\mathrm{load}})(\mathrm{e}^{T/T_1}+\bar{p}_{\mathrm{load}}-1)}\eta_m, \tag{A46}$$

$$P_{\mathrm{side}} = \frac{1}{N_{\mathrm{L}}+N_{\mathrm{r}}} \tag{A47}$$

$$P_{\text{mid}} = Y_{11}^{\text{MDI}}(\eta_m, \eta_{m'}), \tag{A48}$$

$$Q_{\text{tot}} = P_{\text{side}} P_{\text{mid}}, \tag{A49}$$

where $N_{\text{r}} = 1$ and $\eta_m = \eta_w \eta_{\text{r0}} \eta_{\text{d}}$. Now, Q^{ab} is the fraction of Q_{tot} that originated from intensities a, b. Note that after a successful loading, the state projected to the QM is always a misaligned qubit. The probability that the middle BSM is successful only depends on the loss coefficients η_m and $\eta_{m'}$, and it is independent of the intensities a, b that caused the loading. Thus, Q^{ab} only depends on how likely intensities a, b are to cause a successful loading, that is,

$$Q^{ab} = Q_{\text{tot}} p_a p_b \frac{\bar{p}^a_{\text{load}} \bar{p}^b_{\text{load}}}{\bar{p}^2_{\text{load}}}. \tag{A50}$$

For e_{ab}, we have that

$$e_{zz} = e^{\text{MDI}}_{11;Z}(\eta_m, \eta'_m, \text{E}\left\{e^{\text{QM}}_{zz}\right\}), \tag{A51}$$

$$e_{ab} = e^{\text{MDI}}_{11;X}\left(\eta_m, \eta'_m, \text{E}\left\{e^{\text{QM}}_{ab}\right\}\right), \quad a, b \in \{w_1, w_2, v\} \tag{A52}$$

where $\text{E}\left\{e^{\text{QM}}_{ab}\right\}$ is the total average misalignment error probability between the two QMs, and depends on whether one considers a dephasing or depolarisation model. The former has no effect on Z-basis states, and therefore

$$\text{E}\left\{e^{\text{QM}}_{zz}\right\} = e^{\text{QM}}_{zz} = 2e^z_{\text{load}}(1 - e^z_{\text{load}}). \tag{A53}$$

For the X-basis intensities, we have that

$$\text{E}\left\{e^{\text{QM}}_{ab}\right\} = e^a_{\text{load}} + e^b_{\text{load}} + \beta_a \text{E}\left\{e_{\text{deph}}\right\} + \beta_b \text{E}\left\{e_{\text{deph}}\right\} - 2e^a_{\text{load}} e^b_{\text{load}} - 2\beta_a \text{E}\left\{e_{\text{deph}}\right\} e^b_{\text{load}} - 2\beta_b \text{E}\left\{e_{\text{deph}}\right\} e^a_{\text{load}}, \tag{A54}$$

where $\beta_k = 1 - 2e^k_{\text{load}}$, and

$$\text{E}\left\{e_{\text{deph}}\right\} = 1 - \frac{\bar{p}_{\text{load}}}{1 - (1 - \bar{p}_{\text{load}})^2} - \frac{\bar{p}^2_{\text{load}}(1 - \bar{p}_{\text{load}} \text{e}^{-T/T_2})}{[1 - (1 - \bar{p}_{\text{load}})\text{e}^{-T/T_2}][1 - (1 - \bar{p}_{\text{load}})^2]}, \tag{A55}$$

using a similar analysis to the one that results in equation (D.8) of [7].

For a depolarisation channel, we have that, for all intensities

$$\text{E}\left\{e^{\text{QM}}_{ab}\right\} = e^a_{\text{load}} + e^b_{\text{load}} + \beta_a \text{E}\left\{e_{\text{depol}}\right\} + \beta_b \text{E}\left\{e_{\text{depol}}\right\} - 2e^a_{\text{load}} e^b_{\text{load}} - 2\beta_a \text{E}\left\{e_{\text{depol}}\right\} e^b_{\text{load}} - 2\beta_b \text{E}\left\{e_{\text{depol}}\right\} e^a_{\text{load}}, \tag{A56}$$

where

$$\text{E}\left\{e_{\text{depol}}\right\} = \frac{2}{3}\text{E}\left\{e_{\text{deph}}\right\}. \tag{A57}$$

A.3. MDI-QKD without QMs

Here, we give the formulas that we have used to simulate the no-memory MDI-QKD with WCP sources.

In general, if Alice and Bob encode in the Z basis and choose intensities a and b, respectively, the gain and error-rate formulas are given by [32]

$$Q^{ab} = Q_c + Q_e, \tag{A58}$$

$$e_{ab} = e_d Q_c + (1 - e_d) Q_e, \tag{A59}$$

where e_d represents the total misalignment error probability given by $e_d = 2e_{\text{mis}}(1 - e_{\text{mis}})$, and

$$\begin{aligned} Q_c &= 2(1 - p_d)^2 \text{e}^{-\zeta/2}(1 - (1 - p_d)\text{e}^{-\eta a/2})(1 - (1 - p_d)\text{e}^{-\eta b/2}) \\ Q_e &= 2p_d(1 - p_d)^2 \text{e}^{-\zeta/2}[I_0(2x) - (1 - p_d)\text{e}^{-\zeta/2}] \\ x &= \eta\sqrt{ab}/2 \\ \zeta &= \eta(a + b), \end{aligned} \tag{A60}$$

where I_0 is the modified Bessel function of the first kind and $\eta = \eta_{\text{ch}}\eta_{\text{d}}$ is the total attenuation between each user and the middle node. If they encode in the X basis, they are given by [32]

$$Q^{ab} = 2y^2[1 + 2y^2 - 4yI_0(x) + I_0(2x)], \tag{A61}$$

$$e_{ab} = \frac{Q^{ab}}{2} - (1-2e_d)y^2[I_0(2x)-1], \tag{A62}$$

where

$$y = (1-p_d)e^{-\zeta/4}. \tag{A63}$$

A.3.1. Asymptotic regime

In the asymptotic regime, the key rate formula is given by

$$R \leqslant R_s\left[Q_{11}^Z\left(1-h(e_{\rm ph})\right) - fQ_Z h(e_Z)\right]. \tag{A64}$$

Q_Z and e_Z are given by equations (A58) and (A59), respectively, by substituting $a=b=z$. In the asymptotic regime, we assume that the users are able to obtain perfect estimates of Q_{11}^Z and $e_{\rm ph}$, which are given by

$$Q_{11}^Z = z^2\ e^{-2z}Y_{11}, \tag{A65}$$

$$e_{\rm ph} = e_{11;X}^{\rm MDI}(\eta,\eta,e_d) = \frac{1}{2} - \frac{1}{Y_{11}}(1/2-e_d)(1-p_d)^2(1-2p_d)\frac{\eta^2}{2}, \tag{A66}$$

where

$$Y_{11} = Y_{11}^{\rm MDI}(\eta,\eta) = (1-p_d)^2\left[\frac{\eta^2}{2} + (4\eta-3\eta^2)p_d + 4(1-\eta)^2p_d^2\right]. \tag{A67}$$

A.3.2. Finite-key regime

We need to simulate the sets $\{M^{ab}\}$ and $\{E^{ab}\}$. In our simulations, we assume that all measurement counts equal their expected values, that is,

$$M^{ab} = Np_{ab}Q^{ab} \quad \text{and} \quad E^{ab} = e_{ab}M^{ab}, \tag{A68}$$

where Q_{ab} and e_{ab} are given by equations (A58) and (A59) for Z-encoded intensities, and by equations (A61) and (A62) for X-encoded intensities, and p_{ab} is the probability that Alice and Bob choose intensities a and b, respectively.

Appendix B. Finite-key analysis

In this appendix, we explain the detailed procedure for finding a lower bound on M_{11}^Z and an upper bound on $e_{\rm ph}$ in equation (4). For our finite-key analysis of MDI-QKD and MA-QKD, we use the analytical estimation procedure introduced in [17], together with the tighter multiplicative Chernoff bounds introduced in [16]. Also, as in [21], we estimate the total single photon measurement counts M_{11} in both bases using data in the X basis only. We then link it with M_{11}^{zz} via random sampling analysis. This allows us to encode decoy intensities in the X basis only, thus wasting fewer rounds for statistical estimation.

B.1. Background

In the protocol, Alice and Bob emit phase-randomised coherent states of a random intensity $a \in \{z, w_1, w_2, v\}$, where the z intensity is encoded in the Z basis and the rest of the intensities are encoded in the X basis. Without knowing the basis information, the output state corresponding to intensity a can be written as

$$\rho_a = \sum_{n=0}^{\infty} p_{n|a}|n\rangle\langle n|, \tag{B1}$$

where $p_{n|a}$ is the probability that a pulse of intensity a contains n photons, and $|n\rangle$ is the n-photon Fock state. For WCPs, we can typically assume a Poisson distribution for the photon number, in which case, $p_{n|a} = a^n e^{-a}/n!$. While most of our analysis does not depend on the choice of the probability distribution, we also use the Poisson assumption for our numerical results. Based on the above diagonal form, for a pulse encoded in a given basis, the only information available to Eve is its photon number n. This implies that, instead of the actual protocol, Alice and Bob could have run the equivalent *virtual* scenario in which

- Alice (Bob) sends a Z-encoded n-photon Fock state with probability $p_{n,Z} = p_z p_{n|z}$.
- Alice (Bob) sends an X-encoded n-photon Fock state with probability $p_{n,X} = \sum_{a\in\{w_1,w_2,v\}} p_a p_{n|a}$.

In this virtual scenario, Alice and Bob can wait until after Eve's attack to assign each emission of an X-encoded n-photon Fock state to intensity $a \in \{w_1, w_2, v\}$ with probability

$$p_{a|n,X} = \frac{p_a p_{n|a}}{p_{n,X}}, \tag{B2}$$

and then 'reveal' their intensity choices in the appropriate step of the protocol, so that Eve cannot tell which scenario (actual or virtual) is being performed.

Note that Fock states encoded in different bases are in general partially distinguishable to Eve, so Alice and Bob must decide their encoding basis before their emission, even in the virtual scenario. There is one important exception, however: single-photon signals encoded in either the X or Z bases are indistinguishable once averaged by their selection probabilities, since

$$\rho_1 = \frac{1}{2}|H\rangle\langle H| + \frac{1}{2}|V\rangle\langle V| = \frac{1}{2}|D\rangle\langle D| + \frac{1}{2}|A\rangle\langle A|. \tag{B3}$$

This implies that the users could have replaced their single-photon emissions by the following purification of ρ_1

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|H\rangle + |1\rangle|V\rangle\right) = \frac{1}{\sqrt{2}}\left(|+\rangle|D\rangle + |-\rangle|A\rangle\right), \tag{B4}$$

where the first qubit, in $|0\rangle$–$|1\rangle$ basis, is held by the users and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. This allows us to alter our virtual scenario in the following way: when Alice and Bob both decide to send a single-photon state, they replace their respective emissions by the generation of $|\psi_1\rangle$, and then wait until after Eve's attack to decide in which basis to measure their ancilla. This delayed basis choice will allow us to estimate the statistics of Z-encoded single-photon emissions using X-basis data.

B.2. Estimation of M_{11}^Z

The estimation is divided in two steps:

(a) Estimation of M_{11}, the total single-photon measurement counts in both basis, using the decoy state analysis.

(b) Estimation of M_{11}^Z from M_{11}, via a random sampling analysis.

B.2.1. Estimation of M_{11}

In our virtual scenario, the users have replaced their decoy-state emissions by Fock states, which are only assigned to a particular intensity after Eve's attack. Let $\mathcal{M}_{nm}^X$, with $(n,m) \neq (1,1)$, be the set of rounds in which Alice (Bob) chooses the X basis, sends n (m) photons, and Charlie reports a successful detection. Also, let $M_{nm}^X = |\mathcal{M}_{nm}^X|$. After her reports, Alice and Bob will assign each event in $\mathcal{M}_{nm}^X$ to intensities $a, b \in \{w_1, w_2, v\}$ with probability

$$p_{ab|nm,X} = p_{a|n,X}p_{b|m,X} = \frac{p_a p_{n|a}}{p_{n,X}}\frac{p_b p_{m|b}}{p_{m,X}}, \tag{B5}$$

where $p_{n,X} = \sum_{a\in\{w_1,w_2,v\}} p_a p_{n|a}$ by the law of total probability. As explained above, Alice and Bob have also delayed their choice of basis on those rounds in which both sent a single photon. Let $\mathcal{M}_{11}$ be the set of rounds in which Alice and Bob sends a single photon and Charlie reports a successful detection, and let $M_{11} = |\mathcal{M}_{11}|$. The probability that they assign each event in $\mathcal{M}_{11}$ to intensities $a, b \in \{z, w_1, w_2, v\}$ is

$$p_{ab|11} = p_{a|1}p_{b|1} = \frac{p_a p_{1|a}}{p_1}\frac{p_b p_{1|b}}{p_1} \tag{B6}$$

where $p_1 = \sum_{a\in\{z,w_1,w_2,v\}} p_a p_{n|a}$ by the law of total probability. Let M^{ab} denote the number of rounds assigned to intensities $a, b \in \{w_1, w_2, v\}$. Its expected value is

$$\mathrm{E}[M^{ab}] = p_{ab|00,X}M_{00}^X + p_{ab|01,X}M_{01}^X + p_{ab|11}M_{11} + \sum_{(m,n)\in S} p_{ab|mn,X}M_{mn}^X, \tag{B7}$$

where $S = \{(m,n)|m,n \in \mathbb{Z}, m,n \geqslant 0\} - \{(0,0),(0,1),(1,1)\}$. Each of these intensity assignments is a Bernoulli random variable, and therefore $\mathrm{E}[M^{ab}]$ is the average value of the sum of some Bernoulli random variables. The values of M^{ab} measured by Alice and Bob correspond to an instance of this sum of Bernoulli random variables.

Let $\chi = \sum_{i=1}^n \chi_i$ be the outcome of the sum of n independent Bernoulli random variables $\chi_i \in \{0,1\}$. Given the observation of the outcome χ, its expectation value $E[\chi]$ can be bounded by [16]

$$\begin{aligned} \mathrm{E}^{\mathrm{L}}[\chi] &= \frac{\chi}{1+\delta^{\mathrm{L}}}, \\ \mathrm{E}^{\mathrm{U}}[\chi] &= \frac{\chi}{1-\delta^{\mathrm{U}}}, \end{aligned} \tag{B8}$$

except with probability ϵ, where δ^{L} and δ^{U} are the solutions of the equations

$$\left[\frac{\mathrm{e}^{\delta^{\mathrm{L}}}}{(1+\delta^{\mathrm{L}})^{1+\delta^{\mathrm{L}}}}\right]^{\chi/(1+\delta^{\mathrm{L}})} = \frac{1}{2}\varepsilon$$
$$\left[\frac{\mathrm{e}^{-\delta^{\mathrm{U}}}}{(1-\delta^{\mathrm{U}})^{1-\delta^{\mathrm{U}}}}\right]^{\chi/(1-\delta^{\mathrm{U}})} = \frac{1}{2}\varepsilon. \tag{B9}$$

These solutions can be expressed in terms of the Lambert W function, the inverse of $f(z) = ze^z$, as follows

$$\delta^{\mathrm{L}} = W_0(-\mathrm{e}^{\ln(\varepsilon/2-\chi)}/\chi)$$
$$\delta^{\mathrm{U}} = W_{-1}(-\mathrm{e}^{\ln(\varepsilon/2-\chi)}/\chi), \tag{B10}$$

which is useful for their quick numerical computation.

We use equation (B8) to find bounds on $E[M^{ab}]$, which by equation (B7) will set constraints on the values of M^X_{nm} and M_{11}. Since we are interested in M^{L}_{11}, our analysis can be reformulated as the optimization problem: find minM_{11} such that

$$\mathrm{E}^{\mathrm{L}}[M^{ab}] \leqslant p_{ab|00,X}M^X_{00} + p_{ab|01,X}M^X_{01} + p_{ab|11}M_{11} + \sum_{(m,n)\in S} p_{ab|mn,X}M^X_{mn} \leqslant \mathrm{E}^{\mathrm{U}}[M^{ab}] \tag{B11}$$

$\forall a, b \in \{w_1, w_2, v\}$. This problem can be solved using linear optimisation techniques [17]. In this work, however, we use the computationally faster analytical estimation method laid out in the supplementary note 1 of [17], for Poisson distributed input signals. Note that to use this analytical method, one needs to define the term $\hat{M}^X_{11}$ such that

$$p_{ab|11}M_{11} = p_{ab|11,X}\hat{M}^X_{11}, \tag{B12}$$

where $p_{ab|11,X}$ is given by equation (B5), and substitute $p_{ab|11}M_{11}$ by $p_{ab|11,X}\hat{M}^X_{11}$ in equation (B11). Then, one can use the results of [17] to find a lower bound on $\hat{M}^X_{11}$, and reuse equation (B12) to turn it into a lower bound M^{L}_{11} on M_{11}.

B.2.2. Estimation of M^Z_{11} from M_{11}

Let $\mathcal{M}^Z_{11}$ be the subset of $\mathcal{M}_{11}$ in which both users employ the Z basis, and let $M^Z_{11} = |\mathcal{M}^Z_{11}|$. By the delayed basis argument, Alice and Bob could decide which events in $\mathcal{M}_{11}$ belong to $\mathcal{M}^Z_{11}$ after Eve's attack. They assign each event in $\mathcal{M}_{11}$ to $\mathcal{M}^Z_{11}$ with probability

$$p_{zz|11} = \left(\frac{p_z p_{1|z}}{p_1}\right)^2. \tag{B13}$$

Let $\chi = \sum_{i=1}^n \chi_i$ be the outcome of the sum of n independent Bernoulli random variables $\chi_i \in \{0, 1\}$. Given the expectation value $E[\chi]$, the outcome χ can be lower-bounded by [16]

$$\chi \geqslant \chi^{\mathrm{L}} = (1-\delta)\bar{\chi}$$
$$\delta = \frac{-\ln(\varepsilon) + \sqrt{[\ln(\varepsilon)]^2 - 8\ \ln(\varepsilon)\bar{\chi}}}{2\bar{\chi}}, \tag{B14}$$

except with probability ε.

The lower bound on M^Z_{11} is then given by $(M^Z_{11})^{\mathrm{L}} = (1-\delta)\bar{\chi}$, where $\bar{\chi} = p_{zz|11}M^{\mathrm{L}}_{11}$ and δ is given by equation (B14).

B.3. Estimation of e_{ph}

The upper bound on e_{ph} is given by

$$e^{\mathrm{U}}_{\mathrm{ph}} = \frac{(E^Z_{11})^{\mathrm{U}}}{(M^Z_{11})^{\mathrm{L}}}, \tag{B15}$$

where E^Z_{11} is the number of phase errors in $\mathcal{M}^Z_{11}$, that is, the number of bit errors that Alice and Bob would have obtained if they had encoded their Z basis single-photon emissions in the X basis. The estimation of this quantity is divided in two steps:

(a) Estimation of E_{11}, the total amount of phase-flip errors in all single-photon emissions.

(b) Estimation of E^Z_{11} from E_{11}, via a random sampling analysis.

B.3.1. Estimation of E_{11}

Let us imagine that, in the virtual scenario, Alice and Bob measure all their pairs of ancillas in $\mathcal{M}_{11}$ in the X basis, even those that they have assigned to $\mathcal{M}_{11}^{Z}$. Let $\mathcal{E}_{11}$ be the subset of $\mathcal{M}_{11}$ in which they find a phase-flip error, and let $E_{11} = |\mathcal{E}_{11}|$. Each event in $\mathcal{E}_{11}$ is assigned to intensity $a, b \in \{z, w_1, w_2, v\}$ with probability $p_{ab|11}$ defined in equation (B6).

Also, let $\mathcal{E}_{nm}^{X}$, with $(n, m) \neq (1, 1)$, be the subset of $\mathcal{M}_{nm}^{X}$ in which Alice and Bob obtain a phase-flip error. Each event in $\mathcal{E}_{nm}^{X}$ is assigned to intensity $a, b \in \{w_1, w_2, v\}$ with probability $p_{ab|nm,X}$ defined in equation (B5). For $a, b \in \{w_1, w_2, v\}$, the expected value of E_{ab} with respect to these assignments is

$$\mathrm{E}[E^{ab}] = p_{ab|00,X}E_{00}^{X} + p_{ab|01,X}E_{01}^{X} + p_{ab|11}E_{11} + \sum_{(m,n)\in S} p_{ab|mn,X}E_{mn}^{X}. \tag{B16}$$

From equations (B8)–(B10), we obtain bounds $\mathrm{E}^{\mathrm{L}}[E^{ab}], \mathrm{E}^{\mathrm{U}}[E^{ab}]$, and redefine our analysis as the optimization problem: find max E_{11} such that

$$\mathrm{E}^{\mathrm{L}}[E^{ab}] \leqslant p_{ab|00,X}E_{00}^{X} + p_{ab|01,X}E_{01}^{X} + p_{ab|11}E_{11} + \sum_{(m,n)\in S} p_{ab|mn,X}E_{mn}^{X} \leqslant \mathrm{E}^{\mathrm{U}}[E^{ab}], \tag{B17}$$

$\forall a, b \in \{w_1, w_2, v\}$. Again, this problem can be solved using linear programing techniques, but we use the analytical estimation method in the supplementary note 1 of [17]. Note that to use this analytical method, one needs to define a term $\hat{E}_{11}^{X}$ such that

$$p_{ab|11}E_{11} = p_{ab|11,X}\hat{E}_{11}^{X}, \tag{B18}$$

where $p_{ab|11,X}$ is given by equation (B5), and substitute $p_{ab|11}E_{11}$ by $p_{ab|11,X}\hat{E}_{11}^{X}$ in equation (B17). Then, one can use the results of [17] to find an upper bound on $\hat{E}_{11}^{X}$, and reuse equation (B18) to turn it into an upper bound E_{11}^{U} on E_{11}.

B.3.2. Estimation of E_{11}^{Z} from E_{11}

By the delayed basis argument, each event in E_{11} will be assigned to E_{11}^{Z} with probability $p_{zz|11}$, defined in equation (B13).

Let $\chi = \sum_{i=1}^{n} \chi_i$ be the outcome of the sum of n independent Bernoulli random variables $\chi_i \in \{0, 1\}$. Given the expectation value $E[\chi]$, the outcome χ can be upper-bounded by [16]

$$\begin{aligned} \chi \leqslant \chi^{\mathrm{U}} &= (1+\delta)\bar{\chi} \\ \delta &= \frac{-\ln(\varepsilon) + \sqrt{[\ln(\varepsilon)]^2 - 8\ \ln(\varepsilon)\bar{\chi}}}{2\bar{\chi}}, \end{aligned} \tag{B19}$$

except with probability ε.

Finally, an upper bound on E_{11}^{Z} is given by $(E_{11}^{Z})^{\mathrm{U}} = (1+\delta)\bar{\chi}$, where $\bar{\chi} = p_{zz|11}E_{11}^{\mathrm{U}}$ and δ is given by equation (B19).

ORCID iDs

Guillermo Currás Lorenzo https://orcid.org/0000-0003-2096-0036
Mohsen Razavi https://orcid.org/0000-0003-4172-2125

References

[1] Pirandola S *et al* 2019 Advances in quantum cryptography arXiv:1906.01645
[2] Gisin N 2015 How far can one send a photon? *Front. Phys.* **10** 100307
[3] Muralidharan S, Li L, Kim J, Lütkenhaus N, Lukin M D and Jiang L 2016 Optimal architectures for long distance quantum communication *Sci. Rep.* **6** 20463
[4] Duan L-M, Lukin M D, Cirac J I and Zoller P 2001 Long-distance quantum communication with atomic ensembles and linear optics *Nature* **414** 413
[5] Sangouard N, Simon C, De Riedmatten H and Gisin N 2011 Quantum repeaters based on atomic ensembles and linear optics *Rev. Mod. Phys.* **83** 33
[6] Piparo N L and Razavi M 2015 Long-distance trust-free quantum key distribution *IEEE J. Sel. Top. Quantum Electron.* **21** 123–30
[7] Panayi C, Razavi M, Ma X and Lütkenhaus N 2014 Memory-assisted measurement-device-independent quantum key distribution *New J. Phys.* **16** 043005
[8] Abruzzo S, Kampermann H and Bruß D 2014 Measurement-device-independent quantum key distribution with quantum memories *Phys. Rev.* A **89** 012301
[9] Lo H-K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution *Phys. Rev. Lett.* **108** 130503

[10] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Overcoming the rate-distance limit of quantum key distribution without quantum repeaters *Nature* **557** 400
[11] Bhaskar M K *et al* 2020 Experimental demonstration of memory-enhanced quantum communication *Nature* **580** 60–4
[12] Piparo N L, Sinclair N and Razavi M 2017 Memory-assisted quantum key distribution resilient against multiple-excitation effects *Quantum Sci. Technol.* **3** 014009
[13] Piparo N L, Razavi M and Munro W J 2017 Memory-assisted quantum key distribution with a single nitrogen-vacancy center *Phys. Rev.* A **96** 052313
[14] Gottesman D, Lo H-K, Lutkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *Int. Symp. on Information Theory, 2004. ISIT 2004. Proc.* p 136
[15] Ma X, Qi B, Zhao Y and Lo H-K 2005 Practical decoy state for quantum key distribution *Phys. Rev.* A **72** 012326
[16] Zhang Z, Zhao Q, Razavi M and Ma X 2017 Improved key-rate bounds for practical decoy-state quantum-key-distribution systems *Phys. Rev.* A **95** 012333
[17] Curty M, Xu F, Cui W, Lim C C W, Tamaki K and Lo H-K 2014 Finite-key analysis for measurement-device-independent quantum key distribution *Nat. Commun.* **5** 3732
[18] Schmidt F and van Loock P 2019 Memory-assisted long-distance phase-matching quantum key distribution arXiv:1910.03333
[19] Takahashi H, Kassa E, Christoforou C and Keller M 2020 Strong coupling of a single ion to an optical cavity *Phys. Rev. Lett.* **124** 013602
[20] Piparo N L, Razavi M and Panayi C 2015 Measurement-device-independent quantum key distribution with ensemble-based memories *IEEE J. Sel. Top. Quantum Electron.* **21** 138–47
[21] Zhou Y-H, Yu Z-W and Wang X-B 2016 Making the decoy-state measurement-device-independent quantum key distribution practically useful *Phys. Rev.* A **93** 042324
[22] Ben-Or M, Horodecki M, Leung D W, Mayers D and Oppenheim J 2005 The universal composable security of quantum key distribution *Theory of Cryptography Conference* vol 3378 (Berlin: Springer) pp 386–406
[23] Renner R and König R 2005 Universally composable privacy amplification against quantum adversaries *Theory of Cryptography Conference* vol 3378 (Berlin: Springer) pp 407–25
[24] Camacho R M, Vudyasetu P K and Howell J C 2009 Four-wave-mixing stopped light in hot atomic rubidium vapour *Nat. Photon.* **3** 103
[25] Yang S-J, Wang X-J, Bao X-H and Pan J-W 2016 An efficient quantum light-matter interface with sub-second lifetime *Nat. Photon.* **10** 381
[26] Maeda K, Sasaki T and Koashi M 2019 Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit *Nat. Commun.* **10** 3140
[27] Currás Lorenzo G, Navarrete A, Azuma K, Kato G, Curty M and Razavi M 2019 Tight finite-key security for twin-field quantum key distribution arXiv:1910.11407
[28] Chen J-P *et al* 2020 Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km *Phys. Rev. Lett.* **124** 070501
[29] Marsili F *et al* 2013 Detecting single infrared photons with 93% system efficiency *Nat. Photon.* **7** 210–4
[30] Yu Y *et al* 2020 Entanglement of two quantum memories via fibres over dozens of kilometres *Nature* **578** 240–5
[31] Piparo N L and Razavi M 2014 Long-distance trust-free quantum key distribution *IEEE J. Sel. Top. Quantum Electron.* **21** 123–30
[32] Ma X, Fung C-H F and Razavi M 2012 Statistical fluctuation analysis for measurement-device-independent quantum key distribution *Phys. Rev.* A **86** 052305