ARTICLE OPEN

Check for updates

Surpassing the repeaterless bound with a photon-number encoded measurement-device-independent quantum key distribution protocol

Özlem Erkılıç[1] ✉, Lorcán Conlon[1], Biveen Shajilal[1], Sebastian Kish[1], Spyros Tserkis[1], Yong-Su Kim[2,3], Ping Koy Lam[1,4] and Syed M. Assad[1] ✉

Decoherence is detrimental to quantum key distribution (QKD) over large distances. One of the proposed solutions is to use quantum repeaters, which divide the total distance between the users into smaller segments to minimise the effects of the losses in the channel. Here we introduce a measurement-device-independent protocol which uses high-dimensional states prepared by two distant trusted parties and a coherent total photon number detection for the entanglement swapping measurement at the repeater station. We present an experimentally feasible protocol that can be implemented with current technology as the required states reduce down to the single-photon level over large distances. This protocol outperforms the existing measurement-device-independent and twin-field QKD protocols by achieving better key rates in general and higher transmission distance in total when experimental imperfections are considered. It also surpasses the fundamental limit of the repeaterless bound at a much shorter transmission distance in comparison to the existing TF-QKD protocols.

npj Quantum Information (2023)9:29 ; https://doi.org/10.1038/s41534-023-00698-5

INTRODUCTION

Quantum key distribution is a method used to securely establish a secret key between two distant trusted parties, namely Alice and Bob[1–3]. Depending on the degrees of freedom of the underlying quantum system involved, QKD protocols are classified into two types: discrete-variable (DV) protocols where the key information is encoded on discrete degrees of freedom of photonic states such as polarisation[4,5]; and continuous-variable (CV) based protocols which encode the keys on continuous degrees of freedom such as amplitude and phase quadratures of the optical field[6,7]. In QKD, the main obstacle in establishing a secure key over large distances for a pure-loss channel is the photon losses.

Quantum repeaters are devices that can be used to improve the transmission distance of QKD protocols by dividing the total distance into smaller portions between the sender and receiver, making the losses in the channel more manageable[8–12]. Quantum repeaters[12] use entanglement swapping[13–15] to distribute entanglement, which is enhanced by entanglement distillation protocols[16–18]. One issue is that a majority of these repeater protocols require the use of quantum memories[11,19,20]. However, quantum memories are limited by their operational wavelengths and memory efficiencies. Even though solid-state quantum memories[21,22] can operate at telecommunication wavelengths, their memory efficiency limits their efficacy. In contrast, cold-atom quantum memories currently hold the record for the efficiency, but operate outside of telecommunication wavelengths requiring frequency conversion to leverage communication infrastructure[23,24]. The frequency conversion results in low efficiencies limiting the performance of the current quantum repeaters[25].

The PLOB bound[26] sets the fundamental limit for the maximum amount of private states that can be transferred in QKD for a given quantum channel without the use of a repeater (See ref. [27] for the strong converse property of the bound and ref. [28] for the bounds generalised to repeater-assisted communication). No point-to-point QKD protocol can surpass this bound unless there is a quantum repeater splitting the channel. Therefore, the PLOB bound can also be used as a benchmark to test the quality of quantum repeaters[3]. It is known that the PLOB bound can be saturated with the squeezed-state protocol without the need for several copies of the states or a collective measurement for the pure-loss channel[3]. When there is a repeater-chain, the end-to-end quantum capacity scales with the number of repeaters[28] and it is still an open question whether the corresponding repeater bounds can be saturated with a simple protocol without multiple copies of the quantum states.

Measurement-device-independent QKD (MDI-QKD) protocols are a type of repeater protocols in which the secret keys are established via the measurement of an untrusted third party[29,30]. These protocols are called 'measurement-device-independent'as Alice and Bob do not perform a measurement in their stations, but the measurement is performed by an untrusted party, called Charlie. These protocols have been explored experimentally in refs. [30–35]. Twin-field QKD (TF-QKD)[36] is a DV based MDI protocol which utilises weak identical coherent states sent by both Alice and Bob to Charlie, who performs entanglement swapping via a probabilistic photon detection measurement. TF-QKD protocol is the first repeater protocol without a quantum memory that is able to surpass the PLOB bound[36–42] as it scales proportionally to the single-repeater bound[28]. CV based MDI (CV-MDI) QKD protocols work in a similar fashion where Alice and Bob both send a distribution of either coherent or squeezed states to Charlie, where he performs a heterodyne measurement[30,43,44]. In order to

[1]Centre of Excellence for Quantum Computation and Communication Technology, The Department of Quantum Science and Technology, Research School of Physics and Engineering, The Australian National University, Canberra, ACT, Australia. [2]Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Republic of Korea. [3]Division of Nano & Information Technology, KIST School, Korea University of Science and Technology, Seoul 02792, Republic of Korea. [4]Institute of Materials Research and Engineering, Agency for Science, Technology and Research (A*STAR), Singapore 138634, Singapore. ✉email: ozlemerkilic1995@gmail.com; cqtsma@gmail.com

achieve a positive key rate in these CV-MDI protocols, the relay is positioned very close to Alice resulting in a very asymmetric set-up. As the relay is not placed right in the middle between Alice and Bob, the protocols scale like the repeaterless bound instead of the single-repeater bound[45]. Hence, these protocols always sit below the PLOB bound.

In this work, we present a photon-number encoded MDI repeater protocol that surpasses the PLOB bound without the use of quantum memories through an entanglement swapping measurement. Unlike the TF-QKD protocol, the entanglement swapping is obtained by a coherent total photon number measurement performed by Charlie who measures the total number of photons coming from Alice and Bob without knowing the individual contributions. Even though the photon-number encoded states are vulnerable to losses, we show that in the short distance regime, the secret key rates are much higher than the ones of the single-photon encoded states. We also propose an experimentally feasible protocol using single-photons as these high dimensional states reduce down to the single-photon level over large distances. This protocol performs better than the existing MDI and TF-QKD protocols as it attains higher key rates for the same transmission distances.

RESULTS

First, we introduce our MDI protocol providing the details of the states that Alice and Bob use for key generation and estimating Eve's information followed by Charlie's entanglement swapping measurement. We then derive the asymptotic key rate formula for the computation of the secret key rate. Finally, we present the results of the high-dimensional protocol followed by the experimentally feasible version of the MDI protocol using single-photons.

Alice and Bob's states for generating a key

Let us assume that both Alice and Bob generate two-mode entangled states in their stations where they keep one arm of the entangled states to themselves and send the other to Charlie. Charlie then performs a joint entanglement swapping measurement on the states that Alice and Bob send.

QKD protocols can be expressed in either entanglement-based or prepare-and-measure schemes. Both of these models are mathematically equivalent[46,47], however the entanglement-based representation is more convenient for the security analysis of a QKD protocol. In the conventional entanglement-based CV-QKD protocols, Alice sends one arm of a two-mode squeezed vacuum state (TMSV) to Bob while performing a heterodyne measurement on the other arm of the TMSV state she kept. This procedure is equivalent to Alice sending a coherent state in the prepare-and-measure scheme[47]. This entangled two-mode state in Fock basis is expressed as

$$|\Psi\rangle_{\mathrm{A_1A_2}} = \frac{1}{\sqrt{N}}\sqrt{1-\gamma^2}\sum_{n=0}^{n_{\max}}\gamma^n|nn\rangle_{\mathrm{A_1A_2}}, \tag{1}$$

where $\gamma \in [0,1)$ is the squeezing parameter and N is the normalisation coefficient given by $\sum_{n=0}^{n_{\max}}(1-\gamma^2)\gamma^{2n}$. $|n\rangle$ denotes the n-photon Fock state. Note that a TMSV state is retrieved with when $n_{\max} \to \infty$[46].

In this paper, we use the entanglement-based version, shown in Fig. 1a, for the security analysis of the prepare-and-measure method, shown in Fig. 1b. We express Alice's and Bob's states as follows:

$$|\Psi\rangle_{\mathrm{A_1A_2}} = \sum_{n=0}^{n_{\max}}\sqrt{a_n}|nn\rangle_{\mathrm{A_1A_2}}, \tag{2}$$

$$|\Psi\rangle_{\mathrm{B_1B_2}} = \sum_{n=0}^{n_{\max}}\sqrt{b_n}|nn\rangle_{\mathrm{B_1B_2}}, \tag{3}$$

where $\sum_{n=0}^{n_{\max}} a_n = 1$ and $\sum_{n=0}^{n_{\max}} b_n = 1$. a_n and b_n represent real coefficients of each Fock-number state $|nn\rangle$ for Alice and Bob, respectively. These coefficients are the same for both Alice and Bob and optimised to achieve an optimal key rate explained in more detail in Calculation of the secret key rate. $n_{\max}$ is the maximum number of photons that Alice and Bob send individually, and each party encodes the key information on the Fock states $|n\rangle$.

In the entanglement-based scheme, Alice and Bob keep one arm of the entangled states to measure the number of photons using a photon-number resolving detector (PNRD) to establish a key while sending the other arm to Charlie. Charlie performs a coherent total photon number measurement on the incoming modes from Alice and Bob, and announces the outcome of his measurement (described in detail in Charlie's measurement).

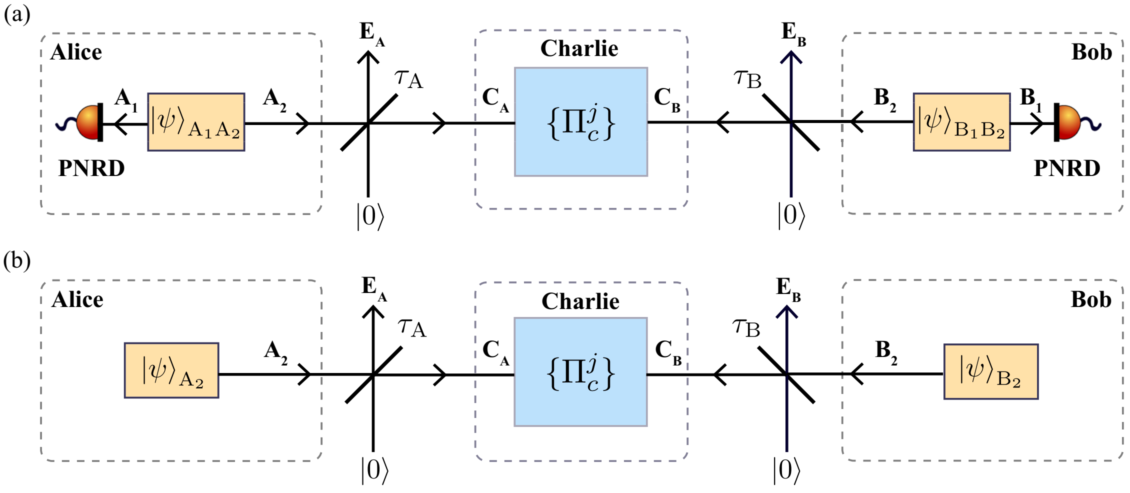

Fig. 1 Equivalent representations of the protocol. **a** Entanglement-based scheme where both Alice and Bob send optimised states with $n_{\max} = 7$ to Charlie while keeping one arm of their states to themselves denoted as modes $\mathrm{A_1}$ and $\mathrm{B_1}$, respectively, and measure the number of photons using photon-number resolving detectors (PNRDs). Charlie interferes modes $\mathrm{A_2}$ and $\mathrm{B_2}$ coming from Alice and Bob and performs a coherent total photon number measurement. **b** Prepare-and-measure scheme where Alice and Bob send single-mode states to Charlie where they encode the key information on the single mode Fock state one at a time. Charlie then performs a total photon number measurement in his station on the modes that Alice and Bob send.

Alice and Bob's measurement in their own stations is represented as

$$\Pi_n = |n\rangle\langle n|, \tag{4}$$

where n denotes the number of photons being measured. In the prepare-and-measure scheme, this corresponds to preparing the Fock state $|n\rangle$ with probability a_n or b_n for Alice and Bob, respectively. The states in the prepare-and-measure scheme can be engineered experimentally with several different methods such as conditional teleportation[48], coherent displacements and photon subtraction[49], and repeated parametric-down conversion[50]. Alternatively, these states can be created by extending the work presented in ref. [51] to higher photon levels by using spontaneous parametric down-conversion on the signal channel and conditional measurements on the idler channel.

Charlie's measurement

The states are sent to Charlie via a channel with a total transmissivity of $\tau \in [0, 1]$, which is split into smaller channels between Alice and Charlie and Charlie and Bob represented as τ_A and τ_B, respectively. Single-repeater protocols can be benchmarked based on the PLOB bound, which is given by $-\log_2(1-\tau)$[26,28]. In order to surpass this bound, the protocol needs to scale like the single-repeater bound[28], which is expressed as $-\log_2(1-\sqrt{\tau})$. This requires Charlie to be positioned in the middle of Alice and Bob such that the key-rate scales with the square root of the transmission probability, $O(\sqrt{\tau})$. In this protocol, Charlie performs a collective photon number measurement on the incoming modes from Alice, A_2, and Bob, B_2. If Alice and Bob send a maximum of n photons each, denoted as $n_{\max}$, Charlie can measure from 0 to $2n_{\max}$ photons. Charlie's measurement can be realised by projecting the modes A_2 and B_2 onto the following states

$$\left|\phi_c^j\right\rangle = \sum_{n=0}^{c} \frac{\omega^{nj}|n\rangle|c-n\rangle}{\sqrt{c+1}}, \tag{5}$$

where $c \in \{0, 1, \cdots, 2n_{\max}\}$ represents the total number of photons Charlie receives from the two modes, and $j \in \{0, 1, \cdots, c\}$ denotes the different states in the c-photon subspace states while ω is given by $\omega = e^{\frac{2\pi i}{c+1}}$.

For example, when $c = 2$, Charlie's three possible outcomes are

$$\left|\phi_2^0\right\rangle = \frac{1}{\sqrt{3}}(|02\rangle + |11\rangle + |20\rangle), \tag{6}$$

$$\left|\phi_2^1\right\rangle = \frac{1}{\sqrt{3}}\left(|02\rangle + e^{\frac{2\pi i}{3}}|11\rangle + e^{-\frac{2\pi i}{3}}|20\rangle\right), \tag{7}$$

$$\left|\phi_2^2\right\rangle = \frac{1}{\sqrt{3}}\left(|02\rangle + e^{-\frac{2\pi i}{3}}|11\rangle + e^{\frac{2\pi i}{3}}|20\rangle\right). \tag{8}$$

These measurements are designed such that even though Charlie knows the total number of photons between Alice and Bob, he does not know the number of photons in each mode separately.

The outcomes of Charlie's measurement form a valid positive operator value measurement (POVM) for a given outcome

$$\Pi_c^j = \left|\phi_c^j\right\rangle\left\langle\phi_c^j\right|, \tag{9}$$

with all the possible outcomes satisfying the identity resolution with $c \in \{0, 1, \cdots, 2n_{\max}\}$ and $j \in \{0, 1, \cdots, c\}$, i.e.,

$$\sum_{c=0}^{2n_{\max}} \sum_{j=0}^{c} \Pi_c^j = \mathbb{I}. \tag{10}$$

The measurement performed by Charlie establishes correlations between Alice and Bob. In the lossless channel, when Charlie detects two photons with his POVM element $\left|\phi_2^0\right\rangle$, Alice and Bob's state becomes $|\psi\rangle_{A_1B_1}\big|^{j=0}_{c=2} = \sqrt{a_0a_2}|02\rangle + a_1|11\rangle + \sqrt{a_2a_0}|20\rangle$. Therefore, Charlie swaps the entanglement between Alice and Bob via the measurement he performs similar to many MDI protocols[29,36].

Alice and Bob's check states for security

A possible security issue is that Charlie can potentially lie to Alice and Bob about his measurement outcome, as he can perform separable measurements on Alice and Bob's modes individually or announce a different photon number from the one he actually measured. When the latter occurs, Alice and Bob can tell that Charlie is not telling the truth as the probabilities of measuring different number of photons are not equal. However, when the former happens, Alice and Bob cannot distinguish whether Charlie is performing a total photon number measurement or a separable measurement on the two modes. Even though the separable measurement does not yield an entangled state between Alice and Bob, it still establishes classical correlations between the parties. The probability of Charlie measuring a given number of photons when he performs a separable measurement ends up being the same as his joint measurement described in Charlie's measurement.

We address this security issue by Alice and Bob randomly switching from their key states and sending some check states to Charlie to detect any abnormalities in the system. One of the possible check states they send consists of a superposition of the photon number states, and are analogous to the original DV diagonal states in the following form

$$|+\rangle = \sum_{n=0}^{n_{\max}} \sqrt{\epsilon_n}|n\rangle, \tag{11}$$

where ϵ_n represents the coefficients a_n and b_n in Eq. (2) and (3) for Alice and Bob, respectively.

The untrusted party, Charlie, is required to announce the total number of photons he measured as well as the outcome index (c, j). Table 1 shows Charlie's probability of measuring $c = 2$ photons as Alice and Bob send a mixture of key states and check states. Whenever both parties send $|{+}{+}\rangle_{AB}$, the probability of Charlie measuring $c = 2$ photons is different for the non-separable and separable measurements. This is due to the nature of Charlie's POVM. For $c = 2$, Charlie has three different outcomes in this set labelled as $\left|\phi_2^0\right\rangle, \left|\phi_2^1\right\rangle$, and $\left|\phi_2^2\right\rangle$. If Alice and Bob send $|{+}{+}\rangle_{AB}$, the probability of measuring $\left|\phi_2^0\right\rangle$ is 1/3 whereas the other two outcomes return 0. In the case of separable measurements, the probability of measuring a two-photon event is equal, allowing Alice and Bob to determine whether Charlie is being unfaithful or not.

The separable measurement is not the only possible measurement that Charlie can make. Ideally, Alice and Bob should not rely on Charlie's announcement of his measurement basis to determine if Charlie was being reliable or estimate how much information is leaked to another malicious party, called Eve. For security purposes, it is essential to utilise two or more non-orthogonal bases in QKD. For example, in BB84[4] and the six-state

Table 1. Charlie's measurement probability for both non-separable and separable measurements for $c = 2$ when Alice and Bob send a combination of their check states, $(+)$, $|+\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$ and key states, (K), $\rho_{A_2} = \frac{1}{3}(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|)$ in the prepare-and-measure representation with $n_{\max} = 2$ photons.

	Non-separable			Separable		
AB	Π_2^0	Π_2^1	Π_2^2	02	11	20
KK	1/9	1/9	1/9	1/9	1/9	1/9
$K+$	1/9	1/9	1/9	1/9	1/9	1/9
$+K$	1/9	1/9	1/9	1/9	1/9	1/9
$++$	1/3	0	0	1/9	1/9	1/9

protocol[52], Alice sends states in two and three different orthogonal bases to Bob, respectively. By calculating the bit-error rates in these bases, Alice and Bob can estimate Eve's information. However, these protocols use only the probabilities of the matched measurement outcomes, which overestimates Eve's information resulting in a lower key rate[53]. Refs. [53,54] showed that full tomography of the quantum state between Alice and Bob can enhance the secret key rate due to bounding Eve's information more accurately. Instead of using the statistics of the matched bases only, Alice and Bob can estimate their joint state from both the matched and unmatched bases. This joint state then can be used to calculate the Holevo bound on Eve's information. The Holevo bound[55] describes the maximum amount of classical information that can be extracted from a quantum channel. In QKD, Holevo bound can be used to upper bound the leaked information to Eve.

Our protocol requires a similar approach to the protocols discussed above[53,54], where Alice and Bob measure their joint state in mutually unbiased bases to perform a full tomography of their joint state in the entanglement-based scheme. Two bases $\{|e_i\rangle\}_{i=0}^{m-1}$ and $\{|h_i\rangle\}_{i=0}^{m-1}$ are called mutually unbiased when $|\langle e_i|h_j\rangle|^2 = 1/m$ for any i and j[56], where m is the dimension of the Hilbert space. If the dimension of the Hilbert space, m, is a power of a prime number, there exists $m+1$ mutually unbiased bases which form a complete set[57]. In Estimating Eve's information using quantum tomography with single-photon states, we show how to estimate Eve's information by reconstructing Alice and Bob's joint state through full tomography when Alice and Bob send single-photon states, i.e., $n_{\max} = 1$. In the entanglement-based scheme, Alice and Bob measure the modes they keep in their stations using the eigenvectors of the X, Y and Z bases which are expressed as

$$|\pm x\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, \tag{12}$$

$$|\pm y\rangle = \frac{|0\rangle \pm \mathrm{i}|1\rangle}{\sqrt{2}}, \tag{13}$$

$$|+z\rangle = |0\rangle, \quad |-z\rangle = |1\rangle. \tag{14}$$

These bases form a complete set of mutually unbiased bases for $m = 2$. In the equivalent prepare-and-measure scheme, Alice and Bob's measurement on the two mode entangled states, $|\Psi\rangle_{\mathrm{A_1A_2}} = \sqrt{a_0}|00\rangle + \sqrt{a_1}|11\rangle$ and $|\Psi\rangle_{\mathrm{B_1B_2}} = \sqrt{b_0}|00\rangle + \sqrt{b_1}|11\rangle$ in the Z basis corresponds to them preparing the following states

$$|\psi_{+z}\rangle = |0\rangle, \tag{15}$$

$$|\psi_{-z}\rangle = |1\rangle, \tag{16}$$

with probability a_0 and b_0, and a_1 and b_1, respectively. Their measurement in the X basis is equivalent to them preparing the following states with equal probability

$$|\psi_{\pm x}\rangle = \sqrt{\epsilon_0}|0\rangle \pm \sqrt{\epsilon_1}|1\rangle, \tag{17}$$

i.e., they prepare $|\psi_{+x}\rangle$ and $|\psi_{-x}\rangle$ with a probability of 0.5, where ϵ_0 and ϵ_1 represent the coefficients a_0 and b_0, and a_1 and b_1, respectively. Similarly, their measurement in the Y bases corresponds to them preparing the following states with equal probability

$$|\psi_{\pm y}\rangle = \sqrt{\epsilon_0}|0\rangle \mp \mathrm{i}\sqrt{\epsilon_1}|1\rangle. \tag{18}$$

We present the detailed results of this protocol in Realistic implementation of the MDI protocol with single-photon states.

When Alice and Bob wish to encode the key onto the higher dimensional states, i.e., $n_{\max} > 1$, the number of check states they need to send increases. However, determining the existence of a complete set of mutually unbiased bases in an arbitrary dimensional Hilbert space is still an open problem in quantum information[58]. In this protocol, if Alice and Bob send states with $n_{\max}$ photons with a dimension of $m = n_{\max} + 1$, they need to send check states using all the eigenvectors of $m+1$ mutually unbiased bases to estimate Eve's Holevo bound provided that m is a power of a prime number. These check states can be determined by following the method discussed in ref. [57]. They can also be implemented experimentally using the methods discussed in refs. [48–50] and scaling the experiment performed by Bimbard et al.[51] from two-photon level to higher dimensions similar to the key states in the prepare-and-measure scheme. We show the key rates of these higher dimensional states later in detail in The Results of the high-dimensional states with $n_{\max} = 7$ photons.

Calculation of the secret key rate

In the entanglement-based protocol, the global state before Charlie's measurement is a four-mode state. The dimension to simulate this protocol scales as m^4. Therefore, the coefficients of Alice and Bob's states in Eq. (2) and (3) are optimised by considering a classical protocol where Eve and Charlie perform a photon number measurement on their modes. We optimise the difference between the classical mutual information between Alice and Bob, and, Eve and Alice. We call this protocol the 'classical protocol' and an explicit method for the implementation of this protocol is shown in Classical protocol used to optimise the coefficients of the high dimensional states. The reason for doing this is to avoid having to optimise a high dimensional four mode joint state with a total dimension of m^4. However, when computing the secret key rates, we do not assume any type of attacks for Eve and calculate Eve's Holevo bound instead and Charlie performs his collective photon number measurement. It is also important to note that the optimisation problem is not convex for the high-dimensional states and the solution provided for the coefficients a_n and b_n in this paper is one possible solution.

The states that Alice and Bob prepare are previously shown in Eq. (2) and (3), respectively. They send these states through a pure-loss channel with a transmissivity τ_{A} and τ_{B} for the channel between Alice and Charlie and Charlie and Bob, respectively. The pure-loss channel is modelled with a beamsplitter with a transmissivity τ, where the beamsplitter mixes the input mode with the vacuum. The beamsplitter transformation can be defined as

$$B(\tau) = \exp[\cos^{-1}(\sqrt{\tau})(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger)], \tag{19}$$

where τ can be written as a function of the fibre distance, d, with a loss of 0.2dB per km with $\tau = 10^{-0.02d}$. $\hat{a}$ and $\hat{b}$ are the annihilation operators, while $\hat{a}^\dagger$ and $\hat{b}^\dagger$ are the creation operators of the two modes, respectively.

In this protocol, we assume that Eve has full access to the channel between Alice and Charlie and Charlie and Bob including Charlie's measurements. Eve mixes vacuum with the incoming modes causing Alice and Bob to lose photons. Thus, we can express the state between Alice and Charlie and Charlie and Bob after Eve's attack as

$$\rho_{\mathrm{A_1C_A}} = \mathrm{Tr}_3\Big[\{\mathbb{I}_m \otimes B(\tau_{\mathrm{A}})\}\{\rho_{\mathrm{A_1A_2}} \otimes |0\rangle\langle 0|\}\{\mathbb{I}_m \otimes B(\tau_{\mathrm{A}})\}^\dagger\Big], \tag{20}$$

$$\rho_{\mathrm{C_BB_1}} = \mathrm{Tr}_1\Big[\{B(\tau_{\mathrm{B}}) \otimes \mathbb{I}_m\}\{|0\rangle\langle 0| \otimes \rho_{\mathrm{B_2B_1}}\}\{B(\tau_{\mathrm{B}}) \otimes \mathbb{I}_m\}^\dagger\Big], \tag{21}$$

where $\mathrm{Tr}_i[\rho]$ stands for tracing out the i-th mode of the state ρ.

After Charlie's measurement and tracing out his modes, the subnormalised state between Alice and Bob becomes

$$\tilde{\rho}_{\mathrm{AB}|^j_c} = \mathrm{Tr}_{23}\Big[\big(\mathbb{I}_m \otimes \Pi^j_c \otimes \mathbb{I}_m\big)\big(\rho_{\mathrm{A_1C_A}} \otimes \rho_{\mathrm{C_BB_1}}\big)\big(\mathbb{I}_m \otimes \Pi^j_c \otimes \mathbb{I}_m\big)^\dagger\Big]. \tag{22}$$

We can calculate Charlie's probability of obtaining outcomes (c, j) from the following expression

$$P_{\substack{j\\c}} = \mathrm{Tr}\Big[\tilde{\rho}_{\mathrm{AB}|^j_c}\Big]. \tag{23}$$

Normalising Alice and Bob's joint state by Charlie's probability of measuring c photons for his measurement j gives us the final conditional state between them as

$$\rho_{\mathrm{AB}|_c^j} = \frac{\tilde{\rho}_{\mathrm{AB}|_c^j}}{P_c^j}. \tag{24}$$

However, for the key states that Alice and Bob send, the probability of Charlie measuring c photons, Alice and Bob's conditional mutual information and Eve's conditional information do not change for each j ranging from 0 to c. As such, there is no need to calculate Alice and Bob's conditional joint state for each value of j. Therefore, we omit j from the following equations and set it to zero.

We then calculate Charlie's total probability of measuring c photons from

$$P_c = \sum_{j=0}^{c} \mathrm{Tr}\left[\tilde{\rho}_{\mathrm{AB}|_c^j}\right] = (c+1)\mathrm{Tr}\left[\tilde{\rho}_{\mathrm{AB}|_c^{j=0}}\right], \tag{25}$$

since there are $c+1$ POVM outcomes with a total photon number c.

In order to calculate Alice and Bob's mutual information, we first generate Alice and Bob's probability table as follows

$$P(n_a, n_b|c) = \langle n_a, n_b|\rho_{\mathrm{AB}|_c}|n_a, n_b\rangle, \tag{26}$$

where each term in Alice and Bob's mutual information is given by the conditional Shannon's entropy as expressed below

$$H(A|c) = -\sum_{n_a=0}^{n_{\max}} P(n_a|c)\log_2 P(n_a|c), \tag{27}$$

$$H(B|c) = -\sum_{n_b=0}^{n_{\max}} P(n_b|c)\log_2 P(n_b|c), \tag{28}$$

$$H(AB|c) = -\sum_{n_a=0}^{n_{\max}} \sum_{n_b=0}^{n_{\max}} P(n_a, n_b|c)\log_2 P(n_a, n_b|c). \tag{29}$$

Using the equations above, we evaluate Alice and Bob's mutual information conditioned on Charlie's measurement outcome from $I_{AB|c} = H(A|c) + H(B|c) - H(AB|c)$.

Eve's information is calculated from Alice and Bob's conditional state after Bob's measurement outcome on this joint state using

$$I_{E|c} = S(\rho_{\mathrm{AB}|c}) - \sum_{b=0}^{n_{\max}} P_b S(\rho_{\mathrm{A}|cb}), \tag{30}$$

where Bob's POVM is shown in Eq. (4) in Alice and Bob's states for generating a key. b represents the number of photons that Bob measures while P_b corresponds to Bob's probability of measuring b photons. The subnormalised state $\tilde{\rho}_{\mathrm{A}|cb}$ is obtained from

$$\tilde{\rho}_{\mathrm{A}|cb} = \mathrm{Tr}_2\left[(\mathbb{I}_m \otimes \Pi_b)\rho_{\mathrm{AB}|_c}(\mathbb{I}_m \otimes \Pi_b)^\dagger\right], \tag{31}$$

where Bob's probability of measuring b photons is given by

$$P_b = \mathrm{Tr}[\tilde{\rho}_{\mathrm{A}|cb}]. \tag{32}$$

Alice's subnormalised state conditioned on Bob's and Charlie's measurement outcomes, $\tilde{\rho}_{\mathrm{A}|cb}$ is then normalised by Bob's measurement probability by

$$\rho_{\mathrm{A}|cb} = \frac{\tilde{\rho}_{\mathrm{A}|cb}}{P_b}. \tag{33}$$

The asymptotic key rate of this protocol requires the combination of all the possible outcomes of Charlie's POVM since Alice and Bob are sending states with n photons each with a possibility of measuring 0 to $2n$ photons by Charlie. However, we discard events where Eve's conditional information is greater than Alice and Bob's conditional mutual information. For example, when a zero photon occurs, Eve gets more information than Alice and Bob due to all the photons being lost to Eve. As such we exclude the case when $c = 0$. Similarly, when Charlie measures $c = 2n_{\max}$ photons, the key rate conditioned on this measurement outcome is zero even though Eve's conditional information is zero. Therefore, the resulting asymptotic key rate can be expressed as

$$K = \sum_{c=0}^{2n_{\max}} P_c \max\left[0, I_{AB|c} - I_{E|c}\right]. \tag{34}$$

The Results of the high-dimensional states

Our simulation results are shown in Fig. 2a for the pure-loss channel with 0.2dB loss per km. We compare our results with the existing MDI protocols such as the CV-MDI protocol from Pirandola et al.[30] and one of the best performing TF-QKD protocols known as TF-QKD without phase post-selection (NPP-TF-QKD) from Cui et al.[59] and Lu et al.[60].

We first show the case where Alice and Bob send the states shown in Eq. (1) with a squeezing coefficient of $\gamma = 0.26$ for each distance with $n_{\max} = 7$ photons. The squeezing level of $\gamma = 0.26$ was determined based on the shortest distance that the protocol exceeds the PLOB bound (refer to Coefficients of the optimised states, Table 4 for the details). With these states, the PLOB bound and the CV-MDI protocol are surpassed at 144 km and 114 km, respectively, while the protocol is performing worse than the TF-QKD protocol. We also demonstrate the key rates of the same states where the values of γ are optimised to give the maximum secret key rate at the corresponding distance. For distances greater than 50 km, there is not much difference compared to the states with $\gamma = 0.26$ and the PLOB bound is still surpassed at the same distance as the case of $\gamma = 0.26$. However, the key rates are now higher at short distances below 50 km. This indicates that in the short distance regime, the contribution of the higher order photons to the key rate is significant while at larger distances, the main contribution comes from the the first few photons of the state as the majority of the photons are lost to the environment at such distances. This can also be seen from the optimal squeezing level given in Table 4, which is higher for short distances and lower for larger distances.

When Alice and Bob send the optimised states shown in Eq. (2) and (3), these states outperform the results of the states with optimised γ by surpassing the repeaterless bound and the CV-MDI protocol at 108 km and 75 km, respectively. These states also do considerably better than the TF-QKD protocol as the TF-QKD protocol exceeds the PLOB bound at only 130 km and its key rates are lower than our protocol at each distance. It is important to note that this result can also be achieved by using the optimised states with $n_{\max} = 1$ photon in the form of $\sqrt{a_0}|00\rangle + \sqrt{a_1}|11\rangle$ as shown in Fig. 2a since both states reach the PLOB bound at the same distance and the key-rates converge beyond 10 km. In Fig. 2a, both high-dimensional and single-photons states have the same gradient, scaling like the single-repeater bound with $O(\sqrt{\tau})$. The probability of receiving n-photons in this case is given by $(\sqrt{\tau})^n$. Therefore, the main scaling of the key rates comes from the single-photon level, while the remaining photons help the key rate incrementally. As the loss gets higher, the probability of receiving higher photons drops. Therefore, beyond 10 km, we are only interested in 1 or 2 photons. This is further emphasised in Fig. 3a where we show the probability of sending each Fock-number state of the optimised states given in Eq. (2) and (3) for each transmission distance. At short distances, the high-dimensional states have contribution from each photon number. It is important to note that at 0 km, the probability of sending each Fock-number state is not equal due to key rate being equal to zero when Charlie

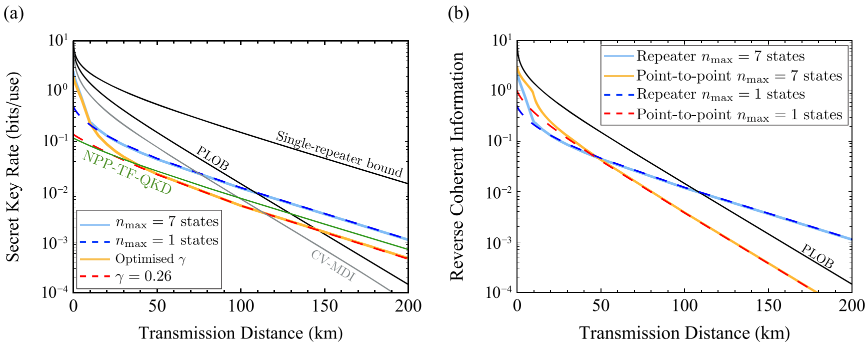

Fig. 2 Simulation results of our repeater protocol for a pure-loss channel with a loss of 0.2 dB/km. a Solid orange and red dashed lines show the key rates of our protocol using the states shown in Eq. (1) with $n_{\max} = 7$ photons with optimised squeezing coefficients and a squeezing coefficient of $\gamma = 0.26$, respectively. Blue dashed line shows the results of the optimised states with $n_{\max} = 1$ photon given in Eq. (2) and (3) and using Charlie's POVM with an outcome of 1 and 2 photons. The solid blue line shows our protocol using the optimised states with $n_{\max} = 7$ photons given in Eq. (2) and (3). Black solid lines show the single-repeater and repeaterless bounds. Solid grey line represents the CV-MDI protocol[30] with a variance of 1000 and relay positioned at 0.01 m away from Alice, while the solid green line shows the TF-QKD protocol with no phase post-selection (NPP-TF-QKD)[60] using optimised coherent states and infinite decoy states. **b** The comparison of the reverse coherent information of the optimised states with $n_{\max} = 7$ and $n_{\max} = 1$ photons in the form of Eq. (2) and (3) in point-to-point communications between Alice and Bob and with a single-repeater. The faint blue and orange lines represent the RCI of the single-repeater and point-to-point communications of the optimised states with $n_{\max} = 7$ photons correspondingly, while the blue and red dashed lines show the RCI of the single-repeater and point-to-point communications of the optimised states with $n_{\max} = 1$ photon. The black solid line shows the reverse coherent information of an infinitely squeezed TMSV state denoted as PLOB.

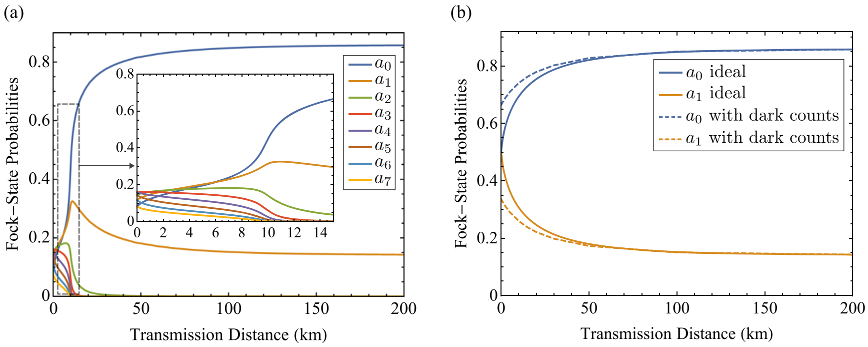

Fig. 3 Simulation results of the optimised coefficients. a The optimised coefficients of the states shown in Eq. (2) and (3) with $n_{\max} = 7$ photons, where the coefficients are explicitly shown in Table 2. **b** The optimised coefficients of the states shown in Eq. (2) and (3) with $n_{\max} = 1$ photon (refer to Table 3 for the optimised coefficients for each distance).

receives 0 or 14 photons in total. Therefore, the coefficients of the Fock states $|0\rangle$ and $|7\rangle$ are minimised accordingly. As the distance increases, the high-dimensional states reduce down to the single-photon level as the coefficients of the Fock states above one photon approach zero. The probabilities of sending zero and one photon, denoted as a_0 and a_1, of these high-dimensional states shown in Fig. 3a converge to the coefficients of the optimised states with $n_{\max} = 1$ photon shown in Fig. 3b beyond approximately 50 km. However, the main advantage of using the optimised states with $n_{\max} = 7$ is the ability of obtaining higher key rates at shorter distances. This is shown in Fig. 4, as the secret key rate increases when the number of encoded photons changes from 1 to 7 photons.

As the key rates of the optimised states with $n_{\max} = 7$ converge with the results of the states with optimised γ below 10 km and with the optimised states with $n_{\max} = 1$ photon, one can use the combination of the states with optimised γ and optimised states with $n_{\max} = 1$ photon beyond this distance to achieve the same results of the states given in Eq. (2) and (3).

As mentioned previously, the maximum key rate achievable by QKD for the point-to-point and single-repeater communication is bounded by the PLOB and single-repeater bounds, respectively[26,28]. These bounds are determined by the maximum amount

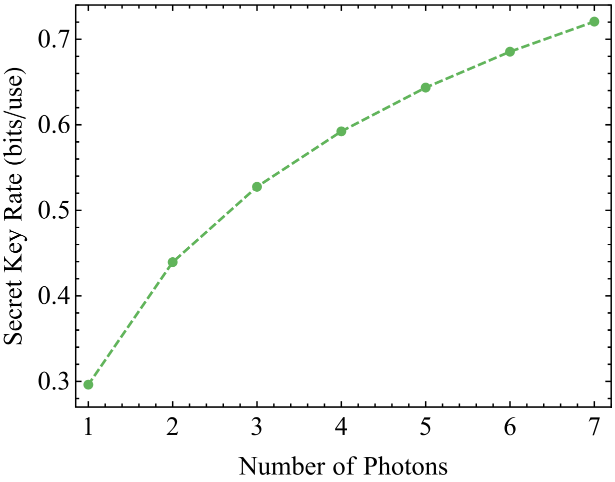

Fig. 4 Simulation results of the secret key rate when the number of encoded photons varies from 1 to 7 photons at 5 km. The states are in the form of Eq. (2) and (3) where the coefficients of each state are optimised.

of entanglement that a channel can sustain, also known as the entanglement flux, which coincides with reverse coherent information (RCI) of a maximally entangled TMSV state for the pure-loss channel[26,61,62]. RCI is used to lower bound the distillable entanglement of a given channel[62] and is a measure of the transmission of quantum information. While the key rates above demonstrate that our protocol surpasses the PLOB bound and acts as a repeater, the secret key rate is a measure of the transmission of classical information. The key rates are also bounded by the amount of entanglement that Alice and Bob can distill. Therefore, we also compute the RCI of our quantum states to verify the distillable entanglement between Alice and Bob after Charlie's measurement using

$$\mathrm{RCI} = \sum_{c=0}^{2n_{\max}} P_c \max\left[0, S(\rho_{\mathrm{A}|c}) - S(\rho_{\mathrm{AB}|c})\right], \tag{35}$$

where $S(\rho_{AB|c})$ and $S(\rho_{A|c})$ are the von Neumann entropies of the joint state between Alice and Bob $\rho_{AB|c}$ and Alice's state $Tr_2[\rho_{AB|c}]$, respectively.

In Fig. 2b, we show the RCI of the optimised states with $n_{\max} = 7$ and $n_{\max} = 1$ when Alice and Bob perform point-to-point and single-repeater communications. We compare these results with the PLOB bound as it coincides with the RCI of a maximally entangled TMSV state in the pure-loss channel. Note that when Alice and Bob communicate directly using the optimised states with $n_{\max} = 7$, they cannot saturate the PLOB bound due to sending states with a limited number of photons. However, they can reach the PLOB bound if they send infinitely squeezed TMSV states with an infinite number of photons[3]. In Fig. 2b, when Alice and Bob perform point-to-point communication, they can distill more entanglement at short distances. However, with the use of a repeater, they are able to distill more entanglement beyond 47 km and surpass the RCI of an infinitely squeezed TMSV state at 108 km. Note that they also surpass the PLOB bound at this distance when we calculate their secret key rate as shown in Fig. 2a and the key rates coincide with the reverse coherent information of Alice and Bob's conditional joint state on Charlie's measurement outcome. This indicates that after Charlie's measurement, Alice and Bob's PNRD measurement is optimal as Alice and Bob achieve the same key rates as the distillable entanglement of their joint state.

Realistic implementation of the MDI protocol with single-photon states

The experimental realisation of the higher dimensional optimised states and Charlie's measurement is quite challenging with state of the art technology. In this section, we present an experimentally feasible implementation of our protocol, shown in Fig. 5, by using single-photon states which can be performed with existing technology. Fig. 2a demonstrates that beyond 10 km, the single-photon states achieve the same key rates as the higher dimensional states and the high-dimensional states reduce down to the single-photon level as demonstrated in Fig. 3a and Fig. 3b.

When Alice and Bob send single-photon states, Charlie can measure from 0 to 2 photons. However, as mentioned previously in Calculation of the secret key rate, when Charlie measures 2 photons, the conditional secret key rate is zero as such the contribution to the key rate comes from only the single-photon detection events. This eliminates Charlie having to distinguish between $c = 2$ photon outcomes, i.e., $|\phi_2^0\rangle, |\phi_2^1\rangle$ and $|\phi_2^2\rangle$ and requires him to only distinguish between the single-photon outcomes. Therefore, we can simplify our protocol to Fig. 5, where Charlie interferes the single photons coming from Alice and Bob at a 50:50 beamsplitter and uses two photon-number resolving detectors up to the two-photon level. After Charlie's measurement, Alice and Bob can estimate their joint state to bound Eve's information using the statistics of their matched and unmatched data of *X*, *Y*, and *Z* bases as mentioned in Calculation of the secret key rate. This protocol is conceptually similar to Protocol 1 and Protocol 2 of Curty et al.[63]. One of the main differences is that our single-photon protocol uses PNRDs at Charlie's station which helps Alice and Bob to disregard any measurement that is a two-photon click (i.e. Charlie receives no clicks at one detector and two clicks on the other), resulting in a lower bit-error rate. Our protocol also estimates Eve's information more tightly as Alice and Bob perform a full tomography of their joint state using the eigenvectors of the *X*, *Y*, and *Z* bases, whereas ref. [63] only uses

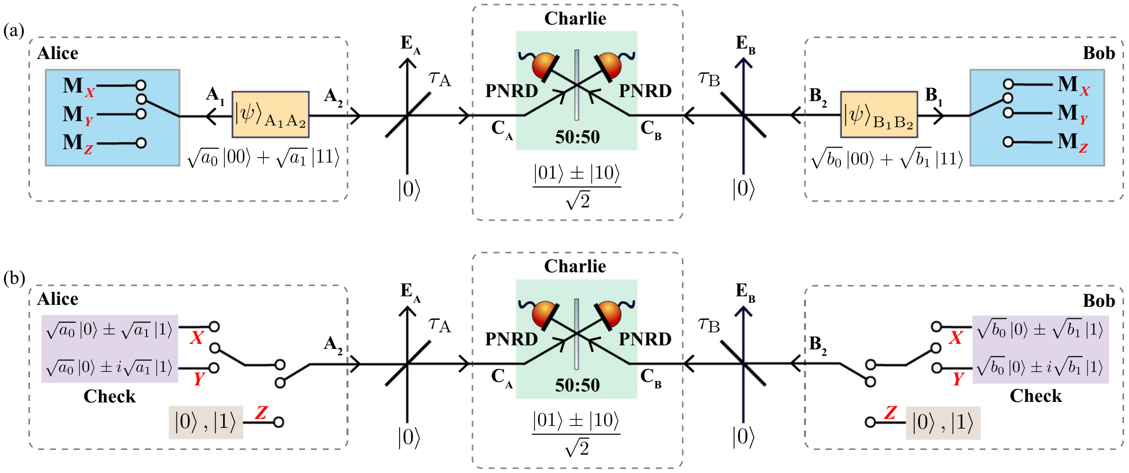

Fig. 5 Equivalent representations of the protocol with single photons. a Entanglement-based scheme where both Alice and Bob send the optimised states in the form of $\sqrt{a_0}|00\rangle + \sqrt{a_1}|11\rangle$ and $\sqrt{b_0}|00\rangle + \sqrt{b_1}|11\rangle$ to Charlie while keeping one arm of their states to themselves denoted as modes A$_1$ and B$_1$. They perform a measurement in the *X*, *Y*, and *Z* bases to compute the statistics of their matched and unmatched results. This measurement also projects the arm they sent to Charlie onto a single-mode state in the corresponding basis as shown in **b**. Charlie interferes modes A$_2$ and B$_2$ coming from Alice and Bob, respectively, at a 50:50 beamsplitter and performs single-photon detection with PNRDs. A successful outcome occurs when Charlie's left (10 event) or right detector (01 event) registers a single click only. Alice and Bob ignore the instances of 02, 20 and 11 photon events. **b** Prepare-and-measure scheme where Alice and Bob send single-mode states to Charlie where they encode the key information in the *Z* basis. They send the states $|0\rangle$ and $|1\rangle$ with probabilities a_0, b_0 and a_1, b_1, respectively. They randomly switch to *X* and *Y* bases to send check states to estimate Eve's information (refer to Alice and Bob's check states for security for the details of the check states). Charlie's measurement is the same as the one in the entanglement-based scheme shown in **a**.

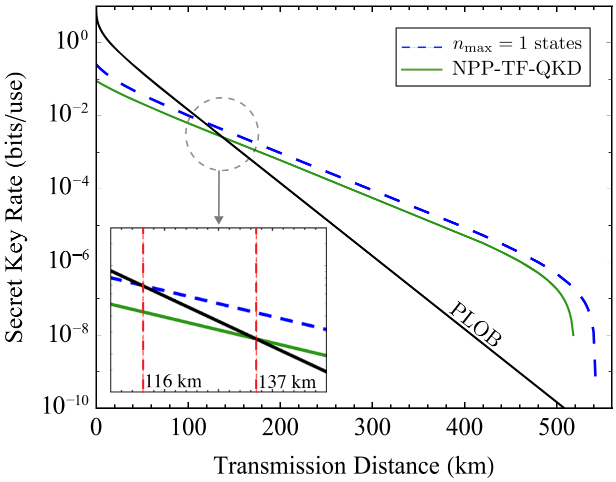

Fig. 6 Simulation results of our repeater protocol using single-photon states with experimental parameters. The blue dashed line shows our protocol using the single-photon states in the form of $\sqrt{a_0}|00\rangle + \sqrt{a_1}|11\rangle$ and $\sqrt{b_0}|00\rangle + \sqrt{b_1}|11\rangle$ with optimised coefficients and perfect single-photon sources. The solid green line and black lines are the NPP-TF-QKD protocol[60] with infinite decoy states and the PLOB bound, respectively. We assume a dark count rate of 5×10^{-8} with a detector efficiency of 0.85 for both protocols.

the measurement results of the X and Z bases. These two differences yield a higher key rate than the results of ref. [63].

Additionally, we consider the detrimental effects of the detector inefficiency and dark counts to the key rates. The single-photon states are optimised for a detector with an efficiency of 85% and a dark count rate of 5×10^{-8}, where the coefficients of the zero and single photons are shown in Table 5 and in Fig. 3b. In a lossless channel, the probability of sending a single-photon initially is half. However, as the channel becomes more lossy, it is likely that the single-photon will be lost during transmission. When Charlie receives no photons, this corresponds to a large bit-error rate reducing the key rates. This is compensated by reducing the probability of sending single-photons to decrease the bit-error rates and increase the key rates[64]. With realistic dark count rates and detector efficiencies, our protocol using perfect single-photon sources surpasses the PLOB bound at 116 km while the NPP-TF-QKD with infinite decoy states surpasses at 137 km as shown in Fig. 6. The NPP-TF-QKD protocol drops to zero beyond 518 km whereas our protocol drops to zero beyond 542 km showing a 24 km advancement in the transmission distance.

To account for a more practical scenario, we simulate our protocol with imperfect single-photon sources and compare it with the NPP-TF-QKD protocol[60] with a finite number of decoy states. When the single-photon sources used by Alice and Bob are heralded with imperfect detectors with a dark count rate of 5×10^{-8} and a detector efficiency of 0.85 for state preparation, the single-photon protocol achieves a total transmission distance of 480 km assuming 0.2 dB loss per km. When NPP-TF-QKD protocol[60] uses finite decoy states with two decoy modes with four intensities and the same dark count rates and detector efficiencies, the protocol achieves a total transmission distance of 470 km. Using a more realistic experimental set-up our protocol still performs better. However, as the heralding detectors used by Alice and Bob for the state preparation get more lossy, our protocol is likely to start performing worse than the TF-QKD protocols as these protocols use coherent states. Current superconducting nanowire single-photon detectors can achieve detector efficiencies up to 90% with dark count rates as low as 10^{-9} as demonstrated previously in ref. [40].

The improvements made to the total transmission distance in our protocol are a result of several factors. Even though both the single-photon and NPP-TF-QKD[60] protocols use optimised states, our protocol has more freedom over optimising the coefficients of the single-photon state while the TF-QKD protocols need to ensure that the intensities of the coherent states are still weak enough while optimising the key rates. This is also one of the key differences between our protocol and the Sending-or-Not-Sending TF-QKD (SNS-TF-QKD) protocol[65], where Alice and Bob send weak coherent states and no states with a probability of ϵ and $1 - \epsilon$, respectively. However, the probability of the single-photon detection is still determined by the intensity of the weak coherent states in the SNS-TF-QKD protocol whereas in this protocol, Alice and Bob send single-photon states with a probability of ϵ which determines the probability of detection at Charlie's detectors. Our protocol also has the ability to distinguish two-photon events occurring at a single detector at Charlie. For example, if Charlie receives no photons on one detector and two photons on the other, these events can be disregarded and do not contribute to bit-error rates. However, in TF-QKD protocols with single-photon detectors, this event would register as one click, causing an increase in the bit-error rate. Therefore, the use of PNRDs in Charlie's station improves the bit-error rates. Furthermore, our protocol can estimate Eve's information more accurately due to the use of the probabilities of the matched and unmatched bases. These are the main factors that distinguish our protocol from the existing MDI and TF-QKD protocols.

DISCUSSION

In this paper, we introduced an MDI protocol using higher dimensional states that surpasses the repeaterless bound without the need of quantum memories as it scales like the single-repeater bound. However, for large distances, the states required in this protocol reduce down to the single-photon level due to the losses in the channel. Based on this, we proposed an experimentally feasible implementation of this protocol just using single-photons and photon-number resolving detectors which performs better than the existing protocols such as NPP-TF-QKD protocol[59,60].

Furthermore, we investigated whether the single-repeater bound can be saturated with a simple protocol by using only single copies of the states sent by Alice and Bob and without collective measurements performed by Charlie. Our results show that unlike the repeaterless bound, this is probably not possible with single copies of the states and likely to require many copies of the states sent by Alice and Bob and collective measurements as previously shown by García-Patrón et al.[62] and a protocol proposed by Winnel et al.[66].

The results presented in this work refer to the asymptotic key rates, and the security of this protocol with finite-size effects needs to be considered in the future. In this protocol, there are no misalignment errors in the Z basis due to sending single-photons. However, the misalignment errors are likely to impact the statistics of the check states in the X and Y bases which can be investigated in future work. The feasibility of extending this protocol to a network of multiple users can also be studied.

Note that there are two challenges in our protocol which are the implementation of the states that Alice and Bob prepare and Charlie's coherent total photon number measurement. Ref. [51] managed to implement the states we require for this protocol up to the two-photon level. We would like to motivate the community with a possible extension of the work presented in ref. [51] to higher dimensions for state preparation and exploring ways to implement Charlie's measurement as they are likely to contribute to many areas in quantum information not only QKD, but also quantum metrology, entanglement swapping, entanglement distillation, optical quantum computing and error correction.

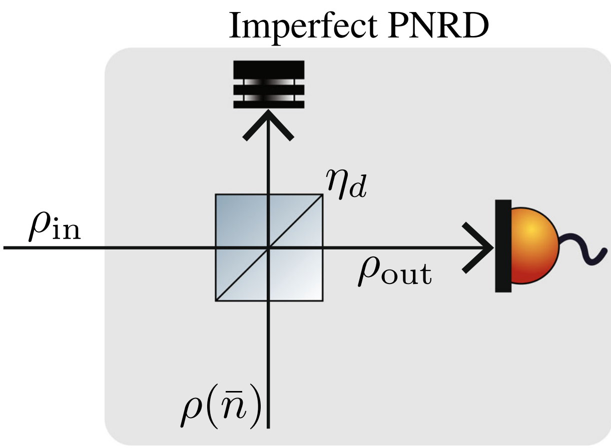

Fig. 7 Diagram of the method used to simulate the effect of dark counts in the PNRDs. ρ_{in} is the density matrix of the input state. The grey box represents a realistic photon number resolving detector with efficiency η_d and dark noise $(1-\eta_d)\bar{n}$.

Table 3. The coefficients of the optimised states with $n_{\max} = 1$ photon.

Distance (km)	a_0 b_0	a_1 b_1
0	0.5	0.5
0.5	0.5308	0.4692
1	0.5505	0.4495
2.5	0.5918	0.4082
5	0.6371	0.3629
10	0.6935	0.3065
15	0.7292	0.2708
20	0.7542	0.2458
30	0.7869	0.2131
50	0.8205	0.1795
100	0.8483	0.1517
200	0.8575	0.1425

Table 2. The coefficients of the optimised states with $n_{\max} = 7$ photons.

Distance (km)	a_0 b_0	a_1 b_1	a_2 b_2	a_3 b_3	a_4 b_4	a_5 b_5	a_6 b_6	a_7 b_7
0	0.0823	0.1162	0.1432	0.1582	0.1582	0.1432	0.1162	0.0823
0.5	0.1073	0.1359	0.1557	0.1603	0.1496	0.1267	0.0968	0.0676
1	0.1226	0.1472	0.1616	0.1600	0.1438	0.1174	0.0868	0.0605
2.5	0.1550	0.1705	0.1710	0.1567	0.1307	0.0994	0.0691	0.0477
5	0.1967	0.2012	0.1786	0.1483	0.1129	0.0787	0.0508	0.0329
10	0.4468	0.3137	0.1410	0.0601	0.0245	9.4433×10^{-3}	3.3895×10^{-3}	1.1308×10^{-3}
15	0.6654	0.2955	0.0366	2.4273×10^{-3}	1.1213×10^{-4}	3.9036×10^{-6}	9.8873×10^{-8}	0
20	0.7230	0.2608	0.0160	2.8606×10^{-4}	2.1895×10^{-6}	3.2584×10^{-9}	0	0
25	0.7548	0.2366	8.5496×10^{-3}	4.9545×10^{-5}	6.2159×10^{-8}	0	0	0
30	0.7760	0.2189	5.0283×10^{-3}	1.0464×10^{-5}	0	0	0	0
50	0.8176	0.1811	1.3468×10^{-3}	1.2642×10^{-7}	0	0	0	0
100	0.8477	0.1520	3.3582×10^{-4}	0	0	0	0	0
200	0.8571	0.1427	1.9467×10^{-4}	0	0	0	0	0

METHODS

Estimating Eve's information using quantum tomography with single-photon states

In this section, we show how Alice and Bob can estimate their joint state conditioned on Charlie's measurement outcome to bound Eve's information.

Alice and Bob measure their joint state in the X, Y, and Z bases in the entanglement-based scheme as introduced in Alice and Bob's check states for security to construct the statistics of their matched and unmatched results. From the probabilities measured in these bases, Alice and Bob can estimate their joint state. Writing their joint state as

$$\hat{\rho}_{\mathrm{AB}|c=1} = \frac{1}{4}\left(\mathbb{I}_4 + \vec{s}_a\cdot\vec{\sigma}_a + \vec{s}_b\cdot\vec{\sigma}_b + \sum_{j,k} r_{jk}(\sigma_j\otimes\sigma_k)\right), \tag{36}$$

where $\vec{s}_a\cdot\vec{\sigma}_a$ and $\vec{s}_b\cdot\vec{\sigma}_b$ describe Alice and Bob's reduced states calculated from their local measurements, while $r_{jk}(\sigma_j\otimes\sigma_k)$ gives the correlations between Alice and Bob determined from their measurements performed in the bases $j=\{X,Y,Z\}$ and $k=\{X,Y,Z\}$, where r_{jk} is the correlation coefficient and σ_j and σ_k are the standard Pauli matrices σ_X, σ_Y and σ_Z. The terms $\vec{s}_a\cdot\vec{\sigma}_a$ and $\vec{s}_b\cdot\vec{\sigma}_b$ can be expressed as

$$\vec{s}_a\cdot\vec{\sigma}_a = a_X(\sigma_X\otimes\mathbb{I}_2) + a_Y(\sigma_Y\otimes\mathbb{I}_2) + a_Z(\sigma_Z\otimes\mathbb{I}_2), \tag{37}$$

$$\vec{s}_b\cdot\vec{\sigma}_b = b_X(\mathbb{I}_2\otimes\sigma_X) + b_Y(\mathbb{I}_2\otimes\sigma_Y) + b_Z(\mathbb{I}_2\otimes\sigma_Z), \tag{38}$$

where $\{a_X, a_Y, a_Z\}$ and $\{b_X, b_Y, b_Z\}$ represent the coefficients given in Eq. (42) and (43) when Alice and Bob measure in the bases $j=\{X,Y,Z\}$.

When Alice and Bob measure their own qubits in any basis $j=\{X,Y,Z\}$, their measurement outcomes can be expressed as

$$\Pi_{\pm j} = |\pm j\rangle\langle\pm j|, \tag{39}$$

which can be calculated using the eigenvectors of the X, Y and Z bases as defined previously in Eq. (12), (13) and (14). The probability of their measurement then can be calculated from

$$P_a(\pm j) = \mathrm{Tr}\left[\left(\Pi_{\pm j}\otimes\mathbb{I}_2\right)\rho_{\mathrm{AB}|c=1}\left(\Pi_{\pm j}\otimes\mathbb{I}_2\right)^{\dagger}\right], \tag{40}$$

$$P_b(\pm j) = \mathrm{Tr}\left[\left(\mathbb{I}_2\otimes\Pi_{\pm j}\right)\rho_{\mathrm{AB}|c=1}\left(\mathbb{I}_2\otimes\Pi_{\pm j}\right)^{\dagger}\right], \tag{41}$$

where $\rho_{AB|c=1}$ is determined from Eq. (24).

Table 4. The optimised squeezing parameters (γ) of the states shown in Eq. (1) with $n_{max} = 7$ photons.

Distance (km)	Squeezing Parameter (γ)
0	0.84
0.5	0.83
1	0.83
2.5	0.82
5	0.81
10	0.71
15	0.52
20	0.44
25	0.40
30	0.37
40	0.33
50	0.30
100	0.26
200	0.25

The coefficients in Eq. (37) and (38) can be computed from Eq. (40) and (41) where

$$a_j = P_a(+j) - P_a(-j), \tag{42}$$

$$b_j = P_b(+j) - P_b(-j). \tag{43}$$

In order to determine the correlation coefficients r_{jk}, Alice and Bob construct a joint probability table of their measurements in all the bases where these probabilities are calculated from

$$P(a=\pm j, b=\pm k) = \mathrm{Tr}\Big[(\Pi_{\pm j}\otimes\Pi_{\pm k})\rho_{\mathrm{AB}|c=1}(\Pi_{\pm j}\otimes\Pi_{\pm k})^{\dagger}\Big]. \tag{44}$$

Using Eq. (44), the correlation coefficients become

$$\begin{aligned} r_{jk} \quad = \quad & P(a=+j, b=+k) + P(a=-j, b=-k) \\ & -P(a=+j, b=-k) - P(a=-j, b=+k). \end{aligned} \tag{45}$$

After Alice and Bob reconstruct their estimated joint matrix $\hat{\rho}_{\mathrm{AB}|c=1}$, they can estimate Eve's information using the Holevo bound as given in Eq. (30).

Classical protocol used to optimise the coefficients of the high dimensional states

This section describes how the states that Alice and Bob prepare are chosen. The coefficients of these states are determined based on the following classical protocol. We assume Eve taps off the signal sent by Alice and Bob, and measures the number of photons denoted as n_{e_a} and n_{e_b}. Then we maximise the average difference in mutual information

$$\max_{\{P(n_a),P(n_b)\}} \left[\sum_{c=0}^{2n_{\max}} P_c(n_c)\big(I_{AB|c} - I_{AE|c}\big)\right], \tag{46}$$

where $I_{AB|c}$ and $I_{AE|c}$ are Alice and Bob's mutual information and mutual information between Alice and Eve conditioned on Charlie's measurement outcome, respectively. $P(n_c)$ represents the probability of Charlie measuring n_c photons in total. Note that $P(n_a)$ and $P(n_b)$ are related to the optimised coefficients from Eq. (2) and (3) as they are the probability of sending n photons for the corresponding Fock-number state $|n\rangle$, also expressed as a_n and b_n throughout this paper.

In the classical protocol, Charlie measures the number of photons coming from Alice and Bob individually with two separate PNRDs. In Fock basis, both classical and quantum simulations yield the same probabilities for Charlie's measurement outcome. The probability of Charlie measuring n_{c_a} or n_{c_b} photons on Alice's and Bob's mode individually can be computed as

Table 5. The coefficients of the single-photon states when the detector dark count rate is 5×10^{-8} and with a detector efficiency of 0.85.

Distance	a_0	a_1
(km)	b_0	b_1
0.5	0.6697	0.3303
1	0.6751	0.3249
2.5	0.6896	0.3104
5	0.7100	0.2900
10	0.7405	0.2595
15	0.7624	0.2376
20	0.7790	0.2210
30	0.8020	0.1980
50	0.8275	0.1725
100	0.8499	0.1501
200	0.8576	0.1424
400	0.8588	0.1412
420	0.8591	0.1409
440	0.8598	0.1402
460	0.8609	0.1391
480	0.8630	0.1370
490	0.8647	0.1353
500	0.8669	0.1331
516	0.8721	0.1279
518	0.8730	0.1270
520	0.8739	0.1261
522	0.8749	0.1251
524	0.8760	0.1240
530	0.8796	0.1204
532	0.8810	0.1190
534	0.8825	0.1175
536	0.8841	0.1159
538	0.8859	0.1141
540	0.8878	0.1122
542	0.8898	0.1102

$$P_{c_a}(n_{c_a}) = \sum_{n_a=0}^{n_{\max}} \binom{n_a}{n_{c_a}} \tau_{\mathrm{A}}^{n_{c_a}} (1-\tau_{\mathrm{A}})^{n_a-n_{c_a}} P(n_a), \tag{47}$$

where $n_{\max}$ refers to the maximum number of photons Alice and Bob are sending individually. τ_{A} is the probability of a photon arriving at Charlie from Alice or Bob as a function of the fibre distance with $\tau_A = 10^{-0.02d}$. $(1-\tau_{\mathrm{A}})^{n_a-n_{c_a}}$ is the probability of losing $n_a - n_{c_a}$ photons to Eve. The probability of the collective photon number measurement performed by Charlie for a given number of photons n_c can be calculated using Eq. (47) as shown below

$$P_c(n_c) = \sum_{n_{c_a}=0}^{n_c} P_{c_a}(n_{c_a}) P_{c_b}(n_c - n_{c_a}), \tag{48}$$

where $n_c - n_{c_a}$ gives the number of photons measured on Bob's mode.

Alice and Bob's mutual information conditioned on Charlie's measurement outcome is obtained from the probability table between Alice and Bob which is as follows

$$P(n_a,n_b|n_c)=\binom{n_a+n_b}{n_c}\frac{\tau^{n_c}(1-\tau)^{n_a+n_b-n_c}P(n_a)P(n_b)}{P_c(n_c)}, \tag{49}$$

where n_a+n_b is equal to the total number of photons in the system and τ in the equation above corresponds to the transmission probability in one channel only. We evaluate Alice and Bob's mutual information conditioned on Charlie's measurement outcome from the same approach shown in Calculation of the secret key rate using $I_{AB|c}=H(A|c)+H(B|c)-H(AB|c)$ and Eq. (27), (28) and (29).

We quantify Eve's information conditioned on each photon measurement in a similar fashion to Alice and Bob's mutual information using $I_{E|c}=H(A|c)+H(E|c)-H(AE|c)$. Since Eve has access to both channels between Alice and Charlie and Charlie and Bob, we need to consider events where each party loses photons to Eve. We compute the probability table between Alice, Bob and the two modes of Eve conditioned on Charlie's outcome as follows

$$P(n_a,n_b,n_{e_a},n_{e_b}|n_c)=\frac{1}{P_c(n_c)}\binom{n_a}{n_{e_a}}\binom{n_b}{n_{e_b}} \tau^{n_a+n_b-(n_{e_a}+n_{e_b})}(1-\tau)^{n_{e_a}+n_{e_b}}P(n_a)P(n_b), \tag{50}$$

provided $n_a+n_b-(n_{e_a}+n_{e_b})=n_c$, where n_{e_a} and n_{e_b} are the photons lost to Eve by Alice and Bob, respectively, and $n_a+n_b-(n_{e_a}+n_{e_b})$ corresponds to the total number of photons measured by Charlie. Therefore, using the probability table between Alice, Bob and Eve, we can calculate the entropies below to compute Eve's information

$$H(E_{\mathrm{A}}E_{\mathrm{B}}|c)=-\sum_{n_{e_a}=0}^{n_{\max}}\sum_{n_{e_b}=0}^{n_{\max}} P(n_{e_a},n_{e_b}|c)\log_2 P(n_{e_a},n_{e_b}|c), \tag{51}$$

$$H(AE_{\mathrm{A}}E_{\mathrm{B}}|c)=-\sum_{n_a=0}^{n_{\max}}\sum_{n_{e_a}=0}^{n_{\max}}\sum_{n_{e_b}=0}^{n_{\max}} P(n_a,n_{e_a},n_{e_b}|c) \log_2 P(n_a,n_{e_a},n_{e_b}|c). \tag{52}$$

Modelling dark noise and detector efficiency in the entanglement swapping measurement and heralded single-photon sources

This section describes how to model the dark noise and detector efficiency at Charlie's photon number resolving detectors to achieve the results of Fig. 6 and the single-photon sources heralded by these detectors. The effects of dark noise is modelled by interacting the incoming state with a thermal state at a beamsplitter as shown in Fig. 7.

The efficiency of the single photon detection in this framework is the transmissivity of the beamsplitter (τ), i.e., $\eta_d=\tau$. The density matrix of the state to be detected can be written down as

$$\rho_{\mathrm{out}}=B(\eta_d)\big(\rho_{\mathrm{in}}\otimes\rho(\overline{n})\big)B(\eta_d)^{\dagger}, \tag{53}$$

where $\rho(\overline{n})$ is the density matrix of the thermal state. The beamsplitter transformation is shown in Eq. (19). The density matrix of the thermal state is given by

$$\rho(\overline{n})=\sum_{n=0}^{\infty}\frac{\overline{n}^n}{(1+\overline{n})^{n+1}}|n\rangle\langle n|, \tag{54}$$

where $\overline{n}=\mathrm{Tr}\,[\rho(\overline{n})a^{\dagger}a]$ is the mean photon number of the thermal state. Consequently, the dark count is given by $(1-\eta_d)\overline{n}$. For low dark counts, the summation in Eq. (54) can be truncated accordingly.

Coefficients of the optimised states

In this section, we present some of the coefficients of the optimised states with $n_{\max}=7$ and $n_{\max}=1$ photons used in Fig. 2a, b for each distance in Tables 2 and 3, correspondingly. These coefficients represent the probability of sending the corresponding Fock-number state. We give the values of the optimised squeezing parameters of the states given in Eq. (1) with $n_{\max}=7$ photons for each distance used in Fig. 2a in Table 4. In Table 5, we present the coefficients of the optimised single-photon states shown in Fig. 6.

DATA AVAILABILITY

The data that supports the findings of this study is available from the corresponding author upon reasonable request.

CODE AVAILABILITY

The codes that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 4 November 2022; Accepted: 10 March 2023;
Published online: 28 March 2023

REFERENCES

1. Ekert, A. & Renner, R. The ultimate physical limits of privacy. *Nature* **507**, 443–447 (2014).
2. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
3. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
4. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, 175 (IEEE, New York, 1984).
5. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
6. Ralph, T. C. Continuous variable quantum cryptography. *Phys. Rev. A* **61**, 010303 (1999).
7. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **61**, 022309 (2000).
8. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932 (1998).
9. Dür, W., Briegel, H.-J., Cirac, J. I. & Zoller, P. Quantum repeaters based on entanglement purification. *Phys. Rev. A* **59**, 169 (1999).
10. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001).
11. Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33–80 (2011).
12. Munro, W. J., Azuma, K., Tamaki, K. & Nemoto, K. Inside quantum repeaters. *IEEE J. Sel. Top. Quantum Electron.* **21**, 78–90 (2015).
13. Goebel, A. M. et al. Multistage entanglement swapping. *Phys. Rev. Lett.* **101**, 080403 (2008).
14. Kaltenbaek, R., Prevedel, R., Aspelmeyer, M. & Zeilinger, A. High-fidelity entanglement swapping with fully independent sources. *Phys. Rev. A* **79**, 040302 (2009).
15. Li, Z.-D. et al. Experimental quantum repeater without quantum memory. *Nat. Photonics* **13**, 644–648 (2019).
16. Zhao, Z., Yang, T., Chen, Y.-A., Zhang, A.-N. & Pan, J.-W. Experimental realization of entanglement concentration and a quantum repeater. *Phys. Rev. Lett.* **90**, 207901 (2003).
17. Vollbrecht, K. G. H., Muschik, C. A. & Cirac, J. I. Entanglement distillation by dissipation and continuous quantum repeaters. *Phys. Rev. Lett.* **107**, 120502 (2011).
18. Bratzik, S., Abruzzo, S., Kampermann, H. & Bruß, D. Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate. *Phys. Rev. A* **87**, 062335 (2013).
19. Simon, C. et al. Quantum repeaters with photon pair sources and multimode memories. *Phys. Rev. Lett.* **98**, 190503 (2007).
20. Dias, J., Winnel, M. S., Hosseinidehaj, N. & Ralph, T. C. Quantum repeater for continuous-variable entanglement distribution. *Phys. Rev. A* **102**, 052425 (2020).
21. Bussières, F. et al. Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory. *Nat. Photonics* **8**, 775–778 (2014).
22. Stuart, J. S., Hedges, M., Ahlefeldt, R. & Sellars, M. Initialization protocol for efficient quantum memories using resolved hyperfine structure. *Phys. Rev. Res.* **3**, L032054 (2021).

23. Cho, Y.-W. et al. Highly efficient optical quantum memory with long coherence time in cold atoms. *Optica* **3**, 100–107 (2016).
24. Hsiao, Y.-F. et al. Highly efficient coherent optical memory based on electromagnetically induced transparency. *Phys. Rev. Lett.* **120**, 183602 (2018).
25. Maring, N. et al. Storage of up-converted telecom photons in a doped crystal. *N. J. Phys.* **16**, 113021 (2014).
26. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 1–15 (2017).
27. Wilde, M. M., Tomamichel, M. & Berta, M. Converse bounds for private communication over quantum channels. *IEEE Trans. Inf. Theory* **63**, 1792–1817 (2017).
28. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 1–10 (2019).
29. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
30. Pirandola, S. et al. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **9**, 397–402 (2015).
31. Liu, Y. et al. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
32. Tang, Z. et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
33. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2014).
34. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
35. Xie, Y.-M. et al. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum* **3**, 020315 (2022).
36. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
37. Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.* **123**, 100506 (2019).
38. Chen, J.-P. et al. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).
39. Liu, H. et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Phys. Rev. Lett.* **126**, 250502 (2021).
40. Chen, J.-P. et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nat. Photonics* **15**, 570–575 (2021).
41. Chen, J.-P. et al. Quantum key distribution over 658 km fiber with distributed vibration sensing. *Phys. Rev. Lett.* **128**, 180502 (2022).
42. Wang, S. et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **16**, 154–161 (2022).
43. Wang, P., Wang, X. & Li, Y. Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers. *Phys. Rev. A* **99**, 042309 (2019).
44. Ma, H.-X. et al. Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation. *Phys. Rev. A* **99**, 022322 (2019).
45. Xu, F., Curty, M., Qi, B., Qian, L. & Lo, H.-K. Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nat. Photonics* **9**, 772–773 (2015).
46. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
47. Grosshans, F., Cerf, N. J., Wenger, J., Tualle-Brouri, R. & Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Preprint at https://arxiv.org/abs/quant-ph/0306141 (2003).
48. Asavanant, W. et al. Wave-function engineering via conditional quantum teleportation with a non-gaussian entanglement resource. *Phys. Rev. A* **103**, 043701 (2021).
49. Fiurášek, J., García-Patrón, R. & Cerf, N. J. Conditional generation of arbitrary single-mode quantum states of light by repeated photon subtractions. *Phys. Rev. A* **72**, 033822 (2005).
50. Clausen, J., Hansen, H., Knöll, L., Mlynek, J. & Welsch, D.-G. Conditional quantum-state engineering in repeated 2-photon down-conversion. *Appl. Phys. B* **72**, 43–50 (2001).
51. Bimbard, E., Jain, N., MacRae, A. & Lvovsky, A. Quantum-optical state engineering up to the two-photon level. *Nat. Photonics* **4**, 243–247 (2010).
52. Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018 (1998).
53. Liang, W.-Y. et al. Tomographic approach in three-orthogonal-basis quantum key distribution. *Commun. Theor. Phys.* **64**, 295 (2015).
54. Watanabe, S., Matsumoto, R. & Uyematsu, T. Tomography increases key rates of quantum-key-distribution protocols. *Phys. Rev. A* **78**, 042316 (2008).
55. Holevo, A. S. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory* **44**, 269–273 (1998).
56. Schwinger, J. Unitary operator bases. *Proc. Natl Acad. Sci.* **46**, 570–579 (1960).
57. Wootters, W. K. & Fields, B. D. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **191**, 363–381 (1989).
58. Horodecki, P., Rudnicki, Ł. & Życzkowski, K. Five open problems in quantum information theory. *PRX Quantum* **3**, 010101 (2022).
59. Cui, C. et al. Twin-field quantum key distribution without phase postselection. *Phys. Rev. Appl.* **11**, 034053 (2019).
60. Lu, F.-Y. et al. Improving the performance of twin-field quantum key distribution. *Phys. Rev. A* **100**, 022306 (2019).
61. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
62. García-Patrón, R., Pirandola, S., Lloyd, S. & Shapiro, J. H. Reverse coherent information. *Phys. Rev. Lett.* **102**, 210501 (2009).
63. Curty, M., Azuma, K. & Lo, H.-K. Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Inf.* **5**, 1–6 (2019).
64. Yin, H.-L. & Fu, Y. Measurement-device-independent twin-field quantum key distribution. *Sci. Rep.* **9**, 1–13 (2019).
65. Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **98**, 062323 (2018).
66. Winnel, M. S., Guanzon, J. J., Hosseinidehaj, N. & Ralph, T. C. Achieving the ultimate end-to-end rates of lossy quantum communication networks. *npj Quantum Inf.* **8**, 129 (2022).

ACKNOWLEDGEMENTS

We thank Matthew S. Winnel for his valuable discussion during this project. This research was funded by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Grant No. CE110001027). Y.-S.K. acknowledges support from the KIST institutional program (2E31021).

AUTHOR CONTRIBUTIONS

O.E. conceived the project. O.E. and S.A. developed the theory. O.E. performed the numerical analysis. O.E. wrote the manuscript. All authors contributed towards the theory, discussions of the results, and the manuscript. S.A. supervised the project.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Özlem Erkılıç or Syed M. Assad.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.