RESEARCH

Nonlinear improvement of measurement-device-independent quantum key distribution using multimode quantum memory

Yusuke Mizutani[1,2] · Tomoyuki Horikiri[1,2]

Abstract

This paper proposes a quantum key distribution (QKD) scheme for measurement-device-independent QKD (MDI-QKD) utilizing quantum memory (QM), which is based on two distinct functions of QM: on-demand storage and multimode storage. We demonstrate a nonlinear increase in the secure key rate due to the utilization of QM. In the protocol incorporating on-demand storage, it is acknowledged that the secure key rate is scaled by $R = O(\sqrt{\eta_{ch}})$ as η_{ch}, while as an alternative approach, we reveal that the improvement is $O(m_s^2)$, with m_s being the number of modes in frequency (spatial) multiplexing in the scheme incorporating multimode storage. We adopt an atomic frequency comb as a QM that incorporates the two functions and propose an architecture based on MDI-QKD to attain experimental feasibility. This scheme can be extended to quantum repeaters, and even for a single quantum-repeater node, there is a nonlinear enhancement and an experimental incentive to increase the number of modes.

1 Introduction

Quantum key distribution (QKD) can distribute secure key bit strings between two parties using information-theoretic security. In recent years, transmission distances have experimentally increased, with demonstrations distances exceeding 800 km [1].

However, theoretical security proofs rely on assumptions about the security of various devices, which may not accurately reflect the conditions of actual experiments. Fortunately, there are also implementation papers that bridge the gap between theory and experiment for device imperfections [2–4]. Among them, measurement-device-independent quantum key distribution (MDI-QKD) [5], which can be classified as a meet-in-the-middle (MM) architecture [6], is particularly noteworthy. This MM-type architecture has yielded numerous leading candidates for both QKDs and quantum repeaters and has achieved theoretical and experimental breakthroughs [7–12].

In the original MDI-QKD scheme, the key rate is strictly limited by the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound $R = -\log_2(1 - \eta_{ch}) \simeq \eta_{ch}/\ln 2 \simeq 1.44\eta_{ch}$ for $\eta_{ch} \ll 1$ [13], where η_{ch} represents the channel transmittance rate between the two users. To exceed the PLOB limit in QKD, twin-field QKD (TF-QKD) [14] and its variants, sending or not sending QKD [15], phase-matching QKD [16, 17], and mode-pairing QKD using asynchronous two-photon interference [7, 18] have been proposed. Additionally, memory-assisted MDI-QKD (MA-MDI-QKD) [19, 20] has been proposed and evaluated with quantum memory (QM) in various physical systems [21]. These architectures increase the key rate up to $O(\sqrt{\eta_{ch}})$. Moreover, MA-MDI-QKD can be extended as an element of a single quantum-repeater node via improvement of QMs. Additionally, when analyzing/comparing the performance of quantum repeaters, it is useful to benchmark with the key rate in the QKD protocol [22, 23].

Beginning with the previously reported concept [24] of quantum repeaters, which are essential for long-distance quantum communication, various applications can be realized through the entanglement distribution, including

✉ Yusuke Mizutani
qvuaalnlteuym@gmail.com

Tomoyuki Horikiri
horikiri-tomoyuki-bh@ynu.ac.jp

1 Yokohama National University, 79-5 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan

2 LQUOM, Inc., 79-5 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan

QKD, distributed quantum computation [25], and world clocks [26]. Additionally, the proof-of-concept for a quantum internet—a communication network utilizing information-theoretic security—is being developed. It is crucial to develop quantum communication protocols that are ready for connection to the physical layer and higher layers of the network [27, 28].

The Duan–Lukin–Cirac–Zoller (DLCZ) protocol realizes a practical experimental implementation of quantum repeaters [29] and has been implemented in several physical systems, such as quantum dots [30], trapped ions [31], and protocols utilizing nitrogen-vacancy centers [11], as well as entanglement distribution using atomic frequency comb (AFC) QM in recent years [9, 10]. However, in the realistic protocols realized in the aforementioned experiments, multiplexing is necessary to achieve practical rates (on the order of Hz or higher) [32–34]. Therefore, our focus has been on the multimode storage of QM, and we propose a scheme that introduces new possibilities.

We adopt AFC as a QM [35] comprising two functions: multimode storage and on-demand storage. These two functions have a distinct impact on the key rate. To this end, we propose an experimentally implementable protocol, which is a one-element MDI type protocol, to analyze the impact of multimode QM on the key rate.

There are two primary methods for achieving a key rate of $O(\sqrt{\eta_{\mathrm{ch}}})$. The first is to utilize a one-photon interference scheme, as exemplified by proposals, such as TF-QKD [14] and mode-pairing schemes that alleviate phase-locking issues in one-photon interference [7, 18]. The second is a scheme akin to MA-MDI-QKD, in which QM allows Bell state measurements (BSMs) to be performed even if photons arrive asynchronously at the central interference system. As a practical proposal, protocols utilizing on-demand storage can achieve $O(\sqrt{\eta_{\mathrm{ch}}})$ within a certain range of distances, contingent upon the decoherence time T_2 of the QM [19, 36].

Herein, we present an alternative approach, whereby we demonstrate that the key rate can be increased by $O(m_{\mathrm{s}}^2)$, with m_{s} representing the number of modes, through the incorporation of frequency multiplexing and frequency shifting in the middle BSM. Even after normalization by the number of modes, it is possible to benefit from frequency multiplexing.

The remainder of this paper is organized as follows. Section 2 describes the structure of the protocol incorporating the functions of QM and proposes a feasible setup for the mechanism. In Sect. 3, in addition to the on-demand storage of QM, the multimode storage of the frequency and spatial modes is incorporated into the calculation and analyzed as the key rate of the one-element MDI-QKD protocol. Finally, Sect. 4 summarizes the study and discusses future extensions to quantum-repeater networks.

2 System description

In this section, we first provide an overview of the fundamental principles of the on-demand/multimode protocol, which is predicated on the functionality of QM. Subsequently, we comprehensively explain the protocol.

2.1 Protocol description

We present a system of protocols that incorporates the functions of QM, specifically on-demand and multimode storage. The first protocol incorporates a QM with on-demand storage, as depicted in Fig. 1a, and the second protocol incorporates a QM with frequency (spatial) multimode storage, as depicted in Fig. 1b.

2.1.1 On-demand QM protocol

First, we describe a protocol that incorporates a QM with on-demand storage, as illustrated in Fig. 1a. The QM on Bob's (Alice's) side is notified of whether a photon has been successfully absorbed by the QM on Alice's (Bob's) side, allowing the determination of whether the photonic quantum state has been stored in the QM on Alice's (Bob's) side. If the presence of the photon is heralded by the successful loading of both QMs, the middle BSM is executed as usual. However, if the loading of the QM on Alice's (Bob's) side is unsuccessful, the QM on Bob's (Alice's) side stores the photon information and awaits the next successful loading of the QM on Alice's (Bob's) side.

2.1.2 Multimode QM protocol

We next describe the protocol incorporating a QM with frequency-multiplexing storage, as illustrated in Fig. 1b. The protocol utilizes a QM with the storage of frequency multiplexing, as demonstrated in the AFC [35]. The frequency mode of the photon successfully absorbed on Alice's (Bob's) side is retrieved from the QM and shifted to a fixed frequency mode with efficiency η_{f}. The frequency mode utilized in the middle BSM is consistently fixed [37]. This protocol does not require on-demand storage and can be implemented with fixed-time storage.

2.2 Protocol setup

Here, we detail the implementation of the scheme depicted in Fig. 1 utilizing QM.

In Fig. 1, the three functions required of the QM are the function of heralding, which nondestructively transmits the arrival of a photon; the on-demand storage; and
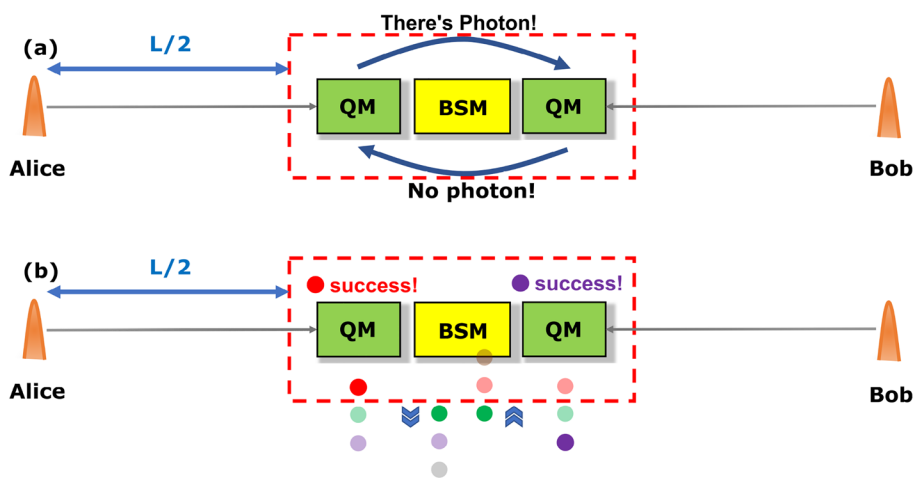
Fig. 1 Schematic of the system of protocols incorporating QM functions, specifically on-demand and multimode storage. **a** On-demand protocol: We assume the presence of a QM with on-demand storage. This function allows the QM on Alice's (Bob's) side to determine whether a photon has been successfully absorbed and obtain its stored information. **b** Multimode protocol: A QM with frequency multiplexing is employed. The frequency mode of the photon that is successfully absorbed on Alice's (Bob's) side is read from the QM and shifted to a fixed frequency mode (depicted as green in the figure). The frequency mode used in the central BSM is consistently fixed

the multimode storage. Specifically, in Fig. 1a, the QM requires the on-demand storage and the function of heralding, and in Fig. 1b, the QM requires the multimode storage and the function of heralding. However, there is currently no practical QM that possesses all three of these functions. Nevertheless, AFC QM has two of these functions: on-demand and multimode storage. Therefore, when utilizing

AFC QM, which is suitable for multimode storage, it is necessary to incorporate the function of heralding separately in actual experiments. Figure 2 illustrates a scheme with heralding. Figure 2a depicts the basic MA-MDI-QKD scheme [19], and we extend the QM in this protocol by replacing it with an AFC.
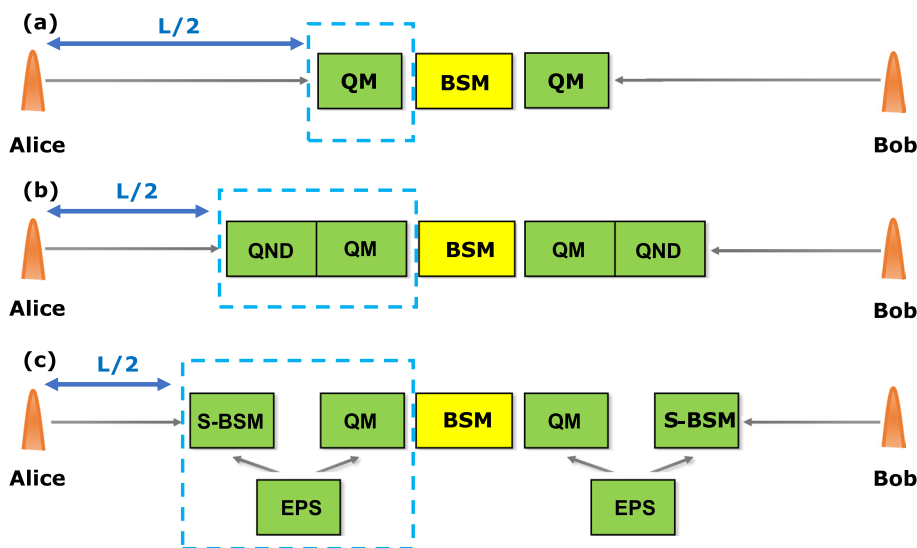

Fig. 2 In **a**, the original MA-MDI-QKD protocol proposed in [19] is presented. In **b**, a heralding scheme utilizing quantum non-demolition (QND) measurement is presented. The QND nondestructively heralds the presence of a photon, indicating successful absorption into the QM. Once both QMs have completed their readings, the stored state of the QMs is retrieved as photons, and a BSM is executed in the middle. In **c**, a heralding scheme utilizing BSM is presented. In each

round, entangled photons from the entangled photon source (EPS) are sent to the QM and a side-BSM (S-BSM), where the QM stores the photon information and the S-BSM performs a BSM with photons from Alice (Bob). If it is successful, the heralding of absorption of the photon stored in the QM is successful, the quantum state is taken as a photon from both QMs, and a BSM is performed in the middle
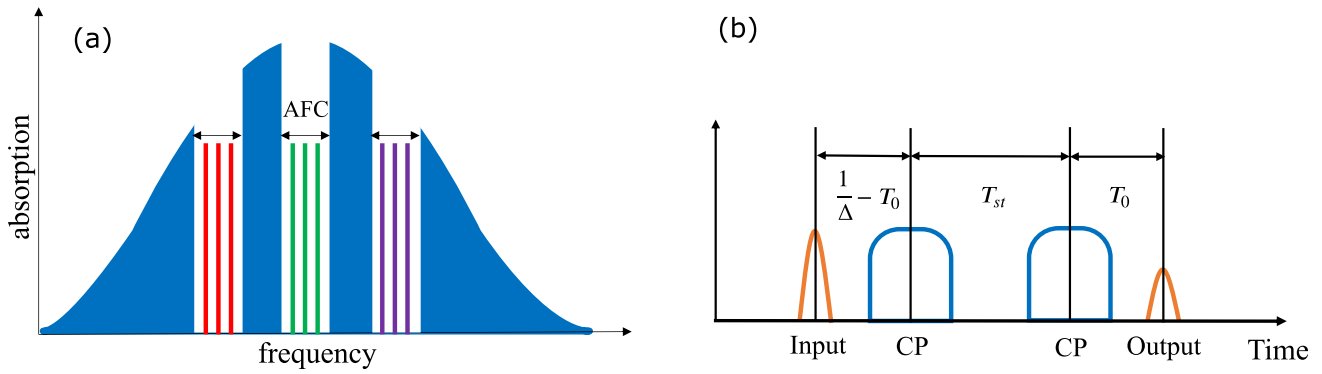
Fig. 3 Process of writing and reading on-demand and multimode AFC QM is illustrated in Fig. 1. **a** Structure of an AFC with frequency-multiplexing storage, where photons are absorbed. **b** Write and read processes are depicted on the time axis. The interval between the peaks of the comb, which is referred to as Δ, depends on the structure of the AFC. A pulse is absorbed by the AFC as an input mode, followed by the application of a control pulse (CP). After a period of T_{st}, a second CP is applied, and photons are regenerated as the output mode after a total of $1/\Delta + T_{st}$

Figure 3 illustrates the physical system that allows the on-demand and multimode storage of the AFC QM. As depicted in Fig. 3a, multiple AFCs can be created through inhomogeneous broadening, allowing absorption of photons of different modes. Additionally, as illustrated in Fig. 3b, the storage time T_{st} can be set to an arbitrary value through the timing of CP irradiation. However, the AFC alone cannot herald the arrival of a photon sent by Alice (Bob) without destroying the quantum information.

There are three conventional methods for heralding the arrival of a photon. The first is heralding with the QM alone, as shown in Fig. 2a. This method has been demonstrated using spin–photon interfaces, e.g., silicon–vacancy centers [38]. The second method is heralding with QND, as depicted in Fig. 2b. This approach incorporates QND [39] to realize the function of heralding external to the QM when the QM does not possess this function. However, QND in AFC has only been achieved at the classical light level—not at the single-photon level. As an alternative, heralding can be realized indirectly by incorporating S-BSM and EPS in Fig. 2c. This method allows the determination of whether a photon has been absorbed into the QM based on the outcome of the BSM, making it useful for ensemble-based QMs with multimode storage, as it is difficult to achieve the function of heralding with such QMs.

2.2.1 Device description

We now provide an overview of each component, assuming the absence of malicious third-party actors.

Photon source

In the proposed scheme, Alice and Bob's single-photon source performs the calculation with a weak coherent pulse (WCP) and an optimized average photon number μ, ν. The utilization of EPSs has been actively studied in recent years.

A high-fidelity degenerate EPS with a telecommunication wavelength was reported in a cavity two-photon configuration [40], as well as a non-degenerate EPS, where the signal and idler are the QM wavelength and telecommunication wavelength, respectively [10]. In practical examples of protocols using EPSs, linear improvements in the key rate have been achieved through multiplexing with existing EPS devices [41]. While the EPSs considered in this study do not take into account the probability of two-photon generation in each mode, simulation results indicate that for $p_2 > 0$, a constant p_2 range in a frequency-multiplexed quantum-repeater scheme has little effect on the key rate [33]. Alternative options have been proposed to replace quantum dot-based photon sources with low p_2 values, such as the approach presented in reference [42] and the setup outlined in reference [21], which eliminates the EPS.

Quantum memory

Our scheme requires a QM with on-demand storage and multimode storage. With regard to the function of on-demand storage, if photon absorption in Bob's (Alice's) QM is unsuccessful, Alice (Bob) must store the quantum state in the QM until Bob (Alice) achieves a successful absorption. However, during this period, the QM becomes susceptible to dephasing due to T_2; the initial state of the QM is ρ, and the state of the QM after dephasing for a period of time t can be modeled using the Completely Positive and Trace Preserving map, as reported in [43].

$$\varepsilon(\rho) = [1 - \lambda_{\mathrm{dp}}(t)]\rho + \lambda_{\mathrm{dp}}(t)Z\rho Z. \tag{1}$$

Here,

$$\lambda_{\mathrm{dp}}(t) = \frac{1 - e^{-\frac{t}{T_2}}}{2}, \tag{2}$$

where Z represents the Pauli Z operator. AFC QM, which is based on rare-earth doped crystals, is the first viable candidate for QM with multimode storage. In recent times, AFC QM has progressed to the experimental stage of multimode storage, and in the case of temporal multiplexing, 51-μs has been achieved with $^{151}Eu^{3+}:Y_2SiO_5$ at 100 modes in fixed-time storage, and 0.541-ms at 50 modes in on-demand storage has been realized. In frequency multiplexing, $Pr^{3+}:Y_2SiO_5$ can achieve 100 modes in fixed-time storage [44, 45]. Furthermore, as an experimental example, entanglement distribution using the time-multimode storage has been reported [10].

Frequency shifter

In the scenario where photons of varying frequency modes are to be regenerated, frequency shifting can be accomplished using an electro-optic modulator to perform a BSM. The technology required for this process is serrodyne frequency shifting, which was demonstrated to have a conversion efficiency of 80% for a frequency shift of approximately 1 GHz in experiments utilizing an AFC [37].

Bell state measurement

In this study, there is a middle BSM and an S-BSM employed for heralding when a photon is successfully absorbed by the QM. The success probability for the middle BSM can be calculated using Y_{11}, as described in Appendix 1:

$$P^{MBSM} = Y_{11}(\eta_A, \eta_B), \tag{3}$$

where η_A and η_B represent the probabilities of photons reaching the middle BSM on Alice's and Bob's sides, respectively. Similarly, the S-BSM used for heralding, which is depicted in Fig. 2c, can be viewed as an asymmetric MDI-QKD system:

$$P_K^{SBSM} = Y_{11}(\eta_K, \eta_{ent}\eta_d) \quad (K = A, B). \tag{4}$$

With regard to multiplexing, a BSM utilizing spatial modes [46] and a BSM utilizing temporal modes [47] have been proposed. Additionally, a BSM setup that exceeds 50% [48] has been proposed.

3 Key rate analysis

In this section, we calculate the key rate for the proposed scheme illustrated in Fig. 2c. In QKD experiments, it is commonly assumed that normal operation proceeds without interference from eavesdroppers and is only affected by system imperfections. Under these conditions, in the setting of an infinite key, the key rate in Fig. 2 setting is bound by the following:

$$R = Y_{11}^{QM}[1 - h(e_X) - fh(e_Z)], \tag{5}$$

where e_X and e_Z represent the qubit error rates (QBERs) between Alice and Bob in the X and Z bases, respectively, and Y_{11}^{QM} represents the rate at which raw key bits are generated. Additionally, $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the Shannon's binary entropy function. In this study, inefficiency is analyzed with $f = 0$, and other parameters are presented in Table 1.

3.1 On-demand AFC protocol

As the protocol depicted in Fig. 1a necessitates the utilization of QM with the function of heralding, we realized an on-demand protocol utilizing AFC QM by integrating S-BSM, as shown in Fig. 2c. The MDI-QKD scheme with on-demand QM has been analyzed in previous studies. In [20], decoherence due to time evolution of the QM was not considered, and in [19], decoherence was considered. As depicted in Fig. 4, the key rate of the protocol scales with $O(\sqrt{\eta_{ch}})$. This scaling appears to be valid over a limited distance range up to 400 km. The reason is that the effects of QM decoherence become increasingly dominant as the distance between the QM and Alice or Bob increases, ultimately causing the key rate to fall below the PLOB limit. The average storage time required for the QM can be calculated using the equation $T_{st} = E\{N_A - N_B\}\tau = \frac{2(1-\eta)\tau}{\eta(2-\eta)} \approx \frac{\tau}{\eta}$ $(\eta \ll 1)$ [19], where N_A and N_B are the probability variables for successful loading of the QM on Alice's and Bob's sides, respectively. Here, τ represents the repetition period. η represents the loading efficiency of the QM, with η_A and η_B corresponding to Alice's and Bob's sides, respectively, and

Table 1 Parameters associated with the QKD protocol discussed in Sect. 3

| Parameter	Symbol
Rate at which the QMs and BSM are successful	Y_{11}^{QM}
Probability of a successful BSM	Y_{11}
QBER in basis $S = X, Z$	e_S
QM reading efficiency	η_r
Frequency-shifting efficiency	η_f
Detector efficiency	η_d
Channel-loss efficiency	η_{ch}
Entangling efficiency	η_{ent}
Probability of successfully loading a QM $K = A, B$	η_K^{mm}
Optical coherence time	T_2
Number of modes in spectral/spatial multimode	m_s
Number of modes in temporal multimode	m_t
Attenuation length	L_{att}
Dark count rate per pulse	p_{dc}
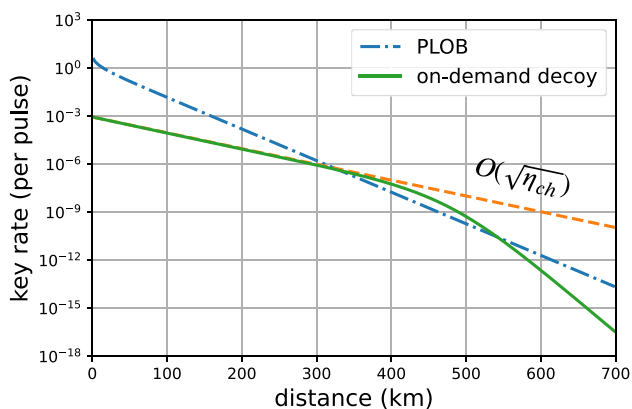
Fig. 4 Comparison of the key rate of the on-demand AFC protocol with the PLOB bound (R=1.44η_{ch}). The parameters were set as follows: $L_{\text{att}} = 22, \eta_{\text{d}} = 0.93, \eta_{\text{ent}} = 0.5, p_{\text{dc}} = 10^{-8}, T_2 = 300 \times 10^{-6}$

$\eta = \eta_A = \eta_B$. Instead of calculation based on the average storage time, an alternative approach is to optimize the number of modes in temporal multiplexing m_{t} according to distance, resulting in the scaling of $R = O(\sqrt{\eta_{\text{ch}}})$, as detailed in Appendix 2.

3.2 Multimode AFC protocol

We realized the multimode protocol utilizing the multimode storage of the AFC QM by integrating S-BSM, as shown in Fig. 2c. When QM is utilized with multimode storage via frequency or spatial multiplexing, Y_{11}^{QM} is expressed as follows:

$$Y_{11}^{\text{QM}} = \mu\nu e^{-\mu-\nu} Y_{11}(\eta_A^{\text{mm}}, \eta_B^{\text{mm}}), \qquad (6)$$

where μ, ν represent the average photon numbers of the WCPs on Alice's and Bob's sides, respectively; $\eta_K^{\text{mm}}(K = A, B)$ represents the success probability of S-BSM in multiplexing, which is given below; and m_{s} represents the number of modes in frequency or spatial multiplexing.

$$\eta_K^{\text{mm}} = 1 - (1 - Y_{11}(\eta_{\text{ch}}(L_K)\eta_{\text{d}}, \eta_{\text{ent}}\eta_{\text{d}}))^{m_{\text{s}}} \quad (K = A, B) \qquad (7)$$

The incorporation of multiplexing in the S-BSM is considered, where $\eta_{\text{d}}, \eta_{\text{ent}}$ represent the detector efficiency and entanglement source efficiency, respectively. The mathematical framework for the analysis of spatial multiplexing is equivalent to that of frequency multiplexing. Despite the experimental differences between frequency and spatial multiplexing, 36 modes of transmission have been achieved using a single fiber [49], with ongoing efforts to develop spatial multiplexing in QMs [50]. As shown in Fig. 5, the plateau region became larger with an increase in the number of modes m_{s}. The key rate of the multimode
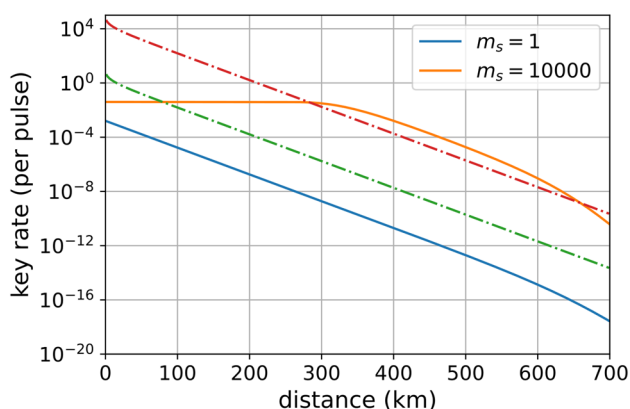

Fig. 5 Key rate of the multimode AFC protocol is compared with the PLOB bound (R = 1.44$m_{\text{s}}\eta_{\text{ch}}$). Simulations were performed with $m_{\text{s}} = 1, 10000$. The parameters used in the simulations were $L_{\text{att}} = 22$ km, $\eta_{\text{d}} = 0.93, \eta_{\text{ent}} = 0.5, p_{\text{dc}} = 10^{-8}$, and $\eta_{\text{f}} = 0.8$. The PLOB bound is depicted as green (lower dashdot) and red (upper dashdot) for $m_{\text{s}} = 1$ and 1000, respectively

AFC protocol, i.e., the original MDI-QKD protocol, for $m_{\text{s}} = 1$ was significantly below the PLOB bound; however, for $m_{\text{s}} = 10,000$, the key rate of the multimode AFC protocol surpassed the PLOB bound. As shown in Fig. 5, the key rate increased by $O(m_{\text{s}}^2)$ at long distances as the number of modes in frequency (spatial) multiplexing m_{s} increased. This analysis indicates that the improvement persists even after normalization by the number of modes, providing motivation for experimental efforts to increase the number of modes in frequency (spatial) multiplexing, even in the absence of a quantum repeater with multiple links ($N \geq 2$).
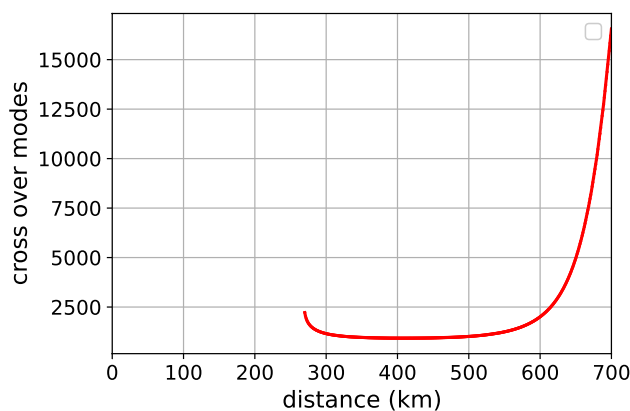

Fig. 6 Number of modes at which the key rate of the multimode protocol exceeds the PLOB limit at each distance (crossover modes). Until the distance reaches approximately 270 km, it is infeasible to surpass the PLOB limit. However, beyond this range, it becomes possible to exceed the PLOB limit utilizing approximately 1000 modes, within the practical distance range

In the scheme depicted in Fig. 1b, it should be noted that the QM necessitates only fixed-time storage, rather than on-demand storage.

Figure 6 illustrates that the number of crossover modes in the multimode protocol is approximately 1000 within the range of 300–500 km. As depicted in Fig. 7, the key rate is also equivalent to the PLOB bound before the number of modes reaches 1000, but in $Pr^{3+} : Y_2SiO_5$, the number of modes that can be stored by frequency multiplexing is currently limited to approximately 100. To exceed this number, the utilization of either spatial or temporal multiplexing is necessary. Theoretically, 100-mode multiplexing is possible through the incorporation of spatial multiplexing [45], increasing the total number of modes to 10^4. In this context, the middle BSM is executed in a single mode. Consequently, despite the increase in η_K^{mm} due to multiplexing, the maximum attainable number of bits in a single round remains limited to 1. Thus, with an increase in the parameter m_s, the key rate eventually reaches a plateau, as depicted in Figs. 5 and 7.

4 Conclusion

We examined the MA-MDI-QKD configuration utilizing a multimode QM. We analyzed the impact on the key rate. The results indicated that the protocol utilizing the QM with on-demand storage yields a key rate of $O(\sqrt{\eta_{ch}})$, which depends on T_2. In comparison, the protocol utilizing multimode storage achieves a key rate increase of $O(m_s^2)$ through frequency
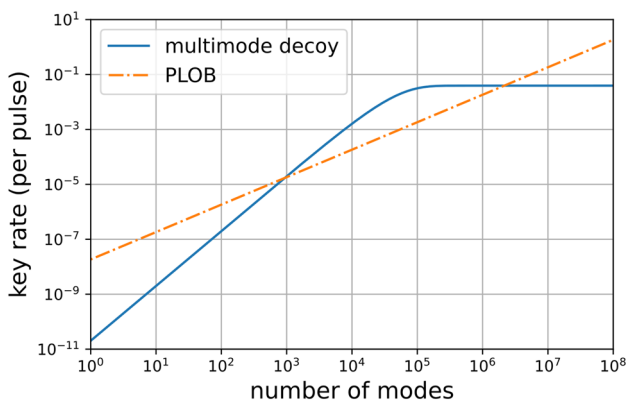

Fig. 7 At a distance of 400 km, the key rate of the multimode AFC protocol depends on the number of modes. Specifically, the rate increases by $O(m_s^2)$ as the number of modes m_s increases. Furthermore, when 1000 modes or more are utilized, the multimode AFC protocol surpasses the PLOB bound

(spatial) multiplexing. Furthermore, with current technology, frequency multiplexing alone yields $m_s \sim 100$ in the AFC, but when frequency multiplexing and spatial multiplexing are combined, it is possible to exceed the PLOB bound. This outcome indicates that multiplexing has considerable potential for single-element QKD protocols and is effective for single quantum-repeater node protocols. In future, advancements in QMs can extend these configurations to scalable quantum repeaters and contribute to rate enhancement through multimode quantum repeaters or QKDs. Additionally, the theoretical and experimental work on these protocols brings us closer to the ultimate goal of the quantum internet, as it serves as a stepping stone between point-to-point QKD and full quantum-repeater networks.

Appendix A: Calculation of key rates dependent on T_2

If QM with on-demand storage is utilized, Y_{11}^{QM} can be described as follows [19, 36]:

$$Y_{11}^{QM} = \frac{Y_{11}(\eta_{early}, \eta_{late})}{N_L(\eta_{\mu A}, \eta_{\nu B})} \cdot \frac{\eta_{1A}\eta_{1B}}{\eta_{\mu A}\eta_{\nu B}} \mu\nu e^{-\mu-\nu}, \quad (8)$$

where $\eta_{1K}, \eta_{\mu(\nu)K}$ $(K = A, B)$ represent the readout efficiency from QM in single-photon states and average photon number $\mu(\nu)$, respectively. Moreover, Y_{11} is given as follows [51]:

$$Y_{11}(\eta_A, \eta_B) = (1 - p_{dc})^2 \times \left[\frac{\eta_A\eta_B}{2} + (2\eta_A + 2\eta_B - 3\eta_A\eta_B)\right.$$
$$\left. p_{dc} + 4(1 - \eta_A)(1 - \eta_B)p_{dc}^2\right], \quad (9)$$

where N_L represents the average number of attempts to load both QMs. The average number of attempts to load both memories, i.e., $N_L(\eta_A, \eta_B)$, is approximated by $N_L = \frac{3-2\eta_A}{\eta_A(2-\eta_A)} \approx \frac{3}{2\eta_A}$ when $\eta_A = \eta_B \ll 1$ in the no-multimode scenario [32]. Furthermore, η_{early} and η_{late} represent the loading efficiencies of the QMs for photons arriving early and late, respectively [19]:

$$\eta_K^{QM} = \begin{cases} \eta_{late} = \eta_{r0}\eta_d, & \text{if QM K is late,} \\ \eta_{early} = \eta_r(t)\eta_d, & \text{if QM K is early,} \end{cases} \quad (10)$$

where t represents the storage time of the QM in the event that it is loaded early, which is given as $(t = |N_A - N_B|\tau)$. The calculation of the expected value for η_{early} is as follows:

$$\overline{\eta_{early}}$$
$$= \eta_d\eta_{r0}E\{\exp(-|N_A - N_B|\tau/T_2)\}$$
$$= \frac{\eta_d\eta_{r0}\eta_A\eta_B}{\eta_A + \eta_B - \eta_A\eta_B} \times \left[\frac{1}{1 - e^{-\frac{\tau}{T_2}}(1 - \eta_A)} + \frac{1}{1 - e^{-\frac{\tau}{T_2}}(1 - \eta_B)} - 1\right].$$
$$(11)$$

Appendix B: Calculation of key rates dependent on temporal multiplexing m_t

The multimode AFC protocol (frequency multiplexing/ spatial multiplexing scheme) in Sect. 3 was considered as temporal multiplexing m_t with $m_t = 1$, but it can be extended to the case of temporal multiplexing ($m_t > 1$). A schematic of the QM when temporal multiplexing is incorporated is depicted in Fig. 8. It is necessary to store $m_s m_t$ photons across m_t slots and match them accordingly.

$$Y_{11}^{QM} = \frac{\mu\nu e^{-\mu-\nu} Y_{11}(\eta_A^{mm}, \eta_B^{mm})}{m_t} \quad (12)$$

Here, Y_{11} represents the success rate of the BSM, as described in Appendix 1. The success probability η_K^{mm} of the frequency-multiplexed and time-multiplexed S-BSM is given as follows:

$$\eta_K^{mm} = 1 - (1 - Y_{11}(\eta_{ch}(L_K)\eta_d, \eta_{ent}\eta_d))^{m_s m_t} \quad (K = A, B). \quad (13)$$

Here, in contrast to frequency/spatial multiplexing, temporal multiplexing results in a linear increase in $O(m_t)$, as m_t appears in the denominator of the rate Eq. 6, reducing the number of middle BSM attempts per unit time.

As illustrated in Fig. 9, as m_t increases, the plateau region expands; however, the overall rate decreases linearly with an increase in the time required to execute BSM, which is $m_t\tau$. Additionally, optimizing the number of temporal modes m_t with consideration of the distance results in rate scaling of $O(\sqrt{\eta_{ch}})$, as observed in the envelope.

Fig. 9 Protocol with temporal multiplexing. Simulations were performed with $m_s = 1$ in frequency multiplexing and $m_t = 1, 10^2, 10^4, 10^6$ for the number of modes in temporal multiplexing

References

1. S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, Nat. Photonics **16**(2), 154–161 (2022)
2. W. Zhang, T. Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C.C.-W. Lim, Nature **607**(7920), 687–691 (2022)
3. D. Nadlinger, P. Drmota, B. Nichol, G. Araneda, D. Main, R. Srinivas, D. Lucas, C. Ballance, K. Ivanov, E.-Z. Tan, Nature **607**(7920), 682–686 (2022)
4. W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, J.-W. Pan, Phys. Rev. Lett. **129**(5), 050502 (2022)
5. H.-K. Lo, M. Curty, B. Qi, Phys. Rev. Lett. **108**(13), 130503 (2012)
6. C. Jones, D. Kim, M.T. Rakher, P.G. Kwiat, T.D. Ladd, New J. Phys. **18**(8), 083015 (2016)
7. P. Zeng, H. Zhou, W. Wu, X. Ma, Nat. Commun. **13**(1), 1–11 (2022)
8. N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J.A. Slater, M. George, R. Ricken, M.P. Hedges, D. Oblak, C. Simon, W. Sohler, Phys. Rev. Lett. **113**(5), 053603 (2014)
9. X. Liu, J. Hu, Z.-F. Li, X. Li, P.-Y. Li, P.-J. Liang, Z.-Q. Zhou, C.-F. Li, G.-C. Guo, Nature **594**(7861), 41–45 (2021)
10. D. Lago-Rivera, S. Grandi, J.V. Rakonjac, A. Seri, H. Riedmatten, Nature **594**(7861), 37–40 (2021)
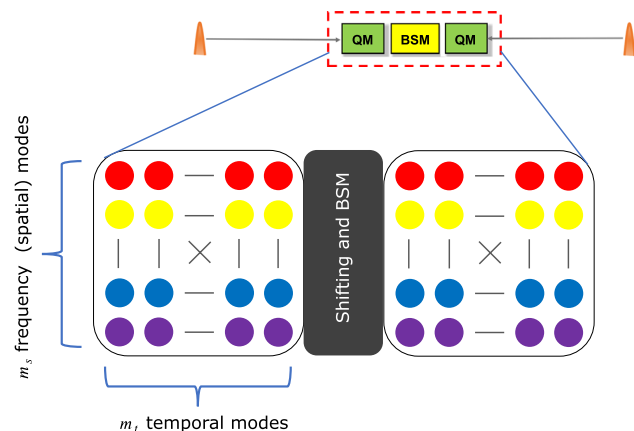

Fig. 8 Schematic of a QM used in protocols that incorporate both frequency (spatial) multiplexing and time multiplexing. Here, each QM stores $m_s m_t$ photons and performs a frequency/time bin shift in the center for BSMs
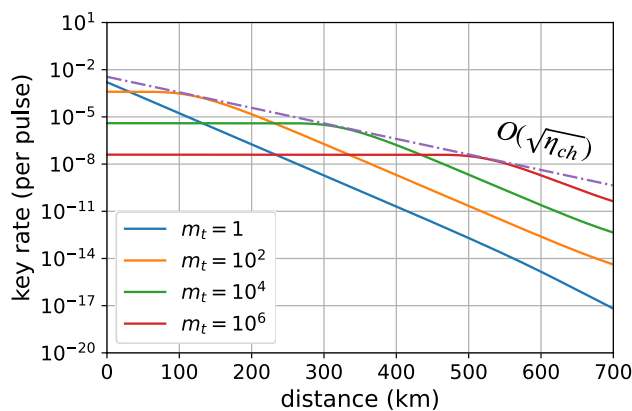
11. M. Pompili, S.L. Hermans, S. Baier, H.K. Beukers, P.C. Humphreys, R.N. Schouten, R.F. Vermeulen, M.J. Tiggelman, L. Santos Martins, B. Dirkse, Science **372**(6539), 259–264 (2021)

12. G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo, Optica **9**(7), 812–823 (2022)

13. S. Pirandola, R. Laurenza, C. Ottaviani, L. Banchi, Nat. Commun. **8**(1), 1–15 (2017)

14. M. Lucamarini, Z.L. Yuan, J.F. Dynes, A.J. Shields, Nature **557**(7705), 400–403 (2018)

15. X.-B. Wang, Z.-W. Yu, X.-L. Hu, Phys. Rev. A **98**(6), 062323 (2018)

16. X. Ma, P. Zeng, H. Zhou, Phys. Rev. X **8**(3), 031043 (2018)

17. P. Zeng, W. Wu, X. Ma, Phys. Rev. Appl. **13**(6), 064013 (2020)

18. Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, Z.-B. Chen, PRX Quantum **3**(2), 020315 (2022)

19. C. Panayi, M. Razavi, X. Ma, N. Lütkenhaus, New J. Phys. **16**(4), 043005 (2014)

20. S. Abruzzo, H. Kampermann, D. Bruß, Phys. Rev. A **89**(1), 012301 (2014)

21. N.L. Piparo, N. Sinclair, M. Razavi, Quantum Sci. Technol. **3**(1), 014009 (2017)

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

23. F. Schmidt, P. Loock, Phys. Rev. A **102**(4), 042614 (2020)

24. H.-J. Briegel, W. Dür, J.I. Cirac, P. Zoller, Phys. Rev. Lett. **81**(26), 5932 (1998)

25. H. Buhrman, H. Röhrig, In: International Symposium on Mathematical Foundations of Computer Science, pp. 1–20. Springer (2003)

26. P. Komar, E.M. Kessler, M. Bishof, L. Jiang, A.S. Sørensen, J. Ye, M.D. Lukin, Nat. Phys. **10**(8), 582–587 (2014)

27. S. Wehner, D. Elkouss, R. Hanson, Science **362**(6412), 9288 (2018)

28. A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpędek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. Oliveira Filho, et al. In: Proceedings of the ACM Special Interest Group on Data Communication, pp. 159–173 (2019)

29. L.-M. Duan, M.D. Lukin, J.I. Cirac, P. Zoller, Nature **414**(6862), 413–418 (2001)

30. R. Stockill, M. Stanley, L. Huthmacher, E. Clarke, M. Hugues, A. Miller, C. Matthiesen, C. Le Gall, M. Atatüre, Phys. Rev. Lett. **119**(1), 010503 (2017)

31. L. Stephenson, D. Nadlinger, B. Nichol, S. An, P. Drmota, T. Ballance, K. Thirumalai, J. Goodwin, D. Lucas, C. Ballance, Phys. Rev. Lett. **124**(11), 110501 (2020)

32. O. Collins, S. Jenkins, A. Kuzmich, T. Kennedy, Phys. Rev. Lett. **98**(6), 060502 (2007)

33. S. Guha, H. Krovi, C.A. Fuchs, Z. Dutton, J.A. Slater, C. Simon, W. Tittel, Phys. Rev. A **92**(2), 022357 (2015)

34. H. Krovi, S. Guha, Z. Dutton, J.A. Slater, C. Simon, W. Tittel, Appl. Phys. B **122**(3), 1–8 (2016)

35. M. Afzelius, C. Simon, H. De Riedmatten, N. Gisin, Phys. Rev. A **79**(5), 052329 (2009)

36. D. Luong, L. Jiang, J. Kim, N. Lütkenhaus, Appl. Phys. B **122**(4), 1–10 (2016)

37. E. Saglamyurek, N. Sinclair, J.A. Slater, K. Heshami, D. Oblak, W. Tittel, New J. Phys. **16**(6), 065019 (2014)

38. M.K. Bhaskar, R. Riedinger, B. Machielse, D.S. Levonian, C.T. Nguyen, E.N. Knall, H. Park, D. Englund, M. Lončar, D.D. Sukachev, Nature **580**(7801), 60–64 (2020)

39. N. Sinclair, K. Heshami, C. Deshmukh, D. Oblak, C. Simon, W. Tittel, Nat. Commun. **7**(1), 1–6 (2016)

40. K. Niizeki, D. Yoshida, K. Ito, I. Nakamura, N. Takei, K. Okamura, M.-Y. Zheng, X.-P. Xie, T. Horikiri, Commun. Phys. **3**(1), 1–7 (2020)

41. J. Pseiner, L. Achatz, L. Bulla, M. Bohmann, R. Ursin, Quantum Sci. Technol. **6**(3), 035013 (2021)

42. M. Müller, S. Bounouar, K.D. Jöns, M. Glässl, P. Michler, Nat. Photonics **8**(3), 224–228 (2014)

43. M. Razavi, M. Piani, N. Lütkenhaus, Phys. Rev. A **80**(3), 032301 (2009)

44. P. Jobez, N. Timoney, C. Laplane, J. Etesse, A. Ferrier, P. Goldner, N. Gisin, M. Afzelius, Phys. Rev. A **93**(3), 032327 (2016)

45. A. Ortu, J.V. Rakonjac, A. Holzäpfel, A. Seri, S. Grandi, M. Mazzera, H. Riedmatten, M. Afzelius, Quantum Sci. Technol. **7**(3), 035024 (2022)

46. O. Pietx-Casas, G.C.D. Amaral, T. Chakraborty, R. Berrevoets, T. Middelburg, J.A. Slater, W. Tittel, (2021) arXiv preprint arXiv: 2111.13610

47. R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V.B. Verma, M.D. Shaw, J. Stern, J.A. Slater, D. Oblak, Opt. Express **22**(20), 24497–24506 (2014)

48. W.P. Grice, Phys. Rev. A **84**(4), 042331 (2011)

49. T. Mizuno, T. Kobayashi, H. Takara, A. Sano, H. Kawakami, T. Nakagawa, Y. Miyamoto, Y. Abe, T. Goh, M. Oguma, et al. In: Optical Fiber Communication Conference, pp. 5–2. Optica Publishing Group (2014)

50. M. Gündoğan, P.M. Ledingham, A. Almasi, M. Cristiani, H. De Riedmatten, Phys. Rev. Lett. **108**(19), 190504 (2012)

51. X. Ma, M. Razavi, Phys. Rev. A **86**(6), 062319 (2012)