Practical Decoy-State Memory-Assisted Measurement-Device-Independent Quantum Key Distribution

Mingshuo Sun,[1,2,3,†] Chun-Hui Zhang,[1,2,3,†] Hua-Jian Ding,[1,2,3] Xing-Yu Zhou,[1,2,3] Jian Li,[1,2,3] and Qin Wang[1,2,3,*]

[1] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

[2] *"Broadband Wireless Communication and Sensor Network Technology" Key Lab of Ministry of Education, NUPT, Nanjing 210003, China*

[3] *"Telecommunication and Networks" National Engineering Research Center, NUPT, Nanjing 210003, China*

(Received 10 February 2023; revised 18 April 2023; accepted 13 June 2023; published 11 August 2023)

The measurement-device-independent quantum key distribution (MDI QKD) can resist all attacks against measurement devices. However, its practical performance is still limited due to very low coincidence counting rates in Bell-state measurements. In this paper, we propose a practical memory-assisted MDI QKD protocol by cooperating the heralded single-photon sources and an all-optical quantum memory. By making use of the heralding characteristic of heralded single-photon sources, the earlier photon will be stored in the Sagnac optical quantum memory, and then released till another photon's arrival. Moreover, by combining with the decoy-state method, the present work exhibits significantly improved key rates and transmission distances compared with all existing MDI QKD protocols without using quantum memories. Therefore, this work can provide valuable references for practical implementation of long-distance quantum communications.

DOI: 10.1103/PhysRevApplied.20.024029

I. INTRODUCTION

Quantum key distribution (QKD) [1], in principle, can provide secure and effective communication between two legitimate users (Alice and Bob), even under the existence of a malicious eavesdropper, Eve. Unfortunately, the theory of QKD sometimes has conflicts with its actual performance, since some assumptions have been made in its security proofs, which are not always valid. Indeed, by exploiting security loopholes in practical realizations, especially imperfections in the measurement part, different attacks have been successfully launched against commercial QKD systems [2–4], highlighting the vulnerabilities in practical QKD systems.

Compared to the prepare-and-measure QKD protocols, the MDI QKD [5–7] shows excellent performance in the immunity to attacks directed on the measurement part [8,9]. And many MDI QKD schemes and experiments have been proposed and demonstrated [10–12]. In the MDI QKD system, two legitimate users, Alice and Bob, send their signals to the middle station, Charlie, where a Bell-state measurement (BSM) will be performed. Based on the measurement results, Alice and Bob can infer certain correlations between their transmitted bits. Moreover, its security can be equivalent to a time-reversal BBM92 protocol [13], which means, Charlie does not need to be trusted, nor does the BSM need to be perfect. Besides, the twin-field QKD also has the MDI character and can overcome the rate-distance limit [14], significantly improving the performance of QKD [15–17].

However, present MDI QKD protocols are suffering from worse influence from the channel loss, resulting in quite poor key rates and transmission distances. Because it needs photons from both Alice and Bob to survive before performing the BSM. In order to improve the performance of MDI QKD, the idea of quantum memory (QM) assisted MDI QKD protocols were proposed [18–22]. However, most of them did not take photon-number-splitting (PNS)[23] attacks into account, and did some assumptions. Here in this work, we implement practical decoy-state methods [24–26] into QM-assisted MDI QKD protocols, and compare their performance with existing MDI QKD protocols.

This paper is arranged as following, we first describe the theory of decoy-state QM-assisted MDI QKD protocols in Sec. II, and then carry out numerical simulations in Sec. III, finally, conclusions are given in Sec. IV.

*qinw@njupt.edu.cn

†The authors contributed equally to this work.

II. THEORY

The schematic of the experimental setup in our protocol is shown in Fig. 1, there are three participants in our scheme, i.e., Alice, Bob, and Charlie, where Alice and Bob are two legitimate users, and Charlie represents the untrusted third party. Alice and Bob independently generates the heralded-single-photon sources (HSPSs) and send to Charlie; In Charlie's side, it mainly consists of one QM module and one BSM module.

In either Alice or Bob's side, a laser is implemented to pump a nonlinear crystal (NC) to generate correlated photon pairs through the spontaneous parametric down-conversion (SPDC) process, and an intensity modulator (IM_1) is utilized to modulate the pump light into three different intensities in the decoy-state method. The correlated photon pairs are then separated by a dichroic mirror, where the idler photons (I) are sent into a local detector (D_0), and the signal photons (S) are collected into the encoding module to encode different states. The photon-number distribution of HSPS [27] can obey different types according to different experimental conditions [28]. Here for simplicity, we take the thermal distribution as an example, i.e., $P_\mu^n = \mu^n/((1+\mu)^{n+1})$, here μ represents the average photon number per pulse, n denotes the number of photons.

In our scheme, we apply the time-bin encoder [29–31] by using a Faraday Michelson interferometer (FMI). When passing through the short arm (s) and the long arm (g) of FMI, the photon pulse can be modulated into the states $|\pm\rangle = 1/\sqrt{2}(|s\rangle \pm |g\rangle)$, by adjusting the phase modulator (PM), constituting the X basis. Then we can generate the Z-basis states, $|s\rangle$ and $|g\rangle$, by the IM_2. When two pulses from Alice and Bob come into the measurement part, a BSM will be carried out, and here we record only the projection results on $|\varphi^\pm\rangle$ state as the successful event. Here, $|\varphi^\pm\rangle := 1/\sqrt{2}(|sg\rangle \pm |gs\rangle)$. The $|\varphi^-\rangle$ denotes a click in either $W^s_{D_1}W^g_{D_2}$ or $W^s_{D_2}W^g_{D_1}$ and the $|\varphi^+\rangle$ denotes a click in either $W^s_{D_1}W^g_{D_1}$ or $W^s_{D_2}W^g_{D_2}$. Here, $W^t_{D_i}$ represents a click at window t of the detector D_i in the BSM, where $t \in (s,g)$ and refers to the detection window.

The QM module consists of one Pockels cell (PC) module [32], one polarization beam splitter (PBS), and two reflecting mirrors. Usually, the PC has two modes including "on" and "off." When the mode is "off," no voltage is applied to the PC and the polarization of the pulse remains the same. In contrast, when the mode is "on," a high voltage is applied to the PC and the polarization of the pulse will switch between horizontal (H) and vertical (V). Before the arrival of any pulses, the mode of the PC is kept as "off." When the early pulse with (H) arrives in the QM, which is heralded by the clicking of local detector, the mode of the PC will immediately switch to "on." Once the polarization state of the arriving pulse switches to V, the PC returns to mode "off." Accordingly, the pulse will be stored in the loop due to the continuous reflecting of the PBS. As long as the later pulse comes, heralded by the corresponding local detector, the mode of the PC will switch to "on" again, the polarization state of the early pulse will be returned back to H. Consequently, both pulses are released from the QM module. Particularly, if the later pulse still comes from the same user, we discard the former pulse and keep the latest pulse to reduce the loss in QM and improve the successful probability. Finally, the successful probability of projection measurements can be written as [18]

$$P_{\text{suc}}^{k_A,k_B} = P_l(k_A|1)P_l(k_B|1) + \sum_{j=2}^{M}[P_l(k_A|j)P_e(k_B|j) + P_l(k_B|j)P_e(k_A|j) + P_l(k_A|j)P_l(k_B|j)], \quad (1)$$

where M is the maximum storage round of the QM. $P_l(k|j)$ is the probability that an HSPS initially heralds and generates a k-photon state at the j th time slot, given by

$$P_l(k|j) = [1 - P_h(j-1)]\sum_{k'=k}^{\infty} P_\mu^{k'} P_d(k') P_t(k|k', j, j), \quad (2)$$

while $P_e(k|j)$ is the probability of heralding at least one time within the j–1 time slots and then emitting a k-photon

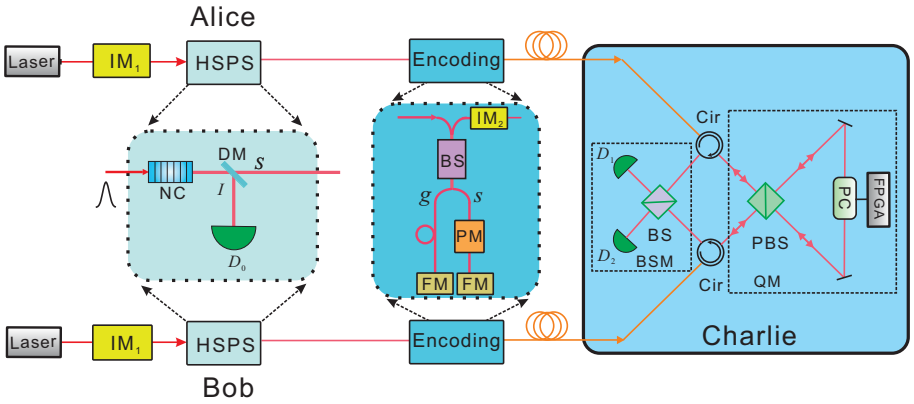

FIG. 1. Schematic of the measurement setup. IM, intensity modulator; NC, nonlinear crystal; DM, dichroic mirror; PM, phase modulator; FM, Faraday mirror; Cir, circulator; D_1 and D_2 are two single-photon detectors; PC, Pockels cell; BS, beam splitter; PBS, polarization beam splitter.

state at the j th time slot, given by

$$P_e(k|j) = \sum_{j'=1}^{j-1}\left[1 - P_h(j - j' - 1)\right] \times \sum_{k'=1}^{\infty}[P_\mu^{k'} P_d(k') P_t(k|k', j, j')(1 - P_h(1)) + P_h(j-1)\sum_{k'=1}^{\infty} P_\mu^{k'} P_d(k') P_t(k|k', j, j)], \quad (3)$$

where $P_h(j)$ is the probability that one HSPS heralds at least one single-photon pulse within the j th time slots, shown as

$$P_h(j) = 1 - [1 - P_h(1)]^j, \quad (4)$$

where $P_h(1) = \sum_1^\infty P_d(k) P_\mu^k$. $P_d(k)$ is the probability that a detector clicks when the source emits a k-photon state, which is expressed as

$$P_d(k) = \sum_{m=1}^{k} \eta_d^m (1-\eta_d)^{k-m} C_k^m \left(\frac{1}{D}\right)^{m-1}. \quad (5)$$

And $P_t(k'|k, j, j')$ is the probability that k' photons can pass through the channel and the QMs to the j th time slot. It can be written as

$$P_t(k'|k, j, j') = (T_C T_{\mathrm{QM}}^{j-j'+1})^{k'} (1 - T_C T_{\mathrm{QM}}^{j-j'+1})^{k-k'} C_k^{k'}, \quad (6)$$

where η_d is the detection efficiency. T_{QM} and T_C are the transmission efficiency of the QM and the optical channel [18], respectively. D is the number of detectors in a trigger-photon mode. Considering the QM itself will introduce polarization errors, we should quantify the change of a state before and after the QM. Supposing imputing a perfectly prepared state $|H\rangle$, the misalignment probability of the optical system is defined as e_d. The state outgoing the QM can be written as

$$\rho_{\mathrm{out}} = (1 - e_{\mathrm{BG}})[(1 - e_d)|H\rangle\langle H| + e_d|V\rangle\langle V|] + e_{\mathrm{BG}}\frac{|H\rangle\langle H| + |V\rangle\langle V|}{2}, \quad (7)$$

where e_{BG} refers to the probability that our QM has been loaded by a background (unpolarized) photon conditioned on a successful releasing. Therefore, the storage fidelity F can be written as [33]

$$F_Z = (1 - e_{\mathrm{BG}})(1 - e_d) + \frac{e_{\mathrm{BG}}}{2}, \quad (8)$$

$$F_X = \frac{1 + (1 - e_{\mathrm{BG}})(1 - 2e_d)}{2}. \quad (9)$$

Considering the practical value of e_{BG} is usually quite small, it can be ignored [19,34], then we can simplify it as

$$F = F_Z = F_X \approx 1 - e_d. \quad (10)$$

Once both QMs are loaded and the pulses are successfully interfered, the rest of our scheme is similar to that of the original MDI QKD in terms of key-rate analysis [34]. Charlie performs BSM on the pulse pairs released from the QMs.

In Z basis, a correct event corresponds to the situation that Alice and Bob send out different time-bin state ($|sg\rangle$ or $|gs\rangle$), and a wrong event corresponds to the situation that Alice and Bob send out the same time-bin state ($|ss\rangle$ or $|gg\rangle$). While in X basis, the correct event corresponds to the following situations:

1. Alice and Bob send out the same time-bin state $(++, --)$, and Charlie detects $\varphi^+(W_{D_1}^s W_{D_1}^g, W_{D_2}^s W_{D_2}^g)$;
2. Alice and Bob send out different time-bin states $(+-, -+)$, and Charlie detects $\varphi^-(W_{D_1}^s W_{D_2}^g, W_{D_2}^s W_{D_1}^g)$.

The rest correspond to the wrong events.

Based on the above, we can calculate the conditional probabilities for various correct and wrong events in $K \in \{Z, X\}$ basis when Alice (Bob) sends $k_A(k_B)$-photon pulses with intensity $x(y)$ [35] as

$$q_R^{K,x,y}(k_A, k_B) = P_{\mathrm{suc}}^{k_A,k_B} P^{k_A,k_B} P_R^{K,k_A,k_B}, \quad (11)$$

$$q_C^{K,x,y}(k_A, k_B) = P_{\mathrm{suc}}^{k_A,k_B} P^{k_A,k_B} P_C^{K,k_A,k_B}, \quad (12)$$

where P^{k_A,k_B} represents the probability of clicks in the detection part and $P_C^{K,k_A,k_B}(P_R^{K,k_A,k_B})$ denotes the conditional probabilities corresponding to the correct (wrong) events in K basis.

By referring to Ref. [26], we can model the gains and the error rates with the three-intensity decoy-state MDI QKD method. Assuming that Alice (Bob) has three identical intensities (μ, ν, o) in their source preparation, we could estimate the lower bound of the yield for the single-photon pulse pairs and their upper bound of the phase-flip error rate as

$$Y_{11}^K \geqslant \underline{Y_{11}^K} = \frac{P_\mu^1 P_\mu^2 (\underline{Q_{\mu,\mu}^K} - \overline{\hat{Q}_0^{K,\mu}}) - P_\nu^1 P_\nu^2 (\overline{Q_{\nu,\nu}^K} - \underline{\hat{Q}_0^{K,\nu}})}{P_\nu^1 P_\mu^1 (P_\nu^1 P_\mu^2 - P_\mu^1 P_\nu^2)}, \quad (13)$$

$$e_{11}^K \leqslant \overline{e_{11}^K} = \frac{\overline{\mathrm{QE}_{\nu,\nu}^K} - \underline{\hat{\mathrm{QE}}_0^{K,\nu}}}{P_\nu^1 P_\nu^1 \underline{Y_{11}^K}}, \quad (14)$$

where $\hat{Q}_0^{K,x}$ and $\hat{\mathrm{QE}}_0^{K,x}$ each represents the gain and the quantum bit errors of events including vacuum states, respectively. Here, $\overline{\hat{Q}_0^{K,x}} = \overline{Q_{x,o}^K} + \overline{Q_{o,x}^K} - \underline{Q_{o,o}^K}$, $\underline{\hat{Q}_0^{K,x}} = \underline{Q_{x,o}^K} + \underline{Q_{o,x}^K} - \overline{Q_{o,o}^K}$ and $\underline{\hat{\mathrm{QE}}_0^{K,x}} = \underline{\mathrm{QE}_{x,o}^K} + \underline{\mathrm{QE}_{o,x}^K} - \overline{\mathrm{QE}_{o,o}^K}$. Due to the implementation of the QM, the overall gain and the quantum bit errors of quantum states under K basis when Alice sends the intensity x and Bob sends the intensity y can be written as

$$Q_{x,y}^K = \sum_{k_1,k_2} [q_R^{K,x,y}(k_A, k_B) + q_C^{K,x,y}(k_A, k_B)], \tag{15}$$

$$\mathrm{QE}_{x,y}^K = Q_{x,y}^K E_{x,y}^K, \tag{16}$$

where $E_{x,y}^K$ refers to the modified error rate in K basis, and it should be written as

$$E_{x,y}^K = e_d(1 - 2\widetilde{E}_{x,y}^K) + \widetilde{E}_{x,y}^K, \tag{17}$$

$\widetilde{E}_{x,y}^K$ denotes the bit-flip rate and is calculated as

$$\widetilde{E}_{x,y}^K = \frac{\sum_{k_1,k_2} q_R^{K,x,y}(k_A, k_B)}{\sum_{k_1,k_2} [q_R^{K,x,y}(k_A, k_B) + q_C^{K,x,y}(k_A, k_B)]}. \tag{18}$$

Considering the finite-size effect [36], we apply the Chernoff bound method [37] on parameter estimations. The overline and the underline each corresponds to the upper bound and the lower bound of the variables. For a variable χ, $\underline{\chi} = \chi - \Delta_1 \le \chi \le \chi + \Delta_2 = \overline{\chi}$. More details about Δ_1 and Δ_2 can be seen in Ref. [37]. With the above, we could calculate the final key rate as [5,35]

$$R = (P_\mu^1)^2 \underline{Y_{11}^Z}(1 - H(\overline{e_{11}^X})) - f\underline{Q_{\mu,\mu}^Z} H(E_{\mu,\mu}^Z), \tag{19}$$

where f is the factor of the error correction efficiency, $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

III. NUMERICAL SIMULATION

In the following, we carry out corresponding numerical simulations with reasonable system parameters [18], as listed in Table I.

To show the validity of our present work, we perform comparisons between our present memory-assisted MDI QKD and other existing QKD protocols, including the BB84 QKD using either WCS or HSPS [24,25], and the MDI QKD using either WCS [26] or HSPS [35] under the asymptotic case, i.e., without considering the finite-size effect, as shown in Fig. 2. In the simulation, we set reasonable parameters for the QM utilized in our scheme, i.e., the storage round is $M = 40$; the transmission efficiency of the QM is $T_{\mathrm{QM}} = 98\,\%$; the state fidelity is $F = 98.5\,\%$. We can see from Fig. 2 that, at short transmission distance (< 220 km), the BB84 QKD presents the highest key rate; while at longer transmission distance (> 220 km), our present scheme exhibits outstanding performance in either key rates or transmission distances. For example, its transmission distance is more than 100 km longer than the MDI QKD with HSPS, 170 km longer than the MDI QKD with WCS, and 300 km longer than the BB84 QKD. Besides, its secure key rate is more than one order of magnitude higher than all other schemes at the transmission distance of 400 km.

TABLE I. List of experimental parameters used in numerical simulations. Here, Pd and Pd_t denote the dark count rate of detectors in measurement and local part; e_d is misalignment probability of the optical system; η_d and η_t is the efficiency of detectors in measurement and local part; f is the error correction inefficiency; ξ is the failure probability of statistical fluctuation analysis; α is the fiber loss coefficient (dB/km).

e_d	Pd	Pd_t	η_d
0.015	10^{-7}	10^{-7}	0.6
η_t	ξ	f	α(dB/km)
0.75	10^{-10}	1.16	0.2

We further carry out investigation on the performance influence of the system parameters on the memory-assisted MDI QKD, e.g., the storage round (M) is changing from 5 to 40, or the transmission efficiency of the QM (T_{QM}) is ranging from 80 % to 98 % , as shown in Figs. 3(a) and 3(b), individually. We can see from Fig. 3(a) that, the key rate and the transmission distance will increase with the increasing of the storage round, while the trend slows down when M is larger than 20, and almost can be neglected when M is over 30. From Fig. 3(b), we find that, the key rate and the transmission distance will decline

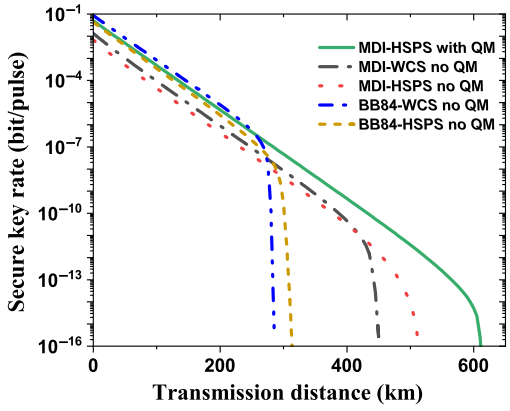

FIG. 2. Comparisons of the key rate between our present scheme and other existing QKD methods, including MDI QKD and BB84 QKD protocols. Here, $T_{QM} = 98\,\%$, $F = 98.5\,\%$ and $M = 40$.

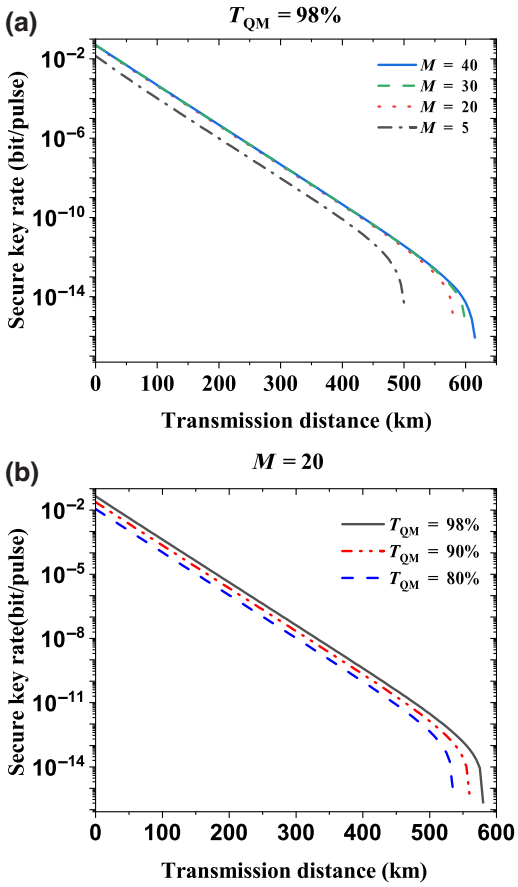

FIG. 3. The variation of the key rate with the transmission distance for different storage rounds (a), and different storage efficiencies (b).

their values when the transmission efficiency of the QM is reducing from 98 % to 80 %.

Next, we explore the inner correlation between the key rate and some system parameters including the storage round M and the efficiency of the quantum memory T_{QM}. In Fig. 4, we choose the transmission distance at 150 km, the solid line, the dot dash line and dot line depict the relation between key rate and storage rounds when the $T_{QM} =$ 75 %, $T_{QM} = 90$ %, $T_{QM} = 98$ %, individually. In general, the larger storage round corresponds to the higher key rate. However, when M reaches some threshold value i.e., 18 rounds in 75 %, 24 rounds in 90 %, 34 rounds in 98 %, the key rate will start to decrease. The threshold comes from the compromise between the cavity enhancement and the cavity leakage. Therefore, in practical applications, an appropriate transmission efficiency of the QM should be designed according to practical experimental conditions.

We also perform investigations on how the storage fidelity affects the key rate and the transmission distance, see Fig. 5. From the top to the bottom, the first three lines correspond to the storage fidelity at 98.5 %, 95 % and 90 %, respectively, with the fixed storage round at 20; the fourth

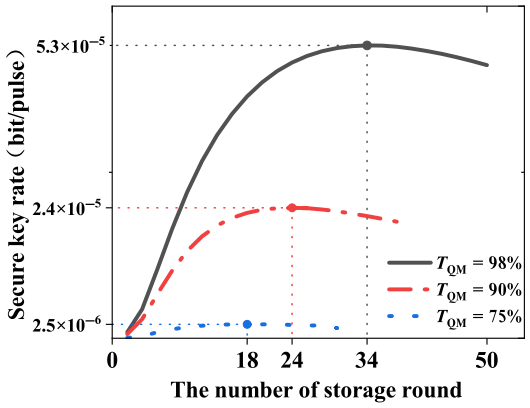

FIG. 4. The variation of the secure key rate with the number of storage rounds under different transmission efficiencies of the QM.

and fifth lines each refer to the storage fidelity at 98.5 % and 95 % with the fixed storage round at 5. Obviously, the key rate only slightly declines its value with the decreasing of the storage fidelity when the storage round is relatively higher, e.g., at 20; while the key rate drops significantly with the decreasing of the storage fidelity when the storage round is relatively lower, e.g., at 5. Therefore, the storage round seems a primary influencing factor among several parameters, and should be given more attention. Furthermore, we also take the finite-size effect into account and do comparisons between our present work and conventional MDI QKD protocols using either WCS or HSPS, as shown in Fig. 6. We can see from Fig. 6 that, first, for our present scheme, there is only a small difference between the line with the storage fidelity at 40 and the one at 20, while a big gap between the one with the storage fidelity at 20 and the one at 5, which is consistent with the above without considering finite-size effects. Second, the key rate of using our present method completely surpasses all conventional MDI QKD protocols using either WCS or HSPS

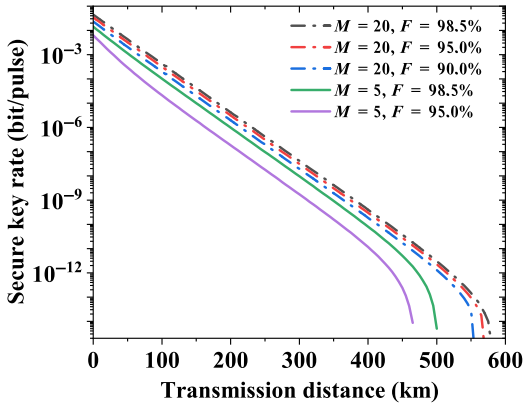

FIG. 5. The variation of the key rate with the transmission distance under different storage fidelities. Here, $T_{QM} = 98$ %.

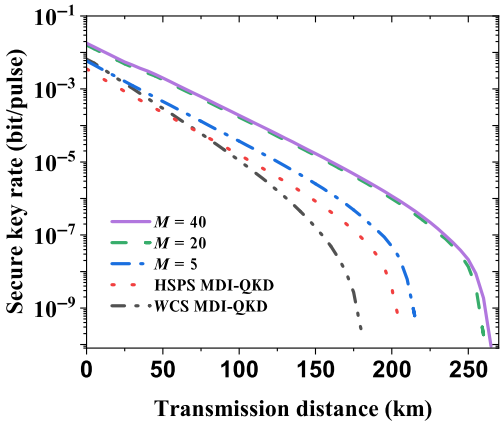

FIG. 6. Comparisons of the key rate between our present memory-assisted MDI QKD and conventional MDI QKD protocols using either WCS or HSPS by taking finite-size effects into account. Here, $T_{\mathrm{QM}} = 98\,\%$, $F = 98.5\,\%$, and $N = 10^{12}$.

at any transmission distance under practical experimental conditions.

Besides, there still exists some challenges on experimental realizations of the memory-assisted MDI QKD scheme. The first challenge is to maintain a high transmission efficiency T_{QM}. To solve it, we need to focus on enhancing the efficiency of all components within the quantum memory (QM) system. For instance, we can achieve a reflection efficiency of over 99.5 % for mirrors (10Q20UF.42PAIR in Newport), a transmission rate exceeding 99.28 % for the PC (PCR4-1560-NW in EKSMA OPTICS). These improvements make it feasible to achieve a total efficiency $T_{\mathrm{QM}} \approx 98\,\%$. The second challenge is to keep a high state fidelity after quantum storage. To solve it, a high extinction ratio of the PBS and the PC should be implemented. Effectively controlling the multiple memory rounds M is the third challenge. On one hand, a fast and precise synchronization among the devices of Alice, Bob, and Charlie is needed. On the other hand, we should carefully control the light dispersion and adjust the beam-waist position inside the cavity to get good spacial overlap of different modes.

IV. CONCLUSION

In conclusion, we suggest a practical proposal on the memory-assisted MDI QKD, constructed the model, and further carried out systematic investigations on its performance influence by a few factors. We also perform comparisons between our present work and conventional QKD protocols without QM, including MDI and BB84. Simulation results demonstrate that, the storage round plays a pivotal role in the key rate and transmission distance for our scheme. Moreover, no matter if considering the finite-size effect or not, our present work can surpasses the conventional MDI and BB84 protocols. It thus seems a very promising candidate for practical applications of long-distance secure communications in the near future. Next, we have a plan to construct some implementations on experiment and an experimental scheme has been designed. Therefore, our present work may provide another way for the practical implementation of long-distance quantum communications.

ACKNOWLEDGMENTS

We gratefully acknowledge the National Key R&D Program of China (2018YFA0306400), the National Natural Science Foundation of China (12074194, U19A2075, 12104240, 62101285), the leading edge technology Program of Jiangsu Natural Science Foundation (BK2019 2001), the Industrial Prospect and Key Core Technology Projects of Jiangsu provincial key R&D Program (B2022071), the Natural Science Foundation of Jiangsu Province (BK20210582), and NUPTSF (NY220122, NY220123).

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, (IEEE, New York, 1984), p. 175.

[2] B. Qi, C. H. F. Fung, H. K. Lo, and X. F. Ma, Time-shift attack in practical quantum, Quantum Inf. Comput. **7**, 073 (2007).

[3] C. H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, Phase-remapping attack in practical quantum-key distribution systems, Phys. Rev. A **75**, 032314 (2007).

[4] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors, New J. Phys **13**, 073024 (2011).

[5] H. K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[6] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[7] X. B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, Phys. Rev. A **87**, 012320 (2013).

[8] L. Lydersen, C. Wiechers, C. Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[9] I. Gerhardt, Q. Liu, A. Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).

[10] Y. Liu, T. Y. Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and J. W. Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).

[11] H. L. Yin, T. Y. Chen, Z. W. Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[12] G. J. Fan-Yuan, F. Y. Lu, S. Wang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Zheng Zhou, Ze-Hao Wang, Jun Teng, Guang-Can Guo, and Zheng-Fu Han, Robust and adaptable quantum key distribution network without trusted nodes, Optica **9**, 812 (2022).

[13] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography Without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[14] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeof for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[15] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[16] S. Wang, Z. Q. Yin, D. Y. He, Wei Chen, Rui-Qiang Wang, Peng Ye, Yao Zhou, Guan-Jie Fan-Yuan, Fang-Xiang Wang, Wei Chen, Yong-Gang Zhu, Pavel V. Morozov, Alexander V. Divochiy, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonic **16**, 154 (2022).

[17] M. Pittaluga, M. Minder, M. Lucamarini, Mirko Sanzaro, Robert I. Woodward, Ming-Jun Li, Zhiliang Yuan, and Andrew J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nat. Photonics **15**, 530 (2021).

[18] F. Kaneda, F. H. Xu, J. Chapman, and P. G. Kwiat, Quantum-memory-assisted multi-photon generation for efficient quantum information processing, Optica **4**, 1034 (2017).

[19] C. Panayi, M. Razavi, X. F. Ma, and N. Lütkenhaus, Memory-assisted measurement-device-independent quantum key distribution, New. J. Phys **16**, 043005 (2014).

[20] N. L. Piparo, M. Razavi, and C. Panayi, Measurement-device-independent quantum key distribution with ensemble-based memories, IEEE J. Sel. Top. Quantum Electron **21**, 138 (2015).

[21] J. Nunn, N. K. Langford, W. S. Kolthammer, T. F. M. Champion, M. R. Sprague, P. S. Michelberger, X. Jin, D. G. England, and I. A. Walmsley, Enhancing Multiphoton Rates with Quantum Memories, Phys. Rev. Lett. **110**, 133601 (2013).

[22] T. Chanelière, D. Matsukevich, S. Jenkins, S.-Y. Lan, T. A. B. Kennedy, and A. Kuzmich, Storage and retrieval of single photons transmitted between remote quantum memories, Nature **438**, 833 (2005).

[23] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[24] X. B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[25] H. K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[26] X. B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, Phys. Rev. A **87**, 012320 (2013).

[27] Q. Wang, X. B. Wang, and G. C. Guo, Practical decoy state method in quantum key distribution with heralded single photon source, Phys. Rev. A **75**, 012312 (2007).

[28] Q. Wang and A. Karlsson, Performance enhancement of a decoy-state quantum key distribution using a conditionally prepared down-conversion source in the Poisson distribution, Phys. Rev. A **76**, 014309 (2007).

[29] H. Jayakumar, A. Predojević, T. Kauten, Tobias Huber, Glenn S. Solomon, and Gregor Weihs, Time-bin entangled photons from a quantum dot, Nat. Commun. **5**, 4251 (2014).

[30] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real World Two Photon Interference and Proof of Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. **111**, 130501 (2013).

[31] H.-L. Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[32] I. Goswami, M. Mandal, and S. Mukhopadhyay, Alternative study of using electro-optic Pockels cell for massive reduction in the intensity of central frequency by multi-passing technique, J. Opt. **51**, 379 (2022).

[33] R. Jozsa, Fidelity for mixed quantum states, J. Mod. Opt **41**, 2315 (1994).

[34] S. Abruzzo, H. Kampermann, and D. Bruβ, Measurement-device-independent quantum key distribution with quantum memories, Phys. Rev. A **89**, 012301 (2014).

[35] Q. Wang and X. B. Wang, Simulating of the measurement-device independent quantum key distribution with phase randomized general sources, Sci. Rep. **4**, 4612 (2014).

[36] F. H. Xu, M. Curty, B. Qi, and H. K. Lo, Practical aspects of measurement-device-independent quantum key distribution, New J. Phys. **15**, 113007 (2013).

[37] M. Curty, F. H. Xu, W. Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun **5**, 3732 (2014).