Quantum Information Processing (2024) 23:253
https://doi.org/10.1007/s11128-024-04453-3

Quantum conference key agreement based on differential-phase-shift quantum key distribution

Kyo Inoue[1] · Toshimori Honjo[2]

Received: 14 December 2023 / Accepted: 4 June 2024

Abstract
A quantum conference key agreement (QCKA) protocol based on differential-phase-shift quantum key distribution is presented, which provides a common secret key for secure communication between more than two parties. In the proposed protocol, one party simultaneously broadcasts a weak coherent pulse train with $\{0, \pi\}$ phases to multiple parties that measure the phase differences between adjacent pulses using a delay interferometer followed by photon detectors, and the transmitter and receivers share secret key bits from the coincident counts in the receivers. The system setup and operation are simpler than those of conventional QCKA schemes that use a multipartite quantum entanglement state. The key creation performance is evaluated by considering the eavesdropping probability. The results indicate that the proposed scheme offers better performance than the conventional entanglement-based QCKA system.

Keywords Quantum conference key agreement · Differential phase shift quantum key distribution · Common key creation rate

1 Introduction

Quantum key distribution (QKD), which provides a secret key to two distant parties for encrypting and decrypting a message with security guaranteed by quantum mechanics, has been studied and developed [1]. It is basically used for one-to-one communication in which one party sends a message to another. However, there can be situations in which one party wants to simultaneously send a message to more than two parties. One scheme for securely achieving such communication requires the sender to pre-share a secret key individually with each receiver using QKD and send a common

✉ Kyo Inoue
kyo@comm.eng.osaka-u.ac.jp

[1] Graduate School of Engineering, Osaka University, Suita, Japan

[2] NTT Basic Research Laboratories, NTT Corporation, Atsugi, Japan

Published online: 24 June 2024

secret key to be used to encrypt a message to each receiver using the individually pre-shared secret key. However, several processes must be performed in such a scheme, making the key distribution task time consuming. To avoid this limitation, quantum communication systems that simultaneously provide a secret key to multiple parties have been studied. These systems are called multiparty QKD or quantum conference key agreements (QCKA) [2].

Several QCKA protocols have been proposed, most of which utilize a multipartite quantum entanglement state such as a Greenberger–Horne–Zeilinger (GHZ) state [2–8]. The central node generates a multipartite entangled state and sends one photon in the entangled state to each party. The receivers then measure the transmitted photons, from which the bits are created. Owing to the quantum correlation between photons in an entanglement state, the created bits are identical between receivers, which can form a common secret key. In this scheme, multiple parties share a secret key at the same time. However, its implementation is difficult in practice because of the difficulty in generating a multipartite entanglement state. In fact, although a QCKA experiment using four-photon polarization-entangled GHZ states has been demonstrated [9], its key creation performance was low at a key creation rate of 1 bit/s when the transmission lengths from the central node to receivers were 0, 20, 10, and 20 km, respectively, even using high-performance nanowire single-photon detectors.

To avoid the use of a multipartite entanglement state, others QCKA protocols have been also proposed, which are based on measurement-device-independent QKD or twin-field QKD [10–16]. In these protocols, multiple parties send quantum states to a central node, which then performs a joint measurement on the incoming states. The multi-parties can share a common secret key without using a multipartite entanglement state. However, the transmission phases, the polarization states, and the time positions should be precisely and stably adjusted in practical implementation, which makes the transmission system complicated. When a decoy method of varying the signal intensity is employed to beat the photon number splitting attack, the creation rate of a common key becomes low because the pulse intensity coming from all senders should be matched for the key creation. In addition, some protocols are restricted to three-party systems.

Another QCKA protocol that seems the most practical is one in which one sender sends identical quantum states of $\{|0>, |1>\}$ and $\{|+> = (|0> + |1>)/\sqrt{2}, |-> = (|0> - |1>)/\sqrt{2}\}$, i.e., states used in BB84-QKD, to multiple recipients simultaneously, from which the recipients create key bits [17]. The sender and receivers can share a common secret key with one quantum transmission from the sender to recipients, and no additional QKD transmission is required in this protocol. This QCKA scheme is a simple extension of BB84-QKD, which has been intensively studied and developed and is the most practical quantum communication system.

Following the idea of the above BB84-based QCKA scheme, this study presents a QCKA protocol based on differential-phase-shift (DPS) QKD [18]. One party broadcasts a weak coherent pulse train with a phase of 0 or π for each pulse to multiple receivers, who then individually measure the phase differences of adjacent pulses using a delay interferometer followed by photon detectors. Subsequently, the sender and receivers create common key bits from the coincident counts in the receivers.

Its setup and operation are simple compared with entanglement-based QCKA. Compared to the BB84-based scheme, the key creation efficiency of the proposed protocol is expected to be higher because key bits are created from basis-matched detection events in the BB84 scheme, while all coincident counts contribute to key creation in the proposed scheme. We formalize the key creation performance of the proposed scheme considering the eavesdropping probability and perform calculations. The results indicate that a key creation rate of 10^{-7} bit/pulse, corresponding to 100 bit/s for a pulse repetition rate of 1 GHz, is achievable in a four-party system with a 40-km distance for each receiver even when APD-based photon detectors are used.

2 Setup and operation

The setup of the proposed DPS-QCKA is illustrated in Fig. 1. A transmitter (Alice) broadcasts a weak coherent pulse train to receivers (Bobs), in which each pulse is phase-modulated by 0 or π and has a mean photon number of less than one. Bobs detect the transmitted signal using a delay Mach–Zehnder interferometer with a delay time equal to the pulse interval, at the output of which threshold single-photon detectors are placed. Using this apparatus, Bobs measure the phase differences between adjacent pulses, which are 0 or π. Here, measurement results are obtained occasionally and randomly in time owing the small photon number of the incoming pulses. When the measured phase difference is 0 (or π), they create bit 0 (or 1) while recording the clicking time slot and created bit.

After signal transmission, Alice and Bobs create a secret key as follows: (1) Bobs announce the time slots in which the bits were created. (2) Bobs extract bits that are created from time slots identical to all Bobs, and discard the other bits. (3) Alice creates bits from the phase modulation data corresponding to the time slots from which all

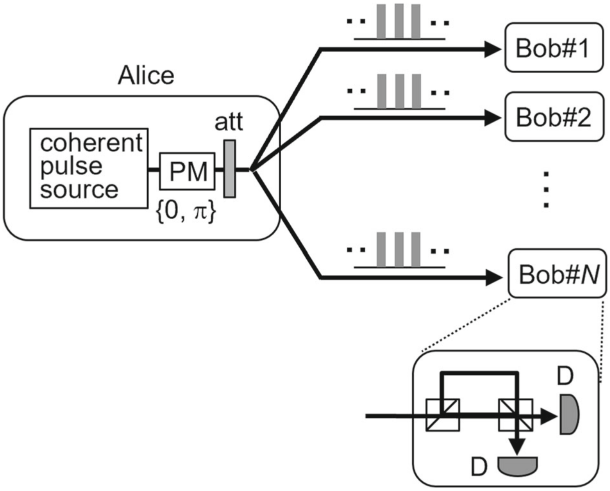

Fig. 1 Setup of DPS-QCKA. *PM* phase modulator, *D* photon detector

Bobs created their bits. (4) Alice and each Bob exchange a portion of their bits and estimate the bit error rate (BER) in them. Subsequently, they discard the bits used for the BER estimation, and hold the remaining bits as a raw key. (5) Based on the estimated BER, error correction is performed between Alice and Bob, such that Alice conveys error correction information (i.e., syndrome) to Bob, who then corrects his bits to match Alice's bits. (6) Privacy amplification is applied to the raw key, and a common secure key is shared between Alice and Bobs.

3 Key creation performance

In this section, we evaluate the key creation performance of DPS-QCKA. Specific eavesdropping is assumed in the evaluation rather than general or conceptional eavesdropping using sophisticated quantum mechanical means. This is because a weak coherent pulse train, in which a number of bits is embedded, is transmitted instead of qubits in the traditional QKD in the present protocol, against which conventional general attacks cannot be applied (Appendix).

In the present system, error correction is performed such that all Bobs correct their bits to match Alice's bits. For such systems, the creation rate of a common key bit R can be evaluated using mutual information as follows:

$$R = R_{\mathrm{r}}(I_{\mathrm{AB}} - I_{\mathrm{AE}}) \tag{1}$$

with.

$$I_{\mathrm{AB}} = 1 + e_{\mathrm{AB}} \log_2 e_{\mathrm{AB}} + (1 - e_{\mathrm{AB}}) \log_2 (1 - e_{\mathrm{AB}}) \tag{2}$$

$$I_{\mathrm{AE}} = 1 + e_{\mathrm{AE}} \log_2 e_{\mathrm{AE}} + (1 - e_{\mathrm{AE}}) \log_2 (1 - e_{\mathrm{AE}}) \tag{3}$$

where R_{r} denotes the raw-key rate; I_{AB} and I_{AE} denote the mutual information between Alice and each Bob and that between Alice and an eavesdropper (Eve), respectively; and e_{AB} and e_{AE} refer to the bit mismatch ratios between Alice and each Bob and that between Alice and Eve, respectively. In DPS-QCKA systems with N Bobs, the raw-key rate R_{r} is given by.

$$R_{\mathrm{r}} = (\kappa T \mu_0)^N \tag{4}$$

where μ_0 denotes the mean photon number per pulse sent from Alice, T denotes the transmittance from Alice to each Bob, which is assumed to be identical for all Bobs, and κ signifies Bob's detection efficiency.

The bit mismatch between Alice and each Bob results from imperfections in their signal transmission apparatus. Here, we assume that the dark count of Bob's photon detectors and imperfect visibility in Bob's interferometer are the causes of the bit mismatch. The bit mismatch ratio resulting from these causes is expressed as

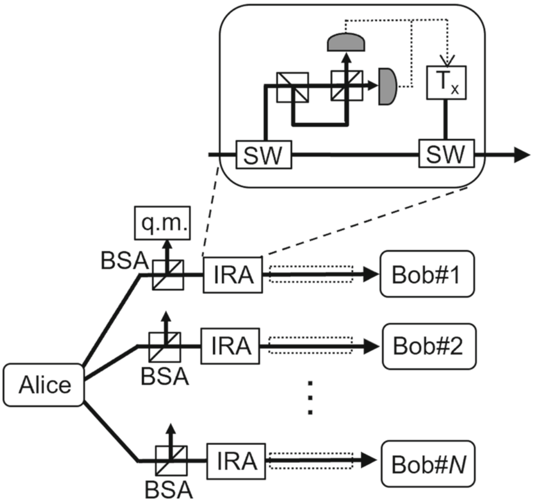

Fig. 2 Eavesdropping against DPS-QCKA. *BSA* beam splitting attack, *IRA* intercept-and-resend attack, *q.m.* quantum memory, *SW* optical switch, and T_x transmitter. Dashed boxes overlapped onto transmission lines indicate lossless media

$$e_{\mathrm{AB}} = \frac{2d}{\kappa T \mu_0 + 2d} + e_{\mathrm{MZ}} \tag{5}$$

where d indicates the dark count rate of the photon detector per time slot and e_{MZ} denotes the bit mismatch ratio owing to imperfect interference.

Meanwhile, the bit mismatch ratio between Alice and Eve is given by $e_{\mathrm{AE}} = (1–\eta)/2$, with η being Eve's eavesdropping probability on Alice's raw-key. In this study, Eve is assumed to perform beam splitting (BS) and intercept-and-resend (IR) attacks against a DPS-QCKA system, as illustrated in Fig. 2. Eve performs a BS attack on the transmission line to each Bob, where she splits and stores a portion of Alice's signals. The remaining signal is sent to each Bob via a lossless transmission medium to unchange the number of photons detected by each Bob. Subsequently, after all Bobs announce the time slots at which photons are detected, Eve extracts pulses clicking Bobs' detectors from the stored signals and makes them interfere with each other, the result of which gives her the phase difference of the mutually interfering pulses, that is Alice's bit. The eavesdropping probability of this BS attack is $\eta_{\mathrm{BS}} = 2\mu_0\ (1–T) \times N$.

In addition to the BS attack, Eve conducts an IR attack. She directly measures Alice's signal using the same apparatus as Bob's, in which Eve successfully measures the phase differences occasionally and randomly because of the small number of photons. When she succeeds in the measurement, she resends two pulses of one photon with the measured phase difference to the target Bob via a lossless transmission line. From these double pulses, the Bob detects the photon possibility in three time slots at the delay interferometer outputs. Detection in the middle slot occurs according to the phase difference of the double pulses, whereas detection in the first or third slot occurs randomly because there is no interference. Subsequently, a bit mismatch can be induced between Alice's and Bob's bits created from the detection in the first or third time slot, with a probability of (1/4 + 1/4) × 1/2 = 1/4, from which eavesdropping is revealed. Therefore, Eve partially conducts the IR attack, using optical switches, as illustrated in Fig. 2, such that the eavesdropping-induced bit errors are confused with the original system errors caused by imperfections of the transmission apparatuses. The upper bound of the IR attack ratio r_{IR} is given by $r_{\mathrm{IR}}/4 \leq e_{\mathrm{AB}}$, where e_{AB} denotes the bit error rate between Alice and the target Bob, given by Eq. (5).

When the IR attack is conducted, the target Bob detects a photon, possibly in three time slots, as described above. The Bob announces the clicking slot and Alice creates her bit by referring to the phase difference of the pulses that have clicked Bob's detector. Here, Eve knows Alice's bit that is created from the photon detection in the middle time slot, but does not that created from the detection in the first or third slot. The probability of detection in the middle slot is 1/2, and thus the probability of Eve obtaining Alice's bit through the IR attack on the transmission line to the target Bob is 1/2. This eavesdropping probability of 1/2 is for the conventional DPS-QKD. In DPS-QCKA, Eve performs the IR attack against multiple Bobs, as illustrated in Fig. 2, for which further consideration is necessary. In the following, we consider the probability of eavesdropping through the IR attack in DPS-QCKA.

As described above, the IR attack is performed partially such that the eavesdropping-induced bit error rate is confused with the original bit error rate. The timing of the partial attack should be synchronized on the transmission lines to all Bobs, because key bits are created from coincident counts at all Bobs. Thus, Eve wants to know Alice's phase differences that cause the coincident counts. Here, we consider the probability of Eve obtaining Alice's phase difference that induces Bobs' coincident counts at a given time slot, hereafter denoted as slot#i, through the synchronous IR attack. Three double-pulse patterns resent from Eve can click each Bob's detector in slot#i, which are illustrated and labeled A, B, and C in Fig. 3. In the figure, the pulse positions at the delay interferometer output are depicted on the right side of Bob. In pattern A, an incident pulse at slot (b) passes through the long path of the interferometer, and clicks the detector at slot#i. In pattern B, an incident pulse at (c) passing through the short

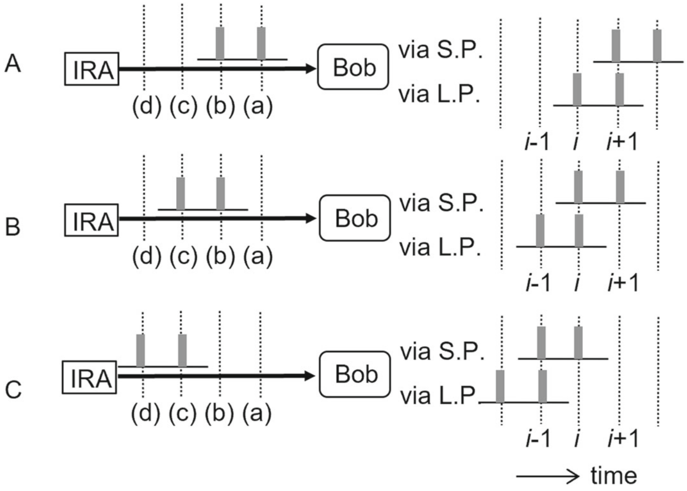

Fig. 3 Pulse patterns when IR attack is conducted. IRA denotes intercept-and-resend attack, and S.P. and L.P. stand for the short and long paths, respectively

Table 1 Combination of pulse patters causing a click at a given time slot in a two-Bob system

	Bob#1	Bob#2	Prob
(1)	A	A	$(1/4)^2 = 1/16$
(2)	A	B	$1/4 \times 1/2 = 1/8$
(3)	A	C	$(1/4)^2 = 1/16$
(4)	B	A	$1/2 \times 1/4 = 1/8$
(5)	B	B	$1/2 \times 1/2 = 1/4$
(6)	B	C	$1/2 \times 1/4 = 1/8$
(7)	C	A	$(1/4)^2 = 1/16$
(8)	C	B	$1/4 \times 1/2 = 1/8$
(9)	C	C	$(1/4)^2 = 1/16$

path and that at (b) passing through the long path cause a click at slot#*i*. In pattern C, an incident pulse at (c) passes through the long path, and clicks the detector at slot#*i*. Eve obtains Alice's bit when one Bob counts a photon at slot#*i* in pattern B, but not in patterns A and C. The probability of a click at slot#*i*, conditioned such that one Bob receives one photon super-positioned over double pulses, is 1/4 in pattern A, 1/2 in pattern B, and 1/4 in pattern C.

In DPS-QCKA, Eve conducts the IR attack against the broadcast signal, as illustrated in Fig. 2, through which she obtains Alice's bit created from the click at slot#*i* when at least one Bob counts a photon from pattern B. Here, we evaluate the probability of Eve obtaining Alice's bit, assuming a two-Bob system as an example. In a system with two Bobs, the number of combinations of pulse patterns that causes a click at slot#*i* is $3^2 = 9$, as listed in Table 1, where the probability of each combination is also given. Eve obtains Alice's bit when at least one Bob counts a photon from pattern B, which are combinations of (2), (4), (5), (6), and (8). Therefore, the probability of Eve obtaining Alice's bit, provided that the IR attack is conducted, is given by the sum of their probabilities as $1/8 \times 4 + 1/4 = 3/4$. Subsequently, the upper bound of the eavesdropping probability through the IR attack is $\eta_{\mathrm{IR}} = r_{\mathrm{IR}} \times (3/4) \leq 3e_{\mathrm{AB}}$ in a two-Bob system, where $r_{\mathrm{IR}} \leq 4e_{\mathrm{AB}}$ is substituted. The eavesdropping probability of the IR attack against other DPS-QCKA systems with more than two Bobs can be similarly evaluated. This is $\eta_{\mathrm{IR}} = r_{\mathrm{IR}} \times (10/11)$ in a three-Bob system and $\eta_{\mathrm{IR}} = r_{\mathrm{IR}} \times (15/16)$ in a four-Bob system, although the details of the evaluation processes are not presented here to avoid redundancy. The eavesdropping probability conditioned by the IR attack approaches one as the number of Bobs increases.

Using the eavesdropping probabilities through the BS and IR attacks evaluated above, that is, η_{BS} and η_{IR}, the bit mismatch ratio between Alice's and Eve's bits is expressed as.

$$e_{\mathrm{AE}} = \frac{1 - (\eta_{\mathrm{BS}} + \eta_{\mathrm{IR}})}{2} \tag{6}$$

The mutual information between Alice and Eve I_{AE} can be evaluated by substituting this expression into Eq. (3), and the key creation rate R in DPS-QCKA system is evaluated by using Eq. (1) with Eqs. (2–5).

4 Calculation

Based on the previous section where the creation rate of systems suffering from the beam split attack and the intercept-and-resend attack is analyzed, we calculated the key creation rate R in DPS-QCKA systems. The results are shown in Fig. 4, where the number of Bobs is assumed to be $N = 2$, 3, or 4. The key creation rate drastically decreases with the transmission distance because the raw-key rate is proportional to T^N, as shown in Eq. (4). It is also notably lower in systems with a larger number of Bobs because the eavesdropping probability increases in addition to the raw-key rate being proportional to $(\kappa T\mu_0)^N$. Even though the key creation rate is drastically reduced for a long distance and a large number of Bobs, it is still 10^{-7} bit/pulse, corresponding to 100 bits/s at a 1-GHz pulse repetition rate, which is achievable in a four-party system ($N = 3$) with a transmission distance of 40 km for each Bob using APD-based photon detectors. This value would be one order of magnitude higher if high-performance superconducting nanowire single-photon detectors are assumed, which is much higher than that in a QCKA experiment that employs a protocol based on a four-photon GHZ state [9].

In the last of this section, we briefly discuss the system performance of QCKA broadcasting BB84 signals instead of DPS signals. The present idea of broadcasting weak coherent lights to all recipients simultaneously can be also employed in BB84-based QCKA [17], such as weak coherent states as quasi single photons of $\{|0>, |1>\}$ and $\{|+> = (|0> + |1>)/\sqrt{2}, |-> = (|0> - |1>)/\sqrt{2}\}$ are broadcast to all recipients. A common secret key can be shared between multiple parties with one quantum transmission, similarly to the present scheme. However, the key creation rate in BB84-based systems would be lower than that in the present one. Provided that the eavesdropping probability is the same, the key creation rate in QCKA broadcasting phase-encoded BB84 signals, that is, $|0> = (|t_1> + |t_2>)/\sqrt{2}$, $|0> = (|t_1> - |t_2>)/\sqrt{2}$, $|+> = (|t_1> + i|t_2>)/\sqrt{2}$, and $|-> = (|t_1> - i|t_2>)/\sqrt{2}$ where $|t_{1,2}>$ represents the single-photon state at time-bin $t_{1,2}$, would be $1/3 \times (1/2)^N$ of that broadcasting DPS signals (where N is the number of recipients). The factor $(1/2)^N$ arises from the fact that the measurement basis is randomly selected and it must be matched in

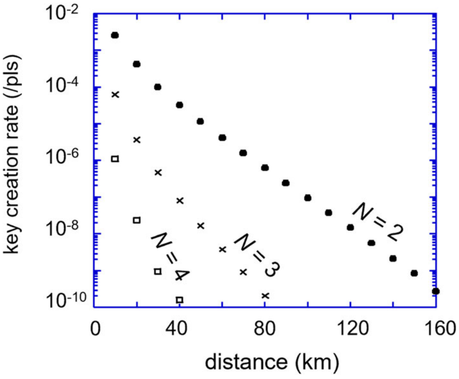

Fig. 4 Key creation rate R in DPS-QCKA systems with two, three, or four Bobs. The parameter values assumed are as follows: dark count rate: $d = 10^{-7}$, detection efficiency: $\kappa = 0.25$, fiber attenuation: 0.2 dB/km, and interference error rate: $e_{MZ} = 0.01$. The mean photon number sent from Alice is optimized for the key creation rate to be maximum at each distance

all participants in BB84-based schemes while there is no such basis selection in the present scheme. Besides, the factor 1/3 arises from the fact that isolated two pulses convey one bit information in phase-encoded signal suitable for fiber transmission, and three time slots are necessary for a recipient to create one bit, whereas each time slot serves to provide one bit in the DPS scheme.

5 Summary

This study presented a QCKA scheme based on DPS-QKD. One party broadcasts a weak coherent pulse train, as in DPS-QKD, to multiple parties, that measure their relative phases. Subsequently, the transmitter and receivers share a secret key based on the receivers' coincident counts. Its setup and operation are simpler than those of conventional QCKA schemes that utilize a multipartite entanglement state. The key creation performance was evaluated by considering the eavesdropping probability, and calculations were conducted accordingly. The results indicate that a higher key creation performance than that of conventional entanglement-based QCKA is expected.

Appendix

In this appendix, we describe why specific eavesdropping, rather than general eavesdropping, was assumed in this study. In traditional QKD protocols, bit information is conveyed by single photons, namely, qubits. Therefore, in general attacks against conventional QKD systems, an eavesdropper (Eve) prepares a probe photon, entangles it with a transmitted signal photon through an interaction (or unitary operation), stores it, and then measures the stored probe photon after obtaining the basis information on the signal photons.

By contrast, a coherent pulse train is transmitted in DPS-QCKA, in which a number of bits are embedded such that their positions are ambiguous during the transmission. When conducting a general attack against such a signal, Eve may regard the pulse train as an ensemble of single photons super-positioned over all pulses and entangles a probe photon with each signal photon, following conventional general attacks [19]. However, the global phase of a single-photon is not determined owing to the quantum mechanical uncertainty between the photon number and phase; thus the phase of each pulse is random if the pulse train is modeled as an ensemble of single-photon states, which contradicts the state of a coherent pulse train. That is, a coherent pulse train cannot be regarded as an ensemble of single photons. We do not know if the operation in conventional general attacks of entangling a probe state with each signal photon is feasible for such a pulse train. In addition, even if such probe photons entangled with signal photons can be created and stored, Eve could not select and measure the probe photon that is entangled with a target signal photon having Bob's detector clicked, because signal photons are indistinguishable and Eve cannot specify a probe photon that is entangled with the target photon.

Based on the above considerations, we do not assume general attacks in this study.

Author's contribution KI primarily proposes and evaluates the scheme. TH discusses with K. Inoue on the scheme and provides precious comment and suggestion.

Funding Open Access funding provided by Osaka University.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Pirandola, S., et al.: Advances in quantum cryptography. Adv. Opt. Photon. **12**, 1012–1236 (2020)
2. Murta, G., Grasselli, F., Kampermann, H., Brubß, D.: Quantum conference key agreement: a review. Ad. Quant. Info. **3**, 2000025 (2020)
3. Chen, K., Lo, H.: Multi-partie quantum cryptographic protocols with noisy GHZ states. Quant. Info. Comput. **7**, 589 (2007)
4. Ribeito, J., Murta, G., Wehner, S.: Fully device-independent conference key agreement. Phys. Rev. A **97**, 022307 (2018)
5. Zhang, Z., Shi, R., Guo, Y.: Multipartite continuous variable quantum conferencing network with entanglement in the middle. Appl. Sci. **8**, 1312 (2018)
6. Grasselli, F., Kampermann, H., Bruß, D.: Finite-key effects in multipartite quantum key distribution protocols. New J. Phys. **20**, 113014 (2018)
7. Nilesh, K.: Simple proof of security of the multiparty prepare and measure QKD. Quant. Info. Process **21**, 351 (2022)
8. Pickston, A., Ho, J., Ulibarrena, A., Grasselli, F., Proietti, M., Morrison, C., Barrow, P., Graffitti, F., Fedrizzi, A.: Conference key agreement in a quantum network. Quant. Info. **9**, 82 (2023)
9. Proietti, M., Ho, J., Grasselli, F., Barrow, P., Malik, M., Fedrizzi, A.: Experimental quantum conference key agreement. Sci. Ad. **7**, 395 (2021)
10. Fu, Y., Yin, H., Chen, Z.: Long-distance measurement-device-independent multiparty quantum communication. Phys. Rev. Lett. **114**, 090501 (2015)
11. Ottaviani, C., Lupo, C., Laurenza, R., Pirandola, S.: Modular network for high-rate quantum conferencing. Commun. Phys. **2**, 118 (2019)
12. Zhao, S., Zend, P., Cao, W., Zhen, Y., Ma, X., Li, L., Liu, N., Chen, K.: Phase-matching quantum cryptographic conferencing. Phys. Rev. Appl. **14**, 024010 (2020)
13. Cao, X., Gu, J., Lu, Y., Yin, H., Chen, Z.: Coherent one-way quantum conference key agreement based on twin field. New J. Phys. **23**, 043002 (2021)
14. Bai, J., Xie, Y., Li, Z., Yin, H., Chen, Z.: Post-marching quantum coherence key agreement. Opt. Express **30**, 28865 (2022)
15. Carrara, G., Murta, G., Grasselli, F.: Overcoming fundamental bounds on quantum conference key agreement. Phys. Rev. Appl. **19**, 064017 (2023)
16. Li, C., Fu, Y., Liu, W., Li, B., Zhou, M., Yin, H., Chen, Z.: Breaking universal limitations on quantum conference jey agreement without quantum memory. Commun. Phys. **6**, 122 (2023)
17. Matsumoto, R.: Multiparty quantum-key-distribution protocol without use of entanglement. Phys. Rev. A **76**, 062316 (2007)

18. Inoue, K., Waks, E., Yamamoto, Y.: Differential-phase-shift quantum key distribution using coherent light. Phys. Rev. A **68**, 022317 (2003)
19. Waks, E., Takesue, H., Yamamoto, Y.: Security of differential-phase-shift quantum key distribution against individual attacks. Phys. Rev. A **73**, 012344 (2006)

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