frontiers | Frontiers in Quantum Science and Technology

TYPE Original Research
PUBLISHED 03 May 2023
DOI 10.3389/frqst.2023.1182637

OPEN ACCESS

EDITED BY
Bao-Sen Shi,
University of Science and Technology of China, China

REVIEWED BY
Shuang Wang,
University of Science and Technology of China, China
Chuan Wang,
Beijing Normal University, China

*CORRESPONDENCE
Yu-Guang Yang,
yangyang7357@bjut.edu.cn

RECEIVED 09 March 2023
ACCEPTED 13 April 2023
PUBLISHED 03 May 2023

CITATION
Liu B-X, Huang R-C, Yang Y-G and Xu G-B (2023), Measurement-device-independent multi-party quantum key agreement.
Front. Quantum Sci. Technol. 2:1182637.
doi: 10.3389/frqst.2023.1182637

Measurement-device-independent multi-party quantum key agreement

Bing-Xin Liu[1], Rui-Chen Huang[1], Yu-Guang Yang[1,2]* and Guang-Bao Xu[3]

[1]Faculty of Information Technology, Beijing University of Technology, Beijing, China, [2]Beijing Key Laboratory of Trusted Computing, Beijing, China, [3]College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao, China

Quantum key agreement (QKA) is an important quantum cryptography primitive. In a QKA protocol, two or more untrusted parties can agree on an identical key in such a way that they equally influence the key and no subset can decide it alone. However, in practical QKA, the imperfections of the participant's detectors can be exploited to compromise the security and fairness of QKA. To remove all the detector-side-channel loopholes, a measurement-device-independent multi-party QKA protocol is proposed. The protocol exploits the post-selected GHZ states to generate a secure agreement key between legitimate participants, while ensuring the fairness of key agreement. Our protocol provides a new clue for the design of practical QKA protocols.

KEYWORDS

quantum key agreement, measurement-device-independent, detector-side-channel, fairness, multiparty

1 Introduction

Securing group communication has received lots of attention in recent years. The approach of supporting secure group communication is to maintain a secret known only to all group members. The way of generating this secret is known as group key establishment. There are two ways to realize it. One is centralized key establishment, i.e., key distribution, where one party generates a group secret. It is appropriate for 2-party (e.g., client-server or peer-to-peer) communication as well as for large multicast groups. However, many collaborative group settings (e.g., remote board meetings, teleconferences, white-boards, shared instruments, secure and efficient data sharing, collaborative workspaces, cloud computing, and command-and-control systems) require distributed key establishment techniques, i.e., distributed group key agreement.

A key agreement protocol aims to generate a common conference key for multiple participants to ensure the security of their later group communications in such a way that all influence the outcome. Since it was introduced by Diffie-Hellman in their seminal paper (Diffie and Hellman, 1976), the key agreement protocol has become one of the fundamental cryptographic primitives. However, classical key agreement protocols are based on public key cryptography where the security is based on the assumption of computational complexity. With the proposal of quantum computer, the classical cryptosystem faces certain security threats, so quantum cryptography came into being.

The security of quantum cryptography depends on the basic principles of quantum mechanics. In recent years, quantum cryptography has developed rapidly, and has extended a series of branch fields, such as quantum key distribution (Bennett and Brassard, 1984; Gisin

et al., 2002), quantum secure direct communication (QSDC) (Boström and Felbinger, 2002; Deng et al., 2003), quantum authentication (Dušek et al., 1999), quantum private comparison (Yang et al., 2009; Yang and Wen, 2009; Chen et al., 2010), quantum signature (Yang et al., 2016a; Yang et al., 2017a), quantum private query (Gao et al., 2012; Yang et al., 2014; Gao et al., 2015; Yang et al., 2016b; Yang et al., 2016c; Wei et al., 2016; Yang et al., 2017b; Yang et al., 2019a; Gao et al., 2019), and quantum key agreement (QKA), *etc.*

Generally speaking, a secure QKA should satisfy four conditions (C1) Correctness: At the end of the protocol, each participant will get the correct agreement key (C2) Fairness: All participants have equal influence on the agreement key, that is, any non-trivial subset of participants cannot determine the agreement key alone (C3) Security: No external eavesdropper can obtain the information about the agreement key without being detected (C4) Privacy: All participants' sub keys must remain confidential, and only the participants themselves know their own sub-keys. Since Zhou et al. proposed the first QKA protocol (Zhou et al., 2004) in 2004, various novel two-party and multi-party QKA protocols have been proposed (Tsai and Hwang, 2009; Chong and Hwang, 2010; Liu et al., 2013a; Shi and Zhong, 2013; He and Ma, 2015; Sun et al., 2016; He and Ma, 2017; Mohajer and Eslami, 2017; Wang et al., 2017; Yang et al., 2019b; Li and Li, 2020; Naresh et al., 2020; Naresh and Reddi, 2020; Zhou et al., 2020; Zhu et al., 2021a; Zhu et al., 2021b; Huang et al., 2021; Lin et al., 2021; Yang et al., 2022).

In practice, deviations in the actual behavior of a physical device from its ideal behavior can lead to significant practical safety issues. Quantum hackers can exploit these device flaws, especially detector defects, to perform time-shift attacks, bright light blinding attacks, and other attacks on detectors (Qi et al., 2007; Makarov, 2009; Lydersen et al., 2010; Xu et al., 2020). To address this security issue, measurement-device-independent QKD (MDI-QKD) was proposed, which removes all detector-side channel loopholes (Lo et al., 2012). The advantage of MDI-QKD is that it is only necessary to assume that legitimate participants have a trusted state preparation device. Thus, the measurement device can be considered as a black box, which naturally removes all detector-side channels. Various MDI-QKD experimental systems have been successfully demonstrated (Liu et al., 2013b; Ferreira da Silva et al., 2013; Rubenok et al., 2013; Woodward et al., 2021) and extended to the communication network (Tang et al., 2016). Various new MDI-QKD protocols, such as twin-field QKD (Lin and Lütkenhaus, 2018; Lucamarini et al., 2018; Ma et al., 2018; Wang et al., 2018) and mode-pairing QKD (Zeng et al., 2022), have also been proposed. Recently, the MDI-QKD proposed by Fan et al. achieves networking of QKD by combining cost and the user needs, enabling the network to meet high key rates or achieve high security levels (Fan-Yuan et al., 2021). Next, they proposed the MDI-QKD protocol, which is robust to environmental disturbances and highly adaptive to multi-user access (Fan-Yuan et al., 2022). Wang et al. proposed the long-distance TF-QKD protocol, which can achieve long-distance key distribution of more than 830 km. This is a great breakthrough and in ensuring similar distances, compared to previous key distribution, the security key rate of this protocol is two orders of magnitude greater (Wang et al., 2022).

However, there is little work related to MDI-QKA. Recently, Cai et al. proposed a three-party MDI-QKA protocol (Cai et al., 2022). In this protocol, the participant Charlie needs to implement Z-basis or X-basis measurement on his Greenberger-Horne-Zeinger (GHZ) particle c, where the Z-basis measurement result is just the agreement key. However, if an external eavesdropper manipulates Charlie's measurement device, Charlie's measurement device may leak Charlie's Z-basis measurement result, i.e., the agreement key to the external eavesdropper, thus threatening the security of the MDI-QKA protocol.

To eliminate all detector-side channel loopholes in QKA, a new multi-party MDI-QKA protocol is proposed. The protocol utilizes post-selected GHZ states to generate secure agreement keys among the multiple participants while ensuring fairness in key agreement. The protocol only needs to assume that the participants' state preparation devices are trusted, and thus the security is better than that of Cai et al.

The rest of this paper is organized as follows: In Section 2, a three-party MDI-QKA protocol is first proposed. In Section 3, the protocol is analyzed in terms of correctness, fairness, and security. In Section 4, the generalization of the three-party MDI-QKA protocol to n-party is proposed. The last section gives the discussion and conclusion.

2 The three-party MDI-QKA protocol

Suppose that the three participants Alice, Bob and Charlie want to jointly negotiate a key K. David is the untrusted relay for implementing GHZ state measurements. The process of the three-party MDI-QKA protocol is described as follows.

(1) Alice, Bob and Charlie independently prepare a single-photon sequence S_A, S_B, and S_C, respectively. Every single photon in the sequence is randomly in state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sent to the relay David via the quantum channel, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

(2) David performs three-particle GHZ state measurements on photons received at the same positions in the three sequences and publishes the results of his measurements. The three-particle GHZ state can be described as

$$
\begin{aligned}
|\Phi_0^+\rangle &= \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle),\\
|\Phi_0^-\rangle &= \frac{1}{\sqrt{2}}(|000\rangle-|111\rangle),\\
|\Phi_1^+\rangle &= \frac{1}{\sqrt{2}}(|001\rangle+|100\rangle),\\
|\Phi_1^-\rangle &= \frac{1}{\sqrt{2}}(|001\rangle-|100\rangle),\\
|\Phi_2^+\rangle &= \frac{1}{\sqrt{2}}(|010\rangle+|101\rangle),\\
|\Phi_2^-\rangle &= \frac{1}{\sqrt{2}}(|010\rangle-|101\rangle),\\
|\Phi_3^+\rangle &= \frac{1}{\sqrt{2}}(|100\rangle+|011\rangle),\\
|\Phi_3^-\rangle &= \frac{1}{\sqrt{2}}(|100\rangle-|011\rangle).
\end{aligned}
\tag{1}
$$

In fact, David's GHZ state analyzer (Pan and Zeilinger, 1998) constructed using linear optics can identify only two of the eight

GHZ states, namely, $|\Phi_0^+\rangle$ and $|\Phi_0^-\rangle$. Therefore, the output of the GHZ state analyzer is $|\Phi_0^+\rangle, |\Phi_0^-\rangle$ or failure.

(3) Alice, Bob and Charlie randomly select the photon subset corresponding to successful GHZ state measurement by David as the decoy photons, notify the other two parties of the location of the photon subset and ask them to announce their decoy photon states, respectively. They discard the positions with different tripartite preparation bases. When the bases are the same, they check whether the correlation between the tripartite decoy photon states and David's GHZ state measurements satisfies formulas (2)-(17). If the error rate is higher than the preset value, they will terminate the protocol, otherwise continue to the next step.

$$|0\rangle|0\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|\Phi_0^+\rangle+|\Phi_0^-\rangle\right), \tag{2}$$

$$|0\rangle|0\rangle|1\rangle = \frac{1}{\sqrt{2}}\left(|\Phi_1^+\rangle+|\Phi_1^-\rangle\right), \tag{3}$$

$$|0\rangle|1\rangle 0\rangle = \frac{1}{\sqrt{2}}\left(|\Phi_2^+\rangle+|\Phi_2^-\rangle\right), \tag{4}$$

$$|0\rangle|1\rangle|1\rangle = \frac{1}{\sqrt{2}}\left(|\Phi_3^+\rangle-|\Phi_3^-\rangle\right), \tag{5}$$

$$|1\rangle|0\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|\Phi_3^+\rangle+|\Phi_3^-\rangle\right), \tag{6}$$

$$|1\rangle|0\rangle 1\rangle = \frac{1}{\sqrt{2}}\left(|\Phi_2^+\rangle-|\Phi_2^-\rangle\right), \tag{7}$$

$$|1\rangle|1\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|\Phi_1^+\rangle-|\Phi_1^-\rangle\right), \tag{8}$$

$$|1\rangle|1\rangle|1\rangle = \frac{1}{\sqrt{2}}\left(|\Phi_0^+\rangle-|\Phi_0^-\rangle\right), \tag{9}$$

$$|+\rangle|+\rangle|+\rangle = \frac{1}{2}\left(|\Phi_0^+\rangle+|\Phi_1^+\rangle+|\Phi_2^+\rangle+|\Phi_3^+\rangle\right), \tag{10}$$

$$|+\rangle|+\rangle|-\rangle = \frac{1}{2}\left(|\Phi_0^-\rangle-|\Phi_1^-\rangle+|\Phi_2^-\rangle-|\Phi_3^-\rangle\right), \tag{11}$$

$$|+\rangle|-\rangle|+\rangle = \frac{1}{2}\left(|\Phi_0^-\rangle+|\Phi_1^-\rangle-|\Phi_2^-\rangle-|\Phi_3^-\rangle\right), \tag{12}$$

$$|+\rangle|-\rangle|-\rangle = \frac{1}{2}\left(|\Phi_0^+\rangle-|\Phi_1^+\rangle-|\Phi_2^+\rangle+|\Phi_3^+\rangle\right), \tag{13}$$

$$|-\rangle|+\rangle|+\rangle = \frac{1}{2}\left(|\Phi_0^-\rangle+|\Phi_1^-\rangle+|\Phi_2^-\rangle+|\Phi_3^-\rangle\right), \tag{14}$$

$$|-\rangle|+\rangle|-\rangle = \frac{1}{2}\left(|\Phi_0^+\rangle-|\Phi_1^+\rangle+|\Phi_2^+\rangle-|\Phi_3^+\rangle\right), \tag{15}$$

$$|-\rangle|-\rangle|+\rangle = \frac{1}{2}\left(|\Phi_0^+\rangle+|\Phi_1^+\rangle-|\Phi_2^+\rangle-|\Phi_3^+\rangle\right), \tag{16}$$

$$|-\rangle|-\rangle|-\rangle = \frac{1}{2}\left(|\Phi_0^-\rangle-|\Phi_1^-\rangle-|\Phi_2^-\rangle-|\Phi_3^-\rangle\right). \tag{17}$$

(4) After all participants complete the eavesdropping detection, they publish the base information of their remaining single photon states corresponding to the successful GHZ state measurements by David. Finally, the three participants choose the states in Z basis to generate the raw key K'.

(5) Alice, Bob and Charlie generate the final key K by performing error correction and privacy amplification on the raw key K'.

3 Analysis of correctness, fairness and security

3.1 Correctness

Theorem 1. Suppose Alice, Bob and Charlie are honest and they can negotiate a key K together.

Proof. It can be shown that if Alice, Bob and Charlie perform the above agreement honestly, they can negotiate the raw key K' together. This is because when David successfully implements GHZ state measurement and the three preparation bases are Z bases, it can be seen from formulas (2)-(9) that the particle states prepared by Alice, Bob and Charlie can only have two combinations, namely, $|0\rangle|0\rangle|0\rangle$ and $|1\rangle|1\rangle|1\rangle$ with equal probability. Thus, each party can infer from its single photon state that the other two parties have the same state as his preparation. For example, if Alice prepared the single photon state $|0\rangle$, she can infer that Bob and Charlie also prepared the single photon state as $|0\rangle$. So, "0" can be used as the agreement key. Therefore, Alice, Bob and Charlie can jointly negotiate a key K'. On this basis, Alice, Bob and Charlie generate an agreement key K after implementing error correction and privacy amplification on K'.

3.2 Fairness

Theorem 2. No subset of participants can determine the agreement key K alone.

Proof. It follows from Theorem 1 that if the subset of participants wants to determine the key K alone, they must first determine the raw key K'. However, this is not possible. Suppose Alice and Bob want to independently determine the generation key K'. Since the raw key K' is generated when the composite states of Alice, Bob and Charlie are $|0\rangle|0\rangle|0\rangle$ or $|1\rangle|1\rangle|1\rangle$, and each single photon state of Charlie is randomly selected from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, Alice and Bob cannot clearly distinguish these four non-orthogonal states, that is, they cannot identify the single photon state of Charlie according to the Heisenberg uncertainty principle. If Alice and Bob try to intercept Charlie's single photon sequence and send the forged single photon sequence to David, it will be detected with non-zero probability in step 3) when Charlie performs the security detection. The most common attack strategy is for Alice and Bob to prepare an auxiliary particle $|\epsilon\rangle$ and entangle it with Charlie's single photon, and then the state evolution of the composite system consisting of Alice and Bob's auxiliary particle and Charlie's single photon is

$$\begin{aligned}
|0\rangle|\epsilon\rangle &\rightarrow |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle,\\
|1\rangle|\epsilon\rangle &\rightarrow |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle,\\
|+\rangle|\epsilon\rangle &\rightarrow \frac{1}{2}[\,|+\rangle(\,|\epsilon_{00}\rangle + |\epsilon_{10}\rangle+|\epsilon_{01}\rangle + |\epsilon_{11}\rangle) + |-\rangle(\,|\epsilon_{00}\rangle+|\epsilon_{10}\rangle\\
&\qquad -|\epsilon_{01}\rangle-|\epsilon_{11}\rangle)],\\
|-\rangle|\epsilon\rangle &\rightarrow \frac{1}{2}[\,|+\rangle(\,|\epsilon_{00}\rangle - |\epsilon_{10}\rangle+|\epsilon_{01}\rangle - |\epsilon_{11}\rangle) + |-\rangle(\,|\epsilon_{00}\rangle\\
&\qquad -|\epsilon_{10}\rangle - |\epsilon_{01}\rangle+|\epsilon_{11}\rangle)],
\end{aligned} \tag{18}$$

where $\langle\epsilon_{00}|\epsilon_{00}\rangle + \langle\epsilon_{01}|\epsilon_{01}\rangle = 1, \langle\epsilon_{10}|\epsilon_{10}\rangle + \langle\epsilon_{11}|\epsilon_{11}\rangle = 1, \langle\epsilon_{00}|\epsilon_{10}\rangle + \langle\epsilon_{01}|\epsilon_{11}\rangle = 0$. Therefore, the probability that Alice and Bob implement this attack without disturbing Charlie's state is

$$\begin{aligned} P_{nd}(|0\rangle) &= \langle\epsilon_{00}|\epsilon_{00}\rangle, \\ P_{nd}(|1\rangle) &= \langle\epsilon_{11}|\epsilon_{11}\rangle, \\ P_{nd}(|+\rangle) &= \frac{1}{2}(1 + \langle\epsilon_{00}|\epsilon_{11}\rangle + \langle\epsilon_{10}|\epsilon_{01}\rangle), \\ P_{nd}(|-\rangle) &= \frac{1}{2}(1 + \langle\epsilon_{00}|\epsilon_{11}\rangle + \langle\epsilon_{10}|\epsilon_{01}\rangle). \end{aligned} \tag{19}$$

For simplicity and without loss of generality, assume that Charlie chooses the decoy state $|+\rangle$ for security detection and Alice and Bob prepare states $|+\rangle|+\rangle$. Without eavesdropping, according to formula (10), if David implements the GHZ state measurement successfully, only $|\Phi_0^+\rangle$ will be obtained, and $|\Phi_0^-\rangle$ is impossible. However, under the entangle-ancilla attack, the state of the composite system of all single photons and auxiliary particles evolves into

$$\begin{aligned} |+\rangle|+\rangle|+\rangle|\epsilon\rangle \rightarrow \frac{1}{2}|+\rangle|+\rangle[|+\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle + |\epsilon_{01}\rangle + |\epsilon_{11}\rangle) \\ + |-\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle - |\epsilon_{01}\rangle - |\epsilon_{11}\rangle)]. \end{aligned} \tag{20}$$

Therefore, the probability of being detected under Alice and Bob's entangle-ancilla attack, i.e., David's probability of getting $|\Phi_0^-\rangle$ is

$$P_d(|+++\rangle) = \frac{1}{16}\left(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle - |\epsilon_{01}\rangle - |\epsilon_{11}\rangle|^2\right), \tag{21}$$

where $|X|^2 = X^+X$. In order not to be detected, we should let $P_d(|+++\rangle) = 0$ and $P_{nd}(|0\rangle) = P_{nd}(|1\rangle) = P_{nd}(|+\rangle) = P_{nd}(|-\rangle) = 1$. We can deduce that $|\epsilon_{01}\rangle = |\epsilon_{10}\rangle = 0$. This means that Alice and Bob's auxiliary particle and Alice, Bob and Charlie's single photons must be in the tensor product state. So, Alice and Bob cannot obtain the information on Charlie's single photon state.

Finally, we consider another possible attack strategy, that is, when Charlie chooses a subset of photons as decoy photons, Alice and Bob deliberately declare their bases differently. In this case, Charlie could not successfully implement security detection. However, if Alice and Bob adopt such strategy for all the decoy photons, Charlie will find the occurrence of abnormal behaviors. For a decoy photon, the probability that Alice's base and Bob's base are different is 1/2. If the number of decoy photons is m, the probability of Alice and Bob's base inconsistency is $\frac{1}{2^m}$ for all m decoy photons. When m is large, the probability of such occurrence is negligible. Charlie will detect the occurrence of this abnormal behavior.

3.3 Security

The proposed MDI-QKA protocol uses the post-selected GHZ state to generate the negotiation key when the three-photon state of Alice, Bob and Charlie is $|0\rangle|0\rangle|0\rangle$ or $|1\rangle|1\rangle|1\rangle$. To obtain the negotiation key, the external eavesdropper Eve must attack when the three parties send their single-photon states to David. However, because these single-photon states are randomly in one of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, Eve cannot directly intercept and measure these single-photon states without being detected. The most common attack strategy is for Eve to prepare an auxiliary particle $|\epsilon\rangle$ and entangle it with a single photon of a participant such as Alice. Eve can use a similar approach to eavesdrop the single photon states of Bob and Charlie. For simplicity and without loss of generality, assume that Alice, Bob, and Charlie each choose the decoy state $|+\rangle$ for security detection. Without eavesdropping, according to formula (10), if David's implementation of the GHZ state measurement is successful, only $|\Phi_0^+\rangle$ will be obtained while $|\Phi_0^-\rangle$ is impossible. Under Eve's entangle-ancilla attack, the state of the composite system consisting of Alice, Bob and Charlie's single photons and Eve's auxiliary particles will evolve into

$$\begin{aligned} &|+\rangle|+\rangle|+\rangle|\epsilon\rangle|\epsilon\rangle|\epsilon\rangle \\ &\rightarrow \frac{1}{2}[|+\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle + |\epsilon_{01}\rangle + |\epsilon_{11}\rangle) + |-\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle \\ &- |\epsilon_{01}\rangle - |\epsilon_{11}\rangle)]\frac{1}{2}[|+\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle + |\epsilon_{01}\rangle + |\epsilon_{11}\rangle) + |-\rangle(|\epsilon_{00}\rangle \\ &+ |\epsilon_{10}\rangle - |\epsilon_{01}\rangle - |\epsilon_{11}\rangle)]\frac{1}{2}[|+\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle + |\epsilon_{01}\rangle + |\epsilon_{11}\rangle) \\ &+ |-\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle - |\epsilon_{01}\rangle - |\epsilon_{11}\rangle)] \\ &= \frac{1}{8}[|+\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle + |\epsilon_{01}\rangle + |\epsilon_{11}\rangle) + |-\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle - |\epsilon_{01}\rangle - |\epsilon_{11}\rangle)] \\ &\times [|+\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle + |\epsilon_{01}\rangle + |\epsilon_{11}\rangle) + |-\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle - |\epsilon_{01}\rangle - |\epsilon_{11}\rangle)] \\ &\times [|+\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle + |\epsilon_{01}\rangle + |\epsilon_{11}\rangle) + |-\rangle(|\epsilon_{00}\rangle + |\epsilon_{10}\rangle - |\epsilon_{01}\rangle - |\epsilon_{11}\rangle)] \\ &= \frac{1}{8}(|+\rangle A + |-\rangle B)(|+\rangle A + |-\rangle B)|) \\ &= \frac{1}{8}[(|+\rangle|+\rangle|+\rangle AAA + |+\rangle|-\rangle|-\rangle ABB + |-\rangle|+\rangle|-\rangle BAB + |-\rangle|-\rangle| \\ &+\rangle BBA) + (|+\rangle|+\rangle|-\rangle AAB + |+\rangle|-\rangle|+\rangle ABA + |-\rangle|+\rangle| \\ &+\rangle BAA + |-\rangle|-\rangle|-\rangle BBB)], \end{aligned} \tag{22}$$

where $A = |\epsilon_{00}\rangle + |\epsilon_{10}\rangle + |\epsilon_{01}\rangle + |\epsilon_{11}\rangle$, $B = |\epsilon_{00}\rangle + |\epsilon_{10}\rangle - |\epsilon_{01}\rangle - |\epsilon_{11}\rangle$.

Then the probability that Eve is detected, that is, David's probability of getting $|\Phi_0^-\rangle$ is

$$P_d(|+++\rangle) = \frac{1}{256}\left(|AAB|^2 + |ABA|^2 + |BAA|^2 + |BBB|^2\right). \tag{23}$$

In order not to be detected, we let $P_d(|+++\rangle) = 0$ and $P_{nd}(|0\rangle) = P_{nd}(|1\rangle) = P_{nd}(|+\rangle) = P_{nd}(|-\rangle) = 1$. We can deduce $|\epsilon_{01}\rangle = |\epsilon_{10}\rangle = 0$. This means that Eve's auxiliary particle and Alice, Bob and Charlie's single photons must be in the tensor product state. So, Eve cannot obtain any information on the key by measuring the auxiliary particle.

Consider another scenario where the untrusted relay David tries to obtain the raw key K'. When David gets the measurement result $|\Phi_0^+\rangle$ or $|\Phi_0^-\rangle$, the states of Alice, Bob and Charlie are in $|0\rangle|0\rangle|0\rangle$ and $|1\rangle|1\rangle|1\rangle$ with equal probability according to formulas (2) and (9). Therefore, David cannot obtain any information on the raw key K'.

4 Generalization to the *n*-party

The above three-party protocol can be easily extended to the *n*-party one. Suppose that the *n* participants Alice_1, Alice_2, . . . , Alice_n ($n > 3$) want to jointly negotiate a key *K*. David is the untrusted relay for implementing GHZ state measurements. The process of the *n*-party MDI-QKA protocol is described as follows.

(1) Alice_1, Alice_2, . . . , Alice_n independently prepare a single-photon sequence $S_{A1}, S_{A2}, \ldots, S_{An}$, respectively. Every single photon in the sequence is randomly in state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sent to the relay David via the quantum channel.
(2) David performs *n*-particle GHZ state measurements on the received photons at the same positions in the *n* sequences and publishes the results of his measurements.
(3) Alice_1, Alice_2, . . . , Alice_n randomly select the photon subset successfully measured by David as the decoy photons, notify the other *n*-1 parties of the location of the photon subset and ask them to announce their decoy photon states. They discard the positions with different preparation bases of the *n* parties. When the bases are the same, they check whether the correlation between the *n* parties' decoy photon states and David's GHZ state measurements is satisfied. If the error rate is higher than the preset value, they will terminate the protocol, otherwise continue to the next step.
(4) After all participants complete the eavesdropping detection, they publish the base information of their remaining single photon states corresponding to the GHZ state measurements successfully performed by David. Finally, the *n* participants choose the states in Z basis to generate the raw key K'.
(5) Alice_1, Alice_2, . . . , Alice_n generate the final key *K* by performing error correction and privacy amplification on the raw key K'.

5 Discussion and conclusion

Since both Cai et al.'s protocol (Cai et al., 2022) and the proposed one are based on GHZ-states, we will clarify the difference between them and why the proposed one is more "secure". In Cai et al. protocol, the participant Charlie needs to implement Z-basis or X-basis measurement on his Greenberger-Horne-Zeinger (GHZ) particle *c*, where the Z-basis measurement result is just the agreement key. However, if an external eavesdropper manipulates Charlie's measurement device, Charlie's measurement device may leak his Z-basis measurement result, i.e., the agreement key to the external eavesdropper, thus threatening the security of the MDI-QKA protocol.

In contrast, the proposed protocol exploits the post-selected GHZ states to generate a secure agreement key between legitimate participants. In our protocol, the measurement device is treated as a black box. David takes charge of performing GHZ state measurement and publishing the GHZ state measurement result. The participants prepare a single photon sequence separately, and every single photon is randomly in state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. When David successfully implements GHZ state measurement and all the participants choose the Z bases on the instances, the states combinations prepared by the participants are only $|0\rangle|0\rangle|0\rangle$ and $|1\rangle|1\rangle|1\rangle$ with equal probability. The agreement key is just the subkeys of the participants. So, even if the eavesdropper obtains the GHZ state measurement result, as long as he does not conspire with the participant, he will not be able to obtain the agreement key. Therefore, the proposed protocol is more secure than that of Cai et al.

One main difference between MDI-QKD and MDI-QKA is that in MDI-QKD, all the participants except the untrusted third party are honest while in MDI-QKA, not all the participants are honest. As we know, fairness is one of the conditions required for an MDI-QKA protocol. Fairness in QKA means that all participants have equal influence on the agreement key, that is, any non-trivial subset of participants cannot determine the agreement key alone. In contrast, fairness is not required for MDI-QKD. Only the security against outsider eavesdroppers is taken into account in an MDI-QKD protocol.

Yang et al. (2022), a detector-device-independent (DDI) QKA (DDI-QKA) protocol was proposed based on single-photon Bell-state measurement. Only the time-bin and path encoding are needed. Complete Bell-state measurement can be achieved based on the time-bin and path. It is implemented with linear optical elements only and thus it is feasible with current technology. In this paper, a multi-party MDI-QKA protocol is proposed. The protocol exploits the post-selected GHZ states to generate a secure agreement key between legitimate participants, while ensuring the fairness of key agreement. Only GHZ state measurements and the single photon state are required, making the operation simple.

In this paper, we propose a new MDI-QKA protocol that removes all detector-side channels. We discuss the efficiency of generating secret keys for this protocol. Regardless of eavesdropping detection, the raw key of the protocol is generated when the participants select the Z-basis, while the single photon for each individual is randomly selected from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and the probability of selecting the Z-basis is $\frac{1}{2}$. For the three-party protocol, the probability that the participants all pick Z-basis is $(\frac{1}{2})^3 = 12.5\%$. When extended to *n*-party users, the probability will be $(\frac{1}{2})^n$. It is obvious to see that the raw key rate generated decreases significantly when the number of participants increases, which is lower than the existing QKA protocols (Tsai and Hwang, 2009; Chong and Hwang, 2010; Liu et al., 2013a; Shi and Zhong, 2013; He and Ma, 2015; Sun et al., 2016; He and Ma, 2017; Mohajer and Eslami, 2017; Wang et al., 2017; Yang et al., 2019b; Li and Li, 2020; Naresh et al., 2020; Naresh and Reddi, 2020; Zhou et al., 2020; Zhu et al., 2021a; Zhu et al., 2021b; Huang et al., 2021; Lin et al., 2021; Yang et al., 2022). Similar to the protocol of Cai et al., the actual efficiency of the protocol will be lower if channel loss and compression are considered. Therefore, the future work will focus on how to improve the efficiency of the MDI-QKA protocol to enhance its practicality. Since the implementation of the protocol is inevitably affected by noise, the threshold value for the error rate should be

provided before implementing it. However, in this paper, no exact threshold value is given, which is also the case for many multiparty quantum cryptography protocols and becomes an open problem. Combined with quantum state discrimination, we will study this problem in the future.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

B-XL: Conceptualization, Methodology, Writing—Original draft preparation. R-CH: Security analysis. Y-GY: Supervision, Writing—Reviewing and Editing. G-BX: Writing—Reviewing and Editing.

Funding

This work is supported by the National Natural Science Foundation of China (Grant Nos. 62071015, 62171264).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Bennett, C. H., and Brassard, G. (1984). "Quantum cryptography: Public key distribution and coin tossing," in *Proceed IEEE int conf comput, syst signal process* (New York: IEEE), 175–179.

Boström, K., and Felbinger, T. (2002). Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.* 89, 187902. doi:10.1103/physrevlett.89.187902

Cai, X. Q., Liu, Z. F., Wei, C. Y., and Wang, T. Y. (2022). Long distance measurement-device-independent three-party quantum key agreement. *Phys. A* 607, 128226. doi:10.1016/j.physa.2022.128226

Chen, X. B., Xu, G., Niu, X. X., Wen, Q. Y., and Yang, Y. X. (2010). An efficient protocol for the private comparison of equal information based on the triplet entangled state and single particle measurement. *Opt. Commun.* 283 (7), 1561–1565. doi:10.1016/j.optcom.2009.11.085

Chong, S. K., and Hwang, T. (2010). Quantum key agreement protocol based on BB84. *Opt. Commun.* 283, 1192–1195. doi:10.1016/j.optcom.2009.11.007

Deng, F. G., Long, G. L., and Liu, X. S. (2003). Two-step quantum direct communication protocol using the EinsteinPodolsky-Rosen pair block. *Phys. Rev. A* 68, 042317. doi:10.1103/physreva.68.042317

Diffie, W., and Hellman, M. E. (1976). New directions in cryptography. *IEEE Trans. Inf. Theory* IT-22 (6), 644–654. doi:10.1109/tit.1976.1055638

Dušek, M., Haderka, O., Hendrych, M., and Myska, R. (1999). Quantum identification system. *Phys. Rev. A* 60, 149–156. doi:10.1103/physreva.60.149

Fan-Yuan, G. J., Lu, F. Y., Wang, S., Yin, Z. Q., He, D. Y., Chen, W., et al. (2022). Robust and adaptable quantum key distribution network without trusted nodes. *Optica* 9 (7), 812–823. doi:10.1364/optica.458937

Fan-Yuan, G. J., Lu, F. Y., Wang, S., Yin, Z. Q., He, D. Y., Zhou, Z., et al. (2021). Measurement-device-independent quantum key distribution for nonstandalone networks. *Photonics Res.* 9 (10), 1881–1891. doi:10.1364/prj.428309

Ferreira da Silva, T., Vitoreti, D., Xavier, G. B., do Amaral, G. C., Temporão, G. P., and von der Weid, J. P. (2013). Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* 88, 052303. doi:10.1103/physreva.88.052303

Gao, F., Liu, B., Huang, W., and Wen, Q. Y. (2015). Postprocessing of the oblivious key in quantum private query. *Ieee. J. Sel. Top. Quant.* 21, 98–108. doi:10.1109/jstqe.2014.2358192

Gao, F., Liu, B., Wen, Q.-Y., and Chen, H. (2012). Flexible quantum private queries based on quantum key distribution. *Opt. Exp.* 20, 17411–17420. doi:10.1364/oe.20.017411

Gao, F., Qin, S. J., Huang, W., and Wen, Q. Y. (2019). Quantum private query: A new kind of practical quantum cryptographic protocols. *Sci. China-Phys. Mech. Astron.* 62, 070301.

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. *Rev. Mod. Phys.* 74, 145–195. doi:10.1103/revmodphys.74.145

He, Y. F., and Ma, W. P. (2015). Quantum key agreement protocols with four-qubit cluster states. *Quantum Inf. Process* 14, 3483–3498. doi:10.1007/s11128-015-1060-7

He, Y. F., and Ma, W. P. (2017). Two-party quantum key agreement with five-particle entangled states. *Int. J. Quantum Inf.* 15 (03), 1750018. doi:10.1142/s0219749917500186

Huang, X., Zhang, S. B., Chang, Y., Qiu, C., Liu, D. M., and Hou, M. (2021). Quantum key agreement protocol based on quantum search algorithm. *Int. J. Theor. Phys.* 60, 838–847. doi:10.1007/s10773-020-04703-x

Li, L., and Li, Z. (2020). A verifiable multiparty quantum key agreement based on bivariate polynomial. *Inf. Sci.* 521, 343–349. doi:10.1016/j.ins.2020.02.057

Lin, J., and Lütkenhaus, N. (2018). Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* 98, 042332. doi:10.1103/physreva.98.042332

Lin, S., Zhang, X., Guo, G. D., Wang, L. L., and Liu, X. F. (2021). Multiparty quantum key agreement. *Phys. Rev. A* 104, 042421. doi:10.1103/physreva.104.042421

Liu, B., Gao, F., Huang, W., and Wen, Q. Y. (2013). Multiparty quantum key agreement with single particles. *Quantum Inf. Process* 12, 1797–1805. doi:10.1007/s11128-012-0492-6

Liu, Y., Chen, T. Y., Wang, L. J., Liang, H., Shentu, G. L., Wang, J., et al. (2013). Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* 111, 130502. doi:10.1103/physrevlett.111.130502

Lo, H. K., Curty, M., and Qi, B. (2012). Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* 108, 130503. doi:10.1103/physrevlett.108.130503

Lucamarini, M., Yuan, Z., Dynes, J., and Shields, A. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* 557, 400–403. doi:10.1038/s41586-018-0066-6

Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Phot.* 4 (10), 686–689. doi:10.1038/nphoton.2010.214

Ma, X., Zeng, P., and Zhou, H. (2018). Phase-matching quantum key distribution. *Phys. Rev. X* 8, 031043. doi:10.1103/physrevx.8.031043

Makarov, V. (2009). Controlling passively quenched single photon detectors by bright light. *New J. Phys.* 11, 065003. doi:10.1088/1367-2630/11/6/065003

Mohajer, R., and Eslami, Z. (2017). Cryptanalysis of a multiparty quantum key agreement protocol based on commutative encryption. *Quantum Inf. Process* 16 (8), 197. doi:10.1007/s11128-017-1647-2

Naresh, V. S., Nasralla, M. M., Reddi, S., and García-Magariño, I. (2020). Quantum Diffie-Hellman extended to dynamic quantum group key agreement for e-Healthcare multi-agent systems in smart cities. *Sensors* 20 (14), 3940. doi:10.3390/s20143940

Naresh, V. S., and Reddi, S. (2020). Multiparty quantum key agreement with strong fairness property. *Comput. Syst. Sci. Eng.* 35 (6), 457–465. doi:10.32604/csse.2020.35.457

Pan, J., and Zeilinger, A. (1998). Greenberger-Horne-Zeilinger-state analyzer. *Phys. Rev. A* 57, 2208–2211. doi:10.1103/physreva.57.2208

Qi, B., Fung, C. H. F., Lo, H. K., and Ma, X. (2007). Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* 7, 73–82. doi:10.26421/qic7.1-2-3

Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I., and Tittel, W. (2013). Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* 111, 130501. doi:10.1103/physrevlett.111.130501

Shi, R. H., and Zhong, H. (2013). Multi-party quantum key agreement with Bell states and Bell measurements. *Quantum Inf. Process* 12, 921–932. doi:10.1007/s11128-012-0443-2

Sun, Z., Huang, J., and Wang, P. (2016). Efficient multiparty quantum key agreement protocol based on commutative encryption. *Quantum Inf. Process* 15 (5), 2101–2111. doi:10.1007/s11128-016-1253-8

Tang, Y. L., Yin, H. L., Zhao, Q., Liu, H., Sun, X. X., Huang, M. Q., et al. (2016). Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* 6, 011024. doi:10.1103/physrevx.6.011024

Tsai, C., and Hwang, T. (2009). *On quantum key agreement protocol*. C-S-I-E, NCKU, Taiwan: Technical Report.

Wang, P., Sun, Z., and Sun, X. (2017). Multi-party quantum key agreement protocol secure against collusion attacks. *Quantum Inf. Process* 16, 170. doi:10.1007/s11128-017-1621-z

Wang, S., Yin, Z. Q., He, D. Y., Chen, W., Wang, R. Q., Ye, P., et al. (2022). Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* 16 (2), 154–161. doi:10.1038/s41566-021-00928-2

Wang, X. B., Yu, Z. W., and Hu, X. L. (2018). Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* 98, 062323. doi:10.1103/physreva.98.062323

Wei, C. Y., Wang, T. Y., and Gao, F. (2016). Practical quantum private query with better performance in resisting joint-measurement attack. *Phys. Rev. A* 93, 042318. doi:10.1103/physreva.93.042318

Woodward, R. I., Lo, Y. S., Pittaluga, M., Minder, M., Paraïso, T. K., Lucamarini, M., et al. (2021). Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers. *npj Quantum Inf.* 7, 58. doi:10.1038/s41534-021-00394-2

Xu, F., Ma, X., Zhang, Q., Lo, H. K., and Pan, J. W. (2020). Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* 92, 025002. doi:10.1103/revmodphys.92.025002

Yang, Y. G., Li, B. R., Kang, S. Y., Chen, X. B., Zhou, Y. H., and Shi, W. M. (2019). New quantum key agreement protocols based on cluster states. *Quantum Inf. Process* 18, 77. doi:10.1007/s11128-019-2200-2

Yang, Y. G., Lv, X. L., Gao, S., Zhou, Y. H., and Shi, W. M. (2022). Detector-device-independent quantum key agreement based on single-photon Bell state measurement. *Int. J. Theor. Phys.* 61 (2), 50. doi:10.1007/s10773-022-05052-7

Yang, Y.-G., Guo, X.-P., Xu, G., Chen, X.-B., Li, J., Zhou, Y.-H., et al. (2019). Reducing the communication complexity of quantum private database queries by subtle classical post-processing with relaxed quantum ability. *Comput. Secur.* 81, 15–24. doi:10.1016/j.cose.2018.08.012

Yang, Y.-G., Lei, H., Liu, Z.-C., Zhou, Y.-H., and Shi, W.-M. (2016). Arbitrated quantum signature scheme based on cluster states. *Quantum Inf. process.* 15 (6), 2487–2497. doi:10.1007/s11128-016-1293-0

Yang, Y.-G., Liu, Z.-C., Chen, X.-B., Zhou, Y.-H., and Shi, W.-M. (2017). Robust QKD-based private database queries based on alternative sequences of single-qubit measurements. *Sci. Chin. Phys. Mech. Astron.* 60 (12), 120311. doi:10.1007/s11433-017-9085-0

Yang, Y.-G., Liu, Z.-C., Li, J., Chen, X.-B., Zuo, H.-J., Zhou, Y.-H., et al. (2016). Quantum private query with perfect user privacy against a joint-measurement attack. *Phys. Lett. A* 380 (48), 4033–4038. doi:10.1016/j.physleta.2016.10.017

Yang, Y.-G., Liu, Z.-C., Li, J., Chen, X.-B., Zuo, H.-J., Zhou, Y.-H., et al. (2017). Theoretically extensible quantum digital signature with starlike cluster states. *Quantum Inf. process.* 16 (1), 12–15. doi:10.1007/s11128-016-1458-x

Yang, Y.-G., Liu, Z. C., Chen, X. B., Cao, W. F., Zhou, Y. H., and Shi, W. M. (2016). Novel classical post-processing for quantum key distribution-based quantum private query. *Quantum Inf. process.* 15, 3833–3840. doi:10.1007/s11128-016-1367-z

Yang, Y.-G., Sun, S.-J., Xu, P., and Tian, J. (2014). Flexible protocol for quantum private query based on B92 protocol. *Quantum Inf. process.* 13, 805–813. doi:10.1007/s11128-013-0692-8

Yang, Y. G., Cao, W. F., and Wen, Q. Y. (2009). Secure quantum private comparison. *Phys. Scr.* 80 (6), 065002. doi:10.1088/0031-8949/80/06/065002

Yang, Y. G., and Wen, Q. Y. (2009). An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J. Phys. A Math. Theor.* 42 (5), 055305. doi:10.1088/1751-8113/42/5/055305

Zeng, P., Zhou, H. Y., Wu, W. J., and Ma, X. F. (2022). Mode-pairing quantum key distribution. *Nat. Commun.* 13, 3903. doi:10.1038/s41467-022-31534-7

Zhou, N. R., Zhu, K. N., and Wang, Y. Q. (2020). Three-party semi-quantum key agreement protocol. *Int. J. Theor. Phys.* 59, 663–676. doi:10.1007/s10773-019-04288-0

Zhou, N., Zeng, G., and Xiong, J. (2004). Quantum key agreement protocol. *Electron Lett.* 40, 1149. doi:10.1049/el:20045183

Zhu, H. F., Liu, T. H., and Wang, C. N. (2021). A one-round quantum mutual authenticated key agreement protocol with semi-honest server using three-particle entangled states. *Int. J. Theor. Phys.* 60, 929–943. doi:10.1007/s10773-021-04716-0

Zhu, H. F., Wang, C. N., and Li, Z. X. (2021). Semi-honest three-party mutual authentication quantum key agreement protocol based on GHZ-like state. *Int. J. Theor. Phys.* 60, 293–303. doi:10.1007/s10773-020-04692-x