Frontiers of Physics
https://doi.org/10.1007/s11467-020-1005-1
Front. Phys.
16(1), 11501 (2021)

RESEARCH ARTICLE

Measurement-device-independent quantum key distribution of multiple degrees of freedom of a single photon

Yu-Fei Yan[1], Lan Zhou[2], Wei Zhong[1,3], Yu-Bo Sheng[1,3,†]

[1] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
[2] *Schoool of Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
[3] *Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
Corresponding author. E-mail: [†] *shengyb@njupt.edu.cn*
Received July 20, 2020; accepted August 22, 2020

Measurement-device-independent quantum key distribution (MDI-QKD) provides us a powerful approach to resist all attacks at detection side. Besides the unconditional security, people also seek for high key generation rate, but MDI-QKD has relatively low key generation rate. In this paper, we provide an efficient approach to increase the key generation rate of MDI-QKD by adopting multiple degrees of freedom (DOFs) of single photons to generate keys. Compared with other high-dimension MDI-QKD protocols encoding in one DOF, our protocol is more flexible, for our protocol generating keys in independent subsystems and the detection failure or error in a DOF not affecting the information encoding in other DOFs. Based on above features, our MDI-QKD protocol may have potential application in future quantum communication field.

Keywords measurement-device-independent quantum key distribution, polarization, longitudinal-momentum, key generation rate

1 Introduction

Since the Bennett–Brassard-1984 (BB84) quantum key distribution (QKD) protocol [1] was proposed, quantum secure communication based on QKD has experienced a long-term development, which has become an interesting research area in both theory and experiment [2–16]. Throughout the whole development process of QKD, there are always struggle between attack and anti-attack strategies, which focus on the discrepancy between perfect theory and practice [17]. Although QKD is absolutely secure in theory, in reality, due to the imperfect measurement devices and quantum signal source, QKD system cannot guarantee the unconditional security of keys in practical condition. For example, practical photon detectors are vulnerable to various types of attacks such as the time-shift attacks [18–20], detection blinding attacks [21], beam-splitter attack [22, 23] and fate-stack attacks [24, 25]. In addition, eavesdroppers can also take use of imperfect quantum signal sources to perform attack [26, 27], such as the photon-number-splitting (PNS) attack [28]. The problem from PNS attack can be solved by the decoy state method [29–32].

In 2007, Acín group first put forward the device-independent QKD (DI-QKD) protocol [33]. DI-QKD does not require detailed knowledge of how devices work and ensures the security based on the violation of Bell inequality. DI-QKD can defend all possible attacks from imperfect experimental devices. However, DI-QKD requires quite high detection efficiency, which limits its secure communication distance to be less than 5 km [34–36]. In 2012, the group of Lo proposed the concept measurement-device-independent QKD (MDI-QKD), which is immune to all possible attacks from measurement devices [37]. In MDI-QKD, Alice and Bob prepare single photons randomly in one of two bases and send the encoding photons to a third party (Charlie). Charlie performs a Bell-state analysis (BSA) on them and publishes his result. Here, Charlie needs not to be trusted and can even be completely controlled by the eavesdropper. Combined with the decoy state method, the MDI-QKD can resist all the possible attacks from imperfect photon source and measurement devices. During the past few years, MDI-QKD has well developed [38–46]. For example, in 2016, Yin *et al.* reported results for MDI-QKD over 404 km of ultralow-loss optical fiber and 311 km of standard optical fiber [44]. Besides security, practical application requires

*arXiv: 2009.09555. This article can also be found at http://journal.hep.com.cn/fop/EN/10.1007/s11467-020-1005-1.

© Higher Education Press 2021

high key generation rate. However, comparing with other QKD forms, MDI-QKD has relatively low key generation rate. Increasing single photon's capacity is important for increasing MDI-QKD's key generation rate. In general, there are two methods to increase single photon's capacity. The first one is the high-dimension (HD) encoding in one degree of freedom (DOF) [47–59]. In 2016, the group of Chau proposed the first qudit-based MDI-QKD protocol using linear optics [53]. In 2018, Dellantonio *et al.* designed two HD MDI-QKD protocols based on spatial-encoding and temporal-encoding multi-mode qudits, respectively [56]. The other one is the hyper-encoding in multiple DOFs [60–62]. For hyper-encoding, information is simultaneously encoded in multiple DOFs of a quantum system. The information encoding in different DOFs are independent with each other. The single photons encoded in multiple DOFs have also been used to realize high-capacity quantum communication, such as high-capacity quantum teleportation [63], high-capacity dense coding [64], and high-capacity quantum secure direct communication [65–67].

In this protocol, we propose a general method to increase MDI-QKD's key generation rate by adopting the qudits encoding in multiple DOFs to generate keys. We take the qudits encoding in polarization and two longitudinal momentum DOFs for example, which have been experimentally generated [68]. In this protocol, both Alice and Bob encode their photons in three DOFs independently and send the encoded photons to Charlie for the hyperentanglement Bell state analysis (HBSA). In our MDI-QKD protocol, the encoding information in all DOFs can be used to generate the secure key, so that it can effectively increase MDI-QKD's key generation rate. Each DOF can be manipulated independently and they do not influence each other. We will prove that our MDI-QKD protocol is unconditionally secure and calculate its key generation rate. Our MDI-QKD protocol has big application potential in future quantum secure communication field.

The structure of the paper is organized as follows. In Section 2, we explain MDI-QKD protocol based on the qudits encoding in polarization and two longitudinal momentum DOFs. In Section 3, we make the security analysis of our MDI-QKD protocol and evaluate its key generation rate. In Section 4, we give a discussion. In Section 5, we make a conclusion.

2 The MDI-QKD protocol adopting three DOFs of single photons

Before we begin our protocol, we first introduce our encoding rules in three DOFs. In each DOF, Alice and Bob use two sets of bases, say, rectilinear base and diagonal base. In the polarization DOF, the rectilinear base is $\{|H\rangle, |V\rangle\}$, where $|H\rangle$ and $|V\rangle$ denote horizontal and vertical polarizations, respectively. The diagonal base is $\{|+\rangle_p = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |-\rangle_p = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$. In the first longitudinal-momentum DOF, the rectilinear base is $\{|L\rangle,|R\rangle\}$, where $|L\rangle$ and $|R\rangle$ represent the left and right spatial modes. The diagonal base includes $\{|+\rangle_f = \frac{1}{\sqrt{2}}(|L\rangle + |R\rangle), |-\rangle_f = \frac{1}{\sqrt{2}}(|L\rangle - |R\rangle)\}$. In the second longitudinal-momentum DOF, the rectilinear base is $\{|I\rangle,|E\rangle\}$ and the diagonal base is $\{|+\rangle_s = \frac{1}{\sqrt{2}}(|I\rangle + |E\rangle), |-\rangle_s = \frac{1}{\sqrt{2}}(|I\rangle - |E\rangle)\}$, where $|I\rangle$ and $|E\rangle$ represent the internal and external spatial modes, respectively. In polarization DOF, $|H\rangle$ and $|+\rangle_p$ represent the binary value 0 while $|V\rangle$ and $|-\rangle_p$ represent the binary value 1. In the first (second) longitudinal-momentum DOF, $|L(I)\rangle$ and $|+\rangle_{f(s)}$ represent 0 while $|R(E)\rangle$ and $|-\rangle_{f(s)}$ represent 1.

The basic principle of our MDI-QKD protocol is shown in Fig. 1, whose procedure can be described as follows.

Step 1: Alice and Bob separately prepare single photons from single photon sources (SPSs). First, they make the single photons pass through polarization modulators (Pol-Ms) to realize the encoding in polarization DOF. In Figs. 1(a) and (b), we show the generation principle of qudits in rectilinear and diagonal bases in both longitudinal momentum DOFs, respectively. BS means the 50:50 beam splitter and acts as the Hadamard gate in two longitudinal-momentum DOFs. It can convert $|L\rangle$ into $|+\rangle_f$, $|R\rangle$ into $|-\rangle_f$, $|I\rangle$ into $|+\rangle_s$, and $|E\rangle$ into $|-\rangle_s$. Here, we give a simple example for the generation of qudits in the diagonal base of both two longitudinal-momentum DOFs. As shown in Fig. 1(b), if Alice (Bob) wants to generate $|+\rangle_f \otimes |+\rangle_s$, she (he) first prepares a single photon in the spatial momentum $|L\rangle|E\rangle$. Then, after passing the photon successively through $BS_{2A(B)}$, $BS_{3A(B)}$, and $BS_{4A(B)}$, the photon state $|L\rangle|E\rangle$ will finally evolve to $|+\rangle_f \otimes |+\rangle_s$. In this way, Alice and Bob can prepare single-photon qudits encoding in three DOFs. For instance, if Alice's encoding key is 000, there are totally eight possible states that Alice can prepare, say, $|H\rangle \otimes |L\rangle \otimes |I\rangle$, $|H\rangle \otimes |L\rangle \otimes |+\rangle_s$, $|H\rangle \otimes |+\rangle_f \otimes |I\rangle$, $|H\rangle \otimes |+\rangle_f \otimes |+\rangle_s$, $|+\rangle_p \otimes |L\rangle \otimes |I\rangle$, $|+\rangle_p \otimes |L\rangle \otimes |+\rangle_s$, $|+\rangle_p \otimes |+\rangle_f \otimes |I\rangle$, and $|+\rangle_p \otimes |+\rangle_f \otimes |+\rangle_s$. After encoding, Alice and Bob send their qudits to a third party Charlie through quantum channels, respectively.

Step 2: After Charlie receiving the photon qudits sent by Alice and Bob, he performs a hyperentangled-Bell-state analysis (HBSA) [69] on the photon pairs, which can completely distinguish the four Bell states in each DOF. The Bell states in three DOFs can be written as

$$|\Phi^{\pm}\rangle_p = \frac{1}{\sqrt{2}}(|H\rangle_a|H\rangle_b \pm |V\rangle_a|V\rangle_b),$$
$$|\Psi^{\pm}\rangle_p = \frac{1}{\sqrt{2}}(|H\rangle_a|V\rangle_b \pm |V\rangle_a|H\rangle_b),$$
$$|\Phi^{\pm}\rangle_f = \frac{1}{\sqrt{2}}(|L\rangle_a|L\rangle_b \pm |R\rangle_a|R\rangle_b),$$
$$|\Psi^{\pm}\rangle_f = \frac{1}{\sqrt{2}}(|L\rangle_a|R\rangle_b \pm |R\rangle_a|L\rangle_b),$$

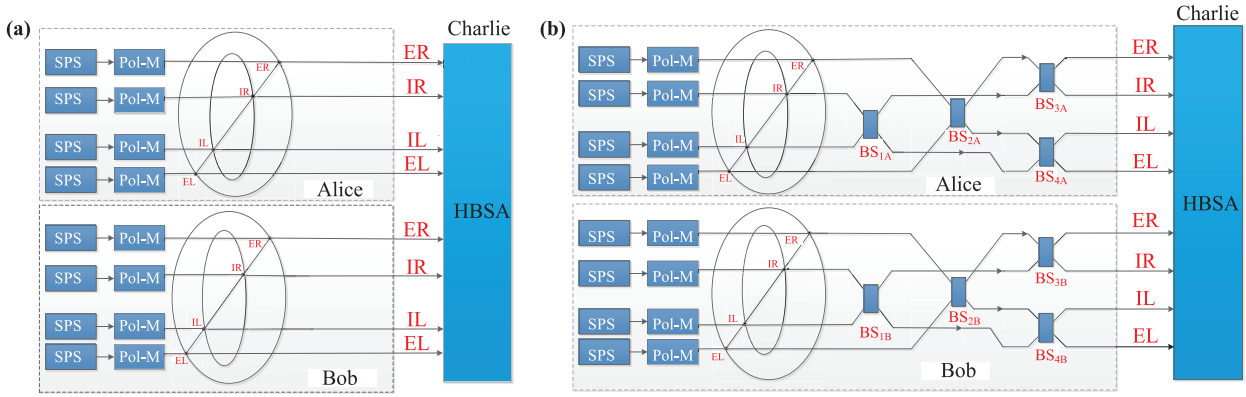


Fig. 1 Schematic diagram of the MDI-QKD protocol adopting three DOFs of single photons. Alice and Bob separately prepare single photons from single photon sources (SPSs). Pol-M is a polarization modulator which is used to implement encoding in polarization DOF. **(a)** and **(b)** represent the encoding in rectilinear and diagonal bases in two longitudinal momentum DOFs, respectively. The BSs are used to perform Hadamard operations in two longitudinal-momentum DOFs. Here, $|L\rangle$ ($|R\rangle$) and $|I\rangle$ ($|E\rangle$) represent the left (right) and internal (external) momentums. After the qudits generation, the qudits from Alice and Bob are sent to Charlie to make the complete hyperentangled-Bell-state analysis (HBSA), which can completely distinguish the four Bell states in each DOF.

$$|\Phi^{\pm}\rangle_s = \frac{1}{\sqrt{2}}(|I\rangle_a|I\rangle_b \pm |E\rangle_a|E\rangle_b),$$
$$|\Psi^{\pm}\rangle_s = \frac{1}{\sqrt{2}}(|I\rangle_a|E\rangle_b \pm |E\rangle_a|I\rangle_b), \quad (1)$$

where the subscript a (b) represents Alice's (Bob's) location. After the measurements, Charlie announces his measurement results in a public channel.

Step 3: Alice and Bob announce the generation bases of all their qudits in all DOFs through public channels. If they select different bases in a DOF, they have to discard the information encoding in this DOF. On the other hand, if they select the same base in a DOF, they can obtain the encoding information for each other in this DOF. Here, we suppose that the key is transmitted from Alice to Bob. To guarantee that their photon strings are correctly correlated, Bob needs to make a post-selection. The post-selection principles in three DOFs are totally the same, which are shown in Table 1. If both they use the rectilinear base in a DOF, Bob has to apply a bit-flip operation to his data corresponding to the measurement result of $|\psi^{\pm}\rangle$, and he keeps his original data corresponding to the measurement result of $|\phi^{\pm}\rangle$. On the other hand, if both they use the diagonal base in a DOF, Bob applies a bit-flip operation to his data corresponding to the measurement result of $|\phi^{-}\rangle$ or $|\psi^{-}\rangle$, and he keeps his original data corresponding to the measurement result of $|\phi^{+}\rangle$ or $|\psi^{+}\rangle$.

Table 1 The post-selection principle of Bob in all DOFs based on the Bell-state measurement (BSM) result and the basis selection.

BSM result	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
Rectilinear basis	–	–	bit flip	bit flip
Diagonal basis	–	bit flip	–	bit flip

Step 4: Alice and Bob repeat steps (1) to (3) until they get enough amount of keys.

Step 5: To ensure the security of the key transmission, Alice and Bob choose the qudits encoding in diagonal bases $\{|+\rangle_p, |-\rangle_p\}$, $\{|+\rangle_f, |-\rangle_f\}$, and $\{|+\rangle_s, |-\rangle_s\}$ to evaluate the quantum bit error rates (QBERs) in three DOFs. In detail, they announce the encoding information in three DOFs over a public channel. This enables them to check Charlie's measurement results by calculating the QBERs in all DOFs. If the QBERs in all DOFs are smaller than the threshold, the key transmission process can be trusted. Otherwise, if the QBER in any DOF is higher than the threshold, the key transmission process has to be abandoned.

Step 6: Alice and Bob perform the error correction and private amplification to complete the generation of final secure keys.

To facilitate understanding, we discuss our protocol in a specific example, where Alice's encoding information is 000 and Bob's encoding information is 101. Here, we neglect the security checking for simplicity. According to the base choice, there are four different cases. In each case, we give an example to illustrate the protocol.

In the first case, the bases in all DOFs of the photons sent by Alice and Bob are the same. We assume that Alice prepares $|H\rangle_a|L\rangle_a|I\rangle_a$ and Bob prepares $|V\rangle_b|L\rangle_b|E\rangle_b$. Under this case, the whole photon state in Charlie's location can be written as

$$\begin{aligned}
&|H\rangle_a|L\rangle_a|I\rangle_a \otimes |V\rangle_b|L\rangle_b|E\rangle_b \\
&= |H\rangle_a|V\rangle_b \otimes |L_a\rangle|L\rangle_b \otimes |I\rangle_a|E\rangle_b \\
&= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_p + |\Psi^-\rangle_p) \otimes \frac{1}{\sqrt{2}}(|\Phi^+\rangle_f + |\Phi^-\rangle_f) \\
&\quad \otimes \frac{1}{\sqrt{2}}(|\Psi^+\rangle_s + |\Psi^-\rangle_s)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2\sqrt{2}}(|\Psi^+\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^+\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^-\rangle_s).
\end{aligned} \tag{2}
$$

According to the measurement results and their base selection, Alice and Bob can know that their encoding in the polarization and second longitudinal-momentum DOFs are opposite and the encoding in the first longitudinal-momentum DOF is same. In this way, Bob only needs to make bit-flip operations in polarization and second longitudinal-momentum DOFs and keeps his original data in the first longitudinal-momentum DOF. Then, he can obtain the encoding keys from Alice.

In the second case, Alice and Bob choose same basis in two DOFs. For example, Alice prepares $|H\rangle_a|L\rangle_a|I\rangle_a$ for 000 and Bob prepares $|V\rangle_b|+\rangle_{fb}|E\rangle_b$ for 101. In this case, the whole photon state at Charlie's side is

$$
\begin{aligned}
&|H\rangle_a|L\rangle_a|I\rangle_a \otimes |V\rangle_b|+\rangle_{fb}|E\rangle_b \\
&= |H\rangle_a|V\rangle_b \otimes |L\rangle_a|+\rangle_{fb} \otimes |I\rangle_a|E\rangle_b \\
&= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_p + |\Psi^-\rangle_p) \otimes \frac{1}{2}(|\Phi^+\rangle_f + |\Phi^-\rangle_f + |\Psi^+\rangle_f \\
&\quad + |\Psi^-\rangle_f) \otimes \frac{1}{\sqrt{2}}(|\Psi^+\rangle_s + |\Psi^-\rangle_s) \\
&= \frac{1}{4}(|\Psi^+\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^+\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^+\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^+\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Psi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Psi^-\rangle_s).
\end{aligned} \tag{3}
$$

In this situation, after the HBSA, Bob can obtain that Alice's encoding in the polarization and second longitudinal-momentum DOFs are opposite with his encoding. However, Bob needs to abandon the information in the first longitudinal momentum DOF. The reason is that the BSA in the first longitudinal-momentum DOF may obtain all the four results with the same probability and Bob may obtain wrong result of Alice's encoding with the probability of 50%.

In the third case, Alice and Bob choose the same base in only one DOF. Assuming that Alice prepares $|H\rangle_a|L\rangle_a|I\rangle_a$ representing 000 and Bob prepares $|V\rangle_b|+\rangle_{fb}|-\rangle_{sb}$ for 101. The HBSA process of the whole photon state can be written as

$$
\begin{aligned}
M &= |H\rangle_a|L\rangle_a|I\rangle_a \otimes |V\rangle_b|+\rangle_{fb}|-\rangle_{sb} \\
&= |H\rangle_a|V\rangle_b \otimes |L\rangle_a|+\rangle_{fb} \otimes |I\rangle_a|-\rangle_{sb} \\
&= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_p + |\Psi^-\rangle_p) \otimes \frac{1}{2}(|\Phi^+\rangle_f + |\Phi^-\rangle_f + |\Psi^+\rangle_f \\
&\quad + |\Psi^-\rangle_f) \otimes \frac{1}{2}(|\Phi^+\rangle_s + |\Phi^-\rangle_s - |\Psi^+\rangle_s - |\Psi^-\rangle_s) \\
&= \frac{1}{4\sqrt{2}}(|\Psi^+\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Phi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Phi^-\rangle_s \\
&- |\Psi^+\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^+\rangle_s - |\Psi^+\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^+\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Phi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Phi^-\rangle_s \\
&- |\Psi^+\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^+\rangle_s - |\Psi^+\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^+\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Phi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Phi^-\rangle_s \\
&- |\Psi^+\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Psi^+\rangle_s - |\Psi^+\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^+\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Phi^+\rangle_s + |\Psi^+\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Phi^-\rangle_s \\
&- |\Psi^+\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Psi^+\rangle_s - |\Psi^+\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Phi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Phi^-\rangle_s \\
&- |\Psi^-\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^+\rangle_s - |\Psi^-\rangle_p \otimes |\Phi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Phi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Phi^-\rangle_s \\
&- |\Psi^-\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^+\rangle_s - |\Psi^-\rangle_p \otimes |\Phi^-\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Phi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Phi^-\rangle_s \\
&- |\Psi^-\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Psi^+\rangle_s - |\Psi^-\rangle_p \otimes |\Psi^+\rangle_f \otimes |\Psi^-\rangle_s \\
&+ |\Psi^-\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Phi^+\rangle_s + |\Psi^-\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Phi^-\rangle_s \\
&- |\Psi^-\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Psi^+\rangle_s - |\Psi^-\rangle_p \otimes |\Psi^-\rangle_f \otimes |\Psi^-\rangle_s).
\end{aligned} \tag{4}
$$

It is obvious that Bob can only obtain Alice's encoding in the polarization DOF after the bit-flip operation.

In the last case, Alice and Bob choose different bases in all DOFs. For example, Alice prepares $|H\rangle_a|L\rangle_a|I\rangle_a$ state and Bob prepares $|-\rangle_{pb}|+\rangle_{fb}|-\rangle_{sb}$. In this case, they have to abandon the two photons.

The possible BSA results and Bob's post-selection operations in three DOFs are described in Table 2, Table 3, and Table 4, respectively.

3 The key generation rate of the MDI-QKD in 3DOFs

In this section, we discuss the security and key generation rate of our MDI-QKD protocol adopting three DOFs of single qudits. Our MDI-QKD protocol is based on the original MDI-QKD protocol from Lo *et al.* [37]. In our MDI-QKD protocol, Alice and Bob use the single photons combined with Pol-Ms and BSs to prepare the signal photon qudits and send them to Charlie to make the HBSA. According to the security proof of the original MDI-QKD protocol, the security proof of our protocol is also based on that of the time-reversed EPR-based QKD protocol [70].

In theory, the encoding space of our MDI-QKD protocol includes three essentially independent subspaces. In ideal scenario, say, ideal single photon sources and quan-

Table 2 Possible BSA results and Bob's post-selection operation in polarization DOF.

Bit data		BSA results and probabilities				Whether or not to bit-flip
Alice	Bob	$\|\phi^+\rangle_p$	$\|\phi^-\rangle_p$	$\|\psi^+\rangle_p$	$\|\psi^-\rangle_p$	
$\|H\rangle$	$\|H\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	–
$\|H\rangle$	$\|V\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	bit-flip
$\|V\rangle$	$\|H\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	bit-flip
$\|V\rangle$	$\|V\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	–
$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	–
$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	bit flip
$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	bit flip
$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	–

Table 3 Possible BSA results and Bob's post-selection operation in the first longitudinal-momentum DOF.

Bit data		BSA results and probabilities				Whether or not to bit-flip
Alice	Bob	$\|\phi^+\rangle_f$	$\|\phi^-\rangle_f$	$\|\psi^+\rangle_f$	$\|\psi^-\rangle_f$	
$\|L\rangle$	$\|L\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	–
$\|L\rangle$	$\|R\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	bit-flip
$\|R\rangle$	$\|L\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	bit-flip
$\|R\rangle$	$\|R\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	–
$\frac{1}{\sqrt{2}}(\|L\rangle+\|R\rangle)$	$\frac{1}{\sqrt{2}}(\|L\rangle+\|R\rangle)$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	–
$\frac{1}{\sqrt{2}}(\|L\rangle+\|R\rangle)$	$\frac{1}{\sqrt{2}}(\|L\rangle-\|R\rangle)$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	bit flip
$\frac{1}{\sqrt{2}}(\|L\rangle-\|R\rangle)$	$\frac{1}{\sqrt{2}}(\|L\rangle+\|R\rangle)$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	bit flip
$\frac{1}{\sqrt{2}}(\|L\rangle-\|R\rangle)$	$\frac{1}{\sqrt{2}}(\|L\rangle-\|R\rangle)$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	–

Table 4 Possible BSA results and Bob's post-selection operation in the second longitudinal-momentum DOF.

Bit data		BSA results and probabilities				Whether or not to bit-flip
Alice	Bob	$\|\phi^+\rangle_s$	$\|\phi^-\rangle_s$	$\|\psi^+\rangle_s$	$\|\psi^-\rangle_s$	
$\|I\rangle$	$\|I\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	–
$\|I\rangle$	$\|E\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	bit-flip
$\|E\rangle$	$\|I\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	bit-flip
$\|E\rangle$	$\|E\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	–
$\frac{1}{\sqrt{2}}(\|I\rangle+\|E\rangle)$	$\frac{1}{\sqrt{2}}(\|I\rangle+\|E\rangle)$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	–
$\frac{1}{\sqrt{2}}(\|I\rangle+\|E\rangle)$	$\frac{1}{\sqrt{2}}(\|I\rangle-\|E\rangle)$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	bit flip
$\frac{1}{\sqrt{2}}(\|I\rangle-\|E\rangle)$	$\frac{1}{\sqrt{2}}(\|I\rangle+\|E\rangle)$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	bit flip
$\frac{1}{\sqrt{2}}(\|I\rangle-\|E\rangle)$	$\frac{1}{\sqrt{2}}(\|I\rangle-\|E\rangle)$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	–

tum channels, one single photon can generate three bits of secure keys. As a result, the key generation rate of our MDI-QKD protocol is $R = 3$. On the other hand, if we take imperfections such as imperfect single photon sources and noisy quantum channels, the key generation rate will be reduced. Here, we investigate the influence from the misalignment in imperfect single photon sources and channels to the QBER and the key generation rate of

our MDI-QKD protocol. In each DOF, we use the encoding in rectilinear base for key generation and the encoding in diagonal basis to evaluate the QBER. According to the original MDI-QKD protocol [3, 7, 9, 37], the secure key generation rate in the ith DOF can be written as

$$R_i = R_0[1 - H(e_{x_i}) - f(e_{z_i})H(e_{z_i})], \tag{5}$$

where $i = p, f, s$, and $f(e_{z_i})$ is an inefficiency function for the error correction in the ith DOF. We suppose that Charlie locates in the middle of Alice and Bob, so that the distance (d_{AC}) from Alice to Charlie is half of the distance from Alice to Bob (d). In this way, $R_0 = 10^{-a_0 d/20} \cdot 10^{-a_0 d/20} = 10^{-a_0 d/10}$ ($a = 0.2$ dB/km). $H(x)$ is the binary entropy with the form of

$$H(x) = -x \log_2 x - (1-x)\log_2(1-x). \tag{6}$$

As the encoding in three DOFs are independent, the total secure key generation rate can be calculated as

$$\begin{aligned} R = R_0\{&[1 - H(e_{x_p}) - f(e_{z_p})H(e_{z_p})] \\ &+ [1 - H(e_{x_f}) - f(e_{z_f})H(e_{z_f})] \\ &+ [1 - H(e_{x_s}) - f(e_{z_s})H(e_{z_s})]\}. \end{aligned} \tag{7}$$

If we suppose the QBERs in three DOFs are the same, R is three times of R_i.

We first consider the misalignment influence from the imperfect single photon sources. We take the source misalignment in polarization DOF as an example. When Alice (Bob) aims to prepare a photon in $|H\rangle$ or $|V\rangle$, the practical photon state expands to $\beta_p|H\rangle + \sqrt{1-\beta_p^2}\,|V\rangle$ or $\beta_p|V\rangle + \sqrt{1-\beta_p^2}\,|H\rangle$, respectively, while when they aim to prepare a photon in $|\pm_p\rangle$, the practical photon state expands to $\beta_p|+_p\rangle + \sqrt{1-\beta_p^2}\,|-_p\rangle$ or $\beta_p|-\rangle + \sqrt{1-\beta_p^2}\,|+\rangle$, respectively [56].

Next, we analyze the most general errors affecting qudits in transmission channels, say, the polarization and spatial-mode misalignments caused by the channel noise. We define that the operator $U_{A_{p(f,s)}}$ and $U_{B_{p(f,s)}}$ represent the misalignment in the polarization (first and second longitudinal momentum) DOF of Alice's and Bob's channel transmission. Here, we consider a simplified model with a two-dimensional unitary matrix as [71]

$$U_i = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}, \tag{8}$$

where $i = p, f, s$, and θ_i is in the scale of $[-\pi, \pi]$. We also take the polarization DOF as an example. Due to the misalignment in channel transmission, we can obtain $|H\rangle \to \cos\theta_p|H\rangle - \sin\theta_p|V\rangle$, $|V\rangle \to \cos\theta_p|V\rangle + \sin\theta_p|H\rangle$, $|+_p\rangle \to \cos\theta_p|+_p\rangle + \sin\theta_p|-_p\rangle$, $|-_p\rangle \to \cos\theta_p|-_p\rangle - \sin\theta_p|+_p\rangle$. As a result, the misalignment error rate is defined as $\sin^2\theta_p$. In the other two DOFs, we can obtain similar misalignment error rates as $\sin^2\theta_f$ and $\sin^2\theta_s$, respectively.

In this way, we combine the misalignment from source and channel transmission. If Alice and Bob aim to send $|H\rangle|H\rangle$ to Charlie, the practical photon states Charlie receiving will evolve to

$$\begin{aligned} |HH\rangle &\to \beta_p^2|HH\rangle + (1-\beta_p^2)|VV\rangle \\ &\quad + \beta_p\sqrt{1-\beta_p^2}(|HV\rangle + |VH\rangle) \\ &\to A_{0p}|HH\rangle + A_{1p}|VV\rangle \\ &\quad + A_{2p}(|HV\rangle + |VH\rangle) \\ &= \frac{A_{0p} + A_{1p}}{\sqrt{2}}|\phi^+\rangle + \frac{A_{0p} - A_{1p}}{\sqrt{2}}|\phi^-\rangle \\ &\quad + \sqrt{2}A_{2p}|\psi^+\rangle, \end{aligned} \tag{9}$$

where

$$\begin{aligned} A_{0p} &= \beta_p^2\cos^2\theta_p + (1-\beta_p^2)\sin^2\theta_p \\ &\quad + 2\beta_p\sqrt{1-\beta_p^2}\cos\theta_p\sin\theta_p, \\ A_{1p} &= \beta_p^2\sin^2\theta_p + (1-\beta_p^2)\cos^2\theta_p \\ &\quad - 2\beta_p\sqrt{1-\beta_p^2}\cos\theta_p\sin\theta_p, \\ A_{2p} &= -\beta_p^2\cos\theta_p\sin\theta_p + (1-\beta_p^2)\cos\theta_p\sin\theta_p \\ &\quad + \beta_p\sqrt{1-\beta_p^2}(\cos^2\theta_p - \sin^2\theta_p). \end{aligned} \tag{10}$$

In this way, there is a probability of $2A_{2p}^2$ that Charlie obtains wrong BSA result $|\psi^+\rangle$, thus increasing the QBER $e_{z_p} = 2A_{2p}^2$. If Alice and Bob both select the diagonal basis, i.e., $|+\rangle_p|+\rangle_p$, they will also obtain error rate $e_{xp} = e_{zp}$. Similarly, we can also calculate the QBER in other two DOFs as $e_{z_f} = e_{x_f} = 2A_{2f}^2$ and $e_{z_s} = e_{x_s} = 2A_{2s}^2$, respectively.

Taking the value of QBER in each DOF into Eq. (5), we can calculate the key generation rate ($R_{p(f,s)}$) in each DOF and the total key generation rate (R). Here, we control $|\beta_{p(f,s)}|^2 = 0.85$ and $\sin^2\theta_{p(f,s)} = 1.5\%$. The inefficiency function for the error correction process is set to $f_{e_{z_{p(f,s)}}} = 1$. In Fig. 2(a), we show the values of R and R_p as a function of the communication distance (d) between Alice and Bob in the scale of $0 \le d \le 50$ km. Actually, R_p equals to the key generation rate of the original MDI-QKD using only one DOF of single photons. It can be found that by encoding in three DOFs of single photons, we can efficiently increase the key generation rate of MDI-QKD. In Fig. 2(b), we show the value of LgR as a function d in the scale of $0 \le d \le 300$ km. Here, we control $\sin^2\theta_{p(f,s)} = 1.5\%$ and $|\beta_{p(f,s)}|^2 = 0.85$ and 0.9. It is obvious that with the growth of QBERs, the total key generation rate obviously reduces.

4 Discussion

In the paper, we propose a high-capacity MDI-QKD protocol, which adopts the photon qudits encoding in three DOFs to generate keys. In our protocol, both Alice and Bob generate single photons encoding in polarization

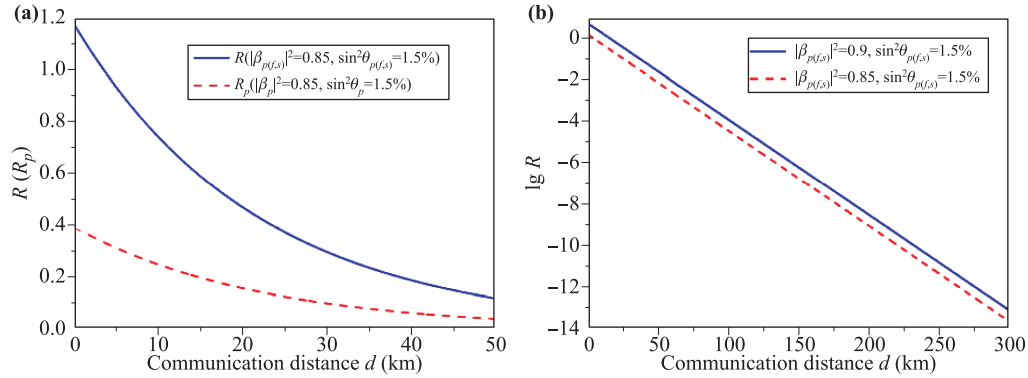


Fig. 2 **(a)** The key generation rate (R_p) in polarization DOF and total secure key generation rates (R) of our MDI-QKD protocol as a function of the communication distance between Alice and Bob. We control $|\beta_{p(f,s)}|^2 = 0.85$ and $\sin^2\theta_{p(f,s)} = 1.5\%$. The inefficiency function for the error correction process is set as $f_{e_{z_{p(f,s)}}} = 1$ [56]. **(b)** The value of LgR as a function d in the scale of $0 \leq d \leq 300$ km, with $\sin^2\theta_{p(f,s)} = 1.5\%$ and $|\beta_{p(f,s)}|^2 = 0.85$ and 0.9.

and two longitudinal-momentum DOFs and send them to Charlie for HBSA. Here, we adopt the HBSA protocol in Ref. [69] to completely distinguish the 64 hyperentangled Bell states with the help of the QND gates constructed by cross-Kerr nonlinearity. As the encoding information in each DOF can be used to generate secure key, encoding in multiple DOFs of single photons can efficiently increase the key generation rate of MDI-QKD. Actually, our MDI-QKD protocol can be extended to use general N DOFs of single photons ($N \geq 2$). In this general case, both Alice and Bob generate single photons encoding in N DOFs. In each DOF, they randomly choose rectilinear or diagonal base to encode the photon. The four Bell states in each DOF can be written as

$$|\Phi^{\pm}\rangle_k = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b \pm |1\rangle_a|1\rangle_b),$$
$$|\Psi^{\pm}\rangle_k = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b \pm |1\rangle_a|0\rangle_b), \quad (11)$$

where $|0\rangle$ and $|1\rangle$ represent two orthogonal states in rectilinear or diagonal base in the kth DOF ($k = 1, 2, 3, \cdots, N$). In the HBSA process, Charlie requires to construct the QND gates, which make he can completely distinguish all the four Bell states in each DOF, that is, 4^N hyperentangled Bell states in total. As long as the QND in each DOF is available, we can calculate the key generation rate in each DOF according to Eq. (5). Therefore, the total key generation rate of our MDI-QKD protocol using N DOFs of single photons can be expressed as

$$R = NR_p. \quad (12)$$

Here, we compare our protocol with the N-dimensional MDI-QKD protocol put forward by Dellantonio *et al.* [56]. In Ref. [56], the MDI-QKD protocol uses the HD qudits encoding in different spatial paths or time slots, which could also increase MDI-QKD's key generation rate. Our protocol has an attractive advantage over theirs, that is, our protocol is more flexible. In detail, for the protocol in Ref. [56], if a detection failure or an error occurs in a qudit, this qudit cannot be used to generate the key. For our MDI-QKD protocol, the HD system includes N essentially independent subsystems. The N subsystems can be manipulated and measured independently. As a result, if a detection failure or an error occurs in one DOF, the encoding information in this DOF has to be discarded. However, the encoding information in other DOFs can also be used to generate the key. We have to abandon a single photon qudit only when the error or detection efficiency happens in all DOFs. In this way, the more DOFs of single photons the MDI-QKD protocol uses, the MDI-QKD protocol shows the stronger resistance to errors and detection inefficiency. On the other hand, our MDI-QKD protocol requires single-photon sources. In practical experiments, the phase-randomized coherent state source is often used instead of the traditional single-photon source. However, the secret key rate will decrease significantly due to the vacuum state with large probability. For increasing the secret key rate, we may also adopt the coherent-state superpositions source, which can avoid the disadvantage of the phase-randomized coherent state source and has been used in MDI-QKD field [42].

The key step of our multiple-DOF MDI-QKD protocol is the HBSA. Such HBSA protocol was also used in realizing the high-capacity quantum secure direct communication [65] and constructing the two-photon three DOFs hyper-parallel controlled phase-flip gate [72]. However, the complete HBSA protocol adopted in our MDI-QKD protocol requires the cross-Kerr nonlinearity technique, which is still a challenge under current experimental condition. The main reason is that the natural cross-Kerr nonlinearity is quite weak, so that it is difficult to use homodyne detection to discriminate two overlapping coherent states [71]. However, some great progresses on the cross-Kerr nonlinearity have been made in recent years [73–77]. For example, in 2016, Dürr *et al.* reported that they realized a strong interaction in

Rydberg electromagnetically induced transparency (EIT) experiments to create a large controlled phase shift of 3.3 ± 0.2 rad, with the incoming control pulses containing an average of 0.6 photons [76]. In 2019, the group of Sinclair observed the nonlinear phases of 8 mrad/nW of signal power, corresponding to a χ^3 of 10^{-8} m^2/V^{-2} [77]. In addition, several attractive HBSA protocols based on other nonlinear optical elements have also been proposed, such as quantum-dot spins in optical microcavities [78–80], nitrogen-vacancy centers in resonators [81], and a three-level Λ-type system [82]. Recently, based on probabilistic HBSA, the first quantum teleportation of a single photon encoded in both spin and orbital angular momentum DOFs has also been achieved by the group of Pan [63]. Therefore, based on these works, we believe that the N-DOF complete HBSA may be experimentally realized in the future.

5 Conclusions

In summary, we propose a high-capacity MDI-QKD protocol, which adopts single photons encoding in multiple DOFs to generate secure keys. We take the qudits encoding in polarization and two longitudinal momentum DOFs as an example. Alice and Bob randomly prepare the qudits encoding in above three DOFs and send them to a third party Charlie through quantum channels. Then, Charlie makes the complete HBSA on the photon pairs and publishes his results. According to Charlie's HBSA results and the bases of photon qudits in three DOFs announced by both sides, Bob can obtain Alice's secure key when they choose same base. Our MDI-QKD protocol is unconditionally secure. By adopting the qudits encoding in multiple DOFs, our protocol can obviously increase the information capacity of single photon, and thus increase MDI-QKD's key generation rate. Moreover, comparing with previous HD MDI-QKD protocol in one DOF, our protocol still has some advantages. The HD system in our protocol includes some essentially independent subsystems, which can be manipulated and measured independently. As a result, a detection failure or an error in one DOF does not affect the encoding information in other DOFs, which can also be used to generate the key. In this way, our MDI-QKD protocol is more flexible. The more DOFs we adopt, our MDI-QKD protocol has the stronger resistance to errors or detection inefficiency. Based on above features, our MDI-QKD protocol may have application potential in the near future.

Acknowledgements This work was supported by the National Natural Science Foundation of China under Grant Nos. 11974189 and 12005106, the Postgraduate Research & Practice Innovation Program of Jiangsu Province under Grant No. SJCX19-0241, and a Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions.

References

1. C. H. Bennett and G. Brassard, in: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India IEEE, New York, 175 (1984)
2. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* 67(6), 661 (1991)
3. H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* 283(5410), 2050 (1999)
4. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d-level systems, *Phys. Rev. Lett.* 88(12), 127902 (2002)
5. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, Quantum key distribution over 67 km with a plug play system, *New J. Phys.* 4, 41 (2002)
6. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, *Nature* 421(6920), 238 (2003)
7. H. K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, *J. Cryptol.* 18(2), 133 (2005)
8. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, *Phys. Rev. Lett.* 98(1), 010504 (2007)
9. M. Koashi, Simple security proof of quantum key distribution based on complementarity, *New J. Phys.* 11(4), 045018 (2009)
10. S. Wang, W. Chen, Z. Q. Yin, D. Y. He, C. Hui, P. L. Hao, G. J. Fan-Yuan, C. Wang, L. J. Zhang, J. Kuang, S. F. Liu, Z. Zhou, Y. G. Wang, G. C. Guo, and Z. F. Han, Practical gigahertz quantum key distribution robust against channel disturbance, *Opt. Lett.* 43(9), 2030 (2018)
11. X. D. Wu, Y. J. Wang, H. Zhong, Q. Liao, and Y. Guo, Plug-and-play dual-phase-modulated continuous variable quantum key distribution with photon subtraction, *Front. Phys.* 14(4), 41501 (2019)
12. S. Wang, D. Y. He, Z. Q. Yin, F. Y. Lu, C. H. Cui, W. Chen, Z. Zhou, G. C. Guo, and Z. F. Han, Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system, *Phys. Rev. X* 9(2), 021046 (2019)
13. F. H. Xu, X. F. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* 92(2), 025002 (2020)
14. Y. Zhang and Q. Ni, Design and analysis of random multiple access quantum key distribution, *Quant. Engineer.* 2(1), e31 (2020)
15. G. Chai, D. W. Li, Z. W. Cao, M. Zhang, P. Huang, and G. Zeng, Blind channel estimation for continuous-variable quantum key distribution, *Quant. Engineer.* 2(2), e37 (2020)

16. M. J. He, R. Malaney, and J. Green, Multimode CV-QKD with non-Gaussian operations, *Quant. Engineer.* 2, e40 (2020)
17. H. K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* 8(8), 595 (2014)
18. B. Qi, C. H. F. Fung, H. K. Lo, and X. F. Ma, Time-shift attack in practical quantum cryptosystems, *Quantum Inf. Comput.* 7, 73 (2007)
19. Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Quantum hacking: experimental demonstration of timeshift attack against practical quantum-key-distribution systems, *Phys. Rev. A* 78(4), 042333 (2008)
20. N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device calibration impacts security of quantum key distribution, *Phys. Rev. Lett.* 107(11), 110501 (2011)
21. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photonics* 4(10), 686 (2010)
22. H. W. Li, S. Wang, J. Z. Huang, W. Chen, Z. Q. Yin, F. Y. Li, Z. Zhou, D. Liu, Y. Zhang, G. C. Guo, W. S. Bao, and Z. F. Han, Attacking a practical quantum-key-distribution system with wavelength dependent beam-splitter and multiwavelength sources, *Phys. Rev. A* 84(6), 062308 (2011)
23. J. Z. Huang, C. Weedbrook, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, G. C. Guo, and Z. F. Han, Quantum hacking of a continuous-variable quantum-key distribution system using a wavelength attack, *Phys. Rev. A* 87(6), 062329 (2013)
24. V. Makarov and J. Skaar, Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols, *Quantum Inf. Comput.* 8, 6 (2007)
25. V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, *Phys. Rev. A* 74(2), 022313 (2006)
26. Y. Zhao, B. Qi, and H. K. Lo, Quantum key distribution with an unknown and untrusted source, *Phys. Rev. A* 77(5), 052327 (2008)
27. X. Peng, H. Jiang, B. J. Xu, X. F. Ma, and H. Guo, Experimental quantum-key distribution with an untrusted source, *Opt. Lett.* 33(18), 2077 (2008)
28. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, *Phys. Rev. Lett.* 85(6), 1330 (2000)
29. W. Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* 91(5), 057901 (2003)
30. H. K. Lo, X. F. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* 94(23), 230504 (2005)
31. X. B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* 94(23), 230503 (2005)
32. X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A* 72(1), 012326 (2005)
33. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, *Phys. Rev. Lett.* 98(23), 230501 (2007)
34. S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, *New J. Phys.* 11(4), 045021 (2009)
35. L. Masanes, S. Pironio, and A. Acín, Secure deviceindependent quantum key distribution with causally independent measurement devices, *Nat. Commun.* 2(1), 238 (2011)
36. A. Máttar, J. Kolodynski, P. Skrzypczyk, D. Cavalcanti, K. Banaszek, and A. Acín, Device-independent quantum key distribution with single-photon sources, arXiv: 1803.07089 (2018)
37. H. K. Lo, M. Curty, and B. Qi, Measurement-deviceindependent quantum key distribution, *Phys. Rev. Lett.* 108(13), 130503 (2012)
38. Y. Liu, T. Y. Chen, L. J. Wang, H. Liang, G. L. Shentu, J. Wang, K. Cui, H. L. Yin, N. L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C. Z. Peng, Q. Zhang, and J. W. Pan, Experimental measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* 111(13), 130502 (2013)
39. F. H. Xu, M. Curty, B. Qi, and H. K. Lo, Practical aspects of measurement-device-independent quantum key distribution, *New J. Phys.* 15(11), 113007 (2013)
40. Z. Y. Tang, Z. F. Liao, F. H. Xu, B. Qi, L. Qian, and H. K. Lo, Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* 112(19), 190503 (2014)
41. Y. L. Tang, H. L. Yin, S. J. Chen, Y. Liu, W. J. Zhang, X. Jiang, L. Zhang, J. Wang, L. X. You, J. Y. Guan, D. X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T. Y. Chen, Q. Zhang, and J. W. Pan, Measurement-device-independent quantum key distribution over 200 km, *Phys. Rev. Lett.* 114(6), 069901 (2015)
42. H. L. Yin, W. F. Cao, Y. Fu, Y. L. Tang, Y. Liu, T. Y. Chen, and Z. B. Chen, Long-distance measurement-device-independent quantum key distribution with coherent-state superpositions, *Opt. Lett.* 39(18), 5451 (2014)
43. C. Wang, X. T. Song, Z. Q. Yin, S. Wang, W. Chen, C. M. Zhang, G. C. Guo, and Z. F. Han, Phase-reference-free experiment of measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* 115(16), 160502 (2015)
44. H. L. Yin, T. Y. Chen, Z. W. Yu, H. Liu, L. X. You, Y. H. Zhou, S. J. Chen, Y. Mao, M. Q. Huang, W. J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X. B. Wang, and J. W. Pan, Measurement device-independent quantum key distribution over a 404 km optical fiber, *Phys. Rev. Lett.* 117(19), 190501 (2016)
45. C. Wang, Z. Q. Yin, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Measurement-device-independent quantum key distribution robust against environmental disturbances, *Optica* 4(9), 1016 (2017)
46. X. D. Wu, Y. J. Wang, D. Huang, and Y. Guo, Simultaneous measurement-device-independent continuous variable quantum key distribution with realistic detector compensation, *Front. Phys.* 15(3), 31601 (2020)

47. J. Mower, Z. S. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, High-dimensional quantum key distribution using dispersive optics, *Phys. Rev. A* 87(6), 062322 (2013)

48. M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Higherdimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, *Phys. Rev. A* 88(3), 032305 (2013)

49. T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, Photon-efficient quantum key distribution using time – energy entanglement with high-dimensional encoding, *New J. Phys.* 17(2), 022002 (2015)

50. D. Bunandar, Z. S. Zhang, J. H. Shapiro, and D. R. Englund, Practical high-dimensional quantum key distribution with decoy states, *Phys. Rev. A* 91(2), 022336 (2015)

51. S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zhou, G. C. Guo, and Z. F. Han, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, *Nat. Photonics* 9(12), 832 (2015)

52. H. Z. Bao, W. S. Bao, Y. Wang, R. K. Chen, and H. W. Li, Detector-decoy high-dimensional quantum key distribution, *Opt. Express* 24(19), 22159 (2016)

53. H. Chau, C. Wong, Q. Wang, and T. Huang, Qudit-based measurement-device-independent quantum key distribution using linear optics, arXiv: 1608.08329 (2016)

54. F. T. Tabesh, S. Salimi, and A. S. Khorashad, Witness for initial correlations among environments, *Phys. Rev. A* 95(5), 052323 (2017)

55. G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers, *Phys. Rev. A* 96(2), 022317 (2017)

56. L. Dellantonio, A. S. Sorensen, and D. Bacco, Highdimensional measurement-device-independent quantum key distribution on two-dimensional subspaces, *Phys. Rev. A* 98(6), 062301 (2018)

57. G. I. Struchalin, E. V. Kovlakov, S. S. Straupe, and S. P. Kulik, Adaptive quantum tomography of highdimensional bipartite systems, *Phys. Rev. A* 98(3), 032330 (2018)

58. S. Wang, Z. Q. Yin, H. F. Chau, W. Chen, C. Wang, G. C. Guo, and Z. F. Han, Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme, *Quan. Sci. Technol.* 3(2), 025006 (2018)

59. F. M. Wang, P. Zeng, J. P. Zhao, B. Braverman, Y. Zhou, M. Mirhosseini, X. Wang, H. Gao, F. Li, R. W. Boyd, and P. Zhang, High-dimensional quantum key distribution based on mutually partially unbiased bases, *Phys. Rev. A* 101(3), 032340 (2020)

60. F. X. Wang, W. Chen, Z. Q. Yin, S. Wang, G. C. Guo, and Z. F. Han, Characterizing high-quality highdimensional quantum key distribution by state mapping between different degrees of freedom, *Phys. Rev. A* 11, 024070 (2019)

61. J. Chapman, C. Lim, and P. Kwiat, Hyperentangled time-bin and polarization quantum key distribution, arXiv: 1908.09018 (2019)

62. Z. X. Cui, W. Zhong, L. Zhou, and Y. B. Sheng, Measurement-device-independent quantum key distribution with hyper-encoding, *Sci. China Phys. Mech. Astron.* 62(11), 110311 (2019)

63. X. L. Wang, X. D. Cai, Z. E. Su, M. C. Chen, D. Wu, L. Li, N. L. Liu, C. Y. Lu, and J. W. Pan, Quantum teleportation of multiple degrees of freedom of a single photon, *Nature* 518(7540), 516 (2015)

64. X. M. Hu, Y. Guo, B. H. Liu, Y. F. Huang, C. F. Li, and G. C. Guo, Beating the channel capacity limit for superdense coding with entangled ququarts, *Sci. Adv.* 4(7), eaat9304 (2018)

65. F. Z. Wu, G. J. Yang, H. B. Wang, J. Xiong, F. Alzahrani, A. Hobiny, and F. G. Deng, High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states, *Sci. China Phys. Mech. Astron.* 60(12), 120313 (2017)

66. S. S. Chen, L. Zhou, W. Zhong, and Y. B. Sheng, Three-step three-party quantum secure direct communication, *Sci. China Phys. Mech. Astron.* 61(9), 90312 (2018)

67. L. Y. Li, T. J. Wang, and C. Wang, The analysis of high-capacity quantum secure direct communication using polarization and orbital angular momentum of photons, *Mod. Phys. Lett. B* 34(02), 2050017 (2020)

68. G. Vallone, R. Ceccarelli, F. De Martini, and P. Mataloni, Hyper-entanglement of two photons in three degrees of freedom, *Phys. Rev. A* 79(3), 030301 (2009)

69. Q. Liu, G. Y. Wang, Q. Ai, M. Zhang, and F. G. Deng, Complete nondestructive analysis of two-photon six-qubit hyperentangled Bell states assisted by cross-Kerr nonlinearity, *Sci. Rep.* 6(1), 22016 (2016)

70. H. Inamori, Security of practical time-reversed EPR quantum key distribution, *Algorithmica* 34(4), 340 (2002)

71. P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Linear optical quantum computing with photonic qubits, *Rev. Mod. Phys.* 79(1), 135 (2007)

72. Y. B. Wei, W. Q. Liu, and N. Y. Chen, Implementing two-photon three-degree-of-freedom hyper-parallel controlled phase flip gate through cavity-assisted interactions, *Ann. Phys.* 532(4), 1900578 (2020)

73. C. Zhu and G. Huang, Giant Kerr nonlinearity, controlled entangled photons and polarization phase gates in coupled quantum-well structures, *Opt. Express* 19(23), 23364 (2011)

74. I. C. Hoi, A. F. Kockum, T. Palomaki, T. M. Stace, B. Fan, L. Tornberg, S. R. Sathyamoorthy, G. Johansson, P. Delsing, and C. M. Wilson, Giant cross-Kerr effect for propagating microwaves induced by an artificial atom, *Phys. Rev. Lett.* 111(5), 053601 (2013)

75. K. M. Beck, M. Hosseini, Y. H. Duan, and V. Vuletic, Large conditional single-photon cross-phase modulation, *Proc. Natl. Acad. Sci. USA* 113(35), 9740 (2016)

76. D. Tiarks, S. Schmidt, G. Rempe, and S. Dürr, Optical π phase shift created with a single-photon pulse, *Sci. Adv.* 2(4), e1600036 (2016)

77. J. Sinclair, D. Angulo, N. Lupu-Gladstein, K. Bonsma-Fisher, and A. M. Steinberg, Observation of a large, resonant, cross-Kerr nonlinearity in a free-space Rydberg medium, arXiv: 1906.05151 (2019)

78. B. C. Ren, H. R. Wei, M. Hua, T. Li, and F. G. Deng, Complete hyperentangled-Bell-state analysis for photon systems assisted by quantum-dot spins in optical microcavities, *Opt. Express* 20(22), 24664 (2012)

79. T. J. Wang, Y. Lu, and G. L. Long, Generation and complete analysis of the hyperentangled Bell state for photons assisted by quantum-dot spins in optical microcavities, *Phys. Rev. A* 86(4), 042337 (2012)

80. G. Y. Wang, Q. Ai, B. C. Ren, T. Li, and F. G. Deng, Error-detected generation and complete analysis of hyperentangled Bell states for photons assisted by quantum-dot spins in double-sided optical microcavities, *Opt. Express* 24(25), 28444 (2016)

81. Q. Liu and M. Zhang, Generation and complete nondestructive analysis of hyperentanglement assisted by nitrogen-vacancy centers in resonators, *Phys. Rev. A* 91(6), 062321 (2015)

82. T. J. Wang and C. Wang, Complete hyperentangled-Bell state analysis for photonic qubits assisted by a three-level Λ-type system, *Sci. Rep.* 6(1), 19497 (2016)