

Measurement-device-independent quantum secret sharing with hyper-encoding

Xing-Xing Ju(居星星), Wei Zhong(钟伟), Yu-Bo Sheng(盛宇波), and Lan Zhou(周澜)
Citation: Chin. Phys. B, 2022, 31 (**10**): 100302. DOI: 10.1088/1674-1056/ac70bb
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Deterministic nondestructive state analysis for polarization-spatial-time-bin hyperentanglement with cross-Kerr nonlinearity

Hui-Rong Zhang(张辉荣), Peng Wang(王鹏), Chang-Qi Yu(于长琦), and Bao-Cang Ren(任宝藏)
Chin. Phys. B, 2021, 30 (**3**): 030304. DOI: 10.1088/1674-1056/abd7d5

Efficient entanglement concentration for arbitrary less-entangled NOON state assisted by single photons

Lan Zhou(周澜) and Yu-Bo Sheng(盛宇波)
Chin. Phys. B, 2016, 25 (**2**): 020308. DOI: 10.1088/1674-1056/25/2/020308

Bidirectional transfer of quantum information for unknown photons via cross-Kerr nonlinearity and photon-number-resolving measurement

Jino Heo, Chang-Ho Hong, Dong-Hoon Lee, Hyung-Jin Yang
Chin. Phys. B, 2016, 25 (**2**): 020306. DOI: 10.1088/1674-1056/25/2/020306

Bidirectional quantum teleportation of unknown photons using path-polarization intra-particle hybrid entanglement and controlled-unitary gates via cross-Kerr nonlinearity

Jino Heo, Chang-Ho Hong, Jong-In Lim, Hyung-Jin Yang
Chin. Phys. B, 2015, 24 (**5**): 050304. DOI: 10.1088/1674-1056/24/5/050304

Universal quantum computation using all-optical hybrid encoding

Guo Qi, Cheng Liu-Yong, Wang Hong-Fu, Zhang Shou
Chin. Phys. B, 2015, 24 (**4**): 040303. DOI: 10.1088/1674-1056/24/4/040303

Measurement-device-independent quantum secret sharing with hyper-encoding

Xing-Xing Ju(居星星)[1,3], Wei Zhong(钟伟)[3], Yu-Bo Sheng(盛宇波)[2,3], and Lan Zhou(周澜)[1,†]

[1] *College of Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*
[2] *College of Electronic and Optical Engineering & College of Flexible Electronics (Future Technology), Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*
[3] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

(Received 25 March 2022; revised manuscript received 10 May 2022; accepted manuscript online 18 May 2022)

Quantum secret sharing (QSS) is a typical multi-party quantum communication mode, in which the key sender splits a key into several parts and the participants can obtain the key by cooperation. Measurement-device-independent quantum secret sharing (MDI-QSS) is immune to all possible attacks from measurement devices and can greatly enhance QSS's security in practical applications. However, previous MDI-QSS's key generation rate is relatively low. Here, we adopt the polarization-spatial-mode hyper-encoding technology in the MDI-QSS, which can increase single photon's channel capacity. Meanwhile, we use the cross-Kerr nonlinearity to realize the complete hyper-entangled Greenberger–Horne–Zeilinger state analysis. Both above factors can increase MDI-QSS's key generation rate by about 10^3. The proposed hyper-encoded MDI-QSS protocol may be useful for future multiparity quantum communication applications.

Keywords: measurement-device-independent quantum secret sharing, hyper-encoding technology, cross-Kerr nonlinearity, hyper-entangled Greenberger–Horne–Zeilinger state analysis

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.1088/1674-1056/ac70bb

1. Introduction

Quantum communication is an important branch of quantum information. Quantum communication has unconditional security, which is based on the basic principles of quantum mechanics. Quantum communication begins with the research on quantum key distribution (QKD), which was first proposed by Bennett and Brassard in 1984.[1] QKD can distribute secure keys between two remote participants.[2–17] Besides QKD, there are some important branches in the field of quantum communication, such as quantum secret sharing (QSS),[18–33] and quantum secure direct communication (QSDC).[34–49]

QSS was first proposed by Hillery *et al.* in 1999[18] based on quantum technology and traditional cryptographic sharing technology. In QSS protocols, the key sender (dealer) splits a key into several parts and distributes each part to a participant. The participants can read out the key only when they cooperate with each other. Conversely, all the participants can also cooperate to distribute a secure key to the dealer.[20] In 2004, Xiao *et al.*[22] proposed a multi-party QSS protocol using the Greenberger–Horne–Zeilinger (GHZ) state. By choosing an asymmetric measurement basis, their protocol can be 100% efficient. In 2005, based on a QSDC protocol, Zhang *et al.*[23] proposed a (n,n)-threshold multiparty QSS scheme using single photons. In 2014, Bell *et al.*[25] reported an experimental demonstration of the graph state-based QSS. They showed that one can reliably encode, distribute and share quantum information among four parties with the graph state. In practical applications, there are some attack modes focusing on imperfect measurement devices, such as the fake-state attack,[50] time-shift attack,[51,52] and detection blinding attack.[53] Researchers proposed the measurement-device-independent (MDI) technology, which can resist all possible attacks from the imperfect measurement devices.[54–63] In 2015, Fu *et al.* proposed the first MDI-QSS protocol encoded in the polarization degree of freedom (DOF).[56] However, the key generation rate of the original MDI-QSS is relatively low. Hyper-encoding, which means encoding in two or more DOFs of a single photon, is an effective way to increase the channel capacity of single photons. Recently, the hyper-encoding technology has been widely adopted in the MDI-QKD and MDI-QSDC protocols to increase the key generation rate and secure message capacity, respectively.[63–66]

In this paper, we propose a hyper-encoding MDI-QSS protocol. In this protocol, the dealer and the other two participants generate polarization-spatial-mode hyper-encoded photon qudits and send the photons to the forth party. The forth party makes the hyper-entangled GHZ state analysis (HGSA) constructed with the cross-Kerr nonlinearities, which can completely distinguish all the 64 hyper-entangled GHZ states. With the hyper-encoding and HGSA, our hyper-encoding MDI-QSS protocol can achieve higher key generation rate

†Corresponding author. E-mail: zhoul@njupt.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

and extend the communication distance. This hyper-encoding MDI-QSS has potential applications in the field of quantum communication in the future.

This paper is organized as follows. In Section 2, we explain our hyper-encoding MDI-QSS protocol in detail. In Section 3, we analyze the security of the hyper-encoding MDI-QSS protocol and simulate its key generation rate. In Section 4, we give some discussions and draw a conclusion.

2. The hyper-encoding MDI-QSS protocol

Before presenting the hyper-encoding MDI-QSS protocol, we first give an introduction of the hyper-encoding rule. In the protocol, the three parties, i.e., Alice, Bob, and Charlie, encode their keys in the polarization (P) and spatial-mode (S) DOFs of single photons. The polarization DOF contains the rectilinear (Z) basis $\{|H\rangle,|V\rangle\}$ and diagonal (X) basis $\{|+\rangle_{\rm P}=\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle),|-\rangle_{\rm P}=\frac{1}{\sqrt{2}}(|H\rangle-|V\rangle)\}$. Here, $|H\rangle$ and $|V\rangle$ represent the horizontal and vertical polarization states, respectively. The spatial-mode DOF also contains Z basis and X basis. The Z basis in Alice's (Bob's and Charlie's) location contains $\{|a_1\rangle,|a_2\rangle\}$, $(\{|b_1\rangle,|b_2\rangle\},\{|c_1\rangle,|c_2\rangle\})$, where a_1 and a_2 (b_1 and b_2, c_1 and c_2) are different spatial modes. The X basis can be written as $\{|+\rangle_{\rm S}^{a}=\frac{1}{\sqrt{2}}(|a_1\rangle+|a_2\rangle),|-\rangle_{\rm S}^{a}=\frac{1}{\sqrt{2}}(|a_1\rangle-|a_2\rangle)\}$, $(\{|+\rangle_{\rm S}^{b}=\frac{1}{\sqrt{2}}(|b_1\rangle+|b_2\rangle),|-\rangle_{\rm S}^{b}=\frac{1}{\sqrt{2}}(|b_1\rangle-|b_2\rangle)\}$, $\{|+\rangle_{\rm S}^{c}=\frac{1}{\sqrt{2}}(c_1\rangle+|c_2\rangle),|-\rangle_{\rm S}^{c}=\frac{1}{\sqrt{2}}(|c_1\rangle-|c_2\rangle)\})$. In the polarization DOF, $|H\rangle$ and $|+\rangle_{\rm P}$ represent key 0, while $|V\rangle$ and $|-\rangle_{\rm P}$ represent key 1. In the spatial-mode DOF, $|i_1\rangle$ and $|+\rangle_{\rm S}^{i}$ $(i=a,b,c)$ represent key 0, while $|i_2\rangle$ and $|-\rangle_{\rm S}^{i}$ $(i=a,b,c)$ represent key 1.

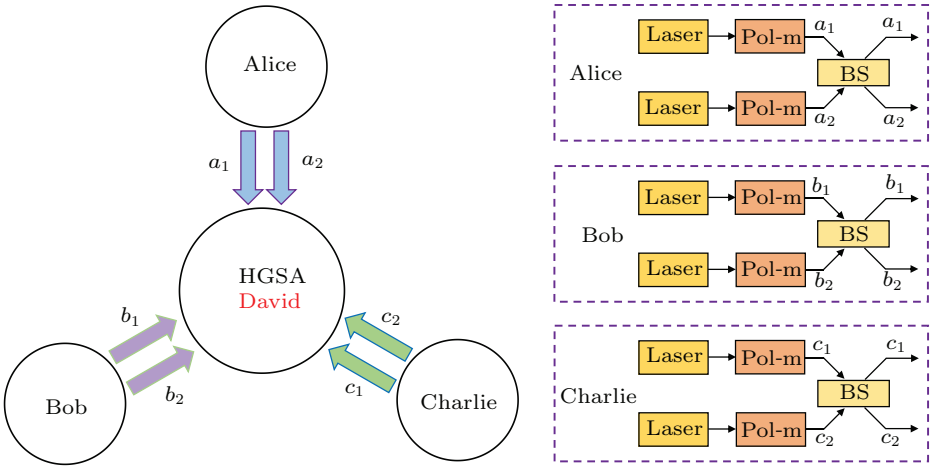


Fig. 1. Illustration of the hyper-encoding MDI-QSS protocol. Alice, Bob and Charlie separately prepares phase-randomized weak coherent pulses (WCPs) in BB84 polarization states. The polarization modulator (Pol-M) controls the encoding in the polarization DOF, while the 50:50 beam splitter (BS) controls the encoding in the spatial-mode DOF. Our protocol adopts the hyper-entangled GHZ state analysis (HGSA) technique proposed in Ref. [64] to completely distinguish the 64 hyper-entangled GHZ states. Here, i_1 and i_2 $(i=a,b,c)$ mean different spatial modes.

Figure 1 illustrates the basic principle of our hyper-encoding MDI-QSS protocol, which proceeds as follows.

Step 1 The dealer Alice, and the other two parties Bob and Charlie randomly select Z basis or X basis in polarization and spatial-mode DOFs to generate a series of single photon qudits. In detail, the three parties first prepare single photons in BB84 polarization states with the help of polarization modulator (Pol-M). In the spatial-mode DOF, if one wants to generate a photon in the Z basis, he can directly generate the photon in the corresponding spatial mode. If he wants to generate a photon in X basis, he uses the 50:50 beam splitter (BS), which can make $|a_1\rangle\rightarrow|+\rangle_{\rm S}^{a}$ ($|b_1\rangle\rightarrow|+\rangle_{\rm S}^{b}$, $|c_1\rangle\rightarrow|+\rangle_{\rm S}^{c}$) and $|a_2\rangle\rightarrow|-\rangle_{\rm S}^{a}$ ($|b_2\rangle\rightarrow|-\rangle_{\rm S}^{b}$, $|c_2\rangle\rightarrow|-\rangle_{\rm S}^{c}$). Then, they send the photons to a forth party David locating in the middle node of the quantum channels. Here, it should be noted that David can be untrustworthy, or even completely controlled by the eavesdropper.

Step 2 When David receives the photon qudits, he performs the HGSA on the photons. Here, we adopt the HGSA protocol in Ref. [67], which can completely distinguish all the possible hyper-entangled GHZ states with the help of the cross-Kerr nonlinearity. The GHZ states in the polarization and spatial-mode DOFs can be written as

$$
\begin{aligned}
|\psi_0^{\pm}\rangle_{\rm P}&=\frac{1}{\sqrt{2}}(|HHH\rangle\pm|VVV\rangle),\\
|\psi_1^{\pm}\rangle_{\rm P}&=\frac{1}{\sqrt{2}}(|VHH\rangle\pm|HVV\rangle),\\
|\psi_2^{\pm}\rangle_{\rm P}&=\frac{1}{\sqrt{2}}(|HVH\rangle\pm|VHV\rangle),\\
|\psi_3^{\pm}\rangle_{\rm P}&=\frac{1}{\sqrt{2}}(|HHV\rangle\pm|VVH\rangle),\\
|\psi_0^{\pm}\rangle_{\rm S}&=\frac{1}{\sqrt{2}}(|a_1b_1c_1\rangle\pm|a_2b_2c_2\rangle),\\
|\psi_1^{\pm}\rangle_{\rm S}&=\frac{1}{\sqrt{2}}(|a_2b_1c_1\rangle\pm|a_1b_2c_2\rangle),
\end{aligned}
$$

$$|\psi_2{}^{\pm}\rangle_{\rm S} = \frac{1}{\sqrt{2}}(|a_1b_2c_1\rangle \pm |a_2b_1c_2\rangle),$$
$$|\psi_3{}^{\pm}\rangle_{\rm S} = \frac{1}{\sqrt{2}}(|a_1b_1c_2\rangle \pm |a_2b_2c_1\rangle). \quad (1)$$

As a result, there are totally 64 hyper-entangled GHZ states with the form of $|\psi_i^{\pm}\rangle_{\rm P} \otimes |\psi_j^{\pm}\rangle_{\rm S}$ $(i = 0,1,2,3,\ j = 0,1,2,3)$. After the measurement, David announces the hyper-entangled GHZ state he has received by a public channel.

Step 3 Alice, Bob, and Charlie announce the generation basis of each photon qudit in both DOFs. If the three photons for the HGSA are generated in different bases in a DOF, the HGSA result and their encoding in this DOF should be discarded. On the other hand, if the three photons are generated in the same basis in a DOF, the HGSA result and their encoding information in this DOF will be retained. When all the parties choose X basis in a DOF, the encoding information in this DOF would be used to generate the original key. Tables 1 and 2 provide all the possible GSA results and Alice's key in the polarization and spatial-mode DOFs when the three parties use the same basis, respectively. When all the parties choose X basis in a DOF, Bob will publish his own encoding information in this DOF. We take the polarization DOF as an example. If the measurement result is $|\psi_y^+\rangle_{\rm P}$ $(y = 0,1,2,3)$, the encoding relationship is $X_A = X_B \oplus X_C$. On the other hand, if the measurement result is $|\psi_y^-\rangle_{\rm P}$ $(y = 0,1,2,3)$, the encoding relationship is $X_A \oplus 1 = X_B \oplus X_C$. As a result, Charlie can infer Alice's encoding information in the polarization DOF as the original key. The rule in the spatial-mode DOF is the same as that in the polarization DOF.

Table 1. Possible GSA results and Alice's key in the polarization DOF when all parties use the same basis.

Bit encoding			Measurement results and probabilities								Alice's key
Alice	Bob	Charlie	$\|\psi_0^+\rangle_{\rm P}$	$\|\psi_0^-\rangle_{\rm P}$	$\|\psi_1^+\rangle_{\rm P}$	$\|\psi_1^-\rangle_{\rm P}$	$\|\psi_2^+\rangle_{\rm P}$	$\|\psi_2^-\rangle_{\rm P}$	$\|\psi_3^+\rangle_{\rm P}$	$\|\psi_3^-\rangle_{\rm P}$	
$\|H\rangle$	$\|H\rangle$	$\|H\rangle$	1/2	1/2	0	0	0	0	0	0	–
$\|H\rangle$	$\|H\rangle$	$\|V\rangle$	0	0	0	0	0	0	1/2	1/2	–
$\|H\rangle$	$\|V\rangle$	$\|H\rangle$	0	0	0	0	1/2	1/2	0	0	–
$\|H\rangle$	$\|V\rangle$	$\|V\rangle$	0	0	1/2	1/2	0	0	0	0	–
$\|V\rangle$	$\|H\rangle$	$\|H\rangle$	0	0	1/2	1/2	0	0	0	0	–
$\|V\rangle$	$\|H\rangle$	$\|V\rangle$	0	0	0	0	1/2	1/2	0	0	–
$\|V\rangle$	$\|V\rangle$	$\|H\rangle$	0	0	0	0	0	0	1/2	1/2	–
$\|V\rangle$	$\|V\rangle$	$\|V\rangle$	1/2	1/2	0	0	0	0	0	0	–
$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	1/4	0	1/4	0	1/4	0	1/4	0	0
$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	0	1/4	0	1/4	0	1/4	0	1/4	0
$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	0	1/4	0	1/4	0	1/4	0	1/4	0
$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	1/4	0	1/4	0	1/4	0	1/4	0	0
$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	0	1/4	0	1/4	0	1/4	0	1/4	1
$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	1/4	0	1/4	0	1/4	0	1/4	0	1
$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)$	1/4	0	1/4	0	1/4	0	1/4	0	1
$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)$	0	1/4	0	1/4	0	1/4	0	1/4	1

Table 2. Possible GSA results and Alice's key in the spatial-mode DOF when all parties use the same basis.

Bit encoding			Measurement results and probabilities								Alice's key
Alice	Bob	Charlie	$\|\psi_0^+\rangle_{\rm S}$	$\|\psi_0^-\rangle_{\rm S}$	$\|\psi_1^+\rangle_{\rm S}$	$\|\psi_1^-\rangle_{\rm S}$	$\|\psi_2^+\rangle_{\rm S}$	$\|\psi_2^-\rangle_{\rm S}$	$\|\psi_3^+\rangle_{\rm S}$	$\|\psi_3^-\rangle_{\rm S}$	
$\|a_1\rangle$	$\|b_1\rangle$	$\|c_1\rangle$	1/2	1/2	0	0	0	0	0	0	–
$\|a_1\rangle$	$\|b_1\rangle$	$\|c_2\rangle$	0	0	0	0	0	0	1/2	1/2	–
$\|a_1\rangle$	$\|b_2\rangle$	$\|c_1\rangle$	0	0	0	0	1/2	1/2	0	0	–
$\|a_1\rangle$	$\|b_2\rangle$	$\|c_2\rangle$	0	0	1/2	1/2	0	0	0	0	–
$\|a_2\rangle$	$\|b_1\rangle$	$\|c_1\rangle$	0	0	1/2	1/2	0	0	0	0	–
$\|a_2\rangle$	$\|b_1\rangle$	$\|c_2\rangle$	0	0	0	0	1/2	1/2	0	0	–
$\|a_2\rangle$	$\|b_2\rangle$	$\|c_1\rangle$	0	0	0	0	0	0	1/2	1/2	–
$\|a_2\rangle$	$\|b_2\rangle$	$\|c_2\rangle$	1/2	1/2	0	0	0	0	0	0	–
$\frac{1}{\sqrt{2}}(\|a_1\rangle+\|a_2\rangle)$	$\frac{1}{\sqrt{2}}(\|b_1\rangle+\|b_2\rangle)$	$\frac{1}{\sqrt{2}}(\|c_1\rangle+\|c_2\rangle)$	1/4	0	1/4	0	1/4	0	1/4	0	0
$\frac{1}{\sqrt{2}}(\|a_1\rangle+\|a_2\rangle)$	$\frac{1}{\sqrt{2}}(\|b_1\rangle+\|b_2\rangle)$	$\frac{1}{\sqrt{2}}(\|c_1\rangle-\|c_2\rangle)$	0	1/4	0	1/4	0	1/4	0	1/4	0
$\frac{1}{\sqrt{2}}(\|a_1\rangle+\|a_2\rangle)$	$\frac{1}{\sqrt{2}}(\|b_1\rangle-\|b_2\rangle)$	$\frac{1}{\sqrt{2}}(\|c_1\rangle+\|c_2\rangle)$	0	1/4	0	1/4	0	1/4	0	1/4	0
$\frac{1}{\sqrt{2}}(\|a_1\rangle+\|a_2\rangle)$	$\frac{1}{\sqrt{2}}(\|b_1\rangle-\|b_2\rangle)$	$\frac{1}{\sqrt{2}}(\|c_1\rangle-\|c_2\rangle)$	1/4	0	1/4	0	1/4	0	1/4	0	0
$\frac{1}{\sqrt{2}}(\|a_1\rangle-\|a_2\rangle)$	$\frac{1}{\sqrt{2}}(\|b_1\rangle+\|b_2\rangle)$	$\frac{1}{\sqrt{2}}(\|c_1\rangle+\|c_2\rangle)$	0	1/4	0	1/4	0	1/4	0	1/4	1
$\frac{1}{\sqrt{2}}(\|a_1\rangle-\|a_2\rangle)$	$\frac{1}{\sqrt{2}}(\|b_1\rangle+\|b_2\rangle)$	$\frac{1}{\sqrt{2}}(\|c_1\rangle-\|c_2\rangle)$	1/4	0	1/4	0	1/4	0	1/4	0	1
$\frac{1}{\sqrt{2}}(\|a_1\rangle-\|a_2\rangle)$	$\frac{1}{\sqrt{2}}(\|b_1\rangle-\|b_2\rangle)$	$\frac{1}{\sqrt{2}}(\|c_1\rangle+\|c_2\rangle)$	1/4	0	1/4	0	1/4	0	1/4	0	1
$\frac{1}{\sqrt{2}}(\|a_1\rangle-\|a_2\rangle)$	$\frac{1}{\sqrt{2}}(\|b_1\rangle-\|b_2\rangle)$	$\frac{1}{\sqrt{2}}(\|c_1\rangle-\|c_2\rangle)$	0	1/4	0	1/4	0	1/4	0	1/4	1

Step 4 The three parties repeat steps 1–3 until Charlie obtains sufficient number of original keys.

Step 5 When Alice, Bob and Charlie all choose Z basis in a DOF, they will publish their encoding information in this DOF to make the security checking. A bit error happens if the measurement result is not the possible results shown in Tables 1 and 2. As a result, they can calculate the quantum bit error rate (QBER) in both DOFs. If the QBER of any DOF exceeds the tolerant threshold, they ensure that the key generation is not secure and discard all the generated original keys. In contrast, if the QBERs in both DOFs are lower than the tolerant thresholds, they will ensure the security of the key generation and retain the original keys.

Step 6 Alice, Bob and Charlie perform error correction and private amplification to form the final secure keys.

3. The security analysis and key generation rate of the hyper-encoding MDI-QSS protocol

In this section, we provide the security analysis and simulate the key generation rate of our hyper-encoding MDI-QSS protocol. In our protocol, as all the measurement tasks are performed by the forth party, the protocol can resist all possible attacks from the measurement devices. Its security proof is similar to that of the original MDI-QSS protocol[56] and MDI-QKD protocol.[54] Here, we have to consider the attack from the forth party David, who can be untrustworthy and totally controlled by Eve. In the first case, if David announces the wrong HGSA results, his dishonesty may make Charlie obtain wrong keys. However, his dishonest behavior would increase the QBER in both DOFs, and thus can be checked out by the security checking. It is worth noting that at the step 3 of the protocol, when all three parties choose X basis, only Bob publishes his encoding information. As Charlie does not announce his encoding information, Eve (David) cannot infer Alice's key even though he can obtain HGSA results. As a result, the forth party cannot cause the key leakage.

Then, we analyze the key generation of the hyper-encoding MDI-QSS protocol. According to the basic selection principle in each DOF, there are totally three different cases.

In the first case, Alice, Bob and Charlie choose the same basis in both DOFs. When they choose X basis in both DOFs, the encoded information in both DOFs can be used to generate the keys. Suppose that Bob's quantum state is $\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)\otimes\frac{1}{\sqrt{2}}(|b_1\rangle+|b_2\rangle)$, Charlie's quantum state is $\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)\otimes\frac{1}{\sqrt{2}}(|c_1\rangle-|c_2\rangle)$. According to Tables 1 and 2, Charlie can infer Alice's key to be 01 if the HGSA result is $|\psi_y^+\rangle_{\rm P}\otimes|\psi_y^+\rangle_{\rm S}$ $(y=0,1,2,3)$. If the HGSA is $|\psi_y^+\rangle_{\rm P}\otimes|\psi_y^-\rangle_{\rm S}$ $(y=0,1,2,3)$, Charlie can obtain Alice's key as 00. Similarly, Alice's key is 11 corresponding to the HGSA result of $|\psi_y^-\rangle_{\rm P}\otimes|\psi_y^+\rangle_{\rm S}$ $(y=0,1,2,3)$. If the HGSA is $|\psi_y^-\rangle_{\rm P}\otimes|\psi_y^-\rangle_{\rm S}$ $(y=0,1,2,3)$, Charlie can obtain Alice's key as 10.

In the second case, Alice, Bob and Charlie choose the same basis in only one DOF. We take the case that they choose the same basis in the polarization DOF as an example. Suppose that Bob's quantum state is $\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)\otimes|b_1\rangle$, and Charlie's quantum state is $\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)\otimes\frac{1}{\sqrt{2}}(|c_1\rangle-|c_2\rangle)$. In this case, only the GSA result and encoding information in the polarization DOF can be retained to generate the key. If the measurement result in the polarization DOF is $|\psi_y^+\rangle_{\rm P}$ $(y=0,1,2,3)$, Charlie can infer Alice's key in the polarization DOF to be 0. If the measurement result is $|\psi_y^-\rangle_{\rm P}$ $(y=0,1,2,3)$, he can obtain Alice's key in the polarization DOF to be 1.

In the third case, Alice, Bob and Charlie choose different bases in both DOFs, i.e., Bob's quantum state is $|H\rangle\otimes|b_1\rangle$, and Charlie's quantum state is $\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)\otimes\frac{1}{\sqrt{2}}(|c_1\rangle-|c_2\rangle)$. At this point, Alice, Bob, and Charlie will discard the measurement results and encoded information in both DOFs.

Next, we make a numerical simulation of this hyper-encoding MDI-QSS protocol's key generation rate under practical experimental condition. Based on previous experimental parameters given in Refs. [68,69], we assume that Alice (Bob, Charlie) uses the common WCP sources, in which the photon number follows the Poisson distribution with an average of μ_a (μ_b, μ_c). The forth party locates in the middle of three parties with the distance between the forth party and any party being d. In this way, the channel transmission efficiency is $t_a=t_b=t_c=10^{-\alpha d/10}$, where $\alpha=0.2$ dB/Km for a standard optical fiber. Based on Ref. [55], we set $\mu_a=\mu_b=\mu_c=0.3$ and consider the total polarization and spatial-mode misalignment error rates as $e_{\rm mP}=e_{\rm mS}=1.5\%$.

According to the original MDI-QSS protocol encoding in polarization DOF,[56] the key generation rate of the MDI-QSS protocol encoding in the polarization DOF can be written as

$$R_{\rm P}=Q_{0\mu\nu}^{\rm XP}+Q_{111}^{\rm XP}[1-H(e_{111}^{\rm ZP})]-H(E^{\rm XP})fQ^{\rm XP}. \qquad (2)$$

Here, $Q_{0\mu\nu}^{\rm XP}$ means the gain in the polarization DOF corresponding to Alice sending out vacuum state in the X basis and the forth party obtaining a successful GSA result. $Q_{111}^{\rm XP}$ and $e_{111}^{\rm ZP}$ mean the gain in the X basis and the bit error rate in the Z basis when each of the three parties emits one photon. $Q^{\rm XP}$ and $E^{\rm XP}$ represent the total gain and total quantum bit error rate in the X basis, respectively; f is the error correction efficiency ($f=1.16$). In the original MDI-QSS,[56] the GSA protocol with linear optical elements can only distinguish two polarization GHZ states $|\psi_0^{\pm}\rangle_{\rm P}$ and cannot distinguish the photon number in each of the three input modes. As a result, the existence of $Q_{0\mu\nu}^{\rm XP}$ can increase $E^{\rm XP}$ to a high level (about 37.5%). For reducing the total error rate, the authors of Ref. [56] also adopted the phase postselection technique.[70] They showed

that with the infinite decoy states model, the maximal distance from the forth party to Alice (Bob, Charlie) can reach about 150 km, and $R_{\rm P}$ under $d = 100$ km is below 10^{-12} corresponding to the single photon detector with the detection efficiency of 93%.

Our hyper-encoding MDI-QSS protocol adopts the complete HGSA constructed with the cross-Kerr nonlinearity in Ref. [67]. The cross-Kerr nonlinearity has been widely used to construct the controlled-not gate[71,72] and the quantum nondemolition detection (QND) gate.[73] With the complete HGSA protocol, David can distinguish the photon number in each incoming mode according to the homodyne measurement results on the coherent states, and the HGSA cannot be successful when Alice sends out vacuum state. In this way, $Q^{\rm XP}_{0\mu\nu}$ can be reduced to 0. Moreover, Alice, Bob and Charlie can employ an optical switch and the QND gate constructed with the cross-Kerr nonlinearities on the three emitted pulses. Only when each photon source emits exactly one photon, the optical switch will let the photon go to the HGSA. As a result, the multi-photon emission case can not enter the HGSA, and we can obtain $Q^{\rm XP} = Q^{\rm XP}_{111}$ and $E^{\rm XP} = e^{\rm XP}_{111}$. During the HGSA process, David firstly distinguishes the eight spatial-mode GHZ states and then distinguishes the eight polarization GHZ states. The GSA in both DOFs can be divided into two steps. In the first step, David divides the eight spatial-mode (polarization) GHZ states into four groups, $|\psi^{\pm}_0\rangle_{\rm S(P)}$, $|\psi^{\pm}_1\rangle_{\rm S(P)}$, $|\psi^{\pm}_2\rangle_{\rm S(P)}$, and $|\psi^{\pm}_3\rangle_{\rm S(P)}$ according to the homodyne measurement results on two coherent states. In the second step, he can distinguish $|\psi^{+}_y\rangle_{\rm S(P)}$ and $|\psi^{-}_y\rangle_{\rm S(P)}$ $(y = 0,1,2,3)$ based on the homodyne measurement result of the third coherent state.

Although the homodyne measurement is proved to be highly efficient (quite close to 100%), in practical cases it will inevitably introduce the inherent loss and error. We define the inherent efficiency η_l as the product of the coupling efficiency, between the photon and the fiber, and the detection efficiency of the homodyne measurement. Meanwhile, the error rate of the homodyne measurement can be calculated as $e_{\rm d} = 1/2{\rm erfc}(\frac{\alpha\theta^2}{2\sqrt{2}})$,[71–73] where α is the average number of the coherent state $|\alpha\rangle$ and θ means the phase shift of $|\alpha\rangle$. When the homodyne measurement provides wrong result, the forth party will obtain wrong HGSA result. According to Ref. [72], $e_{\rm d}$ can be reduced to 0.01 with the weak cross-Kerr nonlinearities in an NV-diamond system. In particular, the authors of Ref. [71] also showed that $e_{\rm d}$ can be further reduced to below 10^{-5} when $\alpha\theta^2 > 9$.

Here, we consider the imperfect homodyne measurement with $\eta_l = 0.98$ and $e_{\rm d} = 0.01$, and $e^{\rm ZP}_{111} = e^{\rm XP}_{111}$. Based on the imperfect QND, we can obtain $e^{{\rm Z(X)}p}_{111}$ and $Q^{{\rm Z(X)}p}_{111}$ as

$$e^{\rm Z(X)P}_{111} = \frac{1}{2}\left[1 - \frac{t_a t_b t_c \eta_l^3 (1-e_{\rm d})^3 (1-e_{\rm mP})^3}{Y^{\rm X(Z)P}_{111}}\right],$$

$$\begin{aligned} Q^{\rm XP}_{111} &= Q^{\rm ZP}_{111} = \mu_a\mu_b\mu_c e^{-(\mu_a+\mu_b+\mu_c)} Y^{\rm X(Z)P}_{111}, \\ Y^{\rm X(Z)P}_{111} &= t_a t_b t_c \eta_l^3 = 10^{-3\alpha d/10}\eta_l^3. \end{aligned} \tag{3}$$

In this way, the key generation rate in the polarization DOF of our MDI-QSS protocol can be written as

$$\begin{aligned} R_{\rm P} &= Q^{\rm XP}_{111}[1 - H(e^{\rm ZP}_{111})] - H(e^{\rm XP}_{111}) f Q^{\rm XP}_{111} \\ &= Q^{\rm XP}_{111}[1 - (1+f)H(e^{\rm XP}_{111})]. \end{aligned} \tag{4}$$

Similarly, we consider $e^{\rm ZS}_{111} = e^{\rm XS}_{111}$ and can obtain the key generation rate in the spatial-mode DOF as

$$\begin{aligned} R_{\rm S} &= Q^{\rm XS}_{111}[1 - H(e^{\rm ZS}_{111})] - H(e^{\rm XS}_{111}) f Q^{\rm XS}_{111} \\ &= Q^{\rm XS}_{111}[1 - (1+f)H(e^{\rm XS}_{111})]. \end{aligned} \tag{5}$$

For simplicity, we consider $Q^{\rm XS}_{111} = Q^{\rm XP}_{111}$ and $e^{\rm Z(X)S}_{111} = e^{\rm Z(X)P}_{111}$, so that we can obtain $R_{\rm S} = R_{\rm P}$.

As a result, the total key generation rate is

$$\begin{aligned} R_{\rm t} &= R_{\rm S} + R_{\rm P} = 2R_{\rm P} \\ &= 2Q^{\rm XP}_{111}[1 - (1+f)H(e^{\rm XP}_{111})]. \end{aligned} \tag{6}$$

Figure 2 provides the key generation rate $R_{\rm t}$ of our hyper-encoding MDI-QSS protocol versus the photon transmission distance d from any party to the forth party. Based on the hyper-encoding technology, the parties can generate keys independently in both DOFs. Meanwhile, with the help of the QND gate constructed with the cross-Kerr nonlinearity, we can completely eliminate the influence from the multi-photon emission and the vacuum state emission, and reduce the total gain and total error rate in both DOFs. As a result, our MDI-QSS protocol does not require the decoy state method. The above features can efficiently increase the key generation rate and extend the photon transmission distance. Under the photon transmission distance $d = 100$ km, $R_{\rm t}$ can achieve about 5.4×10^{-9}, which is about three orders of magnitude higher than that of the original MDI-QSS protocol.[56]

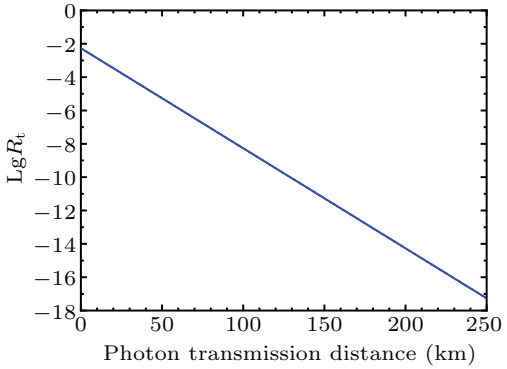


Fig. 2. Total secure key generation rate of our hyper-encoding MDI-QSS protocol altered with the photon transmission distance d from any party to the forth party. Here, we suppose that the average photon numbers of the WCP sources satisfy $\mu_a = \mu_b = \mu_c = 0.3$. The misalignment error rates in both DOFs meet $e_{\rm mP} = e_{\rm mS} = 1.5\%$. The inherent efficiency and error rate of the homodyne measurement are $\eta_l = 0.98$ and $e_{\rm d} = 0.01$, respectively. We also set the inefficiency function for the error correction process in both DOFs to be $f = 1.16$.

4. Discussion and conclusion

In our hyper-encoding MDI-QSS, the high-dimension system comprises two independent subsystems. The two subsystems can be manipulated and measured independently to generate the key, which can effectively increase the key generation rate of our MDI-QSS protocol. Moreover, if the GSA in a DOF fails but the GSA in the other DOF is successful, the parties only need to discard the key encoded in one DOF but still retain the coding information in the other DOF to generate the key. Meanwhile, an error in a DOF does not influence the coding information in the other DOF, which can still be used to generate the key. As a result, the hyper-encoding MDI-QSS protocol is quite flexible.

It is natural that our MDI-QSS protocol can be extended to arbitrary N-party MDI-QSS. In theory, N parties require to randomly prepare a large number of polarization-spatial-mode hyper-encoded photon qudits. Then, they send the photons to the measurement party for performing the N-photon HGSA, which can completely distinguish all the possible N-photon GHZ states in both DOFs. After the HGSA, the measurement party announces the results, and N parties announce the generation basis of each photon. They only preserve the GSA result when they generate the photon qudits in the same basis in a DOF. When all the N parties choose the X basis in a DOF, their encoding bits would be used to generate the original keys. When they all choose the Z basis in a DOF, they will announce their encoding in this DOF to make the security checking. When the security is guaranteed, the parties will perform the error correction and private amplification to form the final secure keys.

Finally, we will briefly discuss the experimental realization of this MDI-QSS protocol. The complete HGSA is the key element of our MDI-QSS protocol. So far, the cross-Kerr is still a challenge in the experiment. The reason is that the natural cross-Kerr nonlinearity is quite weak, so that it is hard to discriminate the weak phase shift by the homodyne measurement. Fortunately, during the recent few years, the cross-Kerr nonlinearity has achieved great progress.[74–76] In 2016, Beck's group experimentally obtained a cross-phase shift of $\pi/6$ between signal fields stored in an atomic quantum memory.[74] Later, Dürr *et al.* reached the strong interactions in the Rydberg electromagnetically induced transparency (EIT) experiments, which created a controlled phase shift of 3.3 ± 0.2 rad by using the incoming pulses with an average of 0.6 photons.[75] In 2019, Sinclair *et al.* realized the cross-Kerr nonlinearity in a free-space medium based on the Rydberg atoms and EIT technology, where the phase shift is 8 mrad/nW of signal power.[76] Based on the above attractive progress, it is possible to realize the complete HGSA in the near future.

In summary, we have proposed a polarization-spatial-mode hyper-encoding MDI-QSS protocol, in which all the three parties, Alice, Bob and Charlie, prepare photon qudits hyper-encoded in spatial-mode and polarization DOFs. They send their photons to the forth party to make the complete HGSA. After the complete HGSA, all the three participants announce the generation basis of their photons in both DOFs, and Bob also announces his codes in both DOFs. If all the three parties choose the X basis in a DOF, Charlie can speculate Alice's raw key in this DOF according to the HGSA result and Bob's code. In the protocol, the parties can encode the keys in both DOFs independently. The measurement errors and imperfect operations in one DOF do not affect the key generation in the other DOF. Meanwhile, the HGSA in the protocol can completely distinguish all the 64 hyper-entangled GHZ states and the incoming number in each input mode, so that the influence from vacuum state emission and multi-photon emission can be eliminated. The above factors can efficiently increase the key generation rate of our MDI-QSS protocol. This hyper-encoding MDI-QSS protocol may have potential applications in the near future.

Acknowledgement

Project supported by the National Natural Science Foundation of China (Grant Nos. 11974189 and 12175106).

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers Systems, and Signal Processing*, December 10–12, 1984, Bangalore, India, pp. 175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[4] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[5] Xu F H, Ma X F, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[6] Zhang Y C, Chen Z Y, Pirandola S, *et al.* 2020 *Phys. Rev. Lett.* **125** 010502
[7] Chen Y A, Zhang Q, Chen T Y, *et al.* 2021 *Nature* **589** 214
[8] Kwek L C, Cao L, Luo W, Wang Y X, Sun S H, Wang X B and Liu A Q 2021 *AAPPS Bull.* **31** 15
[9] Yin Z Q, Lu F Y, Teng J, Wang S, Chen W, Guo G C and Han Z F 2021 *Fundamental Res.* **1** 93
[10] Guo H, Li Z Y, Yu S and Zhang Y C 2021 *Fundamental Res.* **1** 96
[11] Tang G Z, Li C Y and Wang M 2021 *Quantum Engin.* **3** e79
[12] Wang X F, Sun X J, Liu Y X, *et al.* 2021 *Quantum Engin.* **3** e73
[13] Li B H, Xie Y M, Li Z, Weng C X, Li C L, Yin H L and Chen Z B 2021 *Opt. Lett.* **46** 5529
[14] Liu W B, Li C L, Xie Y M, *et al.* 2021 *PRX Quantum* **2** 040334
[15] Sun Z Q, Han Y X, Dou T Q, *et al.* 2021 *Chin. Phys. B* **30** 110303
[16] Chen X T, Zhang L P, Chang S K, Zhang H and Hu L Y 2021 *Chin. Phys. B* **30** 060304
[17] Luo H, Wang Y J, Ye W, Zhong H, Mao Y Y and Guo Y 2022 *Chin. Phys. B* **31** 020306
[18] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[19] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[20] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev. A* **59** 162
[21] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev. A* **63** 042301
[22] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[23] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev. A* **71** 044301
[24] Markham D and Sanders B C 2008 *Phys. Rev. A* **78** 042309
[25] Bell B A, Markham D A, Herrera-Mart D, *et al.* 2014 *Nat. Commun.* **5** 5480
[26] Tavakoli A, Herbauts I, Zukowski M and Bourennane M 2015 *Phys. Rev. A* **92** 030302

[27] Grice W P and Qi B 2019 *Phys. Rev. A* **100** 022339
[28] Williams B P, Lukens J M, Peters N A, Qi B and Grice W P 2019 *Phys. Rev. A* **99** 062311
[29] Wu X D, Wang Y J and Huang D 2020 *Phys. Rev. A* **101** 022301
[30] Lipinska V, Murta G, Ribeiro J and Wehner S 2020 *Phys. Rev. A* **101** 032332
[31] Jia Z Y, Gu J, Li B H, Yin H L and Chen Z B 2021 *Entropy* **23** 716
[32] Gu J, Xie Y M, Liu W B, Fu Y, Yin H L and Chen Z B 2021 *Opt. Express* **29** 32244
[33] Gu J, Cao X Y, Yin H L and Chen Z B 2021 *Opt. Express* **29** 9165
[34] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[35] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[36] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[37] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[38] Zhu F, Zhang W, Sheng Y B and Huang Y D 2017 *Sci. Bull.* **62** 1519
[39] Chen S S, Zhou L, Zhong W and Sheng Y B 2018 *Sci. China Phys. Mech. Astron.* **61** 90312
[40] Yang L, Wu J W, Lin Z S, Yin L G and Long G L 2020 *Sci. China Phys. Mech. Astron.* **63** 110311
[41] Li T and Long G L 2020 *New J. Phys.* **22** 063017
[42] Zhou L, Sheng Y B and Long G L 2020 *Sci. Bull.* **65** 12
[43] Wang C 2021 *Fundamental Res.* **1** 91
[44] Long G L and Zhang H R 2021 *Sci. Bull.* **66** 1267
[45] Gao C Y, Guo P L and Ren B C 2021 *Quantum Engin.* **3** e83
[46] Qi Z T, Li Y H, Huang Y W, Feng J, Zheng Y L and Chen X F 2021 *Light Sci. Appl.* **10** 183
[47] Liu X, Li Z J, Luo D, Huang C F, Ma D, Geng M M, Wang J W, Zhang Z R and Wei K J 2021 *Sci. China Phys. Mech. Astron.* **64** 120311
[48] Sheng Y B, Zhou L and Long G L 2022 *Sci. Bull.* **67** 367
[49] Zhou L and Sheng Y B 2022 *Sci. China Phys. Mech. Astron.* **65** 250311
[50] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev. A* **74** 022313
[51] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 042333
[52] Jain N, Wittmann C, Lydersen L, *et al.* 2011 *Phys. Rev. Lett.* **107** 110501
[53] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[54] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[55] Tang Z Y, Liao Z F, Xu F H, Qi B, Qian L and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[56] Fu Y, Yin H L, Chen T Y and Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501
[57] Yang X Q, Wei K J, Ma H Q, Liu H W, Yin Z Q, Cao Z and Wu L A 2018 *Sci. Rep.* **8** 5728
[58] Wang Y, Tian C X, Su Q, Wang M H and Su X L 2019 *Sci. China Inf. Sci.* **62** 72501
[59] Gao Z K, Li T and Li Z H 2020 *Sci. China Phys. Mech. Astron.* **63** 120311
[60] Yang Y G, Wang Y C, Yang Y L, *et al.* 2021 *Sci. China Phys. Mech. Astron.* **64** 260321
[61] Huang L, Zhang Y and Yu S 2021 *Chin. Phys. Lett.* **38** 040301
[62] Shi G F 2021 *Chin. Phys. B* **30** 100303
[63] Cui Z X, Zhou L, Zhong W and Sheng Y B 2019 *Sci. China Phys. Mech. Astron.* **62** 110311
[64] Yan Y F, Zhou L, Zhong W and Sheng Y B 2021 *Front. Phys.* **16** 11501
[65] Wu X D, Zhou L, Zhong W and Sheng Y B 2020 *Quantum Inf. Process.* **19** 354
[66] Ke Z J, Wang Y T, Yu S, *et al.* 2020 *Chin. Phys. B* **29** 080301
[67] Xia Y, Chen Q Q, Song J and Song H S 2012 *J. Opt. Soc. Am. B* **29** 1029
[68] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[69] Liu Y, Chen T Y, Wang L J, *et al.* 2013 *Phys. Rev. Lett.* **111** 130502
[70] Ma X F and Razavi M 2012 *Phys. Rev. A* **86** 062319
[71] Nemoto K and Munro W J 2004 *Phys. Rev. Lett.* **93** 250502
[72] Munro W J, Nemoto K, Beausoleil R G and Spiller T P 2005 *Phys. Rev. A* **71** 033819
[73] Loock P V 2011 *Laser Photon. Rev.* **5** 167
[74] Beck K M, Hosseini M, Duan Y H and Vuletic V 2016 *Proc. Natl. Acad. Sci. USA* **113** 9740
[75] Tiarks D, Schmidt S, Rempe G and Dürr S 2016 *Sci. Adv.* **2** e1600036
[76] Sinclair J, Angulo D, Lupu-Gladstein N, Bonsma-Fisher K and Steinberg A M 2019 *Phys. Rev. Res.* **1** 033193