

Cryptanalysis of efficient semi-quantum secret sharing protocol using single particles

Gan Gao(高甘)

Citation: Chin. Phys. B, 2024, 33 (**4**): 040301. DOI: 10.1088/1674-1056/ad2bee
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Efficient semi-quantum secret sharing protocol using single particles

Ding Xing(邢丁), Yifei Wang(王艺霏), Zhao Dou(窦钊), Jian Li(李剑),Xiubo Chen(陈秀波), and Lixiang Li(李丽香)
Chin. Phys. B, 2023, 32 (**7**): 070308. DOI: 10.1088/1674-1056/ace159

Measurement-device-independent quantum dialogue

Guo-Fang Shi(石国芳)
Chin. Phys. B, 2021, 30 (**10**): 100303. DOI: 10.1088/1674-1056/ac140a

Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation

Yingming Zhou(周颖明), Xue-Qin Jiang(蒋学芹), Weiqi Liu(刘维琪), Tao Wang(王涛), Peng Huang(黄鹏), Guihua Zeng(曾贵华)
Chin. Phys. B, 2018, 27 (**5**): 050301. DOI: 10.1088/1674-1056/27/5/050301

Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum

Wang Le (王乐), Zhao Sheng-Mei (赵生妹), Gong Long-Yan (巩龙延), Cheng Wei-Wen (程维文)
Chin. Phys. B, 2015, 24 (**12**): 120307. DOI: 10.1088/1674-1056/24/12/120307

Multi-user quantum key distribution with collective eavesdropping detection over collective-noise channels

Huang Wei (黄伟), Wen Qiao-Yan (温巧燕), Liu Bin (刘斌), Gao Fei (高飞)
Chin. Phys. B, 2015, 24 (**7**): 070308. DOI: 10.1088/1674-1056/24/7/070308

Cryptanalysis of efficient semi-quantum secret sharing protocol using single particles

Gan Gao(高甘)[1,2,3,†]

[1] *Department of Electrical Engineering, Tongling University, Tongling* 244061, *China*
[2] *Anhui Engineering Research Center of Intelligent Manufacturing of Copper-based Materials, Tongling University, Tongling* 244061, *China*
[3] *Anhui Joint Key Laboratory of Critical Technologies for High-End Copper-Based New Materials, Tongling University, Tongling* 244061, *China*

(Received 23 October 2023; revised manuscript received 10 January 2024; accepted manuscript online 22 February 2024)

In paper [*Chin. Phys. B* **32** 070308 (2023)], Xing *et al.* proposed a semi-quantum secret sharing protocol by using single particles. We study the security of the proposed protocol and find that it is not secure, that is, the three dishonest agents, Bob, Charlie and Emily can collude to obtain Alice's secret without the help of David.

Keywords: security loophole, rearranging orders, semi-quantum secret sharing, single particles

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/ad2bee

1. Introduction

Cryptography is playing a significant role in the information society, and its development has been greatly promoted by quantum physics. Compared to classical cryptography whose security is based on the assumptions of computational complexity, quantum cryptography demonstrates higher security and efficiency since some special principles of quantum mechanics are used. Thus far, many branches of quantum cryptography have been presented to offer various security properties, including quantum key distribution (QKD),[1–9] quantum secure direct communication (QSDC),[10–26] quantum secret sharing (QSS),[27–59] and so on.

As we all know, QKD is the earliest and maturest branch, in which two communication parties first generate a shared secret key by quantum states, and then apply this key to encrypt and decrypt the secret messages. In 1984, Bennett and Brassard[1] used nonorthogonal single polarization states to propose the first QKD protocol. Since then, plenty of QKD protocols were proposed. For example, in 2004, Deng and Long[3] used practical faint laser pulses to propose a two-step QKD protocol. In 2008, Li *et al.*[5] proposed two QKD protocols over two different collective-noise channels. In 2019, Yan *et al.*[8] proposed an efficient high-dimensional QKD protocol based on qudits transmission with the quantum Fourier transform, and so on. Unlike QKD, QSDC can transfer secret messages directly and safely without a private key to encrypt them. In 2002, Long and Liu[10] proposed the first QSDC protocol using the concept of quantum data block. Since then, plenty of QSDC protocols were proposed. For example, in 2005, Wang *et al.*[12] proposed a QSDC protocol with quantum superdense coding in high-dimensional Hilbert space. In 2020, Wu *et al.*[24] proposed a high-capacity measurement-device-independent QSDC protocol by encoding secure information in photons' polarization and spatial-mode degrees of freedom. In 2023, Hong *et al.*[26] proposed a measurement-device-independent three-party QSDC protocol based on the polarization-spatial-mode hyperentanglement, and so on.

Generally, there are only two communication parties in QKD or QSDC, however, there are at least three ones in QSS. The basic idea of QSS is that the secret of a dealer is split into several sub-secrets, and each agent holds a sub-secret, and the subset of agents can not extract the secret, but the entire set can. Obviously, there exists a collaboration during extracting the secret. In order to prevent the collaboration from dishonestly happening, internal attacks also need to be considered when analyzing the security. By the way, internal attacks need not to be considered in QKD and QSDC.

In 1999, Hillery *et al.*[27] used a three-particle GHZ state and a four-particle GHZ state to propose the first QSS protocol. Since then, plenty of QSS protocols were proposed. For example, in 2003, Bagherinezhad and Karimipour[28] utilized reusable GHZ states as secure carriers to propose a QSS protocol. In 2006, Deng *et al.*[32] proposed a circular QSS protocol, in which the quantum information carrier, single photons or entangled particles, can circularly run. In 2009, Gu *et al.*[37] proposed a high-capacity three-party QSS protocol with quantum superdense coding, in which almost all Einstein–Podolsky–Rosen pairs can be used for carrying useful information. In 2011, Zhu *et al.*[43] used four non-orthogonal two-particle entangled states to propose a multi-party QSS protocol, in which all entangled states can be used for generating the private key except those used for the eavesdropping check. In 2017, Chen *et al.*[49] used the Borras–Plastino–Batle (BPB) state to propose a QSS protocol, in which both the dealer and agents don't perform any unitary operation and only need to perform the projective measurements. In 2022, Ju *et al.*[55]

†Corresponding author. E-mail: gaogan0556@163.com

© 2024 Chinese Physical Society and IOP Publishing Ltd

used the polarization-spatial-mode hyper-encoding technology which can increase single photon's channel capacity to propose measurement-device-independent QSS protocol, and so on.

Recently, Xing *et al.*[56] used single particles (photons) to propose a QSS protocol. For simplicity, we will call this protocol the XWDLCL protocol later. In 2016, Gao *et al.*[50] proposed a QSS protocol in which each agent forms his own sub-secret by only rearranging order. Note that, in the XWDLCL protocol, the manner to form sub-secrets is the same as that in Gao *et al.*'s protocol.[50] In addition, it is also interesting in the XWDLCL protocol that specific secrets can be shared and the rearranging order is used to improve efficiency and ensure security. However, it is somewhat a pity that there exists a security loophole in the five-party case of the XWDLCL protocol, that is, the three dishonest agents, Bob, Charlie and Emily can collude to obtain Alice's secret without the help of David.

2. Review of the XWDLCL protocol

Firstly, let us review the encoding method used in the XWDLCL protocol as follows.

An integer x in the range of $[1, C_{2N}^{N}]$ can be expressed as $x = C_{2N}^{N} - b_1 - b_2 - \cdots - b_N$. When $P_{i-1} = x$, $b_i = 0$; when $P_{i-1} \neq x$, $b_i = \max\{C_{a_i}^{N-i+1} | P_{i-1} - C_{a_i}^{N-i+1} \geq x\}$. Here, $1 \leq i \leq N$, $a_i \in N^+$. The a_i is a parameter to build parameter b_i and indicates encoding positions. The P_i is an intermediate value $P_0 = C_{2N}^{N}$, $P_i = P_{i-1} - b_i$. If each $b_i \neq 0$, the positions from the first 1 to the Nth 1 will be $2N - a_1, 2N - a_2, \ldots, 2N - a_N$, or they will be $2N - a_1, 2N - a_2, \ldots, 2N - a_{k-1}, N + k, N + k + 1, \ldots, 2N$, $(k = \min\{i | b_i = 0\})$.

Next, let us review steps of the five-party case in the XWDLCL protocol as follows.

(i) According to the shared secret and the encoding method, Alice prepares an encoded sequence (simply called sequence T_0) which is composed of single photons.

(ii) Alice reorders the photons in sequence T_0 and the rearrangement order is only known to her. After the reordering, sequence T_0 becomes sequence T_1.

(iii) Alice prepares m decoy photons (here, $m = m_{\rm b} + m_{\rm c} + m_{\rm d} + m_{\rm e} + m_{\rm a}$), each of which is randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\}$. She randomly inserts each decoy photon into sequence T_1, and sends sequence T_1 containing m decoy photons to Bob.

(iv) After confirming that Bob has received sequence T_1, Alice publishes the insertion positions of $m_{\rm b}$ decoy photons. Next, Bob measures $m_{\rm b}$ decoy photons in the Z basis $\{|0\rangle, |1\rangle\}$, and then Alice publishes the states of $m_{\rm b}$ decoy photons. Bob utilizes the decoy photons in $|0\rangle$ or $|1\rangle$ to check the error rate, and the decoy photons in $|+\rangle$ or $|-\rangle$ to check whether the measuring outcomes are evenly distributed. If the error or deviation rate does not exceed a preset threshold, the protocol will continue. After the check, Bob throws away $m_{\rm b}$ decoy photons and disturbs the order of the remaining photons in sequence T_1. At the moment, sequence T_1 becomes sequence T_2. Bob sends sequence T_2 to Charlie.

(v) After Charlie announces the receipt of sequence T_2, firstly Alice publishes the insertion positions of $m_{\rm c}$ decoy photons, secondly Bob publishes the transposition order of those photons, thirdly Charlie measures $m_{\rm c}$ decoy photons in the Z basis, lastly Alice publishes the states of $m_{\rm c}$ decoy photons. According to the measuring outcomes and the published states, Charlie checks the security of sequence T_2 transmission like Bob. After the check, Charlie throws away $m_{\rm c}$ decoy photons and disturbs the order of the remaining photons in sequence T_2. At the moment, sequence T_2 becomes sequence T_3. Charlie sends sequence T_3 to David.

(vi) After David announces that he has received sequence T_3, what he will do is the same as what Charlie does. Then, David sends sequence T_4 to Emily. After Emily announces that she has received sequence T_4, what she will do is also the same as what Charlie does. Then, Emily sends sequence T_5 back to Alice.

(vii) After receiving sequence T_5, Alice publishes the original positions of $m_{\rm a}$ decoy photons. Bob, Charlie, David and Emily publish in turn their transposition order of $m_{\rm a}$ decoy photons. So, Alice can get the final positions of $m_{\rm a}$ decoy photons in sequence T_5, and measures each m_a decoy photon in the corresponding basis. By comparing the original states of $m_{\rm a}$ decoy photons and her measuring outcomes, Alice can calculate an error rate. If the error or deviation rate does not exceed a preset threshold, the protocol will continue.

(viii) Alice throws away $m_{\rm a}$ decoy photons, and measures all the remaining photons, and publishes her measuring outcomes. After that, Alice publishes her rearrangement order. If Bob, Charlie, David and Emily want to extract Alice's secret, they must cooperate honestly. Otherwise, neither of them can get Alice's secret with 100% certainty.

3. Security loophole

In this section, we will propose an efficient attack, which is implemented by the dishonest agents Bob, Charlie and Emily, on the five-party case of the XWDLCL protocol. This attack is described as follows.

In the above step (v), we can see that after the check, Charlie needs to reorder the photons and send sequence T_3 to David. In order to implement the attack, Charlie does not do those, but secretly prepares sequence T_3^* which is as long as sequence T_2 discarding $m_{\rm c}$ decoy photons. Note that almost one half of photons in sequence T_3^* are prepared in $|0\rangle$, the other half in $|1\rangle$, of course, Charlie knows which state each photon

in sequence T_3^* is in. Suppose that sequence T_3^* is denoted with

$$[1(|0\rangle),2(|1\rangle),3(|0\rangle),4(|1\rangle),5(|0\rangle),6(|1\rangle),7(|0\rangle),$$
$$8(|1\rangle),9(|0\rangle),10(|1\rangle),11(|0\rangle),12(|1\rangle),13(|0\rangle)].$$

Next, he sends sequence T_3^* instead of sequence T_3 to David. After David receives the sequence, in order to check whether the receiving sequence is attacked, Alice needs to publish the insertion positions of $m_{\rm d}$ decoy photons. As soon as she publishes those, Bob and Charlie easily find $m_{\rm d}$ decoy photons in sequence T_2. Suppose that sequence T_2 discarding $m_{\rm c}$ decoy photons is denoted with

$$[1(|u\rangle_{13}),2(|u\rangle_7),3(|1\rangle_1^{m_{\rm d}}),4(|u\rangle_8),5(|-\rangle_6^{m_{\rm d}}),6(|0\rangle_5^{m_{\rm d}}),7(|u\rangle_2),$$
$$8(|u\rangle_4),9(|u\rangle_{11}),10(|u\rangle_{12}),11(|u\rangle_9),12(|+\rangle_{10}^{m_{\rm d}}),13(|u\rangle_3)],$$

here, $|u\rangle$ denotes the unknown state that a single photon is in. After knowing that $m_{\rm d}$ decoy photons are in positions 3, 5, 6 and 12, Charlie immediately measures them in the Z basis. Suppose that his measurement outcomes on the 3rd, 5th, 6th and 12th photons are $|1\rangle^{m_{\rm d}}$, $|1\rangle^{m_{\rm d}}$, $|0\rangle^{m_{\rm d}}$ and $|0\rangle^{m_{\rm d}}$, respectively. In step (vi), we see that in order to check whether the sequence David receives is attacked, Charlie is required to publish the transposition orders of $m_{\rm d}$ decoy photons. When publishing those, he plays a trick and tells a lie that his transposition orders are $[3\rightarrow 2,5\rightarrow 8,6\rightarrow 11,12\rightarrow 9]$. Once David uses the Z basis to measure the 2nd, 8th, 11th and 9th photons in sequence T_3^*, his measurement outcomes will be $|1\rangle$, $|1\rangle$, $|0\rangle$ and $|0\rangle$, respectively. Obviously, David's measurement outcomes are the same as Charlie's on $m_{\rm d}$ decoy photons. It is seen that there are four possible measurement outcomes when the 3rd, 5th, 6th and 12th photons in sequence T_2 are measured in the Z basis. By far, we just consider one possible measurement outcome. If other measurement outcomes occur, how does Charlie concoct his transposition orders? The answer is as follows. If his measurement outcomes on the 3rd, 5th, 6th and 12th photons are $|1\rangle^{m_{\rm d}}$, $|0\rangle^{m_{\rm d}}$, $|0\rangle^{m_{\rm d}}$ and $|1\rangle^{m_{\rm d}}$ ($|1\rangle^{m_{\rm d}}$, $|0\rangle^{m_{\rm d}}$, $|0\rangle^{m_{\rm d}}$ and $|0\rangle^{m_{\rm d}}$, or $|1\rangle^{m_{\rm d}}$, $|1\rangle^{m_{\rm d}}$, $|0\rangle^{m_{\rm d}}$ and $|1\rangle^{m_{\rm d}}$), respectively, Charlie concocts that his transposition orders are $[3\rightarrow 2,5\rightarrow 7,6\rightarrow 11,12\rightarrow 4]$ ($[3\rightarrow 2,5\rightarrow 9,6\rightarrow 11,12\rightarrow 13]$ or $[3\rightarrow 2,5\rightarrow 8,6\rightarrow 11,12\rightarrow 10]$). In fact, the reason that four possible measurement outcomes exist is that the 5th photon in $|-\rangle$ and the 12th photon in $|+\rangle$ are measured in the Z basis. Here, it is worth emphasising that the four measurement outcomes are evenly distributed, and as long as the measuring methods and equipments are same, no matter who (Charlie or David) measures the 5th and 12th photons, the deviation rate should be same. Thus, David can not detect that the sequence in his own hands is not the genuine sequence T_3, in other words, he can not detect that Charlie is eavesdropping. After telling a lie, Charlie immediately performs the transposition orders of all photons in sequence T_2. Note that the performed transposition orders must contain his concocting transposition orders. After the transposition orders, sequence T_2 becomes sequence T_3. He secretly sends sequence T_3 discarding $m_{\rm d}$ decoy photons to Emily. Next, let us take a look at what David did again. After his check, David disturbs the order of the remaining photons in sequence T_3^*, and also sends the reordered sequence T_3^* to Emily. So Emily owns the two sequences, sequence T_3 and the reordered sequence T_3^*. She reserves the former and discards the latter. After her check, Emily does not perform transposition orders, but directly sends sequence T_3 discarding $m_{\rm e}$ decoy photons back to Alice. After receiving the sequence, Alice starts to check eavesdropping. First, she publishes the insertion positions of $m_{\rm a}$ decoy photons, and then Bob, Charlie, David and Emily are required to publish in turn their respective transposition orders of $m_{\rm a}$ decoy photons. At this moment, Bob and Charlie publish their respective transposition orders performed on Alice's receiving sequence, and David publishes the transposition orders performed on sequence T_3^*. Since Emily does not perform transposition orders at all, in order not to be detected, she needs to tell a lie that her transposition orders are the same as David's. We all know that if the same transposition orders are twice performed on one sequence, the relative positions of photons in the sequence are not changed, that is, their order is not changed. In a word, Emily's publishing transposition orders must satisfy that the order of photons in sequence T_3 is not changed if Emily's and David's publishing transposition orders are truly performed. Now that no changing occurs, Alice can accurately find $m_{\rm a}$ decoy photons in sequence T_3. Thus, she can not detect the attack that Bob, Charlie and Emily jointly implement either. After her check, Alice publishes the measurement outcomes on all the remaining photons and her rearrangement order. So Bob, Charlie and Emily can obtain Alice's secret without the help of David.

In order to stand against the above proposed attack, the XWDLCL protocol needs to add the processes that check the security of a quantum channel. But, adding the processes will greatly reduce the communication efficiency, which is also one of key considerations when designing a QSS protocol. Therefore, we do not plan to make a modification for the XWDLCL protocol here.

4. Conclusion

By designing a joint attack, we have proved that the five-party case of the XWDLCL protocol is insecure. In other words, it has been pointed out there exists a security loophole in the five-party case of the XWDLCL protocol. The reason for insecurity is that the attack can not be detected by analyzing two kinds of measurement outcomes. The first kind is the error measurement outcomes, that is, the outcomes which the

agents obtain by using the Z basis to measure decoy photons in $|+\rangle$ or $|-\rangle$. In fact, analyzing this kind has little contribution to check eavesdropping. Naturally, the second kind is the correct measurement outcomes, and the contribution of analyzing this kind to check eavesdropping is also limited. In a word, the method that the agents check eavesdropping by using one set of basis to measure decoy photons is not feasible in the XWDLCL protocol.

Acknowledgments

Project supported by the Offline Course Program of "Experiment of College Physics" in the 2022-year Anhui Provincial Quality Engineering Program (Grant No. 2022xxkc134), the Program for Academic Leader Reserve Candidates in Tongling University (Grant Nos. 2020tlxyxs43 and 2014tlxyxs30), the Talent Scientific Research Foundation of Tongling University (Grant No. 2015tlxyrc01), and the 2014-year Program for Excellent Youth Talents in University of Anhui Province.

References

[1] Bennett C H and Brassard G 1984 *IEEE International Conference on Computers, Systems and Signal Processin*, 1984, Bangalore, India, p. 175
[2] Ekert A K 1992 *Phys. Rev. Lett.* **67** 661
[3] Deng F G and Long G L 2004 *Phys. Rev. A* **70** 012311
[4] Cai Q and Tan Y 2006 *Phys. Rev. A* **73** 032305
[5] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **78** 022321
[6] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[7] Gong L H, Song H C, He C S, Liu Y and Zhou N R 2014 *Phys. Scr.* **89** 035101
[8] Yan X Y, Zhou N R, Gong L H, Wang Y Q and Wen X J 2019 *Quantum Inf. Process.* **18** 271
[9] Guo Y, Su Y, Zhou J, Zhang L and Huang D 2019 *Chin. Phys. B* **28** 010305
[10] Long G L and Liu X X 2002 *Phys. Rev. A* **65** 032302
[11] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[12] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[13] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev. A* **73** 022338
[14] Song J, Zhu A D and Zhang S 2007 *Chin. Phys.* **16** 621
[15] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys.* **16** 2149
[16] Wang C, Xiao L, Wang W Y, Zhang G Y and Long G L 2009 *J. Opt. Soc. Am. B* **26** 2072
[17] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[18] Wang T J, Li T, Du F F and Deng F G 2011 *Chin. Phys. Lett.* **28** 040305
[19] Dong L, Xiu X M, Gao Y J, Ren Y P and Liu H W 2011 *Opt. Commun.* **284** 905
[20] Kao S H and Hwang T 2013 *Chin. Phys. B* **22** 060308
[21] Ren B C, Wei H R, Hua M, Li T and Deng F G 2013 *Eur. Phys. J. D* **67** 30
[22] Gong L H, Liu Y and Zhou N R 2013 *Int. J. Theor. Phys.* **52** 3260
[23] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[24] Wu X D, Zhou L, Zhong W and Sheng Y B 2020 *Quantum Inf. Process.* **19** 354
[25] Xiao Y X, Zhou L, Zhong W, Du M M and Sheng Y B 2023 *Quantum Inf. Process.* **22** 339
[26] Hong Y P, Zhou L, Zhong W and Sheng Y B 2023 *Quantum Inf. Process.* **22** 111
[27] Hillery M, Buzk V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[28] Bagherinezhad S and Karimipour V 2003 *Phys. Rev. A* **67** 044302
[29] Schmid C, Trojek P, Bourennane M, Kurtsiefer C, Zukowski M and Weinfurter H 2005 *Phys. Rev. Lett.* **95** 230505
[30] Li C M, Chang C C and Hwang T 2006 *Phys. Rev. A* **73** 016301
[31] Wang H F, Ji X and Zhang S 2006 *Phys. Lett. A* **358** 11
[32] Deng F G, Zhou H Y and Long G L 2006 *J. Phys. A: Math. Gen.* **39** 14089
[33] Xue Z Y, Yi Y M and Cao Z L 2006 *Chin. Phys. B* **15** 1421
[34] Guo Y, Zeng G H and Chen Z G 2007 *Chin. Phys. Lett.* **24** 863
[35] Markham D and Sanders B C 2008 *Phys. Rev. A* **78** 042309
[36] Wang C and Zhang Y 2009 *Chin. Phys. B* **18** 3238
[37] Gu B, Li C Q, Xu F and Chen Y L 2009 *Chin. Phys. B* **18** 4690
[38] Gao G 2009 *Opt. Commun.* **282** 4464
[39] Gao G 2009 *Commun. Theor. Phys.* **52** 421
[40] Zhu Z C and Zhang Y Q 2010 *Chin. Phys. Lett.* **27** 060303
[41] Gao G and Wang L 2010 *Int. J. Theor. Phys.* **49** 2852
[42] Gao G 2010 *Opt. Commun.* **283** 2997
[43] Zhu Z C, Zhang Y Q and Fu A M 2011 *Chin. Phys. B* **20** 040306
[44] Gao G 2011 *Opt. Commun.* **284** 902
[45] Gao G, Fang M and Cheng M T 2012 *Chin. Phys. Lett.* **29** 110305
[46] Zhu Z C, Zhang Y Q and Fu A M 2012 *Chin. Phys. B* **21** 010307
[47] Chen X B, Niu X X, Zhou X J and Yang Y X 2013 *Quantum Inf. Process.* **12** 365
[48] Gao G 2013 *Quantum Inf. Process.* **12** 55
[49] Chen X B, Dou Z, Xu G, He X Y and Yang Y X 2017 *Sci. Rep.* **7** 39845
[50] Gao G, Wang Y and Wang D 2016 *Mod. Phys. Lett. B* **30** 1650130
[51] Gu J, Cao X Y, Yin H L and Chen Z B 2021 *Opt. Express* **29** 9165
[52] Gu J, Xie Y M, Liu W B, Fu Y, Yin H L and Chen Z B 2021 *Opt. Express* **29** 32244
[53] Jia Z Y, Gu J, Li B H, Yin H L and Chen Z B 2021 *Entropy* **23** 716
[54] Chou Y H, Zeng G J, Chen X Y and Kuo S Y 2021 *Sci. Rep.* **11** 6093
[55] Ju X X, Zhong W, Sheng Y B and Zhou L 2022 *Chin. Phys. B* **31** 100302
[56] Xing D, Wang Y F, Dou Z, Li J, Chen X B and Li L X 2023 *Chin. Phys. B* **32** 070308
[57] Kuo S Y, Tseng K C, Yang C C and Chou Y H 2023 *EPJ Quantum Technol.* **10** 29
[58] Shen A, Cao X Y, Wang Y, Fu Y, Gu J, Liu W B, Weng C X, Yin H L and Chen Z B 2023 *Sci. China Phys. Mech. Astron.* **66** 260311
[59] Li C L, Fu Y, Liu W B, Xie Y M, Li B H, Zhou M G, Yin H L and Chen Z B 2023 *Phys. Rev. Res.* **5** 033077