Two-step quantum secure direct communication scheme with frequency coding*

Xue-Liang Zhao(赵学亮)[1], Jun-Lin Li(李俊林)[1], Peng-Hao Niu(牛鹏皓)[1], Hong-Yang Ma(马鸿洋)[2], and Dong Ruan(阮东)[1,†]

[1] *Department of Physics, Tsinghua University, Beijing* 100084, *China*
[2] *School of Science, Qingdao University of Technology, Qingdao* 266000, *China*

(Received 19 October 2016; revised manuscript received 15 December 2016; published online 18 January 2017)

Quantum secure direct communication (QSDC) is an important branch of quantum cryptography. It can transmit secret information directly without establishing a key first, unlike quantum key distribution which requires this precursory event. Here we propose a QSDC scheme by applying the frequency coding technique to the two-step QSDC protocol, which enables the two-step QSDC protocol to work in a noisy environment. We have numerically simulated the performance of the protocol in a noisy channel, and the results show that the scheme is indeed robust against channel noise and loss. We also give an estimate of the channel noise upper bound.

Keywords: quantum cryptography, quantum secure direct communication, frequency coding

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/26/3/030302

1. Introduction

The security of information is more important nowadays than at any other time in history. It is significant to the success and development of our society, and it has become one of the primary concerns in everyday life. Historical conflicts within the last century, such as World War II and the subsequent Cold War have propelled many technological advancements in the security of information. Today, information security is not only crucial to national defense and military affairs, but also has gained profound importance within civilian affairs since the rise of the Internet in the 1990s. The absolute security of classical cryptography has not been proven as it is based on the existence of some difficult mathematical problems. It is always possible that some flaws might exist and the code may be broken without being announced. In contrast, quantum cryptography, which emerged in the 1980s,[1] is provably safe.[2] Since then it has attracted much attention and gained tremendous development.

Secure quantum communication includes several different modes, such as quantum key distribution (QKD),[1,3–15] quantum secret sharing (QSS),[16] and quantum secure direct communication (QSDC).[17–21] The security of these protocols is ensured by the principles of quantum mechanics, such as uncertainty principle, quantum no-cloning theorem, the principle of quantum measurement, and non-locality of entangled particles. In the earliest QKD protocol, the BB84 protocol,[1] two orthogonal bases are used to prepare the photons and encode the states. In 1991, Ekert proposed a QKD scheme based on EPR pair (E91).[3] In QKD schemes, a key is established first, and the secret information is then encoded with the key into ciphertext and sent through a classical communication.

Since the first QSDC scheme was proposed in 2000,[17] many QSDC protocols have been designed and studied.[18–67] Different from QKD, QSDC transmits a secret message directly without establishing a key first. Besides this, QSDC also satisfies two features:[18] direct communication and secure communication. Direct communication of QSDC means that an authorized receiver can obtain the secret information directly from the received quantum states without another classical transmission. Secure communication refers to the capability of QSDC that even if an eavesdropper is able to control the communication channel, she cannot get any useful information about the secret message except blind random results.

Earlier QSDC protocols are designed for ideal conditions. However, in practice, noise is inevitable, and consequently it causes losses and errors of information. There are some technologies to combat against the channel noise, such as entanglement swapping,[68,69] quantum entanglement purification,[70–73] quantum error correction,[74,75] and quantum privacy amplification.[76] Instead of the complicated schemes mentioned above, we propose a simple frequency coding scheme to a two-step QSDC protocol. This coding scheme has been applied in quantum one-time pad QSDC protocol which is also known as DL04 protocol[19] and realized in experiment recently.[77] Rather than encoding quantum qubits on every EPR pair, this frequency coding scheme encodes a block of EPR pairs into a periodic sequence in which we can analyze its frequency by using discrete time Fourier transform.

*Project supported by the National Natural Science Foundation of China (Grant Nos. 11175094, 91221205, and 11547035) and the National Basic Research Program of China (Grant No. 2015CB921002).

†Corresponding author. E-mail: dongruan@tsinghua.edu.cn

© 2017 Chinese Physical Society and IOP Publishing Ltd

The new coding scheme has a large advantage in resisting the channel losses and errors.

2. The two-step QSDC protocol with frequency coding

2.1. A description of the scheme in general

Before the coding procedure, the new protocol is completely identical to the original one.[18] The difference between the original one and this scheme is the introduction of frequency coding. The scheme contains the following five steps.

(i) Alice prepares a sequence of EPR pairs in one of the four Bell states

$$
\begin{aligned}
|\psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B),\\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B),\\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B),\\
|\phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B),
\end{aligned}
$$

where $|0\rangle$ and $|1\rangle$ represent two eigenstates of the photon polarization operator σ_z, respectively. She can prepare them in state $|\psi^-\rangle = (1/\sqrt{2})(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$.

(ii) Then Alice separates the ordered N EPR pairs into two sequences, namely, she picks up one photon from each EPR pair to form an ordered photon sequence A, called A-sequence. The remaining photons form another sequence B, called B-sequence, and there is a one-to-one correspondence between the two sequences.

(iii) Alice sends the A-sequence to Bob, while holding the B-sequence. After the A-sequence is received by Bob, he checks eavesdropping with Alice by the following steps. 1) Bob chooses moderate amounts of photons randomly from the A-sequence. Then he randomly chooses one of two measuring bases Z or X to measure the chosen photons. 2) After the measurement, Bob tells Alice which photons he has chosen, which measuring basis he used, as well as the measuring results. 3) According to the information from Bob, Alice uses the same measuring basis to measure the corresponding photons in the B-sequence. 4) Then Alice compares her results with Bob's, and estimates the error rate. If there is no eavesdropping, the error rate should be lower than the threshold, which means the transmission is safe. If not, the photon sequence should be discarded and the communication process should be ceased.

(iv) If the transmission of the A-sequence is proved secure, Alice can transmit the secret message. In the original protocol,[18] Alice uses a dense coding scheme to encode the message. Instead, the frequency coding scheme is applied with frequency coding, and specific details will be described later. Meanwhile, Alice randomly selects some photons as check bits from the B-sequence and changes their states by randomly performing one of four unitary operations

$$
\begin{aligned}
U_0 &= |0\rangle\langle 0| + |1\rangle\langle 1|, \quad U_1 = |0\rangle\langle 0| - |1\rangle\langle 1|,\\
U_2 &= |1\rangle\langle 0| + |0\rangle\langle 1|, \quad U_3 = |0\rangle\langle 1| - |1\rangle\langle 0|.
\end{aligned}
$$

(v) Alice sends the encoded sequence to Bob, and Bob performs Bell-basis measurement on two sequences simultaneously. After transmission, Alice tells Bob which photon is the check bit and what operation she has chosen. Then Bob can estimate the error rate. If the error rate is lower than the threshold, the transmission is safe. Otherwise, it will be concluded that there is an eavesdropper who is disturbing the transmission. Nevertheless, Eve will not be able to get any useful information because if the first sequence is secure, the eavesdropper cannot obtain the two photons of EPR pair for Bell-basis measurement and cannot speculate on the secret message. After excluding the check bits, Bob can do the decoding procedure to get the secret message sent by Alice.

2.2. Frequency coding with two unitary operations

Next, we will describe the frequency coding scheme in detail. This scheme was first introduced to the QSDC with single photons in Ref. [77]. As is well-known, in the original two-step QSDC protocol, information is encoded on EPR pairs directly with the four unitary operations U_0, U_1, U_2, and U_3, which correspond to 00, 01, 10, and 11, respectively. However, in a practical system, there exist losses and errors. Beyond that, the detection efficiency of single photon detectors is not 100%. This scheme provides solutions against the noises and losses using the frequency coding, which encodes the operations on EPR pairs to a periodic sequence of operations. Receivers can obtain the encoded frequency by discrete time Fourier transform, and they can translate the frequency into the secret message according to the corresponding rules established by the sender and the receiver beforehand.

To better understand this coding scheme, let us go with the single frequency situation first. In this situation, we only keep two unitary operations U_0 and U_1, which represent coding 0 and 1, respectively. First Alice chooses the coding frequency which she wants to send, then she performs the operation on the B-sequence according to the periodic function which is decided by the chosen frequency. For example, if she wants to code frequency $f = 1/T$, she can operate each photon by the following periodic subsection function (of course, she should exclude the checking photons first):

$$
\text{operation} = \begin{cases} U_1, & nT \le t_i < \left(n+\dfrac{1}{2}\right)T, \\ U_0, & \left(n+\dfrac{1}{2}\right)T \le t_i < (n+1)T, \end{cases}
$$

where T is the coding period, each photon corresponds to one time t_i, $i = 1,2,3,\ldots,N$, which is the time when the photon is

emitted, N is the total number of useful photons of B-sequence, and $n = 0, 1, 2, \ldots$ is an integer. Based on this function, Alice can adjust the period T of the flipping operations, or the number of photons of the two operations in the sequence. After the whole operation is finished, Alice sends the B-sequence to Bob in the same order of time as they arrive. After receiving the photons, Bob also records the arrival time τ_i, $i = 1, 2, 3, \ldots, N$. When the transmission is done, he performs Bell-basis measurement on the corresponding pairs of the two sequences, and obtains a periodic discrete function of 0's and 1's.

To obtain the encoded message, namely, the encoding frequency, the periodic discrete function in the time domain is transformed into the frequency domain using discrete time Fourier transform, namely,

$$X(f) = \sum_{i=1}^{N} x(i)\, \mathrm{e}^{-\mathrm{j}2\pi f \tau_i},$$

where $x(i)$ is 0 or 1 according to the operation U_0 or U_1 coded on the photon i. If we draw the frequency spectrum, we will find a peak at the encoding frequency f and other peaks are much lower than it. According to this frequency, Bob is able to get the secret message sent by Alice.

2.3. Frequency coding with multiple unitary operations

The above example explains the working principle of a single frequency coding, where only two dense coding operations U_0 and U_1 are used. Actually all four dense coding operations can be used, or all four Bell states can be used, to encode frequencies on EPR-sequences. Instead of single frequency with two unitary operations we can encode three frequencies with four unitary operations. This can increase the transmission capacity greatly and make it more difficult to crack. Here is the specific procedure. (i) Four unitary operations U_0, U_1, U_2, and U_3 correspond to 0, 1, 2, and 3 respectively, which will be used later in the frequency coding. The secret message is encoded in the frequency, not the unitary dense coding operations themselves. (ii) Here we have four unitary operations, namely, four different amplitudes 0, 1, 2, and 3. With four amplitudes, we can combine three frequencies by adding together three time sequences corresponding to three frequencies, as shown below

$$\begin{aligned} x(t) &= x_1(t) + x_2(t) + x_3(t), \\ X(f) &= X_1(f) + X_2(f) + X_3(f). \end{aligned}$$

An integer number between 0 and 3 can be obtained at each instant of time. For example, 0 corresponds to three U_0 operations, and 3 corresponds to three U_1 operations. Instead of performing three U_1 operations, Alice performs a single U_3 operation, which also represents 3. The details are as follows. Alice first decides which three frequencies to be encoded, and figures out each frequency's time domain by the above methods. Then she adds these three frequencies of operations together. There will be four different amplitudes, which can be represented by 0, 1, 2, and 3. According to this, Alice performs the corresponding unitary operation on the B-sequence. As shown in Fig. 1(c) Alice sends the sequence to Bob. Bob then follows similar steps of the single frequency situation mentioned above, and also obtains a frequency spectrum by using discrete time Fourier transform. The spectrum is the superposition of three frequencies, so three peaks can be found on the spectrum. After getting the three frequencies, Bob can obtain the secret message sent by Alice. An example is given in Fig. 1.

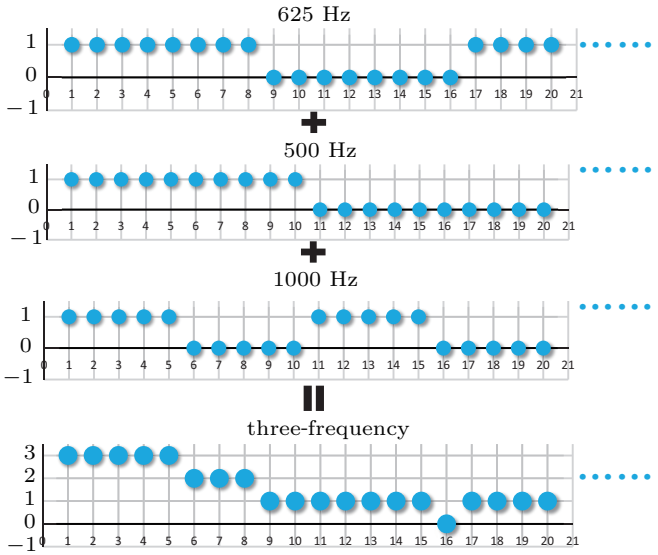


Fig. 1. (color online) Three different frequencies' direct sum in time domain. The dots represent every photon of the B-sequence. The number on the horizontal axis represents the photon number of B-sequence. The number on the vertical axis represents four different amplitudes.

3. Performance analysis in a noisy condition and numerical simulation

As in Ref. [18], if the security of the A-sequence is guaranteed, two parties of communication can ascertain that the transmission is safe. Without both photons of each EPR pair at hand, the only thing Eve could do is to disturb the communication between Alice and Bob, as she cannot perform the Bell-basis measurement to eavesdrop the secret message.

However, in a noisy channel, the situation is different. Eve can hide herself behind the noise from being detected. If she controls the communication channel completely, she can intercept the A-sequence and capture a moderate amount of photons, then replace each captured photon by the photon of an EPR pair that she prepared before. Then she sends the sequence to Bob via a channel with less noise; here we can assume Eve's channel is ideal. When Bob does the security checking, he will mistakenly think the error is generated by noise and the communication is safe. During the transmission

of the *B*-sequence, Eve captures the corresponding photons to perform Bell-basis measurement. As a result, Eve could get some of the secret information without being found. However, if the frequency coding scheme is used, it is useless for Eve to capture a few EPR pairs, since she should have enough EPR pairs for spectrum calculation. Nevertheless, if she continuously captures photons in a period of time, she may have a complete cycle with a few EPR pairs. It is much easier for Eve to speculate the frequency which Alice wants to transmit. In order to avoid this situation, more checking photons are needed (about 50%) for security check. It is also crucial to analyze the error density in different positions of the checking *B*-sequence. Suppose the channel and the instruments are reliable, the errors are generated randomly. If the error density in the sequence is much higher than any other place, it means that the sequence has been eavesdropped by Eve, then the communication should be aborted. Using this method, Eve can only intercept the photon randomly, not continuously. Suppose the error rate of the channel is e, Eve can get a fraction $2e$ of all the useful photons. Because the half photons are *A*-photon, and there is a probability of 50% that Alice and Bob cannot find the error photon caused by Eve, as Eve intercepts more photons, she gains a higher chance to speculate the frequency, so there is a channel noise upper bound for communication security. In this paper, we will give a rough estimate but not a rigorous proof.

There is a sampling theory in classical communication. Only when the sampling rate is higher than twice the maximum frequency component, the signal can be restored almost without distortion. Enlightened by the sampling theory, we borrow the idea to analyze the channel noise upper bound. According to the idea of the sampling theory, the signal cannot be restored when the sampling rate is lower than twice the maximum frequency component. But here, we allow the sampling rate to be lower than twice the minimum frequency component to ensure that the eavesdroppers cannot speculate the frequency at all. Suppose the transmission of 600 photons in each sequence block. Half of the photons in each checking sequence are checking photons, besides Alice chooses 100 photons for the second security check. In other words, there are 200 useful photons in a *B*-sequence. For example, if the minimum frequency of the channel is set as 500 Hz, Eve is unable to speculate the frequency with the sampling rate lower than 1000 Hz. Meanwhile, if the time interval of sending each photon is set as 0.1 ms, it takes 0.02 s to transmit 200 photons. Eve can capture 20 photons with the sampling rate 1000 Hz in 0.02 s. That is to say, Eve cannot get the secret information if the captured EPR pairs are less than 20. In this situation, the channel error rate is 5%, which is a rough estimate of the channel noise upper bound. Actually, according to this theory, the upper bound of the error rate is $e = 1/n$, where n is the number of photons coded in a cycle of minimum frequency. In addition, if Alice wants to transmit three identical frequencies, only 100 photons are needed in one sequence block. The 100 photons not only are enough to transmit the information, but also can reduce the photon captured by Eve. It is because one frequency is less complicated than three frequencies for Eve to guess with limited information. The following is a numerical simulation.

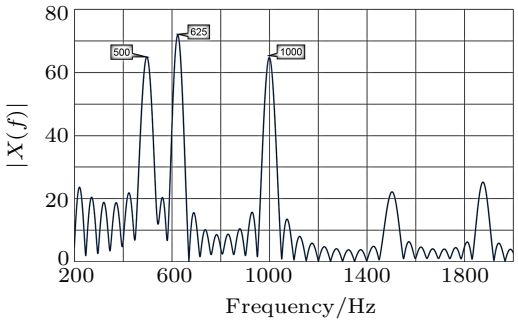


Fig. 2. (color online) The frequency spectrum in an ideal channel. The *x*-axis is the frequency and the *y*-axis is the Fourier transformed amplitude.

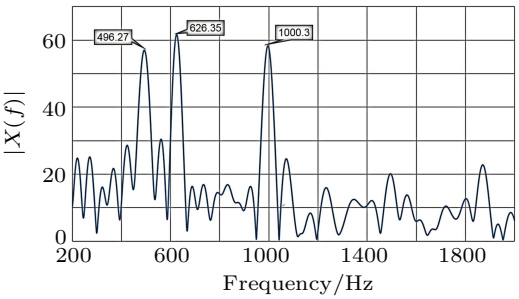


Fig. 3. (color online) The frequency spectrum in a noisy channel with 5% error rate. The *x*-axis is the frequency and the *y*-axis is the Fourier transformed amplitude.

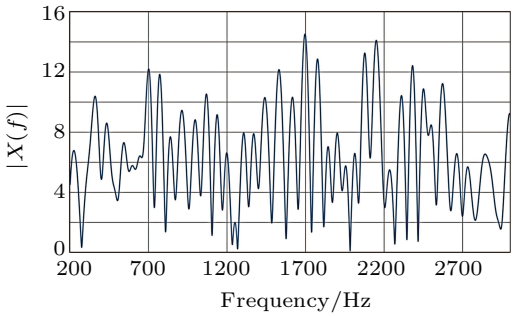


Fig. 4. (color online) The frequency spectrum that the eavesdropper gets from 10% useful photon. The *x*-axis is the frequency and the *y*-axis is the Fourier transformed amplitude.

As shown in Fig. 2, with an ideal channel, Bob's spectrum will appear three peaks obviously, which is exactly what Alice wants to transmit. If we set the frequency channel capacity as $2^4 = 16$, then one frequency can indicate 4 information bits, and three frequencies mean 12 bits of information. As shown in Fig. 3, in the presence of noise, when 20 EPR pairs are incorrect, the peak's height is lower, the width is wider, but the frequency shift is very small. Bob can still get the

accurate information by spectrum analysis. Meanwhile, Eve cannot get any useful information by spectrum analysis using only 20 EPR pairs. As shown in Fig. 4, what she gets is a completely random frequency spectrum.

4. Summary

An anti-noise frequency coding scheme to improve the two-step QSDC protocol is proposed in this paper. The new scheme has a strong ability of resisting channel losses and errors. When the security of communication is guaranteed, the receiver can still get the secret information precisely, even though the error rate is high. Also, the new scheme can improve the security of communication, because the eavesdroppers cannot get any secret information when they only capture a few EPR pairs. Though the transmission efficiency is weakened by this scheme, it can significantly improve the feasibility of the two-step QSDC protocol. It is not a complex technology, and is easy to realize. With the development of quantum entanglement technology, the two-step QSDC protocol can be realized in experiment one day. Recently, an experimental demonstration of the two-step QSDC protocol has been demonstrated.[78]

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing* (Bangalore, India) pp. 175–179
[2] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[6] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863
[7] Townsend P D 1997 *Nature* **385** 47
[8] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[9] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239
[10] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383
[11] Hwang W Y, Koh I G and Han Y D 1998 *Phys. Lett. A* **244** 489
[12] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[13] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol. A* **101** 357
[14] Deng F G and Long G L 2004 *Phys. Rev. A* **70** 012311
[15] Grosshans F and Van Assche G 2003 *Nature* **421** 238
[16] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[17] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[18] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[19] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[20] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[21] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[22] Shi J, Gong Y X, Xu P, Zhu S N and Zhan Y B 2011 *Commun. Theor. Phys.* **56** 831
[23] Meslouhi A and Hassouni Y 2013 *Quant. Inf. Proc.* **12** 2603
[24] Sun Z W, Du R G and Long D Y 2012 *Int. J. Theor. Phys.* **51** 1946
[25] Zhang Q N, Li C C, Li Y H and Nie Y Y 2013 *Int. J. Theor. Phys.* **52** 22
[26] Wang T J, Li T, Du F F and Deng F G 2011 *Chin. Phys. Lett.* **28** 040305
[27] Chang Y, Zhang S B, Yan L L and Han G H 2015 *Chin. Phys. B* **24** 080306
[28] Wang C, Liu J W, Chen X B, Bi Y G and Shang T 2015 *Chin. Phys. B* **24** 040304
[29] Zou X F and Qiu D W 2014 *Sci. China-Phys. Mech. Astron.* **57** 1696
[30] Xue P and Guo G C 2004 *J. Phys. B: At. Mol. Opt. Phy.* **37** 711
[31] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev. A* **78** 064304
[32] Yan F L and Zhang X Q 2004 *Eur. Phys. J. B* **41** 75
[33] Wang J, Zhang Q and Tang C 2006 *Phys. Lett. A* **358** 256
[34] Hong C H, Heo J, Lim J I and Yang H J 2014 *Chin. Phys. B* **23** 090309
[35] Marino A M and Stroud Jr C R 2006 *Phys. Rev. A* **74** 022315
[36] Reid M D 2013 *Phys. Rev. A* **88** 062338
[37] Li X H 2015 *Acta Phys. Sin.* **64** 0160307 (in Chinese)
[38] Ma H Y, Qin G Q, Fan X K and Chu P C 2015 *Acta Phys. Sin.* **64** 0160306 (in Chinese)
[39] Lee H, Lim J and Yang H J 2006 *Phys. Rev. A* **73** 042305
[40] Chamoli A and Bhandari C M 2009 *Quantum Inf. Proc.* **8** 347
[41] Ye T Y 2013 *Int. J. Quantum Inf.* **11** 1350051
[42] Yen C A, Horng S J, Goan H S, Kao T W and Chou Y H 2009 *Quantum Inf. Comput.* **9** 376
[43] Yadav P, Srikanth R and Pathak A 2014 *Quantum Inf. Proc.* **13** 2731
[44] Hassanpour S and Houshmand M 2015 *Quantum Inf. Proc.* **14** 739
[45] Banerjee A and Pathak A 2012 *Phys. Lett. A* **376** 2944
[46] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[47] Naseri M 2009 *Opt Commun.* **282** 1939
[48] Shaari J S, Lucamarini M and Wahiddin M R B 2006 *Phys. Lett. A* **358** 85
[49] An N B 2007 *Phys. Lett. A* **360** 518
[50] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 *Nat. Phys.* **4** 726
[51] Shukla C, Pathak A and Srikanth R 2012 *Int. J. Quantum Inf.* **10** 1241009.
[52] Gnatyuk S, Zhmurko T and Falat P 2015 *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) IEEE* 8*th International Conference on. IEEE* 1: 468–472
[53] Hong C H, Heo J O, Lim J I and Yang H J 2012 *J. Korean Phys. Soc.* **61** 1
[54] Farouk A, Zakaria M, Megahed A and Omara F A 2015 *Sci. Rep.* **5** 16080
[55] Nguyen B A 2004 *Phys. Lett. A* **328** 6
[56] Pirandola S, García-Patrón R, Braunstein S L and Lloyd S 2009 *Phys. Rev. Lett.* **102** 050503
[57] Tsai C W, Hsieh C R and Hwang T 2011 *Eur. Phys. J. D* **61** 779
[58] Vasiliu E V 2011 *Quantum Inf. Proc.* **10** 189
[59] Jahanshahi S, Bahrampour A and Zandi M H 2013 *Quantum Inf. Proc.* **12** 2441
[60] Pavičić M 2013 *Phys. Rev. A* **87** 042326
[61] Ostermeyer M and Walenta N 2008 *Opt Commun.* **281** 4540
[62] Zawadzki P, Puchała Z and Miszczak J A 2013 *Quantum Inf. Proc.* **12** 569
[63] Jain S, Muralidharan S and Panigrahi P K 2009 *Europhys. Lett.* **87** 60008
[64] Sheikhehi F and Naseri M 2011 *Int. J. Quantum Inf.* **9** 357
[65] Pathak A 2015 *Quantum Inf. Proc.* **14** 2195
[66] Zawadzki P 2013 *Quantum Inf. Proc.* **12** 149
[67] Li J, Sun F Q, Pan Z S, Nie J R, Chen Y H and Yuan K G 2015 *Chin. Phys. Lett.* **32** 080301.
[68] Żukowski M, Zeilinger A, Horne M A and Ekert A K 1993 *Phys. Rev. Lett.* **71** 4287
[69] Pan J W, Bouwmeester D, Weinfurter H and Zeilinger A 1998 *Phys. Rev. Lett.* **80** 3891
[70] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722
[71] Pan J W, Simon C, Brukner C and Zeilinger A 2001 *Nature* **410** 1067
[72] Sheng Y B, Pan J, Guo R, Zhou L and Wang L 2015 *Sci. China-Phys. Mech. Astron.* **58** 060301
[73] Du F F and Deng F G 2015 *Sci. China-Phys. Mech. Astron.* **58** 040303
[74] Calderbank A R and Shor P W 1996 *Phys. Rev. A.* **54** 1098
[75] Brassard G and Salrail L 1994 *Euro-crypt 193, Lectures Notes in Computer Sciences Vol.765* (New York: Springer-Verlag) pp. 410–423
[76] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[77] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T, Qin G Q and Long G L 2016 *Light Sci. Appl.* **5** e16144
[78] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2016 *Phys. Rev. A* **93** 022316