Design and Simulation of a Deterministic Quantum Secure Direct Communication and Authentication Protocol Based on Three-Particle Asymmetric Entangled State

Yanyan Hou[1,2(✉)], Jian Li[2,3], Qinghui Liu[4], Hengji Li[3], Xinjie Lv[1], Xuhong Li[1,2], and Yu Zhang[5]

[1] College of Information Science and Engineering, Zaozhuang University, Zaozhuang 277160, Shandong, China
hyy@uzz.edu.cn
[2] Center for Quantum Information Research, Zaozhuang University, Zaozhuang 277160, Shandong, China
[3] School of Computer Science, Beijing University of Posts and Telecommuncations, Beijing 100876, China
[4] Network Center, Zaozhuang University, Zaozhuang 277160, Shandong, China
[5] China Mobile Group Shandong Company Limited Zaozhuang Branch, Zaozhuang 277160, China

Abstract. In order to improve eavesdropping detection efficiency, we propose a quantum secure direct communication and authentication protocol based on three-particle asymmetric entangled state and design an efficient quantum circuit for implementing the protocol. This protocol has two modes, in message mode, a qubit is used to transmit two bits classical information based on a Bell state, in control mode, three-particle asymmetric entangled state is inserted into the particle flow for detecting eavesdropper. Eavesdropping detection efficiency is got by calculating the relationship between the amount of information and detection probability, if eavesdroppers want to obtain all information, detection probability is 63%, the analysis results indicate that this proposal is more secure than other quantum secure direct communication protocol.

Keywords: Quantum secure direct communication · Three-particle asymmetric entangled state · Quantum circuit

1 Introduction

Quantum secure direct communication (QSDC) and authentication is a remarkable branch of quantum information. Different from the quantum key distribution (QKD) whose object is to create a common random key between two remote authorized users, the object of QSDC is to transmit a secret message directly without

This work is supported by the National Natural Science Foundation of China (Grant No. U1636106, No. 61472048).

H. Song et al. (Eds.): SIMUtools 2019, LNICST 295, pp. 258–266, 2019.
https://doi.org/10.1007/978-3-030-32216-8_25

producing quantum keys. When eavesdroppers are detected, QSDC doesn't discard the transmitted information, so communication security is more important for QSDC, some techniques are used to make eavesdroppers get only some random values instead of reading useful information.

Bostrm and Felbinger presented a famous QSDC protocol called original Ping-pong protocol (OPP) [1], in which Bell states were used to quantum secure direct communication and detecting eavesdroppers, but researchers have found many vulnerabilities of Ping-pong protocol, for example, Ping-pong protocol cannot resist the "man-in-middle" attack. Considering two qubits with four dimensional space, Gao et al. improved eavesdropping detection efficiency of Ping-pong protocol by using four Bell states which is called MPP [2], Li et al. proposed an QSDC protocol based on extended three-particle GHZ State (EPP) [3], which is with higher eavesdropping detection efficiency. Subsequently, many researchers begin to research QSDC and authentication, Quan et al. proposed a one-way quantum secure direct communication protocol based on single photon [4], Zawadzki et al. proposed that increasing the security of Ping-pong protocol by using many mutually unbiased bases [5], some researchers researched how to ensure QSDC and authentication security under the noise environment [6–8]. Recently, more and more researchers begin to study how to improve quantum direct communication efficiency [9–14], some researchers proposed using W state for QSDC and authentication [15–20], subsequently, Multi-particle entangled state were used to QSDC protocol [21–24], Zhang et al. proposed a QSDC protocol using semi quantum for improving eavesdropping detection efficiency [25], but researchers have found many vulnerabilities in Ping-pong protocol. In this paper, we not only propose a quantum security detection protocol based on three-particle asymmetric entangled state (TAPP), but also design an efficient quantum circuit for implementing the protocol. If the eavesdropper gets the full information, the detection rate of the original Ping-pong protocol is 50%, the detection rate of proposed protocol is 63%. Compared with other QSDC protocols, this protocol is with higher eavesdropping detection efficiency.

2 The Process of the TAPP Protocol

In original Ping-pong protocol, a Bell state was used to transmit information and detect eavesdroppers and a qubit transmitted one bit classical information, so information transmission efficiency was not high. In proposed protocol, Alice transmits information to Bob by dense coding, in which a qubit transmits two bits classical information. The steps are as follows.

(1) Suppose that Alice wants to transmit an information sequence $x^N = (x_1, \ldots, x_N)$ to Bob, where $x_i \in \{0, 1\}, i = 1, 2, \ldots, N$. Bob prepares N pairs Bell state particles $\left|\psi^+\right\rangle_{AB} = (|01\rangle_{AB} + |10\rangle_{AB})/\sqrt{2}$, all the first particles in Bell states are stored as A sequence (travel particles), all the remaining particles in Bell states are transmitted to Alice as B sequence (home particles).

(2) In order to prevent Eve from eavesdropping and ensure the information communication security, this paper proposes two communication modes, message

mode and control mode. Bob prepares a large number of asymmetric three-particle entangled states $|\varphi\rangle = \frac{1}{2}|011\rangle + \frac{1}{\sqrt{2}}|100\rangle + \frac{1}{2}|101\rangle$ as detection particles, which are inserted into A sequence to form C sequence, only Bob knows the position of detection particles. Compared with B sequence, C sequence contains $3cN/(1-c)$ particles which are used to detect eavesdroppers, here, c is the probability of the control mode.

(3) Bob sends C sequence to Alice and notifies her the location of detection particles. If Alice receives detection particles, she switches to control mode and measures detection particles based on the three-particle unsymmetrical entanglement state. Alice sends the detection result through the public channel to Bob, if eavesdroppers are found, Alice interrupts this communication and transmits the information again, otherwise Bob notifies Alice no eavesdroppers and continues to transmit information.

(4) If Alice receives travel particles, she switches to message mode. According to transmitted information, Alice performs one of four coding operation $\{\hat{I}, \hat{\sigma_z}, \hat{\sigma_x}, i\hat{\sigma_y}\}$ on the travel particles.

$$\begin{aligned}
\hat{I}^{(A)}\left|\psi^+\right\rangle &= \left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
\hat{\sigma}_z^{(A)}\left|\psi^+\right\rangle &= |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\
\hat{\sigma}_x^{(A)}\left|\psi^+\right\rangle &= \left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
i\hat{\sigma}_y^{(A)}\left|\psi^+\right\rangle &= |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)
\end{aligned} \tag{1}$$

The superscript *(A)* refers to the operation of the travel particle in the Bell states. After encoding, each travel particle can indicate two bits classical information, $\left|\psi^+\right\rangle$ indicates 00, $|\psi^-\rangle$ indicates 01, $\left|\phi^+\right\rangle$ indicates 10, $|\phi^-\rangle$ indicates 11.

(5) Alice sends encoded travel particles back to Bob, Bob measures the encoded travel particles and home particles based on Bell states and gets $\left|\psi^+\right\rangle$, $|\psi^-\rangle$, $\left|\phi^+\right\rangle$ or $|\phi^-\rangle$, respectively correspond to classical bits 00, 01, 10 or 11, Bob extracts information and completes quantum secure direct communication.

3 Quantum Circuit Simulation of TAPP Protocol

The circuit simulation is instructive for the realization of QSDC protocol and authentication, quantum circuit is essential to the practical realization of the protocol in experiment. In this section, we construct an efficient quantum circuit for TAPP protocol simulation. Firstly, TAPP protocol is decomposed unitary transformations, secondly,

the effective quantum circuit is designed through the orderly arrangement of the quantum gates. The quantum circuit implementation is shown in Fig. 1.

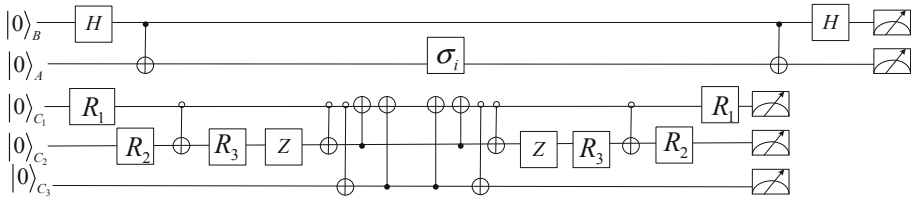

Fig. 1. Quantum circuit for implementation TAPP protocol

In Fig. 1, particle A and B are information carrier, firstly, $|0\rangle_B$ and $|0\rangle_A$ are sent to H gate and Bell state $\left|\psi^+\right\rangle_{AB} = (|01\rangle_{AB} + |10\rangle_{AB})/\sqrt{2}$ is got, then the sender Alice implements quantum information coding through a unitary operation $\sigma_i \in \{\hat{I}, \hat{\sigma_z}, \hat{\sigma_x}, i\hat{\sigma_y}\}$, the receiver Bob realizes quantum measurement through H gate and gets the transmitted information. Three-particle asymmetric entangled state $|\varphi\rangle = \frac{1}{2}|011\rangle + \frac{1}{\sqrt{2}}|100\rangle + \frac{1}{2}|101\rangle$ is got by making unitary transformation for $|0\rangle_{c_1}, |0\rangle_{c_2}, |0\rangle_{c_3}$, Alice measures the received three particle entangled state, so as to realize eavesdropping detection. R_1, R_2, and R_3 are respectively.

$$R_1 = R_y(\frac{\pi}{2}), R_2 = R_y(\frac{\pi}{4}), R_3 = R_y(-\frac{\pi}{4}) \tag{2}$$

$$R_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{3}$$

4 The Security Analysis and Simulation of TAPP

In control mode, Alice inserts asymmetric three-particle entangled state $|\varphi\rangle = \frac{1}{2}|011\rangle + \frac{1}{\sqrt{2}}|100\rangle + \frac{1}{2}|101\rangle$ into A sequence for eavesdropping detection. After Eve's attack operation $\hat{E}$, the particle state $|0\rangle$ is transformed into $\left|\varphi_0^{'}\right\rangle$, the particle state $|1\rangle$ is transformed into $\left|\varphi_1^{'}\right\rangle$.

$$\left|\varphi_0^{'}\right\rangle = \hat{E}|0x\rangle = \alpha|0x_0\rangle + \beta|1x_1\rangle, \left|\varphi_1^{'}\right\rangle = \hat{E}|1y\rangle = m|0y_0\rangle + n|1y_1\rangle \tag{4}$$

$|x\rangle$ and $|y\rangle$ are determined by $\hat{E}$ uniquely, $|\alpha|^2 + |\beta|^2 = 1, |m|^2 + |m|^2 = 1$. After Eve attacks on the asymmetric three-particle entangled state, the state of the compose system is.

$$
\begin{aligned}
&|\varphi\rangle_{Eve}= E\otimes E\otimes E[\frac{1}{2}|011\rangle+\frac{1}{\sqrt{2}}|100\rangle+\frac{1}{2}|101\rangle]\\
&=\frac{1}{2}[\alpha|0x_0\rangle+\beta|1x_1\rangle]\otimes[m|0y_0\rangle+n|1y_1\rangle]\otimes[m|0y_0\rangle+n|1y_1\rangle]\\
&+\frac{1}{\sqrt{2}}[m|0y_0\rangle+n|1y_1\rangle]\otimes[\alpha|0x_0\rangle+\beta|1x_1\rangle]\otimes[\alpha|0x_0\rangle+\beta|1x_1\rangle]\\
&+\frac{1}{2}[m|0y_0\rangle+n|1y_1\rangle]\otimes[\alpha|0x_0\rangle+\beta|1x_1\rangle]\otimes[m|0y_0\rangle+n|1y_1\rangle]\\
&=\frac{1}{2}[\alpha m^2|0x_00y_00y_0\rangle+\beta m^2|1x_10y_00y_0\rangle+\alpha nm|0x_01y_10y_0\rangle+\beta nm|1x_11y_10y_0\rangle\\
&+\alpha mn|0x_00y_01y_1\rangle+\beta m^2|1x_10y_01y_1\rangle+\alpha n^2|0x_01y_11y_1\rangle+\beta n^2|1x_11y_11y_1\rangle]\\
&+\frac{1}{\sqrt{2}}[\alpha^2m|0y_00x_00x_0\rangle+\alpha^2n|1y_10x_00x_0\rangle+\alpha\beta m|0y_01x_10x_0\rangle+\alpha\beta n|1y_11x_10x_0\rangle\\
&+\alpha\beta m|0y_00x_01x_1\rangle+\alpha\beta n|1y_10x_01x_1\rangle+\beta^2m|0y_01x_11x_1\rangle+\beta^2n|1y_11x_11x_1\rangle]\\
&+\frac{1}{2}[m^2\alpha|0y_00x_00y_0\rangle+\alpha nm|1y_10x_00y_0\rangle+m^2\beta|0y_01x_10y_0\rangle+m^2\beta|1y_11x_10y_0\rangle\\
&+\alpha mn|0y_00x_01y_1\rangle+\alpha^2n|1y_10x_01y_1\rangle+mn\beta|0y_01x_11y_1\rangle+\beta^2n|1y_11x_11x_1\rangle]
\end{aligned}
\tag{5}
$$

The probability that Alice not detect eavesdroppers is.

$$
\begin{aligned}
p(|\varphi\rangle)=\frac{1}{4}[\left|\beta m^2\right|^2+\left|\alpha n^2\right|^2+|\beta mn|^2]+\frac{1}{2}[\left|\alpha^2n\right|^2+\\
|\alpha\beta n|^2+\left|\beta^2m\right|^2]+\frac{1}{4}[|mn\alpha|^2+\left|\alpha n^2\right|^2+|\beta mn|^2]
\end{aligned}
\tag{6}
$$

So the lower bound of the detection probability is.

$$
\begin{aligned}
d_l=1-p(|\varphi\rangle)=1-\frac{1}{4}[\left|\beta m^2\right|^2+\left|\alpha n^2\right|^2+|\beta mn|^2]\\
+\frac{1}{2}[\left|\alpha^2n\right|^2+|\alpha\beta n|^2+\left|\beta^2m\right|^2]+\frac{1}{4}[|mn\alpha|^2+\left|\alpha n^2\right|^2+|\beta mn|^2]
\end{aligned}
\tag{7}
$$

Assuming $|\alpha|^2=a, |\beta|^2=b, |m|^2=s, |n|^2=t$, a, b, s, t are positive real numbers and $a+b=s+t=1$, so d_l is.

$$
\begin{aligned}
&d_l=1-p(|\varphi\rangle)\\
&\quad=1-[\frac{1}{4}(1-a)(1-t)+\frac{1}{2}at^2+\frac{1}{2}at+\frac{1}{4}t(1-t)+\frac{1}{2}(1-a)^2(1-t)]
\end{aligned}
\tag{8}
$$

When Alice sends $|0\rangle$ to Bob, the amount of information which be eavesdropped by Eve is.

$$I_0 = -a\log_2 a - (1-a)\log_2(1-a) = H(a) \tag{9}$$

When Alice sends $|1\rangle$ to Bob, the amount of information which be eavesdropped by Eve is.

$$I_1 = -t\log_2 t - (1-t)\log_2(1-t) = H(t) \tag{10}$$

Eve can eavesdrop the total amount of information is.

$$I = \frac{1}{2}(I_0 + I_1) = \frac{1}{2}(H(a) + H(t)) \tag{11}$$

Considering the equal probability of sending $|0\rangle$ and $|1\rangle$ in the general system, that is $a = t$, we can get.

$$d_l = -2a^2 + \frac{7}{4}a + \frac{1}{4} \tag{12}$$

After simple mathematical calculation, we can get a.

$$a = \frac{7}{16} + \frac{1}{16}\sqrt{81 - 128d_l} \tag{13}$$

Under the condition $d_l \leq 0.63$, the relationship between the information function I and detection probability d_l is as follows.

$$I(d_l) = H(\frac{7}{16} + \frac{1}{16}\sqrt{81 - 128d_l}) \tag{14}$$

Under the condition $d_l > 0.63$, eavesdropped information is too large to meet the requirements of quantum secure communication, the situation can be ignored. In order to realize the security detection analysis, TAPP is compared with OPP, MPP and EPP protocol, Fig. 2 shows the relationship between the information function I and detection probability d_l for OPP, MPP, EPP and TAPP protocol.

Comparing with OPP, MPP and EPP, we can see that if Eve eavesdrops the same amount of information (I), he must face greater eavesdropping detection probability in TAPP, this also shows that TAPP is more secure than OPP, MPP and EPP.

In order to get this advantage in TAPP, Alice needs to send $2cN/(1-c)$ particles more than OPP, $cN/(1-c)$ particles more than MPP, in other words, Bob gets better security at the cost of sending more particles. If Eve wants to get all information ($I = 1$) of Alice, d_l is 0.63 in TAPP, d_l is 0.5 in OPP and MPP, d_l is 0.58 in EPP, so detection probability of TAPP is higher than that of OPP, MPP and EPP.

When the probability of control mode is c, the probability of message mode is $r = 1 - c$. Assuming Bob sends the first particle in message mode, the probability of successful eavesdropping is $1 - c$; assuming Bob sends the first particle in control

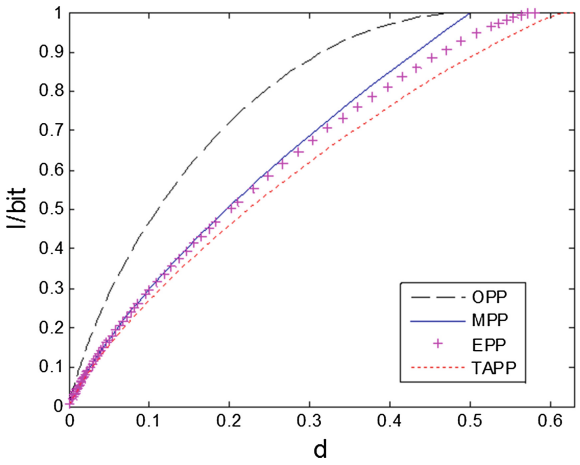

Fig. 2. The comparison of the three detection results

mode and the second particle in message mode, the probability of successful eavesdropping is $c\,(1-d)\,(1-c)$. Similarly, the probability of successful eavesdropping by Eve can be obtained in each case. If Eve is not detected, the probability of successful eavesdropping is.

$$\begin{aligned} s(c,d) &= (1-c)+c(1-d)(1-c)+c^2(1-d)^2(1-c)+\ldots \\ &= (1-c)/[1-c(1-d)] \end{aligned} \tag{15}$$

After n successful eavesdropping, Eve can get $2nI(d)$ bits information, this probability is s^n, the probability for successful eavesdropping $I = 2nI(d)$ bit information is.

$$s(I,c,d) = s(c,d)^{I/2I(d)} = ((1-c)/(1-c(1-d)))^{I/2I(d)} \tag{16}$$

When c = 0.5 and $I(d) = H(\frac{7}{16} + \frac{1}{16}\sqrt{81-128d})$, we get eavesdropping success probability s as a function of the information I. Figure 3 shows eavesdropping success probability as a function of the maximal eavesdropped information I for different detection probabilities d.

In Fig. 3, When $I \to \infty$, $s \to 0$ is got, Eve only gets part of right information but does not even know which part, so the TAPP protocol can be thought as asymptotically secure. If desired, the security can arbitrarily be improved by increasing the control parameter c at the cost of decreasing information transmission rate.

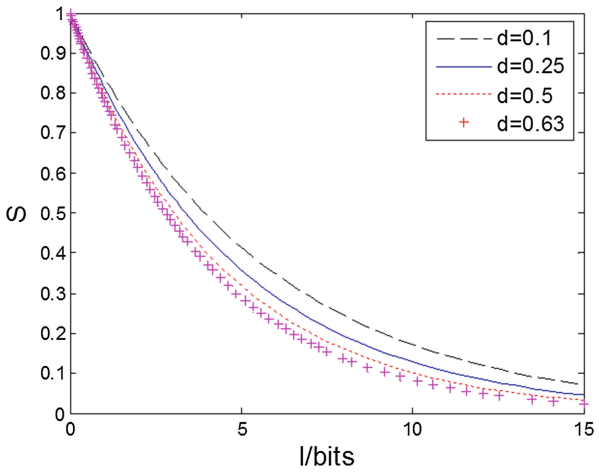

Fig. 3. Eavesdropping success probability as a function of the maximal eavesdropped information I, plotted for different detection probabilities d

5 Conclusions and Future Work

In this paper, a new quantum security direct communication protocol TAPP is proposed based on Ping-pong protocol. Two bits classical information can be transmitted by the Bell state and the three-particle asymmetric entangled state is used to realize quantum secure direct communication. By calculating the relationship between the eavesdropped information and detection probability, we find that the TAPP protocol is with higher eavesdropping detection efficiency compared with the OPP, MPP and EPP. The detection efficiency of TAPP can meet the security requirements of quantum direct communication, but the improvement of detection efficiency is at the cost of decreasing information transmission rate. This protocol is mainly theoretical research and not considering noise and Dos attack, besides, the practical application needs considering the quantum state storage, which needs to be researched in the future work.

References

1. Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett **89**(18), 187902 (2002)
2. Gao, F., Guo, F.Z., Wen, Q.Y., et al.: Comparing the efficiencies of different detect strategies in the ping-pong protocol. Sci. China **51**(12), 1853–1860 (2008)
3. Li, J., Guo, X.J., Song, D.J., et al.: Improved quantum "Ping-Pong" protocol based on extended three-particle GHz state. China Commun. **9**(1), 111–116 (2012)
4. Quan, D.X., Pei, C.X., Liu, D., et al.: One-way deterministic secure quantum communication protocol based on single photons. Acta Physica Sinica **59**(4), 2493–2497 (2010)
5. Zawadzki, P., Puchała, Z., Miszczak, J.A.: Increasing the security of the ping-pong protocol by using many mutually unbiased bases. Quantum Inf. Process. **12**(1), 569–576 (2013)

6. Huang, W., Wen, Q.-Y., Jia, H.-Y., et al.: Fault tolerant quantum secure direct communication with quantum encryption against collective noise. Chin. Phys. B **21**(10), 101–109 (2012)
7. Hu, J.Y., Yu, B., Jing, M.Y., et al.: Experimental quantum secure direct communication with single photons. Light Sci. Appl. **5**(9), e16144 (2016)
8. He, Y.F., Ma, W.P.: Three-party quantum secure direct communication against collective noise. Quantum Inf. Process. **16**(10), 252 (2017)
9. Yang, C.W., Hwang, T.: Improved QSDC Protocol over a collective-dephasing noise channel. Int. J. Theor. Phys. **51**(12), 3941–3950 (2012)
10. Aravinda, S., Banerjee, A., Pathak, A., Srikanth, R., et al.: Orthogonal-state-based cryptography in quantum mechanics and local post-quantum theories. Int. J. Quantum Inf. **12**(07n08), 175–179 (2014)
11. Xu, S.J., Chen, X.B., Wang, L.H., et al.: Two quantum direct communication protocols based on quantum search algorithm. Int. J. Theor. Phys. **54**(7), 2436–2445 (2015)
12. Feng, Z.F., Yang, O.Y., Zhou, L., et al.: Entanglement assisted single-photon W state amplification. Opt. Commun. **340**, 80–85 (2015)
13. Wu, F.Z., Yang, G.J., Wang, H.B., et al.: High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states. Sci. China (Phys. Mech. Astron.) **60**(12), 120313 (2017)
14. Li, J., Li, N., Li, L.L., Wang, T.: One step quantum key distribution based on EPR entanglement. Sci. Rep. **6**, 28767 (2016)
15. Chang, S.K.: Improved protocols of secure quantum communication using W states. Int. J. Theor. Phys. **52**(6), 1914–1924 (2013)
16. Chia-Wei, T., Tzonelih, H.: Deterministic quantum communication using the symmetric W state. Sci. China (Phys. Mech. Astron.) **56**(10), 1903–1908 (2013)
17. Shukla, C.: Design and analysis of quantum communication protocols. Chem. Res. Toxicol. **15**(7), 972–978 (2015)
18. Toshinai, K., Mondal, M.S., Nakazato, M., et al.: On optimising quantum communication in verifiable quantum computing. J. Bacteriol. **165**(1), 321–323 (2015)
19. Wu, Y., Zhou, J., Gong, X., et al.: Continuous-variable measurement-device-independent multipartite quantum communication. J. Phys. Soc. Jpn. **86**(2), 2325 (2016)
20. Nie, Y.Y., Li, Y.H., Liu, J.C., et al.: Quantum state sharing of an arbitrary three-qubit state by using four sets of W-class states. Opt. Commun. **284**(5), 1457–1460 (2011)
21. Wang, M., Ma, W., Shen, D., et al.: A new controlled quantum secure direct communication protocol based on a four-qubit cluster state. Mod. Phys. Lett. B **28**(24), 1450194 (2014)
22. Li, Y.B., Song, T.T., Huang, W., et al.: Fault-tolerant quantum secure direct communication protocol based on decoherence-free states. Int. J. Theor. Phys. **54**(2), 589–597 (2015)
23. Chang, Y., Zhang, S.B., Yan, L.L.: A bidirectional quantum secure direct communication protocol based on five-particle cluster state. China Phys. Lett. **30**(9), 090301 (2013)
24. Liu, Z., Chen, H., Liu, W.: Cryptanalysis of controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. Int. J. Theor. Phys. **55**(10), 4564–4576 (2016)
25. Zhang, M.H., Li, H.F., Xia, Z.Q., et al.: Semiquantum secure direct communication using EPR pairs. Quantum Inf. Process. **16**(5), 117 (2017)