Secure Private Comparison of Equality using Quantum Resources

Tingting Wei and Cai Zhang*

College of Mathematics and informatics, South China Agricultural University, Guangzhou 510642, China

*Corresponding author email: zhangcai@scau.edu.cn

Abstract. Private comparison of equality is an essential task in secure multiparty computation. In this paper, we investigate such a task in quantum settings. Particularly, we design a comparison protocol using quantum resources. The protocol allows three users to verify whether the private inputs of three users are identical and preserve their inputs’ privacy without an extra third party who can help the verifying process. The proposed protocol does not require unitary operations for the information encoding, which, to some extent, facilitates the protocol’s implementation. In addition, the Trojan horse attacks are invalid to the proposed protocol as it only employs one-step quantum transmissions. We also show that the presented protocol is secure against some well-known attacks.

1. Introduction

The protocol for the millionaires’ problem was presented by Yao [1] for the first time in 1998. This protocol aims at determining who is richer between two users and keeping the privacy of their wealth. Since then, many researchers have been investigating how to compare private information. Reference [2] showed a protocol to verify whether two users’ private inputs are the same. Lo [3] proved that two-party equality evaluation in quantum settings is not secure. Yang et al. [4] used Einstein-Podolsky-Rosen pairs and a hash function for the design of the protocol of quantum private comparison (QPC). Reference [5] gave an efficient protocol to check if the users’ inputs are the same using triplet states. Tseng et al. [6] presented a protocol with high efficiency for equality comparison. In their protocol, it is not necessary to utilize EPR pairs. References [7-10] investigated QPC protocols that employ various entangled states like triplet W states and x-type states. Huang et al. [11] proposed a protocol to privately compare the inputs between users and investigated the effect of collective noise on their protocol. In reference [12], single photons are used to design a QPC protocol in which collective detection is involved. In reference [13], a quantum research algorithm is utilized for the construction of a QPC protocol. Ji et al. [14] presented several QPC protocols, in each of which entanglement and dense coding are employed. Note that these protocols are for the private comparison in a two-party scenario. One may be interested in private comparison among multiple parties. Reference [15] gave one of such protocols using GHZ class states. Reference [16] presented another one depending on d-dimensional basis states and in this protocol, entanglement swapping is not required. We were interested in other quantum states that can be employed to devise multiparty QPC protocols. Finally, based on the genuinely maximally entangled six-qubit state, we devise a three-party QPC protocol without an extra third party. Our contributions are: (1) presenting a novel three-party protocol for equality comparison which does not require unitary operations for encoding; (2) and giving a method to
They intend to verify whether the equation $|10\rangle\rangle$, $|\pm\rangle\rangle = \sqrt{\frac{1}{2}}(|0\rangle - |1\rangle)$

Two bases quantum channels are also authenticated. Three users in our protocol can be denoted by

detect participants’ attacks based on fake quantum states. We hope our work can help researchers to

We organize the rest of the paper in the following: Section 2 gives the details of the quantum state we

Quantum entanglement is important and useful, and has been applied in many quantum protocols

Reference [24] first shows a special entangled state that can be written as

We hope our work can help researchers to

Including quantum dense coding [17], quantum teleportation [18], quantum secure direct

Quantum entanglement is important and useful, and has been applied in many quantum protocols

We organize the rest of the paper in the following: Section 2 gives the details of the quantum state we

Reference [24] first shows a special entangled state that can be written as

This six-qubit state is denoted by $\varphi_6$ hereafter and it will be employed to construct a secure three-party

Two bases $B_1 = \{|\eta_1\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi^+\rangle + |1\rangle|\phi^+\rangle), |\eta_2\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\phi^-\rangle - |1\rangle|\psi^-\rangle), |\eta_3\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\phi^+\rangle - |1\rangle|\psi^+\rangle), |\eta_4\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi^-\rangle + |1\rangle|\phi^-\rangle), |\eta_5\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\phi^-\rangle + |1\rangle|\psi^-\rangle)\rangle\rangle$ and $B_2 = \{|\eta_1\rangle\rangle = \frac{1}{\sqrt{2}}(|+\rangle|\phi^+\rangle + |-\rangle|\psi^+\rangle), |\eta_2\rangle\rangle = \frac{1}{\sqrt{2}}(|+\rangle|\psi^-\rangle - |1\rangle|\phi^-\rangle), |\eta_3\rangle\rangle = \frac{1}{\sqrt{2}}(|+\rangle|\psi^+\rangle + |1\rangle|\phi^+\rangle - |1\rangle|\psi^+\rangle), |\eta_4\rangle\rangle = \frac{1}{\sqrt{2}}(|+\rangle|\phi^-\rangle - |1\rangle|\psi^-\rangle)\rangle\rangle, |\eta_5\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi^-\rangle - |1\rangle|\phi^-\rangle), |\eta_6\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\phi^-\rangle + |1\rangle|\psi^-\rangle)\rangle\rangle\rangle\rangle$, where $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\rangle\rangle\rangle\rangle, |\phi^+\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |1\rangle)\rangle\rangle\rangle\rangle, |\phi^-\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |1\rangle)\rangle\rangle\rangle\rangle, |\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\rangle\rangle\rangle\rangle, and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\rangle\rangle\rangle\rangle$, are needed to detect the honesty of the user who generates and distributes the particles of $\varphi_6$.

We adopt the assumption that the classical channels in our protocol are authenticated and that the quantum channels are also authenticated. Three users in our protocol can be denoted by $P_1, P_2$ and $P_3$, respectively. Suppose that $P_i (i = 1, 2, 3)$ has a secret bit string $msg_i$ with length of $l$ as his/her private input. They intend to verify whether the equation $msg_1 = msg_2 = msg_3$ holds, and meanwhile keep their private inputs secret. The protocol works on the assumption that $P_1$ is the user who prepares the state $\varphi_6$. Three users in advance agree on the following encoding: $|\psi^+\rangle$ is encoded as bits 00; $|\psi^-\rangle$ is encoded as bits 10; $|\phi^+\rangle$ is encoded as bits 10; $|\phi^-\rangle$ is encoded as bits 11. This encoding rule will be used to generate users’ private keys according to their measurement results.

The whole process of our protocol is in the following:

(I) $P_1$ generates $\left\lfloor \frac{l}{2} \right\rfloor + \theta$ ( $\left\lfloor \cdot \right\rfloor$ represents the ceiling function) $\varphi_6$. He/she then selects particles 3 and 4 (particles 6 and 5) from each $\varphi_6$ to construct an ordered sequence $T_{34}$ ($T_{65}$). Next, $P_1$ generates $2d$ decoy particles to detect outside eavesdropping. The quantum state of each of the decoy particles is chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ randomly. After that he/she at random puts the first (second) $d$ decoy particles into $T_{34}$ ($T_{65}$) to produce a new sequence $T'_{34}$ ($T'_{65}$). Note that the initial states of the decoy particles and their positions in $T'_{34}$ and $T'_{65}$ should not be revealed to anyone at this step.
Finally, $P_1$ sends $T^*_3$ and $T^*_{65}$ to $P_2$ and $P_3$, respectively, and holds the sequence $T_{12}$ that orderly consists of particles 1 and 2 from each $V_{60b}$ in his/her own lab.

(II) After $P_2$ and $P_3$ have received $T^*_3$ and $T^*_{65}$, respectively, the information of the decoy states and their positions in $T^*_3$ and $T^*_{65}$ is sent to $P_2$ and $P_3$, respectively. $P_2$ ($P_3$) then performs appropriate measurements on the decoy particles with the basis $\{|0\rangle, |1\rangle\}$ (C-basis) or the basis $\{|+, |\rangle\}$ (D-basis) depending on $P_i$’s information. Specifically, given that a decoy particle’s initial state is in $|0\rangle$ or $|1\rangle$ ($|+\rangle$ or $|\rangle\rangle$), the measurement with the C-basis (the D-basis) will be performed on this particle. $P_2$ ($P_3$) then announces his/her measurement results. Based on these results and the decoy particles’ initial states, $P_1$ calculates a rate of errors occurred. A high error rate exceeding the threshold will lead to an abortion of the protocol, and the protocol will then restart from Step (I).

The low error rate below the threshold allows the protocol to proceed.

(III) In this step, $P_2$ collaborates with $P_3$ to detect the honesty of $P_1$, namely $P_2$ ($P_3$) should exactly receive $T_{34}$ ($T_{65}$). First, $P_2$ ($P_3$) takes out the decoy particles from $T^*_3$ ($T^*_{65}$) to obtain $T^*_{34}$ ($T^*_{65}$). Next, they select $\theta$ states of $\varphi_i$ (sample states) randomly for detection and announce the sample states’ positions to $P_1$. $P_2$ and $P_3$ then request $P_1$ to perform measurement with a random basis from $\{|0\rangle, |1\rangle, |+\rangle, |\rangle\rangle\}$ on particles 1 and 2 of each sample state. Given that $P_1$ carries out a measurement with the C-basis (the D-basis) on particles 1 and 2, $P_2$ does a measurement with the C-basis (the D-basis) on particle 3, and $P_2$ and $P_3$ perform a measurement with the basis $B_2$ ($B_2$) on particles 4, 5, 6. At last, $P_2$ and $P_3$ compute a rate of errors occurred by comparing their measurement results. A high rate of errors which exceeds the threshold will give rise to an abortion of the protocol, and the protocol will then restart from Step (I). The low error rate below the threshold suggests that $P_2$ ($P_3$) exactly receives $T_{34}$ ($T_{65}$) and it allows the protocol to proceed to the next step.

(IV) After discarding the sample states, $P_1$ ($P_2$, $P_3$) performs a measurement with the Bell basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ on particles 1 and 2 (particles 3 and 4, particles 6 and 5) of the $k$-th $\varphi_i$ ($k = 1, 2, ..., \left\lceil \frac{n}{2}\right\rceil$). $P_1$ ($P_2$, $P_3$) then uses his/her measurement results and the encoding rule to obtain his/her key $key_1$ ($key_2$, $key_3$) that should not be learned by others. For instance, if the measurement results of the $i$-th $\varphi_i$ is $V^i_{12} = |\phi^+\rangle$ ($V^i_{34} = |\phi^+\rangle$, $V^i_{65} = |\psi^+\rangle$), the $k$-th two bits of $key_1$ ($key_2$, $key_3$) should be 10 (10, 00). $P_2$ ($P_2$, $P_3$) eventually calculates $cmsg_1 = msg_1 \oplus key_1$ ($cmsg_2 = msg_2 \oplus key_2$, $cmsg_3 = msg_3 \oplus key_3$) (Here, $\oplus$ represents the operation of pointwise addition in modulo two.)

(V) $P_2$ and $P_3$ reveal $cmsg_2$ and $cmsg_3$ to $P_1$, respectively, he/she then verifies whether the equation $msg_2 = cmsg_3$ holds. If $msg_2 \neq cmsg_3$, $P_1$ publishes the comparison result and all users obtain it. If $msg_2 = cmsg_3$, $P_1$ calculates either $cmsg_{13} = cmsg_1 \oplus cmsg_3$ or $cmsg_{12} = cmsg_1 \oplus cmsg_2$ at random. In the case where $P_1$ obtains $cmsg_{13}$, he/she announces $cmsg_{13}$ to $P_2$. Later, $P_2$ checks if the equation $msg_1 = cmsg_3$ holds based on $key_2$ and $cmsg_{13}$. In the case where $P_1$ obtains $cmsg_{12}$, he/she announces $cmsg_{12}$ to $P_3$. Later, $P_3$ checks if the equation $msg_2 = cmsg_2$ holds based on $key_3$ and $cmsg_{12}$. In either case, three users are eventually able to verify whether the equation $msg_1 = msg_2 = cmsg_3$ holds, and keep their private inputs secret, respectively.

3. Analysis of the Presented Protocol

3.1. Correctness Analysis

We now analyse the presented protocol’s correctness. The properties of the state $\varphi_i$ and the encoding rule give $key_1 \oplus key_2 \oplus key_3 = 0$ (0 here denotes a bit string that has l 0s) in Step (V) of our protocol. Upon receiving $cmsg_2$ and $cmsg_3$ from $P_2$ and $P_3$, respectively, $P_1$ could compute

$$
key_1 \oplus cmsg_2 \oplus cmsg_3 = key_1 \oplus key_2 \oplus msg_2 \oplus key_3 \oplus msg_3 = msg_2 \oplus msg_3.
$$

After that, $P_1$ can check if $msg_2 \oplus msg_3 = 0$ holds based on the above equation. If $P_1$ learns that $msg_2 \oplus msg_3 \neq 0$, he/she then announces that $msg_1 = msg_2 = msg_3$ does not hold and the
procedure of the protocol terminates. Otherwise, $P_2$ ($P_3$) can check if $msg_1 = msg_3$ ($msg_1 = msg_2$) holds similarly in Step (V). The protocol can eventually correctly check if $msg_1 = msg_2 = msg_3$ holds or not.

3.2. Analysis of Security

3.2.1. Analysis of Security Against Outside attacks. Decoy particles are usually used to detect eavesdropping attacks like intercept-resend and entanglement-measurement attacks. This similar idea was first used in the BB84 protocol [24]. The outside adversary Eve who intends to eavesdrop will be caught in Step (II) of the protocol. Here we analyse the case where Eve starts an attack by intercepting the C-basis measurement to catch in Step (II). Here we analyse the case where Eve starts an attack by intercepting and resending particles. Suppose that a decoy particle’s state is $|0\rangle$. As Eve knows nothing about all the quantum states of decoy particles, she may perform the measurement with the C-basis or the D-basis randomly on this decoy particle, and transmit a fake one generated by her own relying on the result after measurement to $P_2$ or $P_3$. In Step (II), the probability that the attack will be detected is $1/4$. $d$ such decoy particles give the probability of being caught $Pr = 1 - \left(\frac{3}{4}\right)^d$. $Pr$ will be approaching to 1 as $d$ goes large enough. Therefore, this attack started by Eve will be invalid to our protocol. Obviously, Eve can easily obtain $cmsg_{12}$, $cmsg_{3}$, $cmsg_{13}$ and $cmsg_{12}$. However, these ciphertexts are encrypted by the keys that are in users’ hands. Eve thus cannot derive users’ private bit strings without the keys from these ciphertexts.

There exists delay-photon Trojan horse attack as well as invisible photon Trojan horse attack in quantum cryptographic protocols which involve relaying quantum communication [25-27]. Hence these attacks are invalid to the proposed protocol as it only uses one-step quantum communications.

3.2.2. Attacks from either $P_2$ or $P_3$. Let us move on to the analysis of the case where either $P_2$ or $P_3$ wants to learn the others’ private inputs. Without loss of generality, $P_2$ is assumed to be a dishonest user who intends to obtain $P_1$’s and $P_3$’s private bit strings.

To finish this task, $P_2$ has to learn the values of $key_1$ and $key_3$. He will, however, fail to do that. The properties of $q_6$ and the encoding rule only give the equation $key_1 \oplus key_2 \oplus key_3 = 0$ to $P_2$. $P_2$ cannot attain the exact value of $key_1$ and the exact value of $key_3$. In Step (V), $P_2$ could obtain either $cmsg_{13}$ or $cmsg_{12}$, where $c_{13}$ the ciphertext of $m_1 \oplus m_3$ encrypted by $k_2$ and $c_{12}$ is the ciphertext of $m_1 \oplus m_2$ encrypted by $k_3$. However, $P_2$ fails to simultaneously attain $cmsg_{13}$ and $cmsg_{12}$ as $P_1$ randomly generates only one of them in Step (V). For the case where $P_2$ obtains $cmsg_{12}$, he can calculate $cmsg_{12} \oplus cmsg_{3} = cmsg_1 = key_1 \oplus msg_1$. For the case where $P_2$ learns $cmsg_{3}$ and $cmsg_{13}$, he can have $cmsg_{3} \oplus cmsg_{13} = key_1 \oplus msg_1$. In either case, he is unable to attain $P_1$’s private bit string $msg_1$ as he fails to learn the exact value of $key_1$. Similarly, $P_2$ cannot obtain $P_3$’s private bit string $msg_3$ because he cannot obtain the exact value of $key_3$. Hence $P_2$ will fail to get $P_1$’s and $P_3$’s private bit strings. For simplicity, we give an example where two-bit keys are used. Table 1 shows the relations between users’ keys and their measurement results. We can learn from the table that $P_2$ is unable to obtain the exact values of $key_3$ and $key_3$ according to his/her private key $key_2$.

### Table 1. Three users’ measurement results and their corresponding keys

|                | $P_1$                      | $P_2$                      | $P_3$                      |
|----------------|----------------------------|----------------------------|----------------------------|
| Results after  | $|\psi^+\rangle_{12}$ ($|\psi^-\rangle_{12}$) | $|\psi^+\rangle_{34}$ ($|\psi^-\rangle_{34}$) | $|\psi^+\rangle_{65}$ ($|\psi^-\rangle_{65}$) |
| Keys           | 00 (01)                    | 00 (00)                    | 00 (01)                    |
| Results after  | $|\psi^+\rangle_{12}$ ($|\psi^-\rangle_{12}$) | $|\psi^+\rangle_{34}$ ($|\psi^-\rangle_{34}$) | $|\psi^+\rangle_{65}$ ($|\psi^-\rangle_{65}$) |
| Keys           | 00 (01)                    | 01 (01)                    | 01 (00)                    |
| Results after  | $|\psi^+\rangle_{12}$ ($|\psi^-\rangle_{12}$) | $|\psi^+\rangle_{34}$ ($|\psi^-\rangle_{34}$) | $|\psi^+\rangle_{65}$ ($|\psi^-\rangle_{65}$) |
| Keys           | 00 (01)                    | 10 (10)                    | 10 (11)                    |
We now study the attacks launched by $P_1$ who wishes to learn $P_2$’s and $P_3$’s private inputs. In our protocol, $P_1$ is equipped with more quantum devices than $P_2$ and $P_3$ as he/she is in charge of the preparation and distribution of the quantum state $\varphi_6$. $P_1$ may produce fake particles and pass them to $P_2$ and $P_3$. After that, $P_1$ derives the exact values of $P_2$’s and $P_3$’s keys according to the fake particles. Consequently, he/she obtains $P_2$’s and $P_3$’s private bit strings $msg_2$ and $msg_3$ by using $key_2$ and $key_3$ to decrypt $cmsg_2$ and $cmsg_3$, respectively. For example, $P_1$ deliberately transmits particles that form a Bell state $|\psi^-(\varphi^+)|$ to $P_2$ or $P_3$ if he wants some two bits in $key_2$ to be $11$ ($10$). $P_1$ can also be honest to prepare $\varphi_6$ instead of fake particles. $P_1$ then transmits particular particles to $P_2$ ($P_3$) in such a way that he later derives others’ keys based on their measurement results and the encoding rule. However, these attacks are also invalid to our protocol as $P_2$ and $P_3$ can learn the dishonesty of $P_1$ in Step (III) by using $\theta$ quantum states of $\varphi_6$.

$P_1$’s most general attack can be characterized as a unitary operator $U_E$. $P_1$ performs $U_E$ on qubits that contain $\varphi_6$ and a probe state whose initial state is $|0\rangle_v$ before sending $P_2$ and $P_3$ the particles. One can prove that final quantum state of $\varphi_6$ would be unentangled with $P_1$’s probe state if he/she passes the detection in Step (III). This implies that $P_1$ will obtain nothing about $P_2$’s and $P_3$’s measurement results through the probe. Hence $P_1$ cannot learn anything about $key_2$ and $key_3$.

Note that any two users can work together to obtain the third one’s key relying on the equation $key_1 \oplus key_2 \oplus key_3=0$, and therefore steal his/her private bit string. Designing practical multi-party QPC protocols secure against this attack will be our future work.

4. Conclusion

This study has presented a secure three-party QPC protocol using the quantum state $\varphi_6$ for the comparison of equality. Three users can verify whether their private bit stings are the same and protect their inputs’ privacy. Quantum unitary operations are not needed in our protocol for information coding due to the great properties of $\varphi_6$. We have also analysed the protocol’s security in details and shown that the outside and participant attacks are invalid to the presented protocol.

Acknowledgments

Our work is supported by the National Natural Science Foundation of China under Grant Nos. 61902132 and 11647140, the Guangdong Basic and Applied Basic Research Foundation under Grant No. 2021A151011985, the Natural Science Foundation of Guangdong Province of China under Grant No. 2018A030310147, and the Young Talents Program of Colleges and Universities of Chinese Guangdong Province Office of Education under Grant No. 2019KQNCX012.

References

[1] Yao, A.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982) : 160-164 (1982)

[2] Boudot, F., Schoenmakers, B., Traoré, J.: A fair and efficient solution to the socialist millionaires' problem.” Discret. Appl. Math. 111: 23-36 (2001)
[3] Lo, H.-K.: Insecurity of quantum secure computations. Phys. Rev. A 56(2), 1154–1162 (1997)
[4] Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A, Math. Theor. 42(5), 055305 (2009)
[5] Chen, X.B., Xu, G., Niu, X.X., et al.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single particle measurement. Opt. Commun. 283(7), 1561–1565 (2010)
[6] Lin, Jason, Chun-Wei Yang and T. Hwang.: Quantum private comparison of equality protocol without a third party. Quantum Inf. Process. 13, 239-247 (2014)
[7] Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. 284(12), 3160–3163 (2011)
[8] Liu, W., Wang, Y., Jiang, Z., et al.: Protocol for the Quantum Private Comparison of Equality with X-Type State. Int. J. Theor. Phys. 51(1), 69-77 (2012)
[9] Liu, W., Wang, Y., Jiang, Z., et al.: New Quantum Private Comparison Protocol Using $\chi^-$Type State. Int. J. Theor. Phys., 51, 1953-1960 (2012)
[10] Liu, W., Wang, Y., Cui, W.: Quantum private comparison protocol based on Bell entangled states.” Commun. Theor. Phys. 57 (4): 583-588 (2012)
[11] Huang, W., Wen, Q., Liu, B. et al.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. China Phys. Mech. Astron. 56 (9), 1670–1678 (2013)
[12] Liu, B., Gao, F., Jia, H., et al.: Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process. 12, 887-897 (2013)
[13] Zhang, W., Li, D., Song, T., et al.: Quantum private comparison based on quantum search algorithm. Int. J. Theor. Phys., 52, 1466-1473 (2013)
[14] Ji, Z., Fan, P., Zhang, H., Wang, H. Several two-party protocols for quantum private comparison using entanglement and dense coding. Optics Communications, 459: 124911 (2020)
[15] Chang, Y., Tsai, C., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. 12 (2), 1077-1088 (2013)
[16] Liu, W., Wang, Y., Wang, X.: Multi-party Quantum Private Comparison Protocol Using d-Dimensional Basis States Without Entanglement Swapping. Int. J. Theor. Phys. 53, 1085-1091 (2014)
[17] Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. 69, 2881-2884 (1992)
[18] Bennett, C.H., Brassard, G., Crépeau, et al.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 70 13, 1895-1899 (1993)
[19] Zhou, L., Sheng, Y., Long, G.: Device-independent quantum secure direct communication against collective attacks. Chin. Sci. Bull. 65, 12-20 (2020)
[20] Qi, R., Sun, Z., Lin, Z., et al.: Implementation and security analysis of practical quantum secure direct communication. Light, Science & Applications, 8 (2019)
[21] Bennett, C.H., Brassard G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, System and Signal Processing. Pp.175-179, IEEE Press, Bangalore (1984)
[22] Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67 6, 661-663 (1991)
[23] Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A 59, 1829-1834 (1999)
[24] Borras, A., Plastino, A., Batle, J., Zander, C., Casas, M.: Multiqubit systems: highly entangled states and entanglement distribution. Journal of Physics A, 40, 13407-13421 (2007)
[25] Deng, F., Li, X., Zhou, H., Zhang, Z.: Improving the security of multi-party quantum secret sharing against Trojan horse attack. Phys. Rev. A 72, 044302 (2005)
[26] Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems (6 pages). Phys. Rev. A 73, 22320 (2006)
[27] Li, X., Deng, F., Zhou, H.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A 74, 054302 (2006)