Quantum Secure Communication Protocol with Signature

Junluo Wen and Xing Zheng

ABSTRACT

Combining the idea of quantum secure communication and quantum homomorphic signature, we propose a quantum secure communication protocol with signature via EPR pairs, in which the identities of the sender and the recipient could be certified and the integrity of the message transmitted is guaranteed according to their signatures. Comparing with the previous quantum secure communication scheme without signature, our protocol is not only feasible in practice but also can effectively guarantee the reliability and security of the quantum communication. The security of the protocol is analyzed.

INTRODUCTION

Quantum communication exploits the peculiar quantum properties to give us unconditional security and neoteric ways of communication. Quantum communication provides us with an absolute-security advantage, which has been widely developed in the past thirty years. In 1984, the first quantum key distribution (QKD) protocol was presented by Bennett and Brassard which represents the emergence of quantum cryptography [1]. Since then, many researchers focus on quantum cryptography, which incorporates quantum key distribution (QKD) [2, 3], quantum secret sharing (QSS) [4] quantum teleportation [5-8], quantum key agreement [9, 10], quantum secure computation (QSMC) [11–16], etc.

As an important branch of quantum communications, quantum secure direct communication can promote high security communication in the way of transmitting messages over a quantum channel. And the first quantum secure direct communication (QSDC) protocol was presented by Long and Liu [17], which allows that the sender can directly transmit the secret message to the receiver without distributing the key in advance. In 2002, Long and Liu [18] proposed a QSDC protocol by using Einstein-Pololsky-Rosen (EPR) pairs. Based on the exchange of single photons, Biege et al. [19] presented a QSDC protocol for direct and

Junluo Wen1 and Xing Zheng2
1Chongqing University of Posts and Telecommunications, College of Computer Science and Technology, China
2Chongqing University of Posts and Telecommunications, Graduate Department of Computer Science, China
*Xing Zheng: 15223079570@163.com
confidential communication between Alice and Bob, with no need for establishing a shared secret key first. QSDC has received wide attentions and has been widely explored. In 2003, Long and Liu presented a two-step QSDC protocol [20]. Later, many other QSDC protocols were proposed [21–24]. In 2006, Lee et al. presented two QSDC protocols with authentication [25]. Subsequently, many authenticated QSDC protocols were put forward [26–28]. Most of them are designed in ideal situation. That is, there is no noise in the quantum channel. However, noise is inevitable in practice, which will affect the security and fidelity of the information transmitted. Hence, many researchers turn to research practical QSDC protocols [29–35]. In 2011, Liu et al. [36] presented a high-capacity quantum secure direct communication protocol with single photons in both the polarization and the spatial-mode degrees of freedom. The secret messages are only transmitted from one participant to another one.

Then a high-capacity bidirectional QSDC network protocol with hyper entanglement was proposed [37]. In 2013, Yin et al. [38] proposed an efficient 3P-QSDC protocol based on some ideas of quantum dense coding with EPR pairs.

It’s commonly known that the identity authentication and integrity of message is the most important to quantum communication. In order to guarantee the information cannot be denied and forged in quantum communication, signature emerges as the reliability and security requirement.

Quantum signature is an effective approach to identity authentication for data source. As the study of quantum cryptography develops, a few branches of quantum cryptography have been studied in recent years, including quantum key distribution (QKD), quantum secret sharing (QSS), quantum secure direct communication (QSDC), quantum encryption algorithm (QEA), quantum identification (QI), and quantum signature (QS). Quantum signature that concerns about the authenticity and non-repudiation of messages on insecure quantum channels is an important research topic in quantum cryptography. So far, a few quantum signature schemes have been proposed. In 2001, Gottesman and Chuang [39] proposed the first quantum signature scheme based on quantum one-way functions and quantum swap test. In 2002, Zeng and Keitel [40] proposed a pioneering arbitrated quantum signature (AQS) protocol which can be used to sign both classical message and quantum one. Then, a variety of quantum signature schemes based on AQS have been proposed. Lee et al. [41] proposed two quantum signature schemes with message recovery. Wang et al. [42] proposed an arbitrated quantum signature scheme with single photons. Zeng et al. [43] proposed a true quantum signature algorithm based on continuous-variable entangled state. In 2007, Wen and Liu [44] proposed a quantum signature scheme without an arbitrator. Their scheme can be used to sign general quantum superposition states. To protect the privacy of message owners, Wen et al. [45] proposed the first quantum group signature scheme by using quantum teleportation. In order to authenticate the identity of different data source in a network, homomorphic signature scheme [46] is considerably paid attention to instead of standard signature schemes in classical cryptography. Inspired by entanglement swapping [47], Shang et al. [48] first propose a new quantum homomorphic signature scheme which can be used to authenticate data packets of multiple streams for quantum networks. The proposed quantum signature scheme can effectively guarantee the security of secret key and verify the identity of different data sources in a quantum network. Compared with published quantum secure communication protocol without signature, it is thus indispensable to combine quantum secure
communication with quantum signature to guarantee the reliability of quantum communications.

The rest of our paper is structured as follows. Section 2 describes the related works. Section 3 describes the presented protocol in detail. The security analysis is discussed in Section 4. Finally, Section 5 concludes our scheme briefly.

**RELATED WORKS**

**Entanglement Swapping**

Entanglement swapping [49] is a special property of quantum entanglement. The key idea of entanglement swapping is that two non-entangled particles (1, 3) become an entangled state by measurement as shown in Fig.1. Assume the original states of these particles are:

$$|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|0_10_2\rangle + |1_11_2\rangle).$$

$$|\psi^+\rangle_{34} = \frac{1}{\sqrt{2}}(|0_31_4\rangle + |1_30_4\rangle).$$  \hspace{1cm} (1)

Then,

$$|\phi^+\rangle_{12} \otimes |\psi^+\rangle_{34} = \frac{1}{2} (|0_10_20_31_4\rangle + |0_10_21_30_4\rangle + |1_11_20_31_4\rangle + |1_11_21_30_4\rangle)$$

$$= \frac{1}{2} (|0_10_30_21_4\rangle + |0_11_30_20_4\rangle + |1_10_31_21_4\rangle + |1_11_31_20_4\rangle)$$

$$= \frac{1}{2} (|\phi^+\rangle_{13} |\psi^+\rangle_{24} + |\phi^-\rangle_{13} |\psi^-\rangle_{24} + |\psi^+\rangle_{13} |\phi^+\rangle_{24} + |\psi^-\rangle_{13} |\phi^-\rangle_{24})$$  \hspace{1cm} (2)

![Figure 1. Entanglement swapping.](image)

If we perform a Bell-state measurement on the particles 1 and 3, the particles 2 and 4 would collapse to another entangled state. For instance, if the measurement result of the particles 1 and 3 is $|\phi^+\rangle_{13}$, then the state of the particles 2 and 4 would be $|\psi^+\rangle_{24}$. In other cases, the states of particles after entanglement swapping are shown in Table 1 in the protocol proposed [48].

**Quantum homomorphic signature**

An example of homomorphic signature scheme BFKW was given by Boneh et al. [50]. Homomorphic signature scheme can generate a new signature of different data.
without the private keys of participants, it is very important to distributed networks and homomorphic signature scheme can be used to generate new signatures at intermediate nodes through directly manipulating the original signatures of messages without any encryption operation.

Quantum homomorphic signature scheme [48] based on entanglement can effectively guarantee the security of secret key and verify the identity of information in quantum network.

Here, we give a model of homomorphic signature scheme introduced in [49] which inspired us. Assume that the object of the signature is classical message and the carrier of the signature is EPR pairs, the signer sends the data of classical bits \(X_1(X_2)\) with the signature of quantum states to a verifier. Quantum homomorphic signature model is shown in Fig.2. \(A_1(A_2)\) are the signers of classic message, \(M_1\) is aggregator who aggregates the received signatures to generate a new signature according to original signatures, and \(M_2\) is the final verifier.

**Figure 2. Quantum homomorphic signature model.**

**QUANTUM SECURE COMMUNICATION PROTOCOL WITH SIGNATURE**

Our new scheme involves three parties, namely the message sender Alice, the message receiver Bob and trusted third-party Charlie. Assuming that Alice sends classic message \(M\) to Bob through a quantum channel, and the classic message is \(M=\{m_1,m_2,m_3,...,m_n\}, m_i \in \{00,01,10,11\}\). The trusted third-party Charlie verifies the validity of the identities of Alice and Bob with their signatures. They agree on advance that the four unitary operations represent the classical bits in such a way that:

\[
U_{00} \rightarrow I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U_{01} \rightarrow \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\
U_{10} \rightarrow \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad U_{11} \rightarrow -i\sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.
\] (3)

Here, each digital subscript denotes a classical two-bit. The protocol is as follows.

**Step1. Quantum key distribution.**

Alice (Bob) shares a secret key \(K_1 = \{K_{11}^1,K_{12}^2,...,K_{1n}^n\}(K_2 = \{K_{21}^1,K_{22}^2,...,K_{2n}^n\})\) with Charlie by quantum key distribution protocol, such as the improved BB84 protocol with authentication [52] which can defend against the man-in-the-middle.
Alice shares key $K_3$ with Bob. Here, $K'_i \in \{00, 01, 10, 11\}$ and $i=1,2,3,\ldots,n, j=1, 2, 3$.

**Step 2. EPR pairs distribution.**
Charlie prepares three ordered sequences of EPR pairs $S_{12}, S_{34}, S_{56}$ in which the state of each EPR pair is $|\phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$, the subscripts 1,3,5 denote the first particle of each EPR pair in $S_{12}, S_{34}, S_{56}$, and the subscripts 2,4,6 denote the second particle of each EPR pair in $S_{12}, S_{34}, S_{56}$. Then, Charlie prepares a sequence of detection photon $T_i =\{t_1, t_2, \ldots, t_{2n}\}$ and inserts it into $S_2||S_5$ randomly, new sequence of $S_2||S_5$ mixed with $T_i$ is denoted as $S_{CA}$. Each detection photon is prepared according to the key $K_3$ for eavesdropping detection as follows: the detection photon $t_i$ is in the state $|0\rangle$ or $|+\rangle$ randomly when the first bit of $K'_3$ is 0, otherwise, the state is $|1\rangle$ or $|−\rangle$ randomly. Similarly Charlie prepares the sequence of detection photon $T_2 =\{t'_1, t'_2, \ldots, t'_{2n}\}$ and inserts it into $S_4||S_6$ randomly, new sequence of $S_4||S_6$ mixed with $T_2$ is denoted as $S_{CB}$. Then Charlie sends the sequence $S_{CA}, S_{CB}$ to Alice and Bob respectively, and he informs Alice and Bob of the detection photon’s position.

**Step 3 The first eavesdropping detection.**
Alice (Bob) extracts $T_1 (T_2)$ in $S_{CA} (S_{CB})$ according to $K_1 (K_2)$ and measures photon in $T_1 (T_2)$. Thus he can judge whether the channel is secure according to the result of measurement. Alice (Bob) divides the remaining particles in $S_{CA} (S_{CB})$ into two sequences as $S_2 (S_4)$ and $S_5 (S_6)$ in order. Alice goes on to the next step if she confirms that the channel is secure, otherwise the communication is terminated.

**Step 4. Alice’s signature and encoding.**
With the manner expressed in (3), Alice makes the unitary operator on $S_5$ according to the XOR result of her classical bits $M$ and the key $K_3$, note that $S'_5 = U(M \oplus K_3)S_5$. Then, for signing on $S_2$, Alice performs the corresponding operation on the particle in $S_2'$ according to the XOR result of classical bits $M$ and the key $K_1, K_3$, note that $S'_2 = U(M \oplus K_1 \oplus K_3)S_2$, which as Alice's signature.

**Step 5. Alice inserts the detection particles and sends $S_5''$ to Bob.**
Alice prepares a sequence of detection photon $T_3 =\{t''_1, t''_2, \ldots, t''_{n}\}$ and inserts it into $S'_5$ according to the key $K_3$ for eavesdropping detection. The detection photon $t''_i$ is in the state $|0\rangle$ or $|+\rangle$ randomly when the first bit of $K'_3$ is 0, otherwise, the state is $|1\rangle$ or $|−\rangle$ randomly. The position that the detection photons are inserted into $S'_5$ is as follows. If the second bit of $K'_3$ is 0, Alice inserts $t''_i$ before the $i$-th particle in $S'_5$, otherwise, the position of the insertion would be after the $i$-th particle in $S'_5$. The mixed sequence of $T_3$ and $S'_5$ is denoted as $S_5''$. Subsequently Alice sends $S_5''$ to Bob.

**Step 6. The second eavesdropping detection.**
After Bob receives $S_5''$, Bob extracts $T_3$ according to $K_3$ and measures photon in $T_3$. Thus he can judge whether the channel is secure according. Bob goes on to the next step if he conforms that the channel is secure, otherwise the communication would be terminated.

**Step 7. Bob signs on the message that he has received from Alice.**
Bob obtains the XOR value of $M$ and $K_3$ by making Bell-basis measurements on the particles in $S'_5$ and $S_6$. Accordingly, he can obtain Alice’s message in accordance with $K_3$ and denoted as $M'$. Subsequently, Bob performs the
corresponding unitary operator on $S_4$ according to the XOR result of his classical bits $M'$ and key $K_2, K_3$, note that $S_4' = U(M' \oplus K_2 \oplus K_3)S_4$.

**Step8. Charlie’s arbitration by verifying the signature.**

Charlie performs a Bell-state measurement on the sequences $S_1, S_3$ and obtains $S_{13}'$. According to the resulting state after entanglement swapping in Table 1, the state of EPR pair in $S_{24}'$ will be one of the four Bell states as shown. On the basis of Table 1, Charlie compares $S_{24}'$ with $S_{24}$. Then he obtains an operation which satisfies $S_{24}' = c(Z)^{U}(Z)^{(4)}$. Here $Z \in \{00,01,10,11\}$ and the superscript (4) denotes an operation performed on the particles in $S_4$, and $|c(Z)| = 1$. If the measurement result of the particles in $S_1$ and $S_3$ is $S_{13}' = S_{13}$, $S_{24}'$ will denote the resulting state of the original particles in $S_2$ and $S_4$ after entanglement swapping. Theoretically it satisfies $S_{24}' = c(Z)^{U}(M \oplus K_2 \oplus K_3 \oplus M' \oplus K_1 \oplus K_3)^{(4)}$. $S_{24}$ which is $S_{24}' = U(K_1 \oplus K_2)^{(4)}$. $S_{24}$ when $|c(Z)| = 1$. Charlie compares $K_1 \oplus K_2$ with $Z$. If $K_1 \oplus K_2 = Z$, Charlie confirms that the signatures of Alice and Bob are legitimate. Then he publishes that the communication is legitimate.

**SECURITY ANALYSIS**

In this section, we give the analysis of the above quantum communication with signature scheme. We analyze the three kinds of typical attacks in the quantum communication protocol, such as intercept-resend attack, man-in-the-middle attack and entanglement-and-measure attack. The proposed protocol can resist typical attacks and avoid information leakage. We also prove that the signature of Alice and Bob is unforgeable.

**Intercept and Resend Attack**

Taking into account that the BB84 protocol is vulnerable to middle-man attack. Hence, we use an improved BB84 protocol inspired by the literature [51] to distribute the key to defend against middle-man attack. Based on the improved BB84 protocol, this quantum key distribution in this protocol can defend against any middle-man attack, which is proved in [48]. So the secret key $K_i (i=1,2,3)$ is shared by Charlie and Alice(Bob) securely.

Eve may intercept the particles of step 2 and step 5; she may resend a forged sequence to Alice or Bob according to her measurement results. She may try to intercept $S_{CA}$ or $S_{CB}$ in Step 2 and substitute it with her own prepared photons in hope that she can pass the eavesdropping check of Step 3. However, since Eve does not know the positions and the states of $S_{CA}$ or $S_{CB}$, the forged photons of Eve will be detected when Alice or Bob measures them according to $K_1$ and $K_2$ shared with Charlie. In step 5, to obtain the secret message $M$ of Alice, Eve may try to measure the transmitted particles in $S_5''$ and then send the measured $S_5''$ to Bob. Due to the fact that Eve cannot get the secret key $K_3$ and determine the position of the detection photon, if Eve measured the check photons and the entangled states of EPR pairs, Bob can detect the existence of Eve by the detection photon in step 6. One can notice that Eve can only interrupt the transmission of sequence $S_5'$ and cannot obtain any secret information from Alice even if he captured the particles in sequence $S_5'$ without $S_6$. 

260
Man in the Middle Attack

To obtain the secret message from Alice to Bob, Eve plays the role of Bob to communicate with Alice, and also plays the role of Alice to communicate with Bob. In step 5, due to the fact that the checking particles are chosen by Alice according to $K_3$, Eve cannot know the positions in advance to insert these checking particles into the fake sequence prepared by herself. She is also unable to choose the correct basis to measure the checking particles. In this case, if she sneaks into the quantum channel, Eve may disrupt the communication between Alice and Bob. However, she cannot steal any secret information due to the fact that she can only obtain one particle of each EPR pair. In addition, Bob will abandon the communication if Eve is detected.

Entangle and Measure Attack

Eve intercepts the information from Alice and prepares ancillary EPR pairs to entangle the information, and then resends the intercepted particles to the legal receiver. Just as shown in Ref.[51], suppose that Eve prepares a sequence $S_{78}$, in which the state of each EPR pair is $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ as the ancillary EPR pair. When Eve intercepts $S_{5''}$ in step 5, she makes a Bell-basis measurement on particle in $S_5$ and $S_7$, then the particle in $S_6$ and $S_8$ will be in one of the EPR pairs $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$, each with the probability 1/4. The entangled state can be determined by the measurement result as

$$
|\phi^+\rangle_{56} \otimes |\phi^+\rangle_{78} = \frac{1}{2}(|\phi^+\rangle_{58} \otimes (|\phi^+\rangle_{67} + |\phi^-\rangle_{67}) + |\psi^+\rangle_{58} \otimes |\psi^-\rangle_{67})
$$

(6)

In step 5, as we know, the information intercepted by Eve includes single photons and entangled particles. If Eve wants to make the detection photons distinguishable, she will be found in the process of eavesdropping check because the initial states of the photons in $S_{5''}$ had been disturbed.

After Bob receives the message, he makes the Bell-basis measurement on the check pairs. If the correlation of particle in $S_5$ and $S_6$ is destroyed, Bob can confirm the existence of Eve and abandon the communication. Furthermore, Eve can only disturb the transmission because she cannot infer the photons in sequence $S_{5''}$. Accordingly, the proposed protocol can resist the entangle-measure attack.

Information Leakage

Information leakage is a kind of passive attack in which an eavesdropper, Eve, can extract secret messages (or the useful information of secret messages). In the following, we will demonstrate how the information leakage can be prevented in the proposed protocol.

In step 5, Alice encrypts the message $M$ according to the pre-shared $K_3$, which is just one-time pad, Eve cannot get the $K_3$. And Eve cannot obtain the both of two particles of message-coding EPR pair, it is impossible to get the information correctly for him. The information is secure when the Charlie verifies the signature,
because in the process of varication the information is always encryption to Charlie. Above all, there is no information leakage in the protocol proposed.

**The Signature S1 and S2 Is Unforgeable.**

According to our quantum signature scheme, the signature of Alice is $S_{Alice} = U(M \oplus K_1 \oplus K_3) S_2$ and $S_{Bob} = U(M \oplus K_2 \oplus K_3) S_4$. In other words, the key $K_1$, $K_2$ and $K_3$ is necessary to generate signatures of legal participants. Any attacker cannot obtain the key $K_1$, $K_2$ and $K_3$ by wiretap attacks. Hence, without the key $K_1$, $K_2$ and $K_3$, no attacker can forge a signature corresponding to his data. And forging any one of the key $K_1$, $K_2$, $K_3$ or message $M$, their signatures cannot be verified by Charlie in step 8.

**CONCLUSION**

In this paper, we reported the first quantum secure communication protocol with signature, which is designed based on QSC and quantum signature. We proved that our proposed scheme is secure against the popular attacks in current and especially provided a formal security proof of its security and reliability. The reliability of quantum communication is enhanced as the advantages of information integrity verification is added. Moreover, there is no information leakage since Charlie can verifies two parties’ signature simultaneously without any extra public information transmitted in the classical channel. Our scheme is secure by the security analysis.

**REFERENCES**

[1] Bennett C H. Quantum cryptography. Public key distribution and coin tossing[C] Proc. IEEE International Conference on Computers Systems and Signal Processing. 175-179(1984).
[2] Deng, F.G., Long, G.L., Phys. Rev. A 68, 042315 (2003).
[3] Lin, S., Guo, G.D., Gao, F., et al., Q. Inf. Comput. 14(9&10), 845–856 (2014).
[4] Yan, F.L., Gao, T., Phys. Rev. A 72, 012304 (2005).
[5] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R, Peres, A, Wootters, W. K. Phys. Rev. Lett. 70, 1895 (1993).
[6] Bouwmeester, D. et al. Experimental quantum teleportation. Nature 390, 575-579 (1997).
[7] Yin, J. et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. Nature 488, 185-188 (2012).
[8] Wang, X. J., et al. Quantum teleportation of multiple degrees of freedom of a single photon. Nature 518, 516-519 (2015) 489, 269-273 (2012).
[9] Huang, W., Su, Q., Wu, X., et al., Int. J. Theor. Phys. 53(9), 2891–2901 (2014).
[10] Liu, B., Gao, F., Huang, W., et al., Q. Inf. Process. 12(4), 1797–1805 (2013).
[11] Huang, W., Wen, Q.Y., Liu, B., et al., Sci. Chin-Phys. Mech. Astron. 56(9), 1670–1678 (2013).
[12] Li, Y.B., Wang T.Y., Chen H.Y., Li M.-D., Yang Y.T., Int. J. Theor. Phys. 52(8), 2818–2825 (2013).
[13] Li, Y.B., Qin, S.J., Yuan, Z., et al., Quantum Inf. Process. 12(6), 2191–2205 (2013).
[14] Huang, W., Wen, Q.Y., Liu, B., et al., Phys. Rev. A 89, 032325 (2014).
[15] Li, Y.B., Xu, S., Huang, W., Wan, Z.J., J. Phys. A: Math. Theor. 48, 135302 (2015).
[16] Li, Y.B., Wen, Q.Y., Gao, F., Jia, H.Y., Sun, Y. Information leak in Liu et al.’s quantum private comparison and a new protocol. Eur. Phys. J. D. 66(4), 110–115 (2012).
[17] Long, G.L., Liu, X.S., Phys. Rev. A 65, 032302 (2002).
[18] Long, G.L., Liu, X.S., Phys. Rev. A 65, 032302 (2002).
[19] Beige, A., Englert, B.G., Kurtsiefer, Ch., Weinfurter, H. Secure communication with a publicly known key. Acta. Phys. Pol 101(3), 357-368 (2002).
[20] Deng, F.G., Long, G.L., Liu, X.S, Phys. Rev. A 68, 042317 (2003).
[21] Deng, F.G., Long, G.L., Phys. Rev. A 69, 052319 (2004).
[22] Wang, C., Deng, F.G., Li, Y.S., et al., Phys. Rev. A 71, 044305 (2005).
[23] Long, G.L, Deng, F.G., Wang, C., et al., Front Phys China. 2(3), 251–272 (2007).
[24] Sun, Z.W., Du, R.G., Long, D.Y, Int. J. Theor. Phys. 51, 1946–1952 (2012).
[25] Lee, H., Lim, J., Yang, H.J, Phys. Rev. A 73, 42305(2006).
[26] Chang, Y., Zhang, S.B., Yan, L.L., et al, Chin. Phys. Lett. 30, 060301 (2013).
[27] Chang, Y., Zhang, S.B., Yan, L.L., Chin. Phys. Lett. 30, 090301 (2013).
[28] Yu, C.H., Guo, G.D., Lin, S, Int. J. Theor. Phys. 52(6), 1937–1945 (2013).
[29] Huang, W., Wen, Q.Y., Jia, H.Y., et al., Chin. Phys. B. 21(10), 100308 (2012).
[30] Chang, Y., Zhang, S.B., Li, J., et al., Sci. Chin-Phys. Mech. Astron. 57(10), 1907-1912 (2014).
[31] Gu, B., Zhang, C.Y., Cheng, G.S., et al., Sci. Chin-Phys. Mech. Astron. 54(5), 942-947(2011).
[32] Li, Y.B., Song, T.T., Huang, W., Zhan, W.W, Int. J. Theor. Phys. 54(2), 589-597 (2015).
[33] Wu, D., Lv, H.J., Xie, G.J, Int. J. Theor. Phys. 55(1), 457-469 (2016).
[34] Cui, Y.Q., Gao, J.G. Int. J. Theor. Phys. 55(3), 1706-1709 (2016).
[35] Li, Y., Li, X., Nie, L., et al., Int. J. Theor. Phys. 55(2), 837-842 (2016).
[36] Liu, D., Chen, J.L., Jiang, W., Int. J. Theor. Phys 51(9), 2923-2929 (2012).
[37] Gu,B.,Huang,Y.G.,Xia,F., et al., Commun. Theor. Phys 56(4), 659 (2011).
[38] Yin, X.R., Ma, W.P., Shen, D.S., et al., Journal of Quantum Information Science 1, 3 (2013).
[39] Gottesman, D., Chuang, I. Quantum digital signatures, Technical Report. http://arxiv.org/abs/quant-ph/0105032(2001).
[40] Zeng, G., Keitel, C. H., Phys. Rev. A65(4), 12-17(2002).
[41] Lee, H. , Hong, C. , Kim, H., et al., Phys. Lett. A 321, 295-300 (2004).
[42] Wang, J., Zhang, Q., Tang, C. J., Optoelectron. Lett. 2(2), 209-212 (2006).
[43] Zeng,G.,Lee,M.,Guo,Y.,et al., Int. J. Quantum Inf. 5(4), 553-573 (2007).
[44] Wen, X.J., Liu, Y., The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007), Chengdu, China, pp. 496-500, 01-03 Nov (2007).
[45] Wen, X.J., Tian, Y., Ji, L.P., et al., Phys. Scr. 81(5), 055001 (2010).
[46] Johnson, R., Molnar, D., Song, D., et al. Homomorphic Signature Schemes, Topics in Cryptology- CT-RSA 2002. Springer, Berlin (2002).
[47] Lu, H., Guo, G. Teleportation of a two-particle entangled state via entanglement swapping. Phys. Lett. A 276(5), 209-212 (2000).
[48] Shang T, Zhao X J, Wang C, et al. Quantum Information Processing, 2014, 14(1):393-410.
[49] Lu, H., Guo, G., Phys. Lett. A 276(5), 209-212 (2000).
[50] Boneh, D., Freeman, D., Katz, J., et al. Signing a Linear Subspace: Signature Schemes for Network Coding, Public Key Cryptography (PKC2009). Springer, Berlin (2009).
[51] Ljunggren, D., Bourennane, M., Karlsson, A., Phys. Rev. A 62(2), 1-7 (2000).