International Journal of Physical Sciences Vol. 7(27), pp. 5049-5053, 12 July, 2012
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS12.297
ISSN 1992 - 1950 ©2012 Academic Journals

Full Length Research Paper

Secure quantum dialogue using entanglement swapping

Mosayeb Naseri

Islamic Azad University, Kermanshah Branch, Kermanshah, Iran. E-mail: m.naseri@iauksh.ac.ir.

Accepted 25 June, 2012

In this study, a protocol for secure quantum dialogue using entanglement swapping was proposed. The protocol employs two independent communication channels, a classical channel and a quantum channel. In this scheme, the legitimate communicators Alice and Bob can pass the authentication by the classical trusted channel. Afterwards, a quantum channel sequence is provided for them, on which Alice and Bob can communicate with each other directly and privately by virtue of some encoding operations. The first advantage of our protocol is that different from the previews protocols, in the proposed protocol, the server of the quantum channel, Charlie, is not necessarily trusted. The other highlight of our protocol is that in the presented scheme, one party is able to first read the message received from the other party before sending another message back in reply.

Key words: Quantum secure direct communication, entanglement swapping, quantum dialogue.

INTRODUCTION

Quantum key distribution (QKD) is an ingenious application of quantum mechanics, in which two remote legitimate users (Alice and Bob) establish a shared secret key through the transmission of quantum signals and use this key to encrypt (decrypt) secret messages. Since Bennett and Brassard presented the pioneering work in 1984 (Bennett and Brassard, 1984), a variety of QKD protocols have been proposed (Ekert, 1991; Bennett, 1992; Bennett et al., 1992; Gisin et al., 2002). Quantum key distribution has attracted much attention of the researchers. Quantum secure direct communication (QSDC) (Boykin and Roychowdhury, 2003; Leung, 2001; Gisin et al., 2002; Chen et al 2008; Xio-Bo et al., 2008) is a branch of quantum cryptography, which allows the sender to transmits directly the secret (not a random key) to the receiver in a deterministic and secure manner. Quantum encryption algorithm has also been investigated (Gisin et al., 2002; Leung, 2001; Zhou et al., 2007, 2005). The goal of quantum encryption algorithm and classical encryption algorithm is consistent, that is, to protect secret information or keep communications private. Quantum secret sharing (QSS) (Hillery et al., 1999; Karlsson et al., 1999; Xiao et al., 2004) is another important application of quantum mechanics, which allows a secret to be shared among many participants in such a way that only the authorized groups can reconstruct it. Bostrom and Felbinger put forward a ping-pong QSDC scheme by using Einstein-Podolsky-Rosen (EPR) pairs (Bostrom and Felbinger, 2002). Based on the idea of a ping-pong QSDC scheme, Nguyen (2004) proposed a quantum dialogue scheme (the quantum dialogue is actually two-way communication) by using EPR pairs. However, an eavesdropper who adopts the intercept-and-resend attack strategy can steal the secret messages without being detected.

Let us start with the brief description of the quantum dialogue protocol. To get information from Alice, Bob prepares two qubits $|\psi_{kl}\rangle_{ht}$, in one among the four mutually orthogonal Bell states:

$$|\psi_{00}\rangle_{ht} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{ht},$$

$$|\psi_{01}\rangle_{ht} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)_{ht},$$

$$|\psi_{10}\rangle_{ht} = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)_{ht},$$

$$|\psi_{11}\rangle_{ht} = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)_{ht}.$$

where, h and t stand for “home” and “travel” qubits, respectively. Then, he sends qubit t to Alice while stores qubit h with himself. Alice decides to use qubit t as the message mode (MM) or the control mode (CM) randomly. In the MM, Alice encodes her information by performing a unitary operation I or σ_z on qubit t corresponding to her message bit 0 or 1, then he sends it back to Bob, who can obtain Alice’s information by a Bell measurement. In the CM, Alice performs a measurement in the basis $B_z = |0\rangle\langle 0| + |1\rangle\langle 1|$ and sends the result to Bob via a public classical channel. Bob then also switches to the CM and performs a measurement in the same basis $B_z = |0\rangle\langle 0| + |1\rangle\langle 1|$. Comparing his own result with that of Alice, Bob can detect the presence of Eve.

A quantum telephone protocol including the dialing process and the talking one has proposed by Wen et al. (2007). In this protocol in the dialing process, with their respective secret keys, the legitimate communicators Alice and Bob can pass the authentication by Charlie acting as a telephone company. In the talking process, Charlie provides the authenticated Alice and Bob with a quantum channel sequence, on which Alice and Bob can communicate with each other directly and privately by virtue of some encoding operations. Unfortunately, it has been shown that the quantum telephone protocol in its original form is not as secure as it claimed (Sun et al., 2009; Naseri, 2009), that is, recently Sun et al. have shown that an attacker could eavesdrop on the communicator’s conversation without introducing any error by an attack with fake particles and local operations. At the same time, very recently, we have realized that a dishonest server, an eavesdropper, can gain full information of the communication with zero risk of being detected by using fake entangled particles. The authors of the both papers (Sun et al., 2009; Naseri, 2009) have presented a modification procedure to avoid the vulnerability of the protocol against the possible presented attacks.

It is apparent that the modifications presented in Sun et al. (2009) and Naseri (2009), improve the original protocol against the eavesdropping of the secure information, but it is opined the main theoretical source of insecurity of the protocol still remains. Since the main source of theoretical insecurity can be seen, let me spend some more words on the theoretical condition for the security. As a matter of fact, each and every secure quantum communication protocol, in fact, the efficiency of transportation was bounded by Holevo quantity, which shows that n qubits cannot be used to transmit more than n bits of classical information in a 2-level system. Obviously, in secure quantum telephone protocol, Alice and Bob can transmit 4 bits secret message (two for Alice and two for Bob) via per EPR pair in the aforementioned communication. Whereas, Gao et al. (2008) pointed out that among the 4-bit information only 2 bits are transmitted securely. Due to Bob’s declaration, everyone (of course the Eve) can infer that there would be four possibilities for operations performed by Bob and Alice. Assuming four possibilities having equal probability, the channel contains only $-\sum_i p_i \log p_i = -4(\frac{1}{4}\log_2 \frac{1}{4}) = 2$ information for Eve. In other words, 2-bit secret has been leaked to Eve. Since, this capacity has been exceeded in secure quantum telephone protocol, it is undoubtedly insecure.

In this paper, we will introduce a new secure quantum dialogue using entanglement swapping. This paper is organized as follows: A new secure quantum dialogue using entanglement swapping is presented. Afterwards, the security of the protocol will be analyzed. Finally, the discussion and conclusions are given.

SECURE QUANTUM DIALOGUE USING ENTANGLEMENT SWAPPING

Before giving our protocol, let us review an entanglement swapping for two EPR states. The goal of entanglement swapping is to make quantum systems entangled, which are never interacted directly before, through certain physical process. Entanglement swapping plays an important role in quantum communications and quantum network. For example, Entanglement swapping can be used to prepare new entanglement states and extend the distance of quantum communications. Let us review entanglement swapping of two EPR states at first. To become entangled, suppose Alice shares two EPR pairs with Bob For example, entanglement swapping can be used to prepare new entanglement states and extend the distance of quantum communications. Suppose Alice shares two EPR pairs with Bob:

$$|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{12},$$

$$|\phi^+\rangle_{34} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{34}, \quad (1)$$

Photons 1 and 4 are in the site of Alice, and Bob owns the photons 2 and 3. The state of the whole system can be denoted as:

$$|\phi^+\rangle_{12}|\phi^+\rangle_{34} = \frac{1}{2}(|\phi^+\rangle_{14}|\phi^+\rangle_{23} + |\phi^-\rangle_{14}|\phi^-\rangle_{23} + |\psi^+\rangle_{14}|\psi^+\rangle_{23} + |\psi^-\rangle_{14}|\psi^-\rangle_{23}). \quad (2)$$

So, when a Bell state measurement is made on photons 1 and 4 by Alice, the photons 2 and 3 are projected onto one of the following states:

$$|\phi^+\rangle_{14}|\phi^+\rangle_{23}, |\phi^-\rangle_{14}|\phi^-\rangle_{23}, |\psi^+\rangle_{14}|\psi^+\rangle_{23}, |\psi^-\rangle_{14}|\psi^-\rangle_{23}$$

with equal probability of $\frac{1}{4}$ for each, that is to say, the entanglement swapping entangles two photons (2, 3) that have never interacted before by performing a Bell-state measurement on the photons (1, 4) which are from two different entangled pairs. This means that for a known initial state the Bell measurement results after the quantum entanglement swapping are correlated. In fact, similar results can also be arrived at provided that other choices of the initial states are given by Charlie. As can be seen as follows:

$$\left|\psi^{+}\right\rangle_{12}\left|\psi^{+}\right\rangle_{34}=\frac{1}{2}(\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}-\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}-\left|\phi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}-\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}). \quad (3)$$

$$\left|\psi^{+}\right\rangle_{12}\left|\psi^{-}\right\rangle_{34}=\frac{1}{2}(\left|\psi^{+}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}-\left|\psi^{-}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\phi^{+}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}-\left|\phi^{-}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}). \quad (4)$$

$$\left|\psi^{+}\right\rangle_{12}\left|\phi^{-}\right\rangle_{34}=\frac{1}{2}(\left|\psi^{+}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}-\left|\psi^{-}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}-\left|\phi^{+}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}+\left|\phi^{-}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}). \quad (5)$$

$$\left|\psi^{+}\right\rangle_{12}\left|\psi^{+}\right\rangle_{34}=\frac{1}{2}(\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}+\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\psi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}). \quad (6)$$

$$\left|\psi^{-}\right\rangle_{12}\left|\psi^{-}\right\rangle_{34}=\frac{1}{2}(\left|\phi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}-\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}-\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\psi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}). \quad (7)$$

$$\left|\psi^{+}\right\rangle_{12}\left|\psi^{+}\right\rangle_{34}=\frac{1}{2}(\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}+\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\psi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}). \quad (8)$$

$$\left|\psi^{-}\right\rangle_{12}\left|\phi^{+}\right\rangle_{34}=\frac{1}{2}(\left|\phi^{-}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}-\left|\phi^{+}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}+\left|\psi^{-}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}-\left|\psi^{+}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}). \quad (9)$$

$$\left|\psi^{-}\right\rangle_{12}\left|\phi^{-}\right\rangle_{34}=\frac{1}{2}(\left|\phi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}-\left|\phi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}-\left|\psi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}+\left|\psi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}). \quad (10)$$

$$\left|\phi^{+}\right\rangle_{12}\left|\phi^{+}\right\rangle_{34}=\frac{1}{2}(\left|\phi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}+\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}+\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\psi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}). \quad (11)$$

One can see that there is an explicit correspondence between a known initial state of two qubit pairs and its swapped measurement outcomes.

Now, let us give a new secure quantum dialogue in a network using entanglement swapping. The protocol employs two independent communication channels, a trusted classical channel and a quantum channel which is should not be necessarily trusted. In fact, the classical channel is employed to user authentication or user identification. User authentication makes it possible for communicators to prove their identity, often as the first step to log into a system. The new secure quantum dialogue in a network using entanglement swapping can be described as follows:

Step 1: At first the applier of the communication, say Bob, applies to communicate with Alice via classical channel. To prevent the active attack strategy in the protocol, classical identity authentication (CIA) protocols such as Wegman-Carter protocol can be used.

Step 2: Suppose Charlie is a server who provides the service of quantum channels to the registered users Alice and Bob. If the authentication to Alice and Bob is succeeded in the classical channel, Alice and Bob may communicate, Charlie provides the quantum channels to the communicators.

Step 3: Suppose that Alice has a secret message consisting of 2M secret classical bits $\{(i_1, j_1), (i_2, j_2), ..., (i_M, j_M)\}$, where $(i_n, j_n \in (0, 1), n = 1, 2, ..., M)$, and she is willing to send it to Bob, while, Bob wants to send his secret reply message consisting of 2M secret classical bits $\{(k_1, l_1), (k_2, l_2), ...,(k_M, l_M)\}$ to Alice, where $(k_n, l_n \in (0, 1), n = 1, 2, ...,M)$. Charlie prepares a random sequence of $M+\delta$ groups of two entangled Bell states $\{(\left|\chi_1\right\rangle_{12}, \left|\chi_1'\right\rangle_{34}), (\left|\chi_2\right\rangle_{12}\left|\chi_2'\right\rangle_{34})...,(\left|\chi_n\right\rangle_{12}, \left|\chi_n'\right\rangle_{34}),...,(\left|\chi_M\right\rangle_{12}, \left|\chi_M'\right\rangle_{34}), \}$, where $\left|\chi_n\right\rangle_{12}, \left|\chi_n'\right\rangle_{34} \in (\left|\phi^{\pm}\right\rangle, \left|\psi^{\pm}\right\rangle)$, n=1, 2, 3,…, $M+\delta$.

$$\left|\phi^{+}\right\rangle=\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle), \quad (12)$$

$$\left|\phi^{-}\right\rangle=\frac{1}{\sqrt{2}}(\left|00\right\rangle-\left|11\right\rangle), \quad (13)$$

$$\left|\psi^{+}\right\rangle=\frac{1}{\sqrt{2}}(\left|01\right\rangle+\left|10\right\rangle), \quad (14)$$

$$\left|\psi^{-}\right\rangle=\frac{1}{\sqrt{2}}(\left|01\right\rangle-\left|10\right\rangle). \quad (15)$$

This random choice is Charlie's secret information and unknown to the communicators in this step. It is easy to verify that, the four Bell states can be transformed into each other by some unitary operations, which can be performed locally with nonlocal effects. After the preparation of the initial states, to each pair of entangled quantum states, Charlie sends qubits (1, 3) to Alice, while he sends qubits (2, 4) to Bob.

Step 4: To guarantee the security of the transmission of entangled particles from Charlie to the communicators and to check the honesty of the server, the sender, Bob, chooses δ groups randomly from his particle groups, these are called as checking group used to test the security of the communication. The other particles are called as the communication group which is used to communicate. Then he asks Charlie to publicly announce him and Alice which Bell states the initial quantum channels was. Afterwards he performs measurements on his particles in the checking group using computational bases $(\left|+\right\rangle, \left|-\right\rangle, \left|1\right\rangle, \left|0\right\rangle)$ randomly, and then tells Alice

which particles are selected as the checking group and his measurement bases and measurement outcomes, lets her to perform the measurement using the similar bases as used by himself. So, considering the initial quantum channels and the results of their measurements, the communicators can conclude if the quantum channels are secure or not. Also using this method they can check the honesty of the server.

Step 5: If the quantum channel is secure, using the communication group Alice and Bob may communicate. At first, the applier of the communication, Bob, asks the server, Charlie, publicly announces which Bell state the initial quantum channels are. Afterwards, Bob makes Bell state projective measurements on his particles, while Alice makes Bell state projective measurements on her particles, After the measurements, the Alice's and Bob's state is projected onto one of the four EPR states

$$\left|\psi^{i}\right\rangle = U^{i}\left|\psi^{0}\right\rangle. \tag{16}$$

where the two-particle entangled states $\left|\psi^{i}\right\rangle$, (i = 0, 1, 2, 3) can be obtained through performing unitary transformation U^{i} on the first particles in the EPR state $\left|\psi^{0}\right\rangle$. The unitary transformations U^{i} can be denoted as:

$$U^{0} = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, U^{1} = \sigma_{z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, U^{2} = \sigma_{x} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, U^{3} = i\sigma_{y} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \tag{17}$$

Then they agree that each subscript 0, 1, 2, 3 correspond to binary classical bits, 00, 01, 10, 11, respectively. Afterwards, to send his two secret bits to Alice, Bob sends two classical information bits to Alice, which are the outcome of binary subtraction between secret information and his measurement outcome. For instance, if he obtains | 1i after his Bell measurement, and his secret information is 11, he sends the classical information 10 = 11 − 01, to Alice. On the other hand, as Alice knows the outcomes of Bob's Bell measurements, she is able to first read the message received from the Bob, and then using the same method used by Bob, she can send another message back in reply to the Bob's message.

The preceding five steps constitute the description of our new secure quantum dialogue protocol. For clarity, we will show an example:.

If Charlie initially prepares $\left|\psi^{+}\right\rangle_{12}, \left|\psi^{+}\right\rangle_{34}$. Then he sends particles 1 and 3 to Alice, and sends particles (2, 4) to Bob. So the state of the whole system can be denoted as shown in Equation 3. So, if Alice performs a Bell measurement on particles 1 and 3, she will obtain one of the four EPR states $(\left|\psi^{+}\right\rangle_{13}, \left|\phi^{-}\right\rangle_{13}, \left|\phi^{+}\right\rangle_{13}, \left|\phi^{-}\right\rangle_{13}$ with equal probability $\frac{1}{4}$ of for each. Suppose that Alice's measurement outcome is $\left|\phi^{-}\right\rangle_{13} = \left|\psi_{2}\right\rangle = U^{2}\left|\psi_{0}\right\rangle$ and she is willing to send her two bits secret message 01 to Bob. So she sends classical information 11 to Bob. It is needless to say that as Bob knows the outcome of the Alice's Bell measurement, he can deduce Alice's secret message as (1 + 1, 1 + 0) = (0, 1). On the other hands, Bob can also transmit his secret reply message to Alice after he reads Alice's secret message.

SECURITY ANALYSIS

It must be mentioned that every secure communication protocol, whether quantum or classical, needs an authenticated channel. User authentication (also called user identification) makes it possible for a communicator to prove his/her identity, often as the first step to log into a system. Usually the authenticated channel is tacitly assumed. The need for an authenticated channel in any secure communication protocol can be seen immediately when asking: How can Alice be sure that it is Bob she is talking to? If there is no authenticated channel, then a man-in-the-middle attack is always possible, resulting in a complete loss of security. For example, suppose that the public channel in BB84 was not authenticated. Then Eve could simply slip into the role of Bob, capture all qubits and receive all measurement results from Alice, perform her own measurements, compare some of them publicly with Alice and finally establish a shared secret key between herself and Alice. In the meantime, Bob can do nothing, but inform Alice (via public channel) that it is not he who she is talking to all the time. But since the public channel is not authenticated, why should Alice trust Bob more than Eve?

In fact, the perfect security of a quantum communication protocol stands and falls with the integrity of the public channel. That the public channel is rather seldom discussed or questioned in quantum cryptographic publications may be the reason why there is so little attention towards it, with all the focus lying on the quantum channel only. The security of the proposed protocol only depends on the perfect quantum channel (EPR pairs). Thus, as long as the quantum channel is perfect, our scheme is secure and confidential. By the security checking method which is presented in the article, the perfect quantum channel can be obtained, that is, since if the entangled particles are successfully distributed, no particle has to be exchanged in the scheme, the protocol will be secure if the security check can be passed. So, our proposed protocol for secure quantum dialogue in a network using entanglement swapping is absolutely reliable and secure.

For example, suppose that an eavesdropper (Eve) wants to steal the secret information, she may intercept

particles from Charlie to Alice and Bob. And she substitutes Alice and Bob to perform the Bell state projective measurements on these particles. After Eve's measurements, the Alice's and Bob's state is projected onto one of the four EPR states $\left|\psi^A\right\rangle_{AA'} = U^i\left|\psi_0\right\rangle, \left|\psi^B\right\rangle_{BB} = U^j\left|\psi_0\right\rangle$. Then she resents them the fake entangled particles $\left|\psi^A\right\rangle_{aa'}, \left|\psi^B\right\rangle_{bb'}$. In this process, Eve can also deduce the secret information of both communicators according to their classical information. But in this case, there are no entanglement between Alice's particles and Bobs. Alice and Bob will get random measurement outcomes during the checking process. In addition, introducing an independent trusted classical channel as the only authenticated channel would avoid the vulnerability of the protocol against the distrustfulness of the server of the quantum channel, that is, Charlie.

Conclusion

In summary, a new secure quantum dialogue using entanglement swapping is presented. In this scheme, the server of the quantum channel, Charlie, prepares the quantum channels for the communicators, Alice and Bob, if the authentication to the communicators has succeeded in the classical identity authentication process. Then the legitimate communicators may talk securely with each other directly and privately by virtue of some encoding operations. In contrast with the previous secure quantum dialogue protocols, In addition to its security, there are two essential advantages in a proposed scheme. Firstly, in a new secure quantum telephone protocol, the server of the quantum channel, Charlie, should not be necessarily trusted. The other advantage of our protocol is that in our protocol, one party is able to first read the message received from the other party before sending another message back in reply.

ACKNOWLEDGEMENTS

The author would like to thank Soheila Gholipour and Yasna Naseri for their interest in this work. This work is supported by Islamic Azad University, Kermanshah Branch, Kermanshah, Iran.

REFERENCES

Bennett CH (1992). Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68:3121–3124.
Bennett CH, Brassard G (1984). Quantum Cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Syst. Signal Process, Bangalore, India. p. 175-179.
Bennett CH, Brassard G, Mermin ND (1992). Quantum cryptography without bell's theorem. Phys. Rev. Lett. 68:557-569.
Bostrom K, Felbinger T (2002). Deterministic Secure Direct Communication Using Entanglement Phys. Rev. Lett. 89:187902.
Boykin PO, Roychowdhury V (2003). Optimal encryption of quantum bits. Phys. Rev. A 67:42317-042322.
Ekert AK (1991). Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67: 661–663.
Gao F, Guo FZ, Wen QY, Zhu FC (2008). Quantum secure direct communication over the collective amplitude damping channel. Sci. Chin. Ser. G-Phys. Mech. Astron. 51:559.
Gisin N, Ribordy G, Tittel W, Zbinden H (2002), Quantum cryptography. Rev. Mod. Phys. 74:145-195.
Hillery M, Buzek V, Berthiaume A (1999). Quantum secret sharing. Phys. Rev. 59:1829-1834.
Karlsson A, Koashi M, Imoto N (1999). Quantum entanglement for secret sharing and secret splitting. Phys. Rev. 59:162-168.
Leung D (2001). Quantum vernam cipher. Quantum Inf. Comput. 2:14-34.
Naseri M (2009). Eavesdropping on secure quantum telephone protocol with dishonest server. Optics Commun. 282:3375–3378.
Nguyen BA (2004). Quantum dialogue. Phys. Lett. A 328: 6.
Sun Ying, Wen Qiao-Yan; Gao Fei; Zhu Fu-Chen (2009). Improving the security of secure quantum telephone against an attack with fake particles and local operations. Opt. Commun. 282:2278-2280.
Wen X, Liu Y, Zhou N (2007). Secure quantum telephone. Optics Commun. 275:278-282.
Xiao L, Long GL, Deng FG, Pan JW (2004). Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. 69:052307.
Xio-Bo Chen , QIAO-YAN WEN, FEN-ZHUO GUO, YING SUN, GANG XU, FU-CHEN ZHU (2008). Controlled quantum secure direct communication with w state. Int. J. Quant. Inform. 6:899-906.
Zhou N, Liu Y, Zeng G, Xiong J (2007). Novel qubit block encryption algorithm with hybrid keys. Physica A 375:693-698.
Zhou N, Zheng GH (2005). A realizable quantum encryption algorithm for qubits. Chin. Phys. 14:2164.