Network-topology-adaptive quantum conference protocols*

Zhang Sheng(张 盛)†, Wang Jian(王 剑),
Tang Chao-Jing(唐朝京), and Zhang Quan(张 权)

Department of Communication Engineering, National University of Defense Technology of China, Changsha 410073, *China*

(Received 20 February 2011; revised manuscript received 7 April 2011)

As an important application of the quantum network communication, quantum multiparty conference has made multiparty secret communication possible. Previous quantum multiparty conference schemes based on quantum data encryption are insensitive to network topology. However, the topology of the quantum network significantly affects the communication efficiency, e.g., parallel transmission in a channel with limited bandwidth. We have proposed two distinctive protocols, which work in two basic network topologies with efficiency higher than the existing ones. We first present a protocol which works in the reticulate network using Greeberger–Horne–Zeilinger states and entanglement swapping. Another protocol, based on quantum multicasting with quantum data compression, which can improve the efficiency of the network, works in the star-like network. The security of our protocols is guaranteed by quantum key distribution and one-time-pad encryption. In general, the two protocols can be applied to any quantum network where the topology can be equivalently transformed to one of the two structures we propose in our protocols.

Keywords: quantum conference, quantum network, network topology, quantum multicast

PACS: 03.67.Dd, 03.67.Hk, 42.50.Ex **DOI:** 10.1088/1674-1056/20/8/080306

1. Introduction

Quantum communication, based on areas of quantum mechanics such as the no-cloning principle, has the potential to make the process of information transmission more secure. For instance, quantum key distribution (QKD)[1−4] can produce a private key between two authorized users who may be discontent with classical cryptography systems. In addition, the great success of quantum communication in the past two decades has encouraged researchers to attempt to construct a widely covered quantum network.[5−12] Current proposals[5−17] for the implementation of a quantum communication network mainly fall into the paradigm of a network distributing a quantum key, commonly termed as QKD network. A feasibly implemented model of this type so far is the trusted network model, for example the DARPA[13,14] and SECOQC[15−17] networks. Since the deployment of a real QKD network requires the development of network architecture with a specific network topology, it is natural that one should consider network topology when executing an efficient quantum communication process. Widely employed in classical networks, reticulate or star-like topology also plays a large role in the quantum domain. To be specific, the newly established model of the SECOQC QKD network exploits a topology which can be equivalently translated to a combination of reticulate and star-like structures.[15] In addition, the 3-node quantum network demonstrated by Chen *et al.* was based on a triangle structure topology, which is a special reticulated case.[18] A typical example of the star-like topology paradigm is the metropolitan quantum communication network also presented by Chen *et al.*[19]

Quantum secure direct communication (QSDC), which is a new concept in quantum cryptography, permits a confidential message to be transmitted directly without encryption by a private key. The first QSDC scheme based on block transmission was proposed by Deng *et al.* in 2003,[20] although an earlier quasi-secure deterministic communication scheme, termed the ping-pong protocol,[21] paved the way for QSDC. Since the ping-pong protocol may be entirely insecure in a lossy channel, Cai *et al.*[22] improved it by doubling the process described in Ref. [20] and gave another QSDC protocol based on single photons.[23] After that, a lot of elaborately conceived QSDC protocols[24−33] were proposed using the striking quantum effect, such as the quantum one-time

*Project supported by the National Natural Science Foundation of China (Grant No. 60872052).
†Corresponding author. E-mail: shengzhcn@gmail.com, huoxingren112@163.com
© 2011 Chinese Physical Society and IOP Publishing Ltd

pad[31] or dense coding.[26] QSDC protocols based on continuous variables[34,35] were then proposed since it is difficult to prepare an ideal single-photon source with current technology. The above proposals are for one-way communication. Other proposals, concerning the transmisson of messages simultaneously from both sides to the other ones, appeared to make an improvement. Obviously, these schemes are more efficient when we extend the QSDC to a multiparty one, which can be equivalently translated into the quantum conference domain discussed in the next paragraph. For instance, Gao *et al.*[36] presented a simultaneous QSDC scheme between the central party and many other parties based on entanglement swapping. The scheme shows how many parties transmit their secret messages to one party. Recently, Jin *et al.*[37] proposed a three-party simultaneous QSDC scheme by using GHZ states. In their scheme, one user, Alice, can obtain the secret messages from the other two parties, Bob and Charlie. At the same time, Bob (or Charlie) can also obtain secret messages from Alice and Charlie (or Bob). Man *et al.*[38] doubted that most of the quantum two-way communication schemes might provide more chances for an eavesdropper since the particles in the channel are actually transmitted twice in a round. In Ref. [38] he then proposed an improved version using GHZ states and entanglement swapping.

As a new branch of multiparty quantum communication, quantum conference, whose goal is to enable one centre broadcasting messages to many authorized users, will become one of the most prevalent applications in quantum networks. Recently, Li *et al.* proposed a new concept known as quantum secret conference.[39] In his proposal, legitimate conferees first share a private key by a multiparty QKD scheme with GHZ states. Then, quantum state encryption, which is implemented by a CNOT circuit, is employed to broadcast confidential messages to both legitimate conferees, who can decode the messages from the encrypted states with their correspondent keys. Gu *et al.*[40] presented another scheme with partially entangled states, which are considered to be more easy to prepare in the laboratory, to improve its practicality. In this paper, we propose two distinctive protocols, which are sensitive to network topology and only work in a given network, respectively, with entanglement swapping and quantum data compression. In classical communication, network topology is one of the main factors that affect efficiency. We argue that this problem also exists in quantum network communication, especially for quantum secret conference.

2. Network topology

The main obstacle to deploying a multiparty quantum conference is posed by the quantum no-broadcasting principle, which makes the quantum conference much different from its classical counterpart. Obviously, unknown quantum states are not allowed to be transmitted to the users simultaneously. However, any conference scheme needs a broadcast protocol to let all the legal users obtain the messages at any given time. Fortunately, this might not be an obstacle when we concentrate on how to protect the classical information encoded in the quantum state. First, we present two basic topological structures, the reticulate network and the star-like network, as shown in Fig. 1.

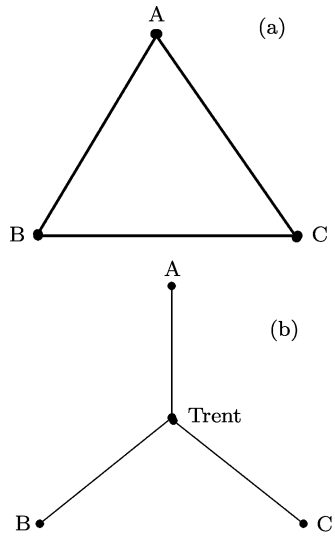


Fig. 1. Topological structures, (a) reticulate structure, (b) star-like structure.

In a reticulate structure, any two nodes are connected with each other, there can be up to $n(n-1)/2$ links in total. Here, we only consider a 3-user network for simplicity. In Fig. 1(a), suppose that three users A, B, C are holding a conference. Any legal listeners, say, B and C, can hear the talker A, simultaneously. In Fig. 1(b), a third node, commonly acting as a trusted party, Trent, is the centre of the structure.

We argue that any users in the quantum internet should be connected either by a physical channel or a virtual one controlled by a quantum switch, and there may be thousands of subnets similar to the counterpart, classical internet. Thus the topology between all the users in such a network can be equivalently transformed to reticulate or star-like topology. Thus these two structures are typical enough to implement a quantum conference protocol between any users in a quantum internet, even though this may not be the optimal one.

3. Our protocols

In this section, we present two quantum conference protocols working in a reticulate network and a star-like one, respectively. In order to avoid broadcasting an arbitrary state, quantum entanglement swapping is introduced to complete the task that a secret classical bit is broadcast to both listeners simultaneously. Essentially, the first can be equivalent to a one-to-many QSDC protocol, the only difference is that it is not necessary for the sender to reveal his result in a one-to-many scenario. The distinction is that quantum data encryption, in which quantum memory is unavoidable, is not needed, whereas quantum memory is indispensable in previous protocols. In the second protocol, the conference task is accomplished by a multiparty QKD and one-time-pad encryption, which guarantee unconditional security. In addition, we combine it with the quantum data compression algorithm exploited in Ref. [41] to improve the efficiency, the central party (Trent) plays the main role, who takes part in the compression and decompression process with both listeners.

3.1. Protocol A

Without loss of generality, suppose A is the talker, and B and C are listeners. First, each prepared n Bell states

$$|\Phi_{\rm A}^{+}\rangle_{12}^{\otimes n} = \frac{1}{\sqrt{2^n}}(|00\rangle_{12} + |11\rangle_{12})^{\otimes n}, \tag{1}$$

$$|\Phi_{\rm B}^{+}\rangle_{34}^{\otimes n} = \frac{1}{\sqrt{2^n}}(|00\rangle_{34} + |11\rangle_{34})^{\otimes n}, \tag{2}$$

$$|\Phi_{\rm C}^{+}\rangle_{56}^{\otimes n} = \frac{1}{\sqrt{2^n}}(|00\rangle_{56} + |11\rangle_{56})^{\otimes n}. \tag{3}$$

B transmits all the particles indexed in '3' to A and reserves the others. Similarly, C also sends all the particles indexed in '5' to A. Before they continue, A, B, and C perform a random test on these particles. Specifically, they choose a random subset and measure them in either the X or Z basis, then they compare the results to obtain an error rate. They continue only if the error rate is tolerable. A carries out a unity measurement on all the pairs indexed in '1, 3, 5'. Thus, the entanglement swapping referred to Fig. 2 is accomplished. The initial state is written by

$$\begin{aligned}
&|\Phi^{+}\rangle_{12} \otimes |\Phi^{+}\rangle_{34} \otimes |\Phi^{+}\rangle_{56} \\
&= \frac{1}{2\sqrt{2}}(|G_1^{+}\rangle_{135} \otimes |G_1^{+}\rangle_{246} + |G_1^{-}\rangle_{135} \otimes |G_1^{-}\rangle_{246}) \\
&\quad + \frac{1}{2\sqrt{2}}(|G_2^{+}\rangle_{135} \otimes |G_2^{+}\rangle_{246} + |G_2^{-}\rangle_{135} \otimes |G_2^{-}\rangle_{246}) \\
&\quad + \frac{1}{2\sqrt{2}}(|G_3^{+}\rangle_{135} \otimes |G_3^{+}\rangle_{246} + |G_3^{-}\rangle_{135} \otimes |G_3^{-}\rangle_{246}) \\
&\quad + \frac{1}{2\sqrt{2}}(|G_4^{+}\rangle_{135} \otimes |G_4^{+}\rangle_{246} + |G_4^{-}\rangle_{135} \otimes |G_4^{-}\rangle_{246}),
\end{aligned} \tag{4}$$

where $|G_i^{\pm}\rangle$ $(i = 1, 2, 3, 4)$ denotes one of the eight GHZ states written below

$$|G_1^{\pm}\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), \tag{5}$$

$$|G_2^{\pm}\rangle = \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle), \tag{6}$$

$$|G_3^{\pm}\rangle = \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle), \tag{7}$$

$$|G_4^{\pm}\rangle = \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle). \tag{8}$$

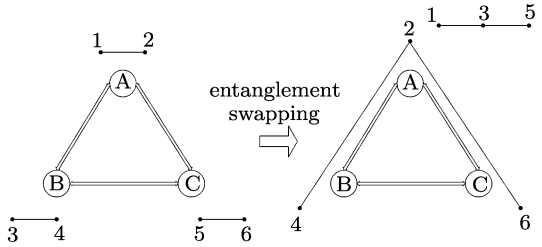


Fig. 2. Schematics of entanglement swapping in our protocol.

To encode the secret information, A should complete the following procedure before performing entanglement swapping. Given a secret sequence $M = \{m_1, m_2, \ldots, m_i, \ldots, m_l\}$, then A randomly performs the operation I (if $m_i = 0$) or σ_X (if $m_i = 1$) on the corresponding qubit state denoted as '2'. Once σ_X is performed, the quantum state is transformed to

$$\begin{aligned}
&|\Psi^{+}\rangle_{12} \otimes |\Phi^{+}\rangle_{34} \otimes |\Phi^{+}\rangle_{56} \\
&= \frac{1}{2\sqrt{2}}(|G_1^{+}\rangle_{135} \otimes |G_4^{+}\rangle_{246} + |G_1^{-}\rangle_{135} \otimes |G_4^{-}\rangle_{246}) \\
&\quad + \frac{1}{2\sqrt{2}}(|G_2^{+}\rangle_{135} \otimes |G_3^{+}\rangle_{246} + |G_2^{-}\rangle_{135} \otimes |G_3^{-}\rangle_{246}) \\
&\quad + \frac{1}{2\sqrt{2}}(|G_3^{+}\rangle_{135} \otimes |G_2^{+}\rangle_{246} + |G_3^{-}\rangle_{135} \otimes |G_2^{-}\rangle_{246}) \\
&\quad + \frac{1}{2\sqrt{2}}(|G_4^{+}\rangle_{135} \otimes |G_1^{+}\rangle_{246} + |G_4^{-}\rangle_{135} \otimes |G_1^{-}\rangle_{246}).
\end{aligned} \tag{9}$$

Next, A, B, and C perform an LOCC on all the qubits in 2, 4 and 6, as follows. First, each one measures their corresponding qubit in Z basis. Then, A reveals his results obtained from the measurement on qubits 1, 3, 5 and 2. B, as well as C, is able to figure out whether σ_X is carried out just from A's results and their own (see Table 1).

Table 1. Secret information decoding

$\|\phi\rangle_{135}$	$\|\varphi\rangle_{246}$	Transformation
$\|G_1^+\rangle_{135}$	$\|G_1^+\rangle_{246}(\|G_4^+\rangle_{246})$	$I(\sigma_X)$
$\|G_2^+\rangle_{135}$	$\|G_2^+\rangle_{246}(\|G_3^+\rangle_{246})$	$I(\sigma_X)$
$\|G_3^+\rangle_{135}$	$\|G_3^+\rangle_{246}(\|G_2^+\rangle_{246})$	$I(\sigma_X)$
$\|G_4^+\rangle_{135}$	$\|G_4^+\rangle_{246}(\|G_1^+\rangle_{246})$	$I(\sigma_X)$
$\|G_1^-\rangle_{135}$	$\|G_1^-\rangle_{246}(\|G_4^-\rangle_{246})$	$I(\sigma_X)$
$\|G_2^-\rangle_{135}$	$\|G_2^-\rangle_{246}(\|G_3^-\rangle_{246})$	$I(\sigma_X)$
$\|G_3^-\rangle_{135}$	$\|G_3^-\rangle_{246}(\|G_2^-\rangle_{246})$	$I(\sigma_X)$
$\|G_4^-\rangle_{135}$	$\|G_4^-\rangle_{246}(\|G_1^-\rangle_{246})$	$I(\sigma_X)$

B or C can always decode the message in sequence M with the classical information A reveals. For instance, A informed B and C in the classical channel that his result state was $|G_1^+\rangle_{135}$, then B (C) performs a measurement in Z basis on particle 4 (6), and obtains the classical information '0' ('0') or '1' ('1'), respectively. Finally, B or C figures out which operation, I or σ_X, was performed, after A revealed the result '0' ('1') or '1' ('0') of the measurement on particle 2 in Z basis.

3.2. Protocol B

In this subsection, inspired by the ideas in Ref. [38], we present a new protocol based on a star-like topology with quantum data compression. A secret key is shared in advance by all the users after they have carried out a multiparty quantum key distribution; this task can be completed by protocol A if σ_X is not concluded for simplification. A encrypts all the quantum states with the key and compresses them into a symmetric subspace, then he sends the compressed data to Trent. Trent decompresses the quantum states and sends them to the corresponding users, B and C, respectively.

Data compression: Suppose that A prepared two identical qubits shown below

$$|\varphi\rangle^{\otimes 2} = (a|0\rangle + b|1\rangle)^{\otimes 2} \ . \tag{10}$$

These qubits were encrypted with the key; the encryption can be realized by a CNOT logic gate where the key is the control bit and the information qubits are taken as the targets. The encrypted quantum state can be written as

$$|\varphi\rangle_{\rm E}^{\otimes 2} = (a'|0\rangle + b'|1\rangle)^{\otimes 2}. \tag{11}$$

These states are not transmitted to B and C directly. Instead, A compresses them and sends the compressed ones to Trent. We conceive a simple quantum lossless compression algorithm introduced in Ref. [38] to complete the task, then the quantum state is compressed into and decompress from the symmetric subspace $SYM(H^{\otimes N})$. The compression procedure can be described by the operation W, which satisfies

$$\begin{aligned} & W : |\varphi\rangle_{\rm E}^{\otimes 2} \otimes |0\rangle^{\lceil \log_2 3 \rceil} \\ = & \sum_{i=0}^{2} c_i |E_i\rangle \otimes |0\rangle^{\lceil \log_2 3 \rceil} \\ & \to |0\rangle^2 \otimes |I\rangle \\ = & \sum_{i=0}^{2} c_i |i\rangle, \end{aligned} \tag{12}$$

where

$$|E_i\rangle = \left(\begin{pmatrix} 2 \\ i \end{pmatrix} \right)^{-1/2} \sum_{x \in \{0,1\}^2, |x|=i} |x\rangle. \tag{13}$$

It is easy to obtain

$$c_0 = a'^2, \tag{14}$$

$$c_1 = 2a'b', \tag{15}$$

$$c_2 = b'^2. \tag{16}$$

From Eq. (12), it is obvious that only $o(\log 3)$ qubits were transmitted to Trent, thus the capacity of channel 'AT' is improved. For decompression, Trent just performs a reverse transformation of Eq. (12) to obtain the original encrypted state $|\phi\rangle_{\rm E}^{\otimes 2} = (a'|0\rangle + b'|1\rangle)^{\otimes 2}$ which will then be transmitted to the listeners, B and C.

Finally, B and C decrypt the states sent by Trent with the key and obtain the initial state $|\varphi\rangle^{\otimes 2} = (a|0\rangle + b|1\rangle)^{\otimes 2}$.

3.3. Security

So far, QKD is proved to be unconditionally secure no matter what strategies the eavesdropper (Eve) performs.[42] Generally, the security of quantum conference depends mainly on quantum principles, such as the no-cloning theorem and the quantum uncertainty principle. In our protocols, entanglement swapping plays an important role in broadcasting the secret information directly and distributing a key to both users. Thus, the security of these two protocols depends mainly on the purity of the Bell states in Eqs. (2) and (3). The best strategy for Eve to employ is to entangle her ancilla with particles '3' and '5', which travel in the public channel controlled by her. Eve just performs a CNOT operation on particle '3' , '5' and her ancilla $|0\rangle_{e_1}|0\rangle_{e_2}$, then we have

$$
\begin{aligned}
|\varphi_{\rm ABCE}\rangle &= U_{\rm CNOT}|\Phi^+\rangle_{12}\otimes|\Phi^+\rangle_{34}\otimes|\Phi^+\rangle_{56}\otimes|0\rangle_{e_1}\otimes|0\rangle_{e_2}\\
&= c_1|\rangle|\Phi^+\rangle_{12}\otimes|G^+\rangle_{34e_1}\otimes|G^+\rangle_{56e_2}+c_2|\Gamma\rangle_{\rm ABCE}\\
&= \frac{c_1}{2\sqrt{2}}(|G_1^+\rangle_{135}\otimes|G_1^+\rangle_{246}+|G_1^-\rangle_{135}\otimes|G_1^-\rangle_{246})|\Phi^+\rangle_{e_1e_2}\\
&\quad+\frac{c_1}{2\sqrt{2}}(|G_2^+\rangle_{135}\otimes|G_2^+\rangle_{246}+|G_2^-\rangle_{135}\otimes|G_2^-\rangle_{246})|\Phi^+\rangle_{e_1e_2}\\
&\quad+\frac{c_1}{2\sqrt{2}}(|G_3^+\rangle_{135}\otimes|G_3^+\rangle_{246}+|G_3^-\rangle_{135}\otimes|G_3^-\rangle_{246})|\Phi^+\rangle_{e_1e_2}\\
&\quad+\frac{c_1}{2\sqrt{2}}(|G_4^+\rangle_{135}\otimes|G_4^+\rangle_{246}+|G_4^-\rangle_{135}\otimes|G_4^-\rangle_{246})|\Phi^+\rangle_{e_1e_2}\\
&\quad+\frac{c_1}{2\sqrt{2}}(|G_1^+\rangle_{135}\otimes|G_1^-\rangle_{246}+|G_1^-\rangle_{135}\otimes|G_1^+\rangle_{246})|\Phi^-\rangle_{e_1e_2}\\
&\quad+\frac{c_1}{2\sqrt{2}}(|G_2^+\rangle_{135}\otimes|G_2^-\rangle_{246}+|G_2^-\rangle_{135}\otimes|G_2^+\rangle_{246})|\Phi^-\rangle_{e_1e_2}\\
&\quad+\frac{c_1}{2\sqrt{2}}(|G_3^+\rangle_{135}\otimes|G_3^-\rangle_{246}+|G_3^-\rangle_{135}\otimes|G_3^+\rangle_{246})|\Phi^-\rangle_{e_1e_2}\\
&\quad+\frac{c_1}{2\sqrt{2}}(|G_4^+\rangle_{135}\otimes|G_4^-\rangle_{246}+|G_4^-\rangle_{135}\otimes|G_4^+\rangle_{246})|\Phi^-\rangle_{e_1e_2}\\
&\quad+c_2|\Gamma'\rangle_{\rm ABCE},
\end{aligned}
\tag{17}
$$

where I is performed. However, the result state is similar when σ_X is performed. $|\Gamma\rangle_{\rm ABCE}$ and $|\Gamma'\rangle_{\rm ABCE}$ represent the state when A and B or A and C obtain inconsistent results in the test, so it is natural that Eve is able to extract a small portion of the key without detection. From Eq. (17), we obtain that Eve is able to extract a key bit with the probability of no more than $|c_1|^2$, since LOCC cannot give any information about the relative phase. Thus the maximal information Eve can obtain is $1-H(|c_1|^2)$, where $H(x)$ is the binary Shannon entropy function. From Eq. (17), we know that random test on the travelled particles is indispensable since the entanglement swapping itself cannot guarantee security. Thus, we can conclude that protocol A is unconditionally secure. So is protocol B, since the multiparty QKD procedure is similar to protocol A and the key will be used in a quantum one-time-pad system.

4. Conclusion

According to the two different network topologies, we propose two corresponding multiparty quantum conference protocols based on GHZ states and entanglement swapping. In protocol A, private information is directly broadcast to both conferees by multiparty entanglement swapping without encryption, entanglement purification provides a way to detect any eavesdropping in the channel. Compared with the protocols proposed in Refs. [36] and [37], it is more efficient because quantum memory is not introduced here and the secret information is broadcast directly to both conferees without encryption. In scheme B, a private key is established to each conferee by multiparty QKD, which is similar to protocol A. Then one-time-pad encryption is applied to the quantum states which will be compressed into a symmetric subspace. Obviously, the channel capacity is improved and is more efficient than previous ones. It is also concluded that network topology should be taken into consideration when the efficiency becomes the main concern, which also coincides with the fact that efficiency is always the most important factor for a secret conference protocol.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers Systems and Signal Processings* Bangalore, India, p. 175

[2] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[3] Wen H, Han Z F, Guo G C and Hong P L 2009 *Chin. Phys.* B **18** 46

[4] Wang H, Yan L S, Pan W, Luo B, Guo Z and Xu M F 2011 *Acta Phys. Sin.* **60** 56 (in Chinese)

[5] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651

[6] Townsend P D 1997 *Nature* **385** 47

[7] Townsend P D 1998 *Opt. Fibre Technol.* **4** 345

[8] Fernandez V, Collins R J, Gordon K J, Townsend P D and Buller G S 2007 *IEEE J. Quantum Electron.* **43** 130

[9] Poppe A, Peev M and Maurhart O 2008 *Int. J. Quantum Infor.* **6** 1

[10] Brassard G, Bussiéres F, Godbout N, Godbout N and Lacroix S 2003 *SPIE* **5260** 149

[11] Toliver P, Runser R J, Chapuran T E, Jackel J L, Banwell T C, Goodman M S, Hughes R J, Peterson C G, Derkacs D, Nordholt J E, Mercer L, McNown S, Goldman A and Blake J 2003 *Technol. Lett.* **15** 1669

[12] Dai J L and Zhang W H 2009 *Chin. Phys.* B **18** 426

[13] Elliott C 2002 *New J. Phys.* **4** 46

[14] Elliott C, Colvin A, Pearson D, Pikalo O, Schlafer J and Yeh H 2005 *Quantum Information and Computation* III (*Proc. SPIE* Vol. **5815**) p. 138 (*arXiv: quant-ph/* 0503058)

[15] www.secoqc.net.

[16] Alléaume R, Bouda J, Branciard C, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier P, Langer T, Leverrier A, Lutkenhaus N, Painchault P, Peev M, Poppe A, Pornin T, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H and Zeilinger A 2007 *arXiv: quant-ph*/0701168

[17] Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, Debuisschert T, Diamanti E, Dianati M, Dynes J F, Fasel S, Fossier S, Fürst M, Gautier J D, Gay O, Gisin N, Grangier P, Happe A, Hasani Y, Hentschel M, Hübel H, Humer G, Länger T, LegréM, Lieger R, Lodewyck J, Lorünser T, Lütkenhaus N, Marhold A, Matyus T, Maurhart O, Monat L, Nauerth S, Page J B, Poppe A, Querasser E, Ribordy G, Robyr S, Salvail L, Sharpe A W, Shields A J, Stucki D, Suda M, Tamas C, Themel T, Thew R T, Thoma Y, Treiber A, Trinkler P, Tualle-Brouri R, Vannel F, Walenta N, Weier H, Weinfurter H, Wimberger I, Yuan Z L, Zbinden H and Zeilinger A 2009 *New J. Phys.* **11** 075001

[18] Chen T Y, Liang H, Liu Y, Cai W Q, Ju L, Liu W Y, Wang J, Yin H, Chen K, Chen Z B, Peng C Z and Pan J W 2009 *Opt. Express* **17** 6540

[19] Chen T Y, Wang J, Liang H, Liu W Y, Liu Y, Xiao J, Wang Y, Wan X, Cai W Q, Ju L, Chen L K, Wang L J, Gao Y, Chen K, Peng C Z, Chen Z B and Pan J W *arXiv: quant-ph*/1008.1508

[20] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[21] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[22] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301

[23] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601

[24] Long G L, Deng F G, Wang C, Li X H, Wen K and Wang W Y 2007 *Front. Phys. China* **2** 251

[25] Xia Y and Song H S 2008 *Phys. Lett.* A **364** 117

[26] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 44305

[27] Yan F L and Zhang X 2004 *Eur. Phys. J.* B **41** 75

[28] Zhang Z J and Man Z X 2005 *Chin. Phys. Lett.* **22** 22

[29] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[30] Wang J, Zhang Q and Tang C J 2007 *Commun. Theor. Phys.* **48** 637

[31] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[32] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338

[33] Lee H, Lim J and Yang H 2006 *Phys. Rev.* A **73** 042305

[34] He G Q, Zhu J and Zeng G H 2006 *Phys. Rev.* A **73** 01231

[35] Pirandola S, Braunstein S L, Mancini S and Lloyd S 2008 *Europhys. Lett.* **84** 20013

[36] Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A: *Math. Gen.* **38** 5761

[37] Jin X R, Jin X, Zhang Y Q, Zhang S, Hong K, Yeon K H and Um C I 2006 *Phys. Lett.* A **354** 67

[38] Man Z X, Xia Y J and An B N 2006 *J. Phys.* B: *At. Mol. Opt. Phys.* **39** 3855

[39] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 23 *arXiv: quant-ph*/0612017v13

[40] Gu B, Li C Q and Chen Y L 2009 *Chin. Phys.* B **18** 2137

[41] Shi Y Y and Soljanin E 2006 *IEEE 40th Annual Conference on Information Science and System* **2** 871

[42] Mayers D 2001 *ACM* **48** 351