Quantum Optical Implementation of Quantum Communication

Li Yongmin, Zhang Kuanshou
State Key Lab of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan, China

ABSTRACT

Quantum theory has found a new field of application in the realm of communication during recent years. In this paper the rapid progress in quantum communication with quantum optics methods is reviewed. A brief introduction is given to quantum bit, entangled states, and Bell state measurement, which as "tools" play a very important role in quantum communications. The main topics of the quantum communication are presented: quantum cryptography, quantum teleportation, quantum dense coding, and purification. Finally technological issues are discussed.

Key words: quantum communication, entanglement, quantum optics

I. INTRODUCTION

It is generally recognized that all the microscopic phenomena that we observed can be described and explained by the principles of Quantum Mechanics. As the twentieth century went by, we witnessed a continuous increase in the applications of quantum mechanics, beginning with atomic physics and continuing with nuclear and particle physics, optics, condensed matter, and countless other developments [1]. One of the most important features of quantum theory is certainly the superposition principle. The superposition-principle can be applied to any physical property, and it is at the origin of quantum information theory that emerged as the twentieth century was closing[2]. It enables new forms of computation and communication, more powerful than its classical analogs. In this article, we review the progress of quantum communication based on quantum optics. The article is structured along the following lines: at first, we give a brief introduction to the "quantum toolbox" of quantum communication including quantum bit (qubit), entangled states, and Bell state measurement. These "tools" play a very important role in quantum communication. Then the main topics of the quantum communication are presented: quantum cryptography, quantum teleportation, quantum dense coding, and purification. Finally, we give a conclusion.

II. "QUANTUM TOOLBOX" OF QUANTUM COMMUNICATION

The most important entity of classical information theory is the bit (or cbit, for classical bit), a classical system with only two states, 0 and 1. Any text can be coded into a string of bits; for instance, it is enough to assign to each symbol its ASCII code number in binary form and append a parity check bit. Each bit can be stored physically (e.g., in classical computers, each bit is registered as a charge state of a capacitor.) and they are distinguishable macroscopic states and rather robust or stable. They are not spoiled when they are

read in and they can be cloned or replicated without any problem [1]. The quantum mechanical analog of the bit is the quantum bit or qubit. It is a two-state quantum system with the basic states $|0\rangle$ and $|1\rangle$ forming an orthogonal basis in the qubit space. In contrast to the classical bit, it is possible to create qubits in a coherent superposition of $|0\rangle$ and $|1\rangle$.

$$|\psi\rangle = \alpha|0\rangle + \beta e^{i\phi}|1\rangle, \ (\alpha^2 + \beta^2 = 1) \quad (1)$$

In contrast to classical bits, the outcome of a measurement of a qubit is not always deterministic. For the general qubit state given in Eq.(1), one finds the value "0" with probability α^2 and the value "1" with probability β^2. The unique feature of a quantum bit is that the basic states $|0\rangle$ and $|1\rangle$ is superposed coherently. When we measure the state $|\psi_1\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ with eigenvectors $|+\rangle = |0\rangle + |1\rangle$ and $|-\rangle = |0\rangle - |1\rangle$, we always find the result "+". This is different with an incoherent mixture state between $|0\rangle$ and $|1\rangle$, one will find the value "+" and "-" with equal probabilities. The most well known realization of a qubit is the one using orthogonal states of polarized photons and they can be created and measured using polarizers and waveplates oriented at various angles. There are also other possibility to realize a qubit, such as, time-bin qubits[3], etc. So far we only discuss the superposition of two orthogonal states, and it can be generalized to high-dimensional cases, i.e., qu-nits [4].

Entanglement can be seen as a generalization of the superposition principle to multi-particle systems. When a state cannot be described as the product states of its subsystem, states of such form are called entangled states and play a fundamental role in quantum communication. The maximum entangled states of two-particle (spin 1/2 particle), known as Bell states, can be written as

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle), \quad (1)$$

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle) \quad (2)$$

In many protocols of quantum communication it is the necessity to determine the state of a two-particle system. For qubits, this means to project on a basis in 4-dimensional Hilbert space, spanned for instance by the four Bell states (Eq.(2)). Such a measurement is known as a Bell-state measurement. It is shown that there is no experimental possibility to differentiate between all of the states as far as linear optics is concerned[5,6]. The best one can do is to identify two of the four Bell states. However, it is possible to obtain a complete Bell-state analysis with linear optics if the two particles are entangled in another degree of freedom as well[6], the disadvantage is it cannot be fulfilled by photons that come from independent sources. By taking advantage of non-linear interactions, one can also performed an complete Bell state measurement[7], the shortcoming is the efficiency is extremely small.

III. MAIN TOPICS OF THE QUANTUM COMMUNICATION

Up to now, some interesting applications of quantum communication have been discovered; they are quantum cryptography (QC), quantum teleportation, and quantum dense coding, etc.

3.1 Quantum cryptography

Quantum cryptography is certainly the most mature application of quantum communication. It provides us with an absolutely secure method for coding. Based on the principles of the quantum mechanics, it provides two parties, a sender Alice and a receiver Bob, with a means to distribute a secret key in a way that guarantees the detection of any eavesdropping: Any information obtained by an unauthorized third party about the exchanged key goes along with an increase of the quantum bit error rate (QBER) of the transmitted data which can be checked using a suitable subset of the data. It has been shown that, as long

as the QBER of the sifted key is below a certain threshold, Alice and Bob can still distill a secure key by means of classical error correction and privacy amplification protocols. The pioneering idea dates back to Stephen Wiesner, who as early as 1969 suggested this possibility, as well as the fabrication of forgery-proof, "quantum banknotes"[8] . The first QC protocol is proposed by Bennett and Brassard in 1984[9](BB84 protocol or four-state protocol), it uses four quantum states (two-level quantum system) that constitute two bases, the security of this protocol is based on the indivisible quanta and No-cloning theorem[10]. Since then, a lot of protocols are proposed by physical scientist: including two-state (B92) protocol[11], six-state protocol[12], Einstein-Podolsky-Rosen (EPR) protocol[13], and other variations. In 1989 the first experimental demonstration of quantum cryptography took place at IBM based on polarization coding with "single photons" over a distance of 30cm in air[14]. A lot of experimental progress has been made after that, to date, several different fiber-based prototype quantum crypto-systems have been constructed. In 2004, C. Gobby et al.[15] reported a quantum key distribution over 122km of standard telecom fiber with a QBER of 8.9%. After error correction and privacy amplification, the maximum bit rate is 1.9 kbit/sec.

All the schemes mentioned above are two-party QC schemes. In 1999[16], Hillery et al., propose the first quantum secret sharing scheme using GHZ states as an entanglement resource. Quantum secret sharing can be thought of as a multi-party generalization of quantum cryptography in which a message is not only protected against potential eavesdroppers, but can only be retrieved from several people who collaborate. Tittel et al.[17] reported in 2001 a proof-of principle demonstration of quantum secret sharing (three party quantum cryptography) in a laboratory experiment. This new protocol enables Alice to send key material to Bob and Charlie in a way that neither Bob nor Charlie alone have any information about Alice's key, however, when they collaborate, they can have full information.

3.2 Quantum teleportation

The aim of quantum key distribution is the communication of classical bits in some sense, quantum teleportation, discovered in 1993 [18], can be thought of as being the exchange of quantum bits. In a world of classical physics, it suffices to measure the properties of the classical bit and then communicate the information about its composition to Bob, who then reconstructs the bit. However, in the quantum case the measurement of an unknown qubit without disturbing it is impossible and cloning is forbidden. If Alice and Bob share an EPR pair (see Fig.1), first Alice makes a Bell measurement on the unknown qubit and her part of the entangled pair, thus projects the two-particle state randomly onto one of the four Bell states. The outcome of this measurement projects Bob's particle onto one of four different states as well. Using two classical bits, Alice now tells Bob the outcome of her measurement and Bob can reconstruct Alice's unknown quantum state by performs one of four unitary operations on his particle. This procedure necessarily destroys Alice's state (thus quantum no-cloning theorem is not violated) and classical information from Alice is needed to reconstruct the unknown state, so faster than light commu-

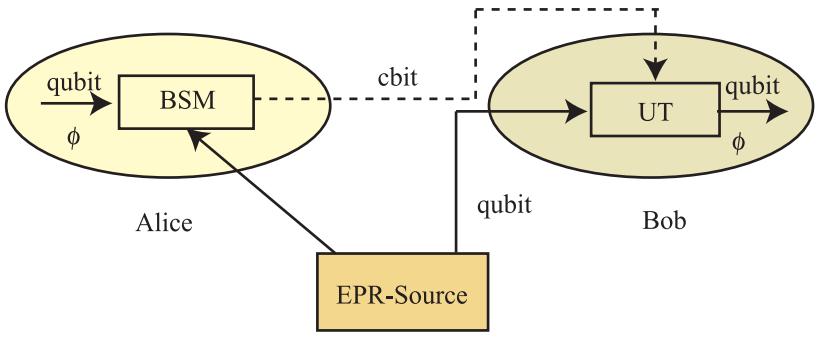

Fig.1 Scheme for quantum teleportation. BSM, Bell state measurement; UT, unitary transformation.

nication is not possible.

Quantum teleportation was realized experimentally with photons (polarization qubits) for the first time in 1997 based on Bell state measurement using linear optics[19]. After that several groups realized it with different setup[20-23]. Particularly, a long-distance experimental demonstration of quantum teleportation over 2km telecommunication fiber was reported in 2003: Qubits carried by photons of 1.3 micron wavelength are teleported onto photons of 1.55 micron wavelength. In addition, quantum teleportation based on continuous quantum variables (infinite dimension system) was also demonstrated in 1998 with fidelity of 0.58[24]. Later several groups realized it with different fidelity[25-27]. Very recently[28], continuous variable quantum teleportation beyond no-cloning limit of 2/3 was also experimentally demonstrated with fidelity of 0.70. The experimental realization of quantum teleportation has invoked a strong reaction in the public. Whereas on can clearly say that quantum teleportation in its current form has no relation to disembodied transport of objects or even humans. In general, quantum teleportation can be thought as the transfer of an unknown state (but still well defined). A natural extension is any relation that original particle has with respect to other systems should be transferred as well. This generalized concept was mentioned for the first time in 1993[29], has become known as entanglement swapping (or teleportation of entanglement) and been demonstrated in experiment for discrete variables[30] and continuous variables[31].

3.3 Quantum dense coding

In quantum physics we can encode information in a novel way into joint properties of elementary systems in entangled states, leading in principle to the possibility to transmit two bits of information by sending only one qubit. This striking application of quantum communication is known as quantum dense coding [32]. Assume for instance, an entangled state of two photons (see Fig.2). One of the photons goes to Alice, the other one to Bob. Alice performs one of the following operations on the polarization of her arriving photon: identity, flipping, change of pi in the relative phase, and the product of the last two. Once this is done, she sends the photon back to Bob, who measures in which of the four Bell states the photon pair is. In this fashion they have been able to share two bits of information over one single particle with only two states, that is by means of qubit. This is twice what can be accomplished classically, hence the name dense coding.

An experiment of this nature was first performed

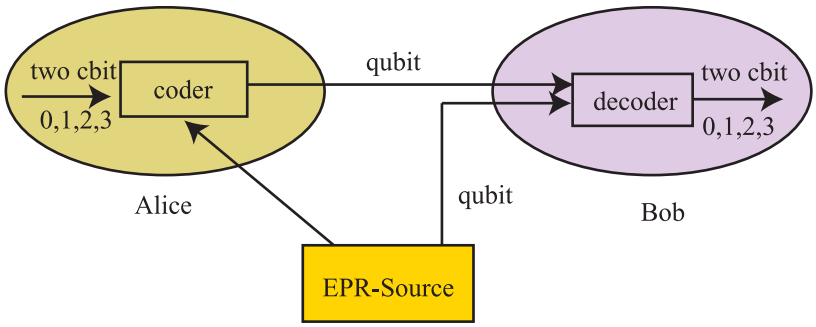

Fig.2 Scheme for quantum dense coding.

in 1996[33] by using polarization entangled photon pair from spontaneous parametric down conversion. In this experiment only two out of four Bell states can be distinguished unambiguously whereas the other two states lead to identical signatures, but it is enough to encode three-valued information (corresponding to 1.58 bit of information) into each transmission event. Recently, quantum dense coding for continuous variables has also been experimentally accomplished by means of a bright EPR beam with anticorrelation of amplitude quadratures and correlation of phase quadratures [34]. When one use multi-partite entangled state instead of two-partite entangled state, a more

sophisticated scheme called controlled quantum dense coding can be realized[35].

3.4 Purification

When the quantum communication protocols are extended to large distance, the quantum states will transmit through a noisy environment and suffer from decoherence unavoidably. Most of the applications in the field of QC are based on the use of superposition of pure states. Fox example, if one would like to perform quantum cryptography over long distances using entangled photons, when they arrive at the final locations their state will also be entangled to the environment and therefore mixed. The longer the distance the photons have to travel, the mixed they will become. If they are significantly mixed, the security of the corresponding cryptographic protocol will no longer be ensured. There are many attempts to overcome this problem, and some approaches have been proposed. Among them are entanglement distillation, purification and concentration, and quantum error correction [36,37]. Recently, the entanglement purification for general mixed states of polarization-entangled photons was experimentally demonstrated[38] by using linear optics.

IV. CONCLUSION

In this article we reviewed the recent advances of quantum communication by using quantum optics. Many laboratories all over the world are working towards developing many different physical implementations of quantum communication devices. It will be interesting to see which technology will be the best. For future technological developments, new sources for single-photon states are needed. Some schemes have been proposed: faint laser pulses, photon pairs generated by parametric down-conversion (one of the photons is used as a trigger). But above-mentioned single-photon sources cannot produce ideal single-photon. The ideal single-photon source is a device that, when one pulls the trigger, one and only one photon is emitted. There has been important progress over the past few years in this field from various directions, including atoms in cavities[39] and solid-state devices such as cavity-coupled quantum dots[40]. At present, the most accessible two and even multi-photon entangled states are produced by optical parametric down conversion. Unfortunately, such sources are probabilistic and post-selection is needed in some cases. So it would be good to have sources that produce any multi-photon state, even entangled ones, on demand. Experiments along this line have been performed in the context of cavity quantum electrodynamics (QED) [41]. Also, more efficient photon detectors are needed that operate over a broader wavelength range than those currently available. Particularly, detector that is able to discriminate clearly photon number.

REFERENCE

[1] A. Galindo and M. A. Martin-Delgado, Reviews of Modern Physics, 74, 347 (2002).

[2] Wolfgang Tittel, Quantum Information and Computation, 1, 3 (2001).

[3] H. Zbinden et al., Electron. Lett. 33, 586 (1997).

[4] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A 61, 062308 (2000).

[5] N. L ü tkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A 59, 3295 (1999).

[6] P. G. Kwiat and H. Weinfurter, Phys. Rev. A 58, R2623 (1998).

[7] Y.-H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. 86, 1370 (2001).

[8] S. Wiesner, SIGACT News 15 (1), 78.

[9] C. H. Bennett, , and G. Brassard, in Proceedings of the international Conference on Computers, Systems & Signal Processing, Bangalore, India (Indian Institute of Science, Bangalore, India), 175 (1984).

[10] W. K. Wooters, and W. H. Zurek, Nature (London) 299, 802 (1982).

[11] C. H. Bennett, , Phys. Rev. Lett. 68, 3121 (1992).

[12] D. Bruss, Phys. Rev. Lett. 81, 3018 (1998).

[13] A. K. Ekert, Phys. Rev. lett., 67, 661 (1991).

[14] C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).

[15] C. Gobby, Z. L. Yuan, A. J. Shields, Appl. Phys. Lett. 84, 3762 (2004).

[16] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A 59, 1829 (1999).

[17] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A 63, 042301 (2001).

[18] C. H. Bennett et al., Phys. Rev. Lett. 70, 1895 (1993).

[19] D. Bouwmeester et al., Nature 390, 575 (1997).

[20] D. Boschi et al., Phys. Rev. Lett. 80, 1121 (1998).

[21] Y.-H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. 86, 1370 (2001).

[22] J. W. Pan, S. Gasparoni, M. Aspelmeyer, T. Jennewein, and A. Zeilinger, Nature 421, 721 (2003).

[23] I. Marcilic, H. de. Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Nature 421, 509 (2003).

[24] A. Furusawa et al., Science 282, 706 (1998).

[25] W. P. Bowen, N. Treps, et al., Phys. Rev. Lett. 86, 4267 (2001).

[26] T. C. Zhang, et al., Phys. Rev. A 67, 023802 (2003).

[27] Z. H. Zhai, Y. M. Li, S. K. Wang, J. Guo, T. C. Zhang, J. R. Gao, Acta Phys. Sin. 54, 6 (2005) (in Chinese).

[28] N. Takei, et al., Phys. Rev. Lett. 94, 220502 (2005).

[29] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. 71, 4287 (1993).

[30] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. 80, 3891 (1998).

[31] X. Jia, X. Su, Q. Pan, J. Gao, C. Xie, K. Peng, Phys. Rev. Lett. 93, 250503 (2004).

[32] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992).

[33] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. 76, 4656 (1996).

[34] X. Li, Q. Pan, J. Jing, J. Zhang, C. Xie, K. Peng, Phys. Rev. Lett. 88, 047904 (2002).

[35] J. Jing, J. Zhang, Y. Yan, F. Zhao, C. Xie, K. Peng, Phys. Rev. Lett. 90, 167903 (2002).

[36] The Physics of Quantum Information, edited by D. Bouwmeester, A. Ekert, and A. Zeilinger (Springer, Berlin, 2000).

[37] H.-K. Lo, S. Popesch, and T. Spiller, Introduction to quantum computation and information (World Scientific, Singapore, 1998).

[38] J. W. pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Nature 423, 417 (2003).

[39] J. McKeever, et al. Science 303, 1992 (2002).

[40] C. Santori, D. Fattal, et al., Nature 419, 594 (2002).

[41] S. Brattke, B. T. H. Varcoe, et al., Phys. Rev. Lett. 86, 3534 (1999).

BIOGRAPHY

Li Yongmin *was born in Shanxi Province, China, in 1977. He received the Ph.D. degree from the Shanxi University in 2003. He is currently with State Key Laboratory of Quantum Optics and Quantum Devices, Institute of Opto-Electronics, Shanxi University. His research interests include experimental and theoretical studies of optical quantum information, laser physics, etc.*

Zhang Kuanshou *was born in Shanxi Province, China, in 1965. He received the Ph.D. degree from the Shanxi University in 1997. He is currently with State Key Laboratory of Quantum Optics and Quantum Devices, Institute of Opto-Electronics, Shanxi University. His research interests include experimental and theoretical studies of quantum optics, laser physics, etc. He can be reached at kuanshou@sxu.edu.cn*