A scheme of optical network for quantum cryptography based on wavelength division multiplexing

Hai-Qiang Ma, Rui-Xue Li, Ke-Jin Wei, Hong-Wei Liu and Zhu Wu
School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876
Corresponding author e-mail address: hqma@bupt.edu.cn

Abstract: Quantum key distribution(QKD), unlike its classical counterparts, provides information-theoretic security and has aroused great interesting among both scientists and engineers. Many researchers has focused on the constructing of quantum network. In this paper, we present a multi-user system for quantum cryptography based on wavelength division multiplexing. It allows for a simple, cost-effective and reliable deployment with its character of auto compensation and accomplishes time division multiplexing at the same time. The way of phase coding and polarization measurement is also certified.
Key words: quantum key distribution, multi-user, wavelength division multiplexing

In the fields of quantum mechanics and standard information theory, a new cryptography is proposed and can offer information-theoretic security as well as easy key management, which is called quantum key distribution (QKD). Normally, QKD system enable two parties, the sender and the receiver, to accomplish a point-to-point secret sharing[1]. After enormous experiments, point-to-point QKD systems have matured with secure key rate exceeding 1Mb/s[2]. In the past two decades, QKD is maturing quickly, and many studies have focused on the development of multi-user quantum communication. Up to data, wavelength division multiplexing (WDM) is becoming a dominant technology in the network construction[3]–[7].

The standardized use of WDM defines a grid of channels, each with a central wavelength, uniformly arranged in the optical spectrum. Depending on the spectral distance between adjacent channels, WDM can be divided into two kinds, coarse WDM (CWDM) and dense WDM (DWDM)[8], [9]. Compared to the single channel for quantum cryptography system, WDM not only enlarges the message capacity and make the best of fiber bandwidth, but also has the advantages of simplicity and stabilization.

Here, we present a multi-user scheme for quantum cryptography based on wavelength division multiplexing. It accomplishes to communicate with multi-users with a simple implement, takes advantage of existing infrastructure, allowing for an easy, cost-effective and reliable deployment.

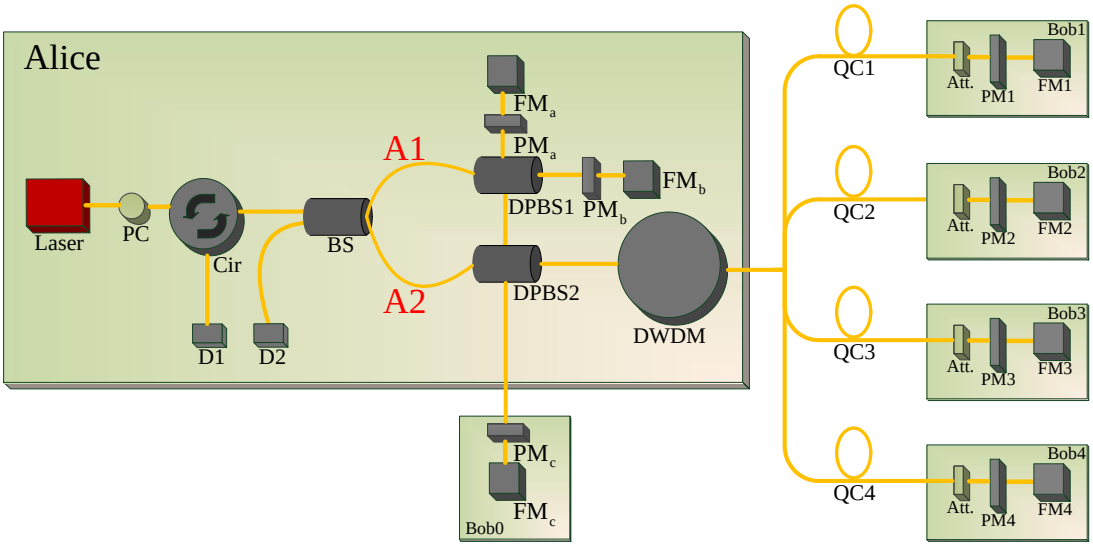

Fig.1. Schematic of multi-user system for quantum cryptography with wavelength division multiplexing. Laser: pulsed laser diode; PC: polarization controller; Cir: circulator; DPBS:

Four-port polarization beam splitter; PM: phase modulators; FM: Faraday mirrors; QC: quantum channel; D1, D2: single photon detectors; Att.: attenuator; DWDM: dense wavelength division multiplexing.

Fig. 1 shows the schematic. The principle can be described as follows: a pulsed laser diode (LD) used as a single photon source sends a single photon pulse which polarization is controlled by a polarization controller (PC). For simplicity, supposing the pulse is parallel polarization, the pulse is divided into two pulses equally, A1 and A2, by the 50/50 beam splitter and the incident pulse into the input port of DPBS1 and DPBS2 respectively. For convenience, we also define the DPBS reflects the vertical polarized pulse and transmits the parallel polarized pulse. The pulse A1 passes through a phase modulation (PM_b) and then is reflected back by a Faraday Mirror (FM_b). In this process, the polarization of the pulse A1 turns into vertical polarized state and is reflected by DPBS1. After that, the pulse A1 is coupled into one port of the DPBS2 and is reflected by it. The pulse A1 then travels to Bob through a wavelength division multiplexing (WDM), where the pulse will be divided into different wavelength and transmitted to corresponding quantum channel. For example, A1 passes through WDM and QC with specific length to Bob1. After reflected by the FM1 in Bob1, it comes back with parallel polarized state. Finally, A1 arrives at the BS where it is separated. In the same way, the pulse A2 takes the opposite route comparing with pulse A1 and arrives at BS at the same time. This process fulfills quantum key distribution between Alice and Bob1. By this way, the quantum key distribution between Alice and other Bobs can be accomplished. For different quantum channels have different length so that the delay time is different. The interference in different processes will not happen in BS at the same time, so the implements realize time division multiplexing as well.

In conclusion, the scheme can be seen as a tree network topology architecture that Alice, the network controller, can communicate with many users such as Bob1, Bob2, Bob3 … by adding DPBS and WDM. Furthermore, the system provides auto compensation of birefringence with just a commercial polarization-sensitive phase modulator connected to a Faraday mirror in every user's station so that the system is maintained over a long time. Thanks to this design, our setup can also automatically provide completely polarization-insensitive phase modulation.

In the next section, we propose a new basic unit model for implementing a fiber based network of quantum key distribution by phase coding and polarization measurement, which is displayed in Fig. 2. A laser emits pulse of photons in a given polarization state, for convenience denoted in the figure as the $+45^{\circ}$ polarization state, which passes through a circulator (Cir) and is equally divided into two orthogonally polarized pulses, A1 and A2, by the four-port polarization beam splitter (DPBS). For convenience of notation we define that DPBS reflects the vertically polarized pulse A1 and transmits the horizontally polarized pulse A2.

The A1 reaches FM_b and is reflected back in the horizontally state, after across DPBS, it is reflected by FM_a with a 90° polarization rotation, and returns back to DPBS. Then the A1 passes through the wavelength division multiplexing and the corresponding quantum channel to reach Bob. Take Bob1 as an example, when A1 passes across to Bob1, it will be phase modulated at PM1 after reflected by FM1 with a 90° polarization rotation, and attenuated to the single-photon level to prevent possible attacks from Eve. The A2 passes straight through DPBS, the WDM and the quantum channel to reach Bob1 directly, and it is reflected by FM1 back to Alice after suitable attenuation as vertically polarized single photons. Then it is reflected by DPBS to FM_a, which rotates the polarization to horizontal again. After modulation at PM_a and reflection back to DPBS the photons will pass through DPBS to reach FM_b and is reflected back in the vertical state. The A1 and A2 will return simultaneously at DPBS and then combine into one pulse, with a polarization determined by the relative phase shifts introduced by Alice and Bob in their phase modulators.

Both pulses pass through the two phase modulators PM1 and PM_a twice on their round-trip journeys, which cancel out the polarization effects of the modulators and the trunk fiber, but one is modulated by PM1 and the other by PM_a.

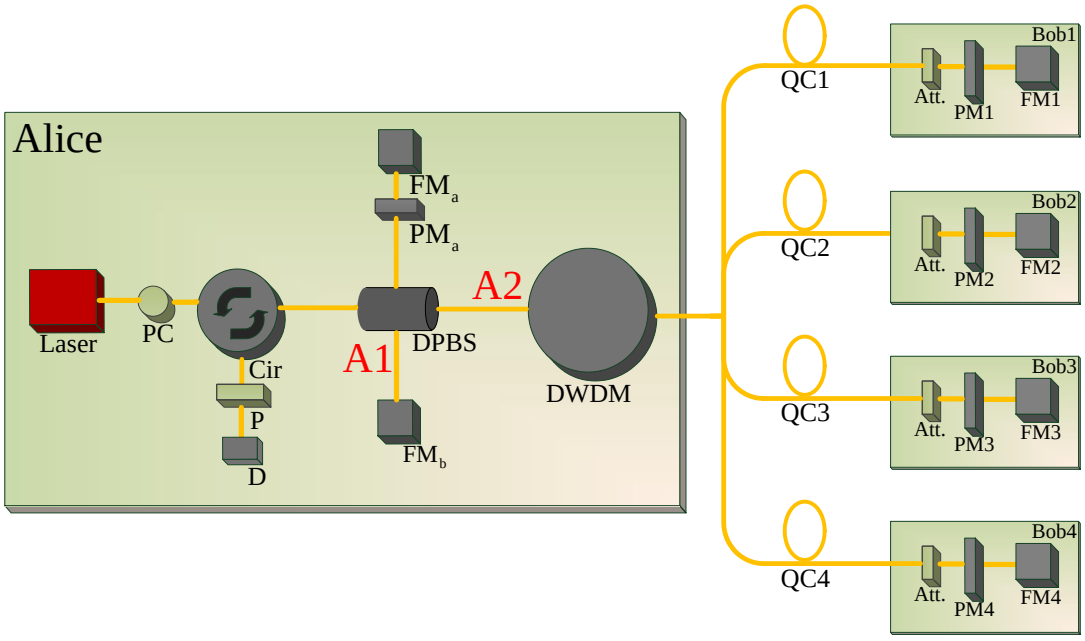

Fig. 2. Schematic of multi-user system with by phase coding and polarization measurement. Laser: pulsed laser diode; PC: polarization controller; Cir: circulator; DPBS: Four-port polarization beam splitter; PM: phase modulators; FM: Faraday mirrors; QC: quantum channel; P: linear polarizer at $+45^{\circ}$; D: single photon detectors; Att.: attenuator; DWDM: dense wavelength division multiplexing.

Let us now look at how the B92 protocol can be implemented. The measurement setup consists of an analyzing polarizer P set at $+45^{\circ}$ and only one detector D, as shown in Fig 2. Alice can choose $PM_a = 0$ or $\pi/2$ for her modulation phase, while Bob1 can choose PM1= π or $3\pi/2$. Table 1 shows that a photon can pass through the polarizer and be detected with a probability of 50% when Alice uses a phase of 0 ($\pi/2$) and Bob chooses $3\pi/2$ (π). Thus Alice and Bob have an identical bit string according to their assumption such as: 0 or $3\pi/2$ represents "0" and $\pi/2$ or π represents "1". Alice and Bob1 exchange only the base not bit value, and the private key can be established and never disclosed to the public. Others are the same.

Table 1. Polarization states and detection probability at the detectors for different values of phase shifts chosen by Alice and Bob.

Alice \ Bob	π	$3\pi/2$
0	0	50
$\pi/2$	50	0

In summary, a fiber-based multi-user network with wavelength division multiplexing has been demonstrated. It allows an easy, cost-effective and reliable deployment. Furthermore, a multi-user system by phase coding and polarization measurement has been proposed, It has a simplified structure in comparison with convention QKD system and uses only one single photon detector for B92 protocol, which further reduces the system cost. Both of the two systems can be maintained over a long time since they can auto compensation of the birefringence in the fiber.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61178010); the Fundamental Research Funds for the Central Universities, China (Grant No. bupt 2014TS01).

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[2] A. Tanaka, M. Fujiwara, K. I. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, “High-speed quantum key distribution system for 1-mbps real-time key generation,” *IEEE J. Quantum Electron.*, vol. 48, no. 4, pp. 542–550, 2012.

[3] B. Frohlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, “A quantum access network,” *Nature*, vol. 501, no. 7465, pp. 69–72, Sep. 2013.

[4] K.-J. Wei, H.-Q. Ma, and J.-H. Yang, “Experimental circular quantum secret sharing over telecom fiber network,” *Opt. Express*, vol. 21, no. 14, pp. 16663–16669, 2013.

[5] C. A. Brackett, “Dense wavelength division multiplexing networks: principles and applications,” *Selected Areas in Communications, IEEE Journal on*, vol. 8, no. 6. pp. 948–964, 1990.

[6] H.-Q. Ma, J.-L. Zhao, and L.-A. Wu, “A simple plug&play quantum key distribution scheme with extremely long-term stability,” in *Conference on Lasers and Electro-Optics/Pacific Rim 2007*, 2007, p. WP_085.

[7] M. Hai-Qiang, W. Ke-Jin, and Y. Jian-Hui, “Experimental single qubit quantum secret sharing in a fiber network configuration,” *Opt. Lett.*, vol. 38, no. 21, pp. 4494–4497, 2013.

[8] T. Ohara, H. Takara, T. Yamamoto, H. Masuda, T. Morioka, M. Abe, and H. Takahashi, “Over-1000-Channel Ultradense WDM Transmission With Supercontinuum Multicarrier Source,” *J. Light. Technol.*, vol. 24, no. 6, p. 2311, 2006.

[9] A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martín, “Quantum metropolitan optical network based on wavelength division multiplexing,” *Opt. Express*, vol. 22, no. 2, pp. 1576–1593, 2014.