A full quantum network scheme

Ma Hai-Qiang(马海强)†, Wei Ke-Jin(韦克金), Yang Jian-Hui(杨建会),
Li Rui-Xue(李瑞雪), and Zhu Wu(朱 武)

School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, *China*

(Received 20 June 2014; revised manuscript received 22 August 2014; published online 12 September 2014)

We present a full quantum network scheme using a modified BB84 protocol. Unlike other quantum network schemes, it allows quantum keys to be distributed between two arbitrary users with the help of an intermediary detecting user. Moreover, it has good expansibility and prevents all potential attacks using loopholes in a detector, so it is more practical to apply. Because the fiber birefringence effects are automatically compensated, the scheme is distinctly stable in principle and in experiment. The simple components for every user make our scheme easier for many applications. The experimental results demonstrate the stability and feasibility of this scheme.

Keywords: quantum key distribution, quantum communication, quantum network

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/23/10/100307

1. Introduction

Quantum key distribution (QKD) exploits the fundamental laws of quantum mechanics rather than algorithms based on mathematical complexity to enable two separated parties (commonly called Alice and Bob) to generate a secret key in the presence of an eavesdropper. QKD was first proposed by Bennett and Brassard in 1984, and the first experimental prototype, which could transmit keys in distance 32 cm through free space, was demonstrated at IBM.[1,2] Subsequently, QKD was developed and realized in a number of different configurations: with entangled photons, single photons, and continuous variables, via single fiber and free spaces, and at visible and telecommunication wavelengths.[3–10] However, none of these implementations are suitable for multiuser communications because they are point-to-point links. Many studies have focused on the development of multiuser QKD networks based mainly on optical power splitters, optical switches, or wavelength-division multiplexing.[11–18] Although such "quantum networks" have represented great advances, they are not full networks because quantum communication can occur only between users and a server and typically require two single-photon detectors for each user, which is prohibitively expensive for many applications.

In this letter, we present a novel quantum network scheme using a modified BB84 protocol in a Sagnac-type interferometer setup containing an optical switch as well as Faraday mirrors. In the protocol, Charlie is an intermediary detecting user located in the middle; he prepares a single qubit and detects it after it is sequentially communicated from Alice to Bob, who act on it with the unitary phase operator. To help Alice and Bob share the key, Charlie publishes the detection results on the public channel. This structure is similar to measurement-device-independent QKD,[19] so our scheme can defend against all potential attacks using loopholes in a detector, such as the blinding attack and the time-shift attack,[20,21] when point-to-point communication occurs in our network. Furthermore, our quantum network is a full network in which a quantum key can be distributed between two arbitrary users. Only the detecting user requires two single-photon detectors; the other users need only a phase modulator and Faraday mirrors, which are often cheap and easy to operate in practical applications. The setup in our scheme does not require any feedback control or constant adjustments because its fiber birefringence effects are automatically compensated.

2. Schematic diagram of modified BB84 protocol

Figure 1 shows the modified BB84 protocol used in our scheme. Charlie initially prepares a qubit in the state $(|0\rangle + |1\rangle)/\sqrt{2}$ and sends it sequentially from Alice to Bob over quantum channels. Finally, the qubit is returned and is detected by Charlie in the basis $(|0\rangle \pm |1\rangle)/\sqrt{2}$. Both users act on the qubit with a phase operator $\hat{U}(\varphi_j)$, applying a randomly chosen $\varphi_j \in (0, \pi/2, \pi, 3\pi/2)$:

$$\hat{U}(\varphi_j) = \left\{ |0\rangle \to |0\rangle, |1\rangle \to \mathrm{e}^{\mathrm{i}\varphi_j} |1\rangle \right\}. \tag{1}$$

After it passes all the users, its state is

$$|X_N\rangle = \left(|0\rangle + \mathrm{e}^{\mathrm{i}(\varphi_\mathrm{A}+\varphi_\mathrm{B}+\varphi_\mathrm{C})} |1\rangle \right) / \sqrt{2}. \tag{2}$$

*Project supported by the National Natural Science Foundation of China (Grant No. 61178010), the Fundamental Research Funds for the Central Universities (Grant No. bupt 2014TS01), the Fund of the State Key Laboratory of Information Photonics and Optical Communications (Grant No. 201318) (Beijing University of Posts and Telecommunications), and the National Program for Basic Research of China (Grant No. 2010CB923202).

†Corresponding author. E-mail: hqma@bupt.edu.cn

© 2014 Chinese Physical Society and IOP Publishing Ltd

To distribute the key, the modulation phase φ_j is divided into two classes: class X corresponds to the choice of $\varphi_j \in (0,\pi)$, and class Y corresponds to $\varphi_j \in (\pi/2, 3\pi/2)$. Charlie's phase choice is 0 or $\pi/2$ as a measurement is performed. The probability of detecting the state $(|0\rangle \pm |1\rangle)/\sqrt{2}$ is

$$p = \frac{1}{2}[1 \pm \cos(\varphi_A + \varphi_B + \varphi_C)]. \quad (3)$$

The probability of detection for different phase values of $\varphi_A, \varphi_B, \varphi_C$ are shown in Table 1. Finally, Alice and Bob publish their phase classes on a public channel but keep their particular choice of φ_j secret. However, Charlie shares not only the phase classes but also the measurement results with Alice and Bob on the public channel. According to the shared class information, Alice and Bob can determine which run leads to a deterministic measurement result, i.e., when $p_- = 1$ or $p_+ = 1$. In these runs, Alice (Bob) can infer Bob's (Alice's) choice of φ_B (φ_A). From Table 1, these runs are half of the total runs. Furthermore, although Charlie's secret, including the phases and detection results, is shared with all the users on a public channel, the key between Alice and Bob is not leaked, so our scheme can defend against all potential attacks depending on the imperfection of a detector. The security of the presented protocol against a general eavesdropping attack follows from the proven security of the well-known BB84 protocol.[22,23] Each communication step between two successive parties can be regarded as a BB84 protocol using two orthogonal bases.

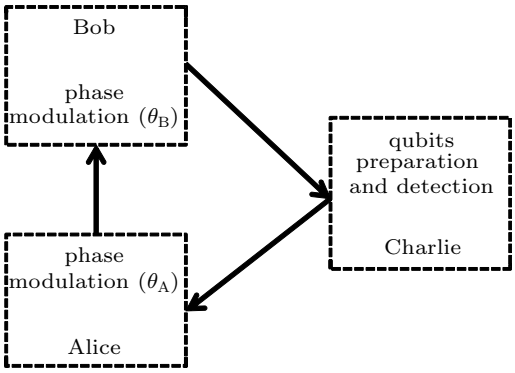


Fig. 1. Schematic diagram of modified BB84 protocol.

Table 1. Detection probabilities for different phase values of φ_A, φ_B, and φ_C.

φ_C	0								$\pi/2$							
φ_A	0				$\pi/2$				π				$3\pi/2$			
φ_B	0	$\pi/2$	π	$3\pi/2$	0	$\pi/2$	π	$3\pi/2$	0	$\pi/2$	π	$3\pi/2$	0	$\pi/2$	π	$3\pi/2$
D1/%	100	50	50	0	50	0	50	100	50	0	50	100	0	50	100	50
D2/%	0	50	50	100	50	100	50	0	50	100	50	0	100	50	0	50

3. Schematic diagram of the network setup

Figure 2 shows the proposed network setup in our scheme with five users, which can be divided into two main parties: the sender/detector Charlie and the two users Alice and Bob who need to share the key. Charlie's station contains a pulsed 1550-nm laser diode, LD; an attenuator, Att; a circulator, Cir; a phase-sensitive modulator, PM_C; two single-photon detectors, D1 and D2; a 50/50 coupler, C; and two polarizing beamsplitters, PBS_1 and PBS_2. A 2×4 optical switch, SW, is connected to the other parties by adjusting an optical connection between two optical common ports, P1 and P2, and one of four output lines. All Charlie's components are polarization maintaining and aligned to the "horizontal" axis. Other users connect to Charlie via a quantum channel and have identical components, including an attenuator and a phase-sensitive modulator terminated by a Faraday mirror. These components are widely used in plug & play quantum key distribution systems and fully compensate for link birefringence.[24] To detect Trojan horse attacks, a 99/1 coupler, which is not shown in Fig. 2, is placed between the quantum channel, QC, and the phase modulator, monitoring the input light by a single detector.[25]

For convenient description, we assume that SW's common port P1 is connect to Alice's output and P2 is connected to Bob's output. The pulsed laser LD emits horizontally polarized pulses at a repetition rate of 2 MHz. After passing through the circulator Cir and the 50/50 coupler C, the pulses are divided along two paths and transmitted through the two polarizing beamsplitters, PBS_1 and PBS_2, and the optical switch SW to Alice and Bob, respectively. The upper pulse, denoted by L1 in Fig. 2, passes through the quantum channel QC_1 to Alice. The pulse is modulated to phase φ_A by the phase modulator PM_A and reflected by the Faraday mirror FM_1 with a polarization rotation of 90°. Attenuated by the attenuator A_1 to the level of a single photon, the pulse returns to Charlie and is reflected by PBS_1 and PBS_2 to reach Bob. Bob has the same setup as Alice and also modulates the phase of the pulse, denoted as φ_B; the pulse is reflected by FM_2 with a polarization rotation of 90° so that it can be transmitted over PBS_1. After Charlie modulates the phase to φ_C by the modulator PM_C, the pulse arrives at the lower arm of coupler C. The lower pulse, denoted by L_2 in Fig. 2, is transmitted over the opposite path, so it arrives at the same time as the upper pulse L_1; however, none of the users modulate its phase when it passes through PM_C, PM_B, or PM_A. Thus, interference occurs at C; a photon is detected at D1 when $\varphi_A + \varphi_B + \varphi_C = 0$ or 2π, and at D2 if $(\varphi_A + \varphi_B + \varphi_C) = \pi$ in the valid run of the mentioned protocol. The detection probabilities of D1 and D2 for different

phase values chosen by Alice, Bob, and Charlie are illustrated in Table 1. As shown in Fig. 2, every user is similar in the network scheme. When they want to distribute keys to each other, e.g., Alice to Elise or Bob to David, they need only to adjust SW's common ports to the corresponding output for the appropriate user, as mentioned above. This setup is easy to be expanded by replacing the 2×4 switch with a $2 \times N$ switch, which is also a commercial device.

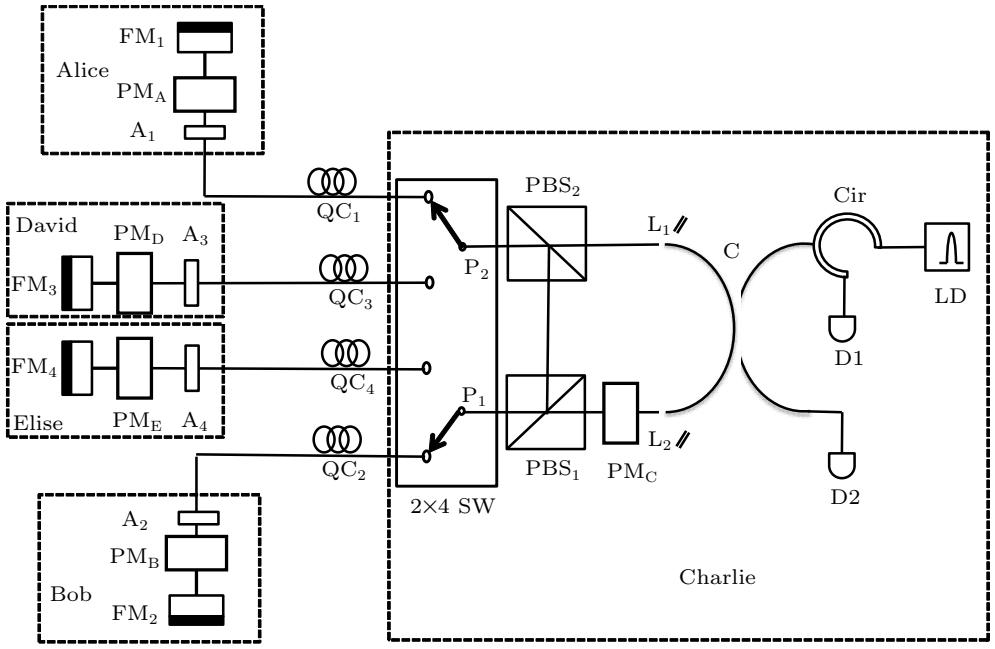


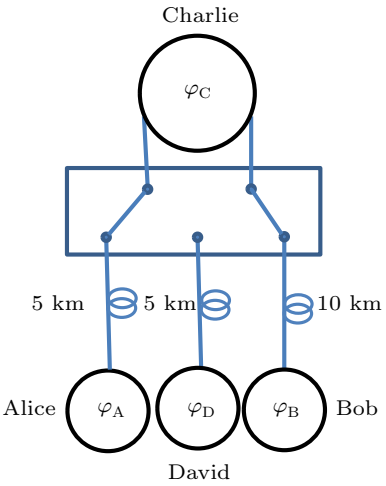
Fig. 2. Schematic diagram of network setup with five users. LD: laser diode; A_1, A_2, A_3, A_4: attenuators; Cir: circulators; PM_A, PM_B, PM_C, PM_D: phase-sensitive modulators; FM_1, FM_2, FM_3, FM_4: Faraday mirrors; D1, D2: single-photon detectors; C: a 50/50 coupler; PBS_1, PBS_2: polarizing beam splitter; 2×4 SW: optical switch; QC_1, QC_2, QC_3, QC_4: quantum channels.

4. Experimental results with the setup

Experiments were performed to test the stability and feasibility of the proposed scheme. A 1550-nm laser (id300, id Quantique, Switzerland) at 2 MHz was applied and was attenuated by A_1 to a very low level that can efficiently reduce the Rayleigh backscattering coming from the quantum channel. The average loss of commercial single-mode fibers is 0.25 dB/km. The insertion of the phase modulator (44, Institute of China Electronics Technology Group Corporation) and the PBS (General Photonics Corporation, USA) contributes to an increase in the attenuation of 3.5 dB and 0.3 dB, respectively. The losses range from 1.5 dB to 1.8 dB when the common ports of the switch (Sercalo, Switzerland) are connected to different parties. When interference occurs, two single-photon detectors (id201, id Quantique, Switzerland) are used to detect the single photons; their dark count rate is 4×10^{-6}, with a gate width of 2.5 ns and an efficiency of 10%. Homemade electronic systems are used to synchronize all the optical setups and drive modulators. We did not consider a photon number splitting attack because, as we know, it is currently technologically unfeasible and can be defeated by the decoy state method.[26–28] There is no additional technological difficulty for the decoy state method, in which the optimized pulse intensity reaches 0.5 photons/pulse, which is higher than our choice of 0.1 photons/pulse and 0.3 photons/pulse. Furthermore, we cannot claim the security of the scheme against a number of specific attacks, like, for instance, the Trojan-horse. However, the fact is that the Trojan-horse attack is a serious threat for all the known quantum key distribution scheme.[29]

The raw rate in the protocol is the product of the pulse rate f, the mean number of photons per pulse μ, the probability t_{link} of a photon from Alice arriving at Charlie, and the probability η of the photon being detected; it is defined as $R_{\text{raw}} = qf\mu t_{\text{link}}\eta$. The factor q is 0.5 in our setup because the measurement bases are compatible in only 50% of the measurement cases. The quantum bit error rates (QBER) for the scheme can be written as $\text{QBER} = \text{QBER}_{\text{opt}} + \text{QBER}_{\text{det}} = p_{\text{opt}} + p_{\text{nosie}}/\mu t_{\text{link}}\eta$, where p_{opt} is the probability of a photon going to the wrong detector, and p_{nosie} is the probability of getting a noise count per gating pulse window. For phase-coding setups, QBER_{opt} and the interference visibility are related as $(1-V)/2$.[30]

Figure 3 shows the experimental results. We achieved a 10-km transmission distance between Alice and David at $\mu = 0.1$ with a visibility of $V = 97.1\%$ and QBER $= 4.4\%$ and at $\mu = 0.2$ with a visibility of $V = 96.9\%$ and QBER $= 2.9\%$. The achieved raw transmission rates were 275 Hz for $\mu = 0.1$ and 590 Hz for $\mu = 0.2$. The achieved transmission distance between Alice and Bob was 15 km at $\mu = 0.1$ with $V = 97.5\%$ and QBER $= 5.2\%$ and at $\mu = 0.2$ with $V = 97.1\%$ and QBER $= 3.0\%$. The achieved raw transmission rates were 204 Hz for $\mu = 0.1$ and 450 Hz for $\mu = 0.2$. The visibility in Fig. 3 can be maintained perpetually without any adjustment to the system for each test.



(a) Alice−Charlie−David

u	0.1	0.2
Visibility/%	97.1	96.9
QBER/%	4.4	2.9
Raw rate/Hz	275	590

(b) Alice−Charlie−Bob

u	0.1	0.2
Visibility/%	97.5	97.1
QBER/%	5.2	3.0
Raw rate/Hz	204	450

Fig. 3. Experimental results with the setup. (a) Measurement results between Alice and David over 10-km fiber. (b) Measurement results between Alice and Bob over 15-km fiber.

5. Conclusion

In summary, we proposed a new full quantum network scheme using a modified BB84 protocol. The security of the protocol follows from the proven security of the well-known BB84 protocol. Unlike other quantum network schemes, it allows quantum keys to be distributed between two arbitrary users with the help of an intermediary detecting user. Moreover, it has a good expansibility and prevents all potential attacks using loopholes in a detector, so it is more practical to apply. Because the fiber birefringence effects are automatically compensated, our scheme is distinctly stable in principle and experimentally. The simple components at every user make our scheme cheaper and easier for many applications. The experimental results demonstrate the stability and feasibility of this scheme. In view of its excellent security, easy expansibility, and simple implementation, we believe it to be a potential network scheme for practical application.

Acknowledgment

Yang Xiu-Qing is gratefully acknowledged for helpful conversations.

References

[1] Bennett C H, Brassard G, *et al.* 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, p. 175
[2] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *Journal of Cryptology D* **5** 3
[3] Buttler W T, Hughes R J, Kwiat P G, Lamoreaux S K, Luther G G, Morgan G L, Nordholt J E, Peterson C G and Simmons C M 1998 *Phys. Rev. Lett.* **81** 3283
[4] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41
[5] Diamanti E, Takesue H, Langrock C, Fejer M M and Yamamoto Y 2006 *Opt. Express* **14** 13073
[6] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nat. Photon.* **1** 343
[7] Wei K J, Ma H Q and Wang L 2013 *Acta Phys. Sin.* **62** 104205 (in Chinese)
[8] Ma H Q, Wei K J and Yang J H 2013 *J. Opt. Soc. Am. B* **30** 2560
[9] Zhou F, Yong H L, Li D D, Yin J, Ren J G and Peng C Z 2014 *Acta Phys. Sin.* **63** 140303 (in Chinese)
[10] Kao S H and Hwang T 2013 *Chin. Phys. B* **22** 060308
[11] Townsend P D 1997 *Nature* **385** 47
[12] Nishioka T, Ishizuka H, Hasegawa T and Abe J 2002 *Photon. Technol. Lett.* **14** 576
[13] Patrick D. Kumavor P D, Beal A C, Yelin S, Donkor E and Wang B C 2005 *J. Lightwave Technol.* **23** 268
[14] Dai J L and Zhang W H 2009 *Chin. Phys. B* **18** 426
[15] Wei K J, Ma H Q and Yang J H 2013 *Opt. Express* **21** 16663
[16] Fröhlich B, Dynes J F, Marco Lucamarini M, Andrew W, Sharpe A W, Yuan Z L and Shields A J 2013 *Nature* **501** 69
[17] Chapuran T, Toliver P, Peters N, Jackel J, Goodman M, Runser R, McNown S, Dallmann N, Hughes R, McCabe K and others 2009 *New J. Phys.* **11** 105001
[18] Chen T Y, Wang J, Liang H, Liu W Y, Liu Y, Jiang X, Wang Y, Wan X, Cai W Q, Ju L, Chen L K, Wang L J, Cao Y, Chen K, Peng C Z, Chen Z B and Pan J W 2010 *Opt. Express* **18** 27217
[19] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[20] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[21] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 042333
[22] Huttner B and Ekert A K 1994 *J. Mod. Phys.* **41** 2455
[23] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[24] Stucki D, Legré M, Buntschu F, Clausen B, Felber N, Gisin N, Henzen L, Junod P, Litzistorf G, Monbaron P and others 2011 *New J. Phys.* **13** 123001
[25] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41
[26] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[27] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[28] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[29] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[30] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320