Experimental realization of quantum cryptography communication in free space

WANG Chuan[1], ZHANG Jingfu[1], WANG Pingxiao[1], DENG Fuguo[1], AI Qing[1] & LONG Guilu[1,2]

1. Department of Physics, Key Laboratory for Quantum Information and Measurements, Tsinghua University, Beijing 100084, China;
2. Center for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, China

Correspondence should be addressed to Zhang Jingfu (email: zhangjfu2000@yahoo.com) and Long Guilu (email: gllong@tsinghua.edu.cn)

Received November 22, 2004

Abstract Utilizing linear optical devices, the principle of B92 quantum key distribution (QKD) protocol is demonstrated in free space with a distance of transmission of 2.2 meters. The faint laser pulses with 650 nm wavelength are used as the single photon sources. The experimental results show that the eavesdropping behavior in the signal transmission can be detected. We also discuss the problems and solutions in using the quantum cryptography communication practically. It is pointed out that one of the approaches to increasing the distance of the quantum communication is to overcome the attenuation of the single photon in transmission. This could not be solved by the use of single photon source, and new quantum communication protocols are needed to solve these problems.

Keywords: quantum key distribution, free space, linear optics, faint pulses.

DOI: 10.1360/04yw0185

Quantum cryptography is a new secure communication protocol with the combination of quantum mechanics and information theory[1]. Its security depends on the laws of physics and has been proved strictly[2,3]. Quantum communication is the art of generating and transmitting the keys through a quantum channel between two parties, usually called Alice and Bob. Unlike the classical key distribution, the quantum keys are generated in the process of transmission instantaneously. The keys can be used to encrypt the messages with the one-time-pad scheme and sent through a classical channel or to be used as seed keys for other crypto-systems. The transmitted information is carried by the elementary quantum states, on which arbitrary eavesdropping can be detected according to the quantum mechanical principles. Unlike the classical key distribution, quantum key distribution is absolutely secure, because the quantum non-cloning theory prohibits the copying of any quantum state. Using the quantum information carrier, secure direct communication can also be realized[4−11]. In the quantum direct communication, messages can be transmitted directly through the quantum channel from one party to the other without the classical communication. At present, the experimental research on quantum cryptography is an important subject worldwide.

In 1984, Bennett and Brassard first proposed the BB84 quantum key distribution protocol[1]. The protocol utilizes two groups of states to encode and decode the messages. In 1992, Bennett proposed a quantum key distribution protocol (B92) using non-orthogonal states for coding messages[12]. B92 protocol is similar to the BB84 protocol, but it is simpler in experimental realization. It is an important quantum communication protocol using single particle quantum states. B92 protocol can be realized in the following steps:

(i) Alice randomly sends photons in 90 ° or 45 ° linearly polarized single photon states. The photon arrives at Bob's site through a quantum channel. The two polarized states represent the classical codes 1 and 0 respectively.

(ii) Bob randomly chooses one of the two 0 ° and 135 ° polarizing films to measure the photon and records the result each time. If Bob chooses the 0 ° film to measure the 90 ° polarized photon, the photon cannot be detected; if he chooses the 0 ° filter to measure the 45 ° polarized photon, the photon can be detected with 50% probability.

(iii) At the end of the transmission sessions, Bob informs Alice through the classical channel which photons have been measured. They use the codes represented by these polarizing photons as the key.

In the last 20 years, experimental quantum key distribution has progressed greatly. In 1995, Christophe et al. realized QKD in optical fibers over 30 km distance[13]. In 2003, Gobby et al. realized the 122 km quantum key distribution in special optical fibers[14]. In 2000, Buttler et al. implemented a daylight quantum key distribution in free space[15], the communication distance is 1.6 km. In 2002, Kurtsiefer et al. improved the distance in free space to about 23 km[16]. Quantum key distribution in free space is expected to be realized between the Earth and the low-orbit satellites.

There is rapid advancement in the field of quantum communication in China. In 1995, Liang et al. realized the quantum cryptography communication in free space[17], and in 2000, they realized the quantum key distribution in 1.1 km long optical fibers[18]. In 2003, Han et al. realized quantum communication with a distance up to 14.8 km in optical fibers[19]. Recently, Zhou et al. realized the quantum cryptography communication in 50 km optical fibers[20].

A photon can be transmitted in optical fibers with high efficiency, and its transmission direction can be changed easily. However, the optical fibers distort the photon polarizations, and this causes errors and losses in the transmission. The phase coding in the quantum cryptography can eliminate such difficulties. The distance of transmission in fibers is limited to 100 km using the present techniques, due to loss of photon in fibers. A photon can be transmitted over a longer distance in free space. Because the photon loss in atmosphere mainly happens below 2 km altitude, the photon can be transmitted over much more than 100 km in free space. The global quantum cryptography communication in future may be implemented by the combination of quantum communication in free space and in fibers, and it has a promising future of applications.

In this paper, we report the realization of the B92 quantum cryptography in free space. Faint laser pulses are used as the single photon sources. The data collection part, which is an important element in quantum cryptography, is purposedly designed using the standard electronic techniques. The data collection system can be easily generalized to adapt in other quantum communication schemes. We also demonstrate the influence caused by eavesdropping.

1 Experimental scheme and principle analysis

The scheme is shown in fig. 1. CA and CB are the control systems of Alice and Bob respectively, where 8255 chips are used as the kernels for data collection. CA generates three pulse sequences. The sequence generated by PA0 is used as the synchronization signal for quantum communication, and goes to the collecting systems of Bob directly. In the practical long distance quantum communication, an atomic clock may be used for time synchronization. The current technology of atomic clock is sufficiently precise for the need of the practical quantum communication. Lasers L1 and L2 are controlled to emit by the low level pulses generated by PC0 and PB0. A low level signal is generated by PB0 or PC0 in the middle of two synchronization signals. We define the emission of laser 1 represents the classical information 1, and that of laser 2 represents 0. Alice produces a string of binary number, which prepares a sequence of single photon pulses. Then she sends the sequence to Bob through a quantum channel. In this experiment, quantum signals sent from L1, L2 travel over 2.2 m distance in free space to D1, D2. In our experiment, the control signals are directly sent to Bob through classical channels. In the practical applications, however, only the synchronization signals are sent to Bob. Two 650 nm semiconductor light-emitting diodes are used to provide light sources. When Bob receives the synchronization signals, he starts to read out and save the data from PB. Then PB is reset to 0 for recording the next synchronization signal. It is obvious that the first number in PB is useless, because it is the data stored before the experiment. We arrange the bits of PB as follows. The signals from PC0, which is used to control L1, enter Bob’s PB0, and the signals from PB0, which is used to control L2, enter Bob’s PB1. The signals from D1 enter PB2, and the signals from D2 enter PB3. If L1 and L2 do not emit light, then all bits in PB are 0. When L1 emits one photon, and D1 detects the signal, PB=0101, where the four bits, from right to left, correspond to PB0—PB3, respectively. For example, in the above string, the second bit is 1, and the zeroth bit is 1, so that PB=8×0+4×1+2×0+1×1=5 (decimal number). When L1 emits an intensive pulse, both D1 and D2 can receive the signals. The decimal number readout from PB is

8×1+4×1+2×0+1×1=13. When L1 emits a single photon, for the ideal case, PB=5 or 1. Similarly, when L2 emits a single photon, PB=10 or 2. The values in detail of PB for various cases are shown in table 1.

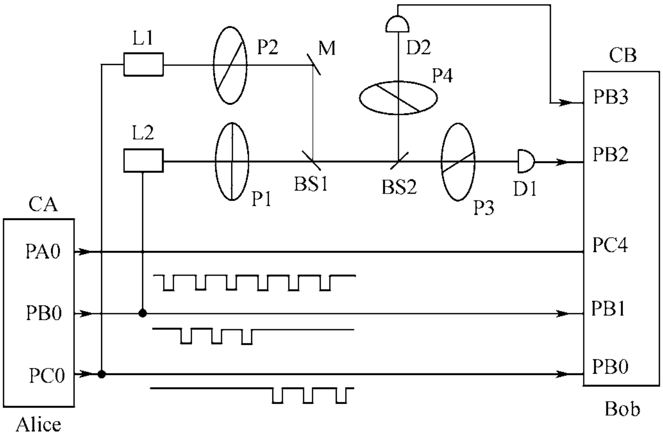

Fig. 1. Experimental scheme to realize B92 quantum key distribution probocol. CA and CB are the control systems of Alice and Bob respectively. Two 8255 chips are used to send and receive signals. PA0, PB0 and PC0 represent the lowest bit of ports A, B, and C, respectively. L1 and L2 denote laser 1 and laser 2. P1—4 are the polarizing films with the polarization directions along 90 °, 45 °, 0 °, 135 °. M denotes a mirror. BS1 and BS2 denote two 50∶50 beam splitters. D1 and D2 denote two single photon detectors. The pulse produced by PA0 is used as the synchronization signal which is sent to PC4 bit of CB through a classical channel. Laser 1 and laser 2 are controlled by the pulse sequences generated by PC0 and PB0, respectively. In the demonstration experiment, the control signals are directly sent to Bob through a classical channel. In the practical applications, however, only the synchronization signals are sent to Bob.

2 Experimental procedures and result

2.1 Preparation of pseudo-single photon

We prepare the pseudo-single photon sources by attenuating the light pulses to such a degree that each pulse contains less than one photon averagely. Such faint pulses can be used as the single photon source. The pseudo-single photon sources are prepared as the following. Let only L1 emit pulses, and remove P3 and P4. An attenuator is put in front of P2. The rate of attenuation is described by *k*. When a light pulse is intensive, it is split by BS2 into two beams. Both D1 and D2 can detect the photons, and PB=13. With the increase of *k*, the light pulse is weakened. When the pulse is weak enough, only D1 or D2 can detect the signal, and PB=5 or 9, noting that P3 and P4 have been removed. The experimental result is shown in fig. 2. With the decrease in the light intensity, the probability of detecting only a single signal becomes dominant, and we conclude that the pseudo-single photon source has been prepared. In our experiment, each pulse contains about 0.2 photon averagely. One pulse is sent every 30 μs. Averagely, the count caused by the dark count and background light is 200 per second. It can be estimated that the error caused by background light and dark count is less than 3%. Laser 2 can be initialized to pseudo-single photon source in the same way.

Table 1 Various values of PB and their implications

PB	PB3	PB2	PB1	PB0	Various cases
0	0	0	0	0	No emission, no reception, a trivial phenomenon.
1	0	0	0	1	L1 emits light, but no reception. Ideally, this case happens with 50% probability. Experimentally, we use the faint laser pulses to simulate the single photon. This case can be explained as L1 emits light, but it is absorbed by attenuators before it enters the channel, or it is lost due to the noisy channel, or is not detected by D1 and D2, or eavesdroppers exist.
2	0	0	1	0	L2 emits light, but no reception. Ideally, this case happens with 50% probability. Experimentally, we use the faint laser pulses to simulate the single photon. This case can be explained as L2 emits light, but it is absorbed by attenuators before it enters the channel, or it is lost due to the noisy channel, or is not detected by D1 and D2, or eavesdroppers exist.
3	0	0	1	1	L1, L2 both emit light, no reception. This case should not occur in experiments.
4	0	1	0	0	No emitting, but signals are detected by D1. This case is caused by the dark counts of D1. The case with a high probability shows the channel is abnormal, i.e. eavesdroppers generate fake signals, or the detector goes wrong.
5	0	1	0	1	L1 emits light, D1 receives the signal. This is the normal case.
6	0	1	1	0	L2 emits light, D1 receives signals. This is a wrong result caused by the imperfection of the polarization films, or the dark count of D1.
7	0	1	1	1	L1 and L2 both emit light, D1 detects the signal. This case should not occur in experiments.
8	1	0	0	0	No emitting, but signals are detected by D2. This case is caused by the dark counts of D2. The case with a high probability shows the channel is abnormal, i.e. eavesdroppers generate fake signals, or the detector goes wrong.
9	1	0	0	1	L1 emits light, D2 receives signals. This is a wrong result caused by the imperfection of the polarization films, or the dark count of D2.
10	1	0	1	0	L2 emits light, D2 receives the signal. This is the normal case.
11	1	0	1	1	L1 and L2 both emit light, D2 detects the signal. This case should not occur in experiments.
12	1	1	0	0	Neither L1 nor L2 emits light, both D1 and D2 receive signals. This is a wrong result caused by the intensive light in the channel, for instance by an eavesdropper, or the failure of the detectors. With very low probability, both detectors get the dark counts.
13	1	1	0	1	L1 emits light, both D1 and D2 receive signals. This case should not appear when faint pulses are used. This is a wrong result caused by the intensive light in the channel, or the failure of the detectors. With very low probability, both detectors get the dark counts.
14	1	1	1	0	L2 emits light, both D1 and D2 receive signals. This case should not appear when faint pulses are used. This is a wrong result caused by the intensive light in the channel, or the failure of the detectors. With very low probability, both detectors get the dark counts.
15	1	1	1	1	Both L1 and L2 emit light, both D1 and D2 receive signals. This case should not appear when faint pulses are used. It is a fault result.

2.2 Demonstration of B92 scheme

What concerns us most is the case that a photon arrives at BS2. When 0 state photon is sent from Alice, the photon cannot be detected by D1, because the polarization

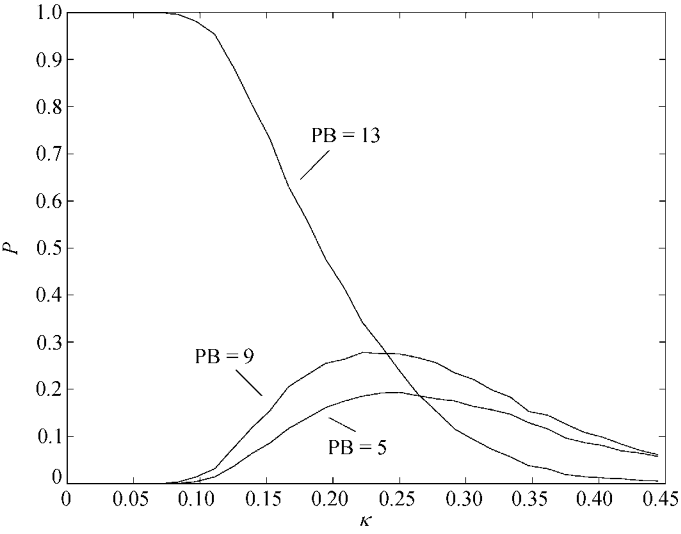

Fig. 2. The probability (P) of detecting photons versus the rate of attenuation (κ). Only L1 emits light pulse. PB=13 corresponds to the case that both D1 and D2 detect photons. PB=9 (or PB=5) corresponds to the case that D2 (or D1) detects a photon.

directions of P1 and P3 are orthogonal. However, it can be detected by D2 with 50% probability, because the separation angle between polarization directions of P1 and P4 is 45 °. Similarly, when 1 state photon is sent from Alice, photon cannot be detected by D2. It can be detected by D1 with 50% probability. When D1 or D2 detects a photon, PB = 5 or 10. In our experiment, 15000 pulses are sent from Alice totally, and we have repeated the experiment for 20 times. On average in each transmission, the number of PB= 5 is 1257±38, and the number of PB=10 is 1321±66. These cases are needed for the key transmission between Alice and Bob. After the start of the transmission, Alice begins to encode the classical random bits into photon states, and then send them to Bob. Bob records the synchronization pulses and measures the state of the encoded photon. Beamsplitter BS2 plays the role of a random choice of measuring-basis. He informs Alice of the positions of those photons in the sequence in which a photon has been detected, but he does not tell her what state he has detected through the public channel. In this way, they obtain a sequence of random binary numbers that they share in common. Alice uses the binary codes represented by these states as the raw key. Error correction and privacy amplifications are needed to process the raw keys to meet the request of security in practical application. We have developed the post processing programs. The probability of PB=9 is 0.0074, corresponding to the case that L1 emits light, D2 receives signals; PB=6 occurs with probability 0.0056, corresponding to the case that L2 emits light, D1 receives signals; PB=13 occurs with probability 0.0019, corresponding to the case that L1 emits light, both D1 and D2 receive; PB=14 occurs with probability 0.0012, corresponding to the case that L2 emits light, both D1 and D2 receive signals. These four cases should not appear in the ideal B92 scheme. The reasons that they appear are summarized in table 1. The probability of PB=1 is 0.407, and of PB=2 is 0.405. We do not care about these two cases in which no photon arrives at or is detected by the detectors. After all these useless cases, there are 2578 effective pulses in the 15000 pulses. The utilization ratio of pulses is 17.2%. The transmission bit rate can be increased by increasing the repetition rate of the driving pulses.

2.3 Detection of eavesdropping

Now we consider the influence caused by an eavesdropper who possesses a quantum device to produce arbitrary state. Eve's goal is to intercept a quantum state and then prepare the same state and resend it to Bob so that her eavesdropping action could evade detection. But quantum mechanical principles prevent her from doing this. Essentially, eavesdropping is a measurement for an unknown state. Thus one kind of Eve's action can be modelled by inserting a polarizing film with separation angle ϕ relative to P1. The experimental results are shown in fig. 3. The probability of PB=5 or PB=10, the normal key distribution cases, reduces greatly in the existence of an eavesdropper. While changing ϕ from 0 ° to 180 °, a complementary trend is presented in the probabilities of PB=10 and PB=5. Compared with the case without Eve, when the probability of PB=10 hardly changes near the position ϕ=0 °, or ϕ=180 °, for example, the probability of PB=5 decreases evidently, even to zero. Similarly, when the probability of PB=5 hardly changes, the probability of PB=10 decreases evidently. Considering the changes of PB=10 and PB=5 simultaneously, Bob can easily find out Eve. The additional polarizing film can cause the attenuation of signal. It is shown that such attenuation is less

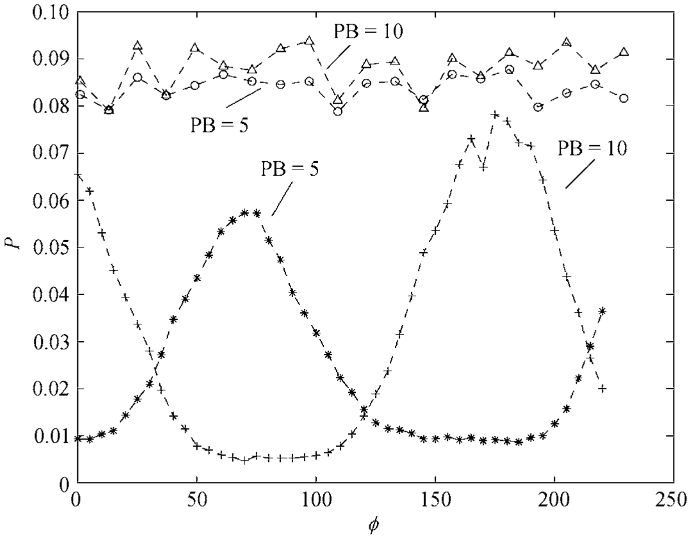

Fig. 3. The influence caused by Eve. A polarizing film with separation angle ϕ relative to P1. The curves marked by "*" and "+" represent the probabilities of PB=5 and PB=10 in the presence of an eavesdropper. Here we connect the points with dashed lines for visual guidance. The two curves marked by "△" and "○" represent the probabilities of PB=10 and PB=5 without eavesdropping.

than 20%, and in theory we assume that Eve has a perfect device and there is no attenuation. The low sections of the curves in fig. 3 show that the influence caused by Eve is much more than the attenuation. The experiment results show an agreement between theory and experiment.

3 Conclusion

In this experiment, we have demonstrated the principle of B92 quantum key distribution protocol in free space and the security in a low noisy channel. The polarized states of photons are utilized to encode the bits. We focus on the physics principle of B92 protocol. The quantum mechanical ideas are represented clearly and emphatically, and the experimental results are direct. Moreover, the device we use in our experiment are ordinary optical devices, usually with low specification, thus there is much room to improve the performance of the apparatus by using devices with higher specifications. In addition, the data collection methods used in the experiment can also be generalized for use in other quantum communication protocols. From this experiment, we can draw the following remarks.

1) The security of quantum cryptography is based on the principles of quantum mechanics. The principle demonstrated in this experiment is the same as those with longer distance. The differences mainly result from the qualities of the experimental devices and the element units, such as the polarizing films, lasers, and so on. Our experiment is suitable for studying the basic principles of quantum cryptography.

2) The loss of single photon in free space is the main obstacle for long distance quantum cryptography. In our experiment, we choose SPCM-AQR-250 single photon detecting modules of Perkin Elmer as the single photon detectors. The detecting efficiency for the light with 650 nm wavelength is more than 70%. The low efficiency of pseudo-single photon produced by the faint pulse can reduce the repetition rate of transmission, but it does not reduce the transmission distance. Hence there are two possible approaches to overcoming the problem. One is to find the appropriate optical windows for which light with specific wavelength attenuates with the smallest rate. This approach requires both experimental and theoretical efforts to study the decay mechanism for laser light. It could be possible to increase the transmission distance if the decay mechanism for single photon and an intensive laser pulse were different. Usually, a laser pulse attenuates exponentially with the increase of the distance, according to Lambert's law. One of the experiences that can be borrowed from classical communication is to increase the intensity of the laser pulse. This may lead to the insecurity of quantum cryptography because such a pulse contains many photons, and particle number split attack could be used to attack the security of such a cryptography. Hence novel protocols are required for long distance quantum communication. In such protocols, a tradeoff between the level of security and the distance has to be made. Some theoretical work has already been carried out[21−24].

3) The main reason of low bit rate in quantum cryptography is the low efficiency of single photon generation. Our experiment only uses two out of ten pulses in communication. An ideal single photon source will improve the bit rate greatly.

4) The advantage of quantum cryptography is its security. Any eavesdropper can immediately be detected by the two communication parties. Present protocols based on single photon source can ensure the security. However, the use of faint laser pulse as pseudo-single photon source limits the transmission distance. It is interesting to search for quantum protocols using intensive laser pulses with high security. As has been pointed out earlier, such a protocol will also increase the transmission distance, and lessen the high demand on detectors. It also has the advantage to combine quantum protocols with the present communication system.

In summary, quantum cryptography is feasible in theory, but the transmission distance is limited by the loss of photons in air in space. For the current techniques, the transmission distance might be lengthened by enhancing the intensity of laser pulses, and this could also improve the transmission bit rate and detection efficiency of the detectors.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant Nos. 10325521 and 60433050), China Postdoctroal Science Foundation; the National Foundation Research Program (Grant No. 001CB309308).

References

1. Bennett, C. H., Brassard, G., Quantum cryptography: public key distribution and coin tossing, in Proceedings of IEEE Interactional Conference on Computers, System and Signal Processing, Bangalore, India, New York: IEEE, 1984, 175—179.
2. Lo, H. K., Chau, H. F., Unconditional security of quantum key distribution over arbitrarily long distances, Science, 1999, 283(5410): 2050—2956. [DOI]
3. Biham, E., Boyer, M., Boykin, P. O. et al., in Proceedings of the 32th Annual Acm Symposium on Theory of Computing, New York: ACM Press, 2000, 715—716.
4. Beige, A., Englert, B. G., Kurtsiefer, C. et al., Secure communication with a public known key, Acta Phys. Pol. A, 2002, 357.
5. Boström, K., Felbinger, T., Deterministic secure direct communication using entanglement, Phys. Rev. Lett., 2002, 89(18): 187902-1—187902-4.
6. Deng, F. G., Long, G. L., Liu, X. S., Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block, Phys. Rev. A, 2003, 68(4): 042317-1—042317-6.
7. Deng, F. G., Long, G. L., Secure direct communication with a quantum one-time pad, Phys. Rev. A, 2004, 69(5): 052319-1—052319-4.
8. Yan, F. L., Zhang, X. Q., A scheme for secure direct communication using EPR pairs and teleportation, The European Physical Journal B, 2004, 41: 75—78.
9. Zhang, Z. J., Man, Z. X., Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations, e-print quant-ph/0403218.
10. Cai, Q. Y., Li, B. W., Deterministic secure communication without using entanglement, Chin. Phys. Lett., 2004, 21(4): 601. [DOI]
11. Cai, Q. Y., Li, B. W., Improving the capacity of the Boström-Felbinger protocol, Phys. Rev. A, 2004, 69(5): 054301-1—054301-3.
12. Bennett, C. H., Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett., 1992, 68(21): 3121—3124. [DOI]

13. Christophe, M., Townsend, P. D., Quantum key distribution over distances as long as 30 km, Opt. Lett., 1995, 20(16): 1695—1697.
14. Gobby, C., Yuan, Z. L., Shields, A. J., Quantum key distribution over 122 km of standard telecom fiber, App. Phys. Lett., 2004, 84(19): 3762—3764. [DOI]
15. Buttler, W. T., Hughes, R. J., Lamoreaux, S. K. et al., Daylight quantum key distribution over 1.6 km, Phys. Rev. Lett., 2000, 84(24): 5652—5655. [DOI]
16. Kurtsiefer, C., Zarda, P., Halder, M. et al., A step towards global key distribution, Nature, 2002, 419: 450. [DOI]
17. Shao, J., Wu, L. A., Quantum cryptography experiment with single photon polarization state, Quantum Optics, 1995, 1: 41—44.
18. Liang, C., Wu, L. A. Fu, D. H. et al., Quantum key distribution over 1.1 km in 850 nm optical fibers, Chinese Physics, 2001, 50(8): 1429—1433.
19. Gui, Y. Z., Han, Z. F., Mo, X. F. et al., Experimental quantum key distribution over 14.8 km in special optical fiber, Chinese Phys. Lett., 2003, 20(5): 608—610. [DOI]
20. Zhou, C. Y., Wu, G., Chen, X. L. et al., Quantum key distribution in 50-km optic fibers, Science in China, Ser. G, 2004, 47(2): 182—188. [Abstract] [PDF]
21. Silberhorn, C., Ralph, T. C., Lütkenhaus, N. et al., Continuous variable quantum cryptography: Beating the 3 dB loss limit, Phys. Rev. Lett., 2002, 89(16): 167901-1—167901-4.
22. Hirano, T., Yamanaka, H., Ashikaga, M. et al., Quantum cryptography using pulsed homodyne detection, Phys. Rev. A, 2003, 68(4): 042331-1—042331-7.
23. Grosshans, F., Van Assche, G., Wenger, J. et al., Quantum key distribution using Gaussian-modulated coherent states, Nature, 2003, 421: 238—240. [DOI]
24. Deng, F. G., Long, G. L., Bidirectional quantum key distribution protocol with practical faint laser pulses, Phys. Rev. A, 2004, 70(1): 012311-1—012311-7.