Vol 18 No 3, March 2009
1674-1056/2009/18(03)/0915-03

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Analysis of the differential-phase-shift-keying protocol in the quantum-key-distribution system*

Jiao Rong-Zhen(焦荣珍), Feng Chen-Xu(冯晨旭), and Ma Hai-Qiang(马海强)

Science School, Beijing University of Post and Telecommunication, Beijing 100876, *China*

(Received 4 August 2008; revised manuscript received 10 September 2008)

The analysis is based on the error rate and the secure communication rate as functions of distance for three quantum-key-distribution (QKD) protocols: the Bennett–Brassard 1984, the Bennett–Brassard–Mermin 1992, and the coherent differential-phase-shift keying (DPSK) protocols. We consider the secure communication rate of the DPSK protocol against an arbitrary individual attack, including the most commonly considered intercept-resend and photon-number splitting attacks, and concluded that the simple and efficient differential-phase-shift-keying protocol allows for more than 200 km of secure communication distance with high communication rates.

Keywords: differential-phase-shift keying protocol，communication rate, error rate
PACC: 0367, 4250

1. Introduction

Quantum key distribution (QKD) is a technique that allows two parties (usually called Alice and Bob) to generate a secret key despite the computational and technological power of an eavesdropper (Eve) who interferes with the signals. The most common QKD protocols are the Bennet–Brassard 1984 (BB84) protocol which uses two nonorthogonal bases as the information carriers,[1−3] and the entanglement-based Bennet–Brassard–Mermin 1992 (BBM92) protocol.[4] In this paper, we consider the differential-phase-shift-keying (DPSK) protocol, which Alice sends Bob a train of weak coherent pulses whose phases are randomly modulated by 0 or π. On the receiving side, Bob measures out each incoming signal by means of an interferometer whose path-length difference is set equal to the time difference between two consecutive pulses.[5−10] The security of the DPSK protocol stems from the fact that the information is encoded on the differential phase of two non-local pulses. We analysed in this paper the relation that the error rate and the secure communication rate as functions of distance for three QKD protocols, and discuss the security of DPSK protocol against any type of individual photon splitting attack.

2. Theory and formulas

In the BB84 protocol, Alice sends Bob single photons randomly modulated in two nonorthogonal bases. Bob measures the polarization states of the single photons in a randomly chosen polarization basis. The secure communication rate of this protocol against an arbitrary individual attack is given by the following expression:

$$R_{\mathrm{BB84}} = \frac{1}{2}vp_{\mathrm{click}}\{\tau(e,\beta) + f(e)[e\mathrm{lb}e + (1-e)\mathrm{lb}(1-e)]\}.$$

In the above equation, the factor 1/2 is the sifting parameter, v is the repetition rate of the transmission, $\tau(e,\beta)$ is the shrinking factor and the function $f(e)$ depends on the error-correction algorithm. The formulas about $\tau(e,\beta)$ and $f(e)$ have been given in Ref.[7]. The probability at which Bob detects a photon is

$$p_{\mathrm{click}} = p_{\mathrm{signal}} + p_{\mathrm{dark}},$$
$$p_{\mathrm{signal}} = \mu\eta 10^{-(\alpha L + L_{\mathrm{r}})/10},$$
$$p_{\mathrm{dark}} = 4d,$$

where μ is the average number of photons per-pulse, η the quantum efficiency of the detector, α the loss coefficient of the optical fibre in dB/km, L the distance in km, L_{r} the loss of the receiver unit in dB, and d the

*Project supported by the Natural Science Foundation of Beijing, China (Grant No XK100130837).
†E-mail: jrz218@163.com

dark counts per measurement time window of the system. The error rate is given by $e = \frac{\frac{1}{2}p_{\rm dark} + bp_{\rm signal}}{p_{\rm click}}$, where b is the baseline system error rate.

The BBM92 protocol is the two–photon variant of BB84. The equation for the secure communication rate against any individual attack is given by the following expression

$$R_{\rm BBM92} = \frac{1}{2}\upsilon p_{\rm coin}\{\tau(e) + f(e)[e{\rm lb}e + (1-e){\rm lb}(1-e)]\}.$$

The shrinking factor $\tau(e)$ becomes

$$\tau(e) = -{\rm lb}\left(\frac{1}{2} + 2e - 2e^2\right).$$

The probability of a coincidence between Alice and Bob is

$$p_{\rm coin} = p_{\rm true} + p_{\rm false}.$$

For deterministic entangled-photon source

$$p_{\rm true} = \eta^2 10^{-(\alpha L + 2L_{\rm r})/10},$$
$$p_{\rm false} = 8d\eta 10^{-(\alpha L + 2L_{\rm r})/20} + 16d^2.$$

The error rate is given by

$$e = \frac{\frac{1}{2}p_{\rm false} + bp_{\rm true}}{p_{\rm coin}}.$$

Instead of using two nonorthogonal bases as in BB84 and BBM92, the DPSK protocol uses fully nonorthogonal four states. A photon split into three pulses is sent from Alice to Bob, in which the phases of two sequential probability amplitudes are randomly modulated. Bob extracts the bit information by measuring the differential phase. In the DPSK protocol, all pulses are highly attenuated and randomly phase modulated by $\{0,\pi\}$. Our analysis takes into account a hybrid attack which consists of the beam-splitter and intercept-resend attacks. The equation for the secure communication rate against any type of individual photon splitting attack is given by the following expression:

$$R_{\rm DPSK} = \upsilon p_{\rm click}\{\tau(e,\gamma) + f(e)[e{\rm lb}e + (1-e){\rm lb}(1-e)]\},$$
$$p_{\rm click} = \mu\eta 10^{-(\alpha L + L_{\rm r})/10} + 2d,$$
$$\tau(e,\gamma) = \gamma - \frac{e}{N\left(1 - \frac{1}{2N}\right)}.$$

When Eve is equipped with a quantum memory,

$$\gamma = 1 - 2\mu + 2p_{\rm signal}.$$

When Eve is not equipped with a quantum memory,

$$\gamma = 1 - \frac{\mu}{N} + \frac{p_{\rm signal}}{N}.$$

The expression of error rate is the same as that of BB84. All the parameters in the above equations are defined as in the previous section.

3. Conclusion

We have compared the error rate and the secure communication rate as functions of distance for three QKD protocols in Figs.1 and 2 respectively. In the cases of the BB84, BBM92 and DPSK protocols, we suppose the BB84 protocol employing a Poisson single-photon source, the BBM92 protocol employing a deterministic entangled-photon source, and the DPSK protocol employing time delay parameter ($N = 1$) when Eve is equipped with an ideal quantum memory. At the same time, as shown in Fig.3, the secure communication rate as a function of distance for the DPSK protocol employing time delay parameters $N = 1$ or $N = 10$ when Eve is equipped with a quantum memory, and $N = 1$, 10, or 100 when she is not. Some parameters are fixed in all simulations: the channel loss is set to 0.2 dB/km at 1.55 μm, the baseline system error rate is set to ($b = 0.01$), and in addition to the fibre losses we assume an extra loss of $L_{\rm r} = 1$ dB at the receiver site.

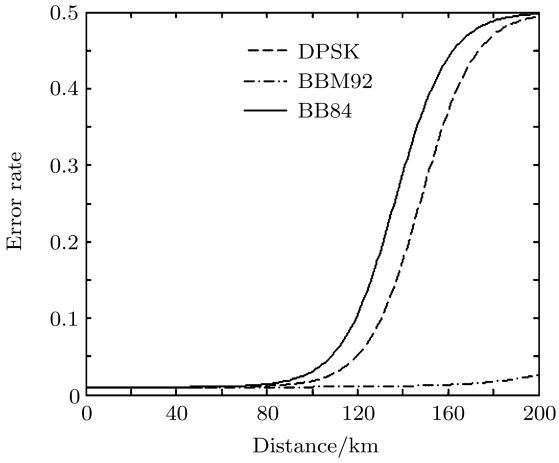


Fig.1. The error rate as a function of distance for the BB84, BBM92, and DPSK protocols.

As shown in Fig.2, the DPSK protocol feature characteristics very similar to BB84 with a single-photon source. We observe in Fig.3 that introducing a time delay parameter N does not have a significant

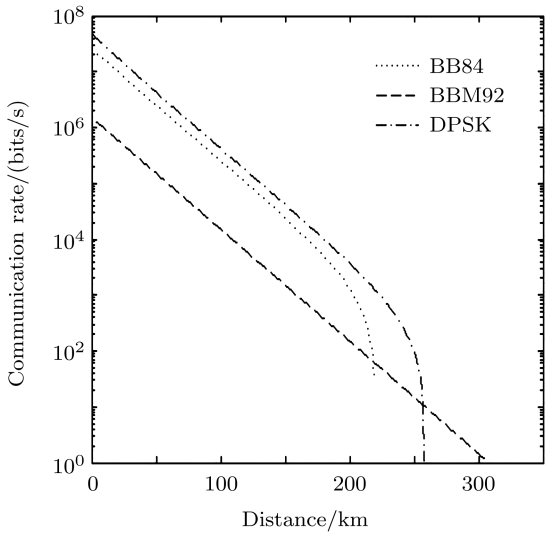


Fig.2. Comparison of the performance of QKD systems implementing the BB84, BBM92, and DPSK protocols.

effect on the performance of the system. However, when a realistic scenario is assumed, Eve does not possess a quantum memory with an infinitely long coherence time. We observe a significant effect on the performance of the system. In this case, introducing a time delay parameter N greater than 1 enhances both the secure communication rate and the communication distance of the system considerably. Nevertheless, the advantage becomes comparatively smaller as N increases to values greater than 10. The result shows that the DPSK protocol is a very practical and appealing alternative for a long-distance QKD system, with the potential of 1 kHz secure key-generation rate over distances longer than 200 km.

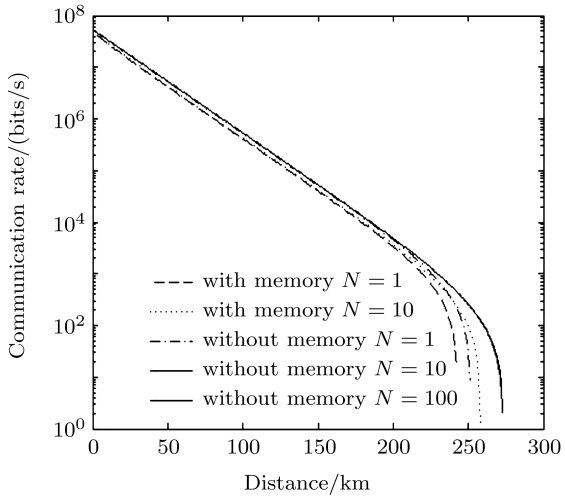


Fig.3. Secure communication rate as a function of distance for the DPSK protocol.

References

[1] Ma H Q, Li Y L, Zhao H and Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese)

[2] Mao E L, Mo X F, Gui Y Z, Han Z F and Guo G C 2004 *Acta Phys. Sin.* **53** 2126 (in Chinese)

[3] Bennet C H and Brassard G 1984 *Proc. IEEE. Int. Conf. Computers, Systems, and Signal Processing* (Bangalore, New York, IEEE)

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

[5] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902

[6] Inoue K, Waks E and Yamamoto Y 2003 *Phys. Rev.* A **68** 022317

[7] Diamanti E, Takesue H, Honjo T, Inoue K and Yamamoto Y 2005 *Phys. Rev.* A **72** 052311

[8] Curty M, Tamaki K and Moroder T 2008 *Phys. Rev.* A **77** 052321

[9] Jiao R Z and Feng C X 2008 *Acta Phys. Sin.* **57** 685 (in Chinese)

[10] Liu Y M, Yu Z Y and Ren x M 2008 *Chin. Phys.* B **17** 3471