World Applied Sciences Journal 21 (Mathematical Applications in Engineering): 29-34, 2013
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2013.21.mae.9999

Quantum Key Distribution in Real Life

[1]Sellami Ali, [2]Abdallah Hassen Ahmed,
[2]Mohamed Hadi Habaebi and [1]Sazzad Hossien Chowdhury

[1]Department of Science in Engineering,
[2]Department of Electrical and Computer Engineering,
Faculty of Engineering, International Islamic University Malaysia

Abstract: The quantum key distribution (QKD) technique establishes secret keys shared between two communicating parties. Theoretically, unconditional security provided by QKD is guaranteed by the fundamental laws of quantum physics. in the real life, it is still possible to obtain unconditionally secure QKD, even with (phase randomized) attenuated laser pulses, as theoretically demonstrated by Gottesman-Lo-L¨utkenhaus-Preskill (GLLP). However, one must pay a steep price by placing severe limits on the distance and the key generation rate. These problems were solved using the decoy state method introduced by Hwang. In this paper, we have proposed a method to estimate parameters of the decoy state method based on two decoy state protocol for both BB84 and SARG04. The vacuum and weak decoy state protocol has been introduced as a special case of two decoy states protocol. This method has given different lower bound of the fraction of single-photon counts ($y1$), the fraction of two-photon counts ($y2$), the upper bound QBER of single-photon pulses ($e1$), the upper bound QBER of two-photon pulses ($e2$) and the lower bound of key generation rate for both BB84 and SARG04. The fiber based QKD systems also have been simulated using the proposed method for BB84 and SARG04. The numerical simulation has shown that the fiber based QKD systems using the proposed method for BB84 are able to achieve both a higher secret key rate and greater secure distance than that of SARG04.

Key words: Quantum cryptography · Quantum key distribution · Decoy state protocol and optical communications

INTRODUCTION

The quantum key distribution (QKD) technique establishes secret keys shared between two communicating parties, conventionally referred to as (Alice and Bob) to exchange information securely in the presence of an eavesdropper (Eve) [1, 2]. Theoretically, unconditional security provided by QKD is guaranteed by the fundamental laws of quantum physics [3].

In spite of the imperfections of practical systems, the QKD has been demonstrated successfully over a distance of 175 km of optical fiber. Imperfect sources, noisy channels and inefficient detectors are negative factors that affect security [4]. In most of these applications, the photon source is a coherent light, which is a superposition of Fock states weighted by Poisson distribution. In this respect, there will be a nonzero probability of getting a state with more than one photon, i.e. multi photon states. Thus Eve assumed with infinite resources, may suppress these states by capturing one photon. Precisely, Eve may block the single photon state, split the multi photon state and improve the transmission efficiency using her superior technology to compensate the loss of the single photon. Therefore, security proofs must take into account the possibility of subtle eavesdropping attacks, including the photon number splitting (PNS) [5].

A hallmark of these subtle attacks is that they introduce a photon-number dependent attenuation. Fortunately, it is still possible to get unconditionally

Corresponding Author: Sellami Ali, Department of Science, Faculty of Engineering, International Islamic University Malaysia.

secure QKD even with phase randomized attenuated laser pulses, which has been theoretically demonstrated [6]. However, there are still some limitations regarding distance and key generation rates. These problems were solved using the decoy state method introduced by Hwang, 2003 [7]. The method achieves unconditional security as well as improves the performance of the QKD dramatically. It estimates the upper bound of multi-photon counting rate faithfully through the decoy–pulses regardless of the type attack. The basic idea of the decoy state QKD is: in addition to the signal state with the specific average photon number, one introduces some decoy states with some other average photon numbers and blends signal states with decoy states randomly in Alice's sides.

Many methods have been developed to improve the performance of the decoy states QKD, including more decoy states [8], nonorthogonal decoy-state method [9], photon number resolving method [10], herald single photon source method [11, 12], modified coherent state source method [13], the intensity fluctuations of the laser pulses [14] and [15]. Some prototypes of decoy state QKD have been already implemented [16-27].

In this paper, we will present a method to estimate parameters of the decoy state method based on one decoy state protocol for both BB84 and SARG04. This method will give different lower bound of the fraction of single-photon counts ($y1$), the fraction of two-photon counts ($y2$), the upper bound QBER of single-photon pulses ($e1$), the upper bound QBER of two-photon pulses ($e2$) and the lower bound of key generation rate for both BB84 and SARG04. We will also simulate the fiber based QKD systems using the proposed method for BB84 and SARG04.

MATERIAL AND METHOD

The Estimation Method of Decoy State Parameters: In this section, we propose a method to evaluate the lower bound of the key generation rate for both BB84 and SARG04 by the estimation of the lower bound of fraction of one photon count y_1, two photon counts y_2, upper bound of quantum bit-error rate (QBER) of one-photon e_1 and upper bound of quantum bit-error rate (QBER) of two-photon e_2. It is assumed that Alice can prepare and emit a weak coherent state $\left|\sqrt{\mu}e^{i\theta}\right\rangle$. Assuming the phase θ of each signal is randomized, the probability distribution for the number of photons of the signal state follows a Poisson distribution with some parameter μ (the intensity of signal states) which is given by $p_i = e^{-\mu}\frac{\mu^i}{i!}$, Alice's pulse will contain i-photon. Therefore, it has assumed that any Poissonian mixture of the photon number states can be prepared by Alice. In addition, Alice can vary the intensity for each individual pulse.

Assuming Alice and Bob choose the signal and decoy states with expected photon numbers μ,ν_1,ν_2 they will get the following gains and QBER's for signal state and two-decoy states which are given by [5].

$$
\begin{aligned}
&Q_{\mu,BB84} = y_0 + 1 - e^{-\eta\mu}\\
&E_{\mu,BB84} = \frac{1}{Q_{\mu,BB84}}\left(e_0 y_0 + e_{\det}(1-e^{-\eta\mu})\right)\\
&Q_{\nu,BB84} = y_0 + 1 - e^{-\eta\nu}\\
&E_{\nu,BB84} = \frac{1}{Q_{\nu,BB84}}\left(e_0 y_0 + e_{\det}(1-e^{-\eta\nu})\right)\\
&Q_{\mu,SARG04} = \frac{1}{4}y_0 e^{-\eta\mu} + \left(\frac{e_{\det ector}}{2} + \frac{1}{4}\right)(1-e^{-\eta\mu}),\\
&E_{\mu,SARG04} = \left[\frac{1}{4}y_0 e^{-\eta\mu} + \frac{e_{\det ector}}{2}(1-e^{-\eta\mu})\right]/Q_{\mu,SARG04}.\\
&Q_{\nu,SARG04} = \frac{1}{4}y_0 e^{-\eta\nu} + \left(\frac{e_{\det ector}}{2} + \frac{1}{4}\right)(1-e^{-\eta\nu}),\\
&E_{\nu,SARG04} = \left[\frac{1}{4}y_0 e^{-\eta\nu} + \frac{e_{\det ector}}{2}(1-e^{-\eta\nu})\right]/Q_{\mu,SARG04}.
\end{aligned}
\tag{1}
$$

The transmittance of the i-photon state with respect to a threshold detector is

$$\eta_i = 1 - (1-\eta)^i \tag{2}$$

For $i = 0,1,2,...$

As in Eq (7) [5]. Here we assume that y_0 (typically 10^{-5}) and η (typically 10^{-3}) are small. The yield of an i-photon state is given by

$$y_i = y_0 + \eta_i - y_0\eta_i \simeq y_0 + \eta_i \tag{3}$$

The error rate of the *i*-photon state is given by

$$e_i = \frac{e_0 y_0 + e_{\det}\eta_i}{y_i} \tag{4}$$

where y_i is the yield of an *i*-photon state which comes from two parts, background (y_0) and true signal. η is the overall transmittance which is given by $\eta = \eta_{Bob} 10^{-\frac{\alpha l}{10}}$, where α (dB/km) is the loss coefficient, l is the length of the fiber and η_{Bob} denotes for the transmittance in Bob's side. e_{det} is the probability that a photon hit the erroneous detector, $e_{\det}$ characterize the alignment and stability of the optical system. The error rate of background is $e_0 = \frac{1}{2}$.

Case 1 Two Decoy States Protocol: Suppose Alice and Bob choose signal state and two decoy state with expected photon numbers μ, v_1 and v_2 which satisfy

$0 \le v_1 < \mu < v_2 \le 1$, $\mu + v_1 < v_2$ and

$$\mu^n - v_1^n \ge \mu^m - v_1^m$$

Whenever $0<v_1 + \mu<1$ and $n \le m$. (5)

By using the inequality (8) in [7] and (5) we get

$$\frac{\sum_{i=2}^{\infty} y_i \left(P_i(\mu) - P_i(v_1)\right)}{\sum_{i=2}^{\infty} P_i(v_2) y_i} \le \frac{\left(P_2(\mu) - P_2(v_1)\right)}{P_2(v_2)} \tag{6}$$

Multiply both sides by $v_2^2 \sum_{i=2}^{\infty} y_i \frac{v_2^i}{i!}$ we get

$$v_2^2 \left(\sum_{i=2}^{\infty} y_i \frac{\mu^i - v_1^i}{i!} \right) \le \left(\mu^2 - v_1^2\right) \sum_{i=2}^{\infty} y_i \frac{v_2^i}{i!} \tag{7}$$

According to Eq (1) we get

$$v_2^2 \left(Q_\mu e^{\mu} - Q_{v_1} e^{v_1} - (\mu - v_1) y_1\right) \le \left(\mu^2 - v_1^2\right)\left(Q_{v_2} e^{v_2} - y_0 - v_2 y_1\right) \tag{8}$$

By solving inequality (8), the lower bound of y_1 is given by

$$y_1^{L,v_1,v_2} = \frac{1}{\left(v_2^2(\mu - v_1) - \left(\mu^2 - v_1^2\right)v_2\right)} \left[v_2^2 \left(Q_\mu e^{\mu} - Q_{v_1} e^{v_1}\right) - \left(\mu^2 - v_1^2\right) Q_{v_2} e^{v_2} + \left(\mu^2 - v_1^2\right) y_0 \right] \tag{9}$$

According to Eq. (1), then the lower bound of the gain of single photon state is given by

$$Q_1^{L,v_1,v_2} = \frac{\mu e^{-\mu}}{\left(v_2^2(\mu - v_1) - \left(\mu^2 - v_1^2\right)v_2\right)} \left[v_2^2 \left(Q_\mu e^{\mu} - Q_{v_1} e^{v_1}\right) - \left(\mu^2 - v_1^2\right) Q_{v_2} e^{v_2} + \left(\mu^2 - v_1^2\right) y_0 \right] \tag{10}$$

According to Eqs (1) and (5) we get

$$\sum_{i=2}^{\infty} e_i y_i \frac{v_2^i}{i!} \ge \sum_{i=2}^{\infty} e_i y_i \frac{\mu^i - v_1^i}{i!} \tag{11}$$

Then,

$$E_{v_2} Q_{v_2} e^{v_2} - e_0 y_0 - v_2 e_1 y_1 \ge \left(E_\mu Q_\mu e^{\mu} - E_{v_1} Q_{v_1} e^{v_1} - (\mu - v_1) e_1 y_1\right) \tag{12}$$

By solving inequality (12), the upper bound of e_1 is

$$e_1 \le e_1^{U,v_1,v_2} = \frac{1}{\left(v_2 - (\mu - v_1)\right) y_1^{L,v_1,v_2}} \left[E_{v_2} Q_{v_2} e^{v_2} - \left(E_\mu Q_\mu e^{\mu} - E_{v_1} Q_{v_1} e^{v_1}\right) - e_0 y_0 \right] \tag{13}$$

Case 2 Two Decoy States Protocol: Suppose Alice and Bob choose signal state and two decoy state with expected photon numbers μ, v_1 and v_2 which satisfy

$0 \le v_1 < \mu < v_2 \le 1$ and $\mu^n - v_1^n \ge \mu^m - v_1^m$

Whenever $0<v_1 + \mu < 1$ and $n \le m$. (14)

By using the inequality (8) in [7] and (14) we get

$$\frac{\sum_{i=3}^{\infty} y_i \left(P_i(\mu) - P_i(v_1)\right)}{\sum_{i=3}^{\infty} P_i(v_2) y_i} \le \frac{\left(P_3(\mu) - P_3(v_1)\right)}{P_3(v_2)} \tag{15}$$

Multiply both sides by $v_2^3 \sum_{i=3}^{\infty} y_i \frac{v_2^i}{i!}$ we get

$$v_2^3\left(\sum_{i=3}^{\infty} y_i \frac{\mu^i - v_1^i}{i!}\right) \le \left(\mu^3 - v_1^3\right)\sum_{i=3}^{\infty} y_i \frac{v_2^i}{i!} \tag{16}$$

Using Eq (1) and solving inequality (16), then we get the lower bound of the gain of two photon state as in [31, 32].

According to Eqs (1) and (14) we get

$$\sum_{i=3}^{\infty} e_i y_i \frac{v_2^i}{i!} \ge \sum_{i=3}^{\infty} e_i y_i \frac{\mu^i + v_1^i}{i!} \tag{17}$$

Using Eq (1) and solving inequality (17), then we get e_2 as in [31, 32].

After estimating the lower bounds of y_1 and y_2 and the upper bounds of e_1 and e_2 for each decoy state protocol. Then, we can use the following formula to calculate the final key generation rate of our QKD system for both BB84 and SARG04 protocols [5] and [28] respectively:

$$R_{BB84} \ge R_{BB84}^L = q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L[1 - H_2(e_1^U)]\} \tag{18}$$

$$R_{SARG04} \ge R_{SARG04}^L = -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L[1 - H_2(e_{1,p}^U)] + Q_2^L[1 - H_2(e_{2,p}^U)] \tag{19}$$

where q depends on the implementation (1/2 for the BB84 protocol due to the fact that half of the time Alice and Bob disagree with the bases and if one uses the efficient BB84 protocol, $q \approx 1$), $f(x)$ is the bi-direction error correction efficiency as a function of error rate, normally $f(x) \ge 1$ with Shannon limit $f(x) = 1$ and $H_2(x)$ is binary Shannon information function having the form $H_2(x) = -x \log_2(x) - (1 - x) \log_2 (1 - x)$. $e_{1,p}$ and $e_{2,p}$ are the phase errors for single photon state and two photon states respectively.

Simulation: In this section, we discuss and give the simulation of practical decoy state QKD system which is important for setting optimal experimental parameters and choosing the distance to perform certain decoy method protocol. The principle of simulation is that for certain QKD set-up, if the intensities, percentages of signal state and decoy states are known, we could simulate the gains and QBERs of all states. This is the key point in the experiment. More precisely, we evaluate the values of the gain of signal and decoy states ($\hat{Q}_0$, $\hat{Q}_\mu$, $\hat{Q}_{v_1}$, $\hat{Q}_{v_2}$), the overall quantum bit error rate (QBER) for signal and decoy states ($\hat{E}_\mu$, $\hat{E}_{v_1}$, $\hat{E}_{v_2}$) and then calculate the lower bound of the single and two photon gains, the upper bound QBER of single and two photon pulses and then substitute these results into Eqs. (18) and (19) for getting the lower bound of key generation rate for both BB84 and SARG04 protocols.

Here, we try to simulate an optical fiber based QKD system using our decoy state method for BB84 and SARG04, the losses in the quantum channel can be derived from the loss coefficient α in dB/km and the length of the fiber l in km. the channel transmittance can be written as $\eta_{AB} = 10^{-\frac{\alpha l}{10}}$, and the overall transmission between Alice and Bob is given by $\eta = \eta_{Bob}\ \eta_{AB}$, where $\alpha = 0.21 dB / km$ in our set-up is the loss coefficient, η_{Bob} is the transmittance in Bob's side. We choose the detection efficiency of $\eta = 1.7 \times 10^{-2}$, detectors dark count rate of $y_0 = 1.7 \times 10^{-6}$, the probability that a photon hits the erroneous detector ($e_{\text{detector}} = 0.033$), the wavelength ($\lambda = 1550nm$), the data size is $N = 6 \times 10^9$. These parameters are taken from the GYS experiment [29]. We choose the intensities, the percentages of signal state and decoy states which could give out the optimization of key generation rate and the maximum secure distance for the protocols which are proposed. The search for optimal parameters can be obtained by numerical simulation.

Figure (1) illustrates the simulation results of the key generation rate against the secure distance of fiber link for different decoy state protocols with statistical fluctuation. (a) The asymptotic decoy state method (with infinite number of decoy states) for BB84. (b) The key generation rate of two decoy state protocol with the statistical fluctuations (BB84). (c) The asymptotic decoy state method (with infinite number of decoy states) for both single and two photons contributions (SARG04). (d) The asymptotic decoy state method (with infinite number of decoy states) for only single photon contributions (SARG04). (e) The key generation rate of two decoy state protocol with the statistical fluctuations (SARG04). Comparing these curves, it can be seen that the fiber based QKD system using the proposed method for BB84 is able to achieve both a higher secret key rate and greater secure distance than SARG04. The maximal secure distances of the five curves are 142 km, 127 km, 97km, 94 km and 73km.

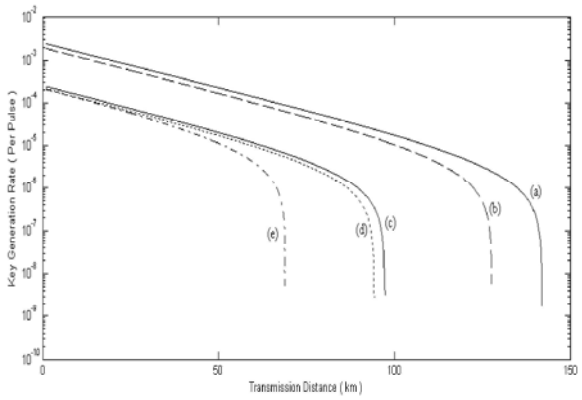

Fig. 1: The simulation results of the key generation rate against the secure distance of fiber link for different decoy state protocols for BB84 and SARG04. (a) The asymptotic decoy state method (with infinite number of decoy states) for BB84. (b) The key generation rate of two decoy state protocol with the statistical fluctuations (BB84). (c) The asymptotic decoy state method (with infinite number of decoy states) for both single and two photons contributions (SARG04). (d) The asymptotic decoy state method (with infinite number of decoy states) for only single photon contributions (SARG04). (e) The key generation rate of two decoy state protocol with the statistical fluctuations (SARG04).

CONCLUSION

We have presented a decoy-state method to implement fiber-based QKD systems over very lossy channels for both BB84 and SARG04. We have clearly demonstrated how to estimate the lower bound of the fraction of single-photon counts ($y1$), the fraction of two photon counts ($y2$), the upper bound QBER of single-photon pulses ($e1$), the upper bound QBER of two-photon pulses ($e2$) and to evaluate the lower bound of key generation rate for both BB84 and SARG04. The simulation results show that the maximum distance which is achieved by QKD system using the proposed decoy state method for BB84 is greater than SARG04 for both fiber based and free space QKD system. Comparing these results, it can be seen that the fiber based system using the proposed method for BB84 is able to achieve both a higher secret key rate and greater secure distance than SARG04. This lead to say that the two-photon part has a small contribution to the key generation rates at all distances.

ACKNOWLEDGMENTS

The author wishes to acknowledge IIUM (EndowmentB) and MOSTI (e-science grant) for their support in providing the various facilities utilized in the presentation of this paper.

REFERENCES

1. Bennett, C.H. and G. Brassard, 1984. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York, 1984), pp: 175-179; IBM Tech. Discl. Bull., 28: 3153-3163.
2. Scarani, V., *et al*., 2004. Physical Review Letters, 92: 057901.
3. Shor, P.W., 2000. J. Preskill, Phys. Rev. Lett., 85(441): 441-444.
4. MO, X.F., *et al*., 2005. Opt. Lett., 30: 2632-2634.
5. Ma. X., *et al*., 2005. Physical Review A 72, (2005) 012326.
6. Gottesman, D., H.K. Lo, N. L¨utkenhaus and J. Preskill, XXXx. Quantum Information. And
7. Computation. 2004. 4(325): 325-360.
8. Hwang, W.Y., 2003. Phys. Rev. Lett., 91: 057901-057905.
9. Wang, X.B., 2005. Phys. Rev. A, 72: 012322-012328.
10. Li, J.B. and X.M. Fang, 2006. Chinese Physics Letters., 23: 4.
11. Qing-yu Cai and Yong-gang Tan, 2007. Phys. Rev. A, 75: 012312.
12. Tomoyuki Horikiri and Takayoshi Kobayashi, 2006. Phys. Rev. A 73: 032331-032336.
13. Qin Wang, X.B. Wang and G.C. Guo, 2007. Phys. Rev. A 75: 012312-012317.
14. Yin, Z.Q., Z.F. Han, F.W. Sun and G.C. Guo, 2007. Phys. Rev. A 76: 014304-014308.
15. Wang, X.B., C.Z. Peng and J.W. Pan, 2007. Appl. Phys. Lett., 90: 011118-1-3.
16. Wang, X.B., 2007. Phys. Rev. A 75: 052301-052309.
17. Zhao, Y., *et al*., 2006. Phys. Rev. Lett., 96: 070502-070506.
18. Yi Zhao, *et al*., 2006. Proceedings of IEEE International Symposiumon Information Theory, pp: 2094-2098.
19. Peng, C.Z., *et al*., 2007. Phys. Rev. Lett., 98: 010505-010509.
20. Rosenberg, D., J.W. Harrington, P.R. Rice, *et al*., 2007. Phys. Rev. Lett. 98: 010503-010507.

21. Yuan, Z.L., A.W. Sharpe and A.J. Shields, 2007. Appl. Phys. Lett., 90: 8465-8471.
22. Tobias Schmitt-Manderbach, *et al*., 2007. Phys. Rev. Lett., 98: 010504-010508.
23. Yin, Z.Q., *et al*., 2008. Phys. Rev. A, 77: 062326.
24. Tan, Y.G. and Q.Y. Cai, 2010. Eur. Phys. J. D, 56: 449-455.
25. Marcos Curty, *et al*., 2010. Phys. Rev. A, 81: 022310.
26. Ali, S. and M.R.B. Wahiddin, 2010. Eur. Phys. J.D, 60: 405-410.
27. Evan Meyer-Scott, *et al*., 2011. Phys. Rev. A, 84: 062326.
28. Yuan-yuan Zhou and Xue-jun Zhou, 2011. Optoelectronics Letters, V 7, N 5, 389-393.
29. Fung, C.H., K. Tamaki and H.K. Lo, 2006. Phys. Rev. A. 73: 012337-012356.
30. Gobby, C., Z.L. Yuan and A.J. Shields, 2004. Appl. Phys. Lett., 84: 3762-3764.
31. Sellami Ali, *et al*., 2012. Fiber based Practical QKD system. Proceedings of the 2nd International Conference on Mathematical Applications in Engineering (ICMAE2012)
32. Sellami Ali, *et al*., 2012. Practical SARG04 quantum key distribution. Opt Quant Electron, 44: 471-482.