Malaysian Journal of Mathematical Sciences 7(S): 39-47 (2013)
Special Issue: The 3rd International Conference on Cryptology & Computer Security 2012 (CRYPTOLOGY2012)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Secure Communication with One Decoy State and Two Way Quantum Key Distribution Scheme

[1,2*]M.F. Abdul Khir, [3]Iskandar Bahari, [1,2]M. N. Mohd Zain and S. Shaari[1]

[1]Photonic Lab, IMEN, Universiti Kebangsaan Malaysia, 43400 UKM Bangi, Malaysia

[2]Photonics Technology and Product Development (PTPD), MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia

[3]Advance Analysis and Modelling, Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia

E-mail: mfared@mimos.my, iskandar.bahari@mimos.my, zman@mimos.my and sahbudin@eng.ukm.my

*Corresponding author

ABSTRACT

Quantum Key Distribution (QKD) provides a mean for unconditionally secure secret key sharing for secure communication. For a practical QKD system, the recently proposed decoy state protocol has become an essential tool. In this work, we conduct numerical analysis against several bounds for one decoy state with two way QKD protocol and compare their performance in terms of key rate and maximum secure distance.

Keywords: Quantum Key Distribution (QKD), secure communication, protocol, secure distance.

1. INTRODUCTION

Dependencies over shared information infrastructure particularly the internet has increased the demand for secure communication between two distant parties. For critically confidential data, cryptography plays very important role. While conventional cryptographic techniques rely on computational difficulties and is operated without security proof, Quantum

Cryptography or better known as Quantum Key Distribution (QKD) combined with one time pad is shown to be the most likely candidate to provide the unconditionally secure information transfer needed by critical organizations.

However, real life QKD systems face implementation problems such as unavailability of true single photon source. Due to this, most QKD implementations rely on weak coherent pulses which cannot avoid emitting multi photon pulses. Attack such as Photon Number Splitting (PNS) attack has been identified as severely affecting QKD practicality in terms of limiting its maximum secure distance. This threat however was encountered by the discovery of the decoy state QKD where one uses several extra states named as decoy states as described by Hwang (2003). By monitoring the statistics of the signal and decoy states, Alice and Bob could easily determine Eve's tempering since her attempt unavoidably affects both signal and decoy states statistic (Lo *et al.* (2005)). This then reduces the pessimistic assumptions and reduces the amount of bits to be discarded at privacy amplification stage. As a result, the secure key generation rate and maximum secure distance is greatly increased, leading to a practical QKD implementation. Example implementations of decoy state can be seen from the work by Zhao *et al.* (2006), Schmitt-Manderbach (2007) and Liu *et al.* (2010).

While it has been shown by Ma *et al.* (2005) that a special case of two decoy states that is the weak+vacuum decoy state where one uses one weak decoy state and the other as vacuum decoy state is optimal for the case of BB84 protocol, in some cases where only one laser source is used such as in "plug and play" QKD system, one need a very good attenuator to obtain a really vacuum state. It is known that there exist difficulties in finding really good attenuator that could totally block photons from laser source (Zhao *et al.* (2006)). In such case, one may resort to one decoy state. It is then interesting to see how would a one decoy state protocol performs in another variant of QKD protocol that is the two way protocol (Ostermeyer *et al.* (2008), Lucamarini *et al.* (2007), Shaari *et al.* (2006), Lucamarini *et al*. (2005), Cere (2006), Kumar *et al.* (2008)).

In this work, we compare three bounds for the case of one decoy state for a two way QKD protocol, specifically the LM05. Using the bounds, we conduct numerical simulation and observe the performance in terms of maximum secure distance. We also include the case of without decoy states as well as the theoretical infinite as base comparison of how would the proposed schemes perform. As such, this letter is organized as follows. We review the bound for the cases of one decoy state in section

two. In section three we discuss the numerical simulation result while section four conclude and suggest future works.

2. THE ONE DECOY STATE

We assume ideal case of infinite decoy state with channel transmission $t_{AB} = 10^{-\left(\frac{2lAB}{10}\right)}$, overall transmission (channel and intrinsic) $\eta = t_{AB}\eta_{Bob}$,transmittance of i-th photon state $\eta_i = 1-(1-\eta)^i$. The lAB is the one way channel loss in dB between Alice and Bob and is a product of distance (l) in km and the optical fiber loss coefficient (α) in dB/km. Notice the factor of two in the channel transmission (t_{AB}) comes from the two way channel loss in a two way QKD protocol.

In the case of one decoy state, Bob and Alice do not know the background rate Y_0 precisely as they do in the case of weak+vacuum decoy state (Ma *et al.* (2005)). This requires them to estimate the upper bound Y_0^U which can directly be imported from Equation 38 of (Ma *et al.* (2005)). Similarly, the lower bound of single photon yield (Y_1^L) and gain (Q_1^L) can also directly be obtained from (Ma *et al.* (2005)). They are given as follow

$$Y_0 \leq Y_0^U = \frac{E_\mu Q_\mu e^\mu}{e_0} \tag{1}$$

where Q_μ and E_μ are respectively gain and QBER from signal state with mean photon number μ.

$$Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu-\nu^2}\left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2-v^2}{e_0\mu^2}\right) \tag{2}$$

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}\left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2-v^2}{e_0\mu^2}\right) \tag{3}$$

where Q_v is the gain from decoy state with mean photon number v.

We have derived the lower bound for double photon yield (Y_2) and gain (Q_2) (Abdul Khir *et al.* (2011b)) and are given by

$$Y_2 \geq Y_2^L = \frac{2\mu\left(Q_v e^v - Q_\mu e^\mu \frac{v^3}{\mu^3} - E_\mu Q_\mu e^\mu \frac{\mu^3-v^3}{e_0\mu^3} - \frac{v\mu^2-v^3}{\mu^2} Y_1^U\right)}{v^2\mu - v^3} \tag{4}$$

$$Q_2 \geq Q_2^L = \frac{\mu^3 e^{-\mu}\left(Q_v e^v - Q_\mu e^\mu \frac{v^3}{\mu^3} - E_\mu Q_\mu e^\mu \frac{\mu^3 - v^3}{e_0 \mu^3} - \frac{v\mu^2 - v^3}{\mu^2} Y_1^U\right)}{v^2\mu - v^3} \quad (5)$$

where Y_1^U is given by

$$Y_1^U = \frac{(2Q_v e^v - 2Y_0^L - Y_2^\infty v^2)}{2v} \quad (6)$$

Now, for the upper bound of single photon error rate e_1^U, we have two options, one from our previous work (Abdul Khir *et al.* (2011b)) and the other from (Ma *et al.* (2005)) which are respectively given as

$$e_{1A} \leq e_1^U = \frac{E_v Q_v e^v \mu^2 - E_\mu Q_\mu e^\mu v^2 - e_0 Y_0^L(\mu^2 - v^2)}{Y_1^L(v\mu^2 - \mu v^2)} \quad (7)$$

$$e_{1B} \leq e_1^U = \frac{E_\mu Q_\mu e^\mu}{Y_1^L e_0} \quad (8)$$

The double photon error rate denoted as e_2^U is as given in (Abdul Khir *et al.* (2011b)):

$$e_2 \leq e_2^U = \frac{2(E_v Q_v e^v \mu - E_\mu Q_\mu e^\mu v - e_0 Y_0^L(\mu - v))}{Y_2^L(\mu v^2 - v\mu^2)} \quad (9)$$

The secure key rate (R) can be calculated by inserting the resulted Y_1,Q_1, Y_2, Q_2,e_1 and e_2 into key rate formula given by Shaari *et al.* (2011) in Equation 13. Now, we would like to review another case of one decoy state, mentioned in our previous work (Abdul Khir *et al.* (2011b)) in which we derived the bound using the second approach proposed in (Shaari *et al.* (2011)), where the yield for single and double photon were lumped for key rate calculation. In this way, the lumped lower bound of yield $(Y1 + Y2)^L$ is given as

$$(Y1 + Y2)^L = \frac{\mu^3 Q_v e^v - (\mu^3 - v^3)\frac{E_\mu Q_\mu e^\mu}{e_0} - v^3 Q_\mu e^\mu + \left(v^3\mu - \frac{1}{2}v^3\mu^2\right)Y_1^L}{\mu^3(v - \frac{1}{2}\frac{v^3}{\mu})} \quad (10)$$

where Y_1^L is from Equation 2.

The lower bound of effective gain $Q_{12}^{L}(\mu)$ is given as

$$Q_{12}^{L}(\mu) = \left[\frac{(Y1+Y2)^{L}}{2}\mu^{2} + (Y_{1}^{L}\mu - \frac{Y_{1}^{L}\mu^{2}}{2})\right]e^{-\mu} \tag{11}$$

where the $(Y1+Y2)^{L}$ and Y_{1}^{L} is from Equation 10 and Equation 2 respectively.

The upper bound of effective error rate ε^{U} is given as

$$\varepsilon^{U} = \frac{E_{\mu}Q_{\mu} - e_{0}Y_{0}e^{-\mu}}{Q_{12}^{L}} \tag{12}$$

The effective gain ($Q_{12}^{L}(\mu)$) and error rate (ε^{U}) can be plugged into the following Equation 14 for the lower bound of key generation rate (R_{12}):

$$R \geq R^{L} = -Q_{\mu}f(E_{\mu})H(E_{\mu}) + \sum_{i=1}^{2} Q_{i}[1-\tau(e_{i})] \tag{13}$$

$$R_{12} \geq R_{12}^{L} = -Q_{\mu}f(E_{\mu})H(E_{\mu}) + Q_{12}^{L}[1-\tau(\varepsilon^{U})] \tag{14}$$

where $H(E_{\mu})$ is the binary Shannon Entrophy and is given by

$$H(E_{\mu}) = -E_{\mu}\log_{2}(E_{\mu}) - (1-E_{\mu})\log_{2}(1-E_{\mu})$$

and $\tau(e)$ as

$$\tau(e) = \log_{2}(1+4e-4e^{2}) \text{ for } e < \frac{1}{2} \text{ and } \tau(e) = 1 \text{ if } e \geq \frac{1}{2}$$

3. RESULT AND DISCUSSION

As previously mentioned, we have three cases of bounds for one decoy state. Let us denote the first as R_{e1A} where we used Equation 7 for e_{1}^{U} estimation and the second as R_{e1B} where we use Eq 8 for e_{1}^{U} estimation. They both used Equation 13 to calculate their secure key rate. The third case is where we lump the Y_{1} and Y_{2} lower bound estimation into $(Y1+Y2)^{L}$ and used Equation 14 to calculate the secure key rate. We denote this asR_{12}. In order to gain confidence in our result, we have made use of real intrinsic system parameters obtained from GYS experiment (Gobby *et al.* (2004)) where the internal transmission of the system $(\eta_{Bob}) = 0.045$, the

erroneous detection probability $(e_{detector}) = 0.033$, the background rate $(Y_0) = 1.7 \times 10^{-6}$and the optical fiber loss coefficient $(\alpha) = 0.21\ [dB/km]$. For the error correction efficiency, we used $f(e) = 1$. The result from numerical simulation is depicted in Figure 1. It includes all the three cases as well as the case of without decoy state and the theoretical infinite decoy state. For the case of without decoy state, the calculation is based on (Lucamarini *et al.* (2007)). We let optimal μ and ν for every distance where μ and ν combination that would yield the highest secure key rate was numerically searched for every distance.

From Figure 1. we can say that all the three cases of one decoy state were able to improve the maximum secure distance of the case of without decoy state. The R_{e1A} was able to extend the maximum secure distance by around 5 km while the $R_{e1B}$was able to extend by 10 km or so. In terms of key rate, prior to around 25 km, both cases perform worse than without decoy state which question the practicality of these bounds at the said region. It is clear that the third case (R_{12}) outperforms the first and the second case in both the key rate as well as the maximum secure distance. The fact that the achieved maximum secure distance were quite far from the theoretical infinite case suggest that one should opt for the weak+vacuum case which has been shown in (Abdul Khir *et al.* (2011a)) to perform very well close to the theoretical infinite case, whenever possible.

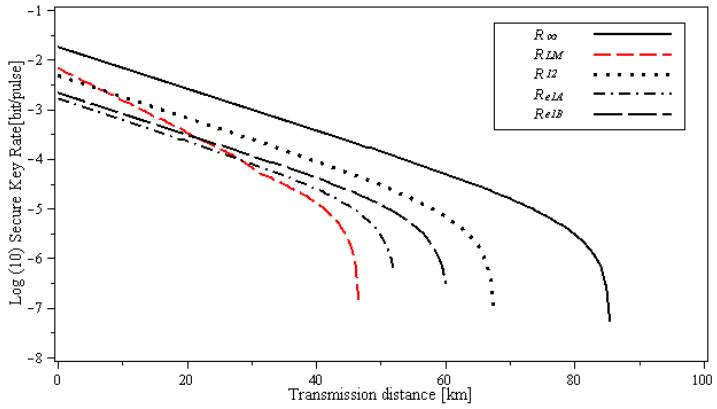

Figure 1: A plot of secure key generation rate against transmission distance. The system intrinsic parameters are from GYS (Gobby et al. 2004) experiment. The dash line shows the simulation result of the case of without decoy state. The solid line shows the case with infinite decoy state (the maximum theoretical case). The dotted line is the case ofR_{12}, the long dash is the case of $R_{e1B}$and the dash dot is the case of R_{e1A}.

4. CONCLUSION

We have conducted numerical analysis to compare the performance of the three bounds for one decoy states with a two way QKD protocol. The result showed that the bound for one decoy state derived from the case of where single and double photon calculation were combined performs better than the bound when single and double photon contribution was separately calculated, in both key rate as well as maximum secure distance. This however is not as good as the case of weak+vacuum which has been shown previously in our previous work (Abdul Khir and Shaari (2011)) to perform very well close to the theoretical infinite case.

REFERENCES

Abdul Khir, M, F, Bahari, I, Ehsan, A. A. 2011a. Two Way Quantum Key Distribution Protocol with Weak+Vacuum Decoy State. In proceeding of the *2nd IEEE International Conference on Photonic (ICP2011)*, Kota Kinabalu.

Abdul Khir, M,F, Bahari, I, Ali, S, Shaari, S. 2011b. Weak+Vacuum and One Decoy State with Two Way Quantum Key Distribution Protocol,arXiv:1108.4756v2 [quant-ph].

Abdul Khir, M,F, Mohd Zain, M,N, Suryadi, Saharudin,S, Shaari, S. 2012a. Implementation of two-way free space quantum key distribution. *Opt. Eng*. 51, 045006.

Abdul Khir, M,F, Mohd Zain, M,N, Bahari, I, Suryadi, Sahbudin, S. 2012b. Implementation of Two Way Quantum Key Distribution Protocol with Decoy State. *Optics Communications*. **285**: 842-845.

Cere, A, Lucamarini, M, Giuseppe, G. D, Tombesi, P. 2006. Experimental Test of Two-Way Quantum Key Distribution in the Presence of Controlled Noise. *Phys. Rev. Lett.* **96**: 200-501

Gobby, C, Yuan, Z. L, and Shields, A. J. 2004. Unconditionally Secure quantum key distribution over 50 km of standard telecom fibre. *Applied Physics Letters*. **84** (19): 3762-3764.

Hwang, W. Y. 2003. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **91**: 057901.

Kumar, R., Lucamarini, M., Giuseppe, G. D., Natali, R., Mancini, S. and Tombesi, P. 2008. Two-way quantum key distribution at telecommunication wavelength. *Phys. Rev. A*. **77**: 022304

Liu, Y., Chen, T.Y., Wang, J., Cai, W. Q., Wan, X., Chen, L. K., Wang, J. H., Liu, S. B,, Liang, H., Yang, L., Peng, C. Z., Chen, K., Chen, Z. B., and Pan, J. W. 2010. Decoy-state quantum key distribution with polarized photons over 200 km. *Optics Express*. **18**(8): 8587-8594

Lo, H. K., Ma, X., Chen, K. 2005. Decoy State Quantum Key Distribution. *Phys. Rev.Lett*. **94**: 230504.

Lucamarini, M. and Mancini, S. 2005. Secure deterministic communication without entanglement. *Phys. Rev. Lett*. **94**: 140501.

Lucamarini, M., Cere, A., Giuseppe, G. D., Mancini, S., Vitali, D. and Tombesi, P. 2007. Two-way Protocol with Imperfect Devices. *Open Systems & Information Dynamics*. **14**(2): 169-178

Ma, X., Qi, B., Zhao, Y. and Lo, H. K. 2005. Practical decoy state for quantum key distribution. *Phys.Rev. A*. **72**: 012326.

Ostermeyer, M. and Walenta, N. 2008. On the Implementation of a Deterministic Secure Coding Protocol using Polarization Entangled Photons. Optics Communications. **281**(17): 4540-4544.

Shaari, J. S., Lucamarini, M. and Wahiddin, M. R. B. 2006. Deterministic six states protocol for quantum communication. *Physics Letters A*. **358**(2): 85-90.

Shaari, J. S., Bahari, I. and Ali, S. 2011. Decoy states and two way quantum key distribution schemes. *Optic Communications*. **284**: 697–702.

Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A. and Weinfurter, H. 2007. Experimental Demonstration of Free-Space Decoy state Quantum Key Distribution over 144 km. *Phys. Rev.Lett*. **98**: 010504.

Zhao, Y., Qi, B., Ma, X., Lo, H. K. and Qian, L. 2006. Experimental quantum key distribution with decoy states. *Phys Rev. Lett.* **96**: 070502.

Zhao, Y., Qi, B., Ma, X., Lo, H. K. and Qian, L. 2006. Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber. *Proceedings of IEEE International Symposium on Information Theory (IEEE, 2006)*, pp. 2094-2098.