Etudes scientifiques

IMPLEMENTATION OF DECOY STATE PROTOCOL

SELLAMI Ali[1], SELLAMI Mohammed[2]

[1] Faculty of Computer Science and Information Technology,
Shaqra University
Shaqra, Kingdom of Saudi Arabia
[2]Institute of Science and Technology, University Centre of
Tamanrasset, Algeria
sellami2003@hotmail.com

Abstract

[The experiment of decoy state QKD has been demonstrated using ID-3000 commercial QKD system based on a standard bi-directional 'Plug & Play' set-up. Two protocols of decoy state QKD have been implemented: one decoy state protocol and vacuum state protocol for both BB84 and SARG04 over different transmission distance of standard telecom fiber. We have achieved a low quantum bit error rate of signal state from 10 to 50 km. The results have shown that the gains of signal are greater than decoy state gains and the QBERs of signal are less than decoy state QBERs. The experimental results are in excellent agreement with simulation results.]

Index Terms: Quantum cryptography, Quantum key distribution**,** decoy state protocol, and Optical Communications.

1. INTRODUCTION:

Quantum key distribution (QKD) is a cryptographic protocol that allows two remote parties (Alice and Bob) to generate a random key (a string of bits) so that only Alice and Bob have any information regarding the key. The most well-known QKD protocol is the BB84 protocol [1], which has been proven to be unconditionally secure against any attacks allowed by quantum

mechanics [2,3, 4];this does not guarantee the security of QKD in practice, due to various types of imperfections in a practical set-up. For real-life experimental set-ups, which are mainly based on faint laser pulses, the occasional production of multi-photons and channel loss make it possible for sophisticated eavesdroppers to launch various subtle eavesdropping attacks, including the PNS (photon number splitting) attack[5], in which she Alice blocks all single-photon pulses and splits multi-photon pulses. She keeps one copy of each of the split pulses to for herself and forwards another copy to Bob. Although [5, 6] showed that secure QKD is still possible even with imperfect devices, the PNS attack puts severe limits on the distance and key generation rate of an unconditionally secure QKD. A novel solution to the problem of imperfect devices in BB84 was proposed by Hwang [8], who used extra test states–called decoy states–to learn the properties of the channel and/or eavesdrop on the key-generating signal states. Lo and co-workers presented an unconditional security proof of decoy-state QKD [9, 10]. By combining the idea of the entanglement distillation approach by Gottesman, Lo, Lutkenhaus, and Preskill (GLLP) [11] with the decoy state method, they showed that decoy state QKD can exhibit a dramatic increase in distance and key generation rate compared to non-decoy protocols [12]. Moreover, many methods have been developed to improve the performance of the decoy state QKD, including more decoy states [13], non-orthogonal decoy-state method [14], photon number-resolving method [15], herald single photon source method [16, 17], modified coherent state source method [18], and the intensity fluctuations of the laser pulses [19] and [20]. Some prototypes of decoy state QKD have already been implemented [21- 26]. A further improvement has been examined, using four-source decoy states [27]. The preparation of phase-randomized coherent pulses could be achieved, for instance, by strongly modulating the laser diode, taking it below and above threshold [28]. Importantly, the security of decoy-state QKD has been obtained in the case of finite-length keys [29,30]. A complete passive decoy-state QKD transmitter with coherent light has been presented in [31].

Here, we have implemented a decoy state QKD using ID-3000 commercial QKD system based on a standard bi-directional 'Plug & Play' set-up. Two protocols of decoy state QKD are implemented: one decoy state protocol and vacuum state protocol for both BB84 and SARG04 over different transmission distance of standard telecom fiber.

2. EXPERIMENTAL SETUP

Before experiment, we have performed the numerical simulation which is important for setting optimal experimental parameters and choosing the distance to perform certain decoy state protocol. Then, we can perform the experiment and observe the values of $\hat{Q}_0$, $\hat{Q}_\mu$, $\hat{Q}_{\nu_1}$ and $\hat{E}_\mu, \hat{E}_{\nu_1}$ (these parameters with statistical fluctuations) and then deduce the optimization of the lower bound of fraction of single-photon and two photon counts and upper bound QBER of single-photon and two photon pulses. Existing commercial QKD systems are bi-directional. To show conceptually how simple it is to apply the decoy state idea to a commercial QKD system, we chose ID-3000 commercial Quantum Key Distribution system manufactured by id Quantique. The id 3000 Clavis system consists of two stations controlled by one or two external computers. A comprehensive software suite implements automated hardware operation and complete key distillation. Two quantum cryptography protocols are implemented (BB84 and SARG04 protocols). The exchanged keys can be used in an encrypted file transfer application, which allows secure communications between two stations.

Figure 1 illustrates the schematic of the optical and electric layouts in our system. The commercial QKD system by id Quantique consists of Bob and "Jr. Alice". In our decoy state experiment, the actual (sender's) system is called "Alice". It consists of "Jr. Alice" and two new optical and electronics components added by us. More concretely, for our decoy state protocol, we place the Decoy intensity modulator (IM) (denoted by DA in Figure 1) right in front of Jr. Alice. Its "idle state" is set to maximum transmittance. When the frame comes from Bob, the Decoy IM is in the idle state. After

the first pulse reaches coupler C2, it will be detected by the classical detector and a synchronization signal will be output to trigger the Decoy Generator. The Decoy Generator (DG in Figure 1), being triggered, will hold a delay time td before outputting NP modulation voltages driving the Decoy IM to attenuate the intensity of each the NP signals to be either that of signal state or decoy state dynamically, according to the Decoy Profile. The Decoy Profile is generated before the experiment and loaded from computer to the Decoy Generator as an "Arbitary Waveform". For preparing the Decoy Profile, we generate a sequence of integers $\{1 \le n_i \le 100\}$ which is equal to the pulses number of each frame. Depending on the optimum pulses distribution, some of the i positions will be assigned as signal state and the rest will be assigned as decoy state. In our experiment, a frame of NP pulses (NP = 624) is generated from Bob and sent to Alice. Within a frame, the time interval between signals is 200ns. The next frame will not be generated until the whole frame has returned to Bob. The long delay line inside Jr. Alice promises that the incoming signal and returning signal will not overlap in the channel between Bob and Jr. Alice so as to avoid Rayleigh Scattering.

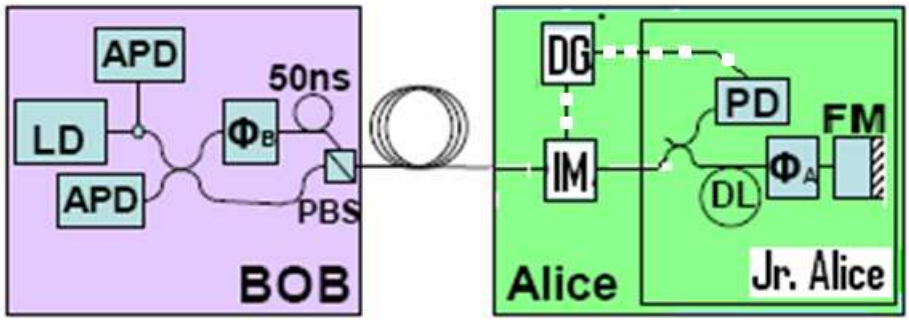

Figure 1: Schematic of the experimental set-up in our system. Inside Bob/Jr. Alice: components in Bob/Alice's package of ID-3000 QKD system. Our modifications: intensity modulator (IM); DG: Decoy Generator. Components of original ID-3000 QKD system: LD: laser diode; APD: avalanche photon diode; Ci: fiber coupler; Φ_i : phase modulator; PBS: polarization beam splitter; PD:

classical photo detector; FM: faraday mirror. Solid line: SMF28 single mode optical fiber; dashed line: electric signal.

3. RESULTS AND DISCUSSION:

We have performed numerical simulation to find out the optimal parameters. For the vacuum state protocol, we set $\mu = 0.85$. The numbers of pulses used as signal state, and vacuum state are $N_\mu = 0.95N$, and $N_0 = 0.05N$ respectively. For the one decoy state protocol, we set $\mu = 0.83$ and $\nu_1 = 0.05$.The numbers of pulses used as signal state, and weak decoy state are $N_\mu = 0.95N$, and $N_{\nu_1} = 0.05N$ respectively, where $N = 100Mbit$ is the total number of pulses sent by Alice in this experiment. After the transmission of all the *N* signals, Alice broadcasted to Bob the distribution of decoy states as well as basis information. Bob then announced which signals he had actually received in correct basis. We assume Alice and Bob announced the measurement outcomes of all decoy states as well as a subset of the signal states.

Figures (2, 3) show the experimental results of the gain and QBER of signal state for vacuum state protocol against the transmission distance for both BB84 and SARG04. Figure 4 shows the experimental results of the gain and QBER of signal and decoy states for one decoy state protocol against the transmission distance for SARG04. For both vacuum state and one decoy state protocol, the experimental results have shown the curves with similar shapes. Using our two decoy state protocols (vacuum state and one decoy state protocols) we have achieved a low quantum bit error rate of signal state from 10 to 50 km. The results show that the gains of signal are greater than decoy state gains and the QBERs of signal are less than decoy state QBERs. From these experimental results, Alice and Bob then can determine the lower bound of the gain of single-photon (Q_1), two-photon (Q_2), the upper bound QBER of single-photon pulses (e_1), the upper bound QBER of two-photon pulses (e_2), and to evaluate the lower bound of key generation rate for both BB84 and SARG04

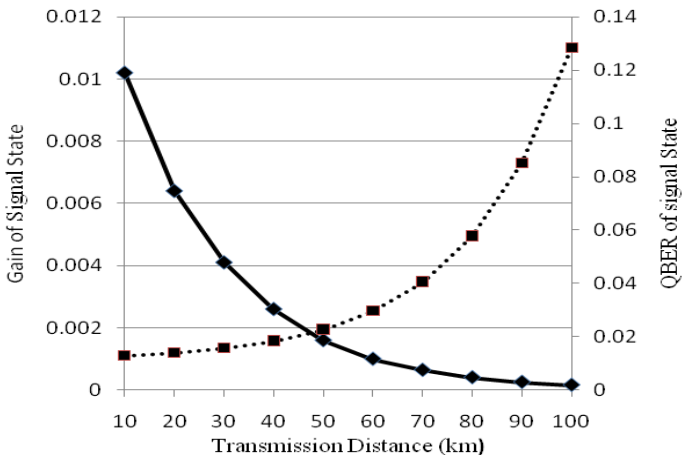

Figure 2: The experimental results of vacuum state for BB84 against transmission distance. The solid line shows the gain of signal state. The dotted line shows the QBER of signal state.

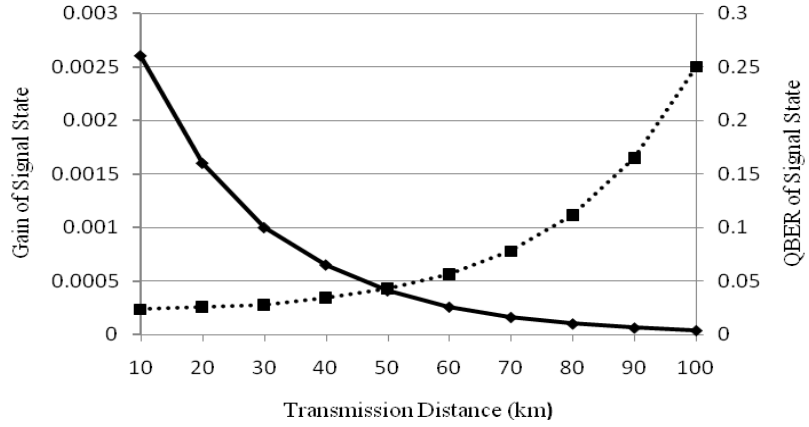

Figure 3: The experimental results of vacuum state for SARG04 against transmission distance. The solid line shows the gain of signal state. The dotted line shows the QBER of signal state.

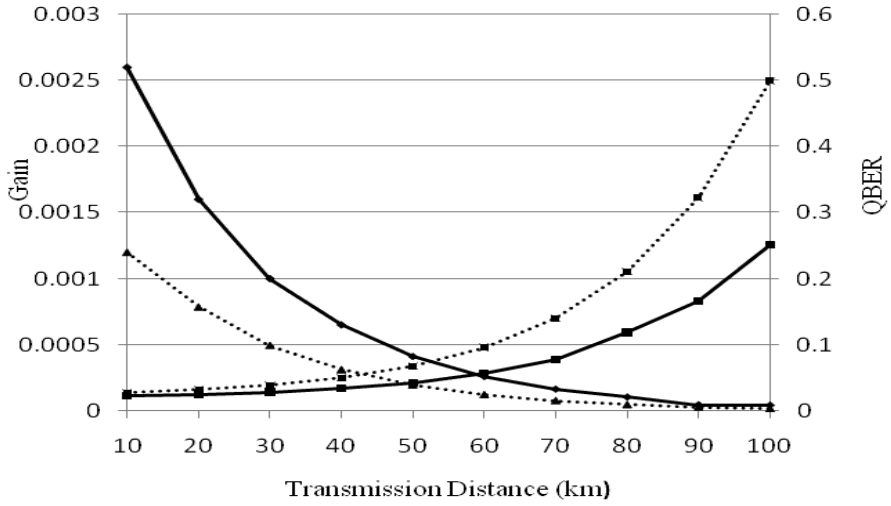

Figure 4: The experimental results of one decoy state for SARG04 against transmission distance. The solid line shows the gain and QBER of signal state. The dotted line shows the gain and QBER of decoy state.

4. CONCLUSION:

The practical vacuum state and one decoy state QKD system using commercial QKD system have been implemented over different transmission distance of standard telecom fiber using ID-3000 commercial QKD system. The experimental results are in excellent agreement with simulation results. For both the experimental and simulation results, we have found that fiber based QKD system using our method for SARG04 is able to achieve both a higher secret key rate and greater secure distance than BB84.

5. REFERENCES:

[1] C.H. Bennett and G. Brassard, in : Proc. IEEE Int. Conf. on Computers, systems, and signal
processing, Bangalore (IEEE, New York, 1984) p.175.

[2] D. Mayer, J. Assoc. Comput. Mach. 48, 351 (2001). Its preliminary version appeared in "Advances in Cryptology-Proc. Crypto'96, Vol. 1109 of Lecture Notes in Computer Science,
Ed. N. Koblitz, Springer-Verlag, New York, 1996, p. 343.

[3] P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).

[4] A.K. Ekert, Phys. Rev. Lett. 67, 661 (1991)

[5] D. Gottesman, H.-K. Lo, N. L¨ukenhaus, and J. Preskill, Quantum Information and Computation 5, 325 (2004), arXiv:quant-ph/0212066.

[6] H. Inamori, N. L¨ukenhaus, and D. Mayers (2001), arXiv:quant-ph/0107017.

[8] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).

[9] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).

[10] H.-K. Lo, in Proc. of IEEE International Symposium on Information Theory (ISIT) 2004
(2004), p. 137, arXiv:quant-ph/0509076.

[11] D. Gottesman *et al.*, Quantum Inf. Comput. **4**, 325 (2004).

[12] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[13] X.-B. Wang, Phys. Rev. A 72, 012322 (2005)

[14] J.-B. Li, and X.-M. Fang, Chin. Phys. Lett. 23, No. 4 (2006)

[15] Qing-yu Cai, and Yong-gang Tan, Phys. Rev. A. 73, 032305 (2006)

[16] Tomoyuki Horikiri, and Takayoshi Kobayashi, Phys. Rev. A 73, 032331 (2006)

[17] Qin Wang, X.-B. Wang, and G.-C. Guo, Phys. Rev. A 75, 012312 (2007)

[18] Z.-Q. Yin, Z.-F. Han, F.-W. Sun, and G.-C. Guo, Phys. Rev. A 76, 014304 (2007)

[19] X.-B. Wang, C.-Z. Peng, and J.-W. Pan, Appl. Phys. Lett. 90, 6031110 (2007)

[20] X.-B.Wang, Phys. Rev. A 75, 052301 (2007)

[21] Y. Zhao et al., Phys. Rev. Lett. 96, 070502 (2006)

[22] Yi Zhao et al, Proceedings of IEEE International Symposiumon Information Theory 2006, pp. 2094-2098

[23] C.-Z. Peng et al., Phys. Rev. Lett. 98, 010505 (2007)

[24] D. Rosenberg, J. W. Harrington, P. R. Rice, et al., Phys. Rev. Lett. 98, 010503 (2007)

[25] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 90 011118 (2007)

[26] Tobias Schmitt-Manderbach et al., Phys. Rev. Lett. 98, 010504 (2007)

[27] Jiang, H., Gao, M., Wang, H., Li, H., & Ma, Z. 2015 Four-intensity Decoy state Quantum Key Distribution with enhanced resistance against statistical fluctuation. Preprint. arXiv:1502.0224

[28] Abellán, C.; Amaya, W.; Jofre, M.; Curty, M.; Acín, A.; Capmany, J.; Pruneri, V.; Mitchell, M.W. Ultra-Fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode.Opt. Express 2014, 22, 1645–1654

[29]. Hayashi, M.; Nakayama, R. Security analysis of the decoy method with the Bennett–Brassard 1984 protocol for finite key lengths. New J. Phys. 2014, 16, 063009.

[30]. Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. Phys. Rev. A 2014, 89, 022307.

[31] Marcos Curty, Marc Jofre, Valerio Pruneri and Morgan W. Mitchell. Passive Decoy-State Quantum Key Distribution with Coherent Light. Entropy 2015, 17, 4064-4082; doi:10.3390/e17064064