DECOY STATE QUANTUM KEY DISTRIBUTION

SELLAMI ALI[1,2*], SUHAIRI SAHARUDIN[2] AND M.R.B. WAHIDDIN[1,2]

[1]Department of Computational and Theoretical Sciences,
Faculty of Science, International Islamic University Malaysia
P. O. Box 141, 25710 Kuantan, Malaysia.

[2]Information Security Cluster, MIMOS Berhad, Technology Park Malaysia.

**E-mail: sellami2003@hotmail.com*

ABSTRACT: Experimental weak + vacuum protocol has been demonstrated using commercial QKD system based on a standard bi-directional 'Plug & Play' set-up. By making simple modifications to a commercial quantum key distribution system, decoy state QKD allows us to achieve much better performance than QKD system without decoy state in terms of key generation rate and distance. We demonstrate an unconditionally secure key rate of 6.2931 x 10^{-4} per pulse for a 25 km fiber length.

KEYWORDS : *Quantum Cryptography, Quantum Key Distribution, Decoy State Protocol, Optical Communications*

1. INTRODUCTION

Quantum key distribution (QKD) has drawn many attentions from scientists. Different from the classical cryptography, quantum key distribution (QKD) [1-3] can help two remote parties to set up the secure key by non-cloning theorem [4]. Further, proofs for the unconditional security over noisy channel have been given [5-8]. Unfortunately, in view of implementation, "perfect" devices are always very hard to build. Therefore most up-to-date QKD systems substitute the desired perfect single photon sources by heavily attenuated coherent laser sources. QKD can be performed with these laser sources over more than 120 km of telecom fibers [9, 10].

However, this substitution raises some severe security concern. The output of coherent laser source obeys Poisson distribution. Thus the occasional production of multi-photon signals is inevitable no matter how heavily people attenuate the laser. Recall that the security of BB84 protocol [3] is guaranteed by quantum non-cloning theorem, the production of multi-photon signals is fatal for the security: the eavesdropper (normally denoted by Eve) can simply keep an identical copy of what Bob possesses by blocking all single-photon signals and splitting all multi-photon signals. Most up-to-date QKD experiments have not taken this photon-number splitting (PNS) attack into account, and thus are, in principle, insecure.

Hwang [11] proposed the decoy state method as an important weapon to combat those sophisticated attack: by preparing and testing the transmission properties of some decoy states, Alice and Bob are in a much better position to catch an eavesdropper. Hwang specifically proposed to use a decoy state with an average number of photon of order 1. Hwang's idea was highly innovative.

Decoy pulse QKD theory gives a rigorous bound of the characteristics of the single photon pulses, which are the only source pulses that contribute to the secure bit rate. In [14], combining the idea of security proofs using the entanglement distillation approach in GLLP [10] with decoy method; they gave a formula for the key generation rate

$$R \ge q\left\{Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\right\} \tag{1}$$

Where q depends on the protocol, the subscript μ is the average photon number per signal in signal states, Q_μ is the gain of signal states, E_μ is the quantum bit error rate (QBER) of signal states, Q_1 is the gain of the single photon states in signal states, e_1 is the error rate of single photon states. $f(x)$ is the bi-directional error correction rate [13], and $H_2(x)$ is binary Shannon information function:

$$H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x). \tag{2}$$

Our implementation is based on BB84 [3] protocol. Among total N pulses sent in experiment, N_S pulses are used as signal states. Therefore the factor q is given by $q = ½ N_S/N$.

Q_μ and E_μ can be measured directly from experiments. In [12], they have proposed a practical protocol with Weak + Vacuum states with average photon number 0 and v. such a protocol is relatively simple to implement. The gain of the weak decoy state Q_v and its error rate E_μ could also be required directly from experiments. Considering statistical fluctuations, the lower bounds of Q_1, and the upper bound of e_1 are given by [12]:

$$Q_1 \ge Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\upsilon - \upsilon^2}\left(Q_\upsilon^L e^\upsilon - \frac{\upsilon^2}{\mu^2} Q_\mu e^\mu - Y_0^U\left(\frac{\mu^2 - \upsilon^2}{e_0 \mu^2}\right)\right) \tag{3}$$

$$e_1 \le e_1^U = \frac{E_\upsilon Q_\upsilon}{Q_1} \tag{4}$$

in which

$$Q_v^L = Q_v\left(1 - \frac{u_\alpha}{\sqrt{N_v Q_v}}\right)$$

$$Y_0^L = Y_0\left(1 - \frac{u_\alpha}{\sqrt{N_0 Y_0}}\right)$$

$$Y_0^U = Y_0\left(1 + \frac{u_\alpha}{\sqrt{N_0 Y_0}}\right)$$

In this paper, we will present the experimental implementation of weak decoy + vacuum states QKD using commercial QKD systems are bi-directional. To show conceptually how simple it is to apply the weak decoy + vacuum state idea to a commercial QKD system, we chose ID-3000 commercial Quantum Key Distribution system manufactured by id Quantique. To implement the one decoy state protocol, we have to add some new optical and electronics components to id Quantique and have to attenuate each signal to the intensity of either signal state or weak decoy or vacuum state randomly. In our implementation, the attenuation will be done by placing a VOA (variable optical attenuator) in Alice’s side. Specifically, our QKD system requires the polarizations of the two pulses from the same signal to be orthogonal. Therefore the VOA must be polarization independent so as to attenuate the two pulses equally. The VOA utilized in our experiment to attenuate signals dynamically is Acousto-Optic Modulator (AOM).

2. EXPERIMENTAL SETUP

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 prototype of this QKD system is described in section 2 of [8]. Here we describe it briefly: a frame of NP pulses (in our experiment, NP = 624) is generated from Bob and sent to Alice. Within a frame, the time interval between signals is 200 ns. 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.

This QKD system is called p&p auto-compensating set-up, where the key is encoded in the phase between two pulses traveling from Bob to Alice and back (see Fig. 1) . A strong laser pulse (@ 1550 nm) emitted at Bob is separated at a first 50/50 beam splitter (BS), after having traveled through a short arm and a long arm, including a phase modulator (PMb) and a 50 ns delay line (DL), respectively. All fibers and optical elements at Bob are polarization maintaining. The linear polarization is turned by 90 degree in the short arm, therefore the two pulses exit Bob’s step-up by the same port of the PBS. The pulses travel down to Alice, are reflected on a Faraday mirror, attenuated and come back orthogonally polarized. In turn, both pulses now take the other path at Bob and arrive at the same time at BS where they interfere. Then, they are detected either in D1, or after passing through the circulator (C) in D2. Since the two pulses take the same path, inside Bob in reversed other, this interferometer is auto-compensated.

The implementation of weak + vacuum protocol requires amplitude modulation of three levels: μ, v and 0. Note that it would be quite hard for high-speed amplitude modulators to prepare the real ‘vacuum ‘state due to finite distinction ratio. However, if the gain of the ‘vacuum’ state is very close (like within a few standard deviations) to the dark count rate, it would be a good approximation. In our implementation, the attenuation is done by placing a VOA (variable optical attenuator) in Alice’s side. 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 four new optical and electronics components added by us. More concretely, for our decoy state protocol, we place the Decoy Acousto Optic Modulator AOM (denoted by DA in Fig. 1) right in front of Jr. Alice. Its "idle state" is set to maximum transmittance. When the frame comes from Bob, the Decoy AOM 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 Fig. 1), being triggered, will hold a delay time td before outputting NP modulation voltages driving the Decoy AOM 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 compensating AOM (CA) is used only for the purpose of shifting the frequency of the signal and, thus maintaining the alignment between Alice's and Bob's interferometers. A compensating generator (CG) is used to drive the compensating AOM (CG).]

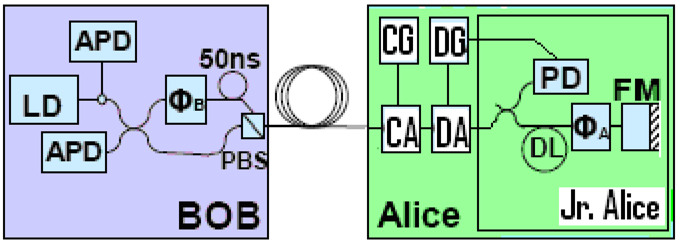

Fig.1: Experimental setup of Weak-Vacuum State Protocol.

3. RESULTS AND DISCUSSION

After the transmission of all the 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. From those experimental data, Alice and Bob then determined Q_μ, Q_v, E_μ, and E_v , whose values are now listed in Table 1. Note that our experiment is based on BB84 [10] protocol, thus $q = (\frac{1}{2})N^S_\mu /N$, where N^S_μ is the number of pulses used as signal state when Alice and Bob choose the same basis, and $N = 105$ Mbit is the total number of pulses sent by Alice in this experiment. We performed numerical simulation to find out the optimal parameters. According to simulation results, we choose the intensities as $\mu = 0.55$, $v = 0.152$. Numbers of pulses used as signal state, weak decoy state and vacuum state are $N_\mu = 0.635$ N, $N_v = 0.203$ N, and $N_0 = 0.162$ N, respectively, where $N = 105$ Mbit is the total data size we used. In our analysis of experimental data, we estimated e_1 and Q_1 very conservatively as within 10 standard deviations (i.e., $u_\alpha = 10$), which promises a confidence interval for statistical fluctuations of $1 - 1.5 \text{ x } 10^{-23}$.

The experimental results listed in Table 1 are the input for Eqs (1), (3), (4), whose output is a lower bound of the key generation rate, as shown in Table 2. Even with our very conservative estimation of e_1 and Q_1, we got a lower bound for the key generation rate $R^L = 6.2931 \times 10^{-4}$ per pulse, which means a final key length of about L = NR = 66 kbit.

Table 1: Direct results from our experiment.

Para.	**Value**	**Para.**	**Value**	**Para.**	**Value**
Qμ	0.0094	Eμ	0.0107	q	0.319
Qν	0.0027	Eν	0.0221	f (E) [13]	1.22

Table 2: The lower bounds of Q_1, R and the upper bound of e_1.

Para.	**Value**	**Para.**	**Value**
Q_1^L	0.0037	R^L	6.2931x 10^{-4}
e_1^U	0.0271		

The values are calculated from Eqs. (1), (3), and (4), taking statistical fluctuation into account.

4. CONCLUSION

Experimental weak + vacuum decoy QKD system using commercial QKD system has been demonstrated over a 25 km fiber with an unconditionally secure key rate of 6.2931×10^{-4}. It is unconditionally secure against all types of attacks, including the PNS attack. We conclude that decoy pulses improve the security and performance of weak pulse QKD. However, sources and detectors must be calibrated accurately to avoid any artifacts that may compromise security.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, UK, 2000.

[2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. 74, 145 (2002), references therein.

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

[4] W.K. Wootters and W.H. Zurek, Nature 299, 802 (1982).

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

[6] H.-K. Lo and H.F. Chau, Science 283, 2050 (1999).

[7] D. Mayers, J. Assoc. Comput. Mach. 48, 351 (2001).

[8] A.K. Ekert, Phys. Rev. Lett. 67, 661 (1991), C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A 54, 3824 (1996).

[9] C. Gobby, Z. L. Yuan, A. J. Shields, *Appl. Phys. Lett.* 84, 3762 (2004)

[10] X. Mo, *et al. Opt. Lett.* 30, 2632 (2005)

[11] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (200).

[12] X.Ma, B. Qi, Y. Zhao and H.-K. Lo, " Practical Decoy State for Quantum Key Distribution". http://www.arxiv.org/abs/quant-ph/0503005(2005)

[13] G. Brassard and L. Salvail, in Advances in Cryptology EUROCRYPT' 93,Vol. 765 of lecture Notes in Computer Science, edited by T.Helleseth (Springer, Berlin, 1994),pp.410-423