American J. of Engineering and Applied Sciences 2 (4): 694-698, 2009
ISSN 1941-7020

Quantum Key Distribution Using Decoy State Protocol

[1,2]Sellami Ali, [2]Shuhairi Saharudin and [1,2]M.R.B. Wahiddin
[1]Department of Computational and Theoretical Sciences,
Faculty of Science, International Islamic University Malaysia, Malaysia
[2]Information Security Cluster, Mimos Berhad, Technology Park Malaysia, Malaysia

Abstract: Problem statement: Quantum key distribution provides unconditional security guaranteed by the fundamental laws of quantum physics. Unfortunately, for real-life experimental set-ups, which 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 Photon Number Splitting (PNS) attack. The decoy state protocols recently proposed to beat PNS attack and to improve dramatically distance and secure key generation rate of Quantum Key Distribution (QKD). **Approach:** Objective of this study was experimental implementation of weak decoy + vacuum states QKD for increasing the performance of QKD system. To show conceptually how simple it was to apply the weak decoy + vacuum state idea to a commercial QKD system, we chosen ID-3000 commercial quantum key distribution system manufactured by id quantique. To implement the weak decoy + vacuum state protocol, we had to add some new optical and electronics components to id quantique and to attenuate each signal to the intensity of either signal state or weak decoy or vacuum state randomly. **Results:** In our implementation, the attenuation will be done by placing a VOA (variable optical attenuator) in Alice's side. Specifically, our QKD system required the polarizations of 2 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 experiment to attenuate signals dynamically was Intensity Modulator (IM). We had implemented weak + vacuum protocol on a modified commercial QKD system over a 25 km of telecom fibers with an unconditionally secure key rate of 6.2931×10^{-4} per pulse. **Conclusion:** By making simple modifications to a commercial quantum key distribution system, we could achieve much better performance with substantially higher key generation rate and longer distance than QKD system without decoy state.

Key words: Quantum cryptography, quantum key distribution, decoy state protocol and optical communications

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 no-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

Corresponding Author: Sellami Ali, Department of Computational and Theoretical Sciences, Faculty of Science, International Islamic University Malaysia, Malaysia

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[12], 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:

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

Where:

- q = Depends on the protocol, the subscript
- μ = The average photon number per signal in signal states
- Q_μ = The gain of signal states
- E_μ = The quantum bit error rate (QBER) of signal states
- Q_1 = The gain of the single photon states in signal states
- e_1 = The error rate of single photon states
- $f(x)$ = The bi-directional error correction rate[13]
- $H_2(x)$ = Binary shannon information function

$$H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x) \quad (2)$$

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 Qv 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]:

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu v - v^2}\left(Q_{1e}^{Lv} - Q_\mu e^\mu \frac{v^2}{\mu^2} - Y_0^U \frac{\mu^2 - v^2}{e_0 \mu^2}\right) \quad (3)$$

$$e_1 \leq e_1^U = \frac{E_\mu Q_\mu - e_0 Y_o^L e^{-u}}{Q_1^L} \quad (4)$$

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 study, 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 weak decoy + vacuum 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 Intensity Modulator (IM).

MATERIALS AND METHODS

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[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 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.

This QKD system is called p and p auto-compensating set-up, where the key is encoded in the

phase between two pulses traveling from Bob to Alice and back (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° 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 Fraday 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_1) 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 shows 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 Intensity Modulator IM (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 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 Fig. 1), being triggered,

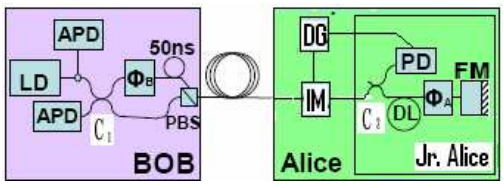

Fig.1: Experimental setup of weak + vacuum state protocol

will hold a delay time td before outputting N_P modulation voltages driving the Decoy IM to attenuate the intensity of each the N_P signals to be either that of signal state or decoy state dynamically, according to the Decoy profile.

RESULTS

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 $N_\mu = 0.635N$, $N_v = 0.203N$ and $N_0 = 0.162N$ respectively, where N = 105Mbit 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. 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 $q = (1/2)\frac{N_\mu^S}{N}$, where N_μ^S is the number of pulses used as signal state when Alice and Bob chose the same basis (Eq. 1).

DISCUSSION

Alice and Bob have to derive a lower bound on the key generation rate, R^L, by applying the theory of one decoy state protocol to their experimental data. To begin, we discuss the theory of weak + vacuum protocol. The weak + vacuum protocol was first proposed and analyzed in[12]. In such a protocol, only vacuum and one decoy state are used (in principle, more decoy states might increase key generation rate) with average photon numbers 0 and v respectively. The transmittance/gain of the decoy state Q_μ and its error rate E_μ could also be acquired directly from experiments. The experimental results are shown in Table 1. Note that the gain of vacuum state is indeed very close to the dark count rate, therefore the vacuum state in our experiment is quite "vacuum". By taking statistical fluctuations into account, we could estimate the lower bound of Q_1 and upper bound of $e_1$by plugging these experimental results into the Eq. 3 and 4[12].

In our analysis of experimental data, we estimated e_1 and Q_1 very conservatively as within 10 standard deviations (i.e., $u_a = 10$), which promises a confidence interval for statistical fluctuations of $1\text{-}1.5\times10^{-23}$.

Table 1: Direct results from our experiment

Para	Value	Para	Value	Para	Value
Q_μ	0.0094	E_μ	0.0107	q	0.319
Qv	0.0027	Ev	0.0221	f (E)[13]	1.22
				Y_0	6.2×10^{-5}

Table 2: The lower bounds of Q_1, R^L and the upper bound of e_1.The values are calculated from Eq. 1-4, taking statistical fluctuation into account

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

The experimental results listed in Table 1 are the input for Eq. 1-4, 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 $R^L = 6.2931\times10^{-4}$ per pulse, which means a final key length of about L = NR = 66 kbit. The finite size of data (105 M) gives a final secure key 66 kbits and introduces statistical fluctuations and therefore reduces the key generation rate (per pulse) below the fundamental limit of $R_{perfect}$, which corresponds to infinite data size and infinite decoy state protocol. We remark that, as discussed in[12], here we consider only the fluctuations of the parameters, Q_1's and e_1's because we believe they, being rather small numbers, are the main source of statistical fluctuations. We do not consider, for example, the fluctuations in the number of different type of pulses (vacuum, single-photon) as such fluctuations are negligible, in comparison. Notice that, even with our very conservative estimation for a confidence of $1\text{-}1.5\times10^{-23}$, the lower bound of R is still roughly 1/4 of $R_{perfect}$. This fact hints that it is not necessary, or rather, not "economical", to use either very large data size or a lot of different decoy states. We performed numerical simulation ranging μ from 0-1, while no positive lower bound on R can be found. This fact indicates that for our set-up, at a distance of 25 km, without decoy states, we would have been unable to prove the security of our protocol in an analogous manner.

We provide the experimental demonstration of decoy state QKD over 25 km of Telecom fibers. Our result shows that, with rather simple modifications (by adding commercial variable optical attenuators) to a commercial QKD system, decoy state QKD allows us to achieve much better performance (in terms of substantially higher key generation rate and longer distance) than what is otherwise possible. Our experiment gives unconditional security against the most general attack allowed by quantum mechanics. Moreover, it gives a rather high key generation rate. We expect that decoy state QKD will play a major role in future QKD systems in both fibers and open air.

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} per pulse. 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.

ACKNOWLEDGMENT

One of the researchers (AS) is grateful to the Faculty of Science of IIUM and Mimos Berhad for the facilities provided to him in the undertakings of his PhD's degree programme.

REFERENCES

1. Nielsen, M.A. and I.L. Chuang, 2000. Quantum Computation and Quantum Information. Illustrated Edn., Cambridge University Press, UK., ISBN: 0521635039, pp: 676.
2. Gisin, N., G. Ribordy, W. Tittel and H. Zbinden, 2002. Quantum cryptography. Rev. Mod. Phys., 74: 145-195. DOI: 10.1103/RevModPhys.74.145
3. Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Proceeding of the IEEE International Conference on Computers, Systems and Signal Processing, (ICCSSP'84), Bangalore, IEEE, New York, pp: 175. http://www.maxpercent.org/papers/BB84.pdf
4. Wootters, W.K. and W.H. Zurek, 1982. A single quantum cannot be cloned. Nature, 299: 802-803. DOI: 10.1038/299802a0
5. Shor, P.W. and J. Preskill, 2000. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett., 85: 441-444. DOI: 10.1103/PhysRevLett.85.441
6. Lo, H.K. and H.F. Chau, 1999. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283: 2050-2056. DOI: 10.1126/science.283.5410.2050
7. Mayers, D., 2001. Unconditional security in quantum cryptography. J. ACM., 48: 351-406. http://doi.acm.org/10.1145/382780.382781

8. Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67: 661-663. DOI: 10.1103/PhysRevLett.67.661
9. Gobby, C., Z.L. Yuan and A.J. Shields, 2004. Quantum key distribution over 122 km of standard telecom fiber. Applied Phys. Lett., 84: 3762-3764. DOI: 10.1063/1.1738173
10. Mo, X. *et al*., 2005. Faraday-Michelson system for quantum cryptography. Optics Lett., 30: 2632-2634. DOI: 10.1364/OL.30.002632
11. Hwang, W.Y., 2003. Quantum key distribution with high loss: Toward global secure communication. Phys. Rev. Lett., 91: 057901. DOI: 10.1103/PhysRevLett.91.057901
12. Ma, X., B. Qi, Y. Zhao and H.K. Lo, 2005. Practical decoy state for quantum key distribution. March 1, 2005. http://www.arxiv.org/abs/quant-ph/0503005
13. Brassard, G. and L. Salvail, 1994. Advances in cryptology EUROCRYPT' 93. Lecture Notes Comput. Sci., 765: 467-467. http://www.springer.com/computer/security+and+cryptology/book/978-3-540-57600-6