Secure quantum key distribution system by applying decoy states protocol

Sura Adil Abbas, Nael A. Al-Shareefi
Department of Communication and Mobile Computing Engineering, Faculty of Engineering, University of Information Technology and Communications (UOITC), Baghdad, Iraq

Article Info

Article history:

Received Jan 08, 2022
Revised Apr 19, 2022
Accepted May 01, 2022

Keywords:

BB84 protocol
Decoy states protocol
PNS
Quantum cryptography

ABSTRACT

Secure quantum key distribution (QKD) promises a revolutionizing in optical applications such as encryption, and imaging. However, their implementation in real-world scenarios continues to be challenged. The goal of this work is to verify the presence of photon number splitting (PNS) attack in quantum cryptography system based on BB84 protocol and to obtain a maximum secure key length as possible. This was realized through randomly interleaving decoy states with mean photon numbers of 5.38, 1.588, and 0.48 between the signal states with mean photon numbers of 2.69, 0.794, and 0.24. Experiment results show that a maximum secure key length obtained from our system, which ignores eavesdropping cases, is 125 with 20% decoy states and 82 with 50% decoy states for mean photon number of 0.794 for signal states and 1.588 for decoy states.

Corresponding Author:

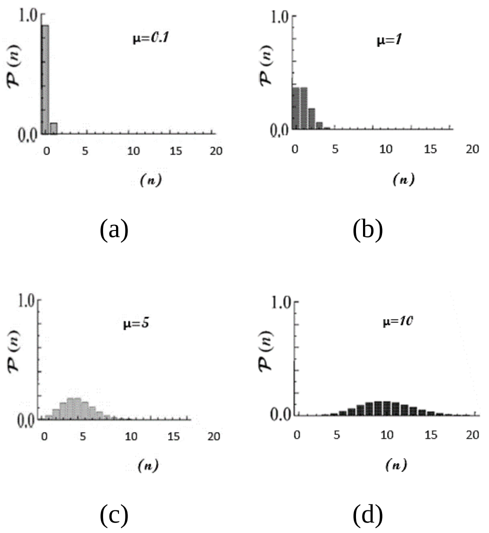
Sura Adil Abbas
Department of Communication and Mobile Computing Engineering, Faculty of Engineering
University of Information Technology and Communications (UOITC), Baghdad, Iraq
Email: sura.adel@uoitc.edu.iq

1. INTRODUCTION

Fifth generation (5G) won't fit all the demands of the future in 2025 and beyond. Sixth generation (6G) wireless communication networks are expected to improve cost/energy/efficiency spectrum and security [1], [2]. 6G networks will rely on new enabling technologies such as quantum computing to meet these requirements. A massive investment has been made in quantum technologies, particularly in the field of quantum computing. Notwithstanding, such developments of quantum computers threaten internet security, easily break down classical encryption and leak private information into malicious adversaries. Hence, quantum secure communication technologies and quantum encryption are the focus of investor interest. In particular, quantum key distribution (QKD) is said to be a secure communication technology that is apparent in the presence of the eavesdropper, Eve, who has unlimited power to break the encryption. Since the invention of the first QKD BB84 protocol in 1984, many researchers have participated in this field to achieve this exciting concept [3].

Several different works have been recently reported to remove attacks on real device defects from theoretical security proofs, such as reference [4]. Nevertheless, Yuen [5], [6] has discovered in theory that even real devices work perfectly along with the standardized theories, there are problems even in theory. Ali *et al.* [7] conducted both a theoretical investigation and an experimental implementation of weak decoy and vacuum states on ID-3000 commercial QKD system for increasing the performance of the system. The type of attack investigated was a photon number splitting (PNS) attack. Lo *et al.* [8] used Gottesman-Lo-Lütkenhaus-Preskill (GLLP) method to prove the security of QKD based on a phase randomized weak coherent state source. The distance increased from 30 km with BB84 protocol to 140 km with decoy states protocol. To bridge the gap between theory and practice, decoy-state measurement-device-independent QKD (mdiQKD) has been proposed, [9]. Nevertheless, its experimental complexity is inappropriate for practical applications [10]-[12]. In addition, the key secret key is very weak with current technology [13], [14]. Also, measurement device independent quantum key distribution (MDI-QKD), allows removing any presumption of confidence from the measuring device, which can be said that the weakest part of QKD realizations [15]-[18].

Using single photon sources in QKD, a perfect secure key is obtained, i.e. eavesdropper would be detected. Utilizing sources of single photons eavesdropper can be detected by monitoring the receiver's quantum bit error rate (QBER) [19]. when an eavesdropper, Eve, gets information, she changes the distribution of the key. This introducing errors in the correlations between the sender and receiver. Eve measurement modifies the state itself [20]. In the current technology, no single-photon devices are available; the best option in quantum key distribution system substitute's single-photon source in QKD BB84 protocol by heavily attenuated laser pulses, these sources obey Poisson distribution, as shown in Figure 1 [17]. Poisson distribution for several values of mean photon number μ of Figure 1(a) 0.1, Figure 1(b) 1, Figure 1(c) 5, and Figure 1(d) 10. These sources have pulses traveling from sender to receiver contain more than one photon, opening the door for a weakness in system security [21]. Heavily attenuated laser pulses source output enables eavesdropper to share some information through a PNS attack.



(a) (b)

(c) (d)

Figure 1. Poisson distribution for several values of mean photon number μ of (a) 0.1, (b) 1, (c) 5, and (d) 10

In this paper, the security of a QKD system has been enhanced by applying decoy states protocol against photon PNS. By randomly interleaving fake states (decoy states) with mean photon numbers of 5.38, 1.588, and 0.48 within the transmitted signal of 2.69, 0.794, and 0.24 mean photon numbers, a PNS has been detected and a secure key has been gotten. The signal states and decoy states were compared to check the efficiency of the system and detect the PNS attack. The average length for a secure key obtained from our system, which ignores eavesdropping cases, is 125 with 20% decoy states and 82 with 50% decoy states.

The paper is organized as: sections 2 and section 3 give a brief description of the PNS attack strategy and main concepts of the decoy-state protocol. Sections 4 and section 5 detail the experimental work and results. Finally, the conclusion is given in section 6.

2. PHOTON NUMBER SPLITTING ATTACK

PNS is a quite powerful attack described by Lütkenhaus. By using attenuated laser pulses instead of the ideal single-photon as the source in BB84 QKD systems, the distribution of photons is as follows. The pulses with no photons decrease the signal rate since no signal will be detected by Bob. The pulses with single PNS is a quite powerful attack described by Lütkenhaus. By using attenuated laser pulses instead of the ideal single-photon as the source in BB84 QKD systems, the distribution of photons is [22]:

- The pulses with single-photon work perfectly.
- The pulses with multi-photons are the problematic part. They have more than one copy of the polarization information, allowing Eve to split off a copy of the information without Alice and Bob knowing it.

- The pulses with multi-photons are the problematic part. They have more than one copy of the polarization information, allowing Eve to split off a copy of the information without Alice and Bob knowing it.

In the PNS attack, Eve knows the number of photons on each signal sent by Alice without disturbing its polarization by a quantum non-demolition measurement. Eve works on the signal depending on the total number of photons. More precisely, the existence of multi-photon signals permits Eve to execute the PNS attack. Photon work perfectly.

- When Eve finds empty pulses, she sends them back to Bob without further errors.
- When she finds the pulses with multi-photons, she steals one photon and retains it in her memory and sends the remainder to Bob. When Eve sends a reminder to Bob, the original lossy quantum channel may be replaced by a lossless channel. Eve's does not change the signal polarization either in the photon she sends on nor in the photon she splits off. Subsequently, in the protocol Alice will announce the basis of the polarization of the signal. This will allow Eve to make the correct measurement on the photon she split off, thus getting perfect information about the polarization of Alice's signal.
- When it is one photon, she just blocks it.

3. DECOY STATE PROTOCOL

The protocol of decoy-state has been proposed for detecting PNS attack, improving transmission distance and rate of the generated secure key of the QKD system [7]. By applying the protocol of decoy-state, Alice implements a BB84 protocol with mean photon number of the signal source (μ_s) and replaces randomly with a mean photon number μ_d (decoy-source). Eve cannot modify the transmission of the channel for more than one value of mean photon number (μ) simultaneously. Eve treats single-photon signals from μ_s or μ_d identically because she does not know which one of μ is Alice used. Bob sends an acknowledgement of receipt of signals then Alice broadcasts pulses of signal states and pulses of decoy states. The rate of single-photon signals differ for each μ, so Alice and Bob analyze separately the QBER of signal and decoy-state, since all characteristics of signal state and decoy-state are similar except μ. The number of detection events from μ_s and μ_d transmissions will be compared to give an estimation bounds of the single-photon transmitted on the channel. PNS attack will be caught because of the modification in the QBER of the system or transmittance characteristics of decoy states and/or signal states. Decoy states are fake states used only for catching an eavesdropper, but not for a key generation [23]. In decoy protocol, let's assume that heavily attenuated laser pulses source contains a single photon with a 90% probability, then multi-photons with a probability of 10% generated randomly, the problem is not known when the multi-photon pulses have been emitted. Let the channel loss (ℓ) equal to 90%, then it has a 10% yield (Q).

$$Q = 1 - \ell \tag{1}$$

By calculating the yield of decoy source, the eavesdropper can be detected. If attenuated laser pulses are used as a source in the QKD system, the fraction of multiphoton counts is called the fraction of tagged photons (Δ). It is a crucial value. Decoy-state protocol improved by Hwang [24] is an important method for the unconditional security of QKD with attenuated laser pulses to verify the upper bound of Δ. The verified upper bound of Δ in case of no eavesdropping is given by [25].

$$\Delta = \frac{\mu_s e^{-\mu_s}}{\mu_d e^{-\mu_d}} \tag{2}$$

By neglecting the pulses which had no light ($\mu_0 = 0$), Δ is given by:

$$\Delta \leq \Delta_i = \frac{\mu_s}{\mu_{d-\mu_s}} \left(\frac{\mu_s\, e^{-\mu_s}\, Q_d}{\mu_d\, e^{-\mu_d}\, Q_s} - 1 \right) \tag{3}$$

Where:
Δ_i = minimum value of tagged photon for the PNS attack.
Q_s = detection probability of signal pulses.
$Q_s = \frac{no.\ of\ signal\ detections}{no.\ of\ signal\ states}$
Q_d = detection probability of the decoy pulses.
$Q_d = \frac{no.\ of\ decoy\ detections}{no.\ of\ decoy\ states}$
The flowchart shown in Figure 2 represents decoy state protocol.

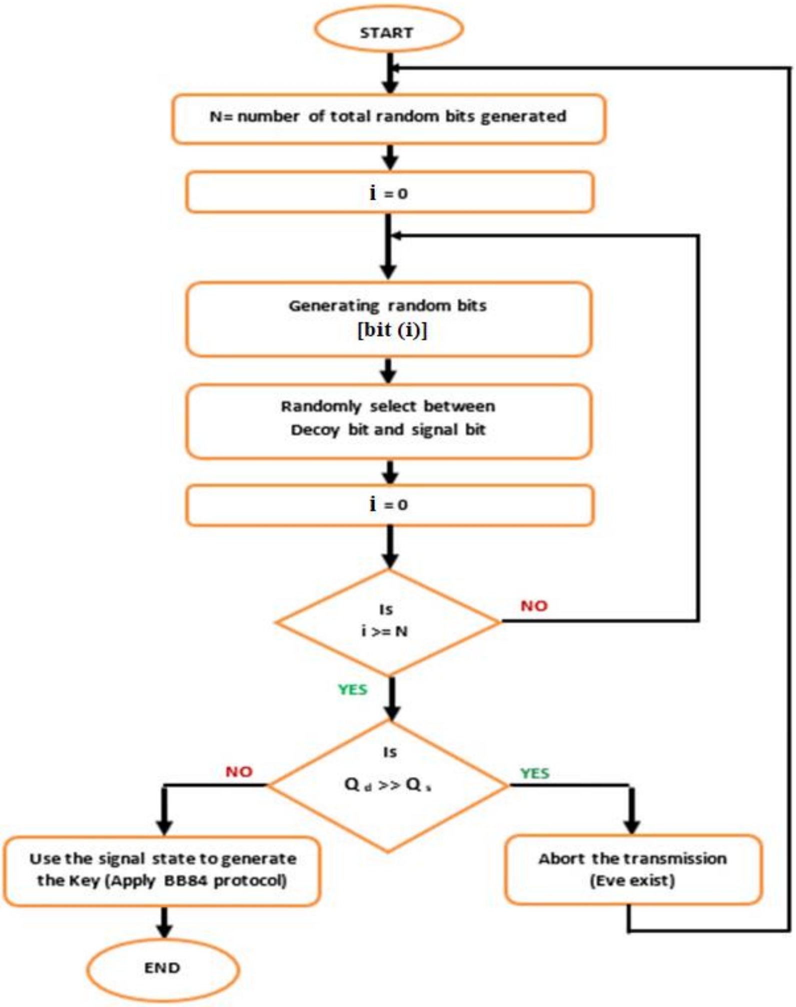


Figure 2. Block diagram of the BB84 protocol with decoy-state

4. EXPERIMENTAL WORK AND RESULTS

Figure 3 and Figure 4 show block diagram and experimental set up of our implemented QKD system based on the BB84 protocol. The transmitter side of the system has four laser diodes that are connected to personal computer (PC) through driver circuits. Trigger signals generated by PC, shown in Figure 5(a), fed driver circuits to generate an electrical signal that is used to operate each laser diode. Signal-states are emitted by running one laser diode randomly during one loop of program execution. The value of μ in the system was controlled by reducing the intensity of the optical signal emitted from each laser diodes by using optical filters shown in Figure 5(b). Decoy-states (fake states) are produced by deriving two laser diodes concurrently, as shown in Figure 6. Decoy-states are interleaved randomly between the signal states within the four laser diodes operating loop of the system. The pulse duration for the electrical signal that is used to operate laser diodes was 200 ns at 11 kHz. The system was running with the BB84 protocol with and without decoy states. The numbers of total random bit generated from PC was equal to N = 30000. A comparison between these two cases was accomplished in order to detect a PNS attack. A program is written in MATLAB R2015a in order to analyze the results of the comparison. In this system, eavesdropping is checked for two types of decoy-states, 1-state decoy, i.e. (20%), and 4-states, i.e. (50%). For each type, two laser diodes were operated simultaneously. The beam splitter (PNS) was applied for all measurements. In the receiver side, for single-photon avalanche photodiode (APD) operating in Geiger mode, two excess voltage were used (V_E = 5 V and V_E = 7 V) at temperature -11 ºC. Figure 7 shows the tests carried out for APD counts when one laser diode (LD) on (signal-states) Figure 7(a) and two LDs on (decoy-states) Figure 7(b). BB84 protocol including privacy amplification stages and error correction was applied to obtain the final key. Keys were extracted for QBER less than 15%. The tests are listed in the diagram shown in Figure 8.

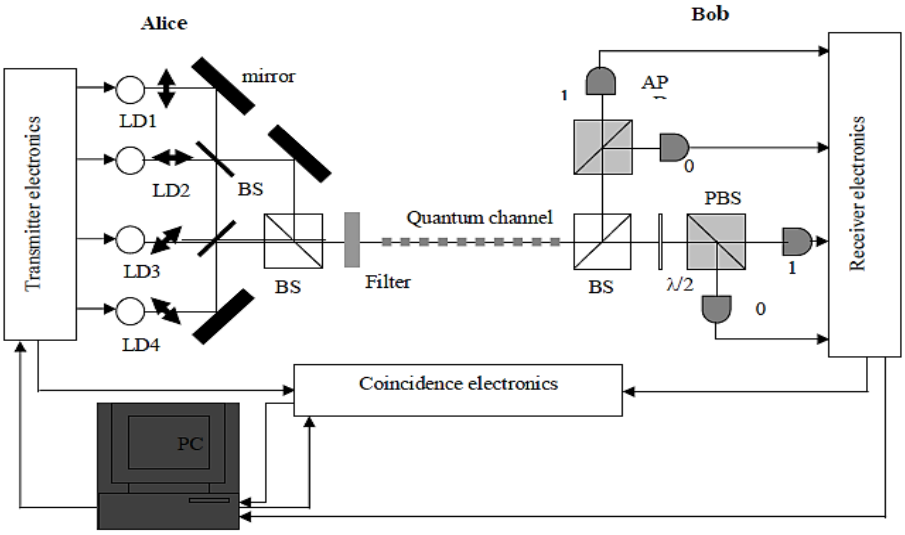


Figure 3. Quantum key distribution system for the BB84 protocol

LD: laser diode, BS: beam splitter, PBS: polarizing beam splitter, APD: avalanche photodiode, $\lambda/2$: half-wave plate, and PC: personal computer.

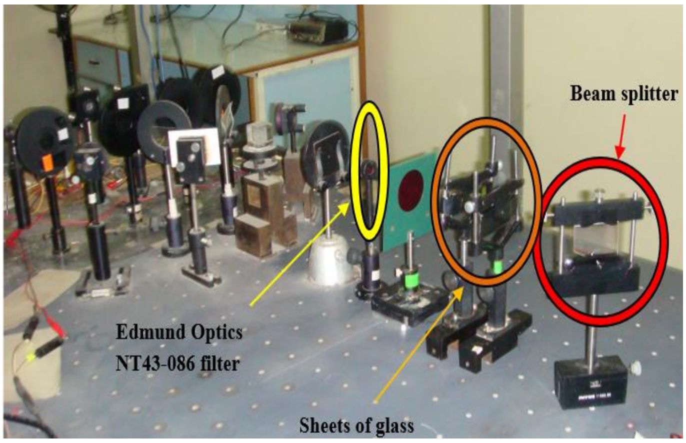


Figure 4. The setup of quantum cryptography system in the lab

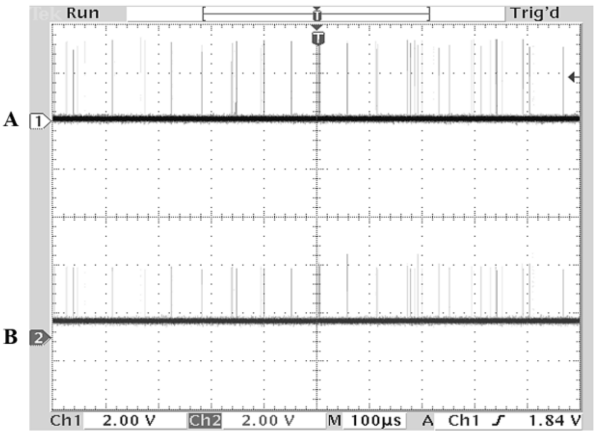


Figure 5. PC signals and triggering signals for LD1: (a) PC signals and (b) firing pulse

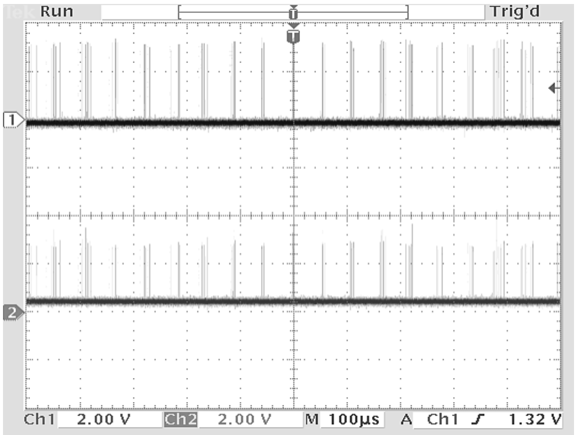
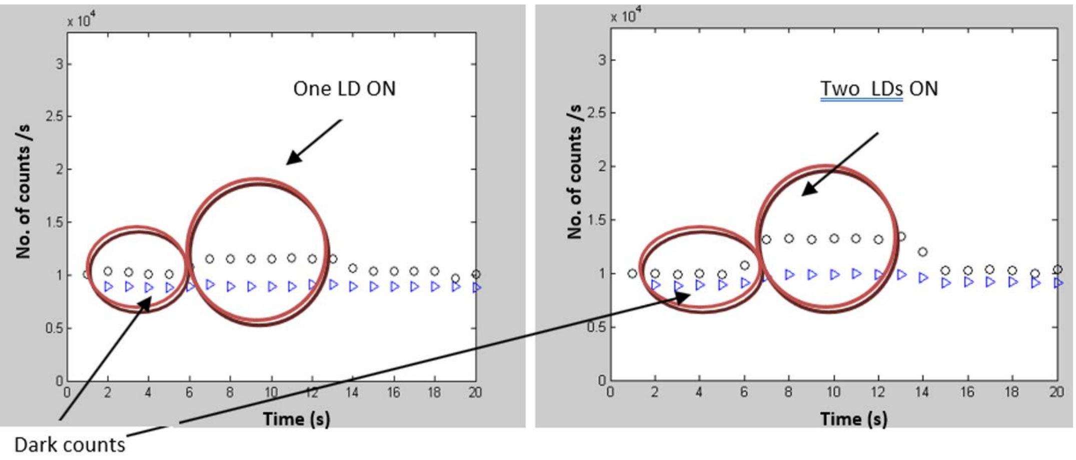


Figure 6. Decoy states pulses



(a) (b)

Figure 7. Number of counts as a response for: (a) one LD on (signal states) and (b) two LDs on (decoy states)

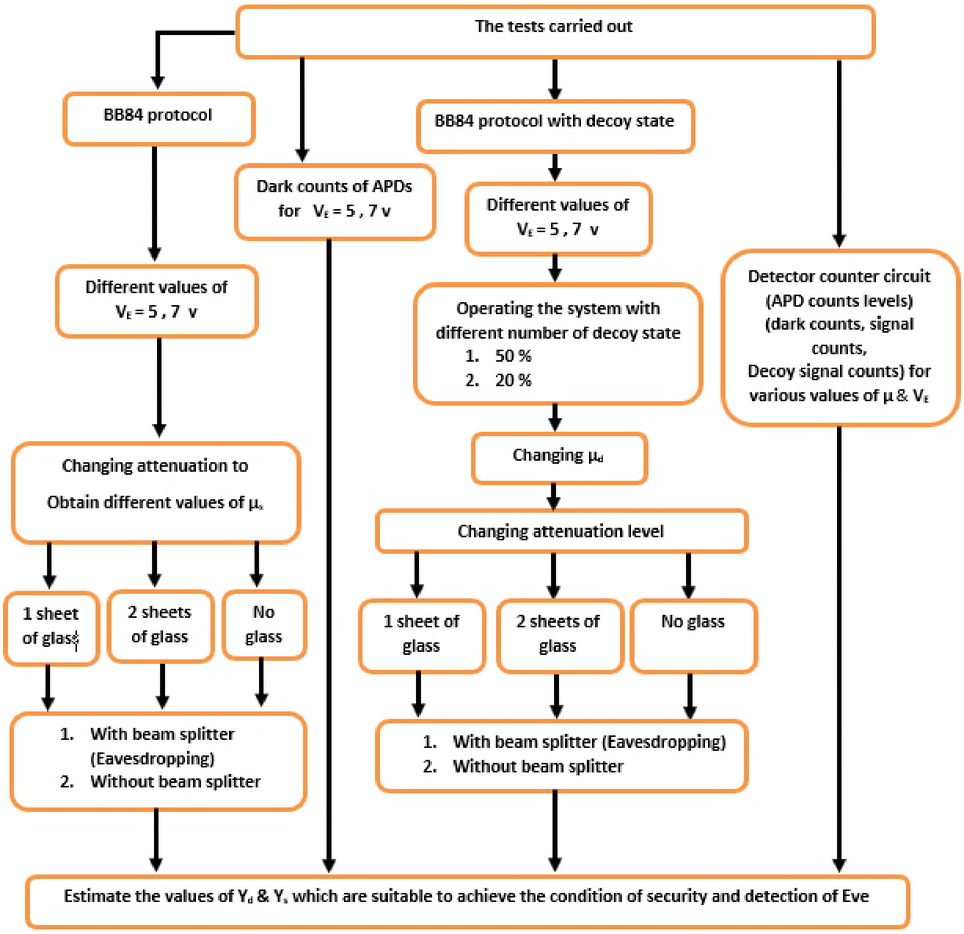

The tests carried out
BB84 protocol
Dark counts of APDs for V_E = 5 , 7 v
BB84 protocol with decoy state
Different values of V_E = 5 , 7 v
Different values of V_E = 5 , 7 v
Operating the system with different number of decoy state
1. 50 %
2. 20 %
Detector counter circuit (APD counts levels) (dark counts, signal counts, Decoy signal counts) for various values of μ & V_E
Changing attenuation to Obtain different values of μ_s
Changing μ_d
Changing attenuation level
1 sheet of glass
2 sheets of glass
No glass
1 sheet of glass
2 sheets of glass
No glass
1. With beam splitter (Eavesdropping)
2. Without beam splitter
1. With beam splitter (Eavesdropping)
2. Without beam splitter
Estimate the values of Y_d & Y_s which are suitable to achieve the condition of security and detection of Eve

Figure 8. Measurements and calculations block diagram

Tables 1 and Table 2 show the average values of final key length with PNS attack for two voltage values V_E = 5 V, 7 V and without PNS attack for V_E = 5 V,7 V and for (μ_s = 0.24) by applying high attenuation on the transmitted signal and (μ_s = 0.794) with less attenuation respectively. The results give for 20% and 50% decoy states.for high attenuation (μ_s = 0.24) the un appropriate to the system, while by using (μ_s = 0.794) secure keys have been obtained.

Table 1. Average values of the final key lengths with and without PNS attack for V_E = 5 V, 7 V and μ_s = 0.24

V_E/V	Average final un attacked key length		Average final attacked key length	
	20% decoy states	50% decoy states	20% decoy states	50% decoy states
5	83	65	76	46
7	96	55	77	47

Table 2. Average values of the final key lengths with and without PNS attack for V_E = 5 V, 7 V and μ_s= 0.794

V_E/V	Average final un attacked key length		Average final attacked key length	
	20% decoy states	50% decoy states	20% decoy states	50% decoy states
5	125	82	104	64
7	140	80	132	63

5. CONCLUSIONS

From our work the maximum average secure key length obtained was equal to 125 with 20 % decoy states and 82 with 50% decoy states which is considered to be short with maximum key length of 388 which was obtained from the same system by applying the BB84 protocol without decoy states. But the security of key is not guaranteed as far as the presence of Eve was not tested. The results obtained with, APD temperature = -11 ºC and distance = 85 cm, the best values of μ to give secure key with QBER < 15% satisfying $\Delta< \Delta i$ is (μ_s = 0.794) for both cases of using 20% and 50% decoy states with BB84 protocol with V_E = 5 V.

REFERENCES

[1] N. A. Al-Shareefi, S. A. Abbas, M. S. Alkhazraji, and A. A. R. Sakran, "Towards secure smart cities: design and implementation of smart home digital communication system," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 21, no. 1, pp. 271–277, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp271-277.

[2] N. A. Al-Shareefi, J. Aldhaibaini, S. Abbas, and H. Obaid, "Comparison of Three Different EOU Techniques for Fifth-Generation MM-W Wireless Networks," *Iraqi Journal for Computers and Informatics*, vol. 45, no. 2, pp. 9-14, 2019, doi: 10.25195/ijci.v45i2.47.

[3] T. Iwakoshi, "On problems in security of quantum key distribution raised by Yuen," *Proceedings Quantum Information Science and Technology III*, 2017, vol. 10442, doi: 10.1117/12.2278625.

[4] K. Tamaki, M. Curty, and M. Lucamarini, "Decoy-state quantum key distribution with a leaky source," *New Journal of Physics*, vol. 18, pp. 1-24, 2016, doi: 10.1088/1367-2630/18/6/065008.

[5] H. P. Yuen, "Fundamental quantitative security in quantum key generation," *Physical Review A*, vol. 82, 2010, doi: 10.1103/PhysRevA.82.062304.

[6] H. P. Yuen, "Universality and The Criterion d in Quantum Key Generation," *arXiv*, 2009. [Online]. Available: https://arxiv.org/abs/0907.4694

[7] S. Ali, S. Saharudin, and M. R. B. Wahiddin, "Quantum key distribution using decoy state protocol," *American Journal of Engineering and Applied Sciences*, vol. 2, no. 4, pp. 694-698, 2009. [Online]. Available: https://thescipub.com/pdf/ajeassp.2009.694.698.pdf

[8] H. -K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical review letters*, vol. 94, 2005, doi: 10.1103/PhysRevLett.94.230504.

[9] H. -K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, 2012, doi: 10.1103/PhysRevLett.108.130503.

[10] B. Hensen *et al.*, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, pp. 682-686, 2015, doi: 10.1038/nature15759.

[11] M. Giustina *et al.*, "Significant-loophole-free test of Bell's theorem with entangled photons," *Physical review letters*, vol. 115, 2015, doi: 10.1103/PhysRevLett.115.250401.

[12] L. K. Shalm *et al.*, "Strong Loophole-Free Test of Local Realism," *Physical review letters*, vol. 115, 2016, doi: 10.1103/PhysRevLett.115.250402.

[13] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier," *Physical review letters*, vol. 105, 2010, doi: 10.1103/PhysRevLett.105.070501.

[14] M. Curty and T. Moroder, "Heralded-qubit amplifiers for practical device-independent quantum key distribution," P*hysical Review A*, vol. 84, 2011, doi: 10.1103/PhysRevA.84.010304.

[15] N. A. Al-Shareefi, J. A. Aldhaibaini, S. A. Abbas, and H. S. Obaid, "Towards 5G millimeter-wave wireless networks: a comparative study on electro-optical upconversion techniques," vol. 20, no. 3, pp. 1471-1478, Dec. 2020, doi: 10.11591/ijeecs.v20.i3.pp1471-1478.

[16] Y. Zhao, C. -H. F. Fung, B. Qi, C. Chen, and H. -K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Physical Review A*, vol. 78, 2008, doi: 10.1103/PhysRevA.78.042333.

[17] N. A. Al-Shareefi, S. I. S. Hassan, F. Malek, R. Ngah, and S. A. Abbas, "Optical Generation of 60 GHz Downstream Data in Radio over Fiber Systems Based on Two Parallel Dual-Drive MZMs," *International Journal of Engineering and Technology (IJET)*, vol. 6, no. 2, pp. 579-587, 2014. [Online]. Available: https://www.enggjournals.com/ijet/docs/IJET14-06-02-026.pdf

[18] N. A. Al-Shareefi and A. A. Sakran, "A novel optimal small cells deployment for next-generation cellular networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, pp. 5259-5265, 2021, doi: 10.11591/ijece.v11i6.pp5259-5265.

[19] A. Gaidash, V. I. Egorov, and A. V. Gleim, "Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices," *Journal of Physics: Conference Series*, 2016, vol. 735, doi: 10.1088/1742-6596/735/1/012072.

[20] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita, "Security analysis of decoy state quantum key distribution incorporating finite statistics," *arXiv*, 2007. [Online]. Available: https://arxiv.org/abs/0707.3541

[21] A. Niederberger, V. Scarani, and N. Gisin, "Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography," *Physical Review A*, vol. 71, 2005, doi: 10.1103/PhysRevA.71.042316.

[22] X. Ma, "Quantum cryptography: from theory to practice," *arXiv*, 2007. [Online]. Available: https://arxiv.org/pdf/0808.1385.pdf

[23] D. Rosenberg *et al*., "Long-distance decoy-state quantum key distribution in optical fiber," *Physical review letters*, vol. 98, 2007, doi: 10.1103/PhysRevLett.98.010503.

[24] W. -Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, 2003, doi: 10.1103/PhysRevLett.91.057901.

[25] X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," *Physical Review A*, vol. 72, 2005, doi: 10.1103/PhysRevA.72.012322.

BIOGRAPHIES OF AUTHORS

Sura Adil Abbas received the Bachelor of electronic and communication engineering from University of Baghdad /collage of engineering /department of electronic and communication engineering / Iraq / Baghdad/ Aljaderiyah, in 2005. The Masters. Degree in electronic and communication engineering from University of Baghdad/institute of laser for postgraduate studies / Iraq / Baghdad / Aljaderiyah, in 2011. She is currently working as an assistant teacher at Department of Communication and Mobile Computing Engineering, faculty of Engineering, University of Information Technology and Communications (UOITC), Baghdad, Iraq. She can be contacted at email: sura.adel@uoitc.edu.iq.

Nael A. Al-Shareefi received the B.Sc. degree in electronic and communications engineering and the M.Sc. degree in communications engineering from the University of Technology, Baghdad, Iraq, in 1999 and 2001, respectively, and the Ph.D. degree in communications engineering from Universiti Malaysia Perlis (UniMAP), Malaysia, in 2014. Since 2019, he has been working as the Head of the Intelligent Medical Systems Department, College of Biomedical Informatics, University of Information Technology and Communications (UOITC), Baghdad. His research interests include 60-GHz millimeter-wave generation, radio-over-fiber, optical fiber communications, and fifth generation of mobile networks. He received an Associate Professorship at University of Information Technology and Communications (UOITC), Baghdad, in 2020. He can be contacted at email: dr.nael.al_shareefi@uoitc.edu.iq.