IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 13, 2018, accepted August 9, 2018, date of publication August 28, 2018, date of current version September 21, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2866554

Evaluation of Parameters Effect in Multiphoton Quantum Key Distribution Over Fiber Optic

NUR ZIADAH HARUN[1,2], ZURIATI AHMAD ZUKARNAIN[1], (Member, IEEE), ZURINA MOHD HANAPI[1], (Member, IEEE), AND IDAWATY AHMAD[1]

[1]Faculty of Computer Science and Information Technology, University Putra Malaysia, Seri Kembangan 43400, Malaysia
[2]Department of Information Security, Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Parit Raja 86400, Malaysia

Corresponding authors: Nur Ziadah Harun (ziadah.harun@gmail.com) and Zuriati Ahmad Zukarnain (zuriati@upm.edu.my)

This work was supported by the Putra Berimpak Grant, University Putra Malaysia.

ABSTRACT BB84 is a single photon that has been widely used since 1984 as the unconditional security of key distribution. Recently, the idea of multiphoton QKD was proposed to exchange the key using the rotational of polarization by over multi-stages protocol. By utilizing the state of polarization, the system does not require one of the four states like it did in the BB84 scheme. The multiphoton has the ability to improve the key rate generation and range of distances as well. Indeed, multiphoton QKD needs to be setup properly to gain the optimal performance over the fiber optic. This paper presents the fundamental implementation of multi-stages and multiphoton approach over the fiber optic by applying secret unitary transformation between Alice and Bob. The step by step operation of unitary transformation is applied using half-wave plates represented as Mueller matrix. This paper also evaluates the effects of parameters in the QKD model. The result reveals that channel loss, dark count rate, detector efficiency, photons' repetition rate, and the average number of photons will affect the QBER and SKR.

INDEX TERMS Half wave plate, mean photon number, multistage, QBER, single photon, secret key rate.

I. INTRODUCTION

Quantum cryptography is a technique which relies on the quantum physics law and the security guarantee does not depend on the computing power [1]. It is also strengthened by the unconditional security as proved by the Heisenberg Uncertainty theory and no-cloning theorem [2]. The quantum state is called as qubit which is the smallest particle unit in quantum information. Heisenberg Uncertainty theory defines that the intruder cannot know the properties of the quantum states without disturbing it while no-cloning theorem theory defined that the unknown quantum states cannot be copied. On the other words, the key generated are guaranteed by the quantum mechanics law. The sender and receiver will notice when an eavesdropper intercepts their communication due to the changes in properties of qubit [3].

Quantum computation gives an excellent solution for energy consumption and heat production. As an example, Shor algorithm, one of the well-known quantum algorithm able to decrypt RSA algorithm in one second while it took about 13 months to decrypt it using a desktop with 4 cores at 2.8 GHz [4]. In addition, the Grover algorithm specifically invented by Lov Grover in 1996 for search and optimization is able to solve the problem of data searching using only 32 comparisons in the 1024 dataset while DES & AES need 1023 comparisons [5]. According to the report in the NIST [6], it is expected that when the quantum technology is fully implemented, most of the cryptographic algorithms such as RSA and Elliptic Curve Cryptography are going to be insecured.

II. THE BASIC OF QUANTUM KEY DISTRIBUTION

Quantum Cryptography or QKD is defined as the behavior of key exchanged using photon for the encryption of sensitive information between parties in the network [1]. The key generated by the QKD can be used by conventional cryptography such as Data Encryption Standard (DES) and Advance Encryption Standard (AES) to enhance the level of security [1], [2]. QKD applies the theory of quantum physic by producing random secret key using a photon to gain communication security between two parties. The quantum physic can be interpreted based on state the bra (|) and ket (>) notation. The mapping from classical bit to qubit can be written as:

$$0 \rightarrow |0> \quad 1 \rightarrow |1> \tag{1}$$

The superposition states can be defined as:

$$|\Psi> \equiv \alpha|0> + \beta|1> = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad (2)$$

Where Ψ is the superposition states, $|0>$ and $|1>$ are qubits states, and α and β are the complex numbers. The $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ is a two dimensional vector, where $|0>$ equals to $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1>$ equals to $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. The probability of α and β coefficients can be satisfied by

$$|\alpha|^2 + |\beta|^2 = 1 \quad (3)$$

where $|\alpha|^2$ is the probability of obtaining $|\Psi>$ in $|0>$ and $|\beta|^2$ is the probability of obtaining $|\Psi>$ in $|1>$.

The transmission of a photon occurs through the quantum channel while the transmission of the data is through public channels such as radio frequency channels and the Internet. The first device using quantum technology was implemented by a physicist named Stephen Wiesner in 1969, followed by Bennet and Brassard whom then proposed a technique which is known as BB84 in 1984. Nowadays, many variants of QKD have been proposed by the researchers to match with the environment and the behaviour of the networks. Generally, the QKD can be implemented in the optical fiber, free space as well as under water channel.

TABLE 1. The comparison of single photon and multiphoton approaches.

Characteristics	Multiphoton	Single photon
Photon per pulse	More than one photon	One photon
Polarization	Any polarization angles	90º, 0º, 45º, -45º
Theory	Heisenberg uncertainty Measuring the state of photon polarization with a fewer number of photons than needed will generate noise	No cloning theorem Copy of photon cannot be generated with accuracy
Mean photon number	≥ 1	≤ 1
Eve's intervention ability	Hard for Eve to identify the angle of the multi-stage polarization but easier for Bob to distinguish between two orthogonal polarization angle.	Easy for Bob and Eve to get the probabilities of four polarizations

III. QUANTUM COMMUNICATION PROTOCOL

There are two types of quantum communication protocol, which are single photon and multiphoton approaches. The type of communication protocol can be determined by the emission of photons using the laser source. Recently, a few multiphoton protocols have been successfully performed [3]–[7]. To differentiate the ability of multiphoton and single photon approaches, Table 1 compares their characteristics in terms of the polarization states, the theories proven and the ability of Eve intervention.

A. SINGLE PHOTON APPROACH

Single photon representing a photon is transmitted per laser pulse. The best example of a single photon is the BB84 protocol. BB84 consists of one-time pad technique, where the random key is equal to the transmitted message and the key is only used once [5]. The basic idea of BB84 protocol is when a sender wants to exchange secret keys with the receiver, the sender needs to send the classical bit 0 and 1 using a polarizer [18] through the quantum channel. The polarizer is a device which is responsible to do the polarization by converting the bit into quantum states known as a qubit. The states of qubits are dependent on the polarization of photon to get the specific spins which consist of vertical, horizontal, diagonal and anti-diagonal [19] to represent the bits as shown in Table 2.

TABLE 2. Photon polarization.

Spin	Vertical	Horizontal	Diagonal	Anti-diagonal
State	90º	0º	45º	-45º
Qubit	↑	→	↗	↖
Bit	1	0	0	1

The generation of the secret key using single photon approach is based on the similarities of the qubits received by Bob and the qubits sent by Alice. The final key agreement is done after key reconciliation process, with the acceptable percentage of QBER. The disturbance of the qubits can only be detected when Eve chooses a different basis from Alice. Thus, the receiver will be notified of the presence of intruder by the detection of photon disturbances through the calculation of QBER. The key will be accepted as the final secret key if the QBER is below than the certain threshold. Otherwise, the process of key generation should be repeated again. The existing QKD such as BB84 is susceptible to Man-in-the-Middle as Eve might be able to take the advantage of the loopholes in the quantum devices. Eve could impersonate as Alice or Bob during the qubit transmission in quantum and classical channels.

The emission of a single photon per pulse from the laser source will limit the number of photons travelled over the quantum channel. In addition, it is quite difficult to get one photon for each laser pulse. The transmission rate for a single photon is low due to a large number of empty pulses. Besides, the single photon is susceptible to the siphoning attack which is also known as PNS attacks that exploit multiple photons emitted accidentally by the attenuated laser source. An eavesdropper will capture a single photon from multiple photons and try to guess the polarization state without disturbing the channel, while the remaining photons will be transmitted to Bob. Since the mean photon number emitted by the laser source is 1 or less, this technique is only suitable for limited distances of communication. It is difficult to ensure that the transmission of a single photon would survive over the channel since there were many errors occurred such as the

disturbance of the networks and the distraction by the eavesdroppers. Otherwise, the practical implementation of a single photon using attenuated laser will result in the probability of more than one photon emitted and makes the protocol unsecured with eavesdropping attacks. The single photon only exchanges one direction over quantum networks and needs the classical channel to acknowledge the polarization base. The involvement of classical channel will introduce a security breach in the communication. In addition, the security breach at the device level will still occur even though the QKD is a widely known unconditional security. To counter back the limitations, it is suggested to implement the single photon QKD technique with another method such as decoy state [8]–[10] to strengthen the robustness of security.

B. MULTIPHOTON APPROACH

The emission of multiple photons per laser pulse is called as multiphoton approach. The implementation of single photon approaches such as BB84 protocol and decoy state BB84 derivatives are vulnerable to PNS attacks because it is impossible for the photonic devices to generate single photon periodically as the time slots may contain less number of photons [21]. It is claimed that multiphoton can provide long photon travelling distance and high transmission rates while single photon is not capable of doing so because it relies on the weak attenuated laser source. The weak photons are more vulnerable to the noise in wireless environment. Multiphoton solves the problem of noise sensitive and complicated photon detector usage, such as homodyne and heterodyne detection. Therefore, a less efficient detector might be applicable to be used in the multiphoton protocol. Besides, the multiphoton approach with multiple number of stages were invented to address the problem of security threats such as Man in the Middle attack, Photon Splitting Number and Trojan Horse attacks that might happen in single photon approach. The current multiphoton does not involve public channel to exchange keys and the process is done through the quantum channel. Basically, the origin idea of multiphoton protocol was implemented for Quantum Secure Direct Communication (QSDC) protocol which directly shares the message over the quantum channel without using the step of key distribution [8], [9]. The idea of the multiphoton QKD [5], [7] is to exchange the key using the rotational of polarization over multi-stages protocol. The implementation of multiphoton QKD is rather simple to the maintained network infrastructure. By utilizing the state of polarization, the system does not require to produce one of the four states like in the BB84 scheme. In fact, it will produce arbitrary state of polarization which is able to avoid the Man-in-the-Middle attack. The rotation operator for polarization [13] state can be described as:

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \tag{4}$$

Alice and Bob will apply the secret unitary transformation U_A and U_B where $U_A U_B = U_B U_A$. The values of rotation operator are $U_A = R(\theta)$ and $U_B = R(\Phi)$, where $R(\theta) = R(\Phi)$.

The operation of unitary transformation is applied using half-wave plates represented as Mueller matrix [6], [14], given by:

$$M_{HWP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4\theta) & \sin(4\theta) & 0 \\ 0 & \sin(4\theta) & -cos(4\theta) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{5}$$

where the value of θ is $0° < \theta < 180°$.
The state of the qubit is represented as a column vector and can be computed by:

$$|X> = |a> \otimes |b> \tag{6}$$

where $\otimes$ is the tensor product between two states $|a>$ and $|b>$ as shown in Table 3.

TABLE 3. Representation of qubits.

Message, X			
$\|00> = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$	$\|01> = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$	$\|10> = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$	$\|11> = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$

1) THE SINGLE STAGE PROTOCOL

Single stage protocol is the simplest multi-photon approach where the transformation of photon happens in a stage. If Bob knows the value of θ, he may directly apply U'_A on the encoded message $U_A(X)$ to obtain the value of X as illustrated in Fig. 1. The security strength of this protocol depends on the secret value of θ and it must be secret along the communication between Alice and Bob. Unfortunately, when the eavesdropper able to get the value of θ, the security of this protocol cannot be compromised anymore.

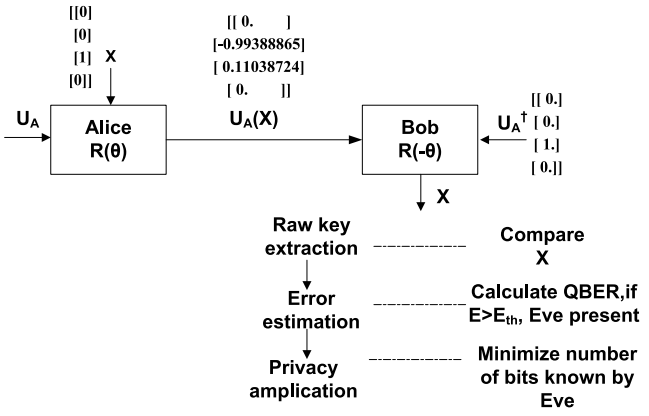

FIGURE 1. The Single Stage operation.

2) THE THREE STAGE PROTOCOL

Currently, the most well-known multi-photon QKD is known as Three-Stage Quantum Cryptography protocol, which is inspired from [12] as shown in Fig. 2. This protocol aims to

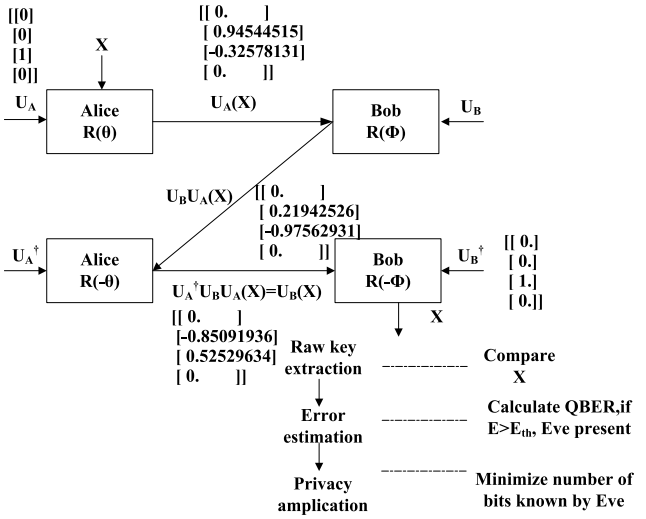

FIGURE 2. The Three Stage protocol operation.

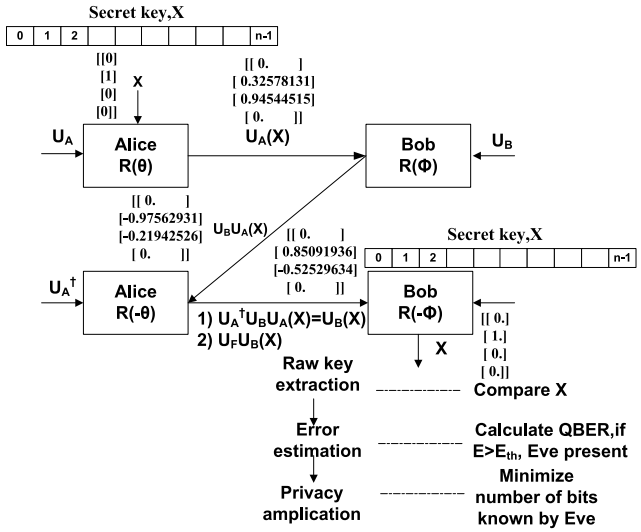

FIGURE 3. The Three Stage protocol using four variable operation [5].

improve the speed of photon transmission and increase the limit of the distance of quantum communication. Apart from that, the multi stages step during the qubit sharing is to make the transmission channel more secure making the Eavesdropper difficult to guess the state of the qubits. This protocol is suggested to be implemented for free space network such as 802.11 WLAN networks and it is expected to be tested in the bigger wireless network environment.

3) THE THREE STAGE PROTOCOL USING FOUR VARIABLES

The three stage protocol is one of the multiphoton approaches [2] that applies the commutative transformation with the feature of the Initialization Vector (IV) in one of the three stages [10]. When Eve knows the state of polarization of each stage, she can access the actual message being sent by solving the set of equations in the three stages. Thus, four variables using α, β, X, and F were introduced in this protocol, where α is the transformation by Alice, β is the transformation by Bob, X is the information or message and F is the IV as shown in Fig. 3. The security strength of this protocol relies on IV. Even if Eve is able to know the polarization angle of each state, she will still need to know the value of IV to decode the messages. Thus, the IV helps to protect the information under the attack of an intruder.

4) THE BRAIDED SINGLE STAGE PROTOCOL

The most well-known dynamic quantum session key is Braided Single-stage protocol [15], which is classified under the multiphoton approach. This protocol does not only reduces the percentage of overhead but also reduce the level of complexity as the photon needs only one-time travel over the channel. This protocol is based on the single stage to encode the qubits. The operation of this protocol does not rely on just one secret value of θ. The new value of θ is updated from the previously transmitted bits and the θ value. After a block of bits received by the receiver, the value of initial θ is

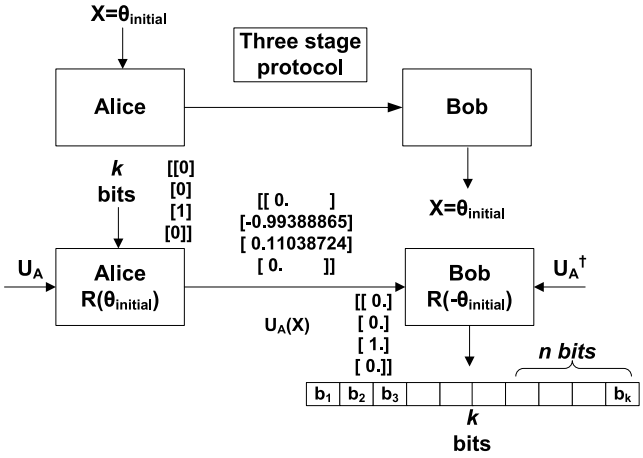

FIGURE 4. The Braided Single stage protocol operation [11].

changed to another value. The new θ is calculated and every transmission of last four bits will be updated. The operation of Braided Single stage protocol is shown in Fig. 4. It has been proven that this protocol gains efficient resource consumption and preserves the degree of security even when number of stages have been reduced.

Multi stages are one of the methods of the photon to transmit between sender and receiver to ensure that the eavesdropper faces difficulties to guess the polarization of the photon where the qubits are exchanged multiple times at multi stages. Apart from that, multi stages will improve the number of a photon emitted by the sender. Unfortunately, multi stages of photons transmission will contribute to the increment of overhead at the sender and the receiver will loss of beam light. To overcome the limitation, the optimum number of polarization stages is needed to ensure that the optimal number of a photon emitted by the sender and at the same time, the receiver will capture all the photons received. The

TABLE 4. A comparison of multi-photon algorithm.

Protocol	Number of stages	Variables	Strength	Level of security
Single Stage	1	α, X	Depends on the secrecy of θ at single stage.	Low
Three Stage	3	α, β, X	Depends on the secrecy of θ at three stages.	Low
Three stage using four variables	3	α, β, X, F	Eve need to know F to solve X.	Intermediate
Braided Single Stage	1	α, X	The value of θ will be changed based on *n* bits and previous θ value.	High

increasing number of stages will significantly make Eve hard to get the properties of a photon. However, too many stages will consume more overheads which means more photons are needed to travel over the channels. Table 4 compares the multi-photon algorithm in terms of number of stages and the strength of each implementation.

IV. FIBER OPTIC QKD MODEL

The performance of multiphoton QKD is evaluated using Secret Key Rate and Quantum Bit Error Rate. SKR can be defined as the probability of receiving a bit of secret key per transmitted quantum signal pulse [16]. SKR consists of two portions, R and r [2], [12]. R is represented as a raw key rate while r is secret fraction.

$$K = Rr \tag{7}$$

The term R is for error correction, in which the raw key becomes shorter and key is correlated. The second one is r for privacy amplification and is aimed to remove Eve's knowledge about the raw keys [17]. The first term is given by

$$R = vsP_{Bob}\left(N_{max}\right) = vs\sum_{n=1}^{Nmax} p_A\left(n\right)\left[1-\left(1-\eta det\,\eta qc\right)^n\right] \tag{8}$$

where vs is the repetition rate and $P_{Bob}\left(N_{max}\right)$ is Bob detection probability. The distribution number of photon n until maximum number of photon, $Nmax$ was calculated according to the Poissonan statistic of $\mu = \langle n\rangle$, $p_A\left(n\right)$ is photon number distribution, given by

$$p_A\left(n\right) = \frac{\mu^n}{n!}e^{-\mu} \tag{9}$$

The typical values of detector efficiency, ηdet is 10% at telecom wavelength. Attenuation in fiber, ηqc is calculated with distance D, showed by Equation (10).

$$n_{qc} = 10^{\frac{-\alpha D}{10}} \tag{10}$$

To formulate the secret fraction in order to extract short key from raw key, R, the one way processing is required. r can be written as

$$r = \left\{\left(1-\frac{\mu}{2\eta_{det}\eta_{qc}}\right)\left\{1-h\left(2Q\right)\right\}-h(Q)\right\} \tag{11}$$

The expression $h(x)$ is the binary entropy. To calculate QBER, the dark count needs to be included. Thus, Equation (8) should be replaced by

$$R = vs\left(P_{Bob}\left(N_{max}\right)+P_d\right) \tag{12}$$

Where P_d is dark count rate can be calculated as

$$P_d = 2p_d\sum\nolimits_{n\geq 0} p_A\left(n\right)\left[1-\left(1-\eta det\eta qc\right)\right]^n \tag{13}$$

The p_d is dark count and its value is 10^{-5} [3]. p_d is the photon false count due to the imperfection device at the receiver [18]. QBER is contributed by the ratio of probability the bits are in error and the total probability of Bob detection. Finally, the expression Q or QBER can be written as

$$Q = \frac{P_{error}}{PD} = \frac{\varepsilon P_{Bob}+\frac{1}{2}P_d}{P_{Bob}+P_d} \tag{14}$$

Where ε is the error probability and set up to 0.005. The formula of optimized SKR can be rewritten as

$$K = R\left\{\left(1-\frac{\mu}{2\eta_{det}\eta_{qc}}\right)\left\{1-h\left(2Q\right)\right\}-h(Q)\right\} \tag{15}$$

V. EXPERIMENTAL DATA

Multiphoton experiments are discussed and reviewed starting from 2006 by many research groups. It is found that the design of Multiphoton QKD implementations have dynamic effects and dependent to several parameters. In this paper, numerical analysis have been conducted to show the impact of key parameters and also to find the optimal parameters over the fiber optic network.

TABLE 5. Key parameters for the multiphoton protocol.

Parameters	Values
Repetition rate (Mhz)	Varied from $1x10^1$ to $1x10^9$
Maximum number of photon (Nmax)	Varied from 1 to 12
Fiber loss (dB)	Varied from 0 to 35
Detector efficiency	Varied from 0 to 1
Error rate	0.005
Dark count	Varied from $1x10^{-1}$ to $1x10^{-6}$
Detector efficiency	Varied from 0 to 1

The key parameters [3] are identified and listed in Table 5 to verify the equations in Section IV using Python. The values for each parameter are varied to achieve optimization. Next, Section VI will discuss the results of SKR and QBER based on the parameters for multiphoton QKD protocol. Thus, the values for optimized parameters are selected accordingly for the future fiber optic simulations.

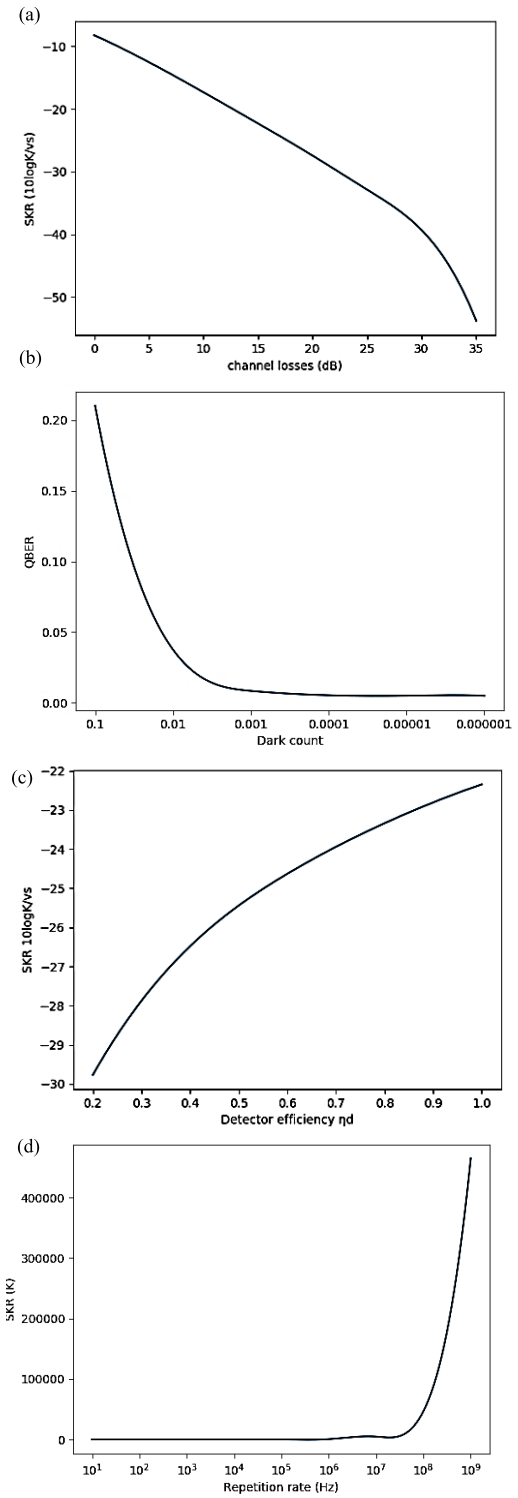

FIGURE 5. Parameter optimization according to the setting in table 4 (a) Secret Key Rate as the function of channel losses (dB); (b) Quantum Bit Error Rate as the function of dark count.; (c) Secret Key Rate as the function of detector efficiency; (d) Secret Key Rate as the function of repetition rate.

VI. RESULTS AND DISCUSSION

In this section, the impact of the experimental setting for multiphoton is evaluated analytically using the equations in section III and the results are discussed. Fig. 5(a) shows

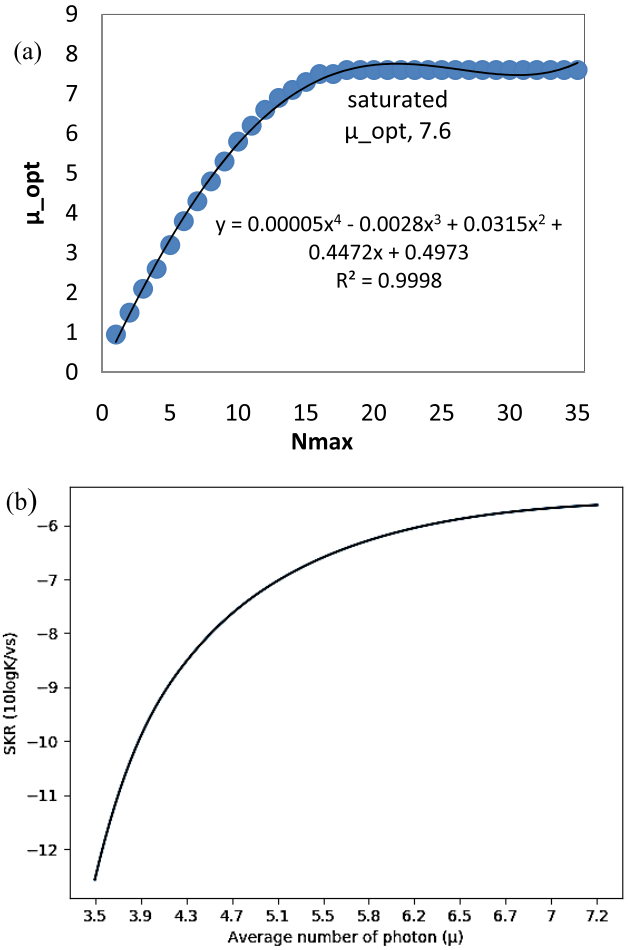

FIGURE 6. The optimizations of mean photon number (a) Optimum mean photon as the function of maximum photon number; (b) Secret Key Rate as the function of average number of photon.

that increasing channel losses (in dB) will reduce the key generation rates. In the fiber optic network, the standard attenuation can be setup based on the operating wavelengths [19]; 1550nm, 1300nm and 800nm for short, medium and long range applications. The attenuation coefficients are 0.25, 0.35 and 2dB/km correspondingly. The 1550 wavelength is the best setup due to the low attenuation. Dark count is the noise detector or false photon count. It can be calculated when the detector clicked but no photon arrived at the receiver. Fig. 5(b) shows that higher rate of dark count will affect on the high QBER as dark counts will generate errors in the transmission even when no eavesdropper is present. Thus, the best photon detector must be served with low dark count probability. In the real experiment using photonic device, the Avalanche Photo Detectors (APD) is used at the detector. To reduce the dark count, the cooling temperature of APC needs to be setup to −50°C [3]. Detector efficiency is an important criteria to identify the total detection of photons at the detector. It can be defined as the detection probability of a photon by getting a click at the detector. As shown in Fig. 5(c), higher detector efficiency will result in less QBER due to most of the bits are received at the receiver.

When the detector efficiency is 1, Bob will detect every pulse that has photons in it. Thus, perfect photon detector could improve the detection rate. The repetition rate is the number of pulses per second emitted from the laser source. The range of repetition rate is from MHz up to few GHz. Fig. 5(d) shows that high source repetition rate will increase the key rate generation. However, the source repetition rate depends on the detector dead time. It is not worthy to send more light than the ability of the detector to detect the pulses. In fact, the unnecessary light will give advantage for Eve to steal the pulses. Thus, the selection of source repetition rate can be opened for discussion.

This analysis shows that the optimum value of SKR significantly depends on the parameters of the fiber setups. Based on the optimum parameters setup in Fig. 3, the average number of photons (μ) in Fig. 6(a) was calculated. The maximum number of photons (Nmax) per signal to encode a bit at a fixed fiber optic distance was varied from 0 to 30 photons per pulse. In the Fig. 6(a), an equation to obtain the optimum mean photon number (μ_opt) can be derived based on the plotted graph. The graph indicates that the saturated value of μ_opt at 7.6 when Nmax is near to 18. One can use the equation to find the μ_opt at any Nmax. In Fig. 6(b), it can be seen that the optimum average number of photons will be used to obtain the optimal SKR. However, the total number of photons need to be restricted to a certain threshold to maintain a level of security. Eve's ability to measure the photon will increase if the number of photons in the beam increases. Thus, more improvements in terms of photon number are required in order to reduce the ability of the photon from being detected by Eve.

VII. CONCLUSION

This paper reviews and discusses the existing multiphoton protocol that has been identified in the literature to implement quantum cryptography using the unitary transformation which is only known by the legitimate parties. This paper also demonstrates the result of the implementation of Three Stages protocols in a matrix representation as an example of multiphoton and multi-stages approach to give a better understanding about the flow of protocol to exchange information without using any optical components. Several parameters contributing to the optimal performance of quantum communication over fiber optic have been investigated in this work. The parameters should be tuned perfectly to achieve the optimal key generation rate and low QBER. It is suggested to figure out other optimum parameters in the free space network as the future works.

ACKNOWLEDGMENT

The author would like to thank Dr. Majed Khodr from Electronics and Communications Engineering Department, American University of Ras Al Khaimah, UAE for fruitful discussion.

REFERENCES

[1] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, G. Baumgartner, and C. McLaughlin, "Performance evaluations of quantum key distribution system architectures," *IEEE Security Privacy*, vol. 13, no. 1, pp. 30–40, Jan. 2015.

[2] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. McLaughlin, and G. B. Baumgartner, "Using modeling and simulation to study photon number splitting attacks," *IEEE Access*, vol. 4, pp. 2188–2197, 2016.

[3] M. El Rifai, "Quantum secure communication using polarization hopping multi-stage protocols," Ph.D. dissertation, School Elect. Comput. Eng., Univ. Oklahoma, Norman, OK, USA, 2016.

[4] M. El Rifai, N. Punekar, and P. K. Verma, "Implementation of an m-ary three-stage quantum cryptography protocol," *Proc. SPIE, Quantum Commun. Quantum Imag. XI*, vol. 8875, 2013, Art. no. 88750S.

[5] K. W. C. Chan, M. El Rifai, P. Verma, S. Kak, and Y. Chen, "Multi-photon quantum key distribution based on double-lock encryption," in *Proc. Conf. Lasers Electro-Opt.*, 2015, pp. 1–13.

[6] M. El Rifai, K. W. C. Chan, and P. K. Verma, "Multi-stage quantum secure communication using polarization hopping," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 4333–4342, 2015.

[7] K. W. C. Chan, M. El Rifai, P. K. Verma, S. Kak, and Y. Chen, "Security analysis of the multi-photon three-stage quantum key distribution," *Int. J. Cryptogr. Inf. Secur.*, vol. 5, nos. 3–4, pp. 1–13, 2015. [Online]. Available: http://www.wireilla.com/papers/ijcis/V5N4/5415ijcis01.pdf

[8] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005, doi: 10.1103/PhysRevLett.94.230504.

[9] L. Mailloux, M. Grimaila, D. Hodson, R. Engle, C. McLaughlin, and G. Baumgartner, "Modeling, simulation, and performance analysis of decoy state enabled quantum key distribution systems," *Appl. Sci.*, vol. 7, no. 2, p. 212, 2017. [Online]. Available: http://www.mdpi.com/2076-3417/7/2/212

[10] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 1, p. 012326, 2005, doi: 10.1103/PhysRevA.72.012326.

[11] A. Parakh and J. van Brandwijk, "Correcting rotational errors in three stage QKD," in *Proc. 23rd Int. Conf. Telecommun. (ICT)*, May 2016, pp. 1–5.

[12] S. Kak, "A three-stage quantum cryptography protocol," *Found. Phys. Lett.*, vol. 19, no. 3, pp. 293–296, 2006.

[13] J. Peatross and M. Ware, "Polarization of light," in *Physics of Light and Optics*, 2015th ed. Provo, UT, USA: Brigham Young Univ., 2015, pp. 143–168. [Online]. Available: optics.byu.edu

[14] M. Lopes and N. Sarwade, "Optimized decoy state QKD for underwater free space communication," *Int. J. Quantum Inf.*, vol. 16, no. 2, p. 1850019, 2018.

[15] B. Darunkar and P. Verma, "The braided single-stage protocol for quantum secure communication," in *Proc. SPIE, Quantum Inf. Comput. XII*, vol. 9123, 2014, Art. no. 912308.

[16] O. Elmabrok and M. Razavi, "Wireless quantum key distribution in indoor environments," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 35, no. 2, pp. 197–207, 2018, doi: 10.1364/JOSAB.35.000197.

[17] M. Mehic, O. Maurhart, S. Rass, D. Komosny, F. Rezac, and M. Voznak, "Analysis of the public channel of quantum key distribution link," *IEEE J. Quantum Electron.*, vol. 53, no. 5, Oct. 2017, Art. no. 9300408.

[18] M. Lopes and N. Sarwade, "Modeling and performance analysis of free space quantum key distribution," in *Information Systems Design and Intelligent Applications*, vol. 435. New Delhi, India: Springer, 2016, pp. 27–40.

[19] K. Xu, L. Sun, Y. Xie, Q. Song, J. Du, and Z. He, "Transmission of IM/DD signals at 2 μm wavelength using PAM and CAP," *IEEE Photon. J.*, vol. 8, no. 5, Oct. 2016, Art. no. 7906407.

NUR ZIADAH HARUN received the B.S. and M.Sc. degrees in information technology from the Faculty of Information Technology, Universiti of Utara Malaysia, in 2008 and 2012, respectively. She is currently pursuing the Ph.D. degree with the Department of Wireless and Communication Networks, University Putra Malaysia. Her research interests focus on computer networks, quantum cryptography, and network security.

ZURIATI AHMAD ZUKARNAIN (M'12) received the bachelor's degree in physics and education and the M.Sc. degree from University Putra Malaysia (UPM) in 1997 and 2000, respectively, and the Ph.D. degree in quantum computing and communication from the University of Bradford, U.K., in 2005. At the faculty, she taught several courses for undergraduate students, such as data communication and networks, distributed system, mobile and wireless, network security, computer architecture, and assembly language. For postgraduate students, she taught few courses, such as advanced distributed and research method. She has been an Academic Staff with the Faculty of Computer Science and Information Technology, UPM, since 2001. She was the Head of the Department Communication Technology and Networks from 2006 to 2011. She was also the Head of the Section of High Performance Computing, Institute of Mathematical Research, UPM, from 2012 to 2015. Her areas of specialization are computer networks, distributed systems, mobile and wireless, network security, quantum computing, and quantum cryptography. She is a member of the IEEE Computer Society.

ZURINA MOHD HANAPI (M'11) received the B.Sc. degree in computer and electronic system engineering, University of Strathclyde in 1999, the M.Sc. degree in computer and communication systems engineering from University Putra Malaysia (UPM) in 2004, and the Ph.D. degree in electrical, electronics, and system engineering from the National University of Malaysia in 2011. She is currently an Associate Professor with the Faculty of Computer Science and Information Technology, UPM. She is also a Lecturer with UPM. She is also a leader of some research projects. She has published many conference and journal papers. Her research interests are in routing, wireless sensor networks, wireless communication, distributed computing, network security, cryptography, and intelligent systems. She has received the excellence teaching awards in 2005, 2006, and 2012. She has also received the silver medal in 2004 and the bronze medal in 2012.

IDAWATY AHMAD received the bachelor's and master's degrees in information science from Saga University, Japan, and the Ph.D. degree in computer network from University Putra Malaysia (UPM). She is currently a Lecturer with the Faculty of Computer Science and Information Technology, UPM, since 2000. She specializes in the areas of real-time systems, network protocols, and simulation/modeling that are core areas in computer science.