Al-Khwarizmi Engineering Journal, Vol. 17, No. 2, June, (2021)
P. P. 31-44

Al-Khwarizmi Engineering Journal

# Modeling and Simulation for Performance Evaluation of Optical Quantum Channels in Quantum key Distribution Systems

**Adil Fadhil Mushatet*** **Shelan Khasro Tawfeeq ****

**Al-Khwarizmi Engineering College/ University of Baghdad/ Iraq*
*** Institute of Laser for Postgraduate Studies/ University of Baghdad/ Iraq*
*Email: adilfadhil@kecbu.uobaghdad.edu.iq
**Email: shelan.khasro@ilps.uobaghdad.edu.iq

(Received 13 March 2021; Revised 13 April 2021; Accepted 16 April 2021)
https://doi.org/10.22153/kej.2021.05.001

## Abstract

In this research work, a simulator with time-domain visualizers and configurable parameters using a continuous time simulation approach with Matlab R2019a is presented for modeling and investigating the performance of optical fiber and free-space quantum channels as a part of a generic quantum key distribution system simulator. The modeled optical fiber quantum channel is characterized with a maximum allowable distance of 150 km with 0.2 dB/km at $\lambda$=1550nm. While, at $\lambda$=900nm and $\lambda$=830nm the attenuation values are 2 dB/km and 3 dB/km respectively. The modeled free space quantum channel is characterized at 0.1 dB/km at $\lambda$=860 nm with maximum allowable distance of 150 km also. The simulator was investigated in terms of the execution of the BB84 protocol based on polarizing encoding with consideration of the optical fiber and free-space quantum channel imperfections and losses by estimating the quantum bit error rate and final secure key. This work shows a general repeatable modeling process for significant performance evaluation. The most remarkable result that emerged from the simulated data generated and detected is that the modeling process provides guidance for optical quantum channels design and characterization for other quantum key distribution protocols.

***Keywords:*** *Optical quantum channel, modeling, quantum bit error rate, quantum key distribution.*

## 1. Introduction

Quantum Key Distribution (QKD), the most advanced technology in the field of quantum information, allows two remote parties to exchange unconditionally secure key and subsequently check their secrecy based on the principles of quantum mechanics [1, 2]. In QKD the quantum channel is not used directly to send meaningful message. It is rather used to transmit a supply of random bits between two users who share no secret information in advance. The reason for naming this channel as a quantum channel because it is used to distribute the shared key between two parities using ideal single photons or high level of attenuation to reach the quantum level of optical pulses [3].

To implement QKD in real-life, ideal models should be used to verify security proofs, which is not the case in reality, as a noisy communication channel in which optical fiber channels suffer from that polarization of photons is changed with the increase of fiber length due to the birefringence character and free space channel losses due to atmospheric effects and diffraction attenuation, opening the door for different eavesdropping attacks to be launched against QKD systems. For this reason, the main challenge is to implement a simulation environment to investigate the optical quantum channel performance. Solving this challenge will enable a swift simulation and evaluation of the quantum channel behavioral operation.

The aim of this work is to model environment GUI tool supports with time-domain plotters to simulate the optical pulses generation and transmission processes for individual testing purpose to simulate both quantum channels, optical fiber (OF) and free space (FS), performance in QKD systems in terms of quantum bit error rate ($QBER$) and final secure key considering the limitations imposed by using practical quantum channels. This research presents a quantum free space channel simulator which to the best of our knowledge, was not considered previously within other QKD simulators.

Few simulation efforts were reported in related literature to develop a model aimed to investigate the optical fiber quantum channels operation performance. For example, Nathaniel T Sorensen et al. have presented two approaches to simulate the optical fiber quantum channels, first one deals with the photons as wave packets while the other as discrete particles [4]. Jonathan C Denton et al. introduced a model to investigate the performance of space-based quantum channels in QKD systems taking into consideration the atmosphere losses and the selection of the orbit [5]. In contrast to the simulators mentioned above that concentrate on the theoretical investigations without connection to the application field, this work aims to get the simulated information generated and detected by real and commercially available physical components. The most important challenge in this work was how the simulator can address the effects due to the propagation of the laser pulses, optical components functions and the behavior of complex interacting single-photon detectors software process present within this system.

## 2. The Optical Quantum Channel Conceptual Model

The optical quantum channel is a passive component with one input and one output as shown in the corresponding conceptual model of Figure (1).

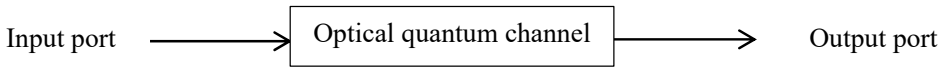



**Fig. 1. Optical quantum channel conceptual model.**

Regarding OF channel, from the conceptual model diagram, the attenuated coherent optical pulses that are usually used in the QKD system, are generated via modeled pulsed laser source which consists of two parts, Binary Pseudo Random Sequence (BPRS) generation unit and laser device. The modeled BPRS unit generates a binary non-return–to-zero (NRZ) sequence of N bits with a defined pulse repetition rate. Based on the input from the BPRS unit, the laser source generates Gaussian optical pulse trains with peak optical power ($P_{peak}$) in the range of (pW) with (ns) pulse duration with the possibility to support different optical wavelengths (λ). Each pulse is generated with known shape, intensity, polarization, period and global phase. To simulate the coherent optical pulse used in this work, the model proposed by Douglas D.Hodson [6, 7] is used. The approximation function of the coherent optical pulse has the following form,

$$\vec{E}(0,t) = E_0 e^{-i\omega_o t} e^{-i\theta} |g(t)| \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) e^{i\Phi} \end{pmatrix} \quad \ldots(1)$$

Where |g (t)| represents the optical pulse Gaussian shape,

$$|g(t)| = \frac{2\Delta^2}{\sqrt{2\pi}} e^{-\Delta^2 (t-t_o)^2} \quad \ldots(2)$$

Where $E_o$ is the pulse maximum electric field, $\theta$ is the phase offset of the pulse, $\alpha$ is the angle of the vector to the $x$ axis, $\Phi$ is the relative phase between the $x$ and $y$ components of the electric field and $\omega_o$ is the angular frequency. The coherent optical pulses are attenuated by the modeled optical power attenuator (PA) and are sent to the modeled OF quantum channel. The propagated optical pulses will be under the influence of fiber attenuation and polarization rotation distortions as a result of fiber geometry and its material characteristics. The output optical pulses will be heavily attenuated as the transmission distance increased. While the polarization of the optical pulses lunched to the fiber will be randomly rotated along the length of the OF quantum channel by an angle ($\vartheta$) when the linearly polarized optical pulses are lunched by the QKD transmitter. As the inputs to the simulation model, the following parameters were considered, optical pulse time profile with linear polarization as defined in Eq.(1) with $P_{peak}$ in (mW), transmitted λ in nm, channel distance ($L$)

and the attenuation constant of the fiber (per Km) ($\alpha_p$). These parameters can be set by the user in the modeling GUI tool.

For the FS channel, the incoming optical pulses from the QKD transmitter will enter the input port and propagate along with it. The transmitted optical pulses will be under the influence of all atmospheric attenuation effects and attenuation due to diffraction. The output optical pulses will be heavily attenuated as the transmission distance increases. While the polarization of the linearly polarized optical pulses launched to space will not change along the path. In this model, the losses due to different atmospheric conditions such as the losses due to atmospheric absorption and scattering ($\delta_{atm}$), space loss ($\delta_{propagation}$), weather impairments and finally the beam divergence losses due to diffraction ($\delta_{diff}$) will be included.

## 3. The Optical Quantum Channel Mathematical Models

This section outlines the mathematical model of a single-mode fiber (SMF) and FS atmospheric model that takes into account the atmospheric and diffraction losses that are believed to be important for the modeling of the QKD quantum channel.

### A. The optical fiber channel

Fiber-based QKD systems are affected by the attenuation which is mainly raised by the absorption and scattering losses. Almost 90% of total attenuation is due to scattering losses only. With respect to the dispersion in SMF, real SMF has a core with a semi-elliptical shape profile rather than an ideal circular core; this, in turn, leads to eliminate the degeneracy of orthogonal modes and leads to different groups velocities. This results in pulse broadening and this effect is known as polarization mode dispersion (PMD) [8].

In this work, the modeled OF quantum channel has been designed as a normal SMF, not as a polarization-maintaining fiber. Thus, the polarization of the transmitted optical pulses is randomly rotated due to PMD and drift from their original encoded basis. In addition, the signal attenuation effect due to OF losses is included in the OF quantum channel model. The impact of these types of errors on the channel performance enhances the $QBER$ of the QKD system and reduce the final shared secure key.

The coherent optical pulse defined in Eq. (1) represents the input to the OF quantum channel model. For a non-dispersive medium; $\theta$ will be constant at all spatial points $z$, .i.e., assumed (0 degrees) in this work. For the sake of simplicity, $|g(t)|$ the term is not considered for the next steps in this model. From the coherent optical pulse representation, the signal parameters that will be affected by the OF quantum channel are $E_0$ and $\alpha_{inc.}$.

To find the behavior of the transmitted optical pulses after passing through the OF quantum channel, the following operation on the coherent optical pulse Jones matrix will be carried out taking into account the amount of the attenuation coefficient and its relation to the transmission distance in addition to the effect of the random polarization variation by an angle ($\vartheta$).

$$\vec{E}_{OF} = E_0 e^{-i(w_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.} + \vartheta) \\ \sin(\alpha_{inc.} + \vartheta) e^{i\Phi} \end{bmatrix} \sqrt{10^{\frac{-(\alpha_p / kmL)}{10}}} \quad \ldots(3)$$

Thus, the optical signal form at the OF quantum channel output port will be as follows:

$$\vec{E}_{OF} = E_0(\alpha_p) e^{-i(w_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.} + \vartheta) \\ \sin(\alpha_{inc.} + \vartheta) e^{i(\Phi)} \end{bmatrix} \quad \ldots(4)$$

### B. The free-space quantum channel

As a solution to the attenuation caused in the fiber- based QKD systems, a free space channel allows greater communication distances because the atmosphere has low absorption in certain wavelengths. In addition, the atmosphere has a nearly non-birefringent character which ensures the conservation of the photon's polarization state [9, 10].

The modeled FS quantum channel is characterized at 0.1 dB attenuation per km at λ =860 nm. In addition to the very low attenuation level feature at this λ, the commercial single-photon detector (SPD) operating within (600-900nm) window show better operation performance with higher quantum detection efficiency reaching 70%. In this model, the channel transmittance model must take into consideration all impairments that affect the performance of the FS quantum channel for better simulation of the behavior of a terrestrial FS quantum channel. In this model, the losses due to different atmospheric conditions such as the losses due to atmospheric absorption and scattering, space loss, weather impairments and finally the

beam divergence losses due to diffraction will be included.

The main source of attenuating of the optical signals transmitted through the FS quantum channel is the absorption and scattering due to dust, aerosols, carbon dioxide, etc. [11]. The propagated light photons will interact with the atmospheric particles which lead to scatter and absorb part of these photons [12]. Thus, the amount of the optical power received at the detector will be investigated by Beer-Lambert Law which relates the optical signal transmittance to the length of the FS link as follows [11],

$$P_R = P_T e^{-OD} \quad \ldots(5)$$

Where $OD$ is the optical depth, $P_R$ and $P_T$ are the received and transmitted power respectively [12],

$$\therefore T_{link} = \frac{P_R}{P_T} = e^{-OD} \quad \ldots(6)$$

Where $T_{link}$ is known as the transmittance of the link which defines the amount of the transmitted light power along the channel [11].

The atmospheric attenuation coefficient ($\sigma(\lambda)$) is related to this atmospheric transmittance by [12],

$$T_{link} = e^{-\sigma(\lambda)L} \quad \ldots(7)$$

The overall $\sigma(\lambda)$ will sum up all the absorption and scattering coefficients within the atmosphere [11, 12],

$$\sigma(\lambda) = \sigma_a(\lambda) + \sigma_m(\lambda) + \beta_a(\lambda) + \beta_m(\lambda) \quad \ldots(8)$$

Where first two terms show the aerosol and molecular absorption coefficients, respectively, and the last two terms are the aerosol and molecular scattering coefficients, respectively. As a result, the total attenuation losses for the transmitted optical beam in dB can be calculated as [11, 12],

$$\delta_{propagation} = -10 \log_{10} T_{link} \quad \ldots(9)$$

To calculate the attenuation of optical signal propagating through FS quantum channel due to atmospheric effects, the channel attenuation ($\delta_{atm}$) in (dB/km) can be expressed as [11, 12],

$$\delta_{atm} = \frac{1}{L} 10 \log \left(\frac{P_T}{P_R}\right) \quad \ldots(10)$$

$$\therefore \delta_{atm} = \frac{1}{L} 10 \log e^{\sigma(\lambda)L} \quad \ldots(11)$$

Finally, the diffraction-limited beam divergence loss in dB can be defined as [10],

$$\delta_{diff} = -10 \log_{10}[\left(e^{-2\gamma_t^2 a_t^2} - e^{-2a_t^2}\right)\left(e^{-2\gamma_r^2 a_r^2} - e^{-2a_r^2}\right)] \quad \ldots(12)$$

Where

$\gamma t, r = \frac{b_{t,r}}{R_{t,r}}$ , $\alpha t, r = \frac{R_{t,r}}{w_{t,r}}$ , $w_t = R_t$ *and* $w_r = \frac{\sqrt{2}\lambda L}{\pi R_t}$ [10]

Where the subscript $t$ refers to the transmit telescope and $r$ is the receive one that are used in free space QKD systems. $R$ and $b$ are the primary and secondary mirrors radii, respectively, $w_{t,r}$ refers to the beam radius at the transmission or reception side.

Thus, the total channel attenuation is given by [9, 10],

$$\delta_{total} = \delta_{propagation} + \delta_{atm} + \delta_{diff} + \delta_{det} \quad \ldots(13)$$

Where $\delta_{det}$ is the single-photon detection efficiency of the SPD.

A list of all the required parameters as inputs to the simulation model is found in Table 1. The telescope's primary and secondary mirror radius in addition to $\delta_{propagation}$ are taken from SILEX experiment and Tenerife's telescope [9, 13, 14] that are considered as global standard experiments for FS- QKD systems. $L$ and $\delta_{atm}$ can be set by the user in the modeled GUI tool.

**Table 1,**
**Input parameters for FS quantum channel modeling**

| Parameter | Value |
|---|---|
| $P_{peak}$ | 1 mW |
| $\lambda$ | 860 nm |
| telescope's primary mirror radius | 50 cm |
| telescope's secondary mirror radius | 5 cm |
| beam radius at the transmitter | 50 cm |
| beam radius at the receiver | For $L$=50km 4 cm |
| | For $L$=100km 7.75cm |
| | For $L$=150km11.62cm |
| Single-photon detector efficiency | 70% @ $\lambda$=860 nm |
| $\delta_{propagation}$ | 1 dB |

To find the behavior of the transmitted optical pulses after passing through the FS link, the following operation on the transmitted coherent pulse Jones matrix will be carried out taking into account the amount all attenuation effects,

$$\vec{E}_{FS} = E_0 e^{-i(w_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} (\delta_{total}) \quad \ldots(14)$$

## 4. The Structured Flow of the Modeling Process and the Methodology Used

The purpose of optical quantum channel modeling is to efficiently relate the system's practical considerations, software design with the theoretical fundamentals such as the optical pulse generation and transmission, the optical pulse properties, the operation principles of the optical components and the system environment conditions. The optical quantum channel simulator modeling process involves a set of actions. The representation of these actions is known as the software development model as shown in-tier architecture in Figure (2). In this section, the structuring flow of the software development model that has been utilized to implement this simulation tool will be explained in addition to the methodology used in this research work.

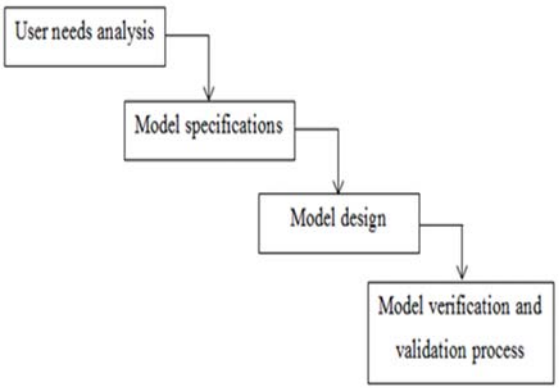



**Fig. 2. Optical quantum channel simulator software.**

In general, there are four actions required to implement any programming model. Firstly, the model specifications must be characterized, secondly, the model design should suit the user prerequisites, thirdly, the designed model must be verified and tested and finally, the implemented model must be flexible and possible to be developed [15, 16]. Each stage will be explained as follows:

### 4.1 User needs analysis

In this stage, the user prerequisites that the designed optical quantum channel simulator can achieve are analyzed. The simulator requirements focused on successfully investigate the channel performance by estimating QBER and final secure key for the following cases, OF quantum channel imperfections such as the polarization rotation and attenuation and FS quantum channel losses due to atmospheric effects and diffraction attenuation.

### 4.2 Model specifications

In this stage, the inputs provided from the simulator users with the expected outcomes will be defined. Table 2 represents the simulator specifications as inputs and outputs for optical quantum channels simulators.

**Table 2,**
**Inputs and outputs for the optical quantum channel simulator.**

| Simulator inputs | Simulator outputs |
|---|---|
| $\lambda$ | $QBER$ |
| $L$ | Sifted bits rate for BB84 protocol ($KEY_{raw}$) |
| $\alpha_p$ | |

### 4.3. Model design

According to this stage, the previous two stages are related to the hardware components for the simulator final design. In this work, the modular and hierarchical approaches were used as architecture for the simulator. Using this approach, the user will be flexible enough to build different implementation scenarios and the model developer will easily modify and extend the model. Figure (3) shows the designed model layers that consist of three layers each with a specific objective. The outer layer represents the application field selected by the user. In this work, only the QKD system for the BB84 protocol is demonstrated. The middle layer represents the main simulation operation phases that involve optical signal generation, transmission and detection. These steps were built using various modules which consist of different integrated physical modeled components. For example, the optical signal preparation and generation phases can be conducted using the transmitter module which consists of BPRS, pulsed laser source and PA. The last layer is established using different physical electrical and optical components. This

layer is considered as the construction of the modules at layer 2. The continuous time-domain simulation approach that was utilized in this work was a time and computation-consuming approach because hundreds of optical pulses will be generated and transmitted through the system's components.

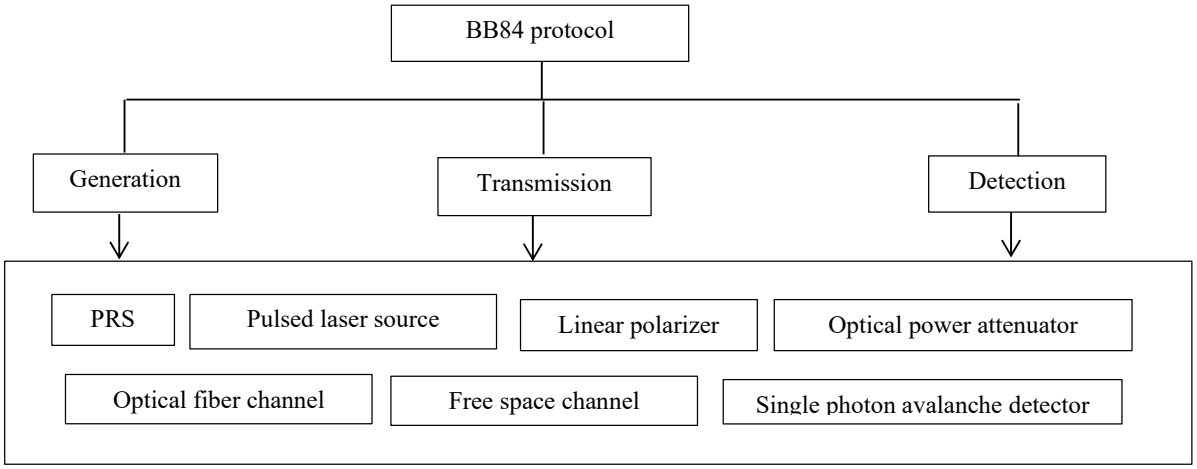



**Fig. 3. QKD simulator reference layers.**

## 4.4 Model verification and validation process

The credibility of the optical quantum channel simulation model and its results are verified using the known verification and validation steps. The approach that has been used for model verification was by running the model under different conditions by applying inputs and checking the outcomes [15, 16, 17]. The recorded results will show how the model is programmed in a sufficiently and correctly way by determining the response of the model to the input parameters. In this research, a Matlab compiler was used to prove the model verification by testing the code as recommended by Sargent and Balci [15, 16].

For the validation technique, the approach that was applied to the mathematical models as recommended by Sargent [15] was established with the help of the specialized references and publications in the field, commercial data sheets to define the allowed input and output limits in addition to the desired specifications to prove that the postulates and the theoretical concepts on which mathematical models are based were correct.

The methodology for the modeling process for each component and module that was followed in this research work is similar as shown in Figure (4).

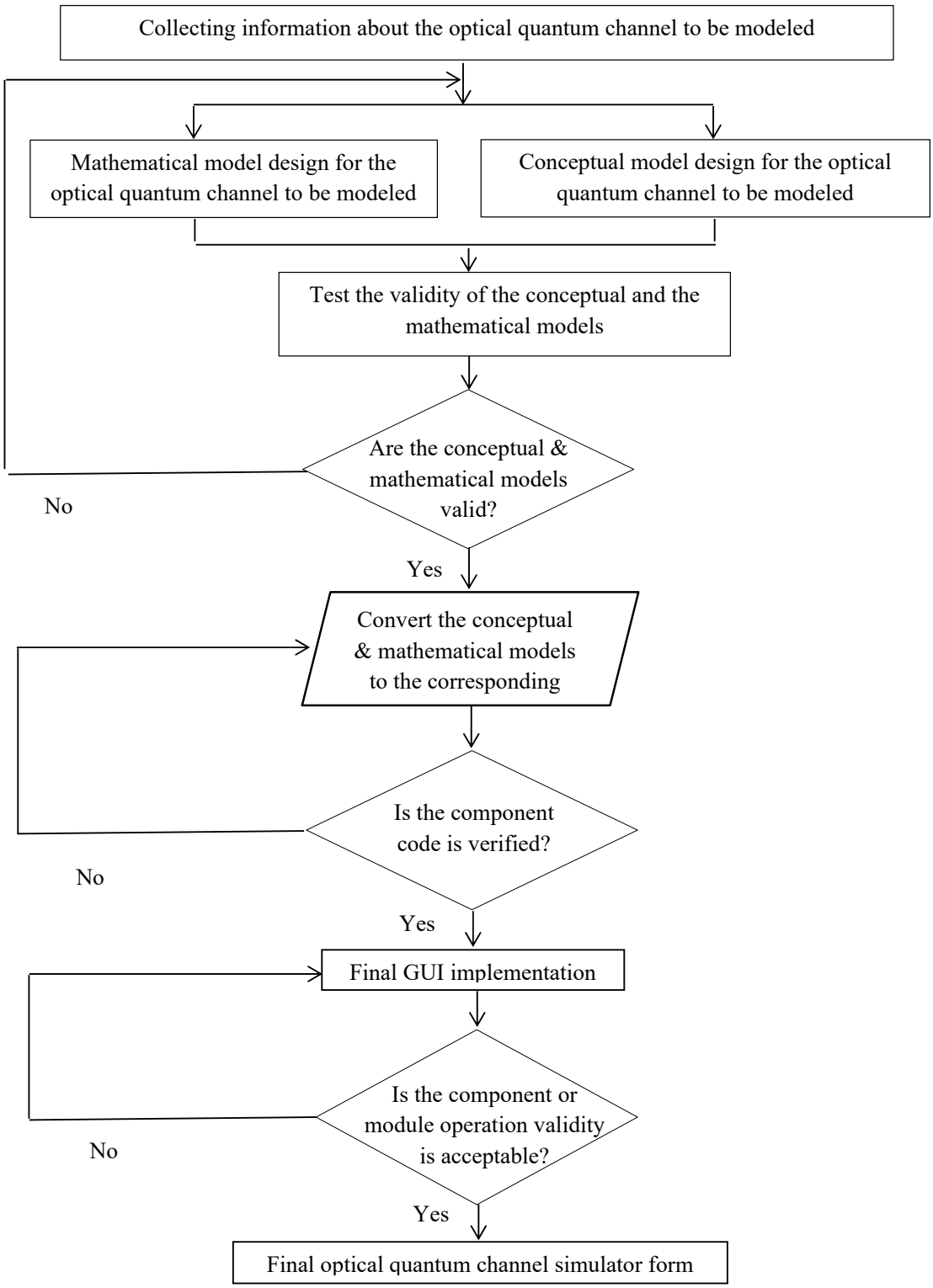



**Fig. 4. Modeling process steps. GUI: graphical user interface.**

**Final Optical Quantum Channel Simulator**

## 5. Results and Discussion

The purpose of this section is to present the results with the analysis of modeling the optical quantum channel.

### 5.1. Simulator testing

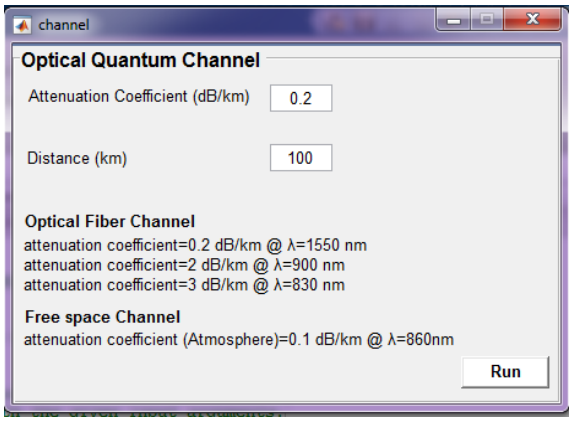
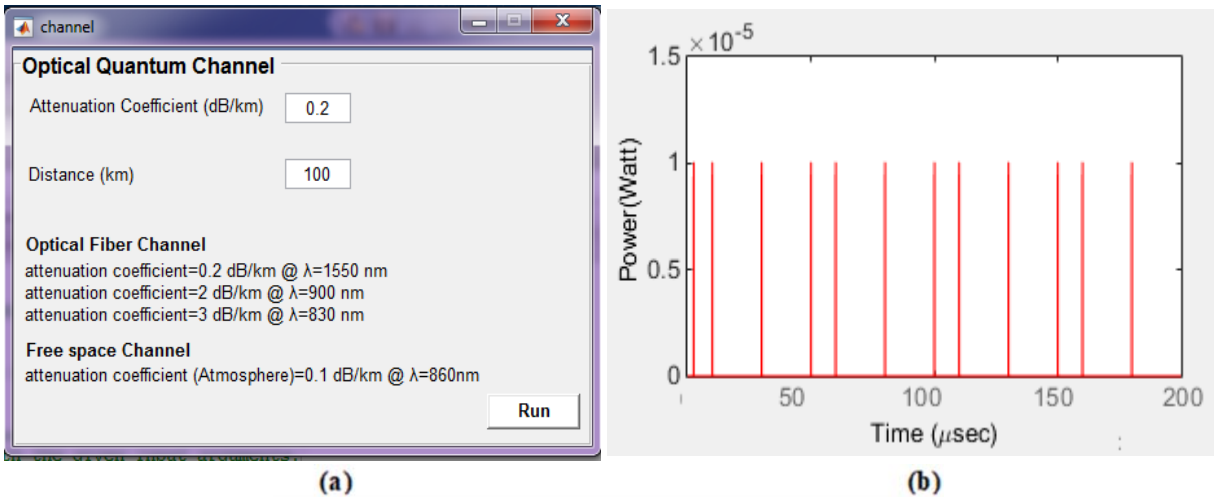



**Fig. 5. OF quantum channel simulator window.**

The optical quantum channel model has been implemented with a friendly GUI as shown in Figure (5) which includes OF and FS quantum channels. This interface with its configurable editing objects is responsible to allow users to configure the OF and FS quantum channels model to enable the attenuation effect in $\alpha_p$ per $km$ and to decide the OF quantum channel $L$ in km. The user allowed $\alpha_p$ values vs. $\lambda$ are listed within the GUI.

For the simulation of the polarization rotation effect, the GUI plotters will not be able to clearly show the alteration in polarization in the transmitted optical pulses over the OF quantum channel. Otherwise, the effect of this error type will be significant on the QKD system performance by reducing both QBER and final shared secure key. Two tests were applied to verify the modeled OF quantum channel model to simulate the OF operation. The incoming optical pulses from the QKD transmitter are linearly polarized with PRR= 100 kHz and P_peak=1mW.

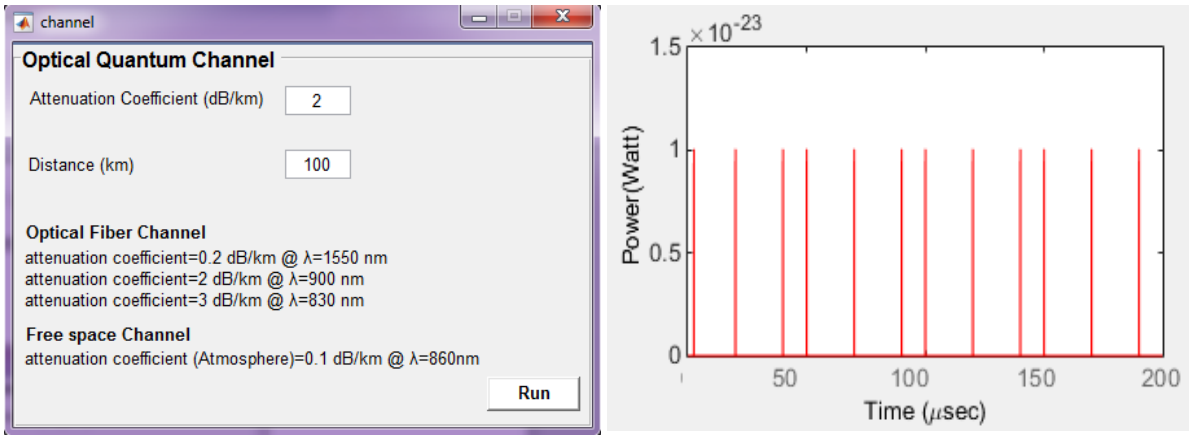
Figure (6a) illustrates Test 1 set up to investigate the attenuation due to absorption and scattering in the transmitted optical pulses after passing through the OF quantum channel model at $\lambda$ =1550 nm. In this test, for 100 km length fiber and α_p =0.2dB/km, the output power is equal to 0.01mW as shown in Figure (6b).




(a) (b)

**Fig. 6. Test 1 (a) GUI set up (b) result for OF quantum channel for L =100km and α_p=0.2 dB/km.**

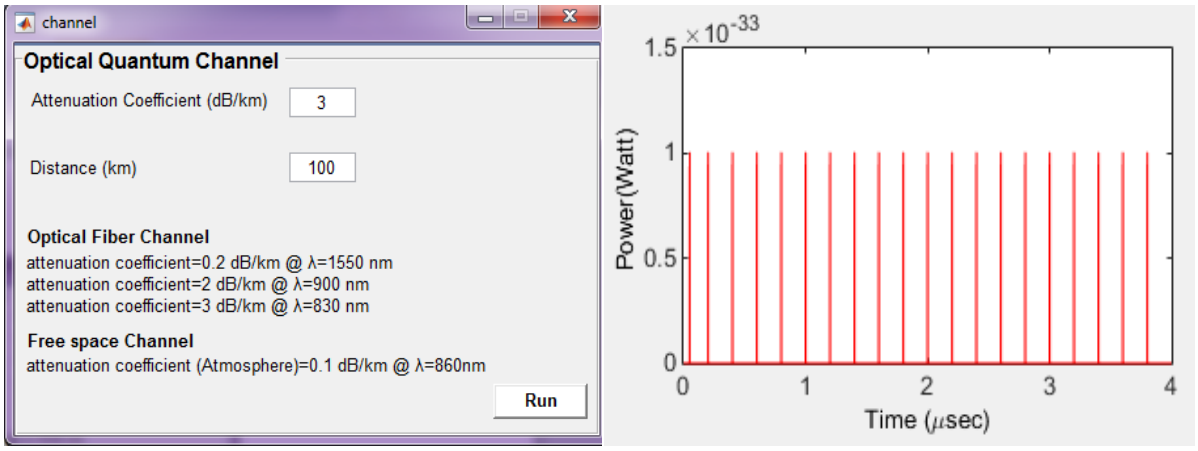
Figure (7a) illustrates Test 2 set up to examine the OF quantum channel model performance for $\lambda$=900 nm. In this test, for 100 km long fiber and α_p=2 dB/km, the output power is equal to $10^{-23}$ W as shown in Figure (7b).




**(a)** **(b)**

**Fig. 7. Test 2 (a) GUI set up (b) result for OF quantum channel for L=100km and α_p=2 dB/km.**

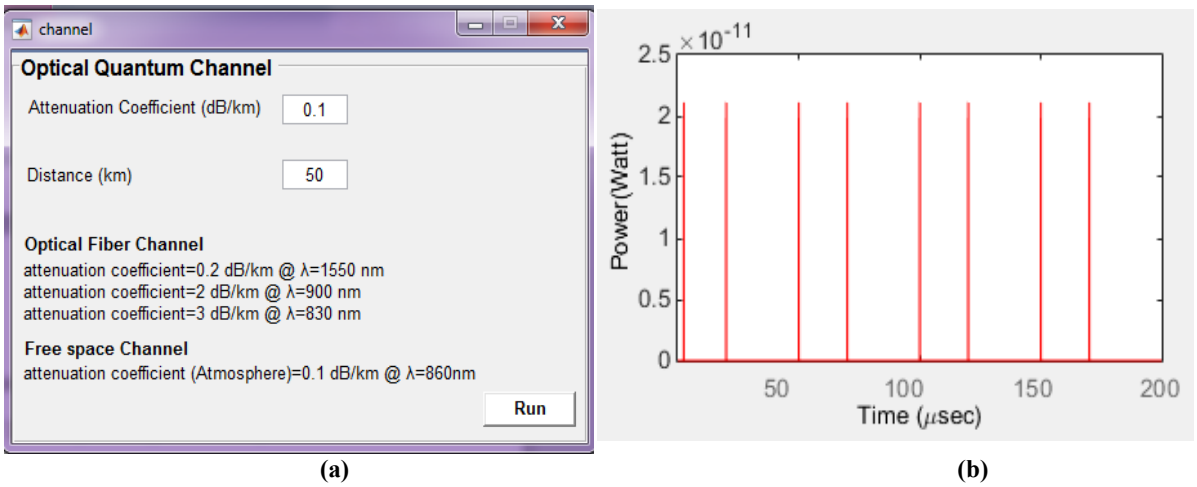
Figure (8a) illustrates Test 3 set up to examine the OF quantum channel model performance for $\lambda$=830 nm. In this test, for 100 km long fiber and $\alpha_p$=3 dB/km, the output power is equal to $10^{-33}$ W as shown in Figure (8b).




**(a)** **(b)**

**Fig. 8. Test 3 (a) GUI set up (b) result for for OF quantum channel for L=100km and α_p=3 dB/km**

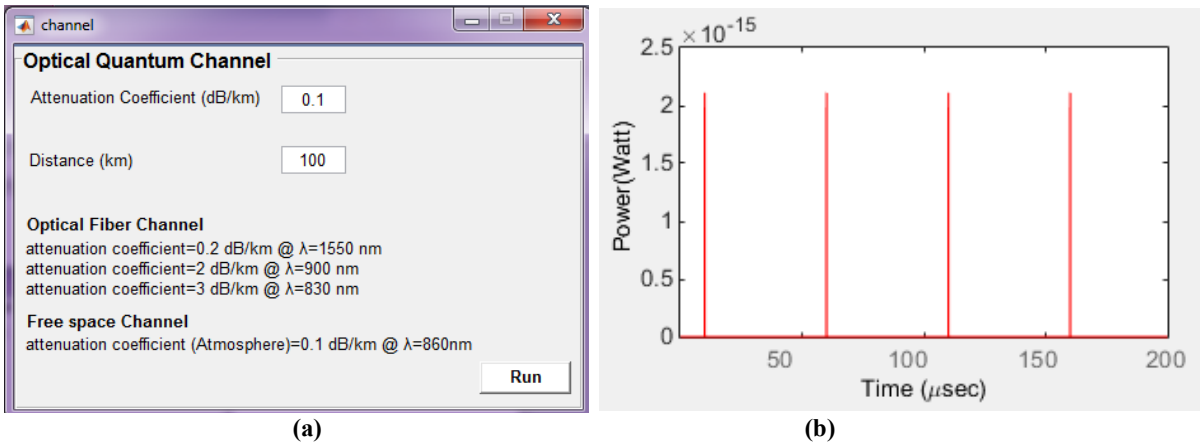
Figure (9a) illustrates Test 4 set up that is used the same parameters as used in last two tests to investigate the attenuation in the transmitted optical pulses after passing through the FS quantum channel model at $\lambda$=860 nm. In this test, for 50 km link length, the output power is equal to 0.02nW as shown in (9b).




**(a)** **(b)**

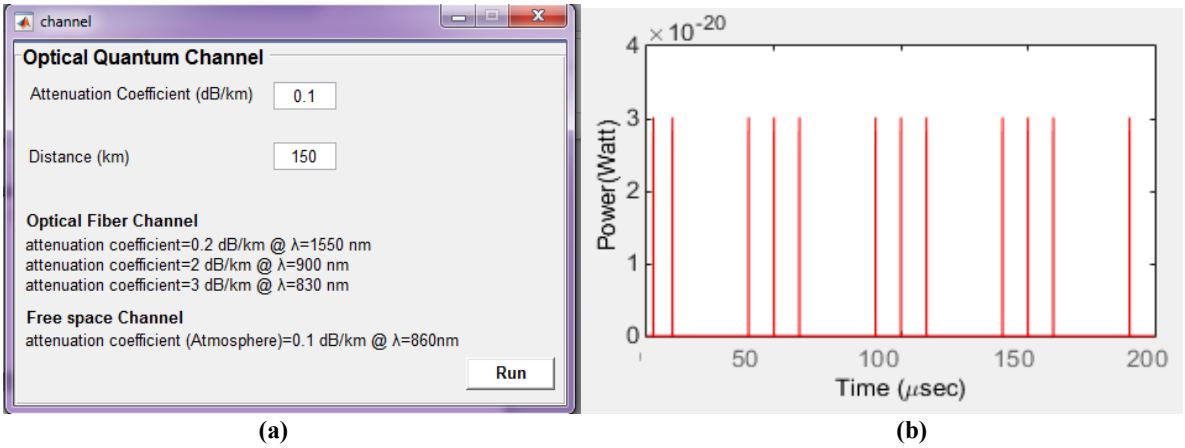
**Fig. 9. Test 4 (a) GUI set up (b) result for FS quantum channel for L =50km.**

Figure (10a) illustrates Test 5 set up. In this test, for 100 km FS quantum channel length, the output power is equal to 2.1 f W as shown in (10b).




**(a)** **(b)**

**Fig. 10. Test 5 (a) GUI set up (b) result for FS quantum channel for L=100km.**




**(a)** **(b)**

**Fig. 11. Test 6 (a) GUI set up (b) result for FS quantum channel for L =150km.**

Figure (11a) illustrates Test 6 set up. In this test, for 150 km link length, the output power is equal to 300 attoW as shown in (11b).

The results obtained from the previous tests illustrate the performance degradation of OF and FS quantum channels due to the effect of the attenuation represented by fiber absorption and scattering and atmospheric, weather conditions in addition to the beam divergence due to diffraction in the FS channel as $L$ increased.

## 5.2 Investigation of the system performance under the effect of the polarization rotation

The effect of the random polarization rotation for the optical pulses traveled inside the OF link within a complete QKD system based on BB84 protocol will be explained in terms of investigating the system quantum bit error rate after the sifting phase ($QBER_{sk}$) which can be calculated by divide the sifted wrong bits to the total number of the received sifted bits. The simulator configuration parameters that have been used in this experiment are, $\lambda$= 830 nm, $L$=20 km, $PRR$= 10 MHz. This effect was modeled using an embedded sub-function within the system to simulate the polarization rotation mechanism where the range of the polarization rotation in degree is from (0° → 45°).

Table 3 summarizes the amount of the polarization rotation in the degree that has been added to the polarization of the generated optical pulses in addition to the resultant $QBER_{sk}$ where the polarization of the propagated optical pulses within the OF link is changed from its original state to a new state randomly. The estimated $QBER_{sk}$ random behavior shows the effect of transmitting wrong polarization states on the system performance.

**Table 3,**
**The effect of the optical pulses polarization rotation on the system $QBER_{sk}$**

| Random rotation of the polarization state inside OF channel | $QBER_{sk}$ (%) |
|---|---|
| 1° | 41 |
| 4° | 60 |
| 5° | 64 |
| 37° | 51 |
| 8° | 47 |
| 4° | 55 |
| 6° | 58 |

## 5.3 Investigation and analysis of system parameters under the effect of quantum channel losses

This study is conducted to examine the relation between the performance of the system represented by the ratio of the dark-count rate to the detection probability ($QBER_{spd}$ ) and the generated $KEY_{raw}$ with average photon number per pulse ($N_0$) and $L$ system parameters. $QBER_{spd}$ can be defined as [18]:

$$QBER_{spd} = \frac{P_{dark} n}{N_0 \eta t_{link}} \quad \dots (15)$$

Where

$P_{dark}$: is the probability of recording a dark count per time window and per detector

$n$: refers to the number of detectors.

$N_0$: mean photon number per pulse

$\eta$ : is the probability of the photon's being detected

$t_{link}$: the transfer efficiency between Alice's output and Bob's detectors and can be defined as [18]:

$$t_{link} = 10^{\frac{-(\alpha_p L + L_{Bob})}{10}} \quad \dots (16)$$

Where $\alpha_p$ is the fiber attenuation constant per km, $L$ is the link length in km and $L_{Bob}$ is Bob's internal loss in dB.

$N_0$ is preferred to be in the range (0.1-1) to ensure security for QKD systems. Both quantum channels types have been used to perform this simulation study i.e. OF channel was operated at 1550nm and FS channel was operated at 860nm. Table 4 shows the main simulation input parameters.

**Table 4,**
**Simulation study input parameters**

| Parameter | Value |
|---|---|
| $\lambda$ | 1550nm, 860nm |
| $PRR$ | 0.1 MHz, 2 MHz, 5 MHz |
| $N_0$ | 0.1, 0.2, 0.4 |
| $L$ | 20 km, 40 km, 60 km, |

Figure (12) illustrates the obtained results that indicate the transmission distance and the amount of the shared $KEY_{raw}$ will be limited as a result of the decline in the system performance, which is represented in increasing calculated quantum bit error rate with the consideration of $QBER_{spd}$ as the channel length increases. Compared to OF channel, FS channel is not suitable for long-distance operation as a result of increasing the noise and the interference with increasing $L$. On the other hand, $N_0$= 0.1 is preferred for high

security issues although the exchanged $KEY_{raw}$ is small compared to $N_0$= 0.2 and 0.4

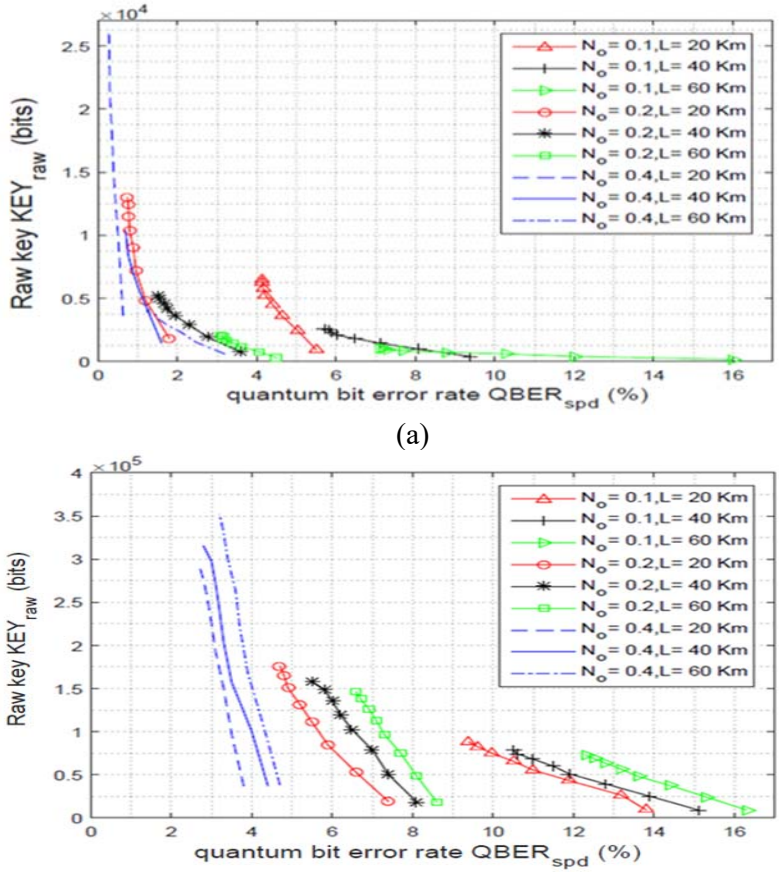



**Fig. 12. KEYraw vs. QBERspd (%) at different L and N_0(a) λ=1550nm (OF) (b) λ=860nm (FS).**

## 6. Conclusion

In this research, a modeling tool of the optical quantum channel was implemented, tested and integrated within a modeled QKD-BB84 practical set-up. A set of tests were conducted to investigate the simulator validation in terms of $QBER$ calculation and final secure key extraction under different operation conditions such as OF attenuation and PMD losses and FS atmospheric and diffraction losses that are believed to be important for the modeling of the QKD quantum channel. The most remarkable result to emerge from the data is that the modeling process provides guidance for optical quantum channel design and characterization. It is possible to conclude that the simulation methodology that has been used within this work is efficient to describe the modeled system components details but at the same time it is processing time and resources consuming. Thus, the recommended approach is to model such a system is to use an approach that deals with the simulation operations as synchronized discrete events organized in a logical form. This method was used because basically the modeled optical quantum channel is not intended to simulate any real optical quantum channel but to evaluate the capabilities of the modeled optical quantum channel presented in this work. For further development of this work, the simulator model performance can be developed by using a discrete event approach supported by more general programming languages such as C++ to increase the simulator reality and trying to model underwater quantum channel and embed it within a general QKD modeling tool.

## 7. References


[1] Douglas D Hodson, Michael R Grimaila, Logan O Mailloux, Colin V McLaughlin, and Gerald Baumgartner, "Modeling quantum optics for quantum key distribution system simulation,"*Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*", vol. 16, Issue 1,2017.

[2] Nicolas Gisin, Gre´ goire Ribordy, Wolfgang Tittel, and Hugo Zbinden," Quantum cryptography", *Reviews of Modern Physics*, Vol. 74, January 2002.

[3] H. Lo, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science (80-. ).*, vol. 283, no. 5410, p. 20502056, 1999, doi: 10.1126/science.283.5410.2050.

[4] Nathaniel T Sorensen1 and Michael R Grimaila, "Discrete Event Simulation of the quantum channel within a Quantum Key Distribution system," The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Vol. 12, Issue 4, page(s): 481-488, 2015.

[5] Jonathan C Denton, Douglas D Hodson, Richard G Cobb, Logan O Mailloux, Michael R Grimaila, and Gerald Baumgartner, " A model to estimate performance of space-based quantum communication protocols including quantum key distribution systems," The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Vol. 16, Issue1, page(s): 5-13, 2017.

[6] D. D. Hodson, M. R. Grimaila, L. O. Mailloux, C. V McLaughlin, and G. Baumgartner, "Modeling quantum optics for quantum key distribution system simulation," *J. Def. Model. Simul.*, vol. 16, no. 1, pp. 15–26, Jan. 2017, doi: 10.1177/1548512916684561.

[7] L. Mailloux, M. Grimaila, D. Hodson, L. E. Dazzio-Cornn, C. McLaughlin, and L. DazzioCornn, "Modeling Continuous Time Optical Pulses in a Quantum Key Distribution Discrete Event Simulation," 2014.

[8] I. P. Kaminow, T. Li, and A. E. Willner, *Optical Fiber Telecommunications V A*, 5th Edition. Elsevier Inc., 2008.

[9] S. Ali and M. R. B. Wahiddin, "Fiber and free-space practical decoy state QKD for both BB84 and SARG04 protocols," *Eur. Phys. J. D*, vol. 60, no. 2, pp. 405–410, 2010, doi: 10.1140/epjd/e2010-00214-5.

[10] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1582–1590, 2009, doi: 10.1109/JSAC.2009.091208.

[11] S. K. Jain, Hemani Kaushal Virander Kumar, *Free Space Optical Communication ,Optical Networks*, 1st edition. Springer, 2017.

[12] S. R. by Z. Ghassemlooy, W. Popoola, *Optical Wireless Communications:System and Channel Modelling with MATLAB*, 1st edition. CRC Press, 2012.

[13] T. Schmitt-Manderbach *et al.*, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, p. 10504, Jan. 2007, doi: 10.1103/PhysRevLett.98.010504.

[14] A. I. Khaleel and S. K. Tawfeeq, "Key rate estimation of measurement-device-independent quantum key distribution protocol in satellite-earth and intersatellite links," *Int. J. Quantum Inf.*, vol. 16, no. 03, p. 1850027, Apr. 2018, doi:10.1142/S0219749918500272.

[15] R. G. Sargent, "Verification and validation of simulation models," *J. Simul.*, vol.7, no. 1, pp. 12–24, 2013, doi: 10.1057/jos.2012.20.

[16] O. Balci, "Principles and techniques of simulation validation, verification, and testing," in *Winter Simulation Conference Proceedings, 1995.*, 1995, pp. 147–154, doi:10.1109/WSC.1995.478717.

[17] Jerry Banks, "Handbook of Simulation Principles, Methodolgy, Advances, Applications and Practice", JOHN WILLEY and SON inc., 1998.

[18] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Fast and user-friendly quantum key distribution," *J. Mod. Opt.*, vol. 47, no. 2–3, pp. 517–531, 2000, doi: 10.1080/09500340008244057.

# نمذجة ومحاكاة لتقييم الإداء لقنوات الأتصال الكمية في منظومات توزيع المفتاح الكمي

**عادل فاضل مشتت*** **شيلان خسرو توفيق****

*قسم هندسة المعلومات والاتصالات/ كلية الهندسة الخوارزمي/ جامعة بغداد/ العراق

**معهد الليزر للدراسات العليا/ جامعة بغداد/ العراق

*البريد الالكتروني:adilfadhil@kecbu.uobaghdad.edu.iq

**البريد الالكتروني:helan.khasro@ilps.uobaghdad.edu.iq

**الخلاصة**

توزيع المفتاح الكمي هو أحد أنواع التجفير الكمي والذي يسمح بتبادل آمن للمفتاح الكمي بين مستخدمين تفصل بينهما مسافة كبيرة يستخدم ضمن نطاقات امنية مشددة مثل المجالات الأقتصادية ,العسكرية والحكومية. بالتالي, أصبح من الضروري خلق بيئة أفتراضية لنمذجة, تحليل والتحقق من أداء قنوات الاتصال الكمية ضمن منظومات توزيع المفتاح الكمي. في هذا العمل البحثي, تم بناء والتحقق من محاكي لقنوات الاتصال الليف البصري والفضاء الحر الكمية كجزء من منظومة توزيع المفتاح الكمي مزود براسمات المجال الزمني لغرض أختباره بشكل منفصل بأستخدام أسلوب محاكاة الزمن المستمر وبأستعمال برنامج Matlab2019a. قناة أتصال الليف البصري صممت بطول يصل الى ١٥٠كم كحد أعلى وبمعامل توهين مقداره ٠,٢ ديسيبيل/كم عند الطول الموجي ١٥٥٠نانومتر نسبة الى المواصفات التجارية لليف البصري (SM-28). بينما عند الأطول الموجية ٩٠٠نانومتر و ٨٣٠ نانومتر فأن معامل التوهين هو ٢ديسيبيل/كم و ٣ ديسيبيل/كم على التوالي. تم تصميم قناة اتصال الفضاء الحر الكمية بطول يصل ايضا الى ١٥٠كم وبمعامل توهين مقداره ٠,١ ديسيبيل/كم عند الطول الموجي ٨٦٠ نانومتر. تم التحقق من عمل المحاكي من خلال تنفيذ بروتوكول BB84 مع ملاحظة العوامل المؤثرة في أداء المنظومة عن طريق تخمين معدل نسبة الخطأ الكمي وطول المفتاح النهائي مع الاخذ بنظر الأعتبار خسائر وعيوب قنوات أتصال الليف البصري والفضاء الحر الكمية. ظهر هذا العمل عملية نمذجة عامة قابلة للتكرار لتقييم أداء المنظومات بشكل فعال. النتيجة الأكثر بروزاً والمستخلصة من بيانات المحاكاة, هو أن عملية النمذجة توفر إلأرشادات المناسبة لتصميم وتوصيف القنوات الكمية البصرية لأمكانية أستخدامها في برتوكولات توزيع المفتاح الكمي الاخرى. أظهرت خطوات التحقق من صحة النتائج لمحاكاة عناصر المنظومة تقارب جيد مع النتائج النظرية المذكورة في المراجع.