Ministry of Higher Education and Scientific Research
University of Baghdad
Institute of Laser for Postgraduate Studies

Modeling and Simulation for Performance Evaluation of Quantum Key Distribution System

A Thesis Submitted to the Institute of Laser for Postgraduate Studies, University of Baghdad in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Laser / Electronic and Communication Engineering

By
Adil Fadhil Mushatet

B.Sc. Electrical and Electronics Engineering- 2003
M.Sc. Communication and Media Engineering -2012

Supervisor
Asst. Prof. Dr. Shelan Khasro Tawfeeq

2020 AD **1442 AH**

Certification

I certify that this thesis was prepared under my supervision at the Institute of Laser for Postgraduate Studies, University of Baghdad, in a partial fulfillment of requirements for the degree of a Doctor of Philosophy in Laser/ Electronic and Communication Engineering.

Signature:
Name: **Dr. Shelan Khasro Tawfeeq**
Title: **Asst. Professor**
Address: Institute of Laser for Postgraduate Studies,
University of Baghdad.
Date: 13/ 9 / 2020

In view of the available recommendation, I forward this thesis for debate by Examining Committee.

Signature: Hanan
Name: **Dr. Hanan Jaafar Taher**
Title: **Asst. Professor**
Address: Head of the Scientific Committee,
Institute of Laser for Postgraduate Studies,
University of Baghdad.
Date: 13 / 9 / 2020

Examination Committee Certificate

We certify that we have read this thesis "Modeling and Simulation for Performance Evaluation of Quantum Key Distribution System" and as examination committee we examined the student in its contents and in our opinion it is adequate with standards as a thesis for the degree of Doctor of Philosophy in Laser/ Electronics and Communication Engineering.

Signature:
Name: **Dr. Abdul Hadi M. Al-Janabi**
Title: Professor
Address: Institute of Laser for Postgraduate Studies, University of Baghdad.
Date: 2 / 12/ 2020
(Chairman)

Signature:
Name: **Dr. Tarik Z. Ismaeel**
Title: Professor
Address: College of Engineering, University of Baghdad.
Date: 30 / 11 / 2020
(Member)

Signature:
Name: **Dr. Jassim K. Hmood**
Title: Professor
Address: Laser and Optoelectronics Engineering Dept., University of Technology.
Date: 30/11 / 2020
(Member)

Signature:
Name: **Dr. Tahreer S. Mansour**
Title: Assistant Professor
Address: Institute of Laser for Postgraduate Studies, University of Baghdad.
Date: 1 / 12/ 2020
(Member)

Signature:
Name: **Dr. Alharith A. Abdullah**
Title: Assistant Professor
Address: College of Information Technology, University of Babylon
Date: 1/ 12/ 2020
(Member)

Signature:
Name: **Dr.Shelan Khasro Tawfeeq**
Title: Assistant Professor
Address: Institute of Laser for Postgraduate Studies, University of Baghdad.
Date: 29/11 / 2020
(Supervisor)

Approved by the deanship of Institute of Laser for Postgraduate Studies, University of Baghdad,

Signature:
Name: **Prof. Dr. Hussein A. Jawad**
Title: Dean
Address: Institute of Laser for Postgraduate Studies, University of Baghdad.
Date: 6 / 12 / 2020

Dedication

To the memory of my mother… i hope I have made you proud

To my wonderful father… You are appreciated

To my awesome wife…Marwa

To my adorable siblings…Shaymaa and Adnan

To my lovely children…Sama, Mohammed & Ali

Acknowledgment

First of all, a special word of thanks to my supervisor **Asst. Prof. Dr. Shelan Khasro Tawfeeq** for her guidance, tips and very precious notes and valuable ideas with me through this thesis.

Appreciation to **Prof. Dr. Hussein A. Jawad**, Dean of the Institute of Laser for Postgraduate Studies, for his support and help during my research work.

Special thanks dedicated to **Lect. Dr. Mahmoud Shaker Mahmoud**, Deputy Dean for his encouraging words and help in completing this work.

Great gratitude to **Asst. Prof. Dr. Mohammed K. Dhaher,** Head of the Engineering and Industrial Applications Branch, for his support and cooperation to proceed in this work.

I would like to present my appreciation to **Prof. Dr. Raad Sami Fyath** for his valuable scientific notes throughout my research work.

I present my deep thanks to members of Quantum Optics and Electronics Group at our Institute, Dr. Maithem Jaber , Miss Salwa Salih, Mr. Farooq Khaleel and special thanks to **Lect. Dr. Ahmed Ismael Khaleel** for his scientific support and discussion concerning this research work.

Finally, I thank my beloved family for their help and encouragement in all my life directions.

Adil Fadhil

Abstract

Quantum key distribution is a branch of quantum cryptography, which permits secure exchange of cryptographic key between two distant partners used in high security domains such as commercial, military and governmental fields.

In this research work a generic QKD simulator based on BB84 protocol is implemented and investigated using continuous time simulation approach with Matlab 2019a. The simulator was investigated in terms of the execution of the BB84 protocol with consideration of the system performance by estimating quantum bit error rate and final secure key taking into account the practical system limitations such as using non-ideal single-photon sources and single-photon detectors, optical fiber and free space quantum channels imperfections and losses.

BB84 protocol setup consists of a transmitter with a pseudo random sequence generator unit to operate four pulsed laser sources randomly with a maximum number of binary bits of 5000. The modeled pulsed laser sources provide train of pulses with ns duration, repetition rate ranging from 0.1 MHz to 10 MHz, 1 mW peak optical output power and three different emission wavelengths (830nm, 900nm and 1550nm) which are widely used in QKD systems. The output was compared to the commercial IDQ (ID300) laser output for validation issue. The transmitter includes other modeled optical components such as linear polarizers and optical power attenuators. Two types of quantum channels are included in this simulator, optical fiber and free space channels. The modeled optical fiber quantum channel is characterized with maximum allowable distance of 150 km with 0.2 dB/km at λ=1550nm according to SMF Corning (SMF-28) specifications. While, at λ=900nm and λ=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 λ=860 nm with maximum allowable distance of 150 km also.

The receiver consists of four single-photon detectors with a non- polarizing beam splitter, two polarizing beam splitters and half wave plate. Single photon avalanche photodiode and superconducting nanowire single photon detectors models were designed depending on commercial device specifications. In this research work, the widely used C30921S silicon avalanche photodiodes and ID281 superconducting nanowire single photon detector are modeled. In this research work, only 830nm and 900nm wavelengths are examined with respect to the single-photon avalanche photodiode while 900nm and 1550nm wavelengths are examined with respect to the superconducting nanowire single-photon detector because both show maximum detection efficiency at these wavelengths.

The main contributions of this research work includes the presentation of the superconducting nanowire single photon detector technique which to the best of our knowledge was not considered previously by other QKD simulators in addition to integrating the free space channel model. Finally, each component within this simulator is supported with time domain visualizers for individual testing purpose.

The validation and testing results of both the individual models separately and the complete simulator showed a good agreement with the theoretical and experimental results reported in literatures and devices data sheets.

Contents

List of Abbreviations

Abbreviation	Description
APD	Avalanche photodiode
B92	Bennett 1992
BB84	Bennett, Brassard 1984
BBM92	Bennet, Brassard, Mermin 1992
BPRS	Binary pseudo random sequence
BS	Beam splitter
BSM	Bell state measurements
COW	Coherent one way
CPU	Central processing unit
CQP	Communicating quantum processes
dB	Decibel
DCP	Dark count probability
DCR	Dark count rate
DPS	Differential phase shift
E91	Ekert 1991
EPR	Einstein, Podolsky, Rosen
FOM	Figure of merit
FP	Fabery-Perot
FS	Free space
GB	Gain–bandwidth product
GUI	Graphical user interface
HOP	High output percentage

IM	Intensity modulator
IR	Infrared
LD	Laser diode
LOP	Low output percentage
LP	Linear polarizer
MDI-QKD	Measurement-device-independent quantum key distribution
NRZ	Non-return –to-zero
NS-3	Network simulator 3
OF	Optical fiber
PA	Power attenuator
PBS	Polarizing beam splitter
PDL	Polarization dependent loss
PMD	Polarization mode dispersion
PNS	Photon number splitting
Pol-M	Polarization modulator
POVM	Positive-operator valued measure
PRR	Pulse repetition rate
QBER	Quantum bit error rate
QCS	Quantum cryptography system
QKD	Quantum key distribution
qubit	Quantum bit
S13	Serna 2013
SARG04	Scarani, Acin, Ribordy, Gisin 2004
SMF	Single mode fiber

SNSPD	Superconducting nanowire single photon detector
SOP	State of polarization
SPAD	Single photon avalanche detector
SPDE	Single photon-detection efficiency
SSP	Six-State protocol
WCP	Weak coherent pulse
XOR	Exclusive-OR

List of symbols

symbol	Description
$\|\Psi\rangle$	Qubit general state
$\|\Phi\pm\rangle, \|\psi\pm\rangle$	Four Bell states
$\|H\rangle$	Horizontal polarization
$\|V\rangle$	Vertical polarization
$\|N>$	n-photon state
$\|\Psi_{in}>$	General optical state as an input to the detector
$P_{click}(\|\Psi_{in}>)$	Total clicks probability of the detector
α , β	Complex numbers
$\alpha_{inc.}$	Polarization of light
α_p	Fiber attenuation constant
η	Photon detection probability
Φ	The ellipticity of the wave
ω	The angular frequency
τ	The pulse width
λ	Wavelength
$\eta_{med.}$	Medium impedance
η_{loss}	Optical losses
γ	Linear polarizer angle
δ	Power attenuator attenuation level
$\sigma(\lambda)$	Atmospheric attenuation coefficient
δ_{atm}	Channel attenuation due to atmospheric effects

δ_{diff}	Diffraction-limited beam divergence loss
$\delta_{propagation}$	Channel attenuation due to channel length
δ_{det}	Detector efficiency
δ_{total}	Total channel attenuation
$\acute{\varphi}$	Internal phase shift due to a single glass-crossing
θ_{ga}	Internal incidence angle at glass-air interface
γ_{LP}	Linear polarizer angle
γ_{PBS}	Polarizing beam splitter angle
γ_{BS}	Beam splitter angle
η_{SPDE}	Single photon-detection efficiency
τ'	Gate pulse width
τ_{tr}	Effective transit time
ΔT	Reciprocal of PRR
τ_{de}	Detrap time constant
τ_{fall}	Fall time
τ_{rise}	Rise time
τ_h	Hot spot life time
τ_d	Dead time
$\Delta t'$	Time jitter
$\binom{m}{n}$	Binomial coefficient
π_1^{NPD}	Click POVM
π_0^{NPD}	No click POVM
bt,r	Telescope's secondary mirror radius

	(t: transmitter, r: receiver)
C_t	Total count rate of the SNSPD
C_j	The junction capacitance
C_s	Stray capacitance
E_0	Amplitude of the wave
GB	Gain–bandwidth product
GT_0	Total count rate of SNSPD when light source is turned off
GT	Average total resistive barrier generation rate
G_m	The enhancement in GT
h	Planck's constant
I	Optical intensity of the signal
I_f	Current steady state
I_{DM}	Primary dark current
I_b	Biasing current
k	Wave number
KEY_{raw}	Sifted bits rate
L	Link length
L_{Bob}	Bob's internal loss
l_g	Glass plate thickness
$L_{insertion}$	The insertion loss
L_{return}	The return losses
L_{PDL}	The polarization dependent loss
L_k	Kinetic inductance

M_o	Average DC gain
M	Number of G_m values
n_h	Number of hotspots
N_{tr}	Average number of carriers trapped after a current pulse
n_g	Glass refractive index
N_s	Signal source mean photon number
N_d	Decoy source mean photon number
N_{wrong}	Number of the wrong bits received
N_{right}	Number of right bits received
N_0	Mean photon number per pulse
OD	Optical depth
P_n	n-photon detection efficiency
P_{ph}	The probability of weather an incident optical pulse contains any photons or not
P_{on}	The probability of a current pulse be generated when the source is ON
P_{ap}	Afterpulse probability
P_{abs}	Absorption efficiency of the photodetector
$P_{transit}$	Transit probability
P_{av}	Avalanche triggering probability
P_R	Received power
P_T	Transmitted power
P_{single}	Average optical power of a single photon

PRR	Pulse repetition rate
P_{dark}	Probability of registering a dark counts
P_{acc}	Probability of finding a second pair within the time window
$p_n(N)$	Probability of the source to emit n- photon
$p_2\,(\,N_s)$, $p_2\,(\,N_d)$	Signal and decoy sources with Poissonian statistics
P_{avg}	Average power
P_{peak}	Peak power
$QBER_{sk}$	Calculated $QBER$ after the sifting phase
$QBER_{spd}$	Calculated $QBER$ with consideration of the ratio of the dark-count rate to the detection probability
q	Electron charge
R_{error}	Rate of wrong bits
r	Atmosphere particles radius
Rt,r	Telescope's primary mirror radius (t: transmitter, r: receiver)
r_{aa}	Amplitude reflection factor from air to air
r_{gg}	Amplitude reflection factor from glass to glass
R_s	Reflectance intensity of the light s-component
R_d	Diode resistance
R_L	Quenching resistor
R_n (t)	Hotspot resistance
t_{link}	Transfer efficiency between Alice's output and

	Bob's detectors
t_0	The point around which the pulse is shaped
T	Time interval
T_{link}	The link transmittance
t_{ag}	Amplitude transmission factor from air to glass
t_{ga}	Amplitude transmission factor from glass to air
T_p	Transmittance intensity of the light p-component
T_q	Quenching time constant
T_r	Recovery time constant
V_c	Characteristic voltage
V_f	Voltage steady state
V_b	Breakdown voltage
V_{ex}	Excess voltage
v	Frequency of the photon
ω	Angular frequency
$w_{t,r}$	Beam radius at the transmit or receive side (t: transmitter, r: receiver)
Y_s	Total yield of signal source
Y_d	Total yield of decoy source
$y_n,\ \grave{y_n}$	The relative frequencies that n-photon pulses from the signal and decoy sources are registered by Bob's detector
Y_s^m	Yield of multi-photon pulses from signal source
Z_0	Load resistor

List of tables

List of figures

Chapter One

Introduction and Basic Concepts

Chapter One

Introduction and Basic Concepts

1.1 General Introduction

Cryptography is the art of hiding information in a string of bits meaningless to any unauthorized party to ensure the security of the communication. The only crypto-system providing proven, perfect secrecy is the "one-time pad" proposed by Vernam in 1935. With this scheme, a message is encrypted using a random key of equal length, by simply "XOR" each bit of the message to the corresponding bit of the key [1]. In 1940, the information – theoretic basis for secrecy was provided by Claude Shannon. The amount of uncertainty that can be introduced into an encoded message can't be greater than that of the cryptographic key used to encode it. In order to achieve perfect secrecy, the key must be as long as the message and never be reused, that is, Vernam ciphers must be used. Distribution of completely secret, completely random, one –time pads needed for Vernam ciphers is difficult, so they haven't been widely used [2].

Research in quantum computation started by Shor who showed that quantum computers can factor much faster than classical computers, this means that public key cryptosystems are insecure. Quantum cryptography provides perfectly secure key distribution; it relies on the laws of physics rather than on ensuring that successful eavesdropping would require excessive computational effort. No information can be obtained by eavesdropping about such a transmission without disturbing it in a random and uncontrollable way likely to be detected by the channel's legitimate users [3].

The Heisenberg uncertainty principle is the essential quantum property involved, which states that the existence of pairs of properties that are incompatible in the sense that measuring one property necessarily

randomizes the value of the other. For example, measuring a single photon's linear polarization randomizes its circular polarization [4].

Quantum cryptography began in late 1960s with unpublished work by Stephan Wiesner, who explained how quantum effects can in principle be used to manufacture banknotes immune to counterfeiting, and to transmit information securely [5]. Unfortunately, this highly innovative paper was unpublished at that time and it went mostly unnoticed. In 1979, in the 20th IEEE Symposium on the Foundations of Computer Science, Gilles Brassard and Wiesner discussed the idea and discovered how to incorporate the notion of public key cryptography [4].

The breakthrough in quantum cryptography was when Bennett and Brassard realized that photons were never meant to store information, but rather to transmit it. This was also shown in Wiesner paper, who dealt precisely with the use of quantum physics for transmission of information. The two scientists Bennett and Brassard put the first step in the quantum cryptography road which is the famous BB84 protocol that is named after their initials and it was set in 1984[1, 3].

In 1991, the theoretical ideas of David Deutsch led Artur Ekert to conceive a different cryptography system based on quantum correlations and making use of EPR (Einstein, Podolsky and Rosen Paradox) and Bell's theorem. Experiments on Ekert's protocol were implemented by Mssimo Palma, John Rarity and Paul Tapster [3].

In classical information theory, the bit is the most important entity. The bit has two values, either "0" or "1", with a large energy gap separation to avoid spontaneous transition between the bit values. The quantum bit (qubit) can be defined as the quantum mechanical version of the bit. The qubit has two quantum states, $|0\rangle$ and $|1\rangle$ which can be considered as basic states that are required to establish the orthogonality in the qubit space [6].

Qubits can be created in a coherent superposition of $|0\rangle$ and $|1\rangle$, where the general state is [6],

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\, e^{i\varphi}|1\rangle \quad (1.1)$$

where,

α and β represent the amplitude coefficients of the qubit in which the quantum information is stored. These coefficients can be calculated but not measured directly.

$|\alpha|^2$ is the probability that the qubit carries the value of "0", α is a complex number

$|\beta|^2$ is the probability that the qubit carries the value of "1", β is a complex number

$$|\alpha|^2 + |\beta|^2 = 1 \quad (1.2)$$

If the qubit is measured it will be found with a probability $|\alpha|^2$ to carry the value of “0” and with probability of $|\beta|^2$ to carry the value of “1” [3].

The basic states of the qubit, $|0\rangle$ and $|1\rangle$, are superposed coherently , i.e., there is always a basis in which the value of the qubit is well defined. On the other hand, for inconsistent mix between, $|0\rangle$ and $|1\rangle$, it remains a mixture in any basis and leads to either of the two outcomes with the same probabilities [3,6]. If the following state is considered,

$$|\Psi\rangle' = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (1.3)$$

this means that with 50% probability the qubit will be found to be either in $|0\rangle$ and $|1\rangle$.

A qubit is typically a microscopic system such as an atom or nuclear spin or polarized photon. In addition to that it can be represented by a fixed pair of reliably distinguishable states (horizontal and vertical polarizations:$|0\rangle = \leftrightarrow, |1\rangle = \updownarrow$).

1.2 Quantum Key Distribution

Quantum key distribution (QKD), allows two physically separated parties to exchange a series of bits over the quantum channel, and then use part of the transmission to test for eavesdropping. If they find any discrepancy between their strings, they can infer that an eavesdropper, usually referred to as Eve, is listening and that their transmission is not secure. If they detect no errors, they can assume that the key is safe [7]. The message security relies upon the key security. In the classical cryptography systems, the key distribution issue will be raised. In conventional physics, the eavesdropper intervention causes key overheard passively, without getting caught by the legal users. QKD has been suggested as an alternative efficient solution to the eavesdropper intervention. As the quantum no-cloning theorem shows, there is no way to produce a precise copy of an unknown quantum state. So, the eavesdropping on a quantum channel makes recognizable disturbances.

Therefore, the eavesdropping effect can be detected if two users use portion of their quantum signals for testing. For low error rates values, the two users utilize the quantum signals to produce a key. Thus, if Eve has an enough amount of information on the final key, she definitely be caught, although she possesses infinite processing power and access to a quantum computer [7].

QKD uses basic laws of quantum physics to guarantee secure key exchange. The key can be used with unprecedented confidence in any classic cryptographic protocol, where it increases the security to maximum achievable value. Together with the “one-time pad” encoding, which is provably unbreakable provided the key is known solely to sender and receiver, absolutely secure communication becomes possible [4].

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 initially in such a way that the users

by subsequent consolation over non-ordinary non-quantum channel subject to passive eavesdropping can tell with high probability weather the original quantum transmission has been disturbed in transit, as it would be by in eavesdropper. If the transmission has not been disturbed they agree to use these shared secret bits and when transmission has been disturbed they discard it and try again [8].

New ideas had come to real world that depend on combining the strength of the one-time pad as a cipher technique and the field of quantum information as an application method. The result was the invention of some protocols in quantum communication that are considered as a new start in direction of cryptography that is provably unconditionally secure [8].

1.3. Quantum Key Distribution Protocols and Architectures

Different QKD protocols have been presented since the invention of the first protocol in 1984. Some protocols depend on the usage of entangled photons which require the application of a nonlinear process to generate such photons, and other protocols depend on using highly attenuated laser pulses which offer practical implementation of quantum cryptography.

The following list summarizes the protocols that depend on using single-photon or highly attenuated laser pulses:

1. BB84
2. MDI-QKD (Measurement-Device-Independent Quantum Key Distribution)
3. B92 (Bennett 1992 protocol)
4. SSP (Six-State protocol)
5. SARG04 (Scarani, Acin, Ribordy, and Gisin 2004 protocol)
6. S13 (Eduin H.Serna 2013 protocol)

While, the following list summarizes the protocols that depend on using entangled photons:

1. E91(Ekert 1991 protocol)

2. BBM92 (Bennet, Brassard and Mermin 1992 protocol)
3. DPS (Differential phase shift protocol)
4. COW (Coherent one way protocol)

In the following sections, a survey of QKD protocols mostly related to this work will be presented.

1.3.1 BB84 protocol

This famous protocol is considered as the first step in achieving QKD protocols practically. The protocol deals with a cryptographic system that consists from Alice (the sender) and Bob (the receiver) communicating over a quantum channel which was a free space (FS) in the very first experiment when Bennett and Brassard implemented it. Also they used another public channel for public conversation between Alice and Bob [8].

Various properties of photons can be employed to encode information for QKD, such as polarization, phase, and quantum correlations of entangled photons. The only requirement on the quantum states is that they belong to non-orthogonal bases of their Hilbert space, where each vector of one basis has equal-length projections onto all vectors of the other basis. That is, if a measurement on a system prepared in one basis is performed in the other basis, its outcome is entirely random and the system loses all the memory of its previous state. Considering polarization property, qubits are encoded in the polarization of individual photons. Alice sends random qubits (0 or 1) encoded in 2 different bases. Bob announces openly his choice of basis (but not the result) and Alice answers "ok" or "no". Bits with different bases are discarded (basis reconciliation). The remaining bits give the "sifted key". The BB84 protocol is summarized in Table (1.1) [9].

Table 1.1 An example for BB84 protocol [10].

QUANTUM TRANSMISSION										
Alice random bits	0	1	1	0	1	1	0	0	1	0
Random sending bases	D	R	D	R	R	R	R	R	D	D
Photon Alice sends	45°	90°	−45°	0°	90°	90°	0°	0°	−45°	45°
Random receiving bases	R	D	D	R	R	D	D	R	D	R
Bits as received by Bob	1		1		1	0	0	0		1
PUBLIC DISCUSSION										
Bob reports bases of received bits	R		D		R	D	D	R		R
Alice says which bases were correct			OK		OK			OK		
Shared information			1		1			0		
Bob reveals some bits					1					
Alice confirms them					OK					
Remaining sifted bits			1					0		
note: null means no detection D stands for diagonal R stands for rectilinear										

A common schematic diagram of quantum cryptography system (QCS) based on BB84 protocol is shown in Figure (1.1)

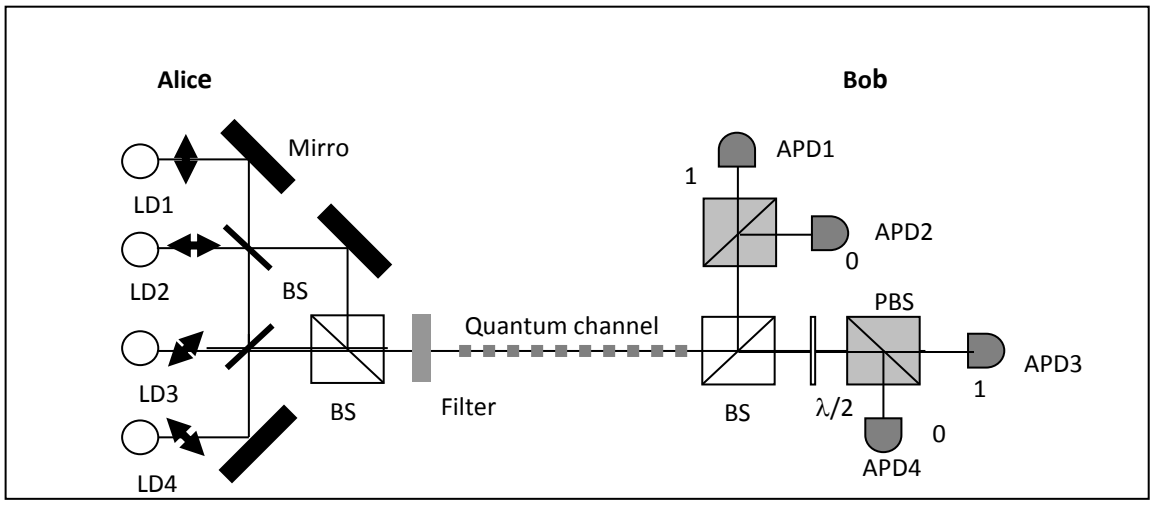


Fig.1.1 Typical quantum cryptography system based on the BB84 protocol. LD: laser diode, BS: beam splitter, PBS: polarizing beam splitter, APD: Avalanche photodiode

The QCS shown in Figure (1.1) consists of the transmitter (Alice), the receiver (Bob), the quantum communication channel FS or optical fiber (OF) and public communication channel. Alice part is constructed from [1, 10]:

- Four laser diodes with optical elements (mirrors, beam splitters (BSs)) to direct the transmitted beam to the quantum channel.
- The four laser diodes emit photons polarized at -45°, 0°, +45°, and 90°.
- For a specific qubit, the optical pulses are generated by a single laser diode and then attenuated by a set of attenuators or filters to minimize the average number of photons to be less than 1.
- These photons are transmitted to Bob using the quantum channel. It is important to maintain the polarization of these pulses at Bob for correct extraction of the information encoded by Alice.

The operation of the optical part of Bob module can be explained as follows [1, 10]:

- An incident photon first sees the 50/50 BS, at this point there are two equal probabilities that the photon either to be transmitted or reflected.
- If the photon is reflected by the BS, it passes through a half-wave plate which is set at an angle of 22.5° so that it causes a polarization rotation by 45°, mapping $+45 \rightarrow H$ and $-45 \rightarrow V$. If a +45° photon hits the half-wave plate, its polarization will be horizontal afterwards so that it will be transmitted through the polarizing beam splitter (PBS1) to be detected by APD1. A -45° polarized photon will be detected by APD 3.
- If the photon is transmitted by the 50/50 BS, it will see the polarizing beam splitter (PBS2), which in combination with the two silicon

APDs 2 and 4 analyses the polarization of the photon in the H/V basis.

- If a photon gets analyzed in the "wrong" basis, the measurement outcome is completely random. For example, if a horizontally polarized photon gets transmitted on the first BS, its polarization will be -45◦ after the half-wave plate, so that it is equally likely to be detected by APD1 or APD3.

After the steps listed in Table (1.1) are implemented other steps are applied to ensure more security for the generated key.

Quantum bit error rate calculation

$QBER$ (quantum bit error rate) is calculated after obtaining the sifted key. It is known as the ratio of the erroneous bits to the total number of received bits [1, 15],

$$QBER = \frac{N_{wrong}}{N_{wrong}+N_{right}} = \frac{R_{error}}{R_{error}+KEY_{raw}} \quad (1.4)$$

For $R_{error} \ll KEY_{raw}$, $QBER \approx \frac{R_{error}}{KEY_{raw}}$

N_{wrong}: number of the wrong bits received

N_{right}: number of right bits received

R_{error}: rate of wrong bits

KEY_{raw}: rate of the sifted bits

$$KEY_{raw} = \frac{1}{2}\, q t_{link}\, PRR N_0 \eta \quad (1.5)$$

PRR: the pulse repetition rate (Hz)

N_0: mean photon number per pulse

t_{link}: the transfer efficiency between Alice's output and Bob's detectors and can be defined as [11],

$$t_{link} = 10^{-\frac{-(\alpha_p L + L_{Bob})}{10}} \quad (1.6)$$

Where α_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.

η : is the probability of the photon's being detected

The factor q ($q \leq 1$, typically 1 or $\frac{1}{2}$) must be introduced for some phase-coding setups in order to correct for non-interfering path combinations.

Three different contributions to R_{error} can be identified:

1. R_{opt} : rates of photons that end up in the wrong detector due to imperfect interference or polarization contrast. The rate R_{opt} is given by [1],

$$R_{opt} = KEY_{raw} P_{opt} = \frac{1}{2} q N_0 t_{link} PRRP_{opt} \eta \quad (1.7)$$

where,

P_{opt}: probability of a photon going to the wrong detector.

2. The detector dark counts (or counts arising from the residual stray light in free-space installations). This count rate is independent of the bit rate. The errors will be raised when the dark counts falling within the short time period when a photon is expected [1],

$$R_{det} = \frac{1}{2}\frac{1}{2} PRRP_{dark} n \quad (1.8)$$

Where,

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

n: refers to the number of detectors.

The meaning of the two factors of $\frac{1}{2}$ is that when Alice and Bob have selected different bases, a dark count has a 50% chance of

occurrence (deleted during sifting) and a 50% chance of happening in the correct detector.

3. For systems based on entangled photon sources, error counts can appear from uncorrelated photons due to non-ideal photon sources. This error type can arise when the photons from different pairs arriving in the same time window are not necessarily in the same state [1],

$$R_{acc} = \frac{1}{2}\frac{1}{2} P_{acc} PRR t_{link} n\eta \quad (1.9)$$

P_{acc} is the probability of finding a second pair within the time window.

Through this research work, $QBER$ will be used under two different designations as will be shown in Ch.5.

1. $QBER_{sk}$: which represents the calculated $QBER$ after the sifting phase of BB84 protocol.
2. $QBER_{spd}$: which represents the calculated $QBER$ with consideration of the ratio of the dark-count rate to η. $QBER_{spd}$ can be defined as [11],

$$QBER_{spd} = \frac{P_{dark} n}{N_0 \eta t_{link}} \quad (1.10)$$

Due to fundamental laws of quantum mechanics, an eavesdropper cannot determine the polarization of a single photon if the polarization states are non-orthogonal. Even worse, she will introduce errors during the polarization measurement, so $QBER_{sk}$ of the sifted key represents an upper limit on the information an eavesdropper might have acquired. The $QBER$ is estimated during the error correction technique and is used to deduce the shrinking ratio that is required to ensure that the key information of an eavesdropper is unimportant [10].

If Eve obtained any information about the exchanged key between Alice and Bob, classical error correction and privacy amplification should be used.

Error correction is the process of correcting errors between Alice's and Bob's keys. It is done by public discussion. To implement this protocol a binary symmetric channel is assumed (BSC) that permits transmission of a string of bits. These bits are exposed to noise independently with a probability *p*. Quantum channel is an example of secret BSC channel [1, 3]. This protocol is divided into three stages BINARY, CONFIRM and BICONF. These stages are discussed briefly,

BINARY: let *n* be the length of the string sent by Alice and also the length of the string received by Bob. When these strings of Alice and Bob have odd number of errors they will perform an interactive binary search to find an error. This is done by exchanging less than (log *n*) bits over the public channel as follows,

1) The parity of the first half of the string is sent to Bob.
2) Bob tests the parity of the first half of his string and compares it with the parity sent by Alice, by this he will determine whether an odd number of errors occurred in the first half or in the second.

CONFIRM: in this stage,

1) A random subset is chosen by Alice and Bob from their strings
2) Alice tells Bob the parity of her subset
3) Bob checks if his subset has the same parity

This process is repeated k times so that to convince themselves that their strings are identical.

BICONF: In this step, steps 1 and 2 are combined to correct several errors. BICONF runs CONFIRM *s* times. In each time the parity difference between Alice and Bob subset is shown by CONFIRM, the BINARY is run by them on this subset and the error is corrected. The error correction steps are shown in the flowchart of Figure (1.2).

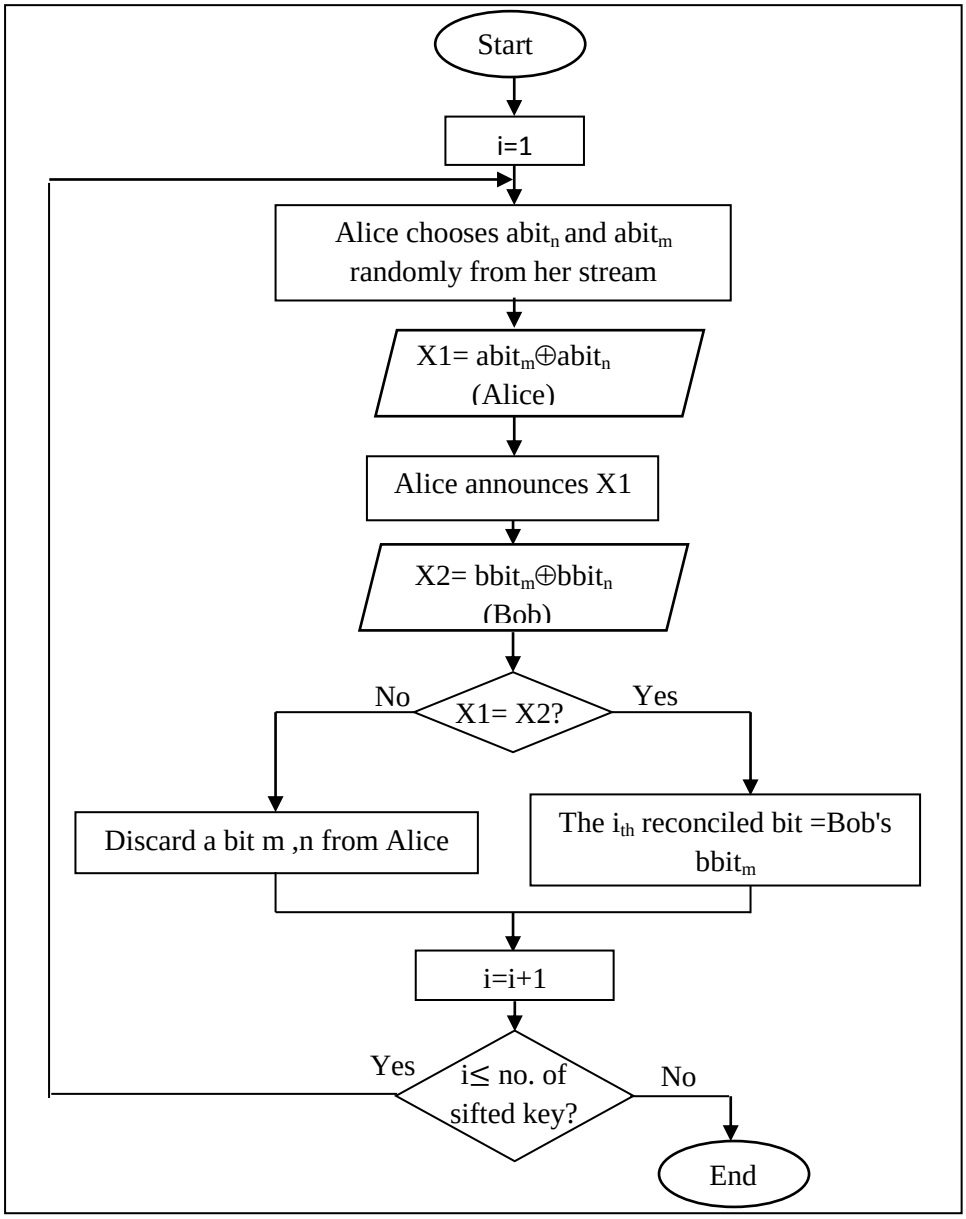


Fig.1.2 Flowchart of the error correction procedure

After completing error correction stage by Alice and Bob, they will share an error – free string. But Eve still has some information about this string during the process of error correction and previously she had information on the raw key.

Privacy amplification is the process of obtaining a nearly uniformly distributed key in a key-space of smaller bit size. By carrying out privacy amplification the key must be shortened by the number of bits of information that have been potentially leaked to Eve [1, 3].

The privacy amplification steps are shown in the flowchart of Figure (1.3).

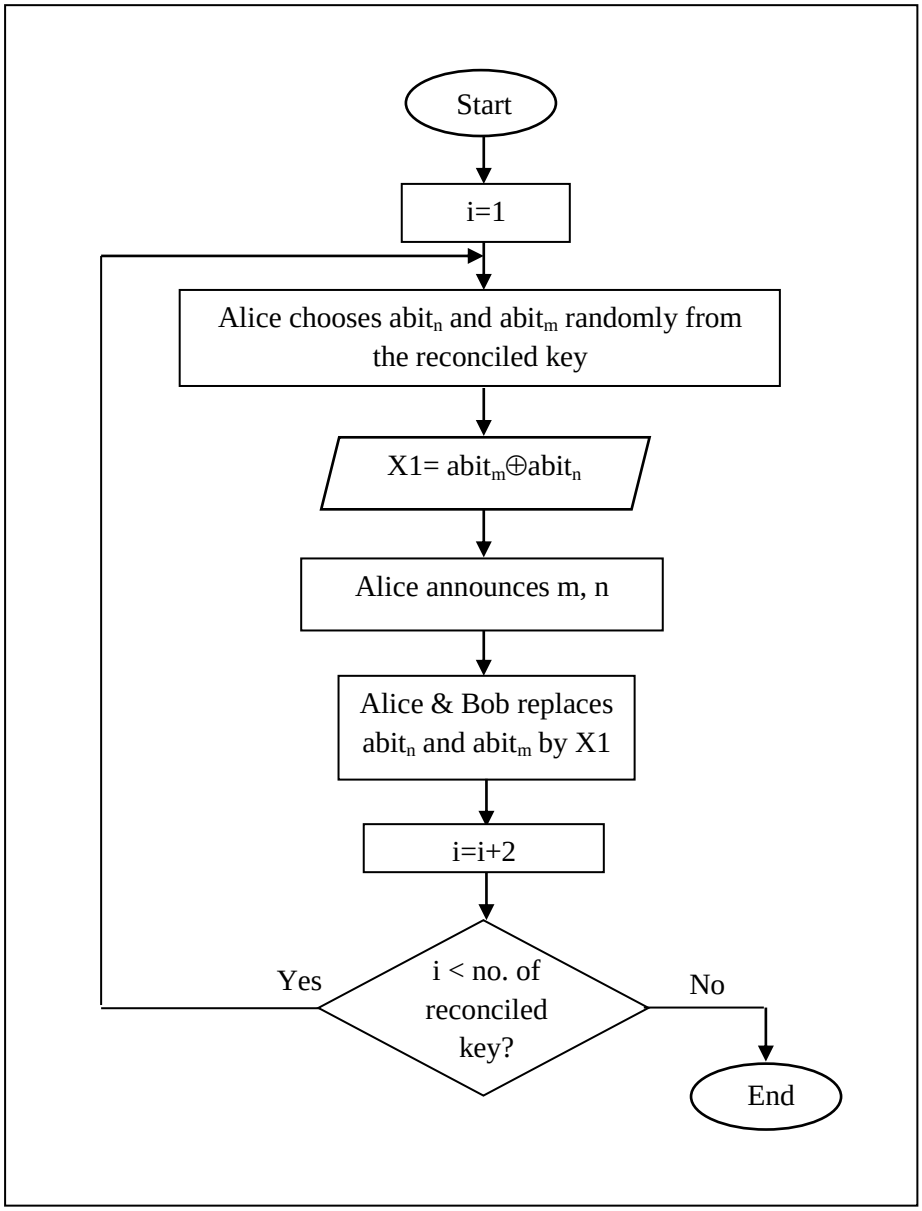


Fig.1.3 Flowchart of the privacy amplification procedure

1.3.2 BB84 protocol with decoy states

Alice adopts two photon sources, that is, signal source with mean photon number N_s and decoy source with mean photon number N_d. Signal source is used to distribute key. Decoy source is used to detect the photon number splitting (PNS) attack. For signal source $N_s < 1$, that is, it mostly emits single photon pulses. For decoy source $N_d \geq 1$, that is, it mostly emits multi-photon pulses. The polarization of the pulses of the decoy source is

randomized such that it cannot be distinguished from those of the signals source as long as photon numbers of the pulses are the same [12, 13].

In this protocol, Alice executes BB84 protocol using signal source. However, the signal source S is randomly replaced by the decoy source S′ with a probability α at Alice's side. Bob states that he has received all the transmitted photon signals. After that, Alice declares which signals are sent from the decoy source. Using public communication link, Alice and Bob investigate the overall yield of signal source Y_s and that of decoy source Y_d [12, 13],

$$Y_s = \sum_n p_n (N_s) y_n \quad (1.11)$$

$$Y_d = \sum_n p_n (N_d) y_n^{\backslash} \quad (1.12)$$

where ,

y_n & $y_n^{\backslash}$ represent the relative frequencies of the registered n-photon signals that are generated by the signal and decoy sources respectively at Bob's detector.

$p_n(N)$: the probability of the source to emit n- photon.

If Y_d value is large compared to Y_s, the protocol will be aborted by Alice and Bob. On the contrary, the protocol will be continued by investigating yield of n-photon pulses from signal source, Y_s^m, using the yield of decoy source Y_d as follows:

where,

$$Y_s^m = \sum_{n=2}^{\infty} p_n(N_s)\, y_n \quad (1.13)$$

Eve's optimal choice is to block pulses containing more than 2 photons. In order that the protocol be secure, the total number of pulses that are detected must be greater than that of attacked ones so the condition for security is,

$$Y_s > \frac{p_2\,(N_s)}{p_2\,(N_d)} Y_d \quad (1.14)$$

Equation (1.10) represents an estimation for the amounts in the status where the attenuated laser pulses are generated by both signal and decoy sources with Poissonian statistics $p_2\,(N_s)$ and $p_2\,(N_d)$ of photon numbers

n, respectively. The same steps for calculating $QBER$ followed by error correction and privacy amplification techniques will be applied to obtain the final secure key as in BB84 protocol.

1.3.3 Measurement-Device-Independent Quantum Key Distribution protocol

The main advantages of Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) protocol are the following [14]:

1. It removes all the detector's side channels and loopholes which threaten security.
2. System performance improvement by using decoy states.
3. It can be implemented with commercial available devices, which makes the protocol more practical. For example, the protocol can be implemented with coherent states instead of entangled or single photons.

Figure (1.4) shows the basic setup for MDI-QKD protocol.

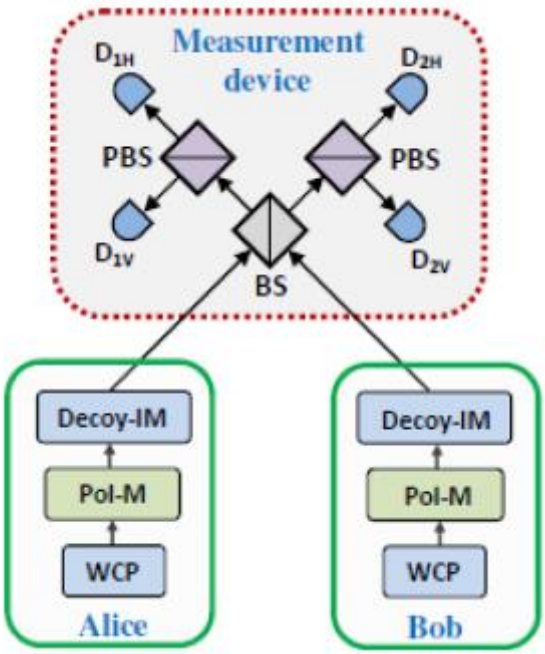


Fig. 1.4 Basic setup of MDI-QKD protocol. Pol-M: polarization modulator; IM: intensity modulator [14]

In MDI-QKD protocol, all measurements are carried out in the rectilinear basis. The incoming photons meet at a 50:50 BS and get projected into either vertical (V) or horizontal (H) polarization states after passing PBSs. Four single photon detectors (SPADs) are used to detect the photons. A successful Bell state measurements (BSMs) [15, 16] is observed when precisely two differently polarized detectors are triggered. BSM have the following forms [15, 16],

$$|\psi-\rangle = 1/\sqrt{2}\ (|HV\rangle - |VH\rangle) \quad (1.15)$$

$$|\psi+\rangle = 1/\sqrt{2}\ (|HV\rangle + |VH\rangle) \quad (1.16)$$

$$|\Phi-\rangle = 1/\sqrt{2}\ (|HH\rangle - |VV\rangle) \quad (1.17)$$

$$|\Phi+\rangle = 1/\sqrt{2}\ (|HH\rangle + |VV\rangle) \quad (1.18)$$

Where

$|\psi-\rangle$ and $|\psi+\rangle$ represent two different qubits.

$|\Phi-\rangle$ and $|\Phi+\rangle$ represent two same qubits.

Table 1.2 shows the states resulting from BSM (referred to Figure 1.4) [14].

Table 1.2 BSM outcomes

Projection into	**A click in**
$\|\psi^+\rangle$	(D_{1H} & D_{1V}) or (D_{2H} & D_{2V})
$\|\psi^-\rangle$	(D_{1H} & D_{2V}) or (D_{2H} & D_{1V})

Table 1.3 summarizes all the valid basis-compatible BSM measurements assuming two cases, the case where single-photon states are sent out by Alice and Bob and the case where weak coherent pulses are sent (which is the actual case in real MDI-QKD protocol).

Table 1.3 Probabilities for basis-compatible valid BSM outputs [14]. SOP: state of polarization, WCP:Weak coherent pulse

Z basis		BSM output				X basis		BSM output			
SOPs		Single-photons		WCPs		SOPs		Single-photons		WCPs	
Alice	Bob	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	Alice	Bob	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
$\|H\rangle$	$\|H\rangle$	0	0	0	0	$\|45\rangle$	$\|45\rangle$	1	0	0.75	0.25
$\|V\rangle$	$\|V\rangle$	0	0	0	0	$\|135\rangle$	$\|135\rangle$	1	0	0.75	0.25
$\|H\rangle$	$\|V\rangle$	0.5	0.5	0.5	0.5	$\|45\rangle$	$\|135\rangle$	0	1	0.25	0.75
$\|V\rangle$	$\|H\rangle$	0.5	0.5	0.5	0.5	$\|135\rangle$	$\|45\rangle$	0	1	0.25	0.75

1.4 QKD Non-idealities and Eavesdropping Strategies

In order to implement QKD in real-life, ideal models should be used to verify security proofs, which is not the case in reality, as imperfect single-photon sources and detectors in addition to the noisy communication channel that are commercially available, opening the door for different eavesdropping attacks to be launched against QKD systems. In the following sections, some of the QKD implementations non-idealities and eavesdropping strategies will be reviewed.

1.4.1 QKD implementations non-idealities

Instead to using ideal single photons sources, attenuated optical pulses are used with $N_0 = 0.1$ to reduce the leakage information but at the expense of reducing the protocol efficiency. The existence of multiple photons in an attenuated optical pulse gives a chance to eavesdropper to use these events to gain information about the key without introducing any extra errors [17].

All quantum cryptographic systems suffer from a main problem. For polarization based encoding systems , the polarization must be kept constant over tens of kilometers, while in interferometric systems , which are generally based on two unbalanced Mach-Zehnder interferometers, they must be adjusted with respect to each other every few seconds to compensate for thermal drifts.

Regarding the transmission media for these systems, choosing OF channel or atmosphere as a transmission media depends on the corresponding wavelengths , for 1330 nm and 1550 nm OF channels are preferred for their low loss at these wavelengths while for 860 nm FS channel is preferred because of the availability of efficient single-photon detectors (SPDs) at this wavelength. OF channels suffer from that polarization of photons is changed with the increase of fiber length due to the birefringence character.

In addition, using photons in QKD systems present a problem of losing the photons in the quantum channel by which the transmission distance is limited to the order of 100km. Practical SPDs have low detection efficiency and rate that leads to an increase in $QBER$. All of these issues will reduce the final secure key rate, erroneous sifted key is created and overall $QBER$ will be increased [17]. The impact of these types of non-idealities on the QKD systems performance is considered through the next four chapters.

1.4.2 Eavesdropping strategies

Mainly, there are two types of eavesdropping, intercept / resend and beam-splitting assuming that Eve has the technology for dealing with single light pulses, i.e., including photodetection and the ability of storing a pulse for an arbitrary long time before measuring it.

1.4.2.1 Intercept / resend strategy

In intercept / resend strategy, Eve intercepts selected light pulses and then reads them in her own choice. For each pulse received by Eve with a probability equal to N_0, efficient detectors will detect the received photons successfully [4]. When this occurs, the received pulses are fabricated and sent to Bob with the same polarization detected by Eve. To ensure that Bob is unsuspicious about the presence of Eve, Eve’s fabricated pulses should be of such intensity slightly higher than one expected photon per pulse in order to have the same net rate of pulse detection by Bob as in the case of no eavesdropping [4].

1.4.2.2 Beam-splitting strategy

This type of attack depends on that weak coherent pulses contain more than one photon in each pulse. The attack is achieved by using a partly – silvered mirror by Eve to divert a fraction of the original beam's intensity to herself, letting the other part to pass to Bob undisturbed. Eve stores her share of each pulse in order to avoid wasting information by measuring pulses in the wrong bases. She stores the pulses until Alice and Bob announce the correct bases by their public discussion then she measures the stored pulses in those bases [4].

The presence of Eavesdropping disturbs the communication between Alice and Bob and errors will be introduced in the sifted key bits, sometimes the presence of Eve will not be noticed by Alice and Bob and it is not the only source of error in quantum cryptographic systems. Physical imperfections in a quantum channel introduce noise and also misalignment may introduce an additional source of errors. To get around these problems Alice and Bob need to reconcile their keys (correcting errors) to make them identical, and then applying privacy amplification for further security but at the expense of more shortening for the final key length [1].

1.5 The Structured Flow of the Modeling Process and the Methodology Used

The purpose of QKD modeling is to efficiently relate the system 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 such as the temperature [18].

The QKD system simulator modeling process involves set of actions. The representation of these actions is known as the software development model. In this section, the structuring flow of the software development

model that utilized to implement this simulation tool, is explained in addition to the methodology used in this research work.

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 [19, 20].

In this work, the software development model structure consists of four stages arranged as a top-down flow as shown in Figure (1.5).

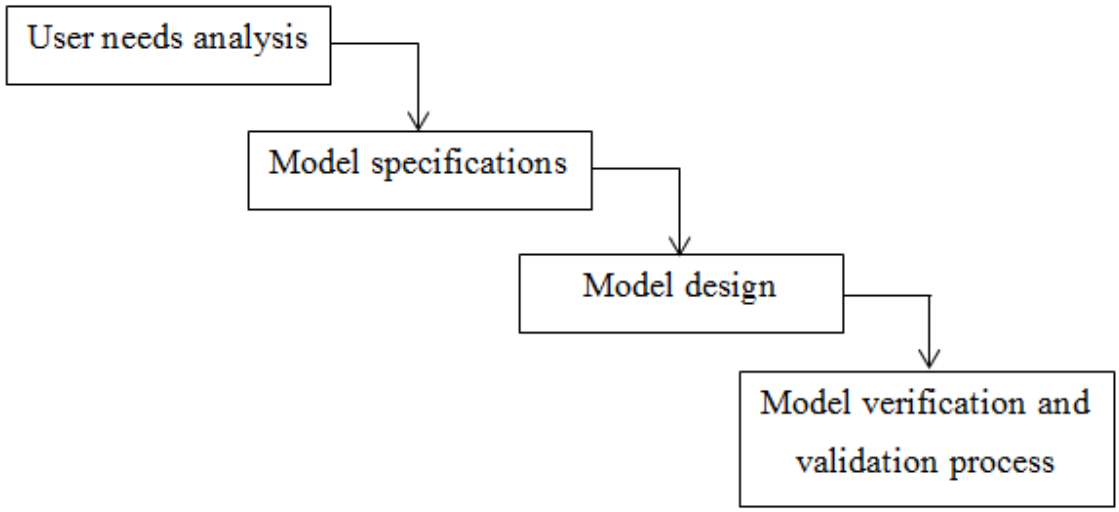


Fig.1.5 QKD simulator software development model

In a nutshell, each stage is explained as follows:

1. User needs analysis

In this stage, the user prerequisites that the designed QKD simulator can achieve are analyzed. The simulator requirements focused on successfully building the BB84 protocol as a first step and investigating the $QBER$ and the final secure key under different operation conditions as well as it should be flexible enough to implement other QKD protocols with the possibility to select different modeled physical components.

2. Model specifications

In this stage, the inputs provided from the simulator's user with the expected outcomes are defined. Figure (1.6) represents the simulator specifications as inputs and outputs.

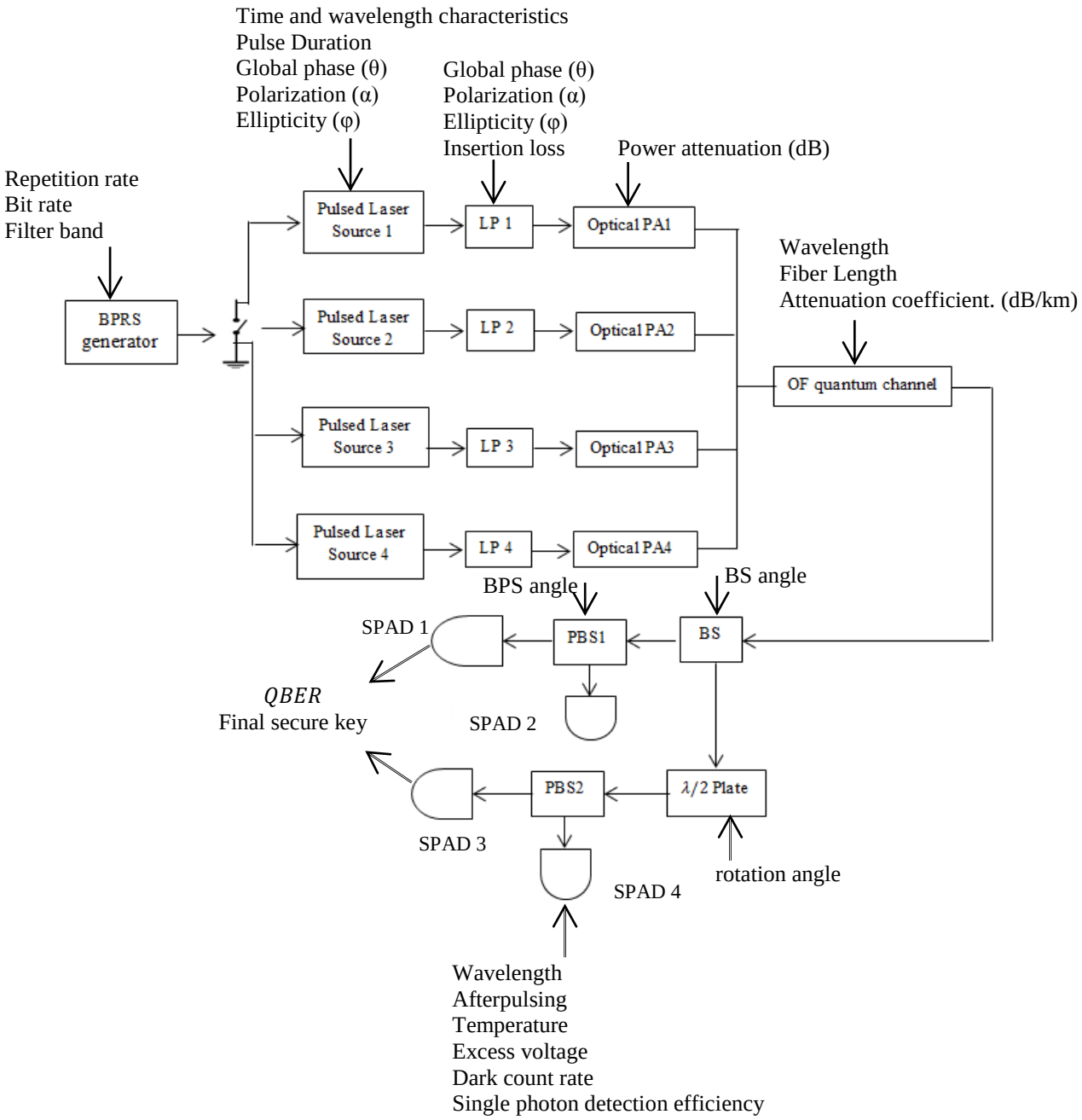


Fig.1.6 Input and output of the QKD simulator. BPRS: binary pseudo random sequence, LP: linear polarizer, BS: beam splitter, PBS: polarization beam splitter, OF: optical fiber, PA: power attenuator.

3. Model design

The QKD simulator is implemented using Matlab 2019a as it provides the essential built in math functions in addition to the programing basics that are found in the main programing languages. 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 approach that has been used as an 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 (1.7) shows the designed model reference layers that consist of three layers each with a specific objective. The outer layer represents the protocol type selection by the user.

Up to this time, only BB84 protocol was demonstrated. The middle layer represents the main QKD operation phases that involve the optical signal generation, transmission, reception and detection. These steps were built using various modules which consists from different integrated physical modeled components. For example, the optical signal preparation and generation phases can be conducted using the transmitter module which consists of binary pseudo random sequence generation unit (BPRS), pulsed laser source, linear polarizer (LP) and optical power attenuator (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.

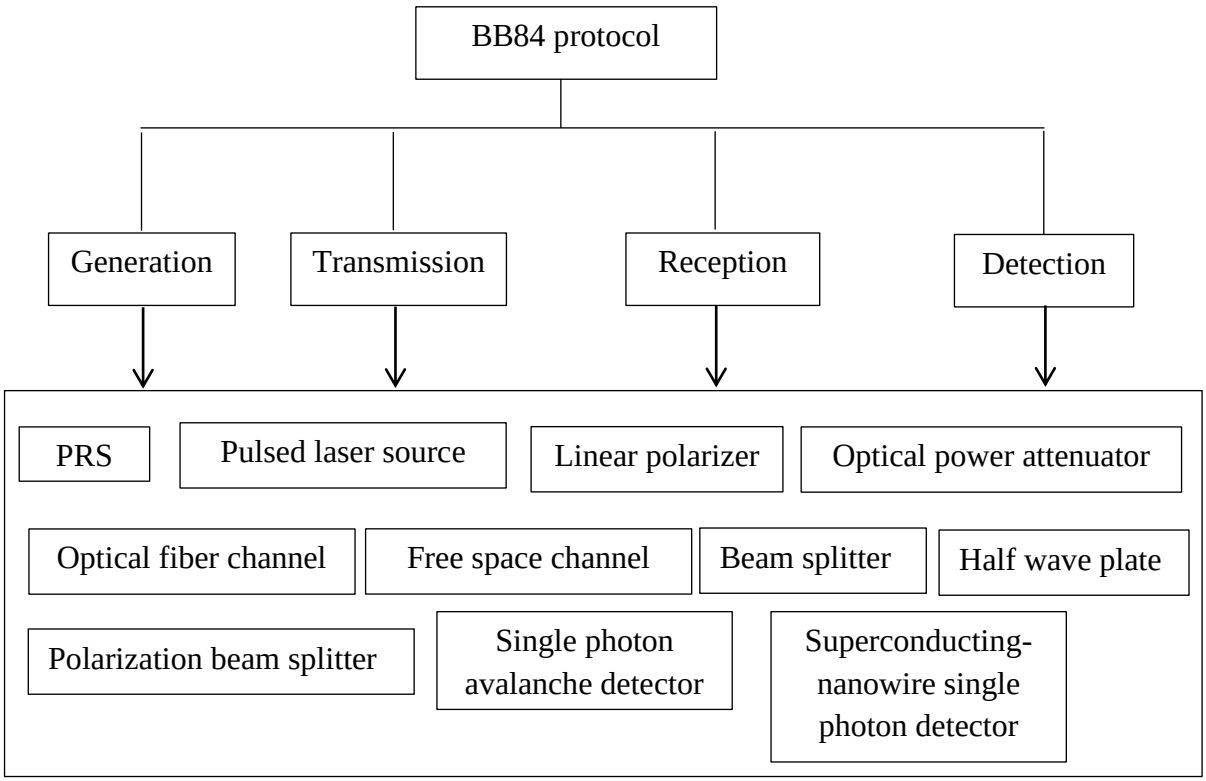


Fig.1.7 QKD simulator reference layers

4. Model verification and validation process

As the modeling are progressively being utilized to help in finding answers to the problems which are difficult to deal with practically, the credibility of the simulation models and their results should be verified [19].

The correctness of the simulation model results can be tested through verification and validation of the simulated model. Literaturally, model verification can be defined as "*ensuring that the computer program of the computerized model and its implementation are correct*" [19]. While, model validation is explained as "*substantiation that a computerized model within its domain of applicability possesses a satisfactory range of accuracy consistent with the intended application of the model*"[20]. Model validation is "*the comparison of model behavior to the behavior of the system under study when both are responding to identical input conditions*"[19].

For each modeled component, the verification process is used to ensure that the simulation model has been coded properly and the programming is in a hierarchical and structured form as recommended by Sargent [19].

The approach that has been used for model verification was by running the models individually under different circumstances and conditions by apply inputs to the component and check the outcomes. The calculated results will show how the model programmed in a sufficient and correct way by determines the response of the model to the input parameters.

In this research, Matlab compiler was used to prove the model verification by testing the code line by line [19].

With respect to the validation technique that has been utilized for each modeled component, the validation approach that was applied on the conceptual and mathematical models as recommended by Sargent [19] was established by the help of the specialized references and publications in the field, commercial data sheets of the optical component to define the allowed input and output limits.

The last step in the validation process used in this research was to test the operational validity of the modeled components. The validation of component operation as defined by Sargent is determining whether the simulation model's output behavior has the accuracy required for the model's intended purpose over the domain of the model's intended applicability [19].

Thus, the methodology that was followed to ensure that the modeled components and hence the modeled QKD simulation framework are sufficiently valid to investigate the performance of the QKD parts individually or as a complete system was to compare the modeling output behavior to the output of other correct and confidence model or to the output from real optical devices. As the modeling results match the valid

models results, the validation will be increased and thus the reliability in the modeled component and its results will be increased too.

In order to connect the ideas presented in the verification and validation activities to the modeling and simulation process, Figure (1.8) shows the most general version of the model design process.

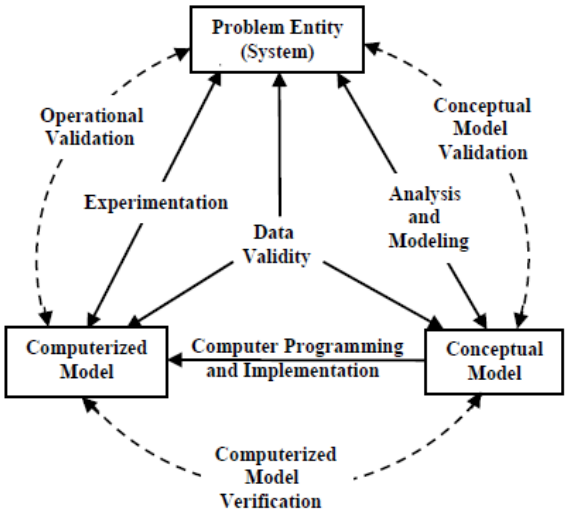


Fig.1.8 General model design process [19]

In this research, three methods were followed to test the validity of the modeled components,

Method 1: Some modeled components behavior is compared to the known results of analytic models as recommended by Sargent, Balci and Banks [19, 20]. This method was used in this work because basically the modeled QKD framework is not intended to simulate any real QKD system but to evaluate the capabilities of the modeled QKD framework presented in this thesis.

The results of the validated mathematical models for the modeled components are compared to the results of the modeled components to test the validation degree of the modeled components.

This approach was applied on the modeled optical components in addition to the quantum OF and FS channels to investigate their validity as will be seen later in the next chapters.

Method 2: This method was used to test the validity of the other modeled components by comparing the results of the modeled components to the results of the valid simulation models as recommended by Sargent, Balci and Banks [19, 20].

This approach was applied on the modeled pseudo binary random generator unit and the modeled laser source to test their validity as will be seen in Ch.2.

Method 3: This method was used to test the validity of the last modeled component by comparing the results of the modeled component to the results from real optical devices as recommended by Sargent, Balci and Banks [19, 20].

This approach was applied on the modeled SPAD and SNSPD components to test their validity as will be seen later in Ch.4.

As it is known that the detection unit is the heart of the QKD systems, the first method was also used to test the validity and the correctness of this unit.

In general, the validation of the QKD system modeling tool was proved via sequence of test cases under different operation conditions and with different input parameters as will be seen later in the next chapters. This methodology of the test cases applied to all the modeled components and modules in addition to the final QKD modeling tool.

The methodology for the modeling process for each component and module that was followed over this research work is similar as shown in Figure (1.9).

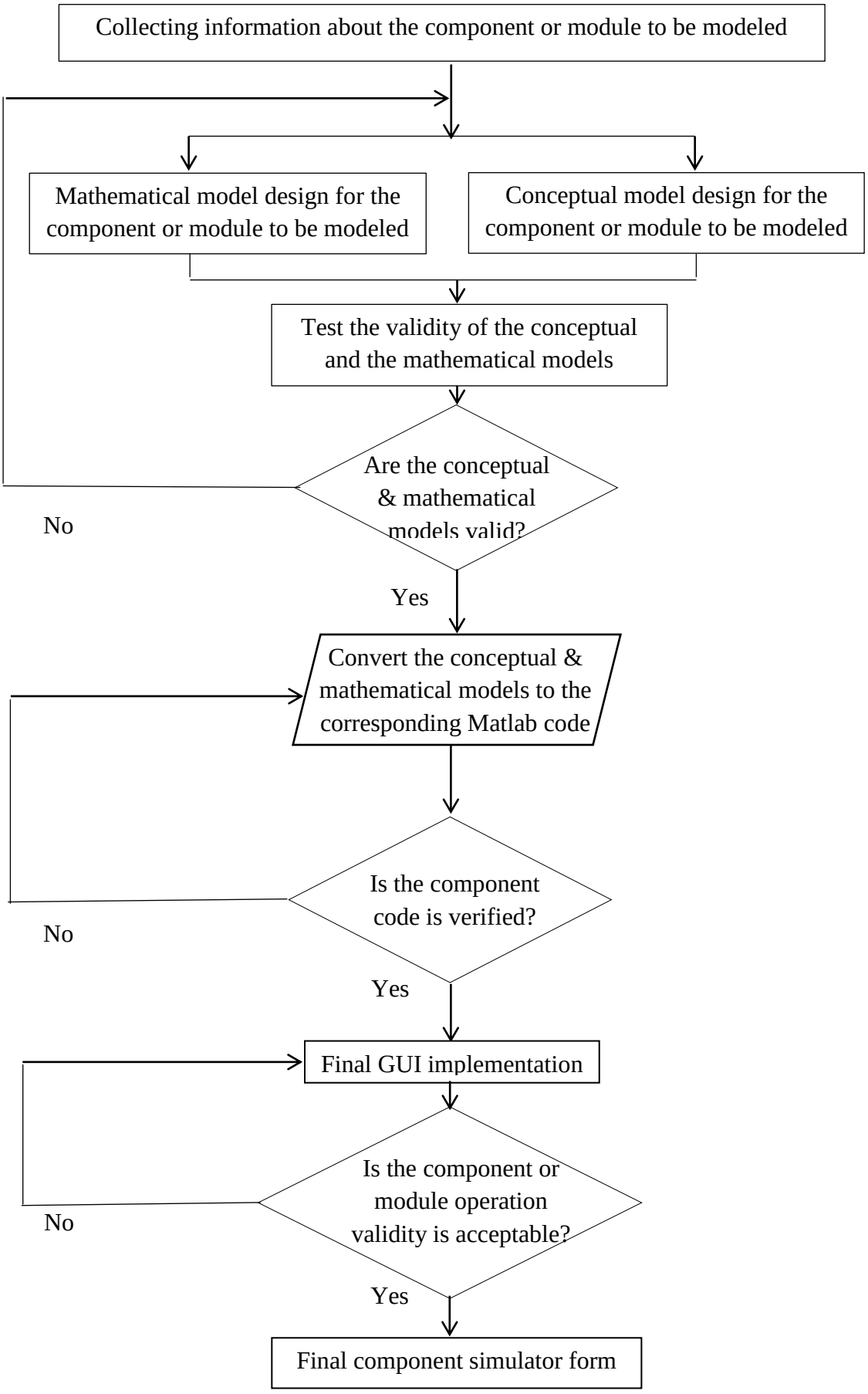


Fig.1.9 Modeling process steps. GUI: graphical user interface

1.6 Problem Statement

Each QKD system, whether commercial or research, is a unique implementation based on the theory and principles of QKD using currently available components, protocols, and technology. As there are no widely accepted security and performance standards for evaluating QKD systems, each system designer architects their system based on their own views and needs. The ability to model accurately and simulate QKD systems at an appropriate abstraction level is an essential capability necessary for analysis of current and next generation QKD cryptographic systems.

Currently, there is a need to develop a flexible, extendable, quantum communication modeling and simulation analysis framework that take advantage of all the best practices in modeling, simulation, and analysis and model QKD systems at an appropriate detailed level to estimate system-level attributes in security, performance, and cost.

Different versions of the simulation study exist; the focus of this research is on the following steps (identifying the problem, setting the objectives and conceptual modeling) leading to two essential issues in building any efficient simulator that are the correct validation and verification for the designed simulator.

1.7 Aim of the Work

The aim of this work is modeling environment tools, which are intended to deal with quantum cryptography systems, by designing and executing a simulator to understand and examine the operation of QKD systems by demonstrating the BB84 protocol and evaluate its performance in terms of $QBER$ and key distribution process efficiency considering the limitations imposed by using practical components.

1.8 Literature Review

Since the presentation of the first QKD protocol (BB84) in 1984, various approaches have been investigated to implement a simulation tool to observe the performance of the QKD implementations and protocols. The following summary shows some of these studies.

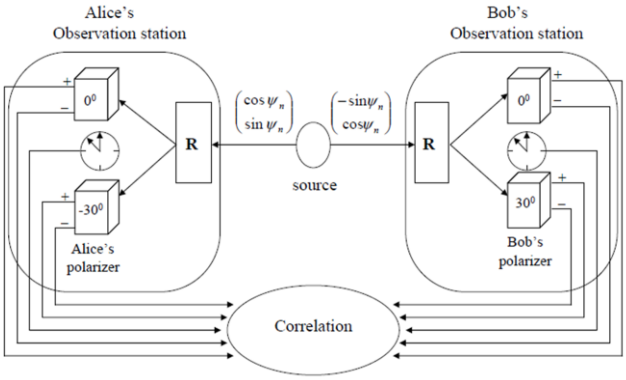
(1) 2008-Shuang Zhao and Hans De Raedt [21**]**

Simulated protocols: BB84 and Ekert protocols.

Approach applied: event by event method was used for the first time.

Simulation tool: Matlab.

Aim of the work: to demonstrate the bits transmission through the system using BB84 and Ekert protocols with and without eavesdropper but without taking into consideration the channel losses and noise.



The proposed simulation scenario

(2) 2011- Marcin Niemiec, Łukasz Romański, and Marcin Święty [22**]**

Simulated protocols: BB84, B92 and other protocols.

Approach applied: object oriented programming approach.

Simulation tool: C++ language.

Aim of the work: to simulate the operation of QKD protocol to provide information about the transmitted key rate, $QBER$ that is determined by some parameters such as transmission channel and eavesdropping.

(3) 2012-Zhu Lijuan [23**]**

Simulated protocol: BB84 protocol.

Approach applied: object oriented programming approach.

Simulation tool: C# .Net language.

Aim of the work: to demonstrate BB84 protocol under the effect of eavesdropper and without taking into consideration the channel limitations.

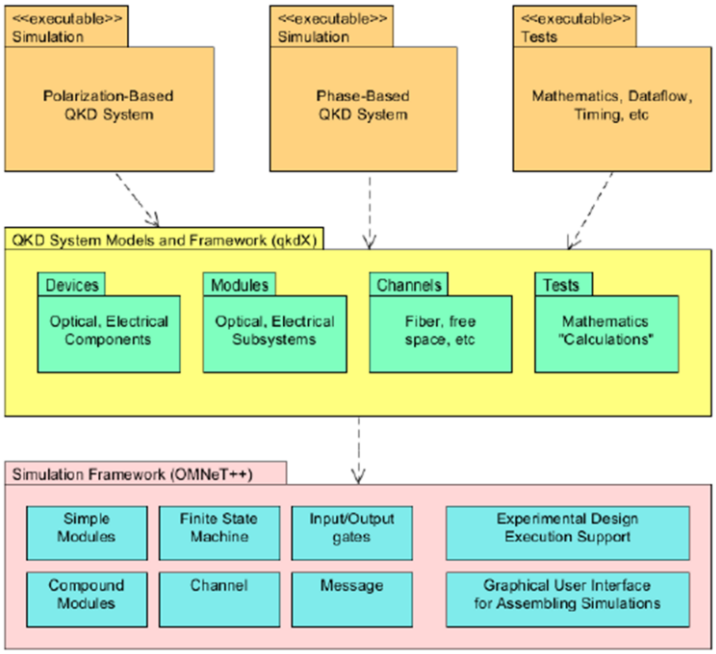
(4) 2015-Logan O. mailloux, Jeffrey D. Morris, Michael R. Griamaila, Douglas D. Hodson, David R. Jacques, John M. Colombi, Colin V. McLaughlin and Jennifer A. Holes [18**]**

Simulated protocols: different QKD protocols.

Approach applied: discrete event approach.

Simulation tool: OMNeT++.

Aim of the work: a complete framework known as (qkdx) has been designed to implement different QKD protocols tacking into account the system non-idealities and to conduct different performance analysis under different operation conditions.



qkdx simulation platform architecture

5) 2015- Logan O. Mailloux, Michael R. Grimaila, John M. Colombi, Douglas D. Hodson, Ryan D. Engle, Colin V. McLaughlin, and Gerald Baumgartner [24**]**

Simulated protocol: Decoy state protocol.

Approach applied: discrete event approach.

Simulation tool: OMNeT++.

Aim of the work: to simulate the decoy state protocol and to investigate the procedure followed to detect photon number splitting attacks.

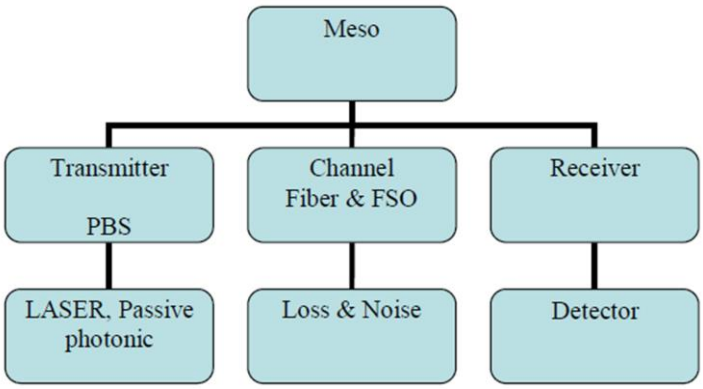
(6) 2016-Abudhahir Buhari1, Zuriati Ahmad Zukarnain, Roszelinda Khalid, Ahmad Zakir Dato and Wira Jaafar [25**]**

Simulated protocol: Non-Entangled based QKD experiment.

Approach applied: discrete and continuous event.

Simulation tool: commercial photonic simulation software OptiSystem.

Aim of the work: to study the QKD implementations using a combination of micro, meso and macro parts to model real world QKD experiments. Microscopic part deals with the qubits, macroscopic part represents the QKD system components and mesoscopic simulation is considered as a link between the microscopic and the macroscopic parts that defines any change in microscopic properties according to the macroscopic properties.



Classification of Meso simulation

(7) 2017-Miralem Mehic, Oliver Maurhart, Stefan Rass and Miroslav Voznak [26**]**

Simulated protocols: different internet networks protocols.

Approach applied: discrete event approach.

Simulation tool: The network simulator NS-3

Aim of the work: to simulate QKD network protocols and investigate the QKD network performance in terms of key generation rate and traffic management.

(8) 2016-Xilong Mao, Yan Li, Yan Peng, and Baokang Zhao [27**]**

Aim of the work: A simulation tool consists of main QKD system components i.e. light source, channel and the SPD used to simulate the QKD system. The main contribution of this tool is to get the generated raw key in hexadecimal as an output and then use it for further works.

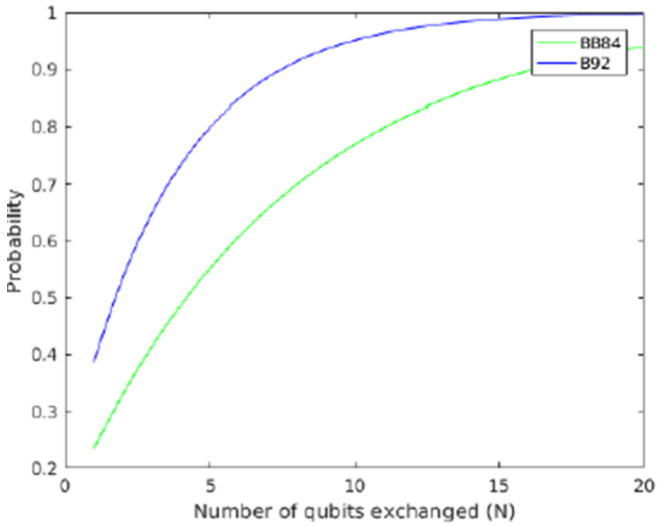
(9) 2018- Satya Kuppam [28**]**

Simulated protocols: BB84 and B92.

Approach used: discrete event approach.

Simulation tool: Communicating Quantum Processes (CQP) language.

Aim of the work: to demonstrate BB84 and B92 protocols under Eve effect and compare between them in terms of their resistance against eavesdropper.

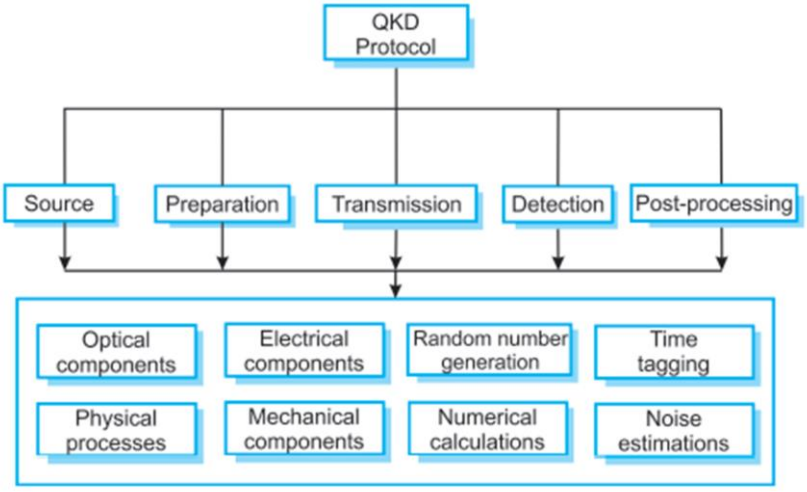


Comparison between BB84 and B92 in terms of Intercept Resend eavesdropper detection

(10) 2020- Rishab Chatterjee, Kaushik Joarder, Sourav Chatterjee, Barry C. Sanders, and Urbasi Sinha [29**]**

Simulated protocol: B92.

Aim of the work: to simulate B92 protocol and to analyze the system behavior in terms of key rate and $QBER$ with considerations the practical system problems and limitations.



Simulation tool reference architecture

1.9 Thesis Layout

This thesis is divided into six chapters

Chapter One gives general introduction and the main concepts about quantum cryptography and QKD. Different types of QKD protocols are presented. The aim of this study and the scientific method that was used in this work are discussed at the end of the chapter.

Chapter Two gives a detailed theoretical background about the QKD transmission parts in addition to extensive explanation of the modeling steps that have been utilized to model each part with samples of testing that was carried out on each component.

Chapter Three presents the material required to model both quantum channel types, OF and FS channels. The modeling methodology that has been used supported by some performance evaluation test will be reported.

Chapter Four contains the identification of the QKD receiver model. The exploration for each part begins with a general component explanation, the most important component behavior of interest will be the basis of the component conceptual model and the mathematical model that takes into account the performance parameters believed to be important for modeling the QKD receiver parts will be introduced. The design of the most important and emerging single-photon detection technologies, SPAD and SNSPD will be presented. Finally, samples of modeled output with the analysis for each modeled optical component will be presented.

Chapter Five includes the final version of the QKD simulator with a demonstration of the BB84 protocol as a case study**.** Initial implementations of this simulator will be addressed and tested. The results obtained from the simulation of the BB84 protocol phases to study the performance of the QKD system considering the distributed keys length and $QBER$ under the effect of using both quantum channel types will be presented.

Chapter Six presents the main conclusions and suggestions for future work.

Chapter Two

The Transmitter of the BB84 Protocol

Chapter Two

The Transmitter of the BB84 Protocol

2.1 Introduction

The purpose of this chapter is to identify the transmitter of the BB84 protocol. The exploration for each part begins with a general component explanation obtained from data sheets and related reference literatures. Based on this research, the most important component behaviors of interest will be the basis of the component conceptual model which will be the first modeling step. Later, the mathematical model that takes into account the performance parameters believed to be important for modeling the BB84 protocol transmitter parts will be presented. Finally, samples of modeled output with the analysis for each modeled optical component will be presented. Figure (2.1) illustrates the main BB84 transmitter parts and the modeling flow that has been conducted in this research.

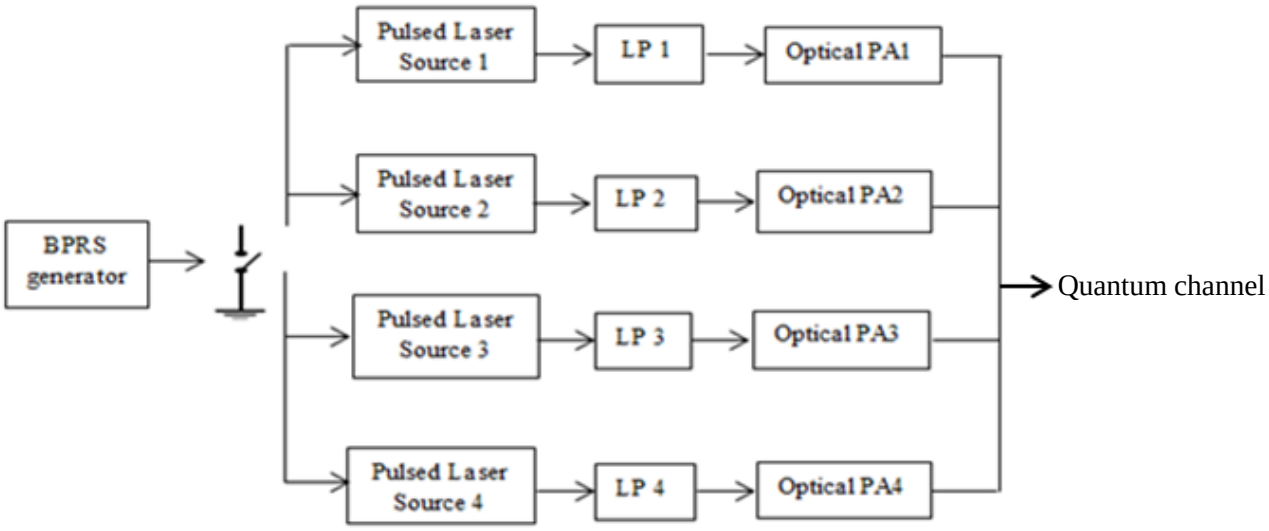


Fig.2.1 The model of the BB84 protocol transmitter

2.2 The Pulsed Laser Source Module

This section outlines the methodology used to model the pulsed laser source. It gives a vision to the operation basics of this component, the concept and the mathematical models that have been used for modeling.

Laser pulse simulation results with the final laser module Graphical User Interface (GUI) will be presented and discussed at the end of this section.

2.2.1 The Device description

The optical source is designed to generate coherent optical pulses that simulates the pulses generated from commercially available laser source.

In the practical setting of any quantum cryptography system, it is the almost only option to substitute single qubits in the original BB84 QKD protocol and other related protocols with heavily attenuated laser pulses because the perfect single-photon emitting devices are not commercially available in the current technology [30].

For coherent laser sources that output a signal which obeys Poisson distribution, the occasional production of multi-photon signals is inevitable no matter how heavily the laser sources are attenuated [31]. In fact, even for these weak pulses, the probability of having two or more photons per pulse may not always be neglected, which gives a malicious eavesdropper (Eve) a chance to obtain some amount of information on the shared key by a photonnumber-splitting attack [30].

The statistical distribution of the number of photons depends on the nature of light source and must be treated by using quantum theory of light. However, under certain conditions, the arrival of photons may be regarded as independent occurrences of a sequence of random events at a rate equal to the photon flux, which is proportional to the optical power [32].

In quantum picture of light, light is considered to consist of a stream of photons. The photon flux φ can be found from the average power (P_{avg}) in the beam [32],

$$\varphi = \frac{P_{avg}}{h\upsilon} \text{ (Photon/ s)} \quad (2.1)$$

υ: is the frequency of the photon

h: is the Planck's constant (6.625×10^{-34} J.s)

A beam of light with a photon flux will nevertheless have random photon number fluctuations at short time intervals [32].

Although the average photon flux has a constant value the photon number on short time scales fluctuates randomly. These fluctuations are described by photon statistics of the light. Perfectly coherent light with a constant intensity has Poissonion photon statistics [32].

For a beam of constant power P_{avg} incident on photodetector, mean photon number per pulse measured in time interval T is given by [32],

$$N_o = \varphi T = \frac{P_{avg}T}{h\upsilon} \tag{2.2}$$

T is large enough so it will be divided into $\acute{N}$ sub intervals of duration $T/\acute{N}$, $\acute{N}$ is very large so that there is only very small probability $p = N_o/\acute{N}$ that one photon is registered & negligibly small probability that 2 or more photon events occur. The probability of observing n events in the $\acute{N}$ intervals in time T is,

$$P(n) = \frac{\acute{N}!}{n!(\acute{N}-n)!}p^n(1-p)^{\acute{N}-n} \tag{2.3}$$

By substitute the value of p [32],

$$P(n) = \frac{\acute{N}!}{n!(\acute{N}-n)!}\left(\frac{N_o}{\acute{N}}\right)^n\left(1-\frac{N_o}{N}\right)^{N-n} \tag{2.4}$$

As $\acute{N} \to \infty$ $\qquad \frac{\acute{N}!}{(\acute{N}-n)!\acute{N}^n} \to 1$

Furthermore as $\acute{N} \to \infty$ $\quad \left(1-\frac{N_o}{\acute{N}}\right)^{N-n} \to e^{-N_o}$

On using these two limits [32],

$$\lim_{N\to\infty} P(n) = \frac{1}{n!}.1.n^{-n}.e^{-N_o} \tag{2.5}$$

The Poisson distribution is used to predict the number of occurrences of a discrete event over a fixed time interval [32],

$$\therefore p(n) = \frac{{N_o}^n}{n!} e^{-N_o} \quad \text{, (n=1, 2, 3…)} \tag{2.6}$$

This distribution is displayed on semi logarithmic plot in Figure (2.2) which shows the Poisson distribution for several values of N_o. The curves become progressively broader as N_o increases [32].

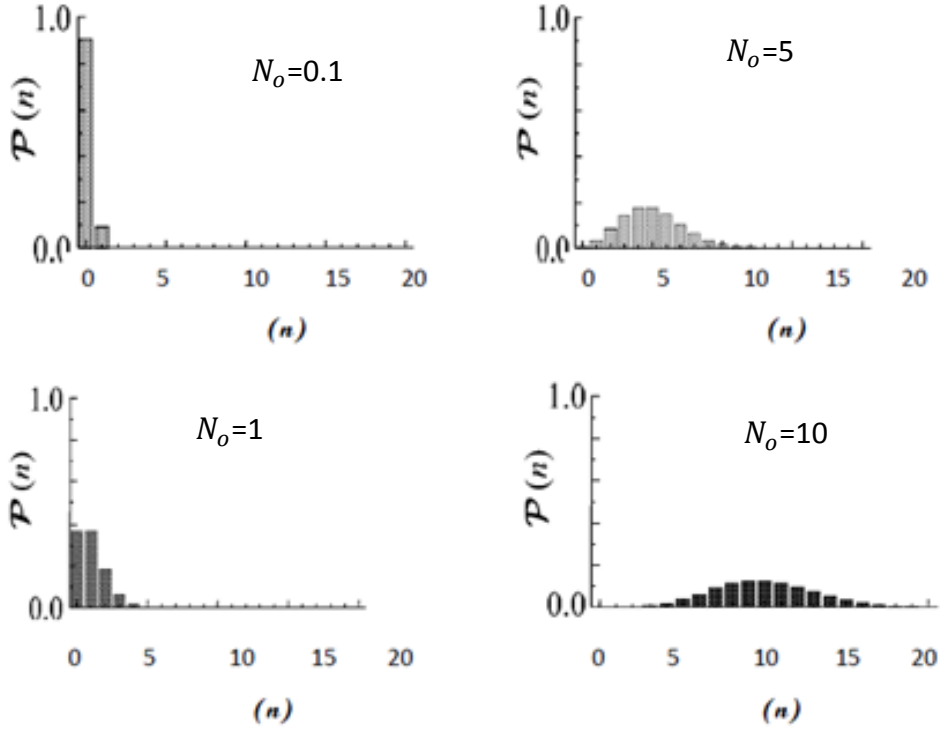


Fig.2.2 Poisson distributions for N_o of 0.1, 1, 5, and 10 [32]

For instance, if N_o = 0.1 is used, then most of the pulses contain no photons, some contain single photons and a fraction of order 0.005 signals contain several photons.

The modeled pulsed laser source provides train of pulses with ns duration, repetition rate ranging from 0.1 MHz to 10 MHz, 1 mW peak optical output power and three different emission wavelengths (830nm, 900nm and 1550nm) which are widely used in QKD systems.

The modeled pulsed laser source has one electrical input port and one optical output port. The electrical port is the input port from the

modeled BPRS generation unit. While, the optical port generates the coherent Gaussian optical pulses.

The first model creation step is to review the functionality, operation and the performance characteristics of the device using different standard references and commercial data sheets. The model output is compared to the commercial IDQ (ID300) (Appendix1) laser output for model validation.

The information provided from the first step is used in the second model creation step to build the conceptual model. In addition to the mathematical model, the conceptual model is utilized to code the pulsed laser model using Matlab.

2.2.2 The Pulsed laser source conceptual model

Laser is an electro-optical component with one input and one output as shown in the corresponding conceptual model of Figure (2.3).

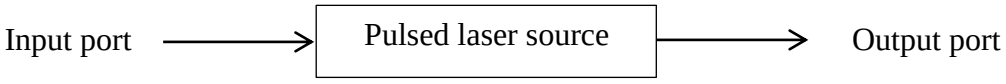


Fig.2.3 Pulsed laser source conceptual model

In Figure (2.3), the laser pulses are generated when the laser receives an electrical trigger from the BPRS generator. The laser pulses are generated based on the electrical input signal repetition frequency, optical wavelength, pulse width, polarization and the orientation of the pulse.

It is important to mention that the generated pulses are processed independently as they pass through different optical components which as a result improve the simulation performance of the modeled system in terms of preventing the pulses accumulation which in turn leads to the interference of the pulses.

2.2.3 The Pulsed laser source mathematical model

As the laser is considered as a source for coherent optical pulses, the approach used to mathematically model a laser is focus on how the optical pulses are modeled in an efficient manner to treat all the optical components following the laser source module. The mathematical representation of the optical pulses used in this work is based on the model implemented by Gerald Baumgartner et al [33, 34].

The complex representation of the electric field for the monochromatic plane wave lies in the x-y plane can be written as [33, 34],

$$\vec{E}(z,t) = \begin{bmatrix} E_x(z,t) \\ E_y(z,t) \end{bmatrix} = E_0 e^{i(kz-\omega t)} \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} \quad (2.7)$$

Where:

E_0 is the amplitude of the wave.

$\alpha_{inc.}$ is the polarization of the wave ,i.e. , angle of the vector with respect to the x axis, with the x and y components of the amplitude being $E_0\cos(\alpha_{inc.})$ and $E_0\sin(\alpha_{inc.})$, respectively

Φ is the ellipticity of the wave ,i.e. , relative phase of E_x and E_y

k is the wave number

ω is the angular frequency

The propagation medium for this plane wave is considered as a homogenous, isotropic in which x and y components propagate with the same phase velocity. The superposition of these plane waves form an electromagnetic pulse propagating in z direction.

By assume E_y=0 in Eq. (2.7), E_x can be expressed as [33, 34],

$$E_x(z,t) = \int_{-\infty}^{\infty} A(k)\, e^{i(kz-\omega(k)t)} dk \quad (2.8)$$

The integration range takes all the possible waves that contribute to the formation of the wave packet or the pulse from $-\infty$ to $+\infty$.

$A(k) = |A(k)|e^{i\gamma(k)}$ is a complex amplitude which is considered as a smoothly varying function of k. For a non-dispersive medium, (e.g. a vacuum), each pulse harmonic component propagates with the same phase velocity (equal to $\frac{\omega}{k}$). In this case, $w = vk$, where v is the constant phase velocity. As a result,

$dw/dk = v$, so Eq. (2.8) can be written as [33, 34],

$$E_x(z,t) = E_0 e^{i(k_0 z - \omega_0 t)} f(z - vt) \quad (2.9)$$

Where:

$f(z - vt)$ is the modulating factor which defines the unchanging shape of the pulse. Its phase is constant with time and regarded as a function of the position. Thus, the phase of $f(z - vt)$ remains preserved for different frequencies as long as the pulse travels [33, 34].

With arbitrary polarization of light, $\alpha_{inc.}$, the EM pulse can be represented as [33, 34],

$$E_x(z,t) = E_0 e^{i(k_0 z - \omega_0 t)} f(z - vt) \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} \quad (2.10)$$

Which can be rewritten as [33, 34],

$$\vec{E}(z,t) = E_0 e^{i(k_0 z - \omega_0 t)} g(t - \tfrac{z}{v}) \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} \quad (2.11)$$

or with most general form as [33, 34],

$$\vec{E}(z,t) = E_0 e^{i(k_0 z - \omega_0 t)} e^{j\theta(t - \frac{z}{v})} \left| g(t - \tfrac{z}{v}) \right| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} \quad (2.12)$$

Where:

$\left| g(t - \frac{z}{v}) \right|$ is a dimensionless, normalized scaling factor which defines the shape of the pulse at any z value or after a time equal to $\frac{z}{v}$ [33, 34],

$\theta(t - \frac{z}{v})$ is the phase of $g(t - \frac{z}{v})$

At z=0, Eq.2.12 can be modified to define the time-profile of the pulse [33, 34],

$$\vec{E}(0,t) = E_0 e^{-i(\omega_0)} e^{j\omega(t)} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} \quad (2.13)$$

A coherent optical pulse has a global phase θ independent of the time coordinate of the pulse, i.e.,$\theta(t) = \theta$ is a constant in Eq. (2.13). Furthermore, due to the light pulse quantization, the photons within the pulse have the same phase as well as, for a non-dispersive medium; θ is constant at all spatial points z. Thus, such a coherent traveling pulse at position z can be defined by [33, 34],

$$\vec{E}(z,t) = E_0 e^{i(k_0 z - \omega_0 t)} e^{j\theta} \left| g(t - \tfrac{z}{v}) \right| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} \quad (2.14)$$

At z=0 [33, 34],

$$\vec{E}(0,t) = E_0 e^{-i(\omega_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} \quad (2.15)$$

For a coherent pulse with a Gaussian shape, $|g(t)|$ can be represented as [33, 34],

$$|g(t)| = \frac{2\Delta^2}{\sqrt{2\pi}} e^{-\Delta^2 (t - t_0)^2} \quad (2.16)$$

Where t_0 is the point around which the pulse is shaped, τ is the standard deviation of the pulse which represents the pulse width, and $\Delta^2 = \frac{1}{2\tau^2}$.

2.2.4 Simulation results and discussion

The purpose of this sub-section is to present the outcome of modeling the pulsed laser source with the analysis via two points,

1. Focusing on the modeled optical laser pulse and how to validate this designed pulse to the actual laser pulse for final laser model component verification.
2. Describing the laser source model that has been implemented in Matlab v.19.

ID300 sub-nanosecond pulsed laser source was used in this research to compare its output to the modeled laser source output. Figure (2.4) represents the measured in the lab. ID300 laser pulse with 3 different peaks. One can easily note how the measured pulse shape differs from the time profile of the same device as illustrated in the device commercial data

sheet. Thus, the best way to model such complex pulse is by using more complex approximation which can be verified by mixing three Gaussian curves.

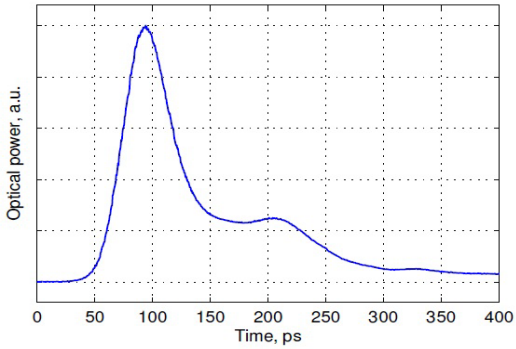


Fig.2.4 Measured ID300 Laser Pulse [34]

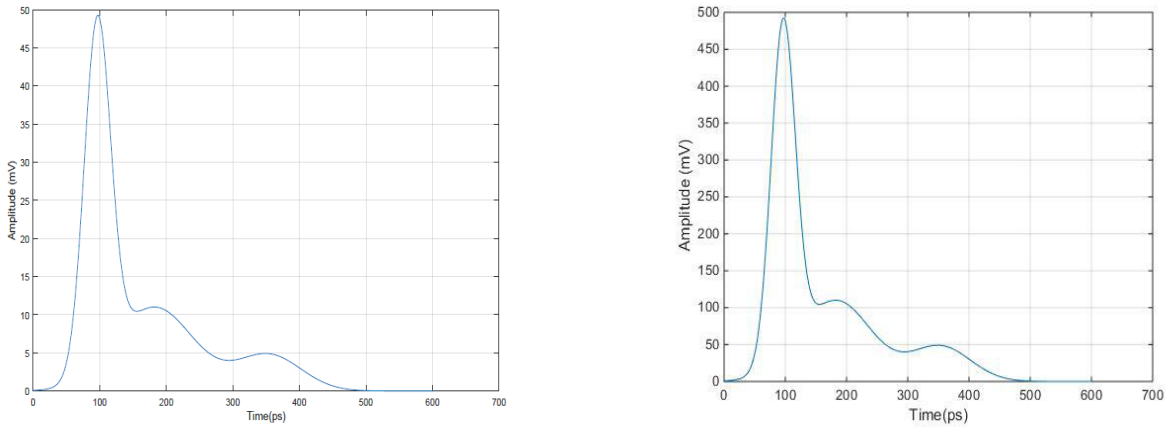
In this research, a sum of three Gaussian functions is used to approximate the ID300 laser pulse. Table (2.1) represents these parameters values.

Table 2.1. Parameters to approximate modeled optical pulse

Gaussian curve	Gaussian amplitude	t_0 (ps)	τ (ps)
1	44.5	93.48	18.72
2	37.1	171.12	57
3	4.57	350.3	47

Figures (2.5) to (2.10) illustrate the results of laser pulse simulation for λ=1550nm under different pulse parameters tests to verify that these results match the expected theoretical results and to ensure how well this pulse was designed to be used it in the simulator. The optical pulse will be tested in terms of pulse amplitude, width, orientation and polarization (Ellipticity).

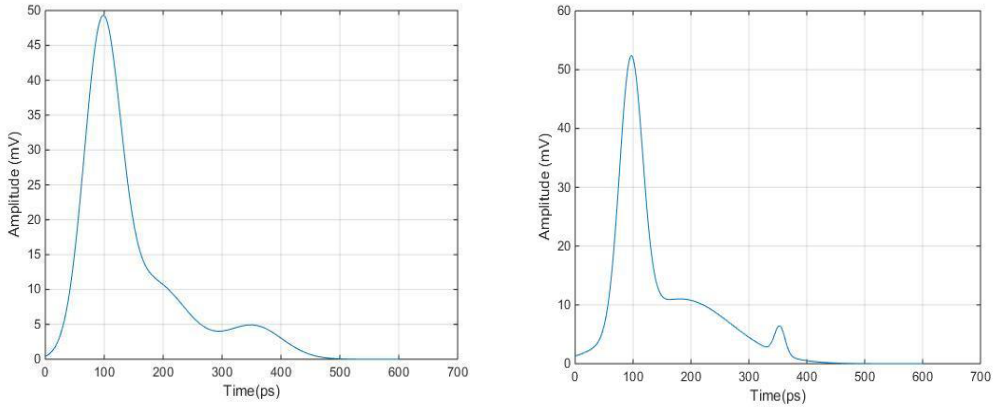
Figure (2.5) shows the simulated laser pulse with different amplitudes.



(a) **(b)**

Fig. 2.5 Simulated laser pulse with θ =0, $\alpha_{inc.}$ =0, Φ =0.
(a) With E_0=1, (b) with E_0=10

Figure (2.6) illustrates the response of the simulated pulse to the change of its temporal width with the same previous assumptions.



(a) **(b)**

Fig.2.6 Simulated laser pulse with θ =0, $\alpha_{inc.}$ =0, Φ =0
(a) Pulse width=0.08ns (b) Pulse width=0.05ns

One of the most important coherent laser pulse parameters which is necessary to model this pulse is the pulse orientation ($\alpha_{inc.}$). Figures (2.7, 2.8 and 2.9) represent three different cases to investigate the performance of the modeled laser pulse to the change in the orientation of its electric field. Figure (2.7) shows how E_{total} of the simulated laser pulse consists of only E_y according to Eq. (2.15) because of $\alpha_{inc.}$ =90°.

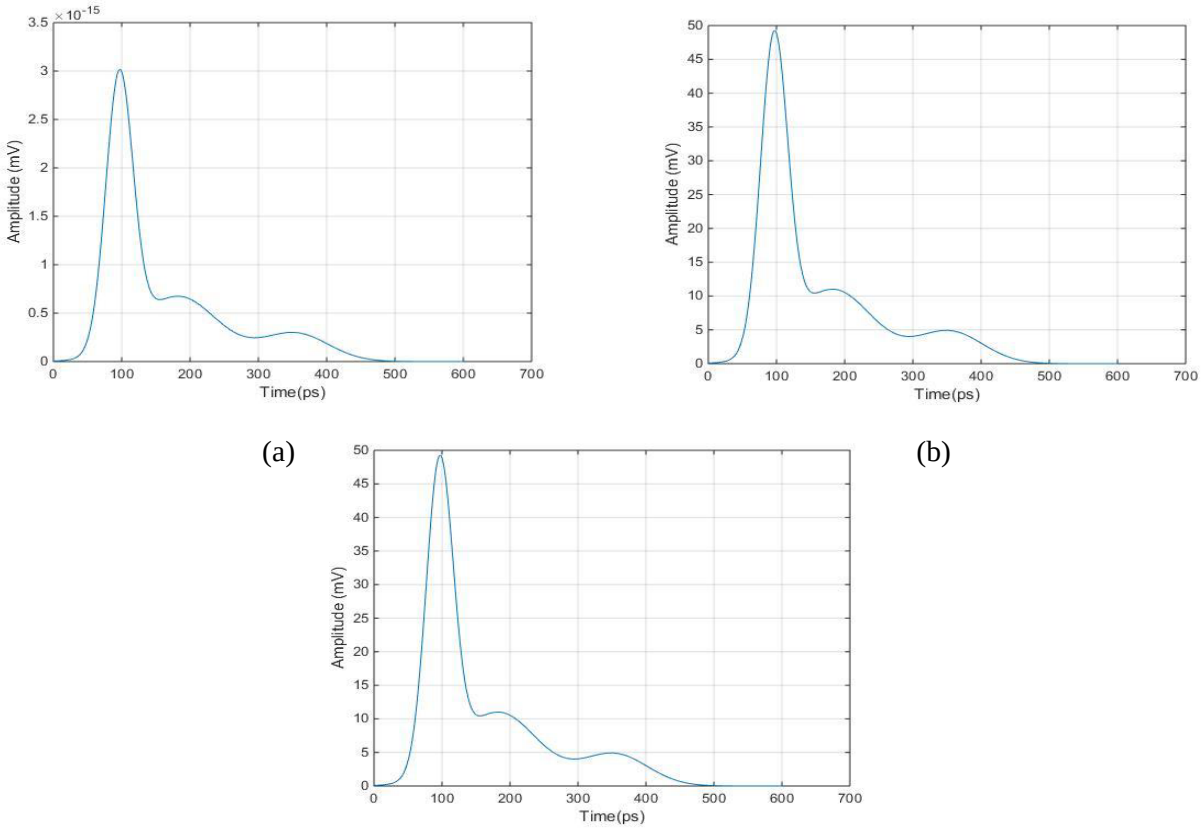


Fig.2.7 Simulated laser pulse with θ =0, $\alpha_{inc.}$ =90, Φ =0
(a) E_x, (b) E_y , (c) E_{total}

Figure (2.8) shows how E_{total} of the simulated laser pulse consists of the effect of both E_x and E_y according to Eq. (2.15) because of $\alpha_{inc.}$ =45°.

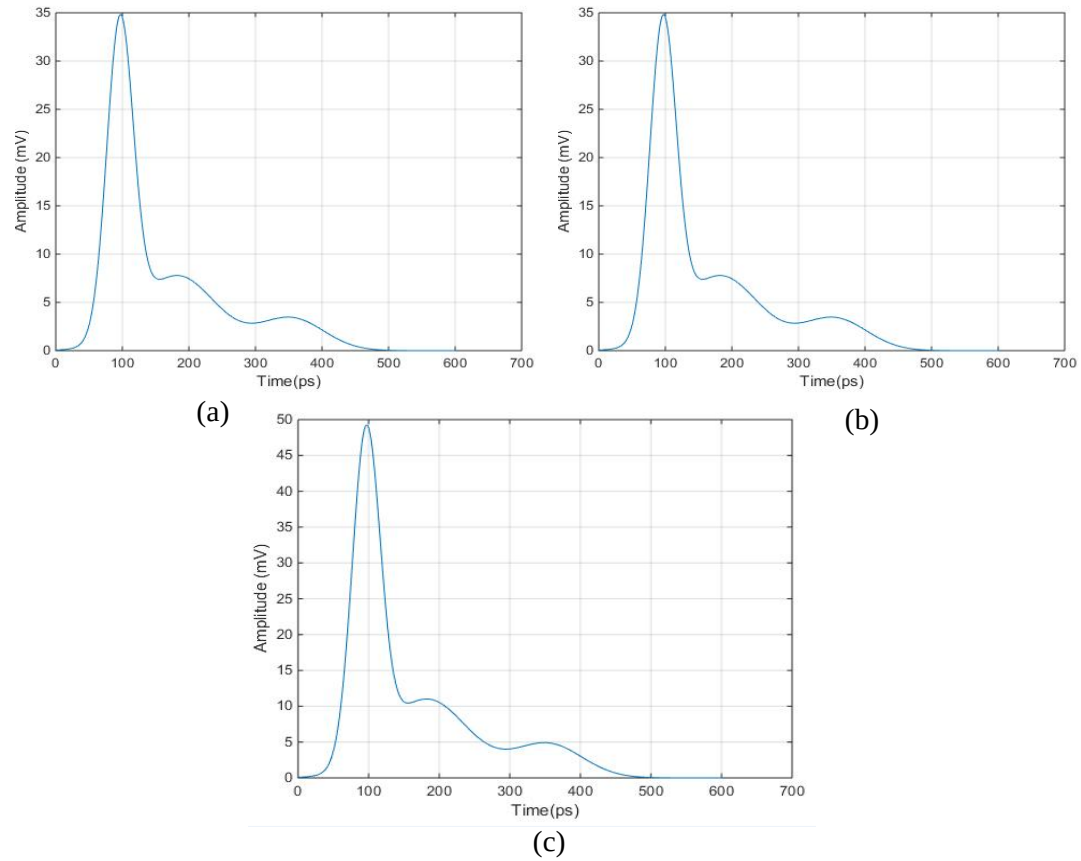


Fig.2.8 Simulated laser pulse with θ =0, $\alpha_{inc.}$ =45, Φ =0
(a) E_x, (b) E_y , (c) E_{total}

Figure (2.9) shows how E_{total} of the simulated laser pulse consists of only E_x because of $\alpha_{inc.}$ =180°.

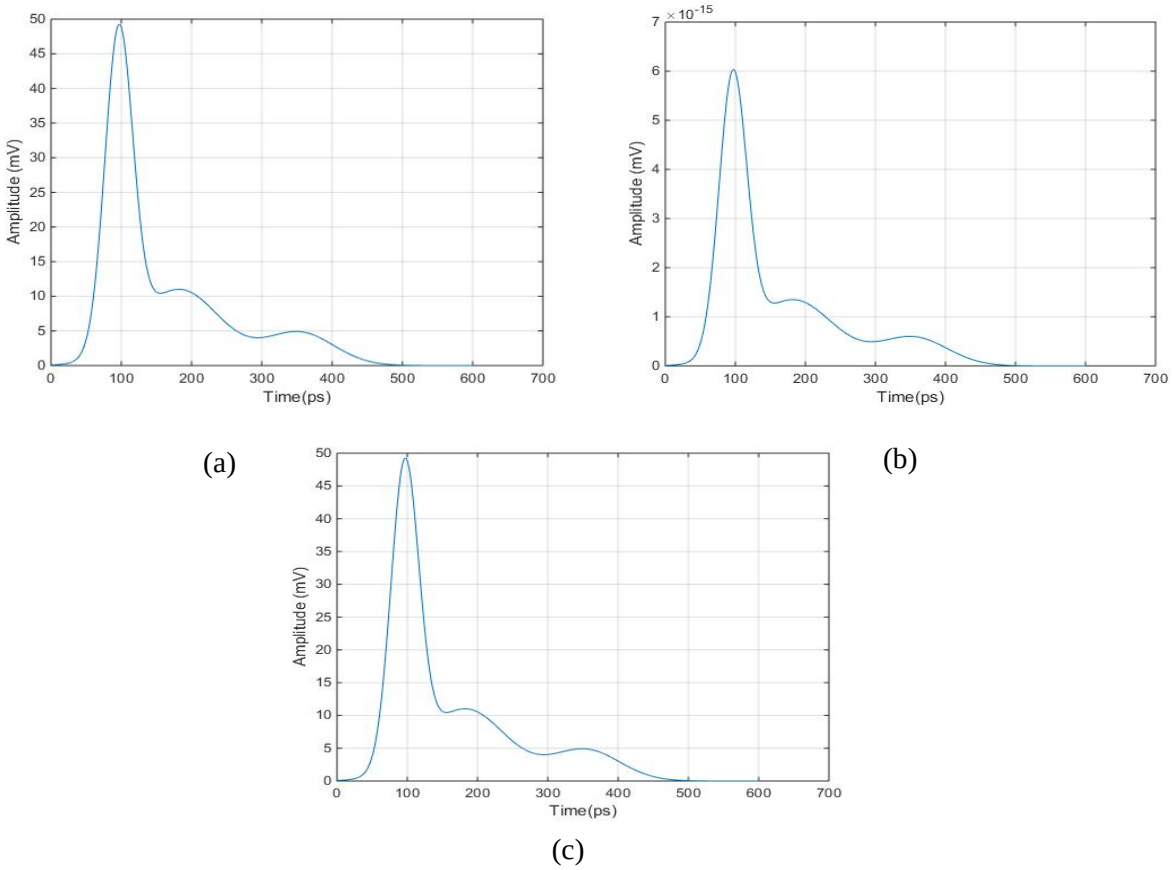


Fig.2.9 Simulated laser pulse with the following assumptions, θ =0, $\alpha_{inc.}$ =180, Φ =0 (a) E_x, (b) E_y , (c) E_{total}

Finally, in order to test the relative phase between E_x and E_y components, .i.e., pulse polarization and how it will affect the resultant E_{total}, three different tests were made as shown in Figure (2.10). The obtained E_{total} results illustrate how Eq. (2.15) responds to the variation in Φ.

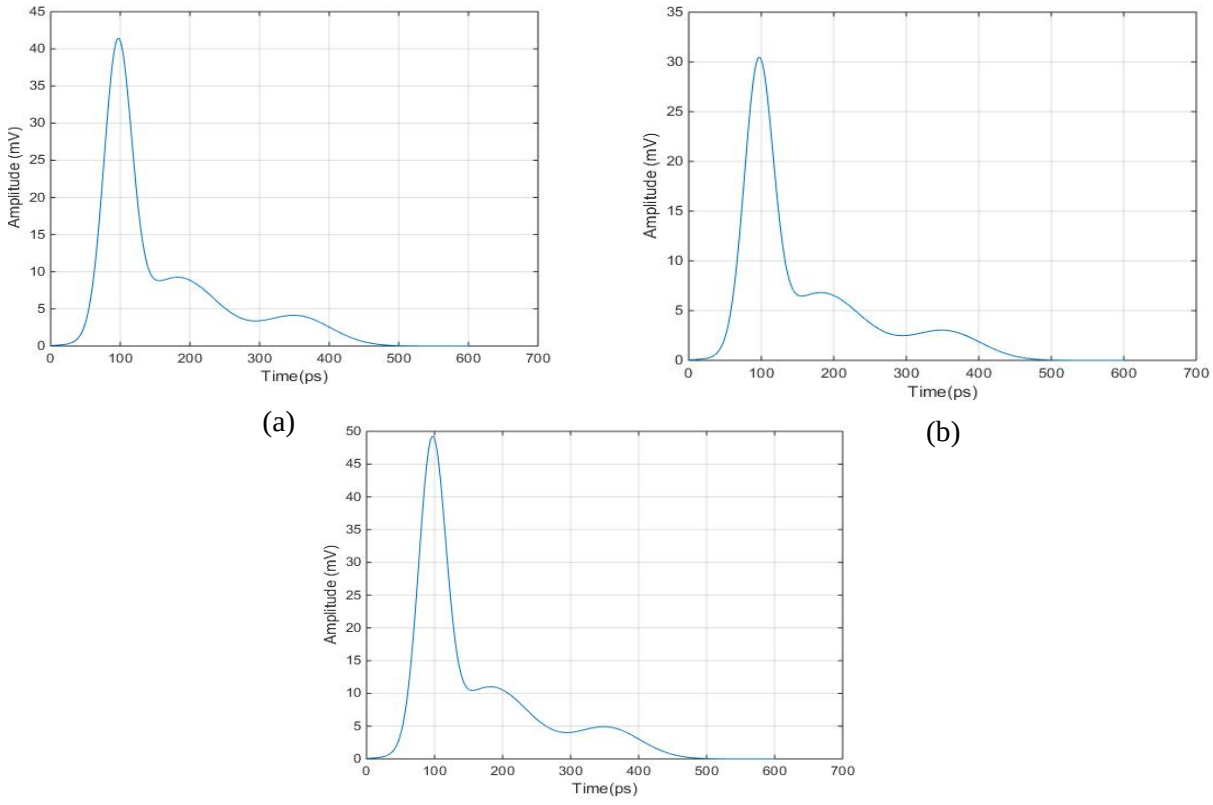


Fig.2.10 Simulated laser pulse with different polarization tests
(a) θ =0, $\alpha_{inc.}$ =45, Φ =45, (b) θ =0, $\alpha_{inc.}$ =45, Φ =67, (c) θ =0, $\alpha_{inc.}$ =45, Φ =90

As a conclusion to the previous tests, the resultant laser pulse simulation results agree with the expected theoretical results obtained from Eq. (2.15) and hence its validity to simulate the propagation of the laser pulse through different modeled optical components in this work.

Based on the designed laser pulse, the laser source module has been implemented with a friendly GUI as shown in Figure (2.11). This interface with its configurable pop-up menus is responsible to allow users to setup input parameters to configure the pulsed laser source module.

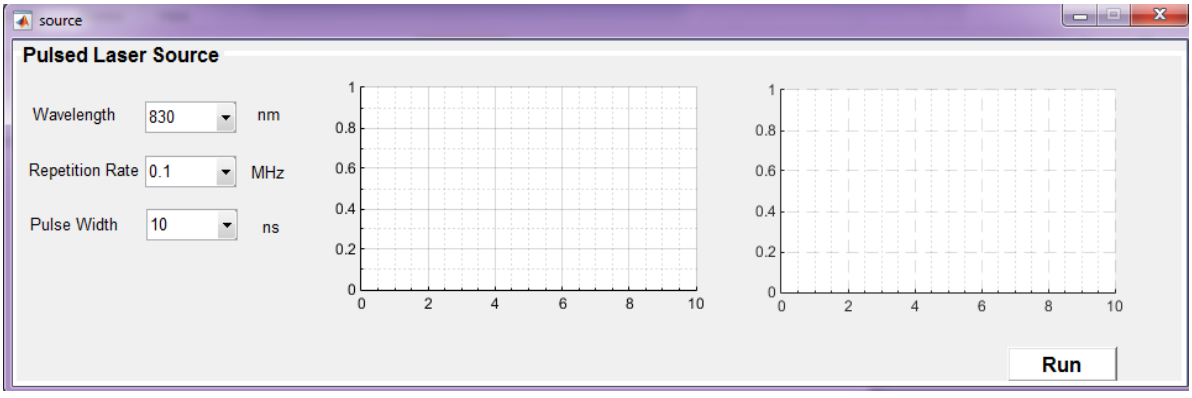


Fig.2.11 Optical source module simulator window

This module consists from two parts, BPRS generation unit and pulsed laser device. The modeled BPRS unit generates randomly a binary non-return –to-zero (NRZ) sequence of 5000 bits with defined pulse repetition rate. This model supply a sequence that can be lengthened to infinity as long as N bits periodically repeated and that is what makes it different from true random sequence sources. This model can also import the date from external files with true random sequences based on physical processes [35, 36]. The optical laser pulses generation rate depends on the electrical trigger signals repetition rate and on the number of input bits from the BPRS unit. This module can support repetition rate from 100 kHz-10 MHz. The width of the generated pulses as well as the optical wavelength of the source can be changed to cover three wavelengths that are used in QKD systems.

These wavelengths are 830nm, 900nm and 1550nm. 830nm and 900nm are utilized when SPAD is used as a detection device where it shows maximum detection efficiency at these wavelengths. While, 900nm and 1550nm are used when SNSPD used as a detection device.

The left plotter of Figure (2.11) represents the electrical trigger signal applied from BPRS with defined pulse repetition rate. The right plotter shows the corresponding generated optical laser pulses according to the trigger signal. After each run, all of these parameters are saved to be used as the user needs. Many parameters can play an important role in the processing speed, such as number of input bits, availability of efficient CPU and large memory space.

Three tests were done to verify the modeled optical source module to simulate the laser device operation. Figure (2.12) illustrates **Test 1** result. In this test, λ is set to 830 nm, PRR is set to 100 KHz, and τ is set to 2ns. P_{peak} is equal to 1mW.

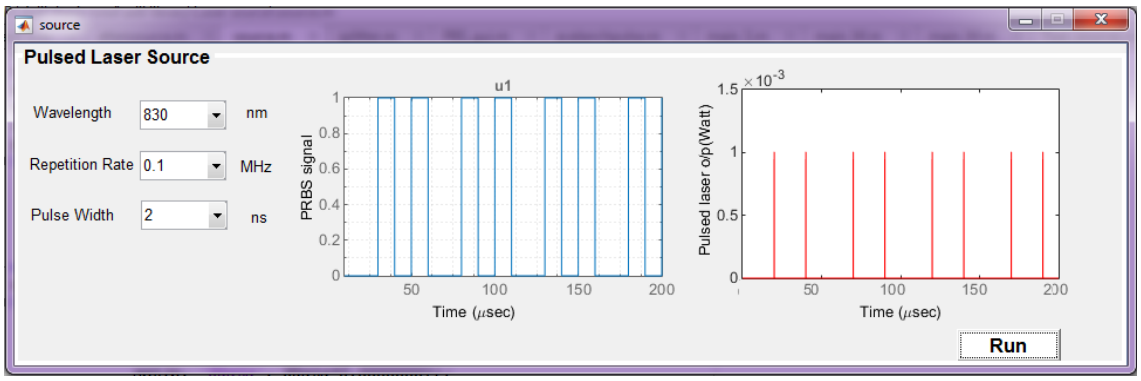


Fig.2.12 Test 1 result for:λ=830nm, *PRR*=100KHz, τ=2ns

Figure (2.13) illustrates **Test 2** result. λ is set to 900nm; *PRR* is set to 2 MHz and τ is set to 2ns.

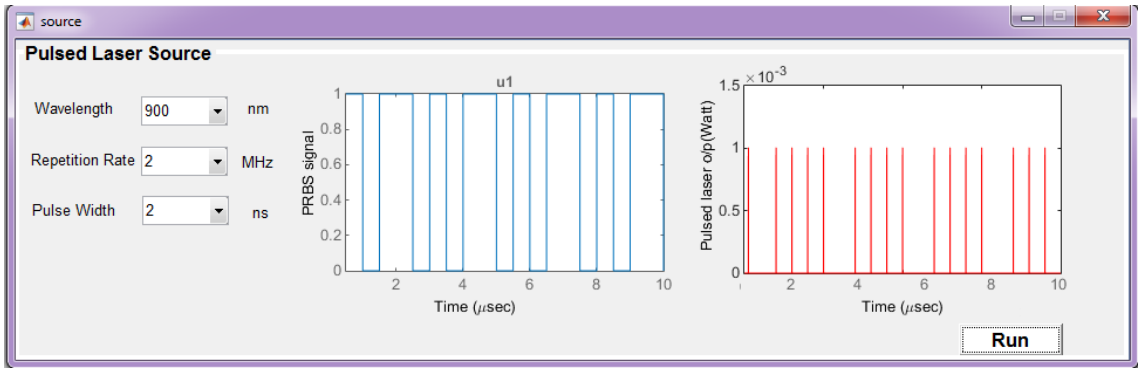


Fig.2.13 Test 2 result for:λ=900nm, *PRR*=2MHz, τ=2ns

Figure (2.14) illustrates the **Test 3** result. λ is set to 1550 nm, *PRR* is set to 10MHz and τ is set to 2ns.

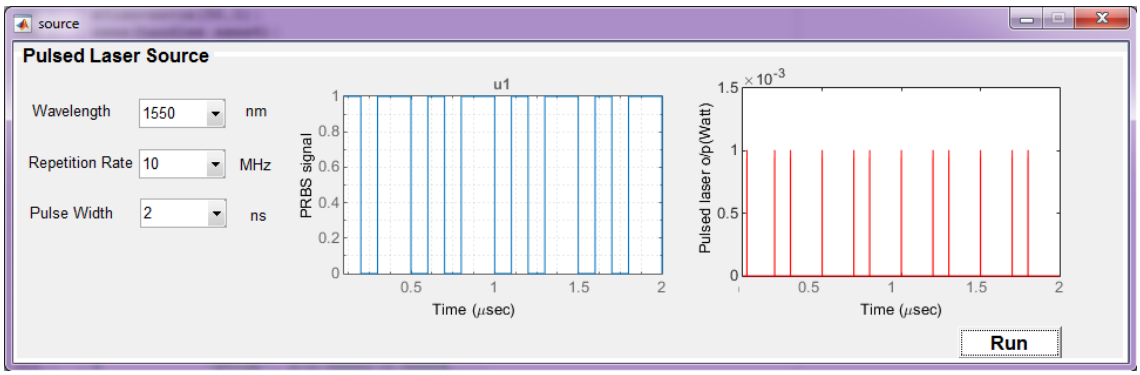


Fig.2.14 Test 3 result for:λ=1550nm, *PRR*=10 MHz, τ=2ns

2.3 The Linear polarizer

This section outlines the methodology used to model the LP device. It gives a vision to the operation basics of this component, the concept and the

mathematical models that has been used to model it. Final LP GUI will be presented and discussed at the end of this section.

2.3.1 The Device description

This component is designed to polarize the input optical signal into a known polarization. The polarizer works as a filter in which is transmitting only the signal component that has the same polarization while filters out the perpendicular component [18].

The direction of $\vec{E}(z,t)$ is responsible for determining the polarization of the light. At each point in z, $\vec{E}(z,t)$ travels in a plane and traces an ellipse. The rotation of $\vec{E}(z,t)$ is periodically continuous as long as the wave moves forward and hence repeating its motion for each wavelength, λ [37].

The polarization of the optical pulse is determined by the direction of the major axis in the ratio of $\frac{\alpha_y}{\alpha_x}$ and the phase difference Φ between x and y components, .i.e., ellipticity. On the other hand, the optical intensity of the signal (I) can be determined by the ellipse size [37],

$$I = \frac{(\alpha_x{}^2 + \alpha_y{}^2)}{2\eta_{med.}} \tag{2.17}$$

Where $\eta_{med.}$ is the medium impedance.

The pulse is said to be linearly polarized if one of the electrical field components becomes zero or if Φ =0 or π as shown in Figure (2.15).

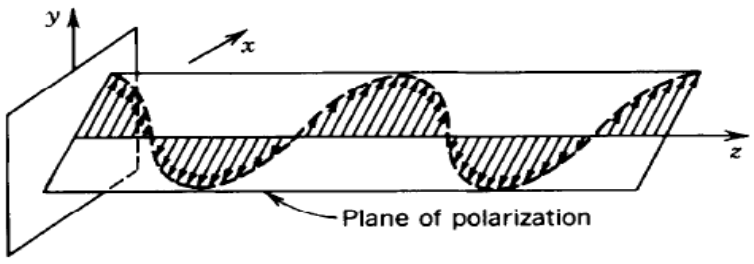


Fig.2.15 Linearly polarized light [37]

On the other side, the pulse is said to be circularly polarized if $\Phi = \pm \pi$ and the electrical field components are equal as illustrates in Figure (2.16).

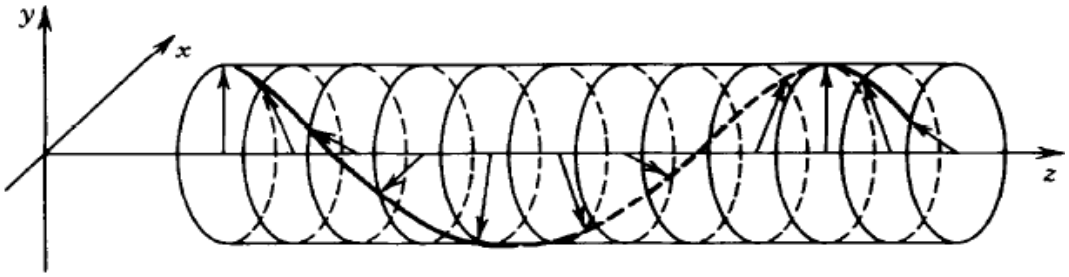


Fig.2.16 Circuilarly polarized light [37]

As it is known, polarization based QKD systems utilize the polarization of the photon for encoding and detection measurements. As a result, LP becomes irreplaceable device in QKD protocols [37].

If the plarization of the incident pulse is denoted by $\alpha_{inc.}$, and the polarization orientation angle for the LP denoted by γ_{LP}, the output power of the output beams P_0 and P_1 will be defined according to Mallu's Law [21],

$$P_0 = cos^2(\alpha_{inc.} - \gamma_{LP}) \tag{2.18}$$

$$P_1 = sin^2(\alpha_{inc.} - \gamma_{LP}) \tag{2.19}$$

Thus, as the pulse leaves the polarizer in beam 0, its polarization is γ_{LP}. On the other hand, if it leaves in beam 1, its polarization is $(\gamma_{LP} + \pi/2)$ [21].

The modeled LP has one optical input port and one optical output port. The input signal is applied via the modeled pulsed laser module. While, the output port generates optical pulses with known polarization.

The first modeling step was to review the functionality, operation and the performance characteristics of the device using different standard references and commercial data sheets. The model performance operation

was compared to the theoretical and experimental device behavior reported in related research work and the device's data sheets for model validation. The information provided from the first step was used in the second modeling step to build the conceptual model. In addition to the mathematical model, the conceptual model will be utilized to code the LP model using Matlab.

2.3.2 The Linear polarizer conceptual model

Linear polarizer is a passive component with one input and one output as shown in the corresponding conceptual model of Figure (2.17).

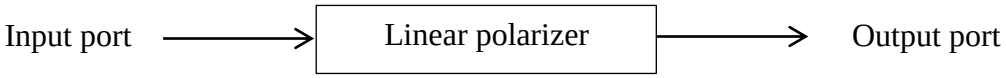


Fig.2.17 Linear polarizer conceptual model

From the conceptual model diagram, the polarized optical signals are generated when the optical signals are sent from the pulsed laser module to the input of the LP. According to its mathematical model, the modeled LP simulates any changes in the polarization, ellipticity and the optical power of the incident laser pulse minus a slight insertion loss estimated by -0.5 dB [18]. In addition, the modeled LP blocks any pulse that has a polarization perpendicular to the device polarization angle and allow for passing the pulses with same polarization only.

2.3.3 The Linear polarizer mathematical model

The coherent optical pulse defined in Eq. (2.15) represents the input to the LP component. For a non-dispersive medium; θ will be constant at all spatial points z [33], .i.e., assumed (0 degree) in this research. For the sake of simplicity, $|g(t)|$ term will not be considered for the next steps in this model.

From the coherent optical pulse representation, the signal parameters related to the LP component and hence modify or change the signal characteristics at the output of the LP are E_0, α and Φ.

The polarizer transformation matrix is defined as [38],

$$LP(\gamma) = \begin{pmatrix} (cos\ (\gamma_{LP}))^2 & (\cos\ (\gamma_{LP})\sin(\gamma_{LP})) \\ (\cos\ (\gamma_{LP})\ \sin\ (\gamma_{LP})) & (sin\ (\gamma_{LP}))^2 \end{pmatrix} \quad (2.20)$$

In order to find the polarized optical signal, the following normalization to the result of the operation of the LP transformation matrix on the coherent pulse Jones matrix will be carried out. The amount of insertion loss must be considered,

$$\vec{E}(\gamma) = Norm\ [\vec{E}(0,t).LP(\gamma_{LP})] \quad (2.21)$$

$$\therefore \vec{E}(\gamma) = E_0\sqrt{10^{\frac{-insertion\ loss}{10}}} * \sqrt{(\cos(\alpha_{inc.})\ cos\ (\gamma_{LP}))^2 + (sin(\alpha_{inc.})\ sin\ (\gamma_{LP}))^2 + 2\ \cos(\alpha_{inc.})\ \cos(\gamma_{LP})\ \sin(\alpha_{inc.})\ \sin(\gamma_{LP})\ \cos(\Phi)} \quad (2.22)$$

Thus, the output polarized optical signal form can be written as follows:

$$\vec{E}(\gamma) = E_0 e^{-i(\omega_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(output\ polarization) \\ \sin(output\ polarization) e^{i(output\ Elipticity)} \end{bmatrix} \quad (2.23)$$

$$\vec{E}(\gamma) = E_0 e^{-i(\omega_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.}\ output) \\ \sin(\alpha_{inc.}\ output) e^{i(\Phi output)} \end{bmatrix} \quad (2.24)$$

2.3.4 Simulation results and discussion

The purpose of this section is to present the results with the analysis of modeling the LP component. LP component model has been implemented with a friendly GUI as shown in Figure (2.18). This interface with its configurable editing object is responsible to allow users to configure the LP component model for polarization and power attenuation tests.

The left plotter represents the incoming laser pulses applied from pulsed laser module. The right plotter shows the corresponding generated

polarized optical pulses. The polarization angle editing text object is used to set up the polarizer angle.

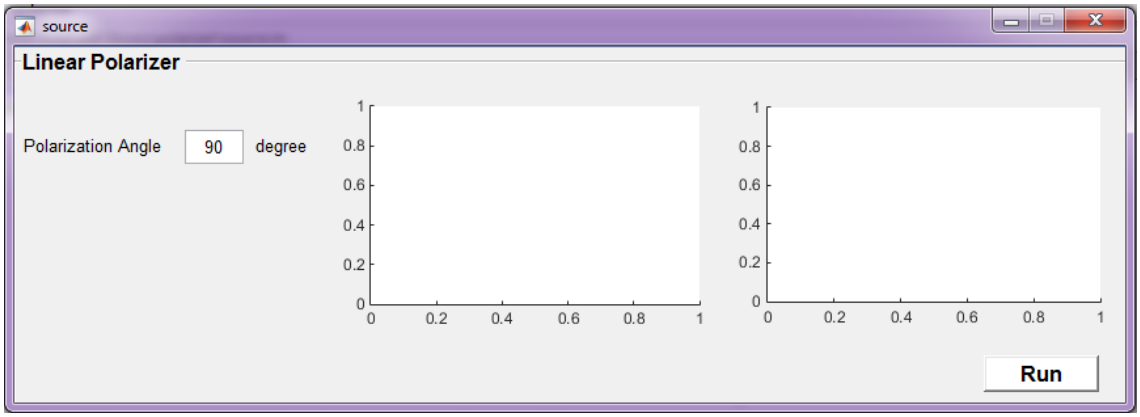


Fig.2.18 LP simulator window

Five tests are applied to verify the modeled LP component to simulate the polarizer device operation. Figure (2.19) illustrates **Test 1** result to investigate the output power of the polarized pulse after passing through the LP component. In this test, the polarization of the input optical pulse ($\alpha_{inc.}$) is the same as the polarizer angle (γ_{LP}) with linear polarization, .i.e.,(Φ) =0. As shown in Figure (2.19), the polarized pulses are slightly attenuated due to -0.5dB insertion loss without any attenuation due to polarization mismatching.

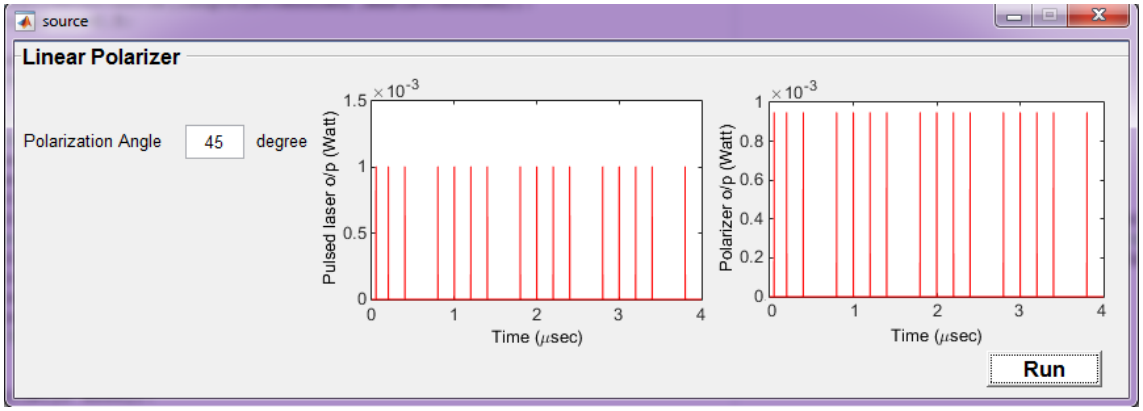


Fig.2.19 Test 1 result for: γ_{LP} =45°, $\alpha_{inc.}$ =45°, Φ =0°.

Figure (2.20) illustrates **Test 2** result to investigate the output power of the polarized pulse when circularly polarized input pulse passing through the LP component. The output polarized pulses are attenuated by a

power factor equal to $(1/\sqrt{2\ input\ power})$ due to polarization rotation in addition to -0.5dB insertion loss

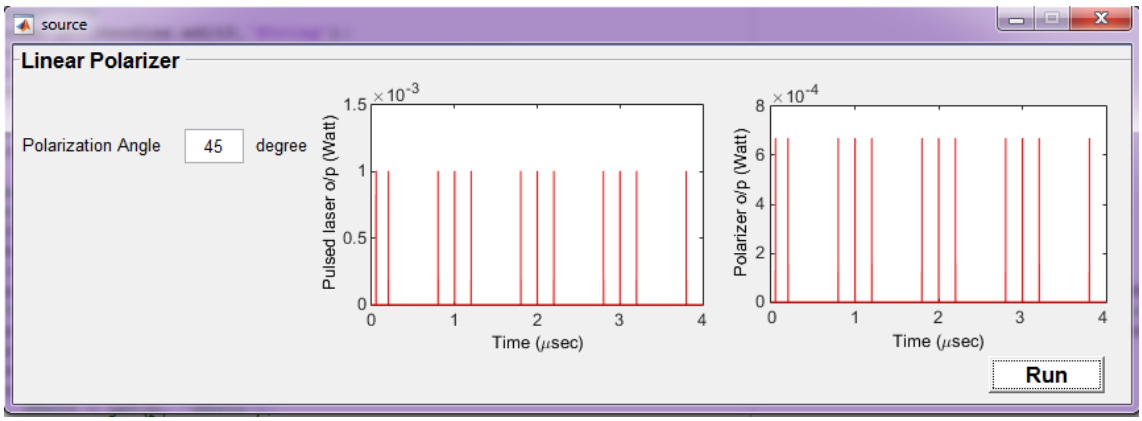


Fig.2.20 Test 2 result for: γ_{LP} =45°, $\alpha_{inc.}$ =45°, Φ =90°.

Figure (2.21) illustrates **Test 3** result to calculate the output power of the polarized pulse when circularly polarized input pulse passing through the LP component.Behavior like this can be understood as the polarizer angle will not have an effect on the polarized input optical pulse power even if it is perpendicular on the polarization of the input optical pulse as long as the input is circularly polarized.

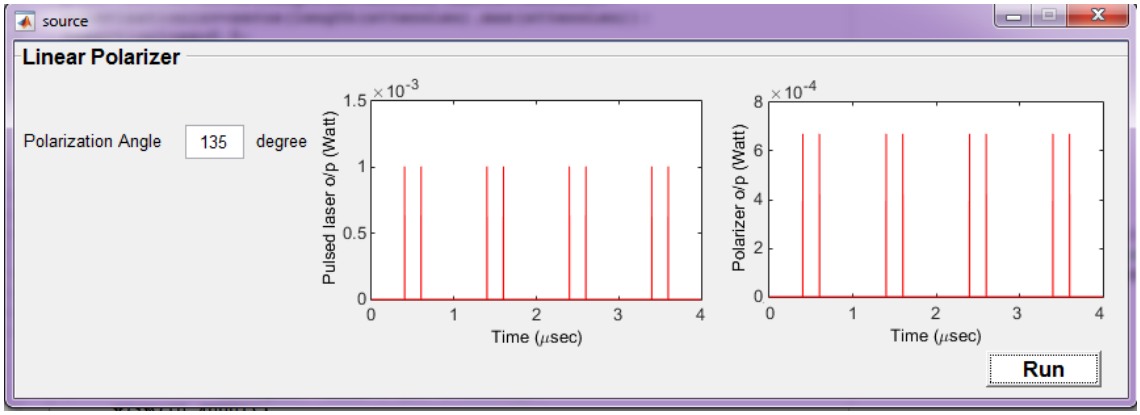


Fig.2.21 Test 3 result for: γ_{LP} =135°, $\alpha_{inc.}$ =45°, Φ =90°.

Figure (2.22) illustrates **Test 4** result to calculate the output power of the polarized pulse when linearly polarized optical input pulse passing through the LP component and the polarization of the input optical pulse is perpendicular on the LP angle. As expected, the output polarized pulses are

highly attenuated due to the effect of high extinction ratio which is > -100 dB as mentioned in the film polarizer from Thorlabs data sheet.

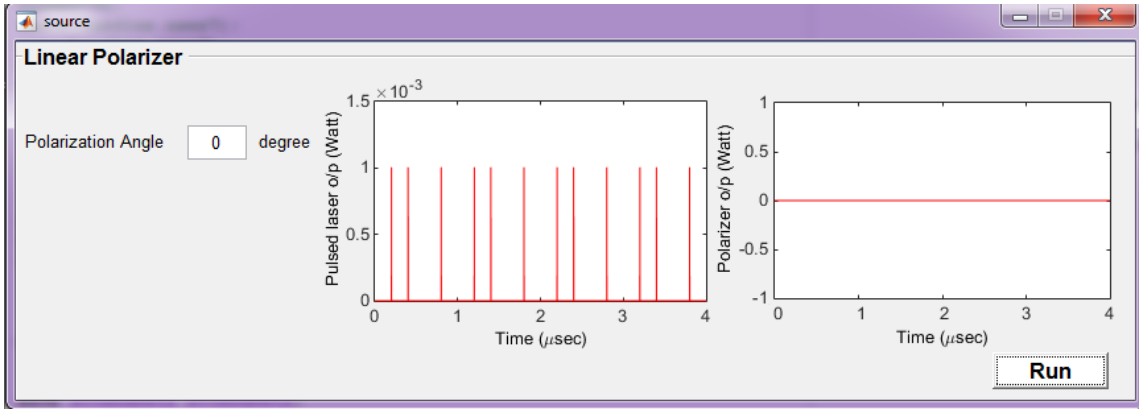


Fig.2.22 Test 4 result corresponding to γ_{LP}=0°, $\alpha_{inc.}$ =90°, Φ =0°.

Figure (2.23) illustrates **Test 5** result to investigate the output power of the polarized pulse after passing through the LP component. In this test, $\alpha_{inc.}$ is the same as γ with linear polarization, .i.e.,(Φ) =0. As shown in this figure, the polarized pulses are slightly attenuated due to -0.5dB insertion loss without any attenuation due to polarization mismatching.

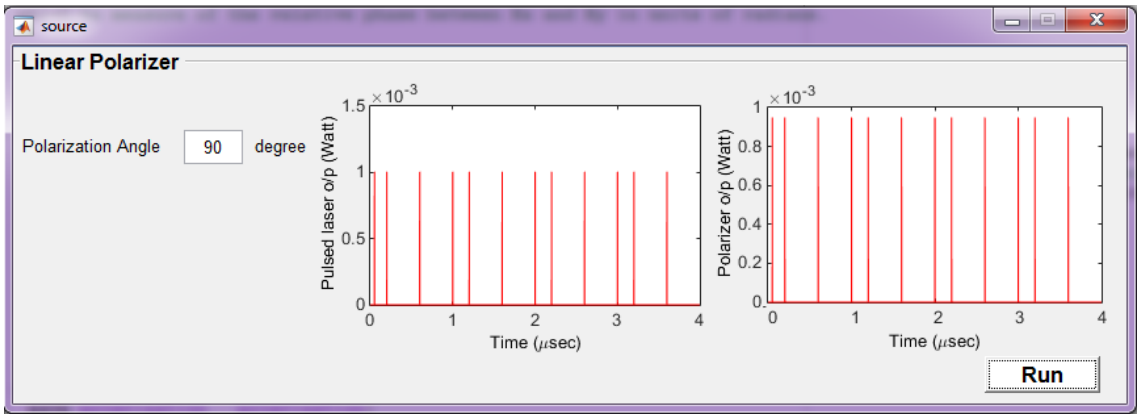


Fig.2.23 Test 5 result corresponding to γ_{LP}=90°, $\alpha_{inc.}$ =90°, Φ =0°.

2.4 The Optical Power Attenuator

This section outlines the methodology used to model the optical PA device. It gives a vision to the operation basics of this component, the concept and the mathematical models that has been used to model it. Final PA GUI will be presented and discussed at the end of this section.

2.4.1 The Device description

This component is designed to attenuate the electrical field for the optical input pulse for both polarizations. PA can be fabricated using one of the two most efficient and inexpensive techniques, misaligned splices or doped fibers [39].

Since the coherent optical pulses generated via the pulsed laser sources may have millions of photons which are inappropriate for QKD applications, in addition, single photon sources are not commercially available in QKD implementations. Thus, the best solution currently used in the QKD systems is by heavily attenuating the laser pulses up to > -40dB to reach the required quantum level with N_o equal to 0.1 [37].

In order to investigate the required attenuation level to reach the appropriate mean photon number, the following derivation can be used,

The average optical power of the laser source is defined according to the following Equation [40],

$$P_{ave} = N_o h\upsilon PRR \tag{2.25}$$

The average optical power of a single photon is [40],

$$P_{single} = h\upsilon PRR \tag{2.26}$$

The number of photons per pulse is related to the duration of the pulse, and is calculated from [40],

$$N_o = \frac{P_{ave}}{P_{single}} \tag{2.27}$$

The single photon generation attenuation level is calculated from [40],

$$\delta = \frac{1}{N} = \frac{P_{single}}{P_{ave}} \tag{2.28}$$

According to [10],

$$N_o = \frac{P_{ave}T}{h\upsilon} \tag{2.29}$$

Where,

T = time interval = $\frac{1}{PRR}$ [40],

$$\therefore\ N_o = \frac{P_{ave}\times\delta\times T}{h\upsilon} = \frac{P_{ave}\times\delta}{h\upsilon PRR} \tag{2.30}$$

The model performance operation was compared to the theoretical and experimental device behavior reported in device's data sheets for model validation.

2.4.2 The Power attenuator conceptual model

The power attenuator is a passive component with one input and one output as shown in the corresponding conceptual model of Figure (2.24).

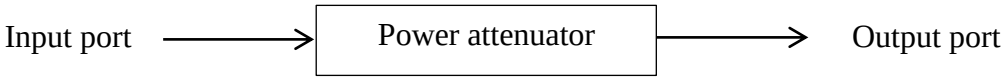


Fig.2.24 Power attenuator conceptual model

In Figure (2.24), the optical power attenuated signals are generated when the polarized optical signals are sent from the modeled LP component to the input of the PA. According to its mathematical model, the modeled PA component will simulate the optical power losses of the incident polarized optical pulses which corresponds to the attenuation level in (dB). The attenuation level is based on the required N_o set up by the user.

2.4.3 The Power attenuator mathematical model

The coherent optical pulse defined in Eq.(2.15) represents the input to the PA component. From the coherent optical pulse representation, the signal parameters related to the PA component and hence modify or change the signal characteristics at the output of PA is E_0.

In order to find the power of the polarized optical pulses after passing through the PA, the following operation on the coherent pulse

Jones matrix will be carried out taking into account the amount of the PA attenuation level.

$$\vec{E}(\alpha)=E_0 e^{-i(\omega_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} \times \sqrt{10^{\frac{-\delta}{10}}} \quad (2.31)$$

Where

δ is the PA attenuation level in dB

2.4.4 Simulation results and discussion

The purpose of this section is to present the results with the analysis of modeling the PA componen. PA component model has been implemented with a friendly GUI as shown in Figure (2.25). This interface with its configurable pop-up menu is responsible to allow users to configure the PA component model for power attenuation tests. The left plotter represents the incoming polarized optical pulses the .i.e., output of LP.

The right plotter shows the corresponding generated attenuated optical pulses. This model can support different N_o values starting from 0.1 to 1. This model responds to the user's N_o selection and calculates the corresponding δ in dB and immediately plot the resultant attenuated optical pulses measured in Watt.

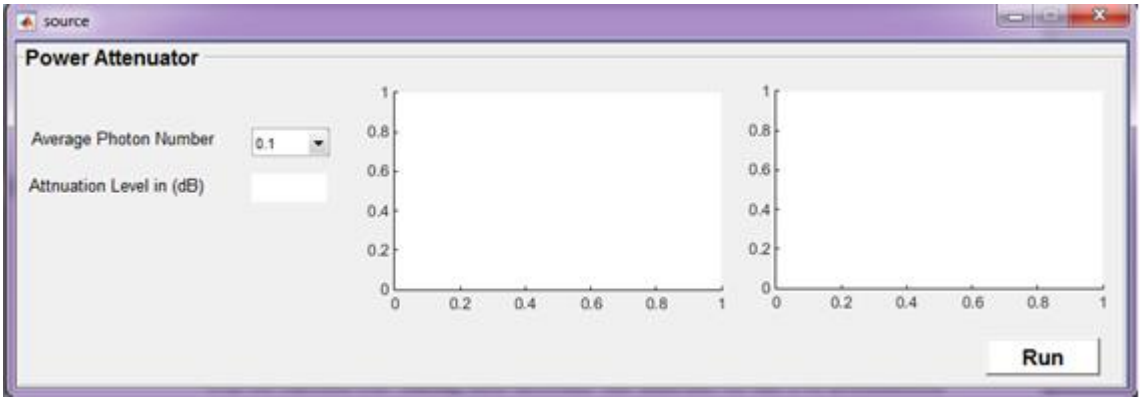


Fig.2.25 PA simulator window

Three tests were done to verify the modeled PA component to simulate the attenuator device operation. For all tests, the input pulses for the PA are linearly polarized. Figure (2.26) illustrates **Test 1** result to

investigate the output power of the polarized optical pulse after passing through the PA component. In order to reach N_o= 1, δ =-136.559 dB, thus, P_{peak} equals to 14 pW as shown in Figure (2.26).

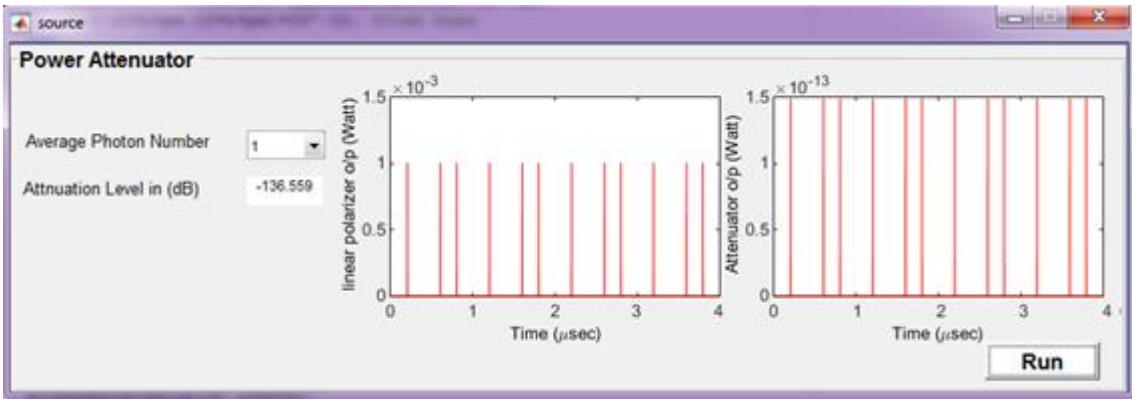


Fig.2.26 Test 1: N_o=1

Figure (2.27) illustrates **Test 2** result. In this test further attenuation was applied in order to reach N_o= 0.6. Therefore P_{peak} of the laser source needs to be attenuated to about 10 pW.

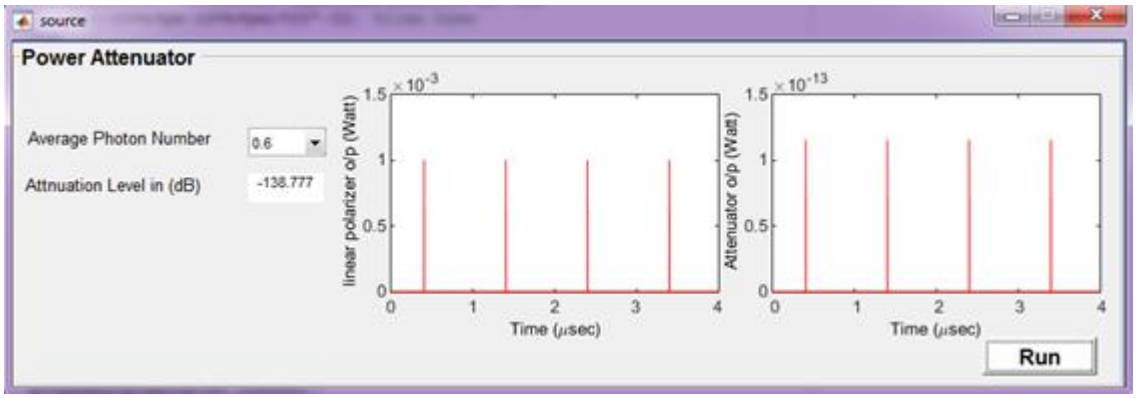


Fig.2.27 Test 2: N_o=0.6

For QKD implementations, generally, the desirable N_o value is equal to 0.1. In this case, heavy attenuation level will be applied to reach this value. Figure (2.28) illustrates **Test 3** result. δ=-146.559 dB, thus, P_{peak} corresponding to N_o = 0.1 is approximately equal to 0.04 pW.

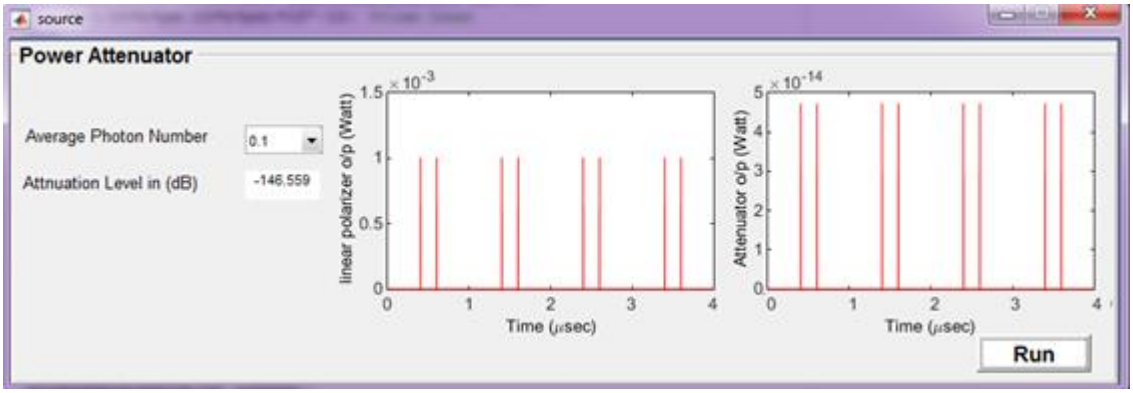


Fig.2.28 Test 3: N_o=0.1

Chapter Three

QKD Quantum Channel

Chapter Three

QKD Quantum Channel

3.1 Introduction

The purpose of this chapter is to identify the modeling of the OF and FS quantum channels. The exploration for each channel type begins with a general explanation obtained from related literatures. Based on this research, the most important channel behaviors of interest will be the basis of the channel conceptual model which is the first modeling step. Later, the mathematical model of a single mode fiber (SMF) and FS atmospheric model that takes into account the atmospheric and diffraction losses that believed to be important for the modeling of the QKD quantum channel. Finally, samples of modeled output with the analysis for each modeled optical quantum channel type will be presented.

3.2 The Optical Fiber Quantum Channel

This section outlines the methodology used to model the OF quantum channel. It gives a vision to the operation basics of this link, the concept and the mathematical models that has been used for modeling. The final OF quantum channel GUI will be presented and discussed at the end of this section.

3.2.1 The Channel description

An optical fiber is a dielectric waveguide with a cylindrical structure able to transfer electromagnetic waves at optical frequencies along the axis of the fiber. The structural design of the optical fiber defines the transmission characteristics. Single mode fibers refer to the structures where the light has only one path to follow. While, multimode fibers refer to the structures where the light has more than one path to follow [41].

Fiber based QKD systems are affected by the attenuation of the signal along the fiber which leads to limit the communication distance. In OF quantum channel the attenuation is mainly raised by the absorption and scattering losses. Almost 90% of total attenuation is due to the scattering losses only.

The absorption losses are related to the material composition and fabrication process of the fiber. While, the scattering losses caused by the imperfections within the fiber structure. Also, the attenuation of the light can be increased due to the microbending of the fiber [41].

To calculate the fiber loss or the fiber attenuation, let the optical power coupled to the OF is $p(0)$ i.e. at origin $z = 0$, at a distance z the power is given by [42],

$$p(z) = p(0)e^{-\alpha_p z} \tag{3.1}$$

Where α_p refers to the attenuation constant of the fiber (per Km) [42],

$$\alpha_p = -\frac{1}{z}\ln\left[\frac{p(0)}{p(z)}\right]$$

$$\therefore\ \alpha_p\left(\frac{dB}{km}\right) = -10\frac{1}{z}\log\left[\frac{p(0)}{p(z)}\right] \tag{3.2}$$

With respect to the dispersion in SMF, real SMF has a core with a semi-elliptical shape profile rather than ideal circular core; this in turn leads to eliminate the degeneracy of orthogonal modes and leads to different group velocities. This results in pulse broadening and this effect is known as polarization mode dispersion (PMD) [43].

Thus, PMD randomly rotates the polarization of the optical pulses transmitted along the OF or in other words, rotate the polarization of the photon and hence enhance the $QBER$ of the QKD system and reduce the final shared secure key.

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.

The modeled OF quantum channel is characterized at 0.2 dB attenuation per km at λ =1550nm according to SMF Corning (SMF-28) specifications. While, at λ =900nm, α_p=2 dB/km and α_p=3 dB/km at λ=830nm according to the attenuation curve as a function of λ shown in Figure (3.1) [44]. As a result, the OF attenuation can be considered as a function of the fiber length (L) and λ.

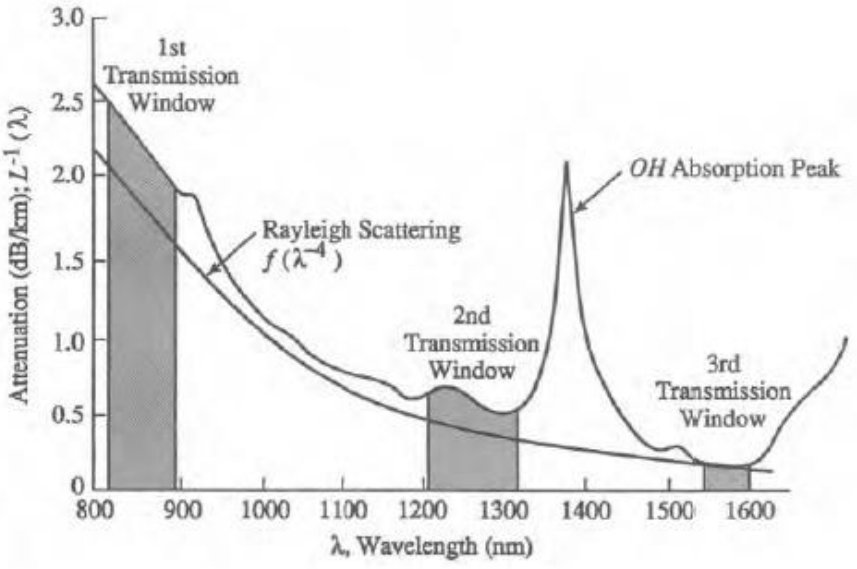


Fig.3.2 Attenuatioin curve vs. λ of the OF link [44]

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 to the polarization rotation disturbance, 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 appears clearly on the overall $QBER$ of the QKD system and the final

secure key rate when studied in Ch.5 and hence limits the communication distances to compensate these effects.

The first step in modeling was to review the functionality, operation and the performance characteristics of the OF quantum channel using different standard references. The information provided from the first step was used in the second modeling step to build the conceptual model. In addition to the mathematical model, the conceptual model will be utilized to code the OF quantum channel model using Matlab.

3.2.2 The Optical fiber quantum channel conceptual model

OF quantum channel is a passive component with one input and one output as shown in the corresponding conceptual model of Figure (3.2).

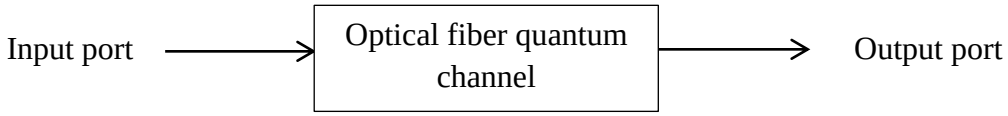


Fig.3.2 Optical fiber quantum channel conceptual model

In Figure (3.2), the incoming optical pulses from the QKD transmitter enter the input port and propagate along the OF quantum channel. The propagated optical pulses will be under the influence of fiber attenuation and polarization rotation distortions as 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 (ϑ) 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.(2.15) with P_{peak}in (mW), transmitted λ in nm, L and α_p can be set by the user in the modeling GUI tool.

3.2.3 The Optical fiber quantum channel mathematical model

The coherent optical pulse defined in Eq.(2.15) represents the input to the OF quantum channel model. For a non-dispersive medium; θ will be constant at all spatial points z, .i.e., assumed (0 degree) in this work. For the sake of simplicity, $|g(t)|$ 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 $\alpha_{inc.}$.

In this proposed model, the suggested solution to simulate the effect of PMD was via randomly rotating the polarization of the optical pulses coupled to the fiber.

In order to find the behavior of the transmitted optical pulses after passing through the OF quantum channel, the following operation on the coherent 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 polarization variation by an angle (ϑ).

$$\vec{E}_{OF} = E_0 e^{-i(w_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.} + \vartheta) \\ \sin(\alpha_{inc.} + \vartheta) e^{i\Phi} \end{bmatrix} \sqrt{10^{\frac{-(\alpha_p / kmL)}{10}}} \tag{3.3}$$

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

$$\vec{E}_{OF} = E_0(\alpha_p) e^{-i(w_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.} + \vartheta) \\ \sin(\alpha_{inc.} + \vartheta) e^{i(\Phi)} \end{bmatrix} \tag{3.4}$$

3.2.4 Simulation results and discussion

The purpose of this section is to present the results with the analysis of modeling the OF quantum channel. OF quantum channel model has been implemented with a friendly GUI as shown in Figure (3.3) which represents the optical quantum channel including 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 α_p/km and to decide the OF quantum channel L in km. The user allowed α_p values vs. λ are listed within the GUI.

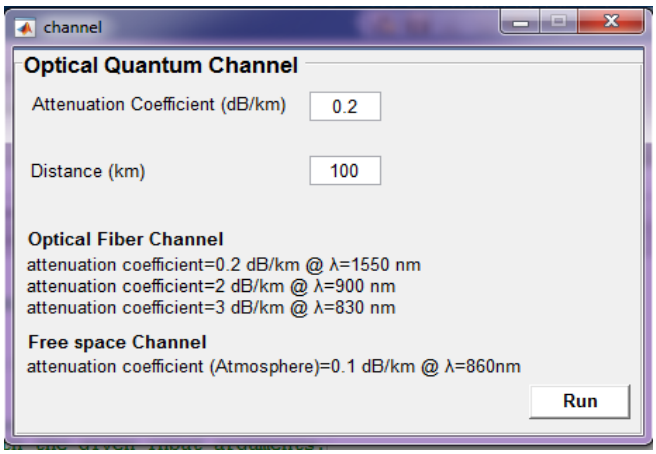
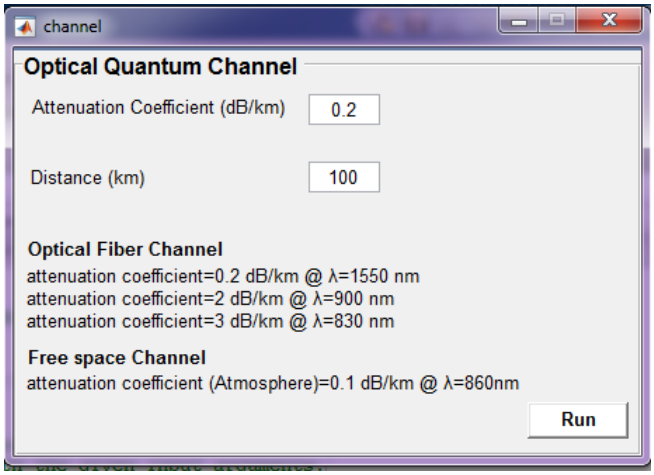


Fig.3.3 OF quantum channel simulator window

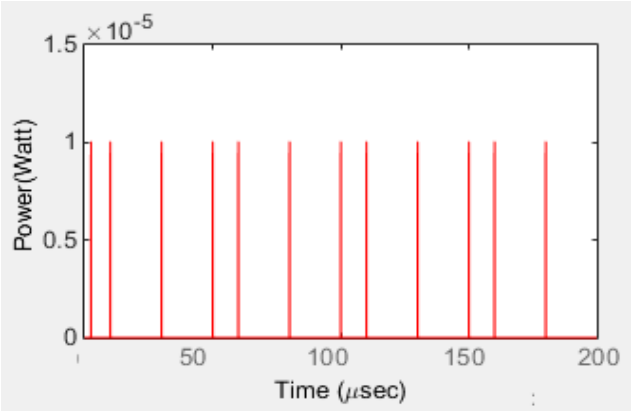
With respect to the simulation of the polarization rotation effect, the GUI plotters will not be able to clearly show the alteration in polarization in the transmitted optical pulses over the OF quantum channel. Otherwise, the effect of this error type will be significant on the QKD system performance by reducing both $QBER$ and final shared secure key as will be described in Ch.5.

Three 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 (3.4a) 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 λ=1550 nm. In this test, for 100 km length fiber and α_p =0.2 dB/km, the output power is equal to 0.01mW as shown in Figure (3.4b)



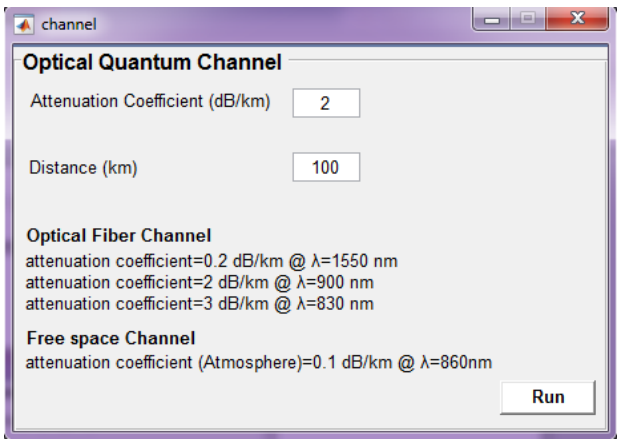
(a)



(b)

Fig.3.4 Test 1 (a) GUI set up (b) result for OF quantum channel for L =100km and α_p=0.2 dB/

Figure (3.5a) illustrates **Test 2** set up to examine the OF quantum channel model performance for λ=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 (3.5b).



(a)

Fig.3.5 Test 2 (a) GUI set up (b) result for OF quantum channel for L=100km and α_p=2 dB/km

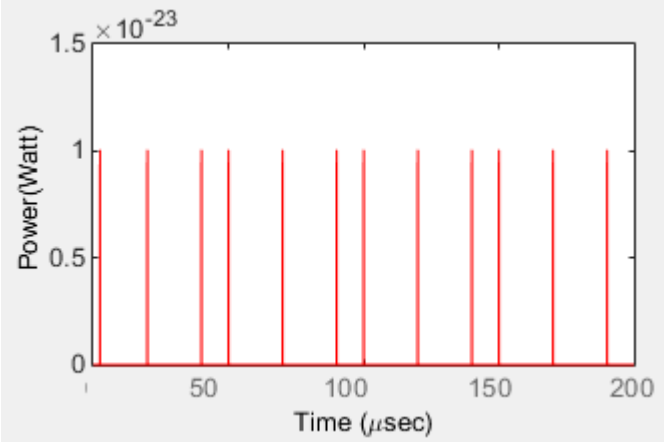
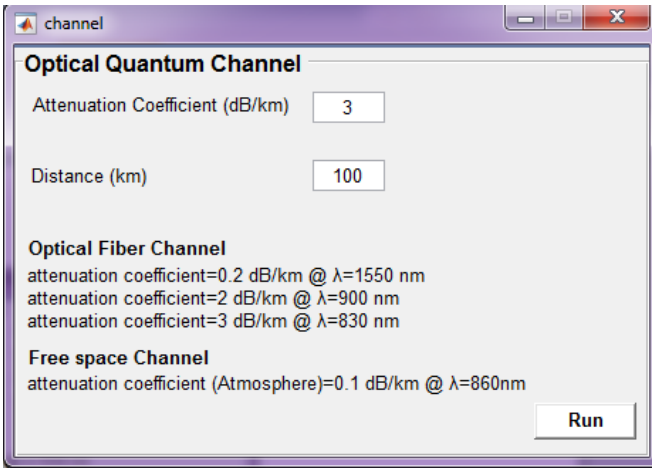
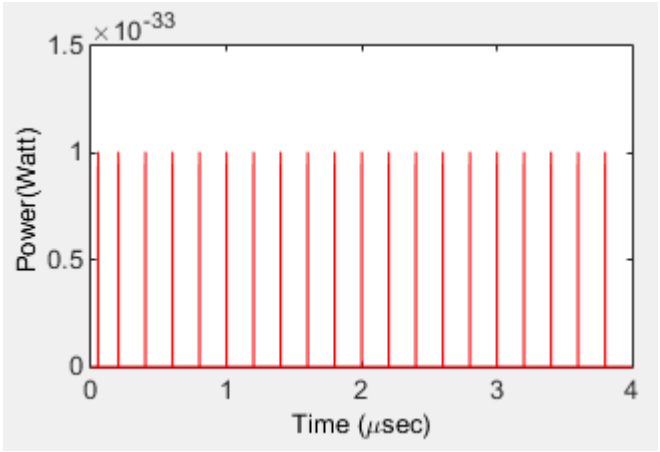


Fig.3.5 (b) continued

Figure (3.6a) illustrates **Test 3** set up to examine the OF quantum channel model performance for λ=830 nm. In this test, for 100 km long fiber and α_p=3 dB/km, the output power is equal to 10^{-33} W as shown in Figure (3.6b).



(a)



(b)

Fig.3.6 Test 3 (a) GUI set up (b) result for for OF quantum channel for L=100km and α_p=3 dB/km

The results obtained from the previous tests illustrate the performance degradation of OF quantum channel due to the effect of the fiber attenuation represented by absorption and scattering as *L* increased.

3.3 The Free-Space Quantum Channel

This section outlines the methodology used to model the FS quantum channel. It gives a vision to the operation basics of this link, the concept and the mathematical models that has been used for modeling. The final FS quantum channel GUI will be presented and discussed at the end of this section.

3.3.1 The Channel description

FS quantum channel can be defined as the physical link between two distant parities. Compared to OF quantum channel, FS quantum channel considered as unguided media. The atmosphere and the space are examples of this path. Optical communication systems including QKD implementations operate within near IR portion of the electromagnetic spectrum between 750nm and 1600 nm, which is used in line of sight and multipoint applications within limited areas [45].

Fiber based QKD systems are affected by the attenuation of the signal along the fiber which leads to limit the communication distance. As a solution to this imperfection, free space channel allows greater communication distances because atmosphere has low absorption in certain wavelengths. In addition, the atmosphere has nearly non-birefringent character which ensures the conservation of photon’s polarization state [46, 47]. However, terrestrial FS links suffer from attenuation caused by the atmosphere and objects in the line of site.

The attenuation in the atmosphere is mainly caused by three main factors. First impairment comes from the interaction of the propagated light beam with the particles and aerosols that constitutes the atmosphere which

results in different losses effects such as absorption, scattering and frequency selective attenuation [48].

It should be noted that the atmospheric attenuation via absorption is a function of λ and hence will obligate the operators to transmit within a minimum absorption range. With respect to the attenuation due to scattering mechanism, it could happen with or without λ variation but in contrast it depends on the atmosphere particles radius (r). For $r < \lambda$, the scattering type is known as Rayleigh scattering, if $r = \lambda$, the scattering type is known as Mie scattering. While, when $r > \lambda$, the diffraction phenomenon will be utilized to describe the scattering effect [49].

Second attenuation source is due to weather conditions. Dense fog could scatter the light energy and hence significantly attenuate it to more than 30dB/km as the fog droplets size is approximately identical to the λ used. In contrast, the attenuation due to rain is approximately equal to 3dB/km as the fog droplets size is larger than the λ used. The transmitted signal strength may also be fade due to slight fluctuations in the atmosphere refraction index. This effect is known as the scintillation [48].

Most of FS systems are operating within the ranges of 780–850nm and 1520–1600 nm because the atmosphere seems to be transparent within these λ windows as shown in Figure (3.7) [50].

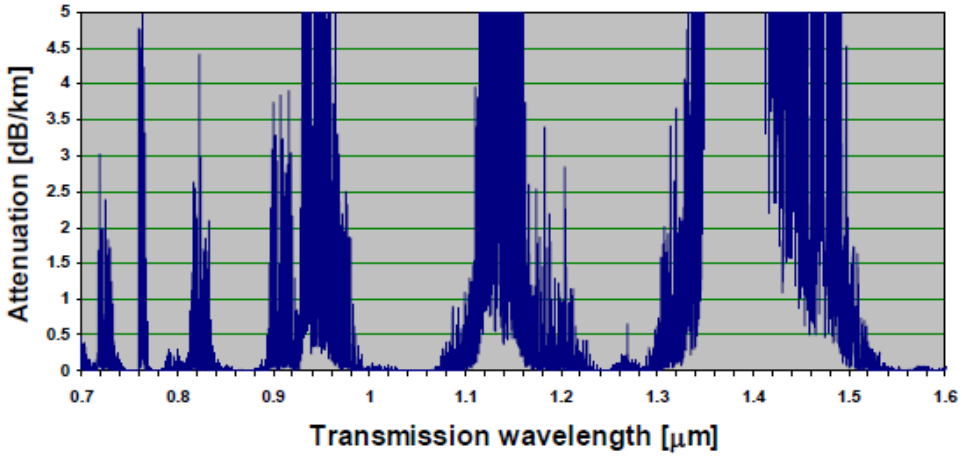


Fig.3.7 Atmosphere attenuation vs. λ in near-IR range [50]

Another source of attenuation is represented by the light beam diffraction. For diffraction problem, the reflective Cassegrain telescope design is used for the transmission and reception of optical signals. The secondary mirror of this telescope adds a central obscuration. Also, the beam can be diffracted due to the distance between the telescopes and their finite dimensions [47].

The modeled FS quantum channel is characterized at 0.1 dB attenuation per km at λ =860 nm according to Figure (3.7). In addition to the very low attenuation level feature at this λ, the commercial SPAD operating within 600-900nm λ window show better operation performance with higher quantum detection efficiency reaching 70% as mentioned in C30921S silicon avalanche photodiode specification data sheet (Appendix2) and [46].

The first modeling step was to review the functionality, operation and the performance characteristics of the FS quantum channel using different standard references. The information provided from the first step was used in the second modeling step to build the conceptual model. In addition to the mathematical model, the conceptual model will be utilized to code the FS quantum channel model using Matlab.

3.3.2 The Free-space quantum channel conceptual model

FS quantum channel is a passive component with one input and one output as shown in the corresponding conceptual model of Figure (3.8).

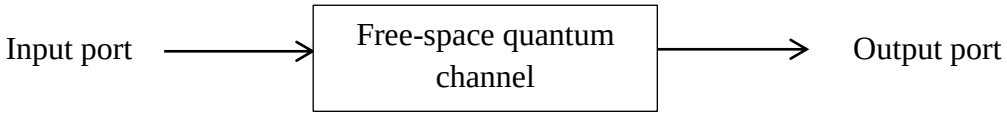


Fig.3.8 Free-space quantum channel conceptual model

In Figure (3.8), the incoming optical pulses from the QKD transmitter will enter the input port and propagate along the FS quantum

channel. 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 lunched to the space will maintain along the path.

3.3.3 The Free-space quantum channel mathematical model

For FS as a quantum channel, the channel transmittance model must take into consideration all impairments that affect the performance of 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 atmosphere 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 are the absorption and scattering due to dust, aerosols, carbon dioxide, etc. [49]. The propagated light photons will interact with the atmosphere particles which lead to scatter and absorb part of these photons [51].

Thus, the amount of the 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[49],

$$P_R = P_T e^{-OD} \tag{3.5}$$

Where OD is the optical depth, P_R and P_T are the received and transmitted power respectively [51],

$$\therefore T_{link} = \frac{P_R}{P_T} = e^{-OD} \tag{3.6}$$

Where T_{link} is known as the transmittance of the link which defines the amount of the transmitted light power along the channel [49].

The atmospheric attenuation coefficient ($\sigma(\lambda)$) is related to this atmospheric transmittance by [51],

$$T_{link} = e^{-\sigma(\lambda)L} \tag{3.7}$$

The overall $\sigma(\lambda)$ will sum up all the absorption and scattering coefficients within the atmosphere [49],

$$\sigma(\lambda) = \sigma_a(\lambda) + \sigma_m(\lambda) + \beta_a(\lambda) + \beta_m(\lambda) \tag{3.8}$$

Where first two terms show the aerosol and molecular absorption coefficients, respectively , whereas, 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 [51],

$$\delta_{propagation} = -10 \log_{10} T_{link} \tag{3.9}$$

To calculate the attenuation of optical signal propagating through FS quantum channel due to atmospheric effects represented in sub-section 3.3.1, the channel attenuation (δ_{atm}) in (dB/km) can be expressed as [49],

$$\delta_{atm} = \frac{1}{L} 10 \log(\frac{P_T}{P_R}) \tag{3.10}$$

$$\therefore \delta_{atm} = \frac{1}{L} 10 \log e^{\sigma(\lambda)L} \tag{3.11}$$

Finally, the diffraction-limited beam divergence loss in dB can be defined as [47],

$$\delta_{diff} = -10 \log_{10}[\left(e^{-2\gamma_t^2 a_t^2} - e^{-2a_t^2}\right)\left(e^{-2\gamma_r^2 a_r^2} - e^{-2a_r^2}\right)] \tag{3.12}$$

Where

$$\gamma_{t,r} = \frac{b_{t,r}}{R_{t,r}}, \alpha_{t,r} = \frac{R_{t,r}}{w_{t,r}}, \; w_t = R_t \; and \; w_r = \frac{\sqrt{2}\lambda L}{\pi R_t}$$

,

Where the subscript t refers to the transmit telescope and r is the receive one. 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 [46, 47],

$$\delta_{total} = \delta_{propagation} + \delta_{atm} + \delta_{diff} + \delta_{det} \quad (3.13)$$

Where δ_{det} is the single-photon detection efficiency of the single-photon detector which is a product of the quantum efficiency times the probability that the primary photo-generated electron – hole pair initiates a pulse of adequate gain to be counted [52].

In addition to the optical pulse time profile with linear polarization as defined in Eq.(2.15) , a list of all the required parameters as inputs to the simulation model is found in Table (3.1). The telescope's primary and secondary mirror radius in addition to $\delta_{propagation}$ are taken from SILEX experiment and Tenerife's telescope [46, 53, 54]. L and δ_{atm} can be set by the user in the modeled GUI tool.

Table 3.1. Input parameters for FS quantum channel modeling

Parameter	**Value**
P_{peak}	1 mW
λ	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% @ λ=860 nm
$\delta_{propagation}$	1 dB

The coherent optical pulse defined in Eq. (2.15) represents the input to the FS quantum channel model. From the coherent optical pulse representation, the signal parameters related to the FS quantum channel model that modify or change the signal characteristics at the output of the FS quantum channel is E_0.

In order 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,

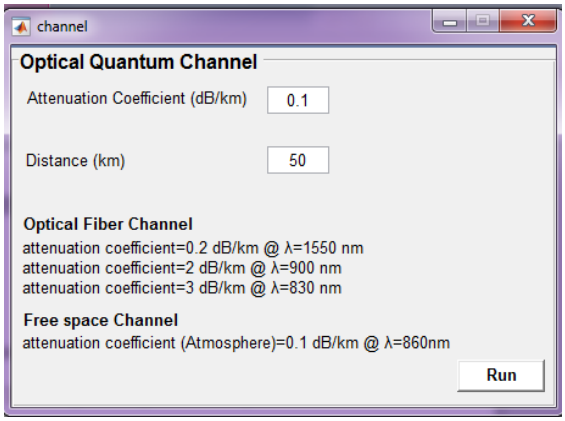
$$\vec{E}_{FS} = E_0 e^{-i(w_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} (\delta_{total}) \quad (3.14)$$

3.3.4 Simulation results and discussion

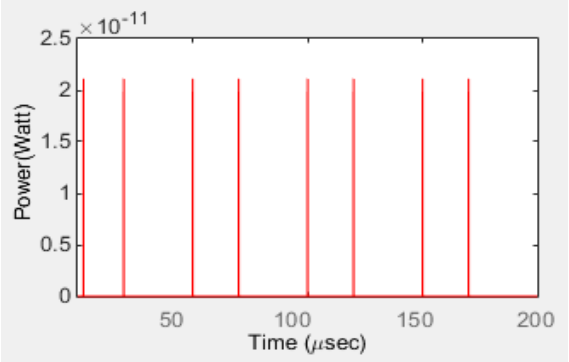
The purpose of this section is to present the results with the analysis of modeling the FS quantum channel. FS quantum channel model has been implemented with a friendly GUI as shown in Figure (3.3). FS quantum channel is modeled at λ= 860 nm because the channel has minimum attenuation losses and seems to be transparent as shown in Figure (3.7).

Three tests were applied to verify the modeled FS quantum channel model to simulate the FS quantum channel operation. The presented results illustrate the FS quantum channel simulation for δ_{atm}= 0.1 only because the selected transmission is at λ=860 nm. This model can support any other scenario as per user requirements to study the performance of FS quantum channel. For all the three tests, the incoming optical pulses from the QKD transmitter are linearly polarized with PRR= 100 kHz and P_{peak}= 1mW.

Figure (3.9a) illustrates **Test 1** set up to investigate the attenuation in the transmitted optical pulses after passing through the FS quantum channel model. In this test, for 50 km link length, the output power is equal to 0.02nW as shown in Figure (3.9b).



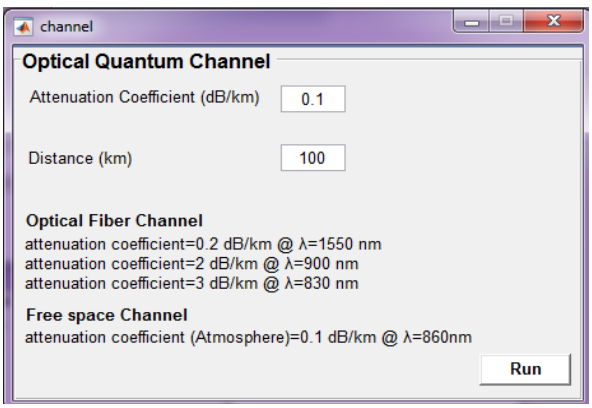
(a)



(b)

Fig.3.9 Test 1 (a) GUI set up (b) result for FS quantum channel for *L* =50km

Figure (3.10a) illustrates **Test 2** 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 (3.10b).



(a)

Fig.3.10 Test 2 (a) GUI set up (b) result for FS quantum channel for *L* =100km

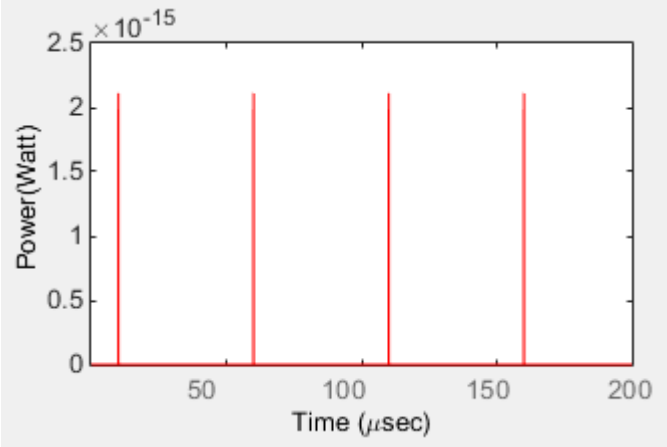
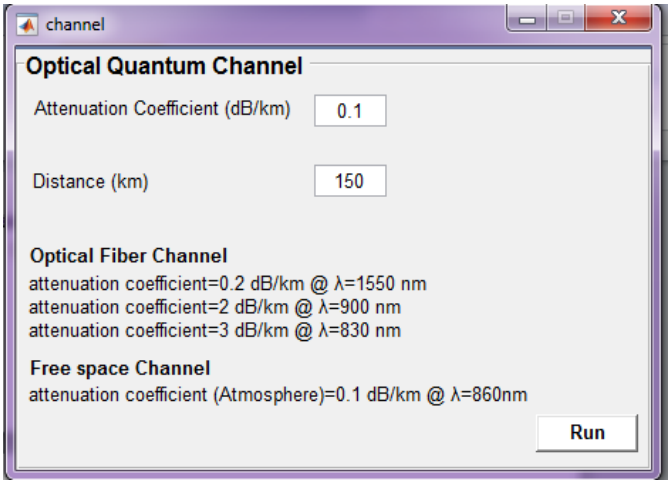
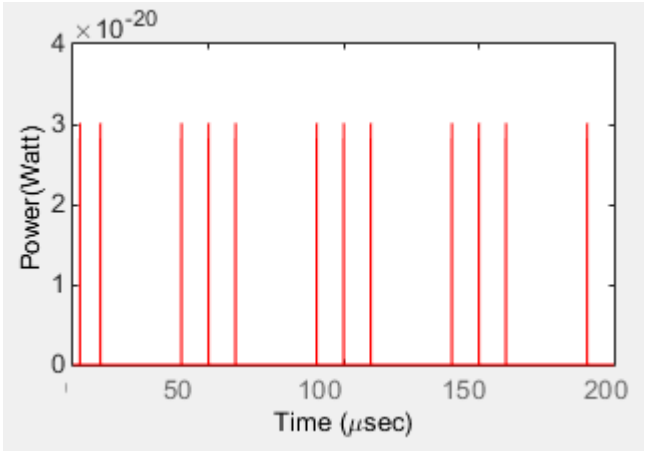


Fig.3.10 (b) Continued

Figure (3.11a) illustrates **Test 3** set up. In this test, for 150 km link length, the output power is equal to 300 aW as shown in (3.11b).



(a)



(b)

Fig.3.11 Fig.3.11 Test 3 (a) GUI set up (b) result for FS quantum channel for *L* =150km

The results obtained from the previous tests illustrate the performance degradation of FS quantum channel due to the effect of atmospheric and weather conditions in addition to the beam divergence due to diffraction as L increased. The impact of the errors produced by all effects that was previously mentioned is significant on the QKD system performance by reducing both $QBER$ and final shared secure key as will be described in Ch.5.

Chapter Four

The Receiver of BB84 Protocol

Chapter Four

The Receiver of BB84 Protocol

4.1 Introduction

The purpose of this chapter is to identify and model the receiver of BB84 protocol. The exploration for each part begins with a general component explanation obtained from data sheets and related reference literatures. Based on this research, the most important component behaviors of interest will be the basis of the component conceptual model which will be the first modeling step. Later, the mathematical model that takes into account the performance parameters believed to be important for modeling the receiver parts will be introduced. Finally, samples of modeled output with the analysis for each modeled optical component will be presented.

Figure (4.1) illustrates the main receiver parts and the modeling flow that has been conducted in this research. The half wave plate part will not be modeled as a separate component, instead, its effect will appear later within the system in Ch. (5) by adding a phase shift to rotate the incoming optical pulses by 45° for the polarization detection process.

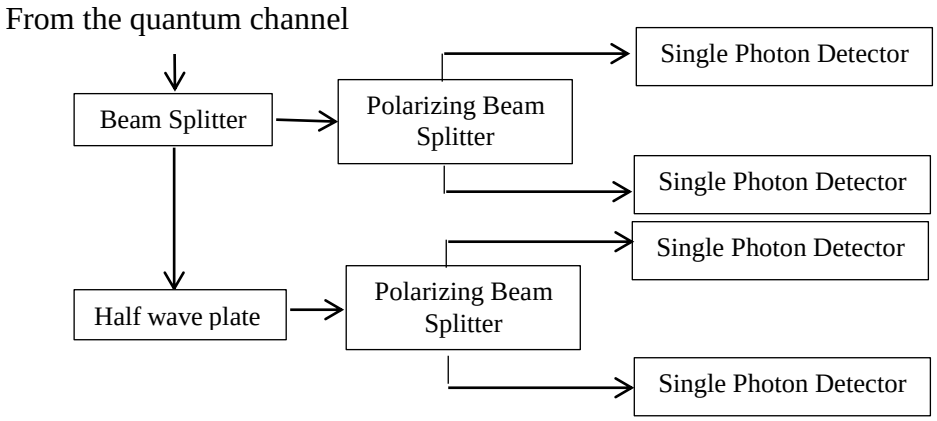


Fig.4.1 Modeled QKD Receiver

4.2 The Beam Splitter

This section outlines the methodology used to model the BS device. It gives a vision to the operation basics of this component, the concept and the mathematical models that has been used for modeling. Final BS GUI will be presented and discussed at the end of this section.

4.2.1 The Device description

BS is a passive optical device used to divide the incident laser beam into two beams [37]. The ratio of the optical power sent to the output ports can be decided by the material inside the BS. According to the QKD systems requirements, 50:50 splitting ratio is required whether the optical source is emitting single photons or attenuated coherent optical pulses. The splitting ratio can be defined as the ratio between high output percentage (HOP) to the low output percentage (LOP). In this case, BS will equally split the input optical power to reflected and transmitted signals. BS can be set to other splitting ratios such as 90:10, 70:30 [37]. This component plays an important role in polarization detection in BB84 receiver implementation where it is used to decide the polarization basis (i.e., diagonal or rectilinear) sent by transmitter [18].

This type of non-polarizing BS can be made by gluing two triangular prisms where the incident optical power is separated at a thin layer acting as an interface between these prisms which form a cube structure [55]. BS with cube design has been adopted through this work. The thickness of this interface is utilized to set the splitting amount for a certain λ. The output beams from BS device is not ideally polarization preserved due to some phase delay between the output polarization components [55]. Another physical BS design can be obtained by using the in-line fiber optic BS which is in addition can be used as a coupler. This type is a best choice for polarization control and measurements.

The BS theoretical concept depends on the Fabery-Perot (FP) interference effect of high quality plane reflectors and two symmetric glass plates encompassed by air as shown in Figure (4.2) that represents a cube BS [56].

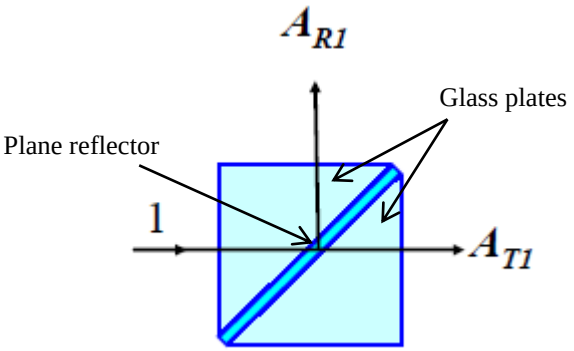
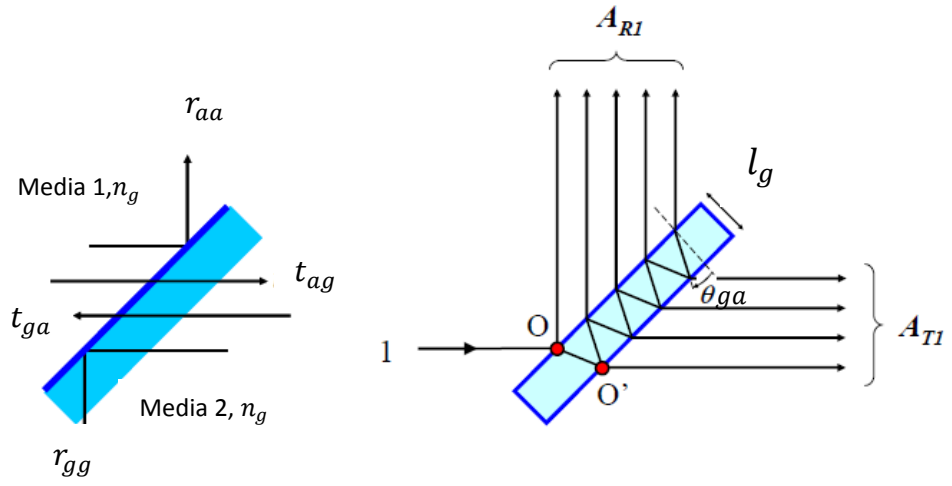


Fig. 4.2 Cube BS [56]

In order to calculate the expressions for the reflected and transmitted signals, FP interferometer model shown in Figure (4.3) will be used. Figure (4.3a) represents the transmission and reflection factors from air to glass and from glass to air. While, Figure (4.3b) shows the interference of reflected and transmitted signals at FP interferometer [56].



(a) **(b)**

Fig.4.3 Fabry-Perot model of the BS. O, O′ are reference points for total optical path difference summation [56]

The amplitude of the reflected signal is calculated as follows [56],

$$A_{R1} = \frac{t_{ag} t_{ga} e^{(i\acute{\varphi})}}{1 - r_{gg}^2 e^{(2i\acute{\varphi})}} \quad (4.1)$$

and the amplitude of the transmitted signal is calculated as [56],

$$A_{T1} = \frac{r_{aa+} r_{gg} (t_{ag} t_{ga}) e^{(2i\acute{\varphi})}}{1 - r_{gg}^2 e^{(2i\acute{\varphi})}} \quad (4.2)$$

$\acute{\varphi}$ can be found as, $\acute{\varphi} = \frac{2\pi}{\lambda} n_g l_g \cos \theta_{ga}$

Where

t_{ag} is the amplitude transmission factor from air to glass.

t_{ga} is the amplitude transmission factor from glass to air.

r_{aa} is the amplitude reflection factor from air to air.

r_{gg} is the amplitude reflection factor from glass to glass.

$\acute{\varphi}$ is the internal phase shift due to a single glass-crossing.

n_g is the glass refractive index.

l_g is the glass plate thickness.

θ_{ga} is the internal incidence angle at glass-air interface.

The first step in modeling was to review the functionality, operation and the performance characteristics of the BS using different standard references. The information provided from the first step was used in the second modeling step to build the conceptual model. In addition to the mathematical model, the conceptual model will be utilized to code the BS model using Matlab.

4.2.2 The Beam splitter conceptual model

BS is a passive component with one input and two output ports, .i.e., transmitted and reflected signals as shown in the corresponding conceptual model of Figure (4.4).

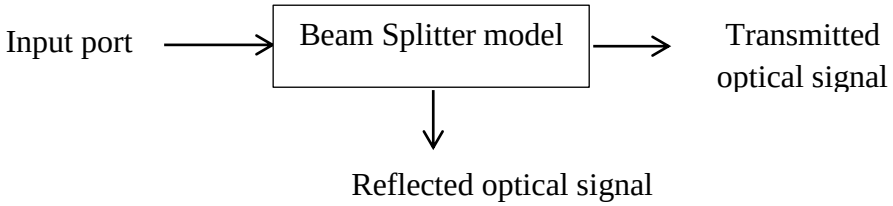


Fig.4.4 BS conceptual model

In Figure (4.4), The BS model will calculate the output optical power at each port with minimum dependence on the incoming optical signals polarization minus some amount of optical power lost due to device insertion loss ($L_{insertion}$), some excess loss such as return losses (L_{return}) and losses due to spatial polarization distribution which is known as polarization dependent loss (PDL) (L_{PDL}) [38].

As the inputs to the simulation model, the following parameters were considered; optical pulse time profile with linear polarization as defined in Eq.(2.15) with P_{peak}in (mW), the wavelength (λ) in nm, the orientation of the incoming optical pulse, $L_{insertion}$, L_{return}, L_{PDL}, HOP, LOP and BS offset angle (γ_{BS}).

4.2.3 The Beam splitter mathematical model

The coherent optical pulse defined in Eq.(2.15) represents the input to the BS component. For a non-dispersive medium; θ is constant at all spatial points z,.i.e., assumed (0 degree) in this research. For the sake of simplicity, $|g(t)|$ term will not be considered for the next steps in this model.

From the coherent optical pulse representation, the signal parameters related to the BS component that can modify the signal characteristics at the output of the BS are E_0 and $\alpha_{inc.}$.

Figure (4.5) shows 1×2 non-polarizing BS. The standard BS transformation matrix has one input E_1 and two outputs E_2, E_3.

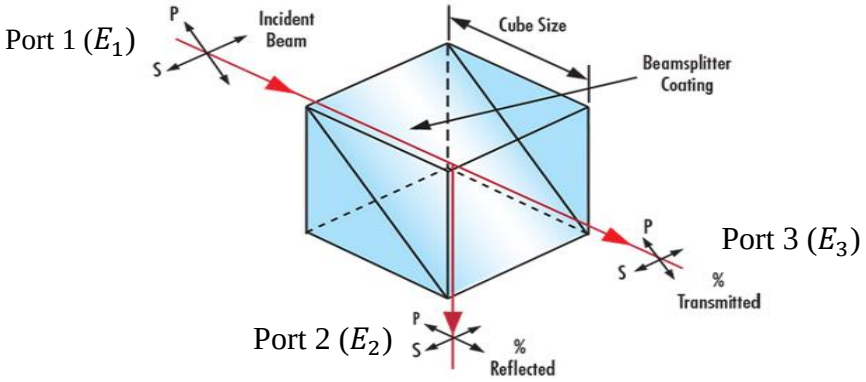


Fig. 4.5 Non-polarizing BS [58]

The 4×4 BS transformation matrix is defined as [38],

$$\epsilon = \frac{1}{10}\begin{pmatrix} \sqrt{LPO} & i\sqrt{HPO} & 0 & 0 \\ i\sqrt{HPO} & \sqrt{LPO} & 0 & 0 \\ 0 & 0 & \sqrt{LPO} & i\sqrt{HPO} \\ 0 & 0 & i\sqrt{HPO} & \sqrt{LPO} \end{pmatrix} \tag{4.3}$$

The electric field components for the transmitted beam can be described by [18],

$$E_{2x} = \frac{E_0}{\sqrt{2}}\cos(\alpha_{inc.} + \gamma_{BS})\sqrt{\frac{LOP}{100}}\sqrt{10^{\frac{-L_{insertion}}{10}}}\sqrt{10^{\frac{-L_{return}}{10}}}\sqrt{10^{\frac{-L_{PDL}}{10}}} \tag{4.4}$$

$$E_{2y} = \frac{E_0}{\sqrt{2}}\sin(\alpha_{inc.} + \gamma_{BS})\sqrt{\frac{LOP}{100}}\sqrt{10^{\frac{-L_{insertion}}{10}}}\sqrt{10^{\frac{-L_{return}}{10}}}\sqrt{10^{\frac{-L_{PDL}}{10}}} \tag{4.5}$$

Thus, the amplitude of the transmitted signal from port3 is [18],

$$E_2 = \sqrt{(E_{2x})^2 + (E_{2y})^2} \tag{4.6}$$

While, the electric field components for the reflected beam can be represented by [18],

$$E_{3x} = \frac{E_0}{\sqrt{2}}\cos(\alpha_{inc.} + \gamma_{BS})\sqrt{\frac{HOP}{100}}\sqrt{10^{\frac{-L_{insertion}}{10}}}\sqrt{10^{\frac{-L_{return}}{10}}}\sqrt{10^{\frac{-L_{PDL}}{10}}} \tag{4.7}$$

$$E_{3y} = \frac{E_0}{\sqrt{2}} \sin(\alpha_{inc.} + \gamma_{BS}) \sqrt{\frac{HOP}{100}} \sqrt{10^{\frac{-L_{insertion}}{10}}} \sqrt{10^{\frac{-L_{return}}{10}}} \sqrt{10^{\frac{-L_{PDL}}{10}}} \quad (4.8)$$

The amplitude of the reflected signal from port 2 is [18],

$$E_3 = \sqrt{(E_{3x})^2 + (E_{3y})^2} \quad (4.9)$$

4.2.4 Simulation results and discussion

The purpose of this section is to present the results with the analysis of modeling the BS component. BS component model has been implemented with a friendly GUI as shown in Figure (4.6). This interface with its configurable editing objects is responsible to allow users to configure the BS component model for beam splitting tests. The left plotter represents the reflected optical pulses, while, the right plotter shows the transmitted optical pulses. This model can support different values of γ_{BS}, $\alpha_{inc.}$, $L_{insertion}$, L_{return}, L_{PDL} and splitting ratios as per user requirements and immediately plots the resultant reflected and transmitted optical pulses measured in Watt.

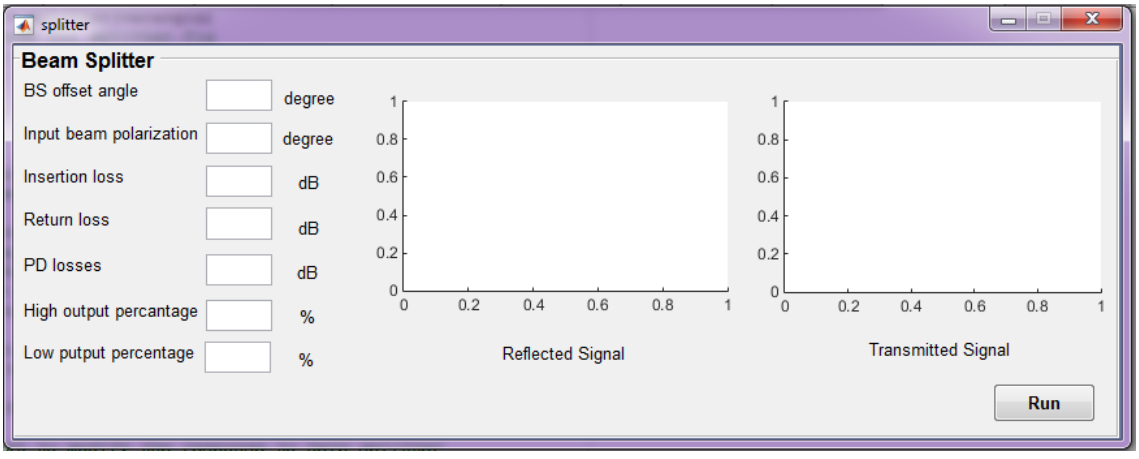


Fig.4.6 BS simulator window

The programming code that was designed to simulate the operation of the BS has been verified by test its capabilities to handle the beam splitting process under different input parameters and conditions. This

verification approach has been applied initially before the final GUI design of the component.

In order to prove the modeled BS operation validity, different use cases were supposed where the expected behavior of the validated BS mathematical model has been compared to the response of the final BS GUI when identical inputs are applied. The calculated results are sufficiently correct as will be seen by the following test cases.

Four tests were carried out to verify the modeled BS component to simulate the device operation. For all four tests, the input pulses for the BS were linearly polarized with $\alpha_{inc.}$=0°, PRR=100 kHz, P_{peak}= 1mW and λ=1550nm. Taking into consideration the device losses where $L_{insertion}$=1 dB, L_{return}=10 dB and L_{PDL}=0.25 dB. Figure (4.7) illustrates **Test 1** result to simulate the operation of BS designed to provide 50:50 splitting ratio with γ_{BS} =0°.

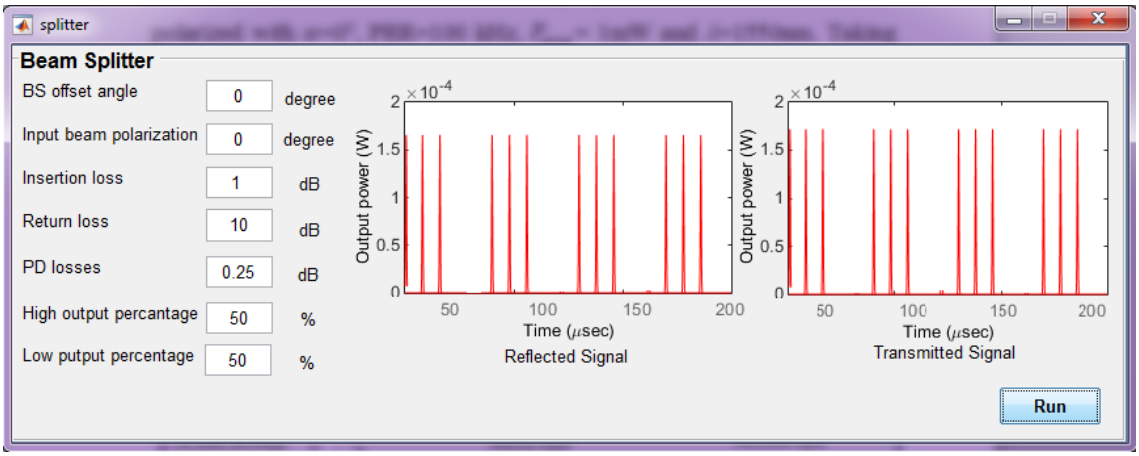


Fig.4.7 BS Test 1 result, splitting ratio 50:50, γ_{BS} =0°

Figure (4.8) illustrates **Test 2** result to simulate the operation of BS designed to provide 50:50 splitting ratio with γ_{BS} =90° to prove the minimum dependency of the modeled BS to the incoming optical signal polarization.

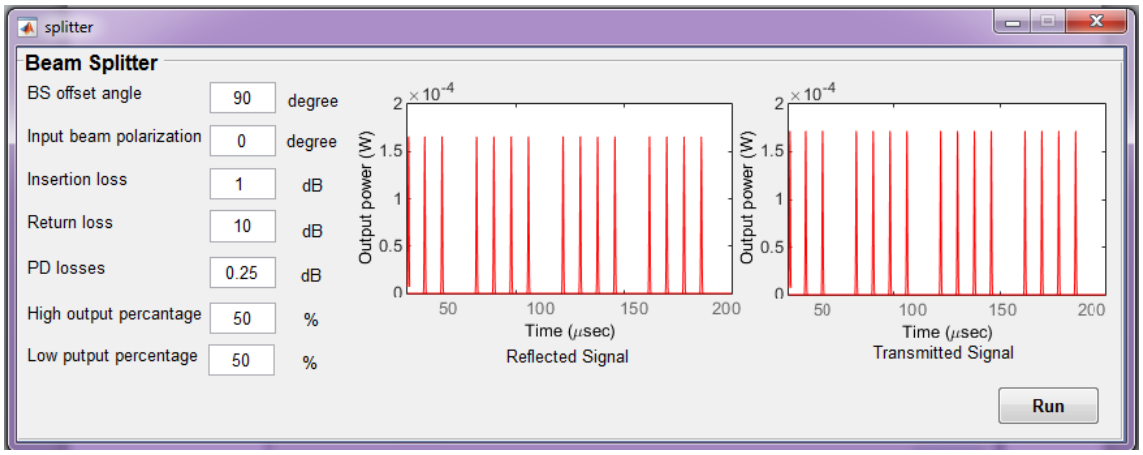


Fig.4.8 BS Test 2 result, splitting, ratio 50:50, γ_{BS} =90°

Figure (4.9) illustrates **Test 3** result to simulate the operation of BS designed to provide 90:10 splitting ratio with γ_{BS} =0. The left plotter shows that the maximum amount of the incident optical power is reflected through the reflection port. While, the right plotter illustrate the remaining 10% of the incident optical power is passed through the transmission port.

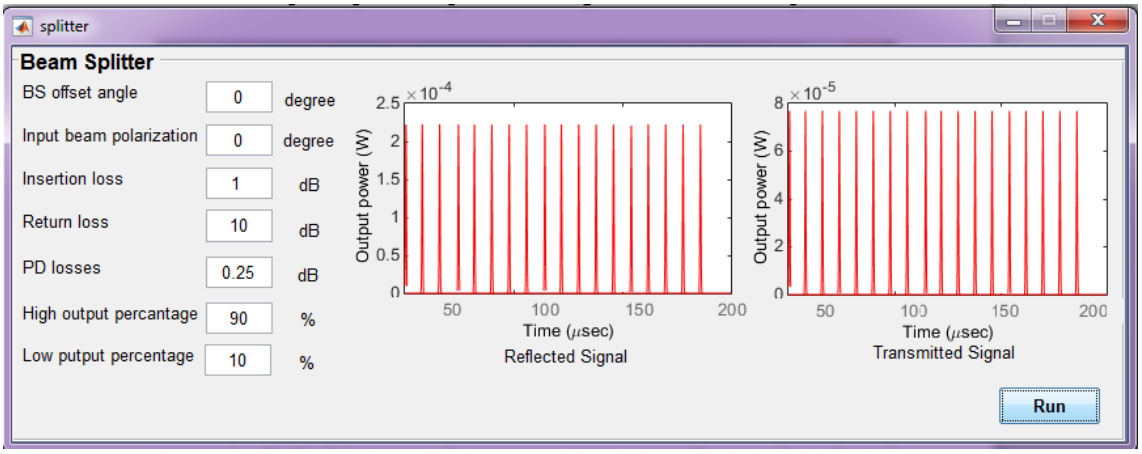


Fig.4.9 BS Test 3 result, splitting ratio 90:10, γ_{BS} =0°

Figure (4.10) illustrates **Test 4** result in which the incident optical power is divided between the output ports according to the selected splitting ratio, 70:30 with γ_{BS} =0°.

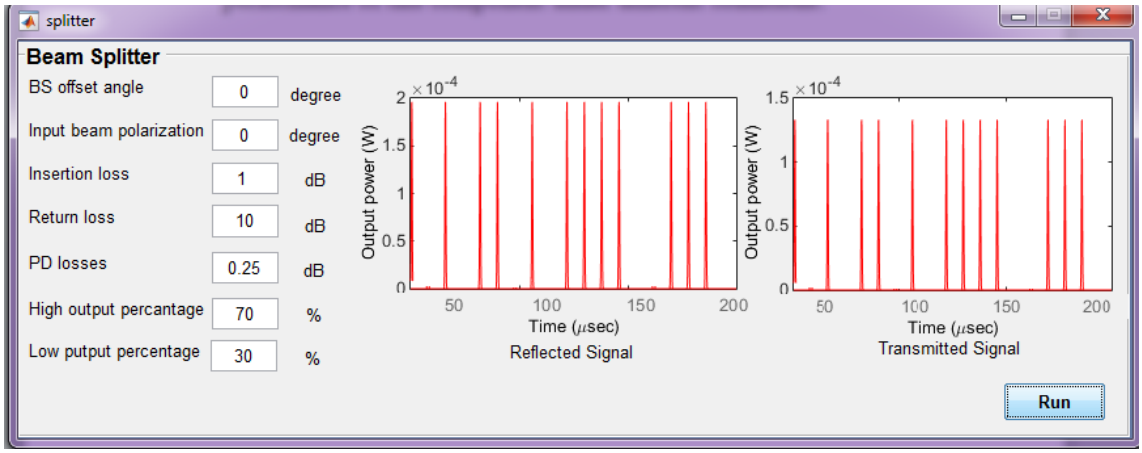


Fig.4.10 BS Test 4 result, splitting ratio 70:30, γ_{BS} =0°

Finally, this model can support any inputs from the user to study the performance of this component under different conditions.

4.3 The Polarizing Beam Splitter

This section outlines the methodology used to model the PBS device. It gives a vision to the operation basics of this component, the concept and the mathematical models that has been used for modeling. Final PBS GUI will be presented and discussed at the end of this section.

4.3.1 The Device description

PBS is a passive optical device used to divide the incident optical signal into two orthogonally polarized transmitted and reflected signals [37]. The transmitted optical signal is horizontally polarized while the reflected optical signal is vertically polarized [18]. This type of polarizing BS can be made by gluing two triangular prisms where the incident light power will be separated into two perpendicular polarization beams at a thin dielectric coating layer that acts as an interface between these prisms [38].

Practical PBS components are restricted by the alternating low and high index of $\lambda/4$ thickness reflectance coatings as applied to real materials [57]. As a result, PBS effective λ and light incident angle range is limited. To improve the performance of the PBS, the preferable PBS

coating design can be verified by using a thin film with a group of plates operating near Brewster's angle to increase the reflection ratio of the vertically polarized component of the light beam. At the Brewster's angle, the entire horizontal polarization component is transmitted while not all the vertical polarization component is reflected to the correct path. Thus, operating near Brewster's angle ensures that the light s-polarization component is completely reflected. Another widely used physical design of the PBS which is called PBS cube can be verified with 45° angle of incidence as shown in Figure (4.11) [57].

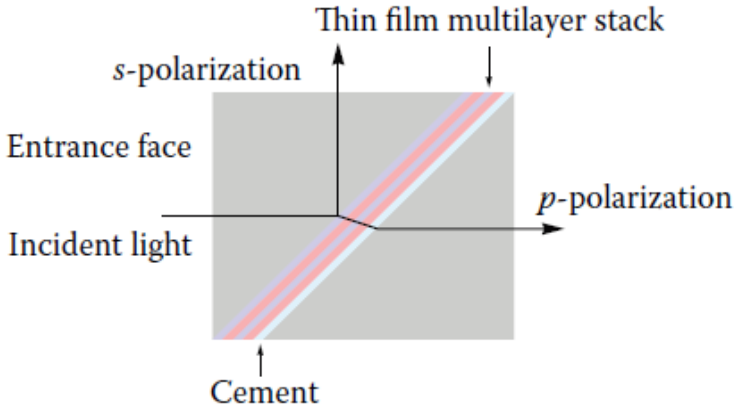


Fig.4.11 polarization beam splitting cube [57]

The number of the coating layers that must be utilized has a great impact on the overall PBS performance as shown in Figure (4.12) which represents the performance of a MacNeille PBS coating. The reflectance intensity of the light s-component (R_s) is enhanced as the number of coating layers increased up to 10 pair layers and then starts to alternate whenever more layers are added. While, the light P-component (T_p) ratio is weakly dependent on the number of the coating layers as it represents the transmission case at the Brewster's angle [57].

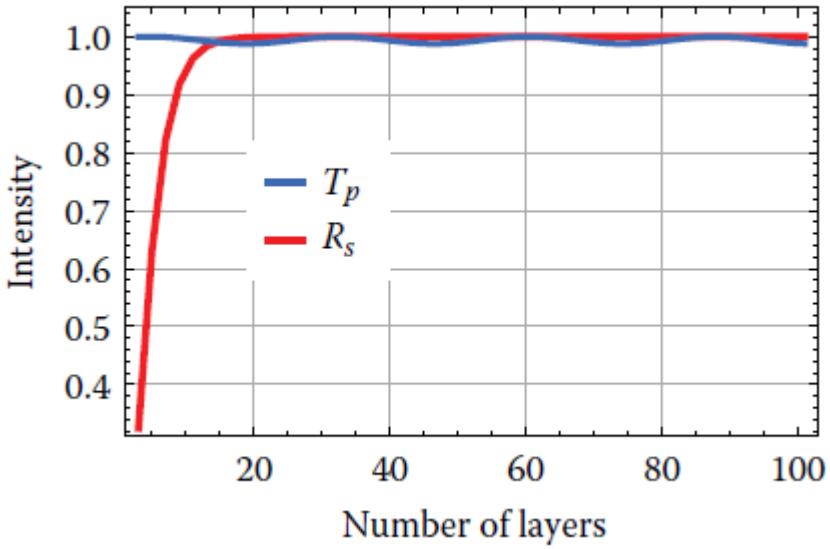


Fig.4.12 Reflected and transmitted light intensity vs PBS coating number of layers [57]

This component plays an important role in polarization detection in QKD systems where it can be used to measure the polarization states (i.e., 0°, 45°, 90° and-45°) sent by transmitter [18].

The modeled PBS has one optical input port and two optical output ports. The input signal is applied via the modeled PBS, while, the output ports generate orthogonally polarized transmitted and reflected optical beams that pass to the modeled single-photon detectors.

The first step in modeling was to review the functionality, operation and the performance characteristics of the PBS using different standard references. The information provided from the first step was used in the second modeling step to build the conceptual model. In addition to the mathematical model, the conceptual model will be utilized to code the PBS model using Matlab.

4.3.2 The Polarizing beam splitter conceptual model

PBS is a passive component with one input and two output ports as shown in the corresponding conceptual model of Figure (4.13).

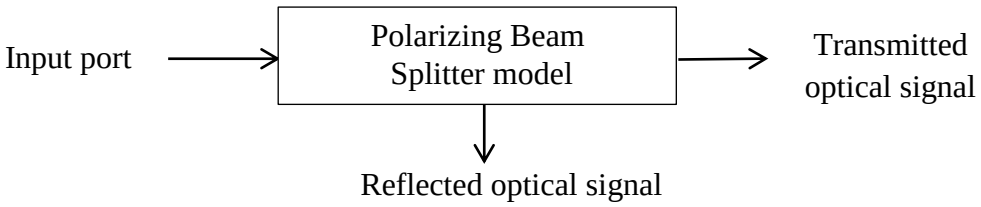


Fig.4.13 PBS conceptual model

In Figure (4.13), the phase of the reflected optical power beam is orthogonal with the phase of the transmitted optical power beam due to additional 90° phase shift results from the reflection inside PBS. The PBS model will calculate the output optical power at each port minus some amount of optical power lost due to $L_{insertion}$, L_{return} and L_{PDL}.

As the inputs to the simulation model, the following parameters were considered, optical pulse time profile with linear polarization as defined in Eq.(2.15) with P_{peak}in mW, transmitted optical signal wavelength λ in nm, the orientation of the incoming optical pulse, $L_{insertion}$, L_{return}, L_{PDL} and γ_{PBS} for PBS.

4.3.3 The Polarizing beam splitter mathematical model

The coherent optical pulse defined in Eq.(2.15) represents the input to the PBS component. From the coherent optical pulse representation, the signal parameters related to the PBS component and hence modify or change the signal characteristics at the output of PBS are E_0 , Φ and $\alpha_{inc.}$.

Figure (4.14) represents a cube PBS with one input $E_1$and with P and S polarization states for the reflected and transmitted signals (E_2 and E_3) respectively.

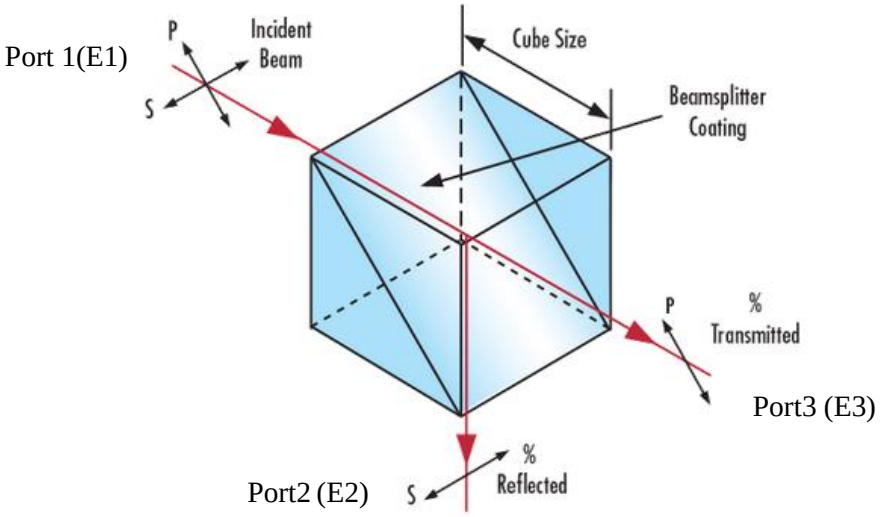


Fig. 4.14 polarizing BS [58]

The PBS transformation matrix is defined as [38],

$$P(\gamma) = \begin{pmatrix} (cos\ (\gamma_{PBS}))^2 & (\cos(\gamma_{PBS})\ \sin(\gamma_{PBS})) \\ (\cos(\gamma_{PBS})\ \sin(\gamma_{PBS})) & (sin\ (\gamma_{PBS}))^2 \end{pmatrix} \quad (4.11)$$

The electric field components for the transmitted beam can be described by:

$$\therefore E_{2x} =$$

$$E_0 e^{-i(\omega_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} P(\gamma_{PBS}) \sqrt{10^{\frac{-L_{insertion}}{10}}} \sqrt{10^{\frac{-L_{return}}{10}}} \sqrt{10^{\frac{-L_{PDL}}{10}}} \quad (4.12)$$

For orthogonality condition it is assumed that γ_{PBS} =90°

Thus [18, 59],

$$E_{2x} = \frac{E_0}{\sqrt{2}}\ e^{-i(\omega_0 t)} e^{j\theta} |g(t)| \sin(\alpha_{inc.} + \gamma_{PBS}) \sqrt{10^{\frac{-L_{insertion}}{10}}} \sqrt{10^{\frac{-L_{return}}{10}}} \sqrt{10^{\frac{-L_{PDL}}{10}}} \quad (4.13)$$

E_{2y}=Extinction Ratio

Where the extinction ratio is the ratio of maximum to minimum transmission of a sufficiently linearly polarized input [38].

Thus, the amplitude of the transmitted signal from port2 is [18, 59],

$$E_2 = \sqrt{(E_{2x})^2 + (E_{2y})^2} \quad (4.14)$$

While, the electric field components for the reflected beam can be represented by:

$$E_{3y} = E_0 e^{-i(\omega_0 t)} e^{j\theta} |g(t)| \begin{bmatrix} \cos(\alpha_{inc.}) \\ \sin(\alpha_{inc.}) e^{i\Phi} \end{bmatrix} P(\gamma_{PBS}) \sqrt{10^{\frac{-L_{insertion}}{10}}} \sqrt{10^{\frac{-L_{return}}{10}}} \sqrt{10^{\frac{-L_{PDL}}{10}}} \quad (4.15)$$

For orthogonality condition it is assumed that γ_{PBS} =0°

Thus [18, 59],

$$E_{3y} = \frac{E_0}{\sqrt{2}} e^{-i(\omega_0 t)} e^{j\theta} |g(t)| \cos(\alpha_{inc.} + \gamma_{PBS}) \sqrt{10^{\frac{-L_{insertion}}{10}}} \sqrt{10^{\frac{-L_{return}}{10}}} \sqrt{10^{\frac{-L_{PDL}}{10}}} \quad (4.16)$$

E_{3x}=Extinction Ratio

Thus, the amplitude of the reflected signal from port3 is [18, 59],

$$E_3 = \sqrt{(E_{3x})^2 + (E_{3y})^2} \quad (4.17)$$

4.3.4 Simulation results and discussion

The purpose of this section is to present the results with the analysis of modeling the PBS component. PBS component model has been implemented with a friendly GUI as shown in Figure (4.15). This interface with its configurable editing objects is responsible to allow users to configure the PBS component model for polarization splitting tests. The left plotter represents the reflected optical pulses. While, the right plotter shows the transmitted optical pulses. This model can support different values of γ_{PBS}, $\alpha_{inc.}$, $L_{insertion}$, L_{return} and L_{PDL} as per user requirements and immediately plot the resultant reflected and transmitted optical pulses measured in Watt.

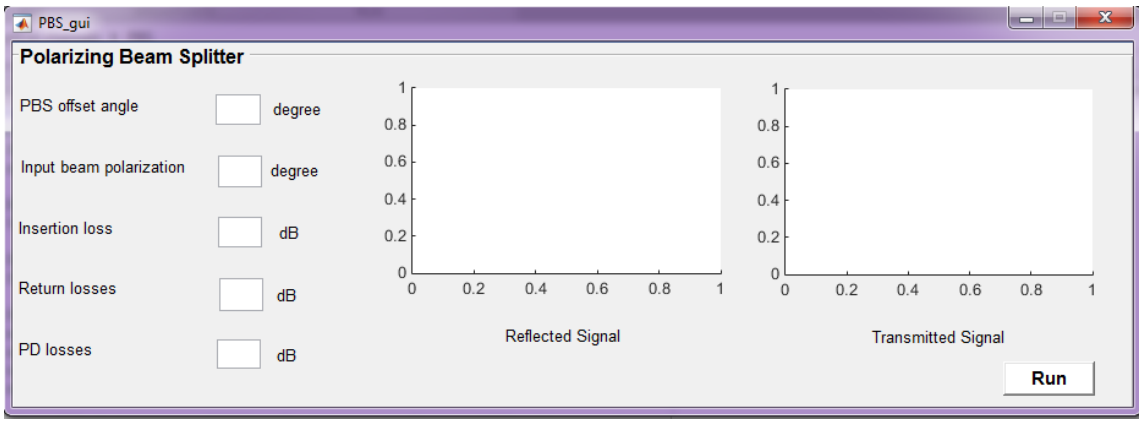


Fig.4.15 PBS simulator window

The programming code that was designed to simulate the operation of the PBS has been verified by testing its capabilities to handle the beam splitting process according to the polarization under different input parameters and conditions. This verification approach has been applied initially before the final GUI design of the component.

In order to prove the modeled PBS operation validity, different use cases were supposed where the expected behavior of the validated PBS mathematical model has been compared to the response of the final PBS GUI when both applying the identical inputs. The calculated results are sufficiently correct as shown in the following results.

Four tests were done to verify the modeled PBS component to simulate the polarization splitter device operation. For all four tests, the input pulses for the PBS are linearly polarized with PRR=100 kHz, P_{peak}=1mW, λ=1550nm, taking into consideration the device losses where $L_{insertion}$=1 dB, L_{return}=10 dB and L_{PDL}=0.25 dB.

Figure (4.16) illustrates **Test 1** result to simulate the operation of the PBS when its transmission axis in a horizontal position (i.e., γ_{PBS}=0°). Assume the incident light beam is vertically polarized (i.e., $\alpha_{inc.}$=90°). It can be shown from this figure, as long as the incident light beam is purely S polarized (i.e., vertically polarized), then the optical beam is reflected by 90°.

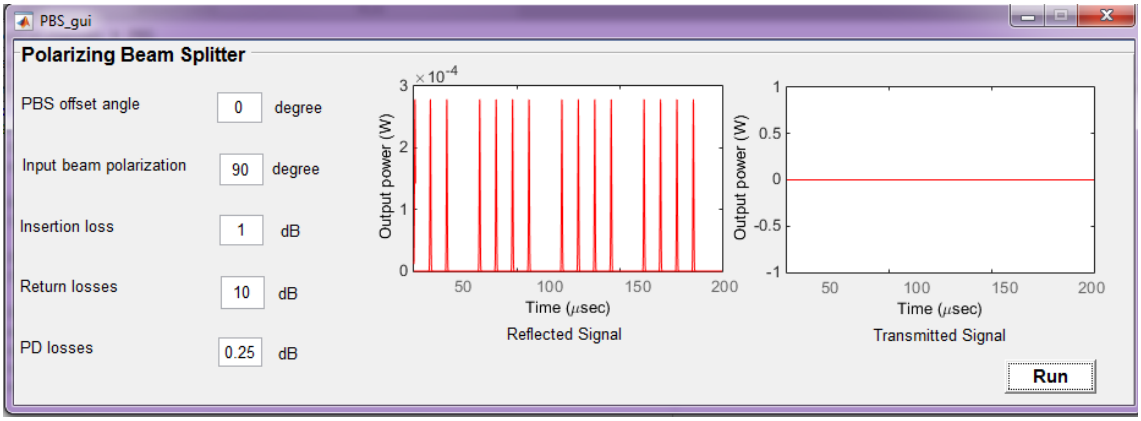


Fig.4.16 PBS Test 1 result, γ_{PBS}=0°, $\alpha_{inc.}$=90°

Figure (4.17) illustrates **Test 2** result to simulate the operation of the PBS designed with same γ_{PBS} and losses values as **Test 1**. Assume the incident light beam is horizontally polarized (i.e., $\alpha_{inc.}$=0°). This figure illustrates how the purely P polarized (i.e., horizontally polarized) incident optical beam will completely transmitted through the PBS because of the transmission axis is parallel with the polarization of the incident optical beam.

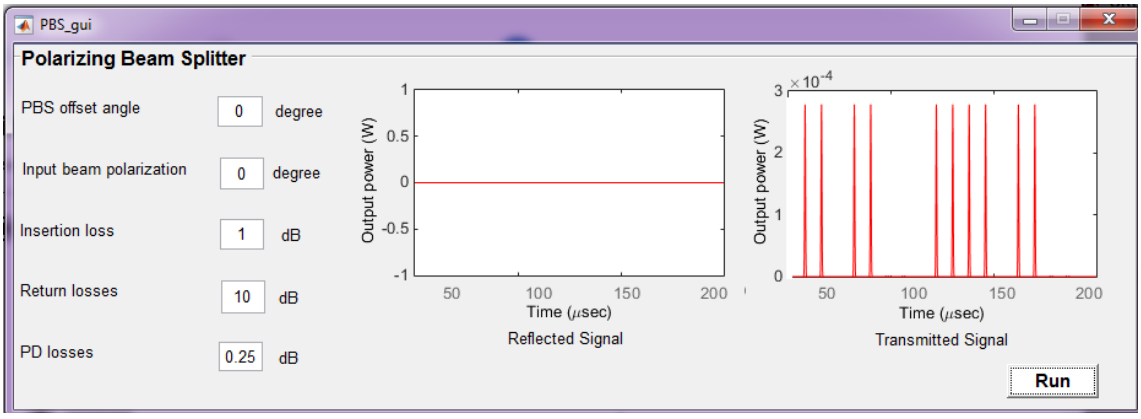


Fig.4.17 PBS Test 2 result, γ_{PBS}=0°, $\alpha_{inc.}$=0°

Figure (4.18) illustrates **Test 3** result to simulate the operation of the PBS with γ_{PBS}=0. Assume the incident light beam is linearly polarized with $\alpha_{inc.}$ =45°. It can be seen that the power of the incident optical beam is equally divided between output ports because of both S and P components will appear at the outputs of PBS as reflected and transmitted signals respectively.

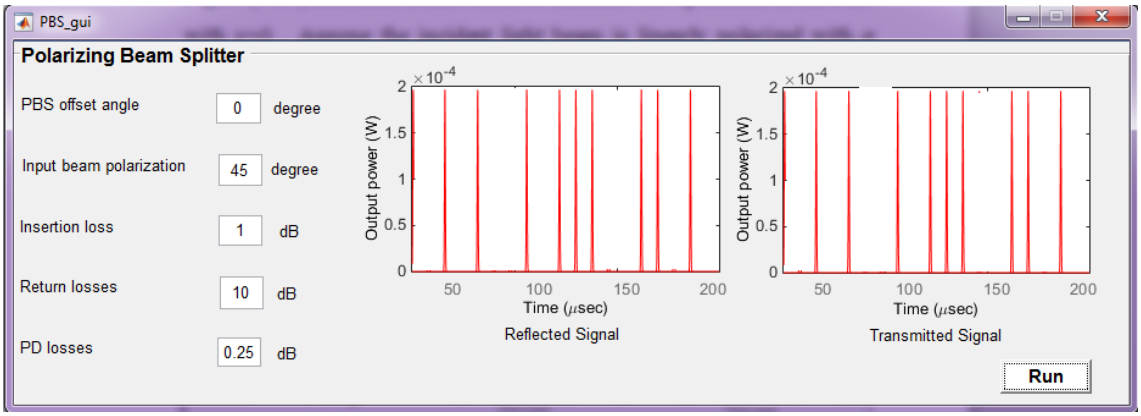


Fig.4.18 PBS Test 3 result, γ_{PBS}=0°, $\alpha_{inc.}$=45°

Figure (4.19) illustrates **Test 4** result to simulate the operation of the PBS when its transmission axis is rotated by 90° (i.e., γ_{PBS}=90°). Assume the incident light beam is horizontally polarized (i.e., $\alpha_{inc.}$=0°). It is clear from this test for minimum transmission through PBS; the transmission axis of the PBS should be orthogonal with the polarization of the incident light. Finally, this model can support any inputs from the user to study the performance of this component under different conditions.

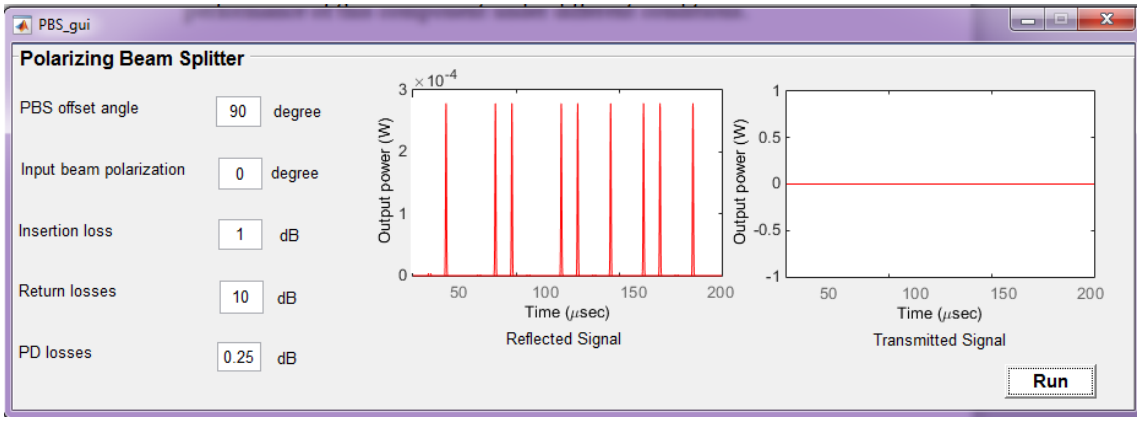


Fig.4.19 PBS Test 4 result, γ_{PBS}=90°, $\alpha_{inc.}$=0°

4.4 Single-Photon Detectors

This section outlines the methodology used to model the most important and emerging SPD technologies, SPAD and SNSPD. It gives a vision to the operation basics of these components, the concepts and the mathematical models that have been used. Final GUI for both types will be presented and discussed at the end of this chapter.

Single photon detection concept is the most crucial and often difficult factor that determines the performance of QKD systems. Thus, special detectors such as SPD are required to perform this task. SPD is a complex system because there is no direct method to decide the performance limits and how to design their interior structure [60]. Moreover, there are a lot of theoretical studies and simulation based works for operation and internal processes of SPD but without connection to the application field and experiment external conditions [61]. To facilitate understanding this concept, a virtual environment for modeling, analyzing and investigating the performance of SPD becomes necessary.

In this work, simulators for both SPAD and SNSPD used in the QKD systems are designed. The SPAD simulator model is intended for examination of parameters and characteristics of SPAD operating in Geiger mode used to detect low level optical signals taking into account the effect of the temperature and the excess voltage on the detector efficiency, dark counts and afterpulsing. On the other hand, the SNSPD simulator model aims to examine of parameters and characteristics of SNSPD in terms of pulse analysis, the impact of biasing current and the temperature on the dark counts rate and single photon-detection efficiency. In contrast to the recently created simulators that concentrate on the theoretical investigations, this work aims to get the simulated information generated and detected by real and commercially available physical components.

The first step in modeling was to review the functionality, operation and the performance characteristics for both SPD types using different standard references. The information provided from the first step was used in the second modeling step to build the conceptual models. In addition to the mathematical models, the conceptual models will be utilized to code the SPD models using Matlab.

4.4.1 Single-photon avalanche detector

This sub-section covers the operation basics, the methodology, the conceptual and the mathematical models that have been utilized to model the SPAD in addition to the main simulation results that are acquired through this research part. Finally, SPAD simulator is tested for many cases results.

4.4.1.1 The Device description

SPADs are class of semiconductor devices based on a p-n junction reverse biased above breakdown voltage (V_b) by the excess voltage (V_{ex}) resulting in large electric field in the depletion region. This makes SPAD's suitable for photon counting in the Geiger mode. In this mode, a single photon can generate an avalanche current pulse in the mA range which leads to discharge the SPAD from its reverse voltage to a voltage less than V_b [61, 64]. The generated current continues to flow until avalanche is quenched, i.e., lowering the bias voltage to a voltage equal to or less than V_b .

In order to be able to detect the arrival of another voltage the bias voltage must be restored [52]. The need of quenching with the APD is considered as the main disadvantage of using APDs in photon detection [62]. There are two methods for performing quenching,

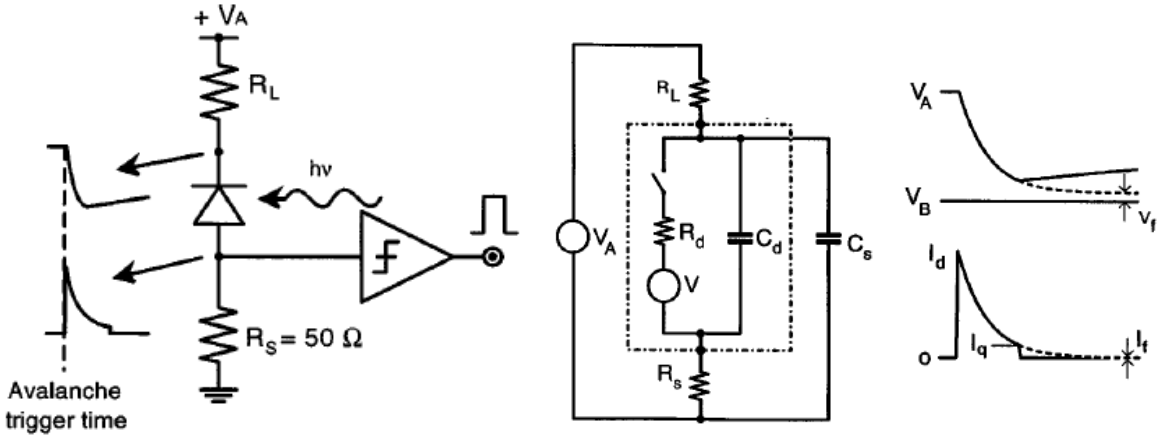
1. Passive quenching – a large resistor is placed in series with the diode, as the avalanche current begins to flow, the bias voltage across the diode drops to less than or equal to V_b. This is the technique used in this research work.
2. Active quenching- in this type of quenching the voltage is actively forced to be decreased below V_b when avalanche is triggered by a photon and the voltage is restored to its normal value in a short time in the range of tens of nanoseconds. Active quenching increases the

maximum counting rate of the APD. The difficulty with active quenching is the need of high – speed electronics.

The time required to quench the avalanche is called the quenching time constant [64, 63],

$$T_q = (C_j + C_s)\, R_d \qquad (4.19)$$

Where C_j is the junction capacitance, C_s is the stray capacitance and R_d is the diode resistance. The simplest quenching circuit that has been used in this work is called passive quenching circuit which is reported for Perkin Elmer C30921S silicon avalanche photodiode [64, 63] as shown in Figure (4.20).



(a) **(b)**

Fig. 4.20 a) SPAD passive quenching circuit b) SPAD equivalent circuit [63]

The quenching circuit consists of high value quenching resistor R_L in series with the cathode of SPAD, so it will stop the self –sustaining avalanche current. The avalanche current discharges the total capacitance made up by the sum of C_j and C_s and induces the voltage drop over R_L. The operation cycle is completed by the reset of the excess voltage to its initial value when the capacitance recharge to V_a with recovery time constant given by [64, 63],

$$T_r = (C_j + C_s)\, R_L \qquad (4.20)$$

So, the output of the detector is a current pulse with constant peak value given by [64],

$$i_{(t)} = (V_a - V_b)/R_L \quad (4.21)$$

Where $(V_a - V_b)$ is the excess voltage above the breakdown voltage.

The current exponentially decreases to the steady state level I_f with a corresponding voltage values V_f given by [64, 63],

$$I_f = \frac{V_a - V_b}{R_d + R_L} \quad (4.22)$$

$$V_f = V_B + R_d I_f \quad (4.23)$$

The leading edge of the output pulse indicates the arrival time of the photon. The detector is insensitive to any photons arriving in the time between the start of the avalanche and the voltage biasing reset. This period is called the dead time (τ_d) of SPAD which is approximately equal to the 0.5 T_r [52].

SPADs operating in Geiger mode are characterized by number of basic performance parameters. The following points describe these parameters,

1. Single photon-detection efficiency

$SPDE$ can be defined as the probability that an incident photon triggers an avalanche (true detection) [65]. $SPDE$ (η_{SPDE}) can be obtained by [65],

$$\eta_{SPDE} = \eta P_{av} \quad (4.24)$$

Where η is the quantum efficiency and P_{av} is the avalanche triggering probability which has a direct relation to the V_{ex}. P_{av} can be defined as the probability that a primary electron-hole pair initiates a self–sustaining avalanche process which can be approximated by the [65],

$$P_{av} = 1 - e^{-(\frac{V_{ex}}{V_c})} \tag{4.25}$$

Where the characteristic voltage V_c depends on the depletion layer thickness and on the weighted average of the ratio of the ionization coefficient of electrons to that of holes [65].On the other hand, η depends upon the photodetector structure and the presence of a properly designed antireflection coating [65]. It can be defined by [66],

$$\eta = P_{abs}P_{transit} \tag{4.26}$$

Where P_{abs} is the absorption efficiency of the photodetector, $P_{transit}$ is the transit probability which depends on the material of the absorption region and the device architecture. Figure (4.21) illustrates the dependency of η_{SPDE} on V_{ex}.

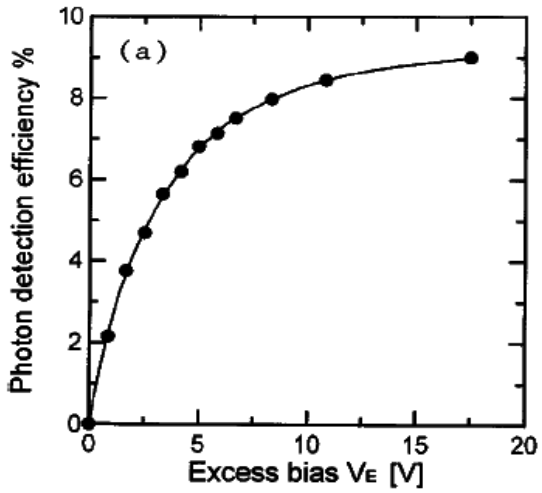


Fig.4.21 $SPDE$ vs V_{ex} [52]

2. Dark count probability

Dark count is due to carriers thermally generated within the SPAD junction. DCP increases with temperature with Poissionian fluctuations act as internal noise source of the detector. Furthermore, DCP also increases with the V_{ex} as shown in Figure (4.22) due to avalanche triggering

probability which also increases detection efficiency but at the expense of the field enhancement of the carrier generation rate [67].

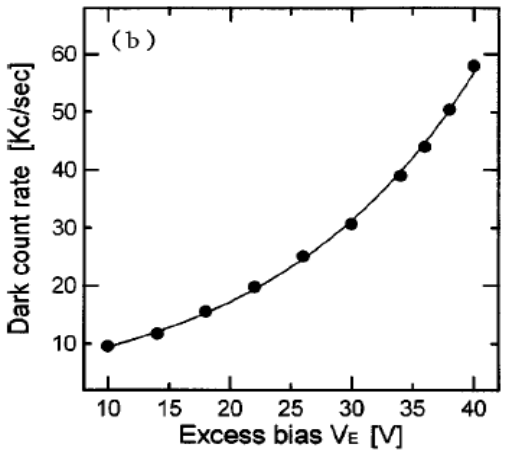


Fig.4.22 Dark count rate vs V_{ex} at room temperature [52]

The number of primary dark pulses due to thermally generated carriers within the SPAD junction can be represented by [68, 69],

$$N_{PD1}=I_{DM}\frac{\tau'}{q} \tag{4.27}$$

Where I_{DM} is the primary dark current, τ' is the gate pulse width, and q is the charge of an electron. The second source for primary dark carriers is through a series of impact ionization with an average DC gain (M_o). Such dark carriers number can be defined as [68, 69],

$$N_{PD2}=I_{DM}M_o\frac{\tau_{tr}}{q} \tag{4.28}$$

Where τ_{tr} is the effective transit time. In contrast, a secondary dark pulses can be generated by afterpulsing effect when few carriers may be trapped from deep levels located at intermediate energies between mid-gap and band edge during each avalanche pulse and subsequently released. These released carriers can trigger the avalanche, thereby generating afterpulses correlated in time to the original avalanche triggered by the photon [65]. The number of these released dark carriers may be written as [68, 69],

$$N_{SD1}=DCPN_{tr}\frac{e^{\left(\frac{t'}{\tau_{de}}\right)}-1}{e^{\left(\frac{\Delta T}{\tau_{de}}\right)}-1} \tag{4.29}$$

Where ΔT is the reciprocal of PRR, τ_{de} is the detrap time constant. Secondary dark carriers can also be generated because of some releasing carriers from the traps can be possible to stay in the multiplication region when arriving the pulse. Thus, the contribution of this type can be written as [68, 69],

$$N_{SD2}=DCPN_{tr}\frac{e^{\left(\frac{\tau_{tr}}{\tau_{de}}\right)}-1}{e^{\left(\frac{\Delta T}{\tau_{de}}\right)}-1} \tag{4.30}$$

By adding these dark counts sources, the total number of dark carriers per pulse can be defined as [66, 69],

$$DCP=1-exp\{-P_{av}[\frac{I_{DM}t}{q}+\frac{I_{DM}Mo^2}{2\pi qGB}+DCPN_{tr}\frac{e^{\left(\frac{t'}{\tau_{de}}\right)}-1}{e^{\left(\frac{\Delta T}{\tau_{de}}\right)}-1}+DCPN_{tr}\frac{e^{\left(\frac{\tau_{tr}}{\tau_{de}}\right)}-1}{e^{\left(\frac{\Delta T}{\tau_{de}}\right)}-1}]\} \tag{4.31}$$

Where GB is the gain–bandwidth product of the SPAD and N_{tr} is the average number of carriers trapped after a current pulse.

Accordingly, $SPDE$ can be calculated as [66, 69],

$$\eta_{SPDE}=P_{on}-\frac{DCP}{P_{ph}} \tag{4.32}$$

Where P_{ph} is the probability of whether an incident optical pulse contains any photons or not which can be given by 1-$e^{(-N_o)}$ with the average number of incident photons per pulse is N_o. P_{on} is the probability of a current pulse be generated due to photon or dark carrier when the source is ON. It is given by [66, 69],

$$P_{on}=1-exp\{-P_{av}[\frac{I_{DM}t}{q}+\frac{I_{DM}Mo^2}{2\pi qGB}+P_{on}N_{tr}\frac{e^{\left(\frac{\tau}{\tau_{de}}\right)}-1}{e^{\left(\frac{\Delta T}{\tau_{de}}\right)}-1}+P_{on}N_{tr}\frac{e^{\left(\frac{\tau_{tr}}{\tau_{de}}\right)}-1}{e^{\left(\frac{\Delta T}{\tau_{de}}\right)}-1}+\eta N_o]\}$$ (4.33)

4.4.1.2 Single-photon avalanche detector conceptual model

SPAD is an optical-electrical component with one input port and one output port as shown in the corresponding conceptual model of Figure (4.23).

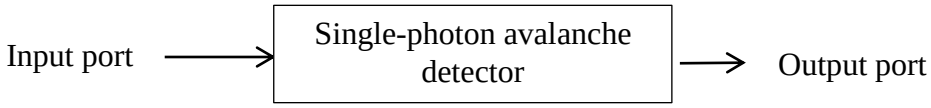


Fig.4.23 SPAD's conceptual model

From the conceptual model diagram, the incoming highly attenuated laser pulses encoded with a specific polarization will be detected and a corresponding avalanche pulses will be generated by correct detections with a number related to the detector efficiency. Dark counts will be generated randomly in time and amplitude with a rate depending on the value of V_{ex} and temperature provided by the user.

The following parameters were considered as inputs to the simulation model, optical pulse time profile with linear polarization as defined in Eq.(2.15) with P_{peak} in (mW), transmitted optical λ in nm, the orientation of the incoming optical pulse, η_{SPDE}, V_{ex}, temperature, dark counts and afterpulsing occurrence probabilities.

4.4.1.3 SPAD simulation results and discussion

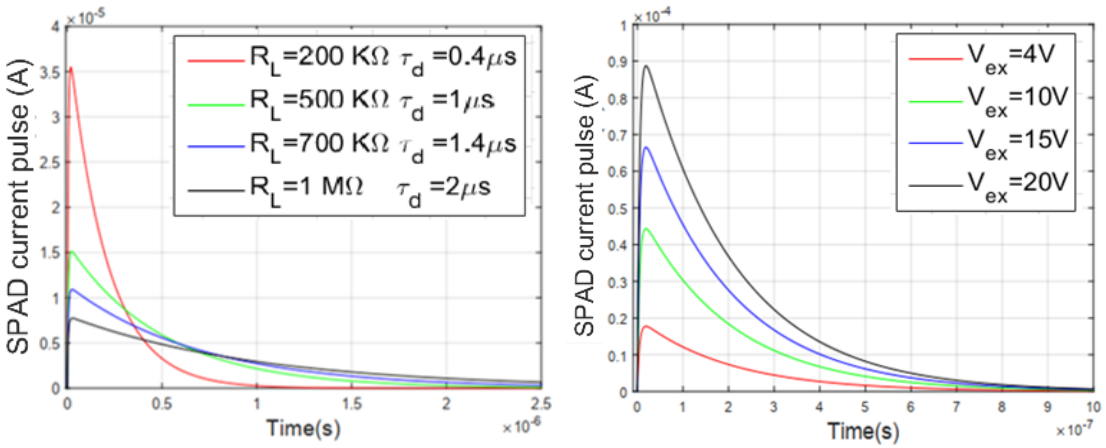
The approach that has been used for model verification was by running the model under different conditions by applying inputs and checking the outcomes to show how the model is programmed in a sufficient and correct way.

To validate SPAD model, the simulated results that belongs to the avalanche pulse analysis is compared to the results acquired for C30921S by the help of its data sheet to define the allowed input and output limits in addition to the desired specifications. While, the simulated SPAD performance parameters results are compared to the valid simulation models presented in [66, 69]. This method was used in this work because basically the modeled SPAD tool is not intended to simulate any real SPAD device but to evaluate the capabilities of the modeled SPAD tool presented in this research. In general, the validation of modeled SPAD modeling tool was proved via sequence of test cases under different operation conditions and with different input parameters as will be presented.

Based on theoretical studies and mathematical models of SPAD circuit design and physical properties that governs its performance explained in Section 4.4.1.1, a simulator is developed to model the SPAD that allows users to relate the SPAD internal structure to its performance. In this section, the avalanche pulse analysis, the impact of V_{ex} on avalanche and dark counts probability, the effect of PRR on the afterpulses rate, the influence of primary dark current, temperature and average DC gain on the $SPDE$ and DCP are presented. Finally, these results are used as the basis for the design of the SPAD modeling simulator to visualize the detection process in addition to the random distribution of DCR to estimate the whole SPAD performance.

In this model, C30921S is chosen because of its wide spread use in the QKD systems. This SPAD type has high quantum efficiency equal to 77% at 830nm and to 60% at 900nm. It can be operated in Geiger mode with low dark count rate (DCR) equal to 350/second at -25°C [Appendix 2].

In the passive quenching circuit assumed for the SPAD model, a load resistor R_L= 200 kΩ is connected in series with the photodetector and R_s=200Ω. In order to simulate the avalanche current pulse on R_s, it is important to consider the internal stray and junction capacitors to accurately determine T_r and τ_d of the output pulse. C_j and C_s are assumed to be 1pf and 3pf respectively as recommended by [63, 64]. To study the effect of $R_L$on the output current amplitude and then on the quenching time, Figure (4.24a) represents the output pulse with different R_L values. As R_L increases, the output current tends to be low with long quenching time constant which as a result limits the quenching speed and hence reduce the count rate. It can be seen from this figure the dead time is not fixed and can be varied according to the value of R_L which changes T_r and C_j. Figure (4.24b) shows the impact of increasing V_{ex} on the SPAD output current. As V_{ex} increases, the probability to trigger an avalanche increases too which as a result leads to an increase in the output peak current.



(a) **(b)**

Fig.4.24 Simulated avalanche current pulse at a) various R_L values. b) Different V_{ex} values

To check the correctness of the simulated avalanche SPAD current signal for validation purpose, it will be compared to the real avalanche pulse generated by C30921S as presented in Figure (4.25) in terms of overall pulse waveform, rise and fall time and τ_d as shown in Table (4.1).

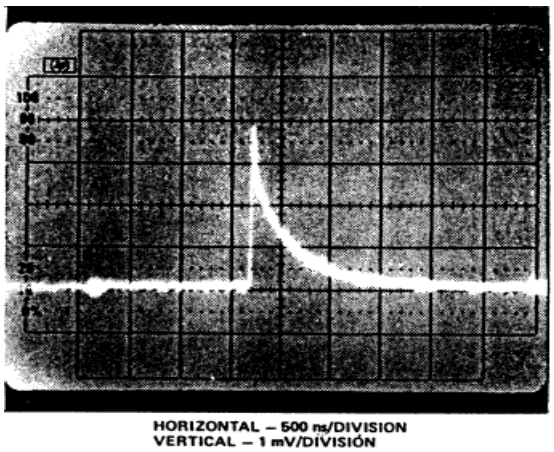


Fig.4.25 C30921S silicon avalanche photodiode avalanche pulse [Appendix 2]

Table 4.4 A comparison between C30921S silicon avalanche photodiode and the SPAD model

Properties	C30921S	Modeled SPAD
Rise time	≅ 0.5ns	≅ 0.5ns
Fall time	≅0.5ns	≅0.5ns
τ_d	≅ 0.3μs @ R_L=200 kΩ	≅ 0.4μs @ R_L=200 kΩ

By comparison, a good agreement between the simulation and the measured results is obtained in terms of the previously mentioned parameters.

The dependence of P_{av} on the V_{ex} is illustrated in Figure (4.26). The number of thermally or optically generated carriers in the multiplication region exponentially increased with V_{ex}. Thus, a chain of ionizations can be obtained and continuously increase till the photodetector is discharged. Hence, the probability of this process to occur is called P_{av}.

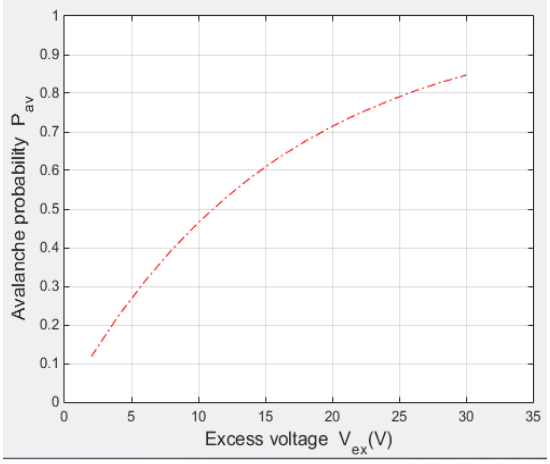


Fig.4.26 Avalanche probability (P_{av}) vs. Excess voltage

In this work, V_{ex} range is between 2V-30V while the characteristic voltage equals to 16V as reported in C30921S specifications. As a final result to the avalanche pulse analysis, Figure (4.27) shows the direct dependence of SPAD current on the V_{ex}.

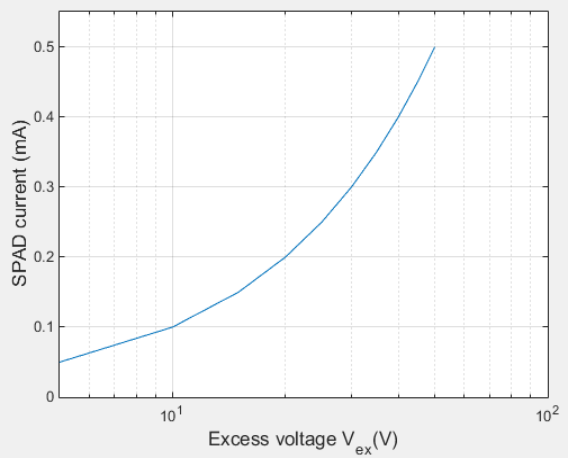
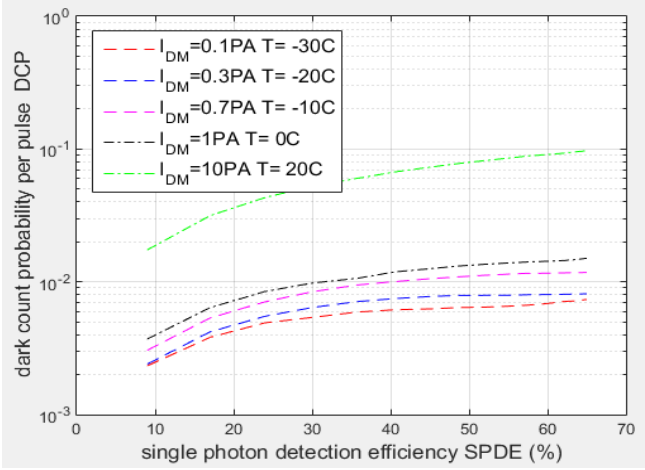


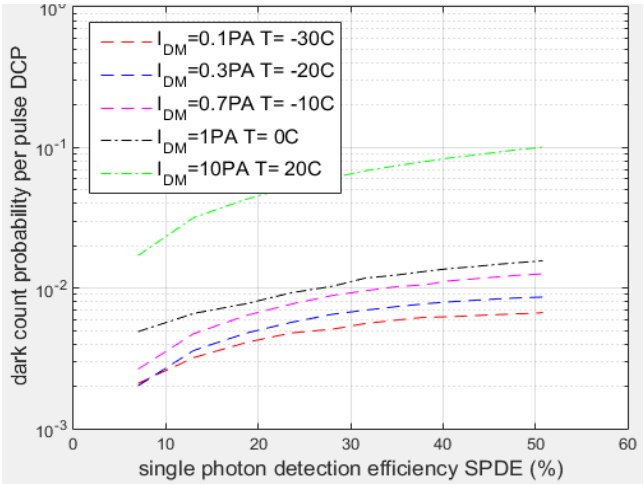
Fig.4.27 SPAD current vs. Excess voltage (V_{ex})

To quantify the performance of SPAD, different terms have to be assessed for optimal characterization and design. First of all, in this research only 830nm and 900nm are examined because of the specific SPAD under study shows maximum detection efficiency at these wavelengths. Figure (4.28) shows how the primary dark current and temperature conditions can enhance or reduce DCP against $SPDE$ for wavelengths, 830nm and 900nm. One can find that the acceptable range for DCP per pulse could be achieved by cooling the system down to -30℃. As the temperature increases, DCP increases too because of the increase in the

number of thermally generated carriers in a random manner or from the type of photodetector fabrication material which leads to tunneling effect. In contrast, the temperature also has a direct influence on $SPDE$ by the fact that as the temperature increases, V_b is forced to increase too. Thus, it is mandatory to work above V_b by the amount of V_{ex} to operate in a Gieger mode. As a result, P_a will be enhanced which in turn the DCP increase and causes a remarkable degradation in $SPDE$. It can be seen from Figure (4.28) that the DCPcan be enhanced with increasing the primary dark current.



(a)

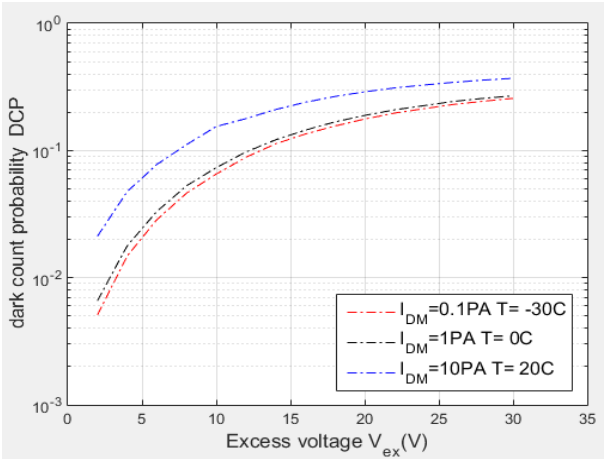


.

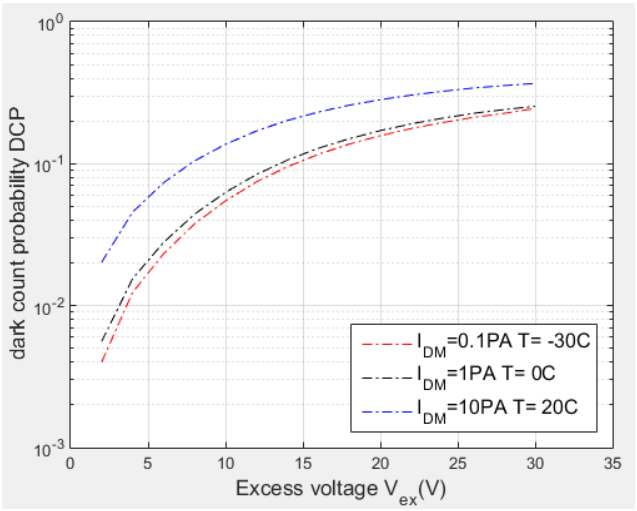
(b)

Fig.4.28 Dark count probability (DCP) vs. $SPDE$
a: λ=830nm b:λ=900nm

Figure (4.29) illustrates the effect of V_{ex} on the DCP of the SPAD model for different temperatures and I_{DM} values for both λ=830nm and λ=900nm.



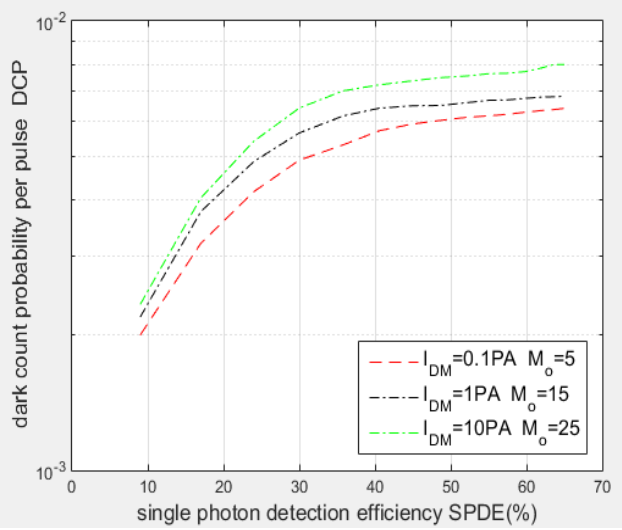
(a)



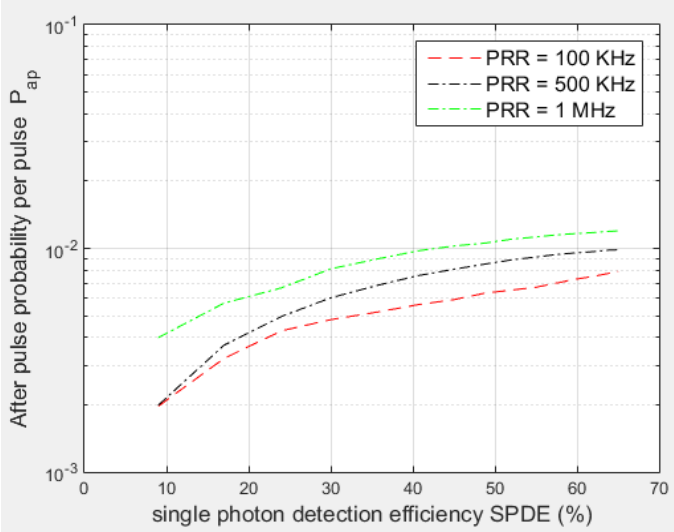
(b)

Fig.4.29 Dark count probability (DCP) vs. Excess voltage (V_{ex})
a: λ=830nm b:λ=900nm

The effect of M_o of the photodetector on the DCP and hence on the performance of the device can be investigated from Figure (4.30). It is clear from this figure that the value of DCP increases as M_o becomes higher. This is because the thermally generated dark carriers that enter the multiplication region pass through a set of impact ionizations with M_o.



(a)



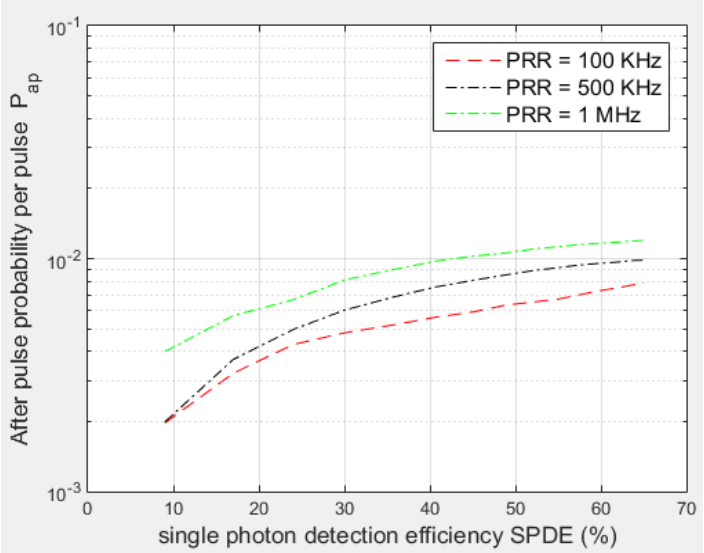
(b)

Fig.4.30 Dark count probability (DCP) vs. $SPDE$ with different M_o values a:λ=830nm b:λ=900nm

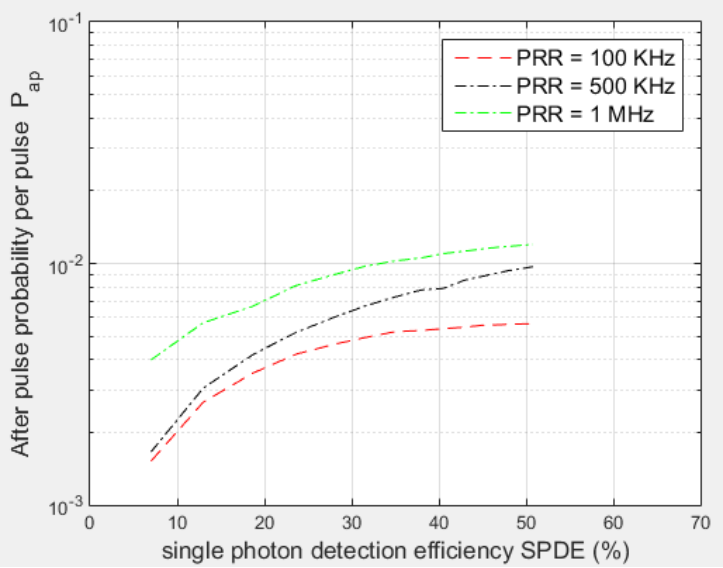
At this point, in order to achieve better performance for ASPD in terms of high photon detection efficiency or low DCP, low M_o and primary dark current are preferable. It is important to mention that the approach used to simulate DCP and P_{on} depends upon the fixed point iteration method to numerically solve these terms in Equations (4.38) and (4.40). In addition, P_{av} was used as a variable parameter to simulate both DCP and $SPDE$.

The afterpulse probability (P_{ap}) behavior can be examined for different PRR's. From Figure (4.31), the contribution of P_{ap} to the total

counts rate could be reasonable for low PRR (e.g. in the range of 10^{-3} per pulse) which can be understood as follows: as long as $\frac{1}{PRR} \gg \tau_d$, this condition ensures long hold off time (i.e., the time required by the SPAD to be insensitive to the incident photons and remains quenched [66]) which as a result makes the trapped carriers emitted before the arrival of the next pulse and thus this reduces the value of afterpulsing.



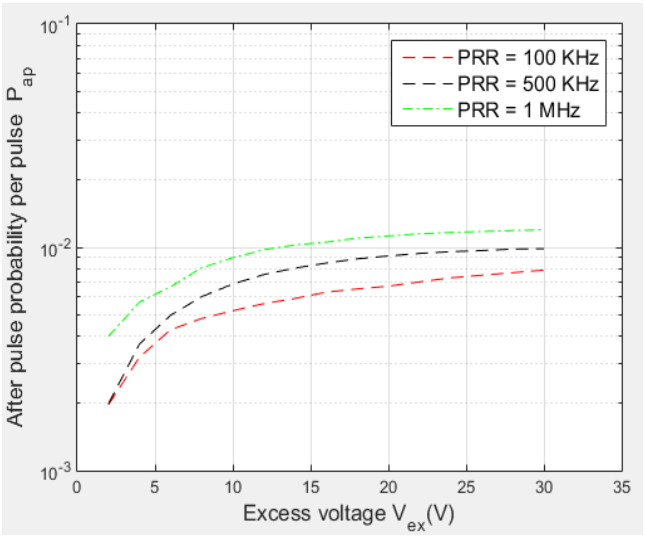
(a)



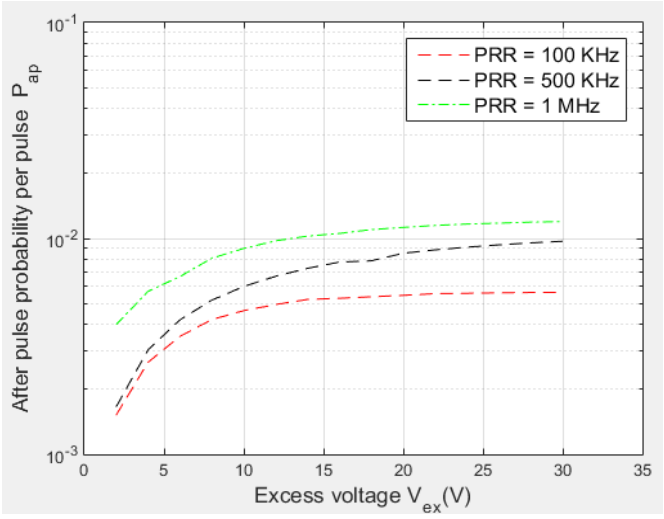
(b)

Fig.4.31 Afterpulse probability (P_{ap}) vs. $SPDE$ for different PRR
a: λ=830nm b:λ=900nm

The impact of V_{ex} on the P_{ap} is shown in Figure (4.32). It is clear that P_{ap} increases as the avalanche probability increases with V_{ex}. P_{ap} can be decreased by reducing V_{ex} but at the expense of worse $SPDE$. As a result some factors have to be considered to reduce P_{ap}, operating with lower PRR but this will be at the expense of operating at high count rate and hence low final key rate can be achieved in QKD systems. The other factor is by using longer τ_d, increasing the temperature conditions but in this case DCR will be enhanced. Finally, reducing the excess voltage above the breakdown voltage but at the expense of $SPDE$.



(a)



(b)

Fig.4.32 Afterpulse probability (P_{ap}) vs. Excess voltage (V_{ex}) for different PRR a: λ=830nm b:λ=900nm

To check the correctness of the SPAD performance simulation results, it will be compared to the results reported in [66, 69] in terms of DCP and P_{ap} ccontribution percentage to the total dark counts as a function of $SPDE$ at different I_{DM}, temperatures and PRR as shown in Tables (4.2) and (4.3).

Table 4.5 A comparison between a model reported in [69] and the SPAD model in terms of DCP as a function of $SPDE$ at different I_{DM}

	Y. Kang et al, model [69]			Modeled SPAD		
$SPDE$ (%)	DCP at I_{DM} = 0.1pA	DCP at I_{DM}= 1pA	DCP at I_{DM} = 10pA	DCP at I_{DM} = 0.1 pA	DCPat I_{DM} =1pA	DCP at I_{DM} =10pA
9	1×10^{-4}	1×10^{-3}	1×10^{-2}	0.2×10^{-4}	3.7×10^{-3}	174×10^{-2}
17	2.5×10^{-4}	2×10^{-3}	2.5×10^{-2}	0.3×10^{-4}	6.3×10^{-3}	315×10^{-2}
24	4×10^{-4}	3.5×10^{-3}	3.7×10^{-2}	0.5×10^{-4}	8.4×10^{-3}	431×10^{-2}
30	5×10^{-4}	4.5×10^{-3}	5.1×10^{-2}	0.53×10^{-4}	9.7×10^{-3}	526×10^{-2}
36	6.5×10^{-4}	6.3×10^{-3}	6×10^{-2}	0.59×10^{-4}	10.6×10^{-3}	602×10^{-2}
40	7×10^{-4}	8×10^{-3}	8.5×10^{-2}	0.61×10^{-4}	11.8×10^{-3}	672×10^{-2}

Table 4.6 A comparison between a model reported in [66] and the SPAD model in terms of DCP as a function of $SPDE$ at different temperatures

	Ahammed Mofasser et al, model [66]			Modeled SPAD		
$SPDE$ (%)	DCP at T=−30℃	DCP at T =0℃	DCP at T=20℃	DCP at T=−30℃	DCP at T=0℃	DCP at T=20℃
9	0.5×10^{-6}	2×10^{-6}	1.5×10^{-5}	0.23×10^{-4}	0.37×10^{-4}	1.74×10^{-4}
17	0.9×10^{-6}	4×10^{-6}	2×10^{-5}	0.38×10^{-4}	0.63×10^{-4}	3.15×10^{-4}
24	1×10^{-6}	5×10^{-6}	3×10^{-5}	0.5×10^{-4}	0.84×10^{-4}	4.31×10^{-4}
30	1.5×10^{-6}	6×10^{-6}	3.5×10^{-5}	0.53×10^{-4}	0.97×10^{-4}	5.26×10^{-4}
36	1.8×10^{-6}	7×10^{-6}	4×10^{-5}	0.59×10^{-4}	1.06×10^{-4}	6.02×10^{-4}
40	2×10^{-6}	9×10^{-6}	4.3×10^{-5}	0.61×10^{-4}	1.18×10^{-4}	6.72×10^{-4}
45	2.5×10^{-6}	1×10^{-5}	5×10^{-5}	0.62×10^{-4}	1.25×10^{-4}	7.3×10^{-4}

The difference between the modeled SPAD results and the results presented in the analytical simulation models are due to the measurement conditions that have been used in the SPAD model calculations such as the average optical power, λ, and η that were extracted from C30921S data sheet are different from the simulation parameters reported in [66, 69]. Furthermore, DCP, P_{ap} and $SPDE$ that were calculated by unconventional approach which is the fixed point iteration method and hence the expected results have approximated values due to iterative inaccuracy. In addition, the main target of this modeling effort is to examine the general functionality of the SPAD behavior and its performance under different operation conditions. Thus, it is possible to say that the presented results accuracy are within the reasonable range which is the amount of accuracy required for the model's intended purpose.

4.4.1.4 SPAD simulator implementation and testing

This section describes the SPAD simulator in addition to the testing cases to prove the simulator capability for SPAD behavior verification by comparisons of the simulator results with the mathematical models based data. The simulator can support wide spectral range starting from 500nm up to 1000nm which represents the allowable spectral range for C30921S. In addition, the user can change both V_{ex} and temperature at the same time to investigate the overall SPAD performance parameters: $SPDE$, DCP and P_{ap}. Depending on the user inputs, the simulator plots the resultant SPAD avalanche pulses in accordance to the incoming optical laser pulses taking into consideration the $SPDE$ to decide if the pulse is detected or not as well as DCP and P_{ap}.

Four tests were applied to verify the simulator capabilities to simulate the SPAD operation and to prove its operation validity. For all four tests, 25 input pulses to the SPAD were linearly polarized with P_{peak} gradually attenuated from 1mW to get the desired level and PRR=1GHz. The results are presented for N_0=0.2. For the main GUI illustrated in Figure (4.33), the plotter to the left represents the incoming laser pulses with defined PRR and N_0. The plotter to the right illustrates the output avalanche pulses comprising the true photon detection and false avalanche detections due to dark and afterpulse detections

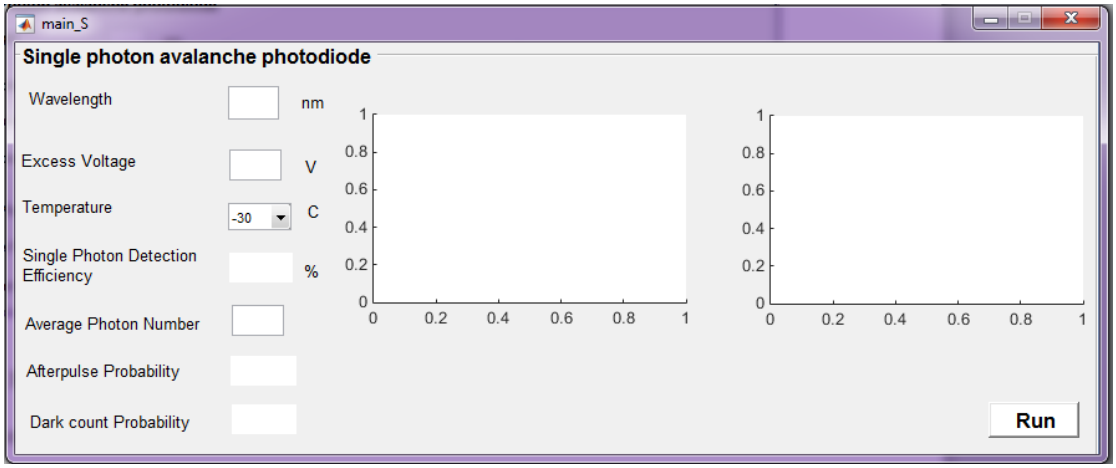


Fig.4.33 Simulator main window

Test 1: V_{ex} is set to 2V and the temperature is set to $-30℃$. According to these inputs, the calculated $SPDE$ was 9%. Therefore, the expected detected optical pulses were 3 pulses out of 25 incoming laser pulses. Figure (4.34) illustrates that there are 3 true photon detection pulses in red which are equal to the expected detected pulses. Pulses in turquoise represent the output avalanche detections due to thermal effects with the number equal to the calculated DCP which is 0.0023. On the other hand, pulses in black illustrate the false detections due to afterpulse effect contribution with the number equal to the calculated P_{ap} which is 0.0019.

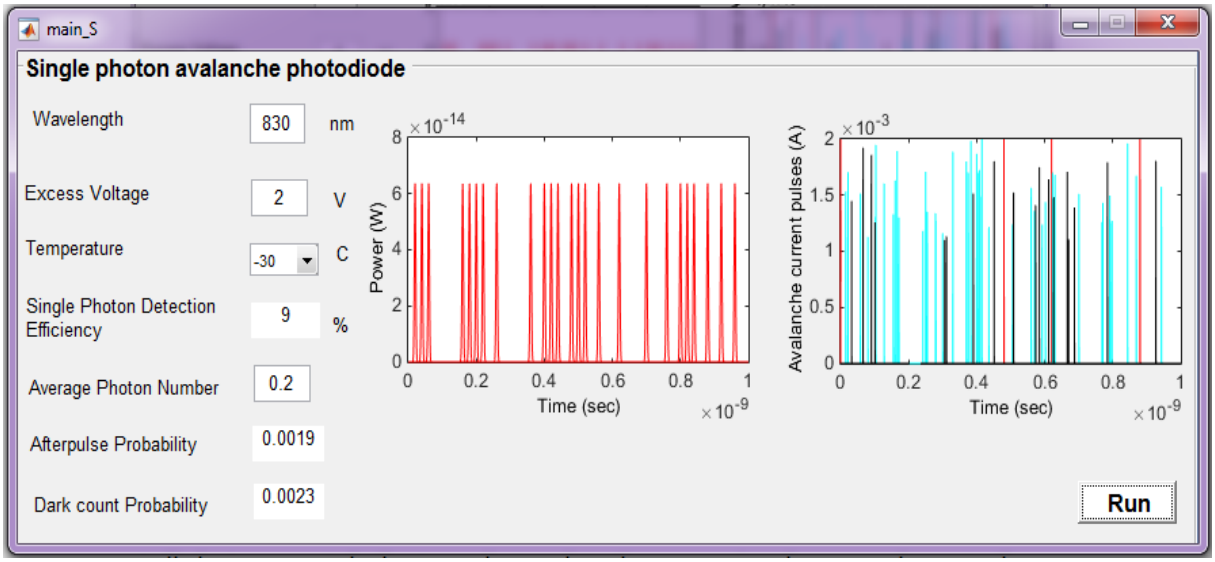


Fig.4.34 Test1 simulation results for: N_0= 0.2, V_{ex}=2V and T=−30℃.

Test 2: V_{ex} is set to 2V and the temperature is increased and set to −20℃ as shown in Figure (4.35). In this test the impact of the temperature on the DCP will be studied. As expected, the true photon detections were 3 pulses accordance to the registered $SPDE$. DCP is increased to 0.0024 in comparison to the previous test as the temperature increases. P_{ap} doesn't change with temperature, it depends on V_{ex} which has the same value as in Test 1.

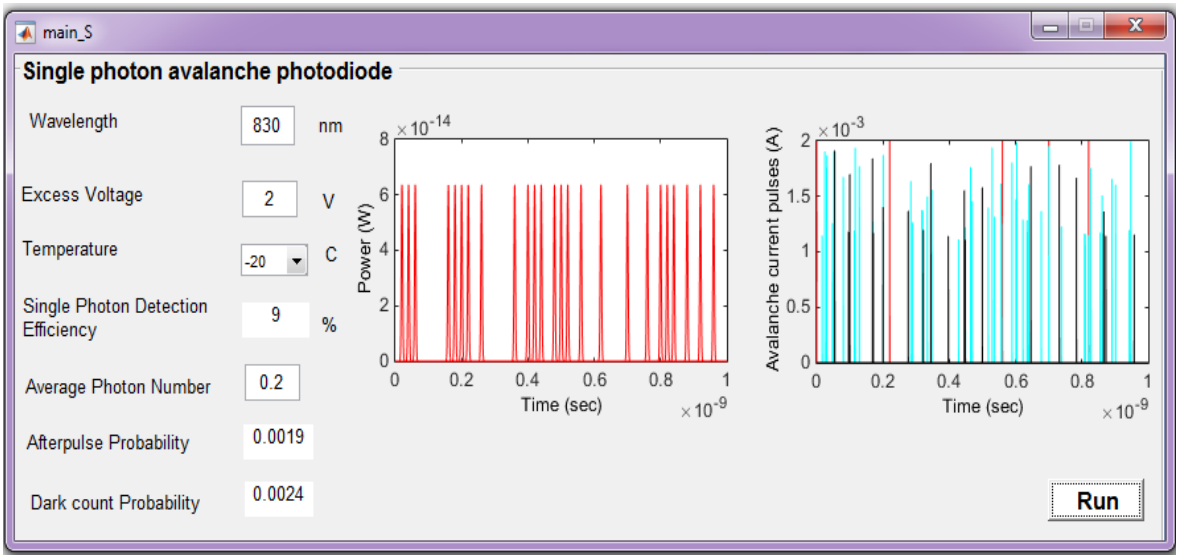


Fig.4.35 Test2 simulation results for:N_0= 0.2, V_{ex}=2V and T=−20℃

Test 3: V_{ex} is set to 10V and the temperature is set to $-30℃$. In this test the effect of increasing V_{ex} on the $SPDE$, DCP and P_{ap} and on the avalanche pulses amplitude will be presented. Figure (4.36) shows the simulator results for these input values. $SPDE$ is increased to 36% as V_{ex} increased. The expected number of true photon detections equals 9 pulses. The simulator result equals to the expected result (i.e. 9 pulses). DCP and P_{ap} increased to 0.0059 and 0.0052 respectively as V_{ex} increases due to the enhancement of the avalanche process probability which means an increases in the $SPDE$. The amplitude of true detection, dark and afterpulse increase as shown in the plotter.

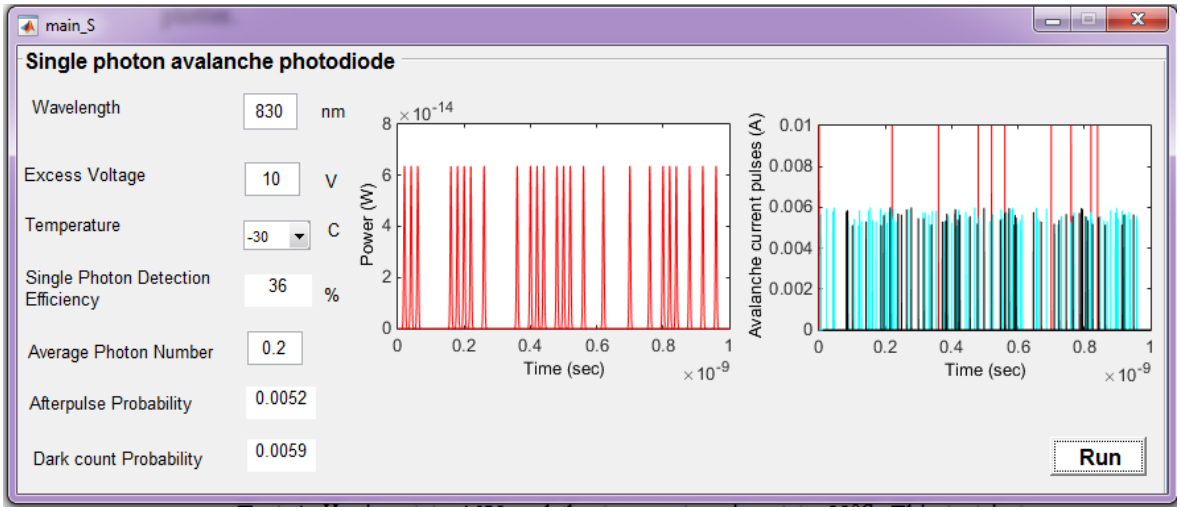


Fig.4.36 Test 3 simulation results for:N_0= 0.2, V_{ex}=10V and T=$-30℃$

Test 4: V_{ex} is set to 10V and the temperature is set to 22℃. This test is to investigate the effect of the temperature on the SPAD performance with an increase in V_{ex}. Figure (4.37) illustrates how the SPAD performance will be affected with temperature by the increase in the thermally generated pulses. DCP is increased to 0.0602 while P_{ap} still has the same value as the effect of the temperature on P_{ap} is not included in these tests. The calculated number of true photon detections equals 8 pulses which is approximately equal to the expected number.

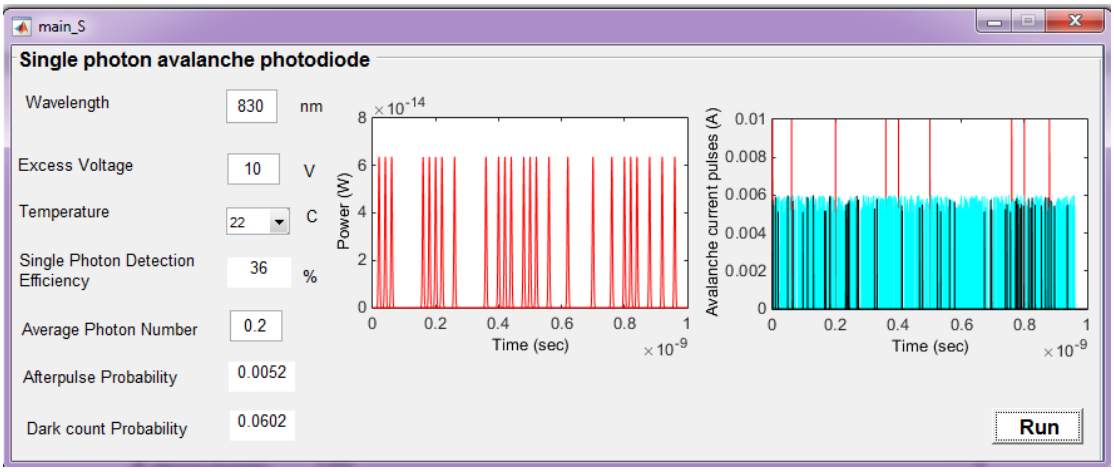


Fig.4.37 Test 4 simulation results for:N_0= 0.2, V_{ex}=10V and T=22℃

In general, by comparing the simulator tests results with the mathematical models results mentioned in the last section, one can find a good agreement which as a result confirms the simulator ability to examine the SPAD performance.

4.5 Superconducting Nanowire Single Photon Detector

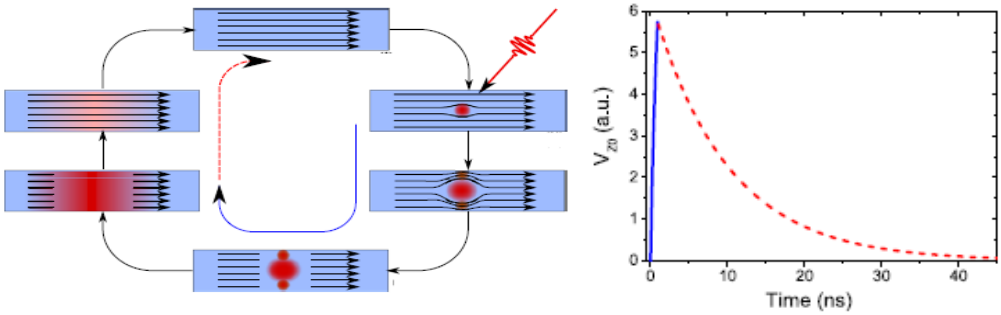
This section covers the operation basics, the methodology, the conceptual and the mathematical models that have been utilized to model the SNSPD in addition to the main simulation results that were acquired through this research part. Finally, SNSPD simulator test cases results will be illustrated.

4.5.1 The Device description

SNSPD with an illumination area for absorbing photons consists from meandering superconducting nanowire with a few nanometers thickness carrying a constant biasing current I_b less than the switching current and near to its critical current value [70]. When a photon is absorbed, a hotspot is generated due to the heat applied by the photon absorption process. As a result, I_b is forced to escape along the hotspot in the nanowire. This process leads to form a resistive barrier across the nanowire. This abrupt

increase in the nanowire resistance results in a measureable voltage signal which represents the detection of a single photon [71].

Figure (4.38) shows the SNSPD operation concept as well as the its generated output voltage signal.Compared to different types of single photon detectors, SNSPD provides an improved detection efficiency, dark counts, timing and energy resolution. All these features have made it the perfect choice for quantum security and communication [71].



(a) **(b)**

Fig.4.38 (a) SNSPD operation principles (b) SNSPD output voltage signal [71]

The electrical circuit model of the SNSPD is shown in Figure (4.39). It consists of an inductor (L_k) which represents the kinetic inductance of the nanowire connected in series with a switch and R_n (t) in parallel. R_n (t) represents the hotspot resistance [71].

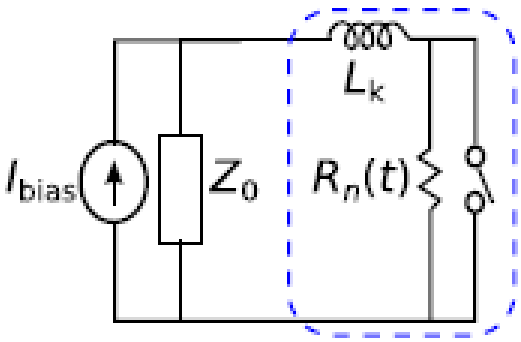


Fig.4.39 SNSPD electrical circuit mode

The resulting output voltage signal can be generated as follows: as the photon absorbed, a resistive bridge in the nanowire is formed. This step can be simulated as a temporary opening of the switch. This switch opening decreases the current through SNSPD but increases the output voltage with a time constant equal to [71, 72],

$$\tau_{rise} = \frac{L_k}{R_n(t)+Z_0} \tag{4.34}$$

Where Z_0 is the load resistor.

Conversely, when the switch is closed, a supercurrent with reverse direction will be recovered with a longer time constant equal to [71, 72],

$$\tau_{\text{fall}} = \frac{\text{L}_\text{k}}{\text{Z}_0} \tag{4.35}$$

For a defined period of time called the dead time, the SNSPD will be insensitive to the incoming photons and the supercurrent recovers to a re-triggerable value. The detector dead time (τ_{dt}) value equals to [71],

$$\tau_{dt} = \tau_{rise} + \tau_{fall} \tag{4.36}$$

The output of the SNSPD is a voltage pulse with a peak value given by [72],

$$v = \frac{Z_0 \times R_n}{Z_0 + R_n} I_b \tag{4.37}$$

SNSPDs are characterized by number of basic performance parameters, $SPDE$ and DCR. These parameters depend on some extrinsic (I_b, temperature and wavelength) and intrinsic (material chemistry, structure, electronic properties and geometry) specifications [73].

1. Dark count rate

DCR is a vital factor that affects the performance of SNSPD which increases exponentially due to detecting false pulses originated from random fluctuations as I_b approaches its critical value and working with high ambient temperature [70]. Shorter wavelengths are preferable for high

$SPDE$ requirements but at the expense of increasing the likelihood of detecting dark counts in addition to the correct detections [73].

This kind of pulses are contributing from pulses originating due to straying photons or fluctuation from superconducting to the normal state in the SNSPD as well as due to thermal fluctuations in I_b in addition to quantum fluctuations in the amplitude and phase of the superconducting order parameter. Electronics fluctuations can add some false pulses to the SNSPD output [73]. Refer to [73] for more information about the effect of intrinsic parameters on the DCR.

According to the unified model suggested in [74] with input light in a coherent state, the total count rate of the SNSPD at the absence of the light intensity is nothing but DCR. In this case when there is no photon absorbed by the meander line, no hotspot could be generated in this line and there is no chance to form a resistive barrier. This idea can be formulated as [74],

$$C_t = \frac{GT_0}{1+GT_0 \times \tau_{dt}} + PRR\left(1 - e^{(-GT \times t_{ex})}\right) \quad (4.38)$$

Where:

C_t : is the total count rate of the SNSPD.

GT_0: is the total barrier generation rate (total count rate) when the light source is turned off which can be determined experimentally by measuring the total count rate when the optical light intensity attenuated to zero Watts.

GT : is the average total resistive barrier generation rate.

t_{ex} : is the time that the excitation created by each laser pulse lasts on the meander line.

Now, when the light source intensity sets to zero [74],

$$C_t = DCR = \frac{GT_0}{1+GT_0 \times \tau_{dt}} \quad (4.39)$$

On the other hand, when the input to the detector is a general optical state$|\Psi_{in}>$, the estimated total clicks probability of the detector is [75],

$$P_{click}(|\Psi_{in}>) = 1 - \sum_{n_h=0}^{\infty}\sum_{p=0}^{\infty} |\Psi_{in}(n_h+p)|^2 \binom{n_h+p}{p} \eta_{loss}^{n_h}(1-\eta)^p \prod_{m=0}^{M-1} (1-P_m)^{\binom{n_h}{m}} \quad (4.40)$$

Where P_m is given by [75],

$$P_m = 1 - e^{(G_m \times \tau_h)} \quad (4.41)$$

G_m : describes the enhancement in GT

τ_h : is the hot spot life time,

n_h: is the number of hotspots,

η_{loss} : is the optical losses between incoming photons and the hotspots that are generated on superconducting nanowires,

M: is the number of G_m values that have significant effect on determining the total GT.

Eq. (4.40) can be modified for Fock state (number state) at the input as follows [74],

$$P_{click}(|N>) = 1 - \sum_{n_h=0}^{N} \binom{N}{n_h} \eta_{loss}^{n_h}(1-\eta_{loss})^{N-n_h} \prod_{m=0}^{M-1} (1-P_m)^{\binom{n_h}{m}} \quad (4.42)$$

Where:

$|N>$: is the n-photon state

To investigate the SPDs response to general light state including a Fock state with different incident photons, detector tomography is used to find the POVM operators of the detector. For binary SPDs which are sensitive to n photons, the No click POVM is [75],

$$\pi_0^{NPD} = \sum_{m=0}^{\infty}(1-P_n)^{\binom{m}{n}} |m><m| \quad (4.43)$$

Where:

P_n: is the n-photon detection efficiency,

$\binom{m}{n}$: is the binomial coefficient $(= 0\ for\ n > m, = 1\ for\ n = 0)$

In this case, dark count probability can be represented by P_0. Click POVM operator is nothing but [75],

$$\pi_1^{NPD} = 1 - \pi_0^{NPD} \quad (4.44)$$

2. Single photon-detection efficiency

$SPDE$ is the most evident performance parameter and it depends on the coupling efficiency which represents the losses due to absorption, scattering or reflection, absorption efficiency which refers to the detector material and geometry and finally, on the registering efficiency which describes the detector triggers after photon absorption [71]. $SPDE$ can be determined by subtracting DCR from C_t and defining the power of the light source in addition to the attenuation range and N_0 using a known PRR and λ as follows [76],

$$C_t = DCR + PRR\left(1 - e^{(-SPDEN_0)}\right) \quad (4.45)$$

In order to relate $SPDE$ to DCR, a useful figure of merit (FOM) for SNSPD is given by [76],

$$FOM = \frac{SPDE}{(DCR \times \Delta t')} \quad (4.46)$$

Where:

$\Delta t'$: is the time jitter.

This is a useful figure for a range of time correlated single photon counting measurements and needed in quantum information applications.

4.5.2 Superconducting nanowire single-photon detector conceptual model

SNSPD is an optical-electrical component with one input port and one output port as shown in the corresponding conceptual model of Figure (4.40).

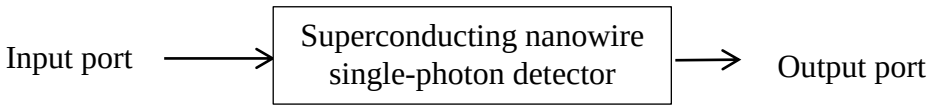


Fig.4.40 SNSPD's conceptual model

From the conceptual model diagram, the incoming highly attenuated laser pulses encoded with a specific polarization will be detected and corresponding pulses will be generated by correct detections with a number related to the detector efficiency. Dark counts will be generated randomly in time and amplitude with a rate depending on the value of I_b and temperature provided by the user.

In addition to the parameters that were mentioned as inputs to the SPAD simulation model, the following parameters were considered also as inputs to the SNSPD model, η_{SPDE}, I_b, N_0, temperature, dark counts occurrence probability.

4.5.3 SNSPD simulation results and discussion

The approach that has been used for model verification in the SPAD model was also be used to verify the SNSPD model. On the other hand**,** the methodology that was followed for the model validation technique was by comparing the modeled SNSPD output behavior to both the output of real SNSPD's device by the help of the commercial data sheet of ID281SNSPD from ID Quantique [Appendix 3] to define the allowed input and output limits in addition to the desired specifications**.** In general, the validation of modeled SNSPD modeling tool was proved via sequence of test cases under different operation conditions and with different input parameters as will be presented. Based on theoretical studies and mathematical models of SNSPD circuit design and physical properties that governs its performance explained in sub-section 4.5.2, a simulator is developed to model the SNSPD that allows users to relate the SNSPD internal structure to its performance. In this section, the SNSPD pulse analysis, the impact of I_b and the temperature on the dark counts rate and $SPDE$, the influence of N_0 on the $SPDE$ are presented. Finally, these results are used as the basis for the design of the SNSPD modeling simulator to visualize the detection

process in addition to the random distribution of DCR to estimate the whole SNSPD performance.

This SNSPD type has high η which is larger than 80% at 1550nm and 900nm. It can be operated with low dark count rate equal to 100C/second at temperature of 0.8K.

The simulation of this component starts with the generation of random in time and amplitude dark pulses with a rate depending on the value of I_b and temperature provided by the user followed by the simulation of electrical pulses caused by correct detection of incoming laser pulses in accordance to the detection efficiency.

In this model, the electrical circuit shown in Figure (4.39) is assumed as an equivalent circuit for the SNSPD. In order to simulate the SNSPD output pulse on Z_0, it is important to define the following: L_k=10nH, R_n (t) = 500Ω, Z_0 =50Ω to accurately determine the rise time, fall time and the dead time of the output pulse. Small $L_k$was assumed in this work because of small kinetic inductance improves the SNSPD performance since it reduces the overall dead time. In addition to this point, the higher the value of L_k, the lower the value of the current passing in the wire. Z_0 is assumed as a conventional 50Ω transmission line impedance [71, 72, 73].

To study the impact of increasing I_b on the SNSPD output voltage, Figure (4.41) represents the output pulse with different I_b values. As I_b increases, the probability of triggering increases too which as a result leads to an increase in the output peak voltage.

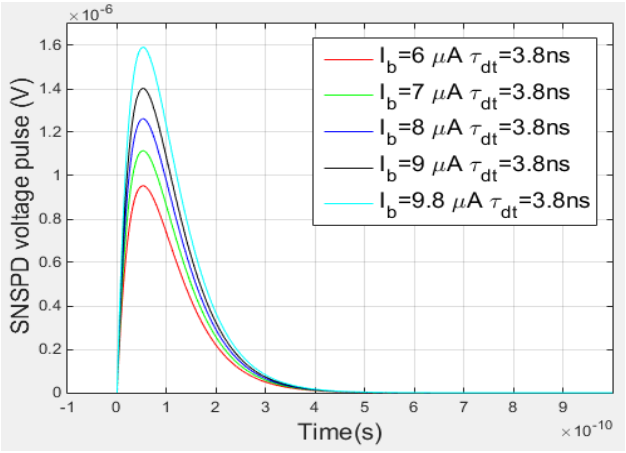


Fig.4.41 SNSPD voltage pulse at different biasing currents (I_b)

To check the correctness of the simulated SNSPD voltage signal for validation purpose, it will be compared to the real pulse generated by ID281SNSPD as presented in Figure (4.42) in terms of overall pulse waveform and τ_d as shown in Table (4.4).

Fig.4.42 ID281SNSPD real pulse

Table 4.7 A comparison between ID281SNSPD and the SNSPD model

Property	ID281SNSPD	Modeled SNSPD
τ_{dt}	≅ 20 ns	≅ 4 ns

To quantify the performance of SNSPD, different terms have to be assessed for optimal characterization and design. First of all, in this research only 1500nm and 900nm wavelengths are examined as ID281SNSPD shows maximum η. The mathematical model parameters used in this work were extracted from [74].

Figures from (4.43) - (4.45) illustrate the simulated SNSPD under study performance parameters results for λ=1550nm while the results obtained from λ= 900nm in addition to λ=1550nm will be used in the simulator to assess its capability by comparing their results. The following parameters calculated from [74] were used in (4.52) to compute $SPDE$ as shown in Table (4.5).

Table 4.8 the calculated parameters used in Eq. (4.52)

		C_t Hz				
δ (dB)	N_0	I_b=6μA	I_b=7μA	I_b=8 μA	I_b=9 μA	I_b=9.8 μA
-100	3.1×10^{-5}	1(DCR)	7 (DCR)	38(DCR)	72(DCR)	1000(DCR)
-80	3.1×10^{-3}	1(DCR)	7(DCR)	38(DCR)	72(DCR)	1000(DCR)
-60	0.31	1(DCR)	8	100	850	5000
-40	31	1(DCR)	100	8000	8×10^{4}	3×10^{5}
-20	3100	110	1×10^{4}	8×10^{5}	8×10^{6}	10^{7}
-1	2.4×10^{5}	9×10^{6}	10^{7}	10^{7}	10^{7}	10^{7}

Figure (4.43) shows the $SPDE$ vs I_b at 1500nm for N_0 ranging from 3.1×10^{-5} to 2.4×10^{5}. It's clear that the detection performance is poor for low biasing current values. $SPDE$ increases linearly as I_b increased. By

further increasing I_b to its critical value, $SPDE$ will saturate at a constant value. Also, it is possible to notice the effect of the average optical power detected by SNSPD on the barrier generation rate. When N_0 approaches to 3.1×10^{-5}; the device has measureable detection efficiency in spite of the little amount of incident optical power. The source for this behavior is the presence of the thermal effect. As the optical power increases the number of photons increases, $SPDE$ increases too due to the contribution of both real photons as well as thermally generated dark carriers.

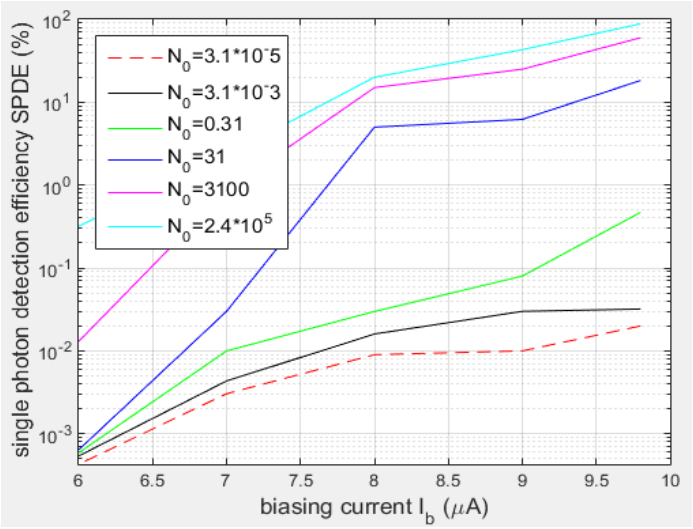


Fig.4.43 $SPDE$ vs. biasing current (I_b)

Figure (4.44) investigates the effect of the temperature and the biasing current on the device detection efficiency as a function of the incoming optical power. At lower temperature, the critical value of the I_b increases which as a result lowers the required I_b and $SPDE$ improves.

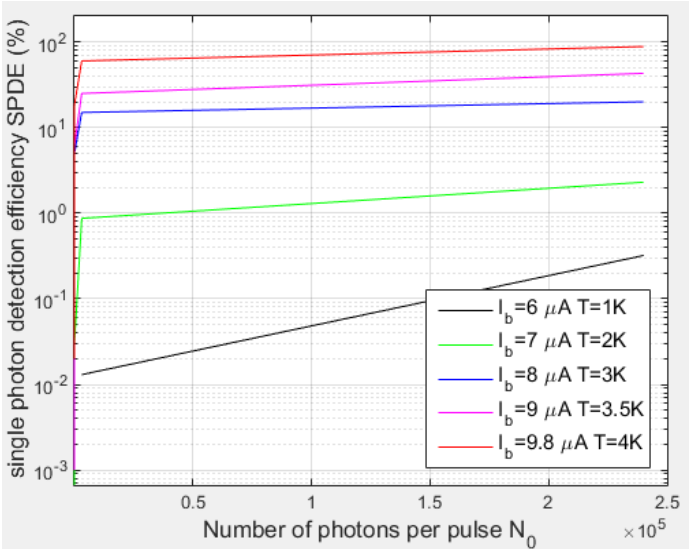


Fig. 4.44 $SPDE$ vs. average number of photons (N_0)

Figure (4.45) shows how I_b and temperature conditions can enhance the SNSPD performance by reducing DCR. One can find that the acceptable range for DCR per pulse could be achieved by cooling the system down to 3.5K according to the ID281SNSPD specification data sheet.

As the temperature reduces, the required I_b for biasing decreases too which in turn improves the DCR performance which is in this case only dominated by the background thermal radiation noise. With high temperature conditions, I_b will increase which reinforce the SNSPD internal noise. So, DCR can be minimized by operating at lower I_b but at the expense of low $SPDE$.

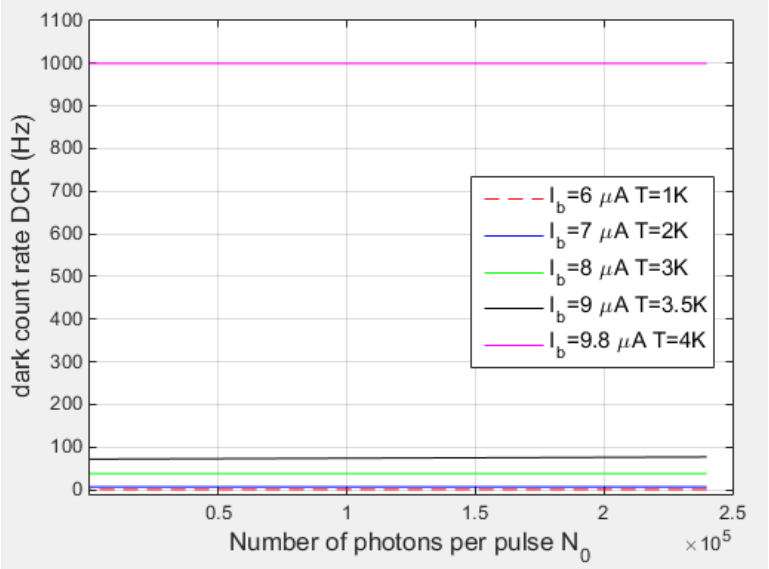


Fig. 4.45 Dark count rate (DCR) vs. average number of photons N_0

To check the correctness of the SNSPD performance simulation results, it will be compared to the results reported in ID281SNSPD data sheet in terms of DCR and η at different temperatures as shown in Table (4.6).

Table 4.9 A comparison between ID281SNSPD and the SNSPD model

parameters	ID281SNSPD	Modeled SNSPD
η @ λ=900nm	>80%	90%
η @ λ=1550nm	>80%	88.3%
Dark counts	< 100 counts @ T=0.8k	1000 counts @ T=4k 72 counts @ T=3.5k 38 counts @ T=3k 7 counts@ T=2k 1 counts@ T=1k

The difference between the modeled SNSPD results and the specifications presented in ID281SNSPD data sheet is due to the simulation parameters and the measurement conditions that have been used in the SNSPD model calculations such as P_{peak}, I_b and the temperature were extracted from [74] are different from ID281SNSPD measurement conditions. The goal is to investigate the operation of the SNSPD under various operation conditions. Therefore, it is clear that the outcomes accuracy is within the acceptable behavior range which is the measure of the precision required for the device's modeling.

4.5.4 SNSPD simulator implementation and testing

This section describes the SNSPD simulator in addition to the testing cases to prove the simulator capability for SNSPD behavior verification by comparisons of the simulator results with the mathematical models based data. The simulator can support wide spectral range starting from 400nm up to 2500nm which represents the allowable spectral range for ID281SNSPD. Figure (4.46) illustrates the simulator main window with plotters, inputs and control objects. The left plotter represents the incoming laser pulses with defined PRR and power. The right plotter illustrates the

output voltage pulses comprises the true photon detection and false detections due to dark noise.

In this section the results for 900nm and 1500nm test cases for ID281SNSPD will be presented. For all four tests, 25 input pulses to the SNSPD were linearly polarized with P_{peak} gradually attenuated from 1mW to get the desired level as shown in Table (4.5) and PRR=1GHz. The user can change I_b, temperature and N_0 at the same time to investigate the overall SNSPD performance parameters: $SPDE$ and DCR. Depending on the user inputs, the simulator will plot the resultant SNSPD trigger pulses in accordance to the incoming optical laser pulses taking into consideration the $SPDE$ to decide if the pulse is detected or not as well as DCR.

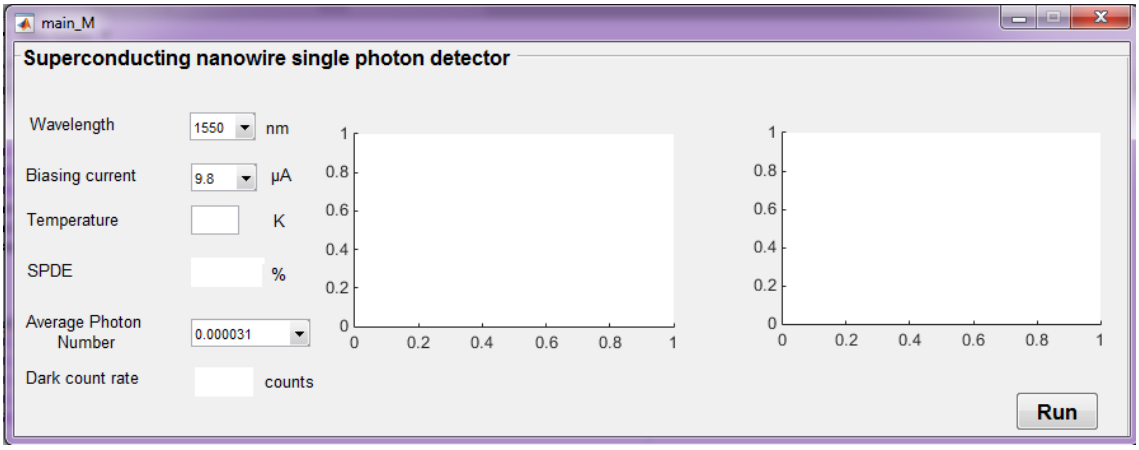


Fig. 4.46 Simulator main window

Four tests were done to verify the simulator capabilities to simulate the SNSPD operation and to prove its operation validity.

Test 1: I_b= 9.8μA, temperature=4K, N_0=240000 and λ=1550nm. The attenuation level is assumed to be -1dB. According to these inputs, the calculated $SPDE$ was 88.3%. Therefore, the expected number of true photon detections is equal to 22 pulses out of 25 pulses. The simulator result is approximately equal to the expected result (i.e. 23 pulses in red) as shown in Figure (4.47). Pulses in blue represent the output detections due to thermal effects with the number equal to the calculated DCR which was 1000 counts. The effect of the incoming optical power represented by N_0

on the detection performance can be observed by testing the amplitude of both true detections and noise pulses. The SNSPD output voltage signals in red increased compared to the noise signals in blue.

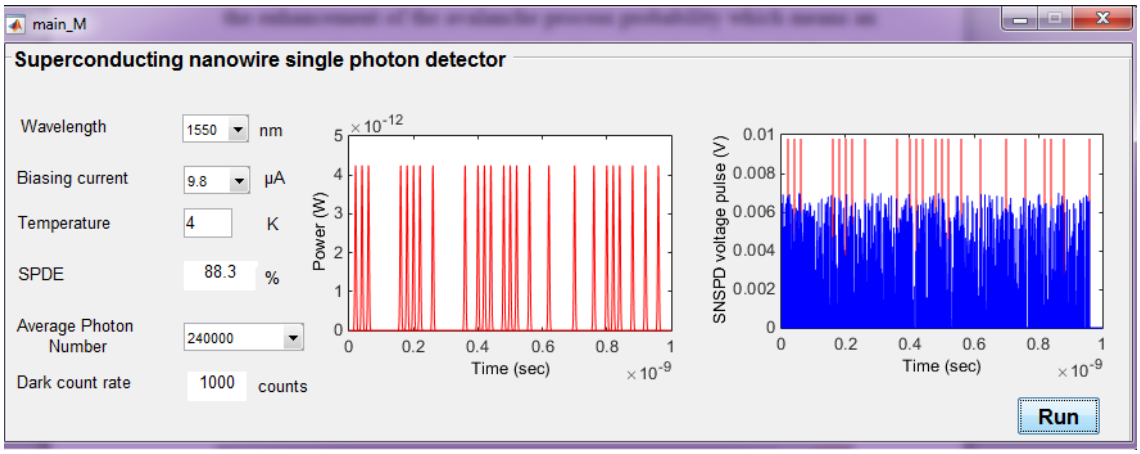


Fig. 4.47 Test1 simulation results for: :λ=1550nm, N_0= 240000, I_b=9.8μA and T= 4K.

Test 2: I_b= 7μA, temperature=2K, N_0=0.3 and λ=1550nm as shown in Figure (4.48). In this test the impact of the temperature on the DCR and the effect of reducing I_b on the $SPDE$ will be studied. As expected, the true photon detection was one pulse in accordance to the registered $SPDE$ which is degraded due to the reduction in I_b. DCR is decreased to seven counts in comparison to the previous test as the temperature is reduced.

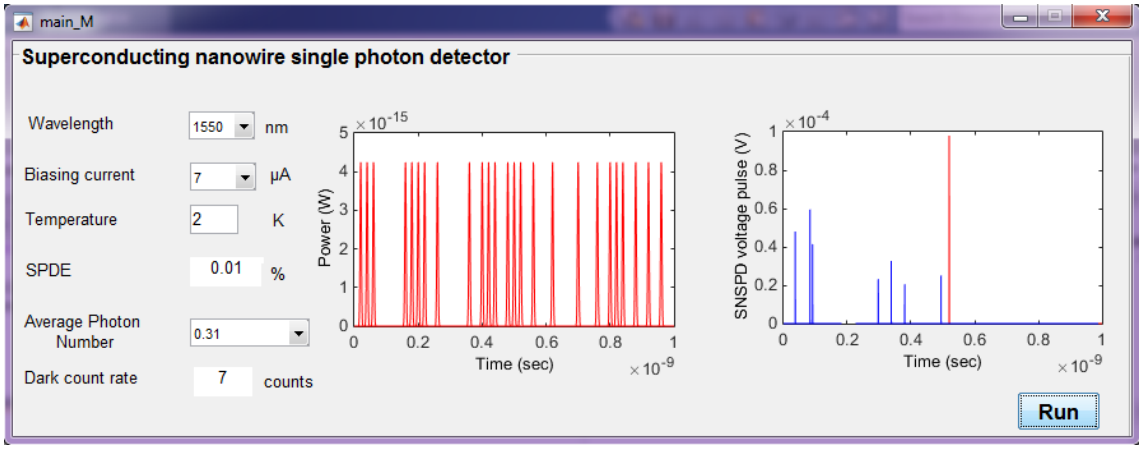


Fig. 4.48 Test2 simulation results for :λ=1550nm, N_0= 0.31, I_b=7μA and T= 2K.

Test 3: I_b= 9.8μA, temperature=4K, N_0=31 and λ=1550nm as shown in Figure (4.49). The strong effect of the average optical power in terms of N_0 detected by the SNSPD on $SPDE$ will be explained in this test. The attenuation level is assumed to be -40dB. Compared to test 1, the measured $SPDE$ is reduced from 88.3% to 18.3% as a result of the apparent decrease in the number of photons falling on SNSPD. The simulator response to the test settings shows five true detections out of 25 laser pulses which is matched to the expected theoretical results.

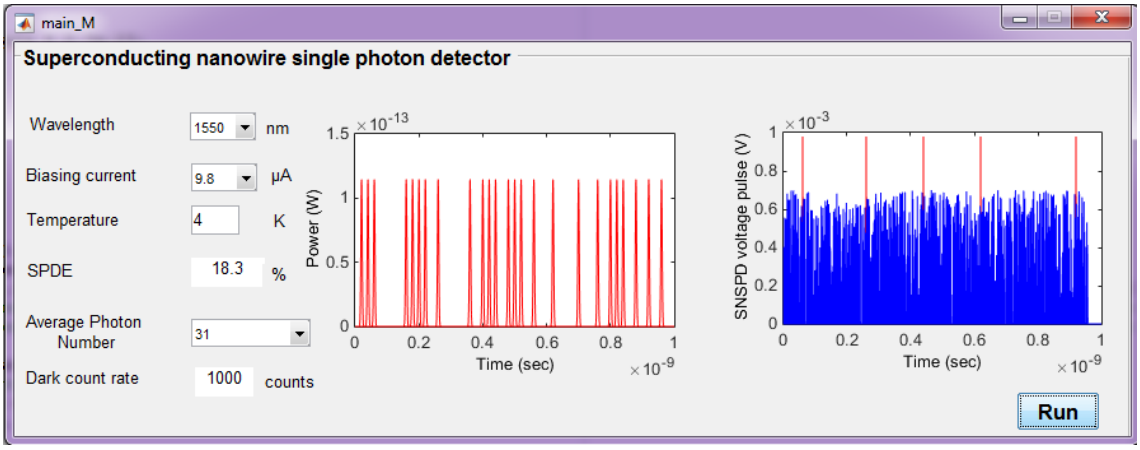


Fig. 4.49 Test3 simulation results for: :λ=1550nm N_0=31, I_b=9.8μA and T= 4K.

Test 4: I_b is set to 9.8μA, temperature=4K, N_0=240000 and λ=900nm as shown in Figure (4.50). In this test, the effect of λ on the device performance will be studied. Compared to the Test 1, one can see how the registered $SPDE$ improves from 88.3% to 90% due to increasing of photon energy as the wavelength becomes shorter. The expected registered true photon detections were 23 pulses.

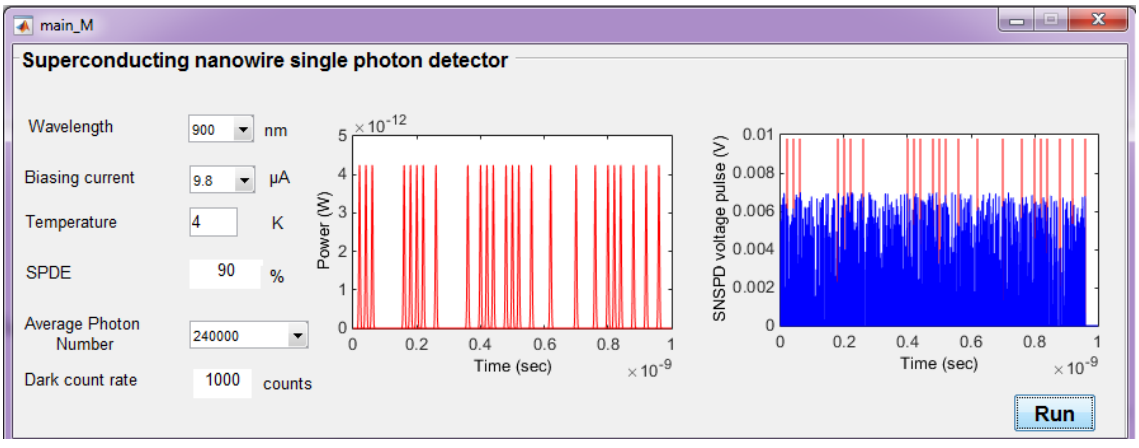


Fig.4.50 Test4 simulation results for:λ=900nm N_0= 240000, I_b=9.8μA and T= 4K.

In general, by comparing the simulator tests results with the mathematical models results mentioned in the last section, one can find a good agreement which as a result confirms the simulator ability to examine the SNSPD performance.

Chapter Five

The Investigation of the BB84

Protocol Simulator

Chapter Five

The Investigation of the BB84 Protocol Simulator

5.1 Introduction

The purpose of this chapter is to present a generic simulator aimed to simulate and analyze the QKD systems with a demonstration of the BB84 protocol as a case study. At the beginning, initial implementations of this simulator will be addressed. The final version of this tool will be described with illustration of the results obtained from the execution of the main BB84 protocol phases. Finally, the quantum optical fiber and free space based QKD systems as test cases will be presented.

5.2 The Simulator Investigation

One of the common basics in software engineering is that the model must be tested and evaluated continuously throughout its life cycle as recommended by Sargent and Balci to disclose any shortage in early time that may occur during the model implementation steps. Errors detection and correction throughout the model life cycle, adequate for both time and cost [19, 20]. Thus, in addition to the tests that were created on each component individually as shown previously, coupled sub-modules have been tested before testing the whole simulation model for validation purposes.

Three important simulation experiments were carried out for three experimental layouts**.** Figure (5.1) illustrates the experiments modeling flow that has been conducted in this section.

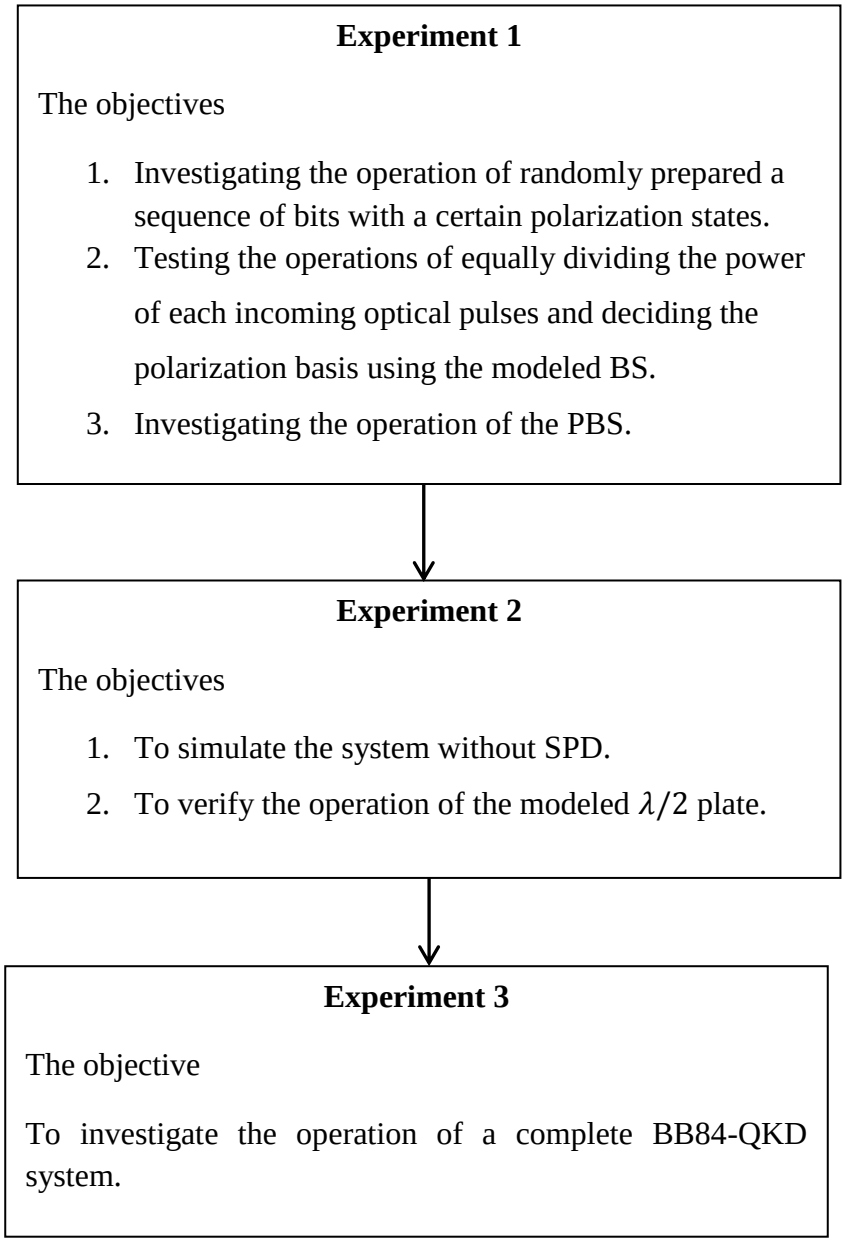


Fig.5.1 BB84-QKD Experiments modeling flow

5.2.1 Experiment 1: testing the transmitter and the PBS operation

Figure (5.2) illustrates the proposed back to back system model scenario for Experiment 1. Each optical path is triggered randomly by BPRS unit. The upper path is dedicated to send 0's while the lower path is used to send 1's at each time for both cases. The receiving bits at the PBS are splitted either as an optical transmitted signal or as an optical reflected signal depending on their polarization states and the PBS device angle.

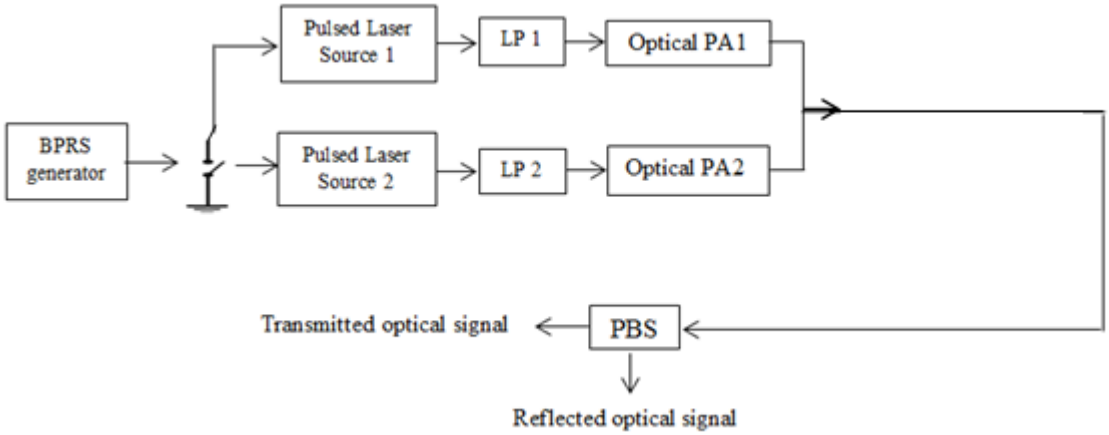


Fig.5.2 Experiment 1 system model scenario

Six simulation tests are carried out to verify the correctness of this Experiment scenario. For all tests, the required simulation parameters are listed in Table 5.1.

Table 5.1 Experiment 1 simulation parameters

Parameter	Value
Number of used optical pulses	25
PRR	100 kHz
P_{peak}	1mW
λ	1550nm
Optical PA attenuation coefficient	0 dB
Insertion loss	0.5 dB
Return loss	10 dB
PDL loss	0.25 dB

The polarization of the transmitted optical signals depends upon the LP angles. The OF quantum channel is assumed as a lossless channel. Figure (5.3) shows the designed GUI to investigate the validation of this experiment. It consists of input objects to set up the

main system parameters such as LP's, PBS polarization angles and the different PBS losses types. Six plotters are used to illustrate the generated pulses through transmission at different system stages as specified for each plotter. Red pulses represent 0's bits while blue pulses represent 1's bits.

Figure (5.3) shows the first simulation test. In this test, $\gamma_{LP1}, \gamma_{LP2}$ and γ_{PBS}= 0°. It can be shown that all input optical pulses to PBS are reflected because of the transmission axis is in a parallel with the polarization of input optical signals.

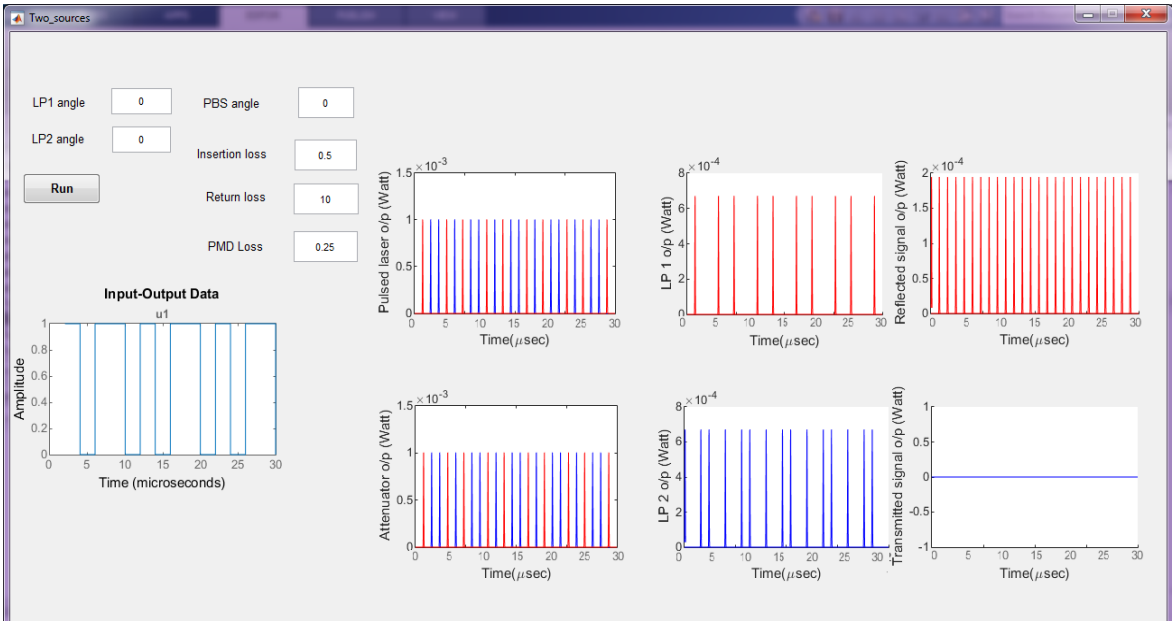


Fig.5.3 Experiment 1, Test 1 results, $\gamma_{LP1}, \gamma_{LP2}$ and γ_{PBS}= 0°

Figure (5.4) illustrates **Test 2** result. In this test, $\gamma_{LP1}$and γ_{LP2} = 90° (i.e. vertically polarized transmitted optical pulses) and γ_{PBS} = 0°. The PBS transmission axis is in parallel with the polarization of input signals. As long as the incident light beam is vertically polarized, the optical beam will be completely transmitted.

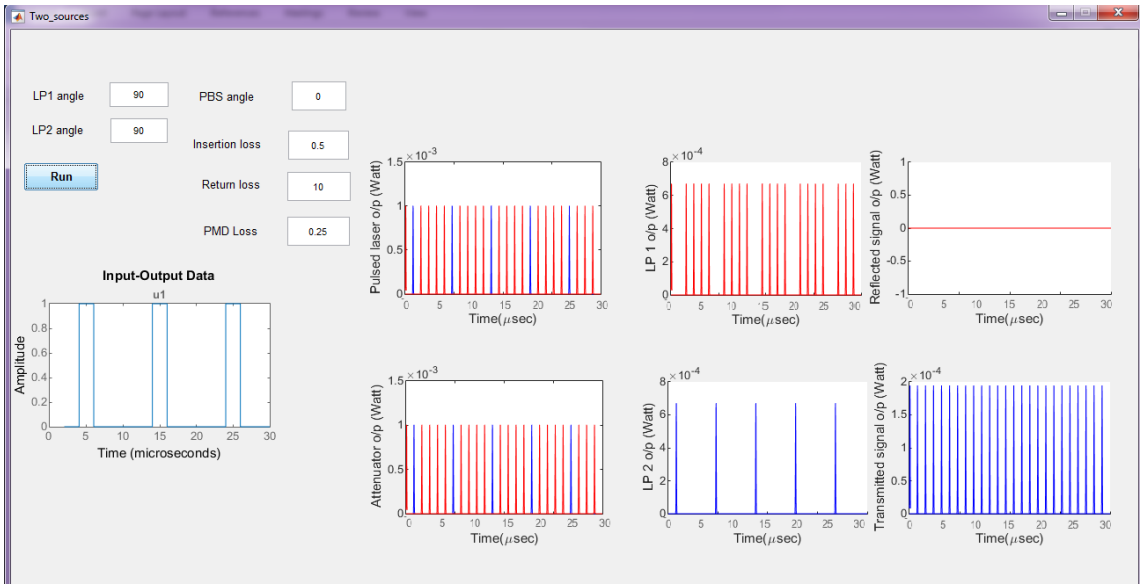


Fig.5.4 Experiment 1, Test 2 results, γ_{LP1} and γ_{LP2} = 90° γ_{PBS} =0°

Figure (5.5) illustrates **Test 3** result with γ_{LP1}, γ_{LP2}=45° and γ_{PBS}=0°. It can be seen that the power of the incident optical beam is equally divided between output ports because of both S and P components will appear at both outputs of PBS as reflected and transmitted signals respectively.

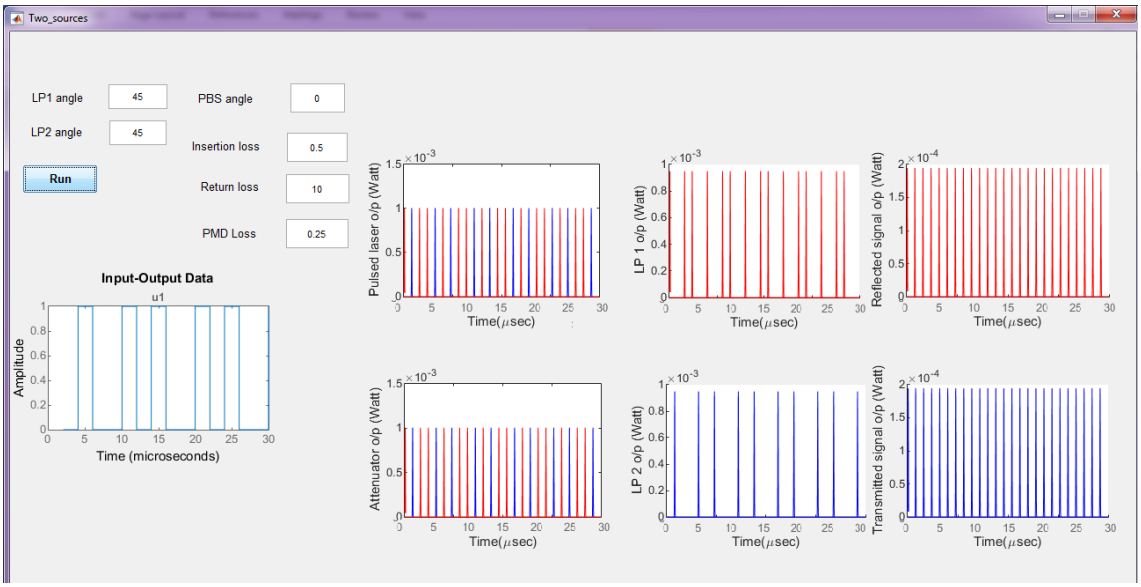


Fig.5.5 Experiment 1, Test 3 results, γ_{LP1}, γ_{LP2}=45° and γ_{PBS}=0°

Figure (5.6) illustrates **Test 4** result with γ_{LP1}, γ_{LP2}= 0° and γ_{PBS}=45°. It can be seen that the behavior of the system is similar to the system behavior in **Test 3** as the power of the incident optical pulses appears at the outputs of PBS as reflected and transmitted signals.

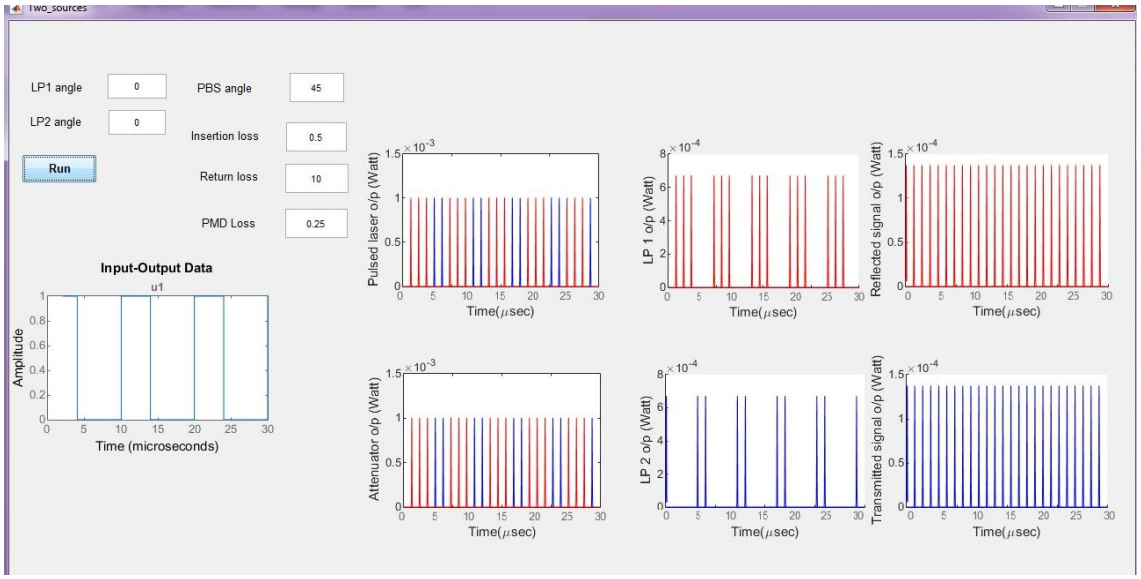


Fig.5.6 Experiment 1, Test 4 results, γ_{LP1}, γ_{LP2}= 0° and γ_{PBS}=45°

Figure (5.7) illustrates **Test 5** result with γ_{LP1}, γ_{LP2}= 90° and γ_{PBS} =45°. The resultant PBS output optical pulses are equally divided as expected because of the PBS transmission axis allows passing both S and P components.

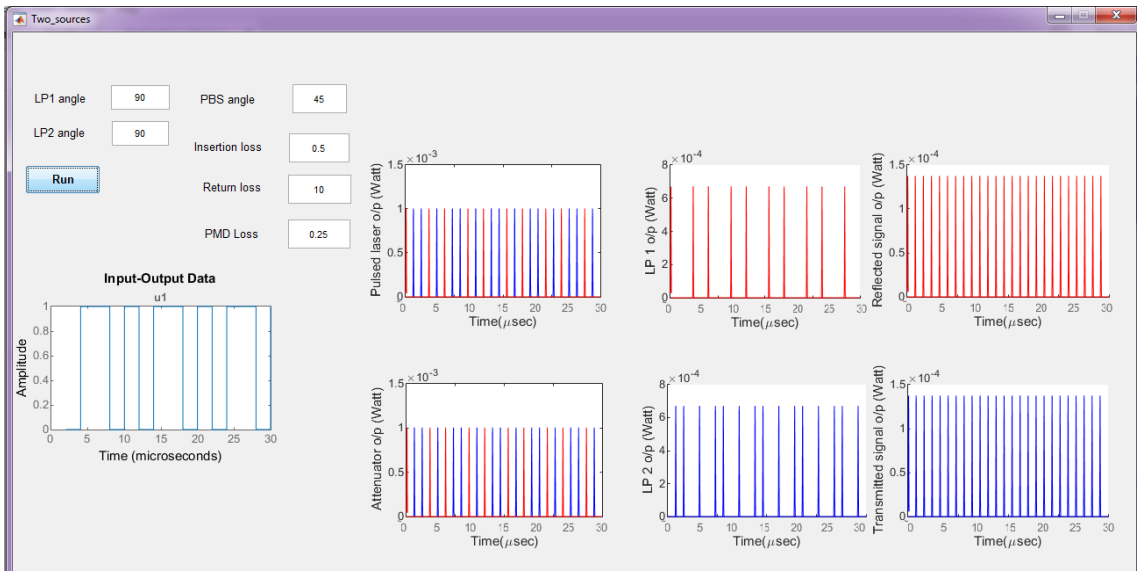


Fig.5.7 Experiment 1, Test 5 results, γ_{LP1}, γ_{LP2}= 90° and γ_{PBS} =45°

Figure (5.8) illustrates **Test 6** result with γ_{LP1}, γ_{LP2} and γ_{PBS}=45°. The optical beam will completely be transmitted through the PBS because of the transmission axis is parallel with the polarization of the incident optical beam.

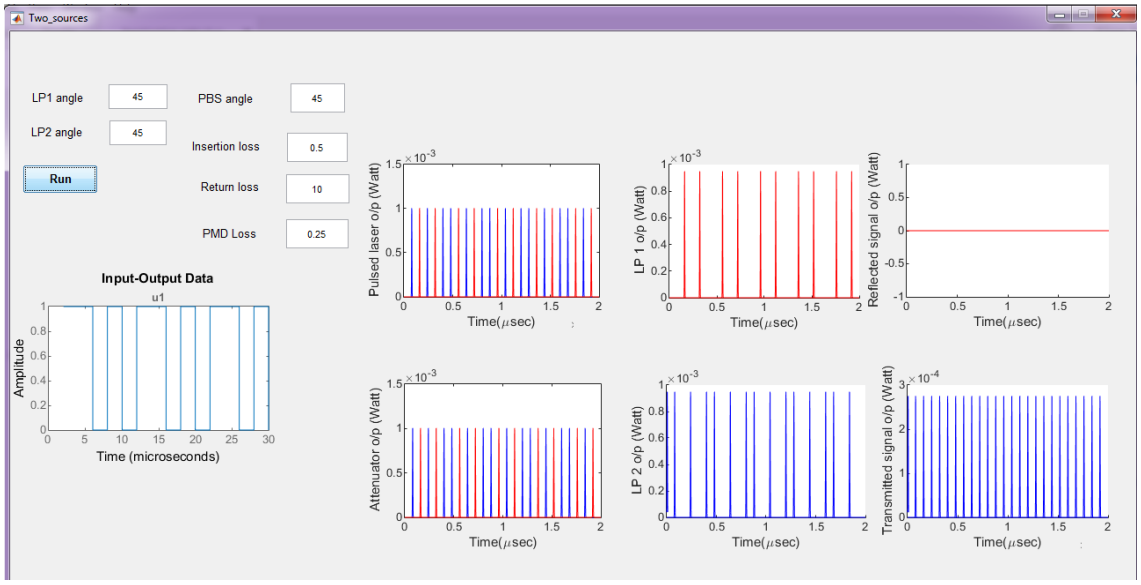


Fig.5.8 Experiment 1, Test 6 results, γ_{LP1}, γ_{LP2} and γ_{PBS}=45°

Table 5.2 summarizes the remaining tests by listing all possible results obtained after system evaluation.

Table 5.2 γ_{LP} and γ_{PBS} settings for LP1, LP2 and PBS with the corresponding results for Experiment 1, where ✓: output signal and ×: no signal.

γ_{LP1}	γ_{LP1}	γ_{PBS} =0°		γ_{PBS} =45°		γ_{PBS} =30°	
LP1	LP2	Transmitted signal	Reflected signal	Transmitted signal	Reflected signal	Transmitted signal	Reflected signal
0	0	×	✓	✓	✓	✓	✓
90	90	✓	×	✓	✓	✓	✓
45	45	✓	✓	✓	×	✓	✓
0	45	✓	✓	✓	✓	✓	✓

45	0	✓	✓	✓	✓	✓	✓
0	90	✓	✓	✓	✓	✓	✓
90	0	✓	✓	✓	✓	✓	✓

5.2.2 Experiment 2: testing the routing of the optical pulses polarization bases and states at system's receiver.

Figure (5.9) illustrates the proposed system model scenario for **Experiment 2**. Table 5.3 illustrates the polarization basis, state and the assigned bit value for each optical path.

Table 5.3 the polarization basis, state and the corresponding bit value used in Experiment 2

Rectilinear Basis			**Diagonal Basis**		
	Bit value	Polarization state		Bit value	Polarization state
Path 1	0	0°	Path 4	0	135°
Path 3	1	90°	Path 2	1	45°

Three simulation tests were carried out to verify the correctness of this Experiment scenario. The assumptions that were used in **Test 1** are used in this test except the BS splitting ratio LOP and HOP=50% respectively.

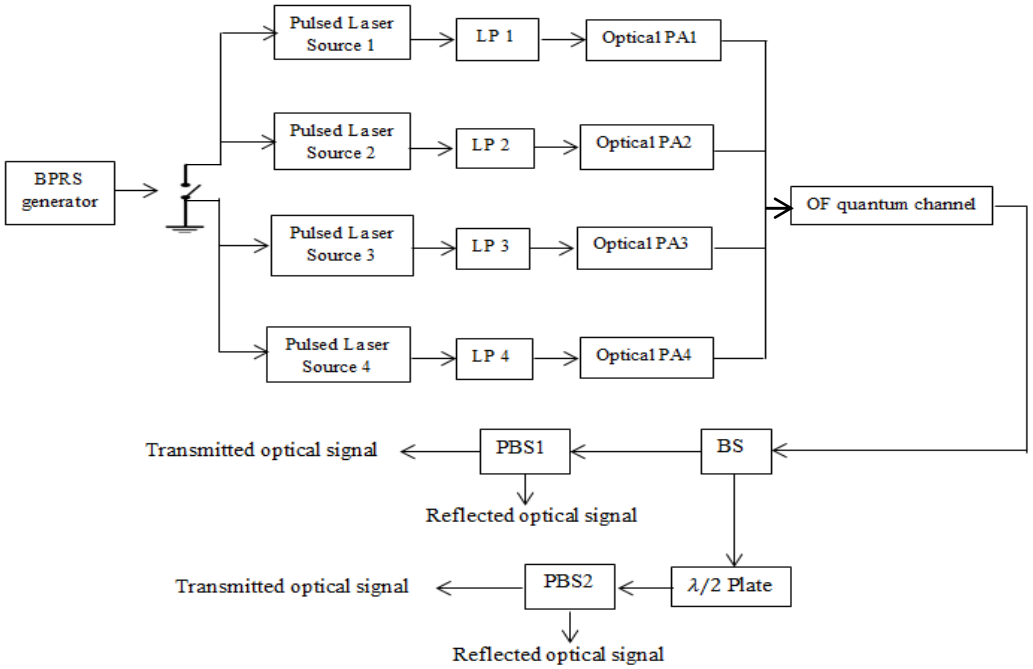


Fig.5.9 Experiment 2 system model scenario

Figure (5.10) shows the designed GUI with the input objects to configure the main system parameters. Eleven plotters are used to illustrate the generated pulses through transmission at different system stages as specified for each plotter. In order to discriminate between the optical pulses those are transmitted in terms of their polarization, each optical path colored in a different color. First path is colored by red, second path is colored by blue, third part is colored by green and finally the yellow pulses represent the output from the fourth path. For all tests, the number of binary bits generated by BPRS is equal to 20 bits as illustrated in the GUI. Two bits are required to fire each pulsed laser source to generate an optical pulse at a time,

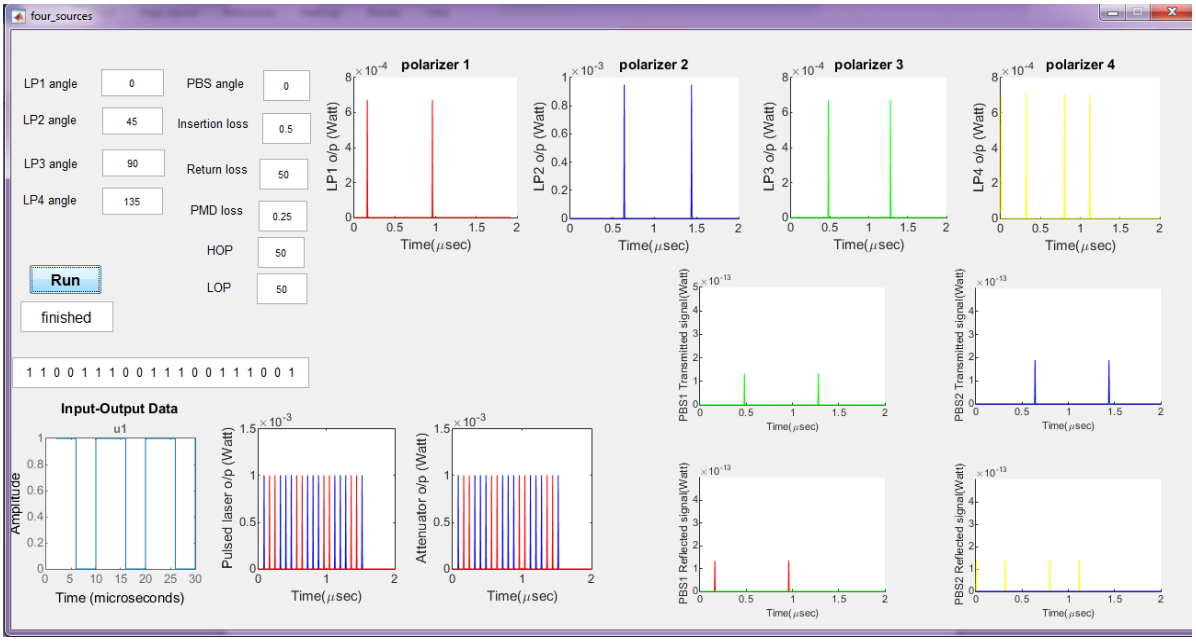


Fig.5.10 Experiment 2, Test 1 results

Pulsed laser source 1 ⟶ 00

Pulsed laser source 2 ⟶ 01

Pulsed laser source 3 ⟶ 10

Pulsed laser source 4 ⟶ 11

Thus, 10 optical pulses will be generated by the optical paths out of 20 random bits. Table 5.4 summarizes the randomly generated bits and the corresponding optical pulses that have been generated out of these bits as shown in the LPs plotters of **Test 1**.

Table 5.4 random bits and the corresponding optical pulses that have been generated in Test 1.

The generated random bits	The corresponding optical pulses
00,00	2 red pulses from LP1
01,01	2 blue pulses from LP2
10,10	2 green pulses from LP3
11,11,11,11	4 yellow pulses from LP4

As shown in Figure (5.10), by checking the PBS1 plotters, red pulses with 0° polarization are passed completely from the PBS1 reflected output port while green pulses with 90° polarization are

passed completely from the PBS1 transmitted output port. In contrast, all optical pulses with diagonal polarization basis are passed through the built in $\lambda/2$ plate modeled function.

Table 5.5 summarizes the randomly generated bits and the corresponding optical pulses that have been generated out of these bits as shown in the LPs plotters of Figure (5.11) of **Test 2** results.

Table 5.5 random bits and the corresponding optical pulses that have been generated in Test 2.

The generated random bits	The corresponding optical pulses
00,00	2 red pulses from LP1
01,01,01,01	4 blue pulses from LP2
10,10,10,10	4 green pulses from LP3

By checking the PBS1 plotters, red pulses with 0° polarization are passed completely from the PBS1 reflected output port while green pulses with 90° polarization are passed completely from the PBS1 transmitted output port. Blue pulses with 45° polarization states are passed completely from the PBS2 transmitted output port.

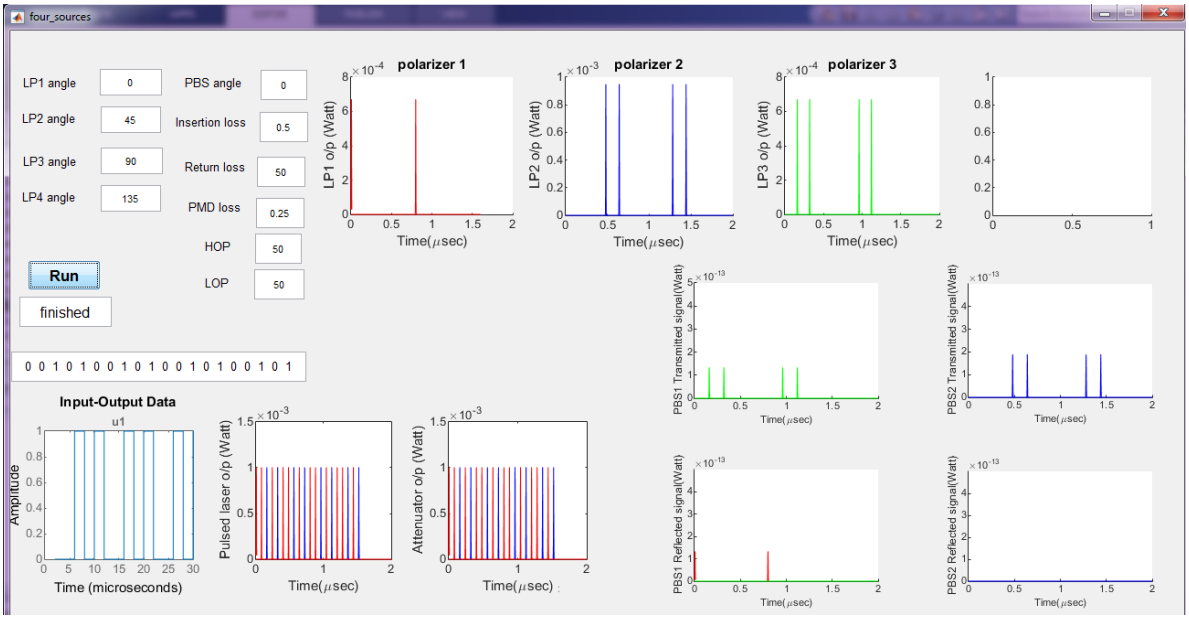


Fig.5.11 Experiment 2, Test 2 results

Table 5.6 summarizes the randomly generated bits and the corresponding optical pulses that have been generated out of these bits as shown in the LPs plotters of Figure (5.12) of **Test 3** results.

Table 5.6 random bits and the corresponding optical pulses that have been generated in Test 3.

The generated random bits	The corresponding optical pulses
01,01	2 blue pulses from LP2
10,10	2 green pulses from LP3
11,11,11,11,11,11	6 yellow pulses from LP4

By checking the PBS1 plotters, green pulses with 90° polarization are passed completely from the PBS1 transmitted output port. Blue pulses with 45° polarization states are passed completely from the PBS2 transmitted output port. Yellow pulses with 135° polarization states are passed completely from the PBS2 reflected output port.

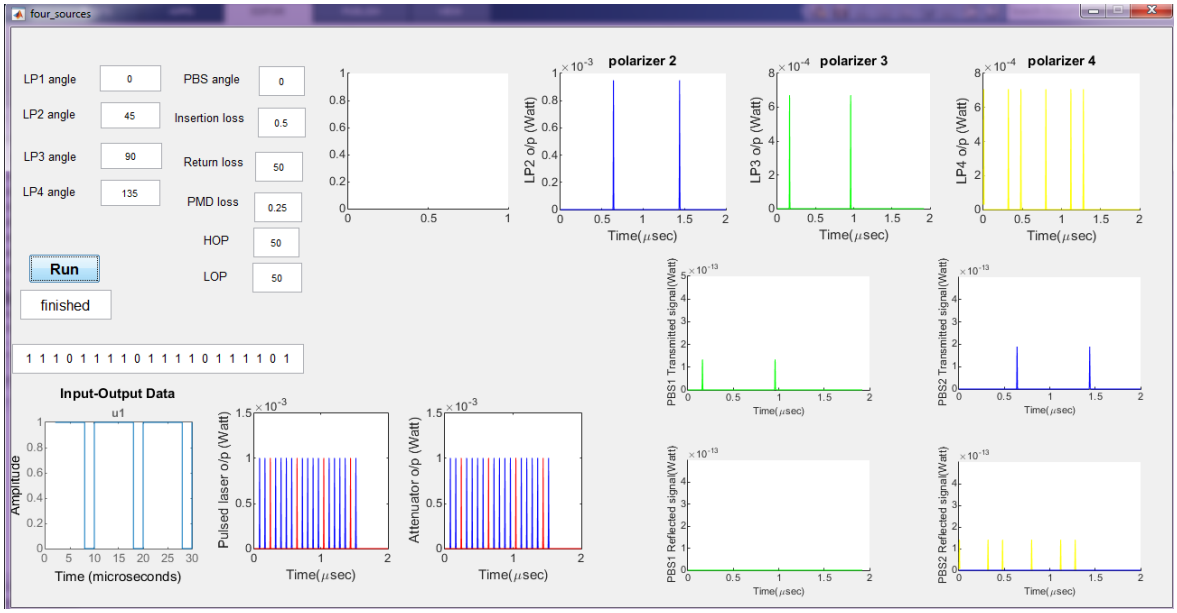


Fig.5.12 Experiment 2, Test 3 results

5.2.3 Experiment 3: Investigating the operation of a complete BB84-QKD system.

Figure (5.13) illustrates the proposed system model scenario for **Experiment 3**. Three simulation tests were carried out to ensure the correctness of this simulation scenario. The assumptions that were used in **Experiment 2** are used in this experiment.

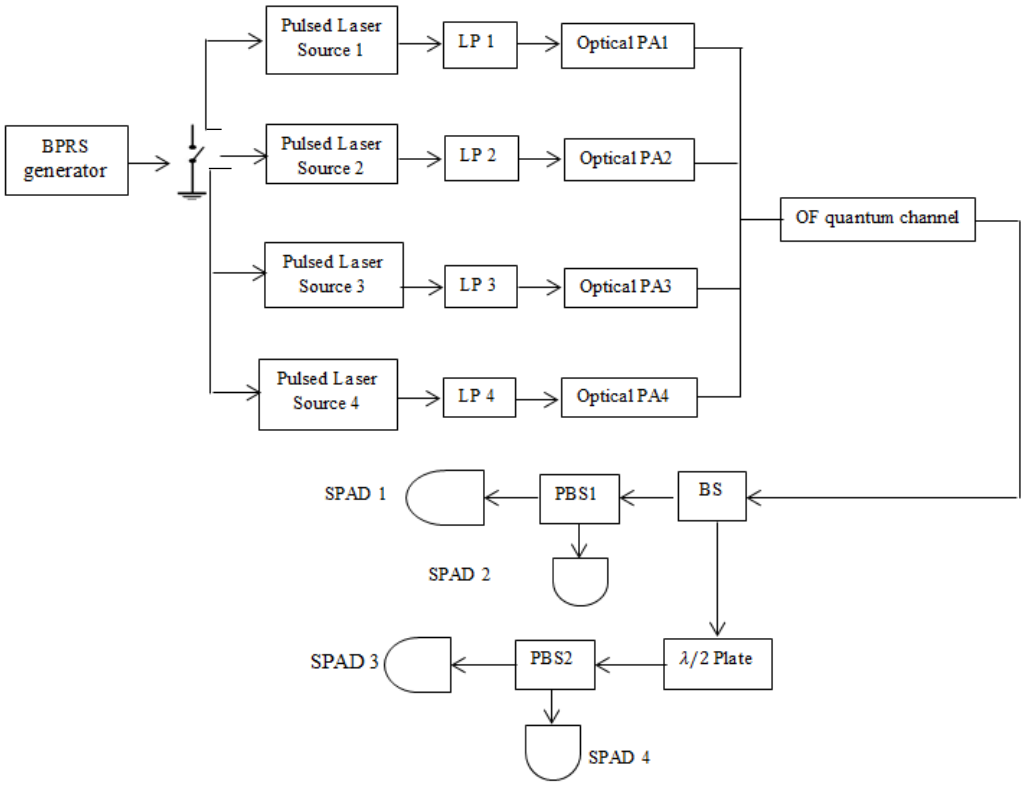


Fig.5.13 Experiment 3 system model scenario

Figure (5.14) shows the designed GUI with the same input objects and plotters that were utilized in **Experiment 2.** For all tests, the number of binary bits generated by BPRS is equal to 100 bits as illustrated in the GUI for the sake of analysis simplicity. Therefore, 50 optical pulses will be generated by the optical paths. For organizational purposes, a secondary GUI that consists of input objects and 4 plotters can be called using (Run SPAD) push button to examine the behavior of the SPAD models within this system model under different operation conditions. Table 5.7 represents the bit value

and the polarization basis that can be detected by each SPAD. For all tests, λ=830nm and N_o= 0.2.

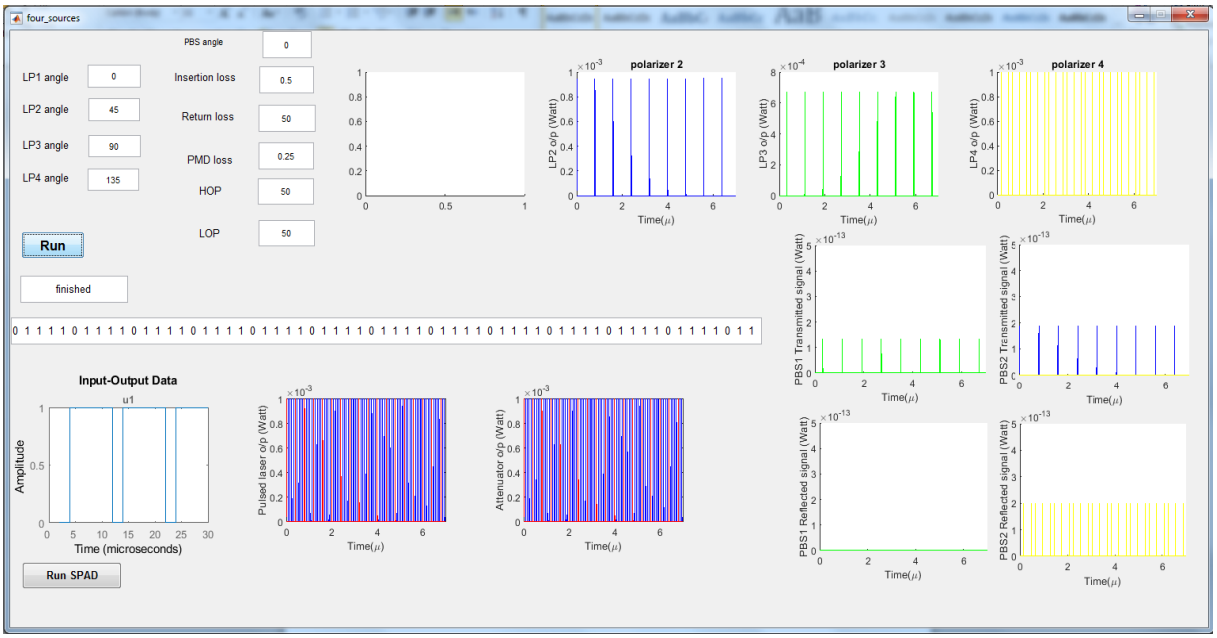
Table 5.7 the bit value and the polarization basis that can be detected by each SPAD for Experiment 3.

Rectilinear Basis		**Diagonal Basis**	
SPAD No.	Bit value	SPAD No.	Bit value
SPAD2	0	SPAD4	0
SPAD1	1	SPAD3	1

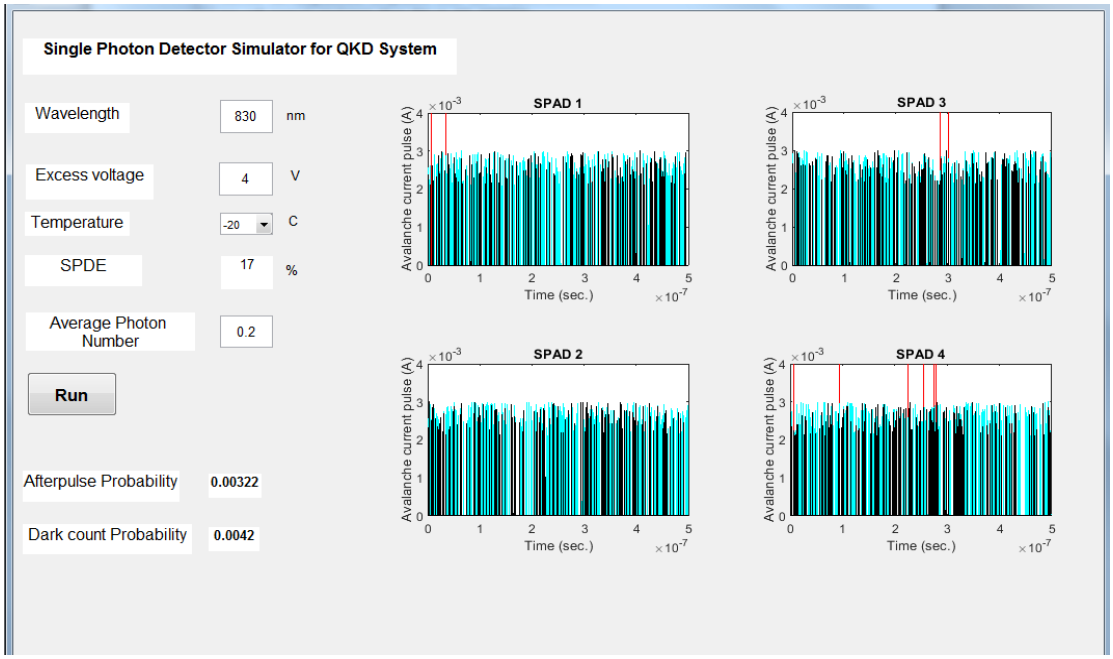
Figures (5.14-5.16) show the simulation tests results. For each figure, (a) illustrates the randomly generated bits and the corresponding optical pulses that have been generated out of these bits as shown in the LPs plotters, (b) shows the SPADs GUI result, and (c) are the numerical simulation results which report the number of input pulses to each SPAD, the number of detected pulses and the number of dark and afterpulsing counts generated for each SPAD for results validation purpose. Table 5.8 reports the SPADs input parameters that have been changed through these tests in addition to the resultant $SPDE$ according to these input parameters.

Table 5.8 SPADs input parameters for Experiment 3.

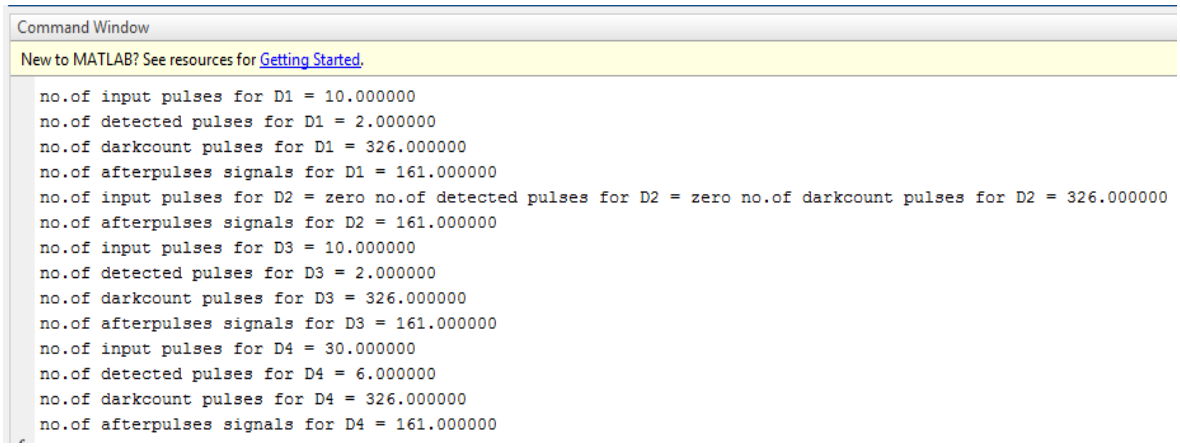
Parameter / Test No.	V_{ex} (V)	Temperature (℃)	Resultant $SPDE$ (%)
Test 1	4	−20	17
Test 2	12	−30	40.5
Test 3	24	−30	60



(a)

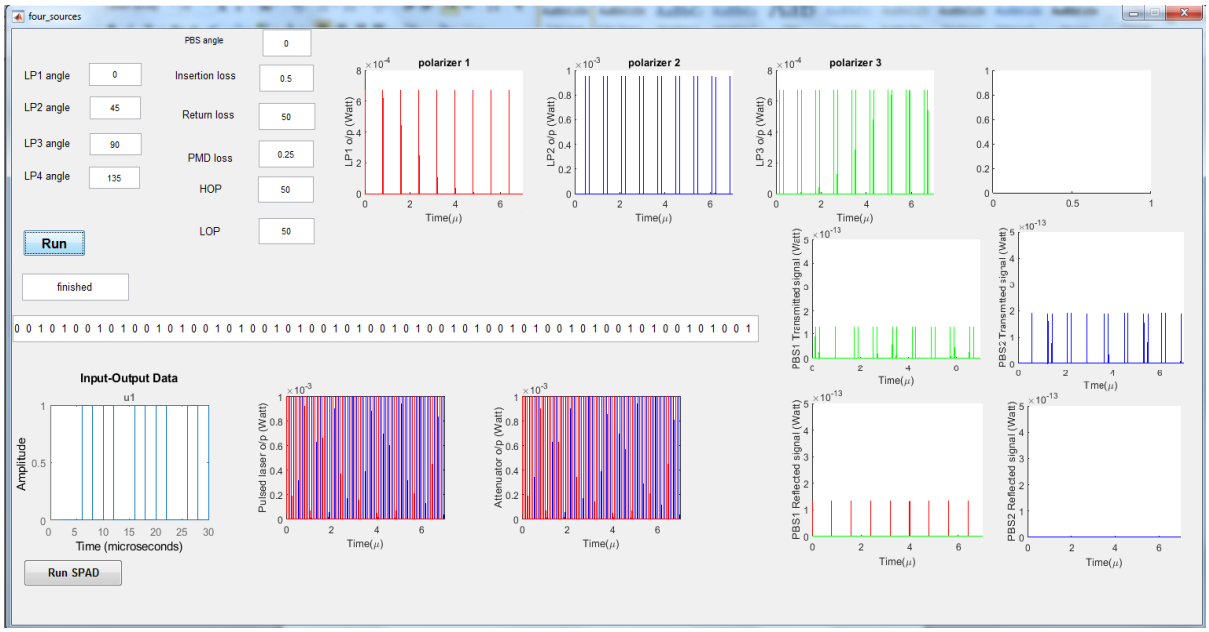


(b)

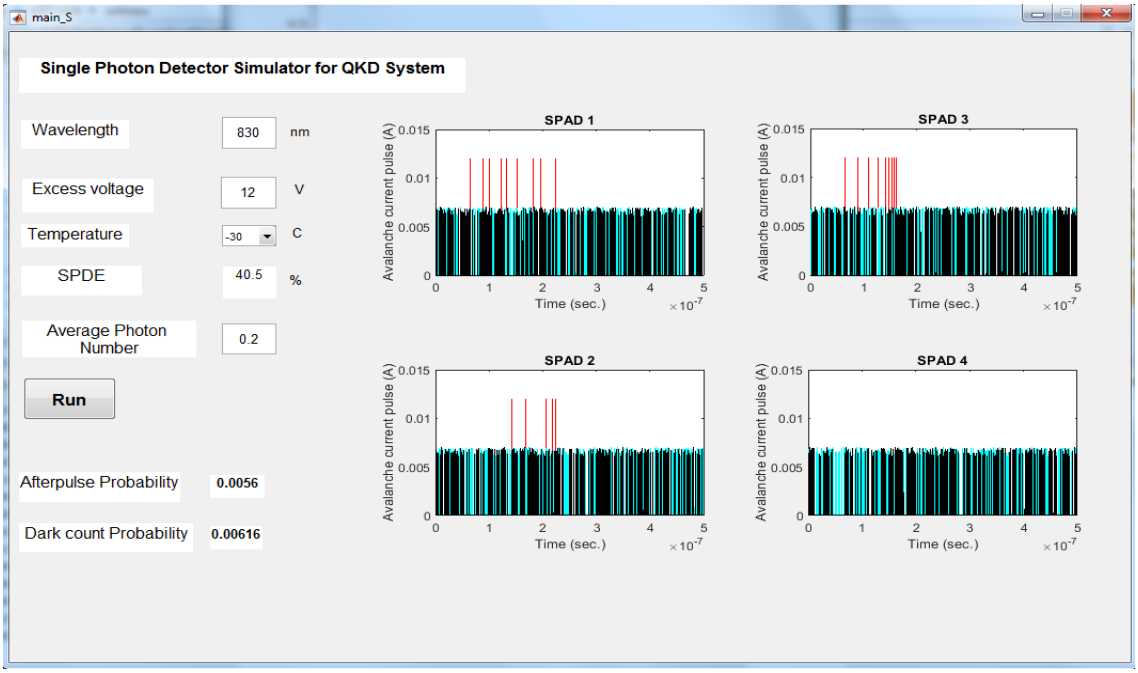


(c)

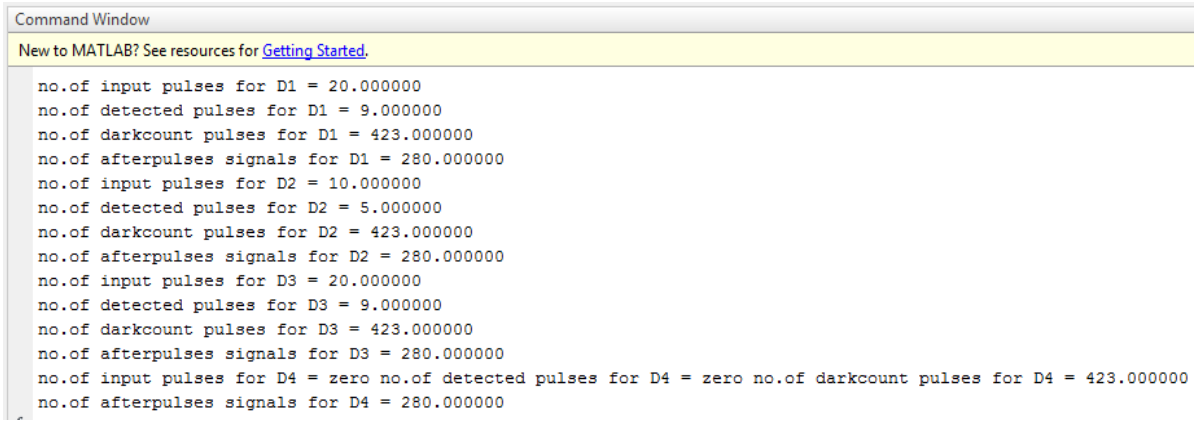
Fig.5.14 Experiment 3, Test 1 results (a) randomly generated bits and the corresponding optical pulses (b) SPADs GUI result (c) the numerical simulation results for V_{ex}=4V, Temperature=−20℃



(a)

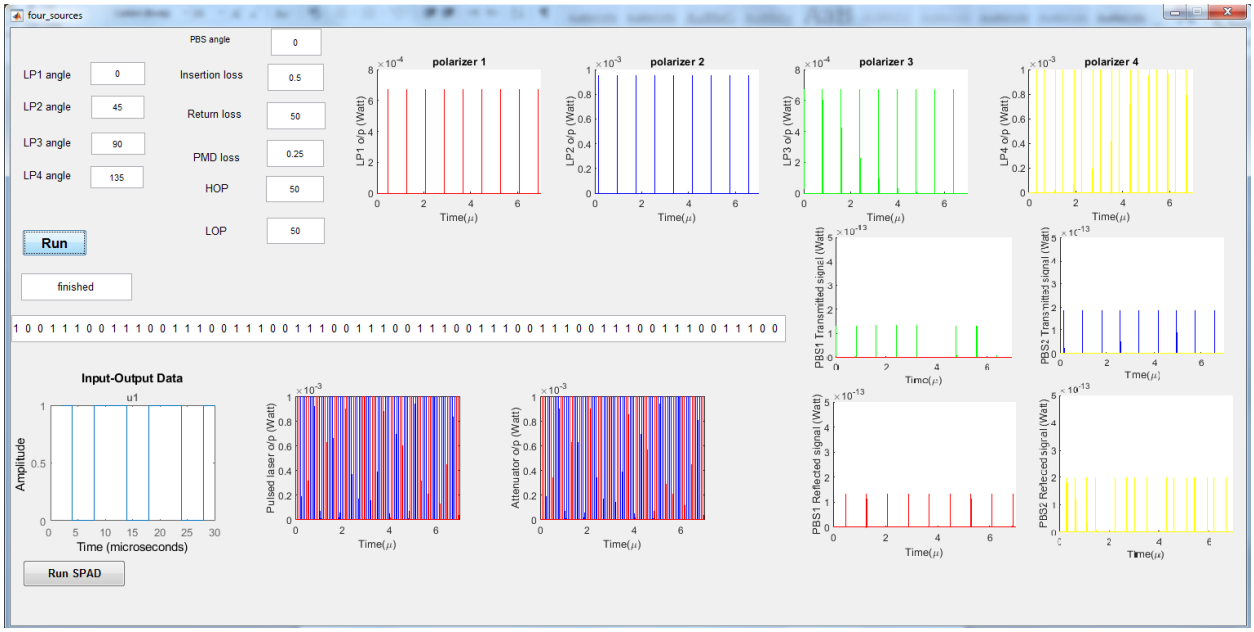


(b)

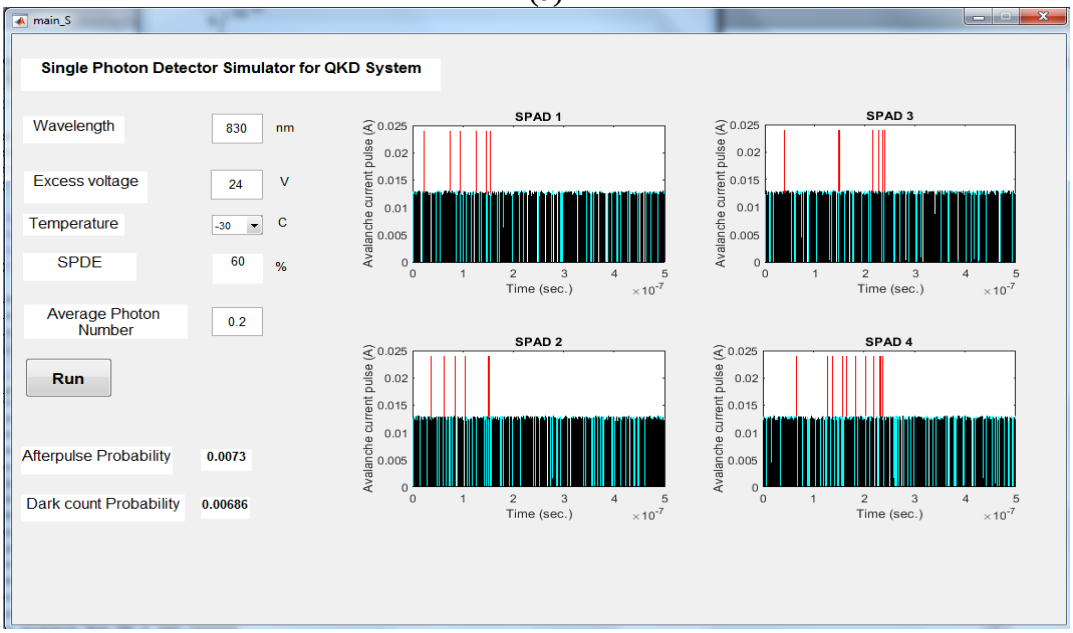


(c)

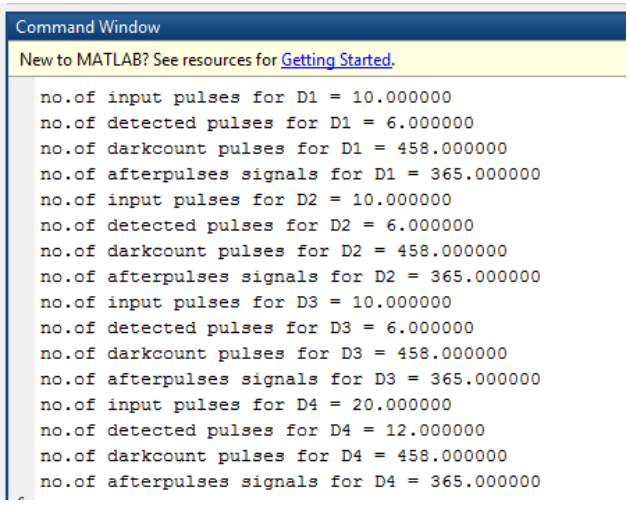
Fig.5.15 Experiment 3, Test 2 results (a) randomly generated bits and the corresponding optical pulses (b) SPADs GUI result (c) the numerical simulation results for V_{ex}=12V, Temperature=−30℃



(a)



(b)



(c)

Fig.5.16 Experiment 3, Test 2 results (a) randomly generated bits and the corresponding optical pulses (b) SPADs GUI result (c) the numerical simulation results for V_{ex}=24V, Temperature=−30℃

Tables (5.9-5.11) summarize the modeled system behavior tests using **Experiment 3** when 100 optical pulses are input to the system. These optical pulses are distributed to the four SPADs as follows,

SPAD 1 $\longrightarrow$ 20 input pulses

SPAD 2 $\longrightarrow$ 0 input pulses

SPAD 3 $\longrightarrow$20 input pulses

SPAD 4 $\longrightarrow$60 input pulses

The SPADs performance behavior was investigated for these optical pulses by changing V_{ex} that result in a variation of $SPDE$ which decides the performance of these SPADs.

Table 5.9 Summary of BB84 system behavior evaluation at temperature =−30℃ for Experiment 3.

		SPAD 1				SPAD 2				SPAD 3				SPAD 4			
V_{ex} (V)	$SPDE$ (%)	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts
2	9	20	2	230	95	0	0	230	95	20	2	230	95	60	6	230	95
4	17	20	4	305	161	0	0	305	161	20	4	305	161	60	11	305	161
6	24	20	5	360	214	0	0	360	214	20	5	360	214	60	15	360	214
8	30	20	6	380	240	0	0	380	240	20	6	380	240	60	18	380	240
10	36	20	8	410	261	0	0	410	261	20	8	410	261	60	22	410	261
12	41	20	9	423	280	0	0	423	280	20	9	423	280	60	25	423	280
14	45	20	9	428	296	0	0	428	296	20	9	428	296	60	27	428	296
16	48	20	10	435	315	0	0	435	315	20	10	435	315	60	30	435	315
18	52	20	11	437	326	0	0	437	326	20	11	437	326	60	32	437	326
20	55	20	11	443	335	0	0	443	335	20	11	443	335	60	33	443	335
22	58	20	12	449	350	0	0	449	350	20	12	449	350	60	35	449	350
24	60	20	12	458	365	0	0	458	365	20	12	458	365	60	36	458	365
26	62	20	13	470	375	0	0	470	375	20	13	470	375	60	38	470	375
28	64	20	13	447	385	0	0	447	385	20	13	447	385	60	39	447	385
30	65	20	13	483	396	0	0	483	396	20	13	483	396	60	39	483	396

Table 5.10 Summary of BB84 system behavior evaluation at temperature =−20℃ Experiment 3.

		SPAD 1				SPAD 2				SPAD 3				SPAD 4			
V_{ex} (V)	$SPDE$ (%)	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts
2	9	20	2	235	95	0	0	235	95	20	2	235	95	60	6	235	95
4	17	20	4	326	161	0	0	326	161	20	4	326	161	60	11	326	161
6	24	20	5	390	214	0	0	390	214	20	5	390	214	60	15	390	214
8	30	20	6	435	240	0	0	435	240	20	6	435	240	60	18	435	240
10	36	20	8	470	261	0	0	470	261	20	8	470	261	60	22	470	261
12	41	20	9	489	280	0	0	489	280	20	9	489	280	60	25	489	280
14	45	20	9	503	296	0	0	503	296	20	9	503	296	60	27	503	296
16	48	20	10	511	315	0	0	511	315	20	10	511	315	60	30	511	315
18	52	20	11	511	326	0	0	511	326	20	11	511	326	60	32	511	326
20	55	20	11	512	335	0	0	512	335	20	11	512	335	60	33	512	335
22	58	20	12	515	350	0	0	515	350	20	12	515	350	60	35	515	350
24	60	20	12	516	365	0	0	516	365	20	12	516	365	60	36	516	365
26	62	20	13	518	375	0	0	518	375	20	13	518	375	60	38	518	375
28	64	20	13	520	385	0	0	520	385	20	13	520	385	60	39	520	385
30	65	20	13	521	396	0	0	521	396	20	13	521	396	60	39	521	396

Table 5.11 Summary of BB84 system behavior evaluation at temperature =−10℃ Experiment 3.

		SPAD 1				SPAD 2				SPAD 3				SPAD 4			
V_{ex} (V)	$SPDE$ (%)	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts	I/P pulses	Detected pulses	Dark counts	Afterpulsing counts
2	9	20	2	268	95	0	0	268	95	20	2	268	95	60	6	268	95
4	17	20	4	382	161	0	0	382	161	20	4	382	161	60	11	382	161
6	24	20	5	469	214	0	0	469	214	20	5	469	214	60	15	469	214
8	30	20	6	536	240	0	0	536	240	20	6	536	240	60	18	536	240
10	36	20	8	589	261	0	0	589	261	20	8	589	261	60	22	589	261
12	41	20	9	617	280	0	0	617	280	20	9	617	280	60	25	617	280
14	45	20	9	643	296	0	0	643	296	20	9	643	296	60	27	643	296
16	48	20	10	660	315	0	0	660	315	20	10	660	315	60	30	660	315
18	52	20	11	675	326	0	0	675	326	20	11	675	326	60	32	675	326
20	55	20	11	686	335	0	0	686	335	20	11	686	335	60	33	686	335
22	58	20	12	695	350	0	0	695	350	20	12	695	350	60	35	695	350
24	60	20	12	695	365	0	0	695	365	20	12	695	365	60	36	695	365
26	62	20	13	699	375	0	0	699	375	20	13	699	375	60	38	699	375
28	64	20	13	701	385	0	0	701	385	20	13	701	385	60	39	701	385
30	65	20	13	703	396	0	0	703	396	20	13	703	396	60	39	703	396

As a conclusion, the collected results prove that the simulation of the initial implementations of the proposed system met the desired system behavior.

5.3 QKD System Simulator with a Demonstration of BB84 Protocol

In this section, the final stage of the QKD system simulator which is constructed by the electrical and optical physical components that have been modeled in this research work will be presented and investigated in terms of the execution of the complete BB84 protocol steps with consideration of the system performance by estimating $QBER_{sk}$, $QBER_{spd}$, KEY_{raw} and final secure key after error correction and privacy amplification for the following cases,

1. The randomness in the polarization at the BS component.
2. OF quantum channel imperfections such as the polarization rotation and attenuation.
3. FS quantum channel losses due to atmospheric effects and diffraction attenuation.
4. The influence of the SPD performance parameters.

Figure (5.17) illustrates the main simulator GUI. It is divided into two parts; the main part contains the experimental setup for demonstration of the BB84 protocol. Each physical component in this setup is enhanced by a configuration window to configure the component specifications and operation conditions as shown in Figure (5.18). The second part is the overview tab that shows the most important outcomes obtained from simulation of BB84 steps. The component configuration windows send the system parameters as inputs from the user to the Matlab processing unit. After code excution, the colected results are passed to the statistics and overview tab for presentation. The initial data from Alice and Bob in addition to

the generated final secure key can be saved in external files to be used later for data encryption.

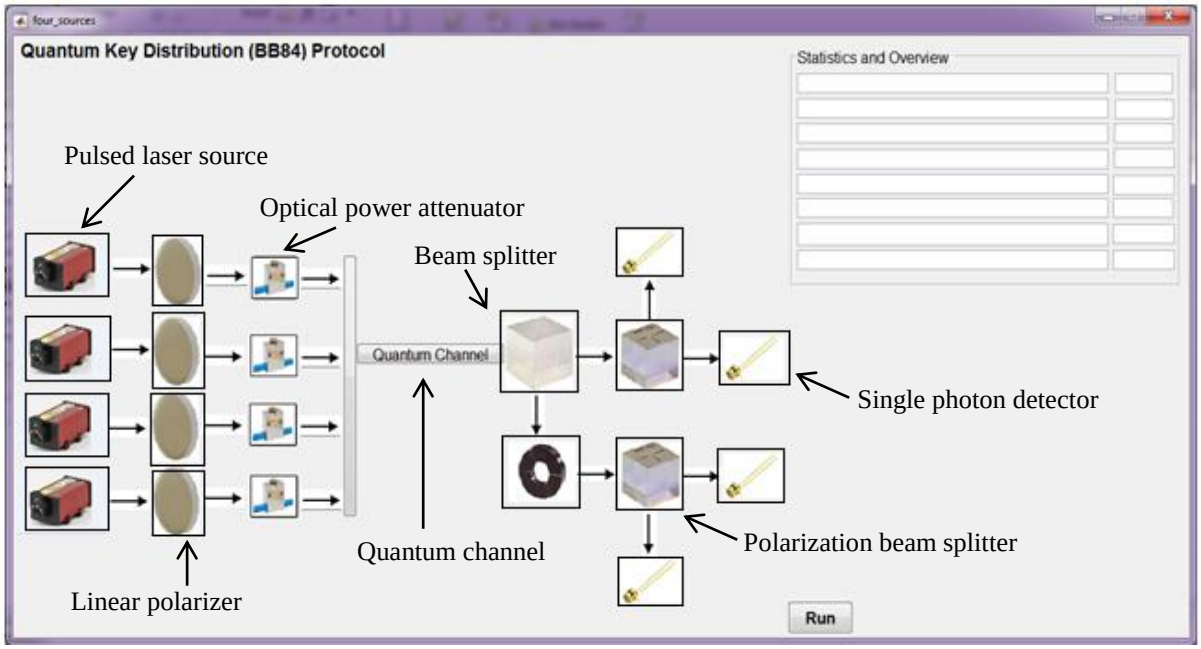


Fig.5.17 BB84 simulator main window

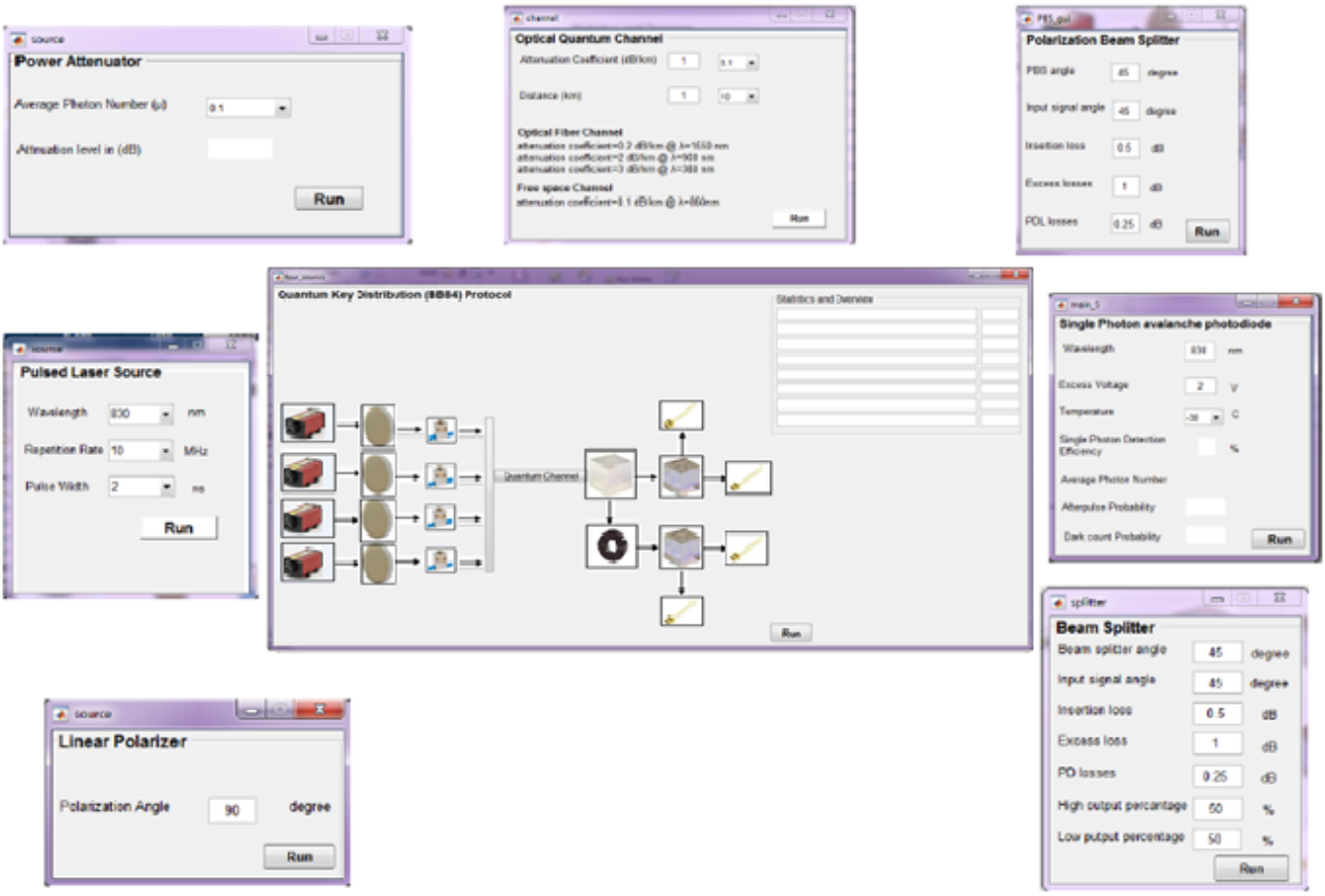


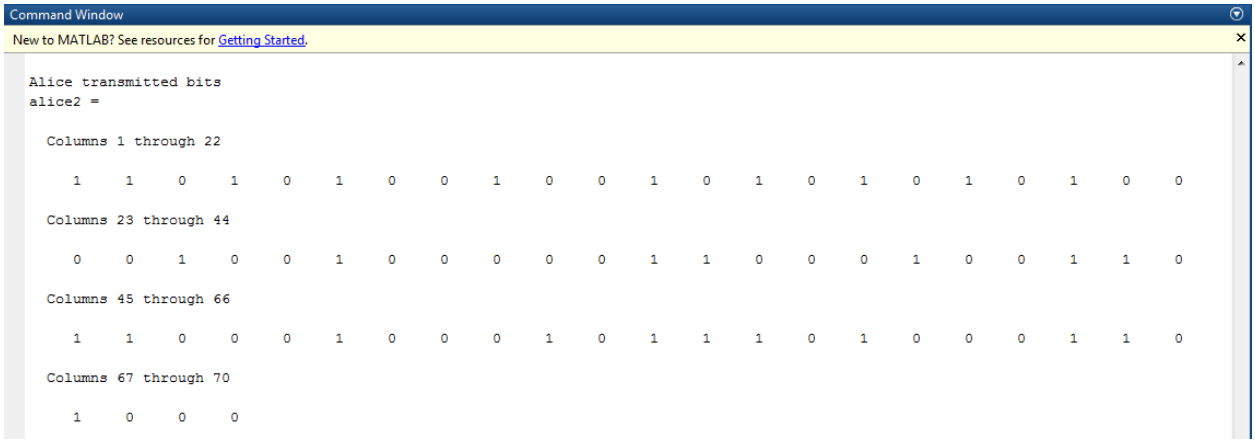
Fig.5.18 BB84 simulator configuration windows

5.3.1 Investigation of BB84 protocol steps

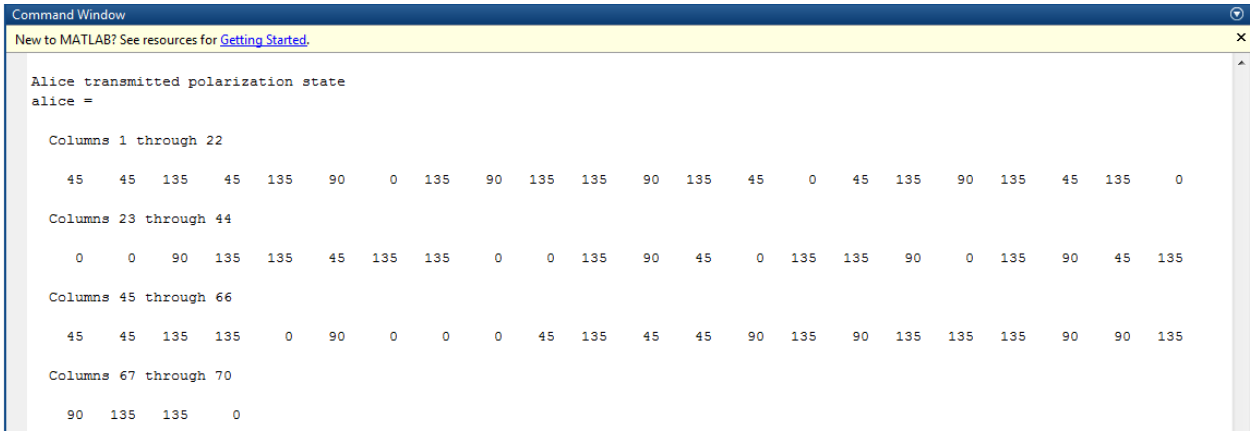
A simulation test is considered to demonstrate the simulator operation to execute the BB84 protocol steps. After a successful simulation, the resultant data consists of the secure key in addition to the estimated $QBER_{sk}$.

The simulation example assumes that Alice sends a sequence of 100 bits to Bob through a quantum channel with randomly chosen polarization basis and states. The procedure of comparing the bases of Alice and Bob is presented, where this comparison procedure is done for each detection of a photon with discarding the blank counts if they exist (when the detectors do not respond to the incident photons). In this test, $SPDE$ is set to 70%. Thus, 70 bits out of 100 bits sent by Alice will be detected.

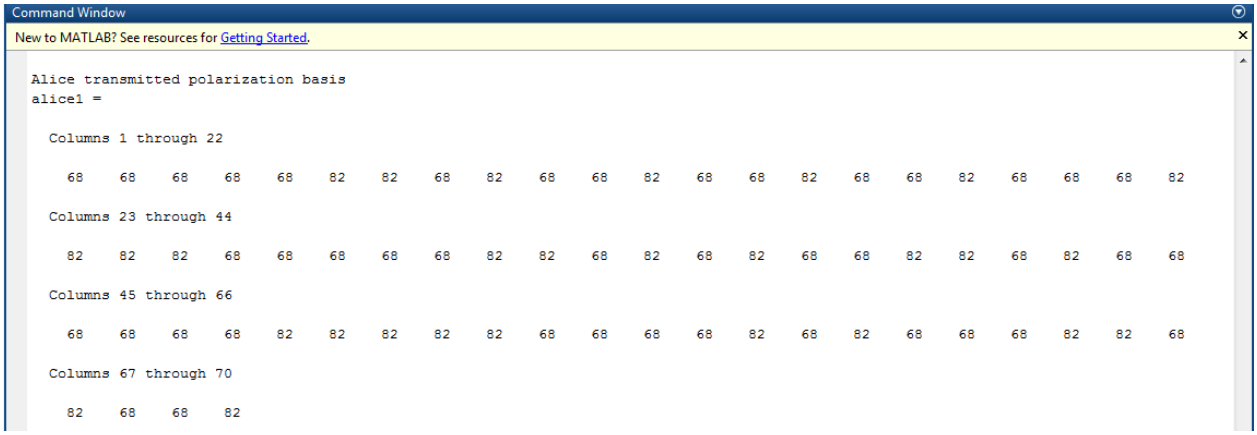
Figure (5.19) illustrates Alice transmitted bits, the corresponding polarization states and finally the associated polarization basis. Rectilinear polarization basis was coded as (68) while, a diagonal polarization basis was coded as (82).



(a)



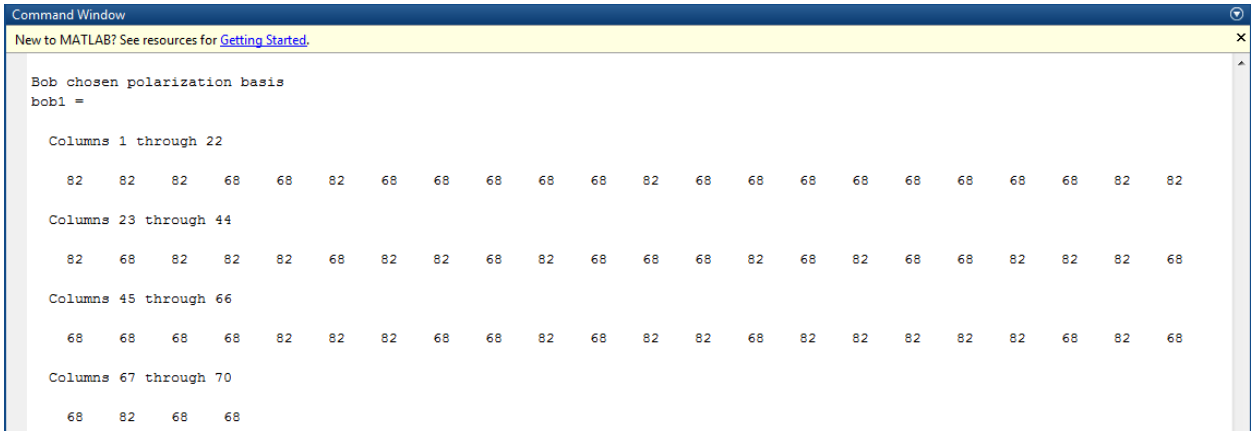
(b)



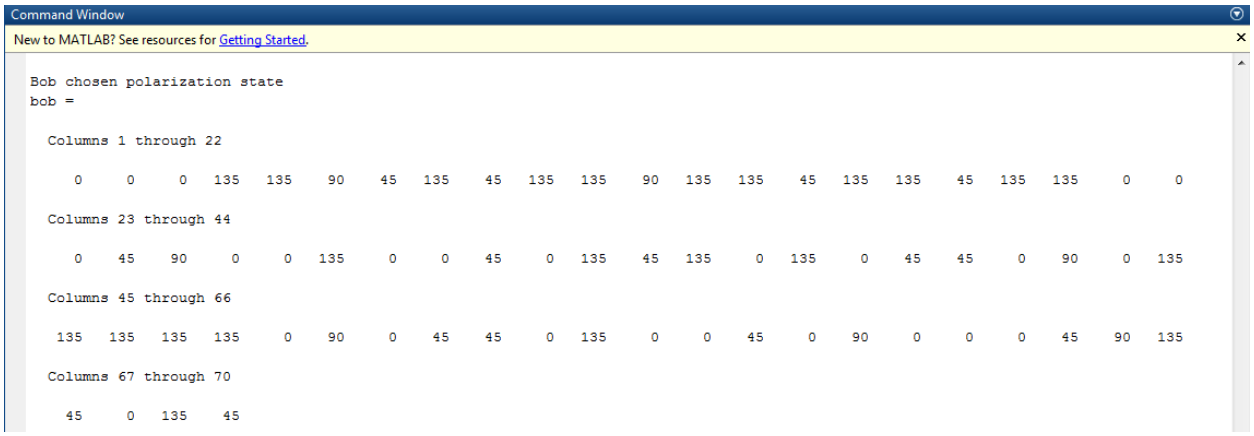
(c)

Fig.5.19 Alice data (a) transmitting bits (b) polarization states (c) polarization bases

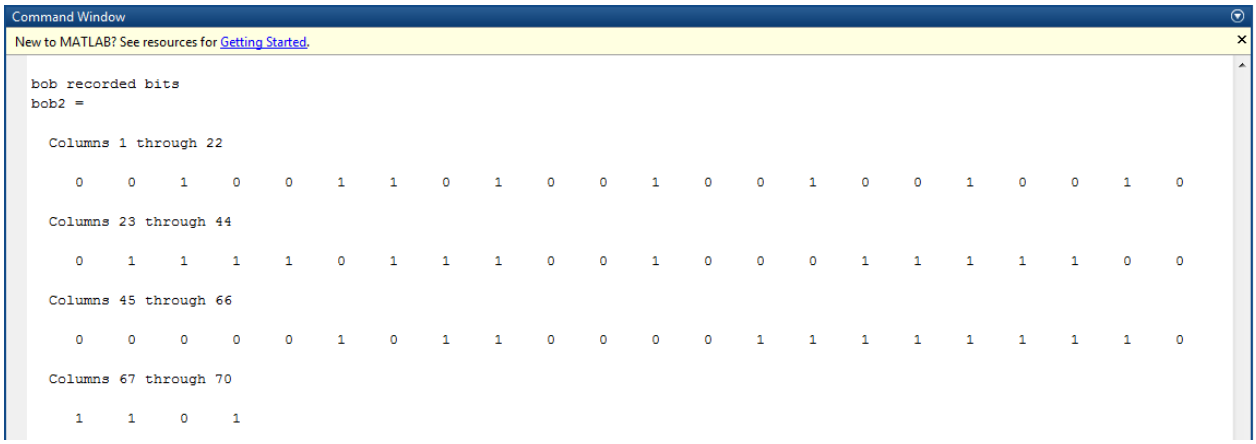
Bob randomly chooses either (68) or (82) basis and records the corresponding bits as shown in Figure (5.20).



(a)



(b)



(c)

Fig.5.20 Bob data (a) polarization bases (b) polarization states (c) recorded bits

Alice and Bob declare and exchange their choice of basis but not the result via a public channel. Bits with different bases are rejected as shown in Figure (5.21) which illustrates the 34 discarded bases locations.

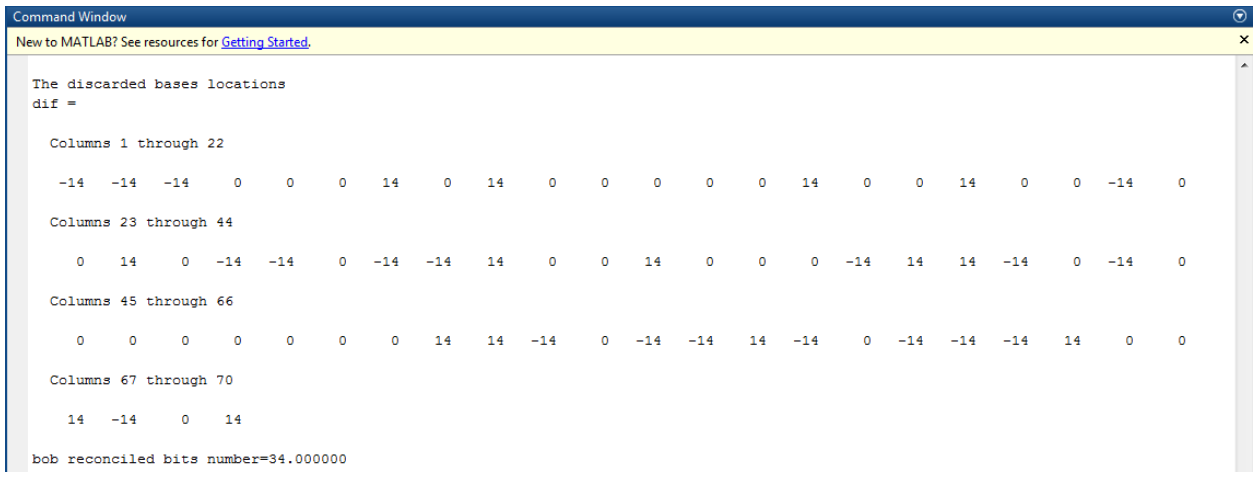


Fig.5.21 Discarded bits locations after Alice and Bob declaration process where −14 and 14 represent the different bases comparision results

After these steps, the sifted key is obtained which is equal to 36 bits as shown in Figure (5.22) then followed by error estimation procedure by calculating $QBER_{sk}$ which is equal to 48.571 %. At the end of the sifting step, the initial bits decreased from 100 to 36 bits.

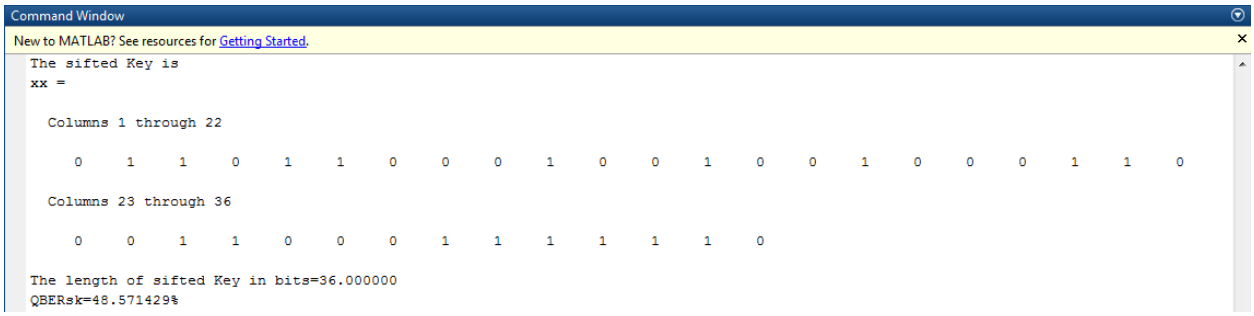


Fig.5.22 Registered sifted key and the $QBER_{sk}$

Due to errors presented in the sifted key, classical error correction procedure can be utilized by randomly redistribute the remaining 36 bits as shown in Figure (5.23) which represents the randomly redistribution of the bits locations. After error correction step, 36 bits key length reduced to 13 bits. Error correction will be followed by Privacy Amplification step to reduce any leakage information to an arbitrary low value, the final secure key length at Alice and Bob is 7 bits.

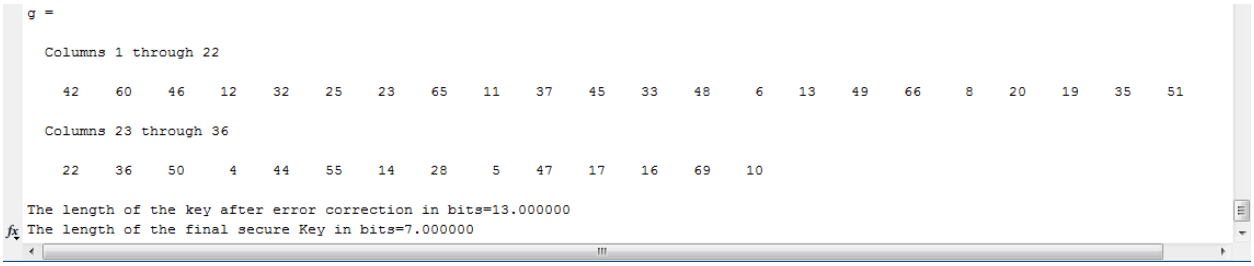


Fig.5.23 Registered key length after error correction and PA

5.3.2 Investigation of QKD simulator based on BB84 protocol

In this sub-section, the performance analysis of the simulator to simulate BB84 system using OF and FS quantum channels and calculating the $QBER_{spd}$ and final KEY_{raw} will be studied.

5.3.2.1 Investigation of the system performance under the effect of quantum channel imperfections and losses.

In this sub-section, the designed simulator ability to simulate the BB84 protocol will be tested in terms of choosing the appropriate system parameters, simulation of BB84 protocol to investigate the keys after each step of the protocol, KEY_{raw} $QBER_{sk}$ and $QBER_{spd}$ calculation. Figures (5.24-5.27) show the detailed information collected from four tests when reacting to 1000 bits taking into consideration the system experimental parameters such as PRR, λ, channel length and the operation conditions such as the imperfections in the OF channel and FS channel noise effects in addition to the SPDs issues i.e. DCR, V_{ex} and $SPDE$. For all tests, N_0=0.2.

Table 5.12 reports the simulator configuration parameters that have been changed for the four tests.

Table 5.12 QKD simulator configuration parameters for BB84 protocol

Parameter / Test No.	λ (nm)	L (Km)	PRR (MHz)	V_{ex} (V)	Temperature (℃)	Resultant $SPDE$ (%)
Test 1	830	20	10	10	−30	36
Test 2	860	40	2	16	−20	48
Test 3	900	60	1	22	−10	57.5
Test 4	1550	100	0.1	30	−10	65

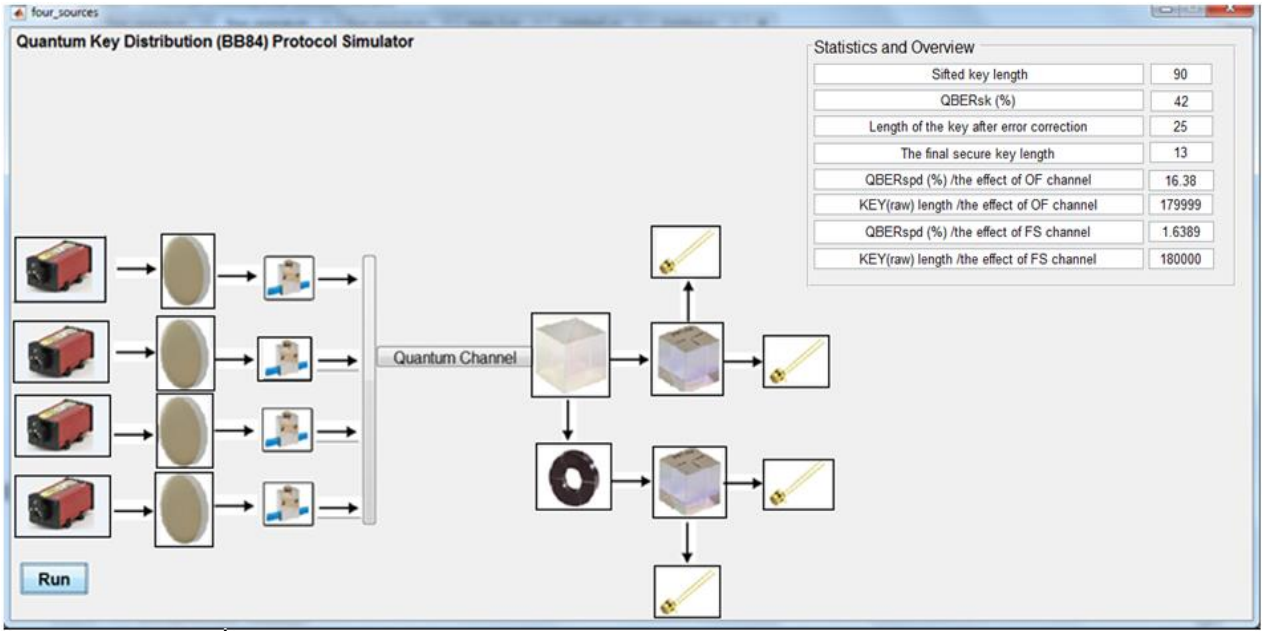


Fig.5.24 BB84 simulator Test1 results

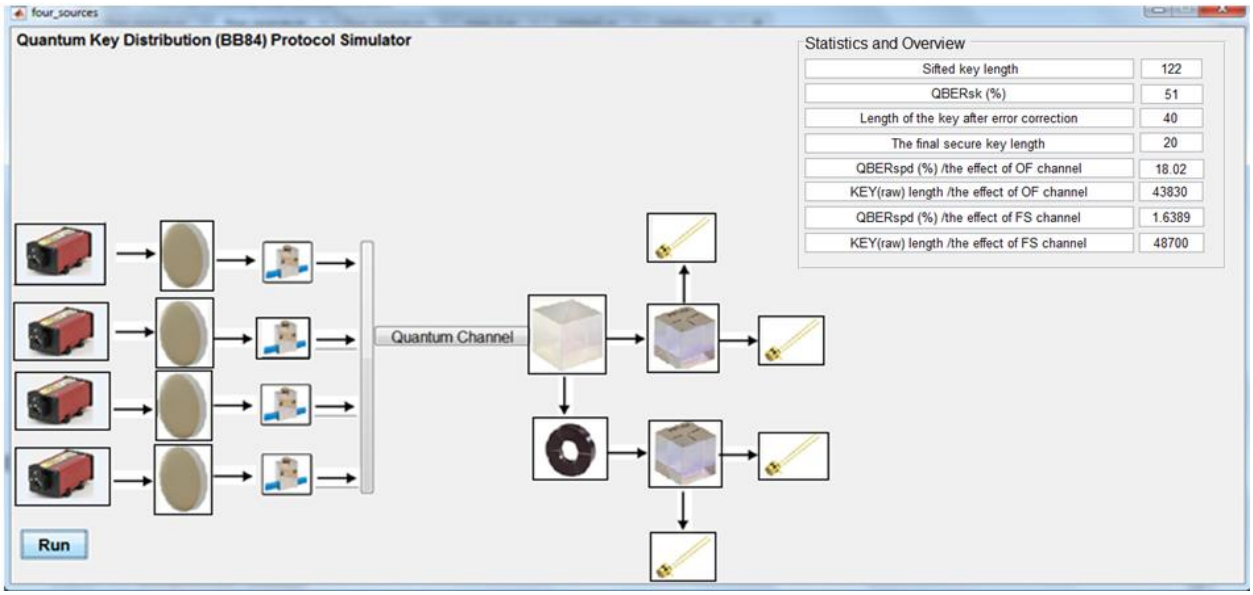


Fig.5.25 BB84 simulator Test2 results

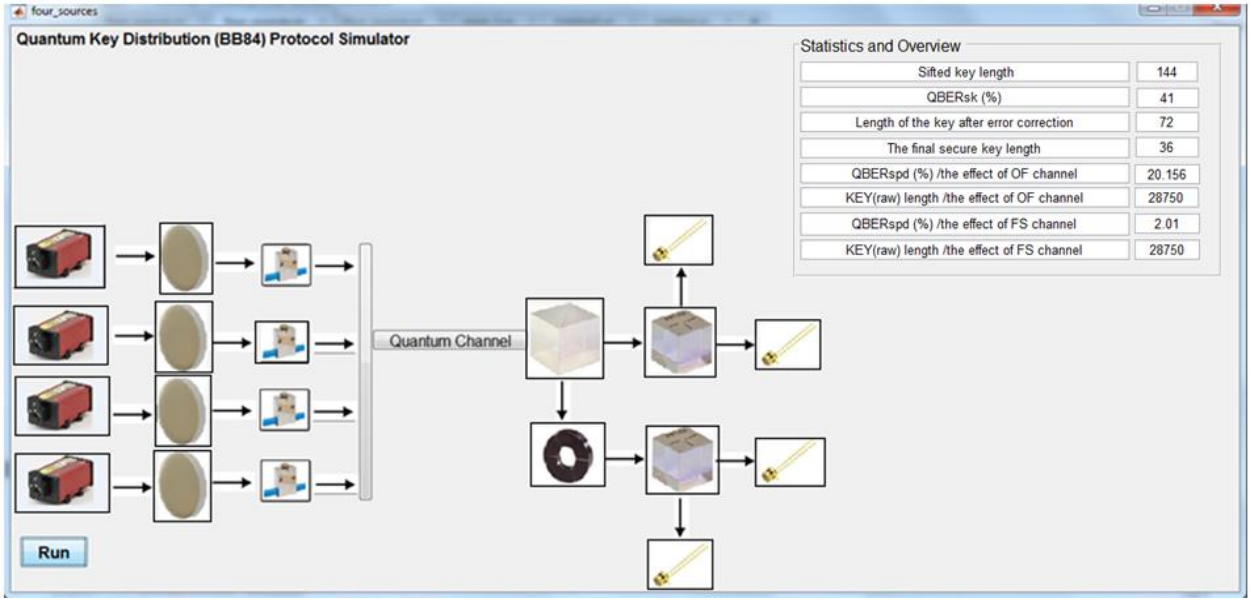


Fig.5.26 BB84 simulator Test3 results

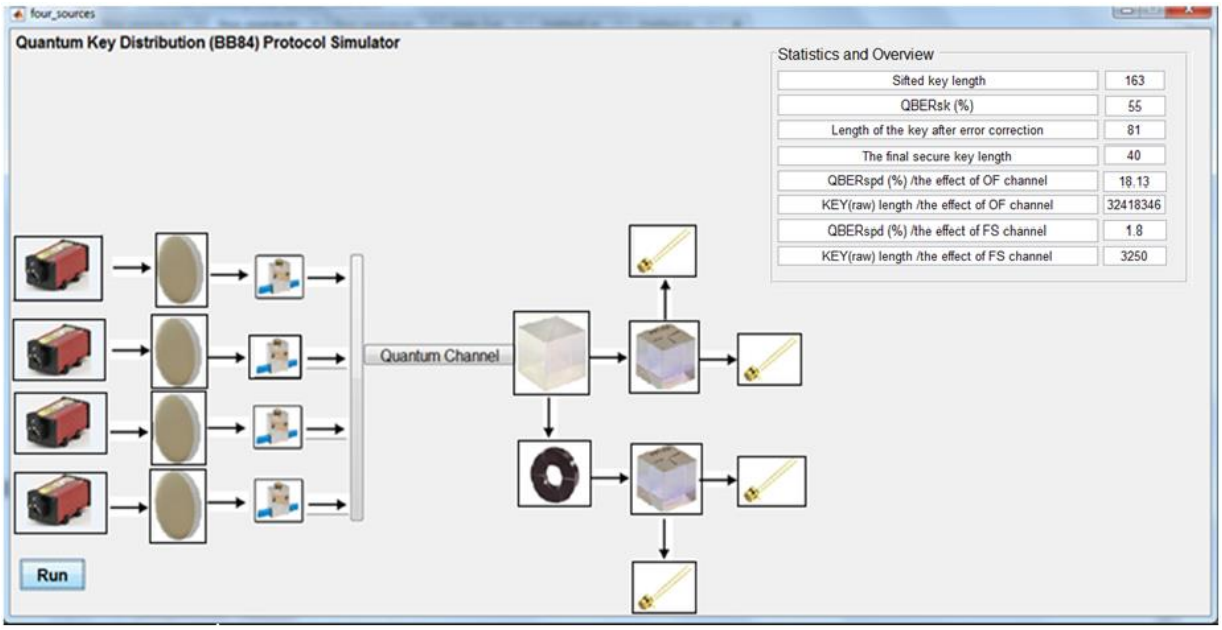


Fig.5.27 BB84 simulator Test4 results

5.3.2.2 Investigation of the system performance under the effect of the polarization rotation

The effect of the random polarization rotation for the optical pulses travelled inside the OF link will be explained in terms of investigating the system $QBER_{sk}$. The setup that has been used in **Test 1** (sub-section 5.3.2.1) is used in this experiment. 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 ($0° \rightarrow 45°$).

Table (5.13) summarizes the amount of the polarization rotation in degree that have 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 5.13 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

5.3.2.3 Investigation and analysis of system parameters using the designed simulator

Three simulation studies have been conducted to analyze the BB84 system performance in terms of KEY_{raw} and $QBER_{spd}$ under different simulation conditions. The following simulation results were collected after running the simulator with 5000 input bits.

Simulation study 1

The objective of this study is to understand the performance of the system while considering the effect of SPAD temperature for different operation wavelengths. Table 5.14 shows the main simulation input parameters that were used in simulation study 1.

Table 5.14 simulation study 1 input parameters

Parameter	Value
λ	830nm, 860nm, 900nm
PRR	2 MHz
N_0	0.1
T	$-30°$ C,$-20°$ C,$-10°$ C

Figure (5.28) shows the registered $QBER_{spd}$ to identify the performance of the system under the influence of increasing the ambient temperature. As the temperature increases, the system performance degrades due to the enhancement of the dark counts inside the SPAD components. As a conclusion, the SPADs are considered as the main noise source within the system that increases the $QBER_{spd}$ and thus the communication distance is reduced. At λ=900nm and λ=860nm, a significant degradation in performance can be seen compared to λ=830nm due to high dark counts values that have been registered.

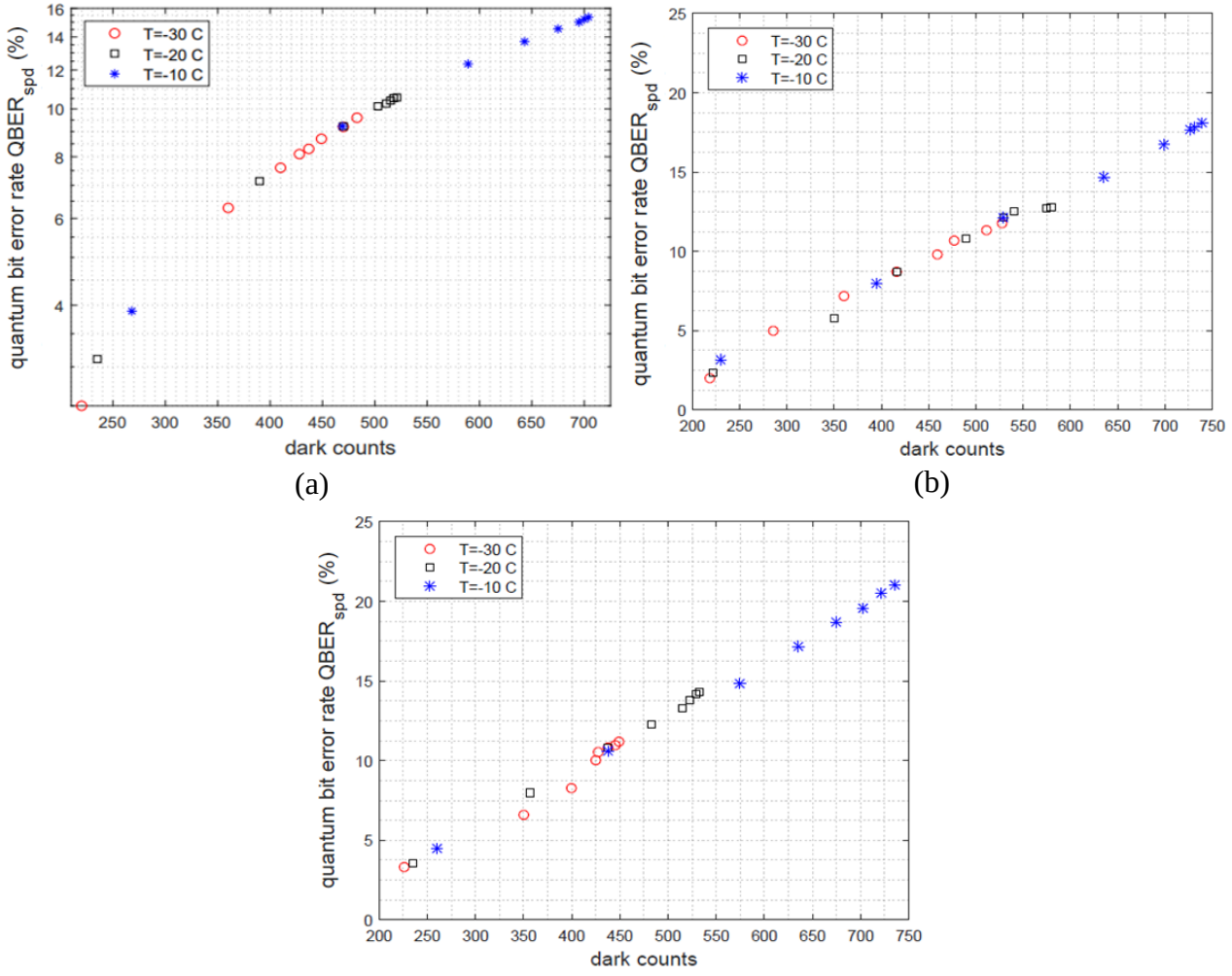


Fig.5.28 $QBER_{spd}$ (%) vs. dark counts (a) λ=830nm (b) λ=860nm (c) λ=900nm

Simulation study 2

The objective of this study is to investigate the effect of the SPAD $SPDE$ on the number of bits for BB84 system for different operation wavelengths. Figure (5.29) illustrates the number of bits after each step of the protocol as a function of the SPAD $SPDE$ using the same simulation parameters as simulation study 1 at Temperature equal to $-30\text{C}°$. The number of the distributed bits between Alice and Bob are increased as $SPDE$ is improved which leads to detection the largest possible number of the transmitted optical pulses from Alice.

Increasing the number of the distributed keys at λ=830 nm is due to that the SPADs have high $SPDE$ values at this λ.

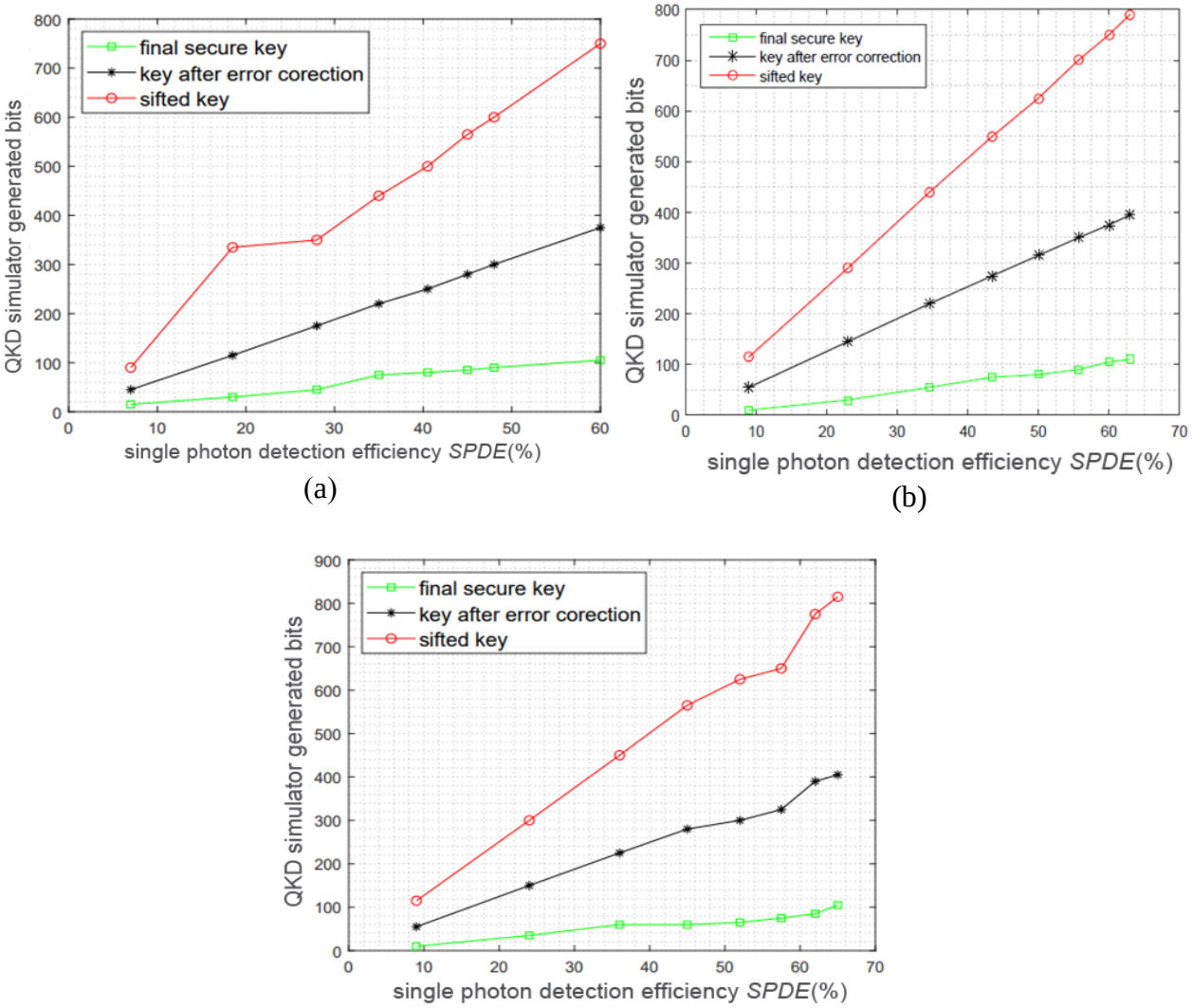


Fig.5.29 The number of the generated bits vs. *SPDE* (%) (a) λ=900nm (b) λ=860nm (c) λ=830nm

Figure (5.30) represents the generated bits vs. $SPDE$ using SNSPD as detection component. Table 5.15 shows the main simulation input parameters that were used in this simulation study.

Table 5.15 simulation study 2 input parameters

Parameter	Value
λ	1550nm, 900nm
PRR	2 MHz
N_0	0.1
T	$4K$
I_b	9.8μA, 8μA

As SNSPD improves the system's performance compared to SPAD, the length of the shared keys between Alice and Bob will be

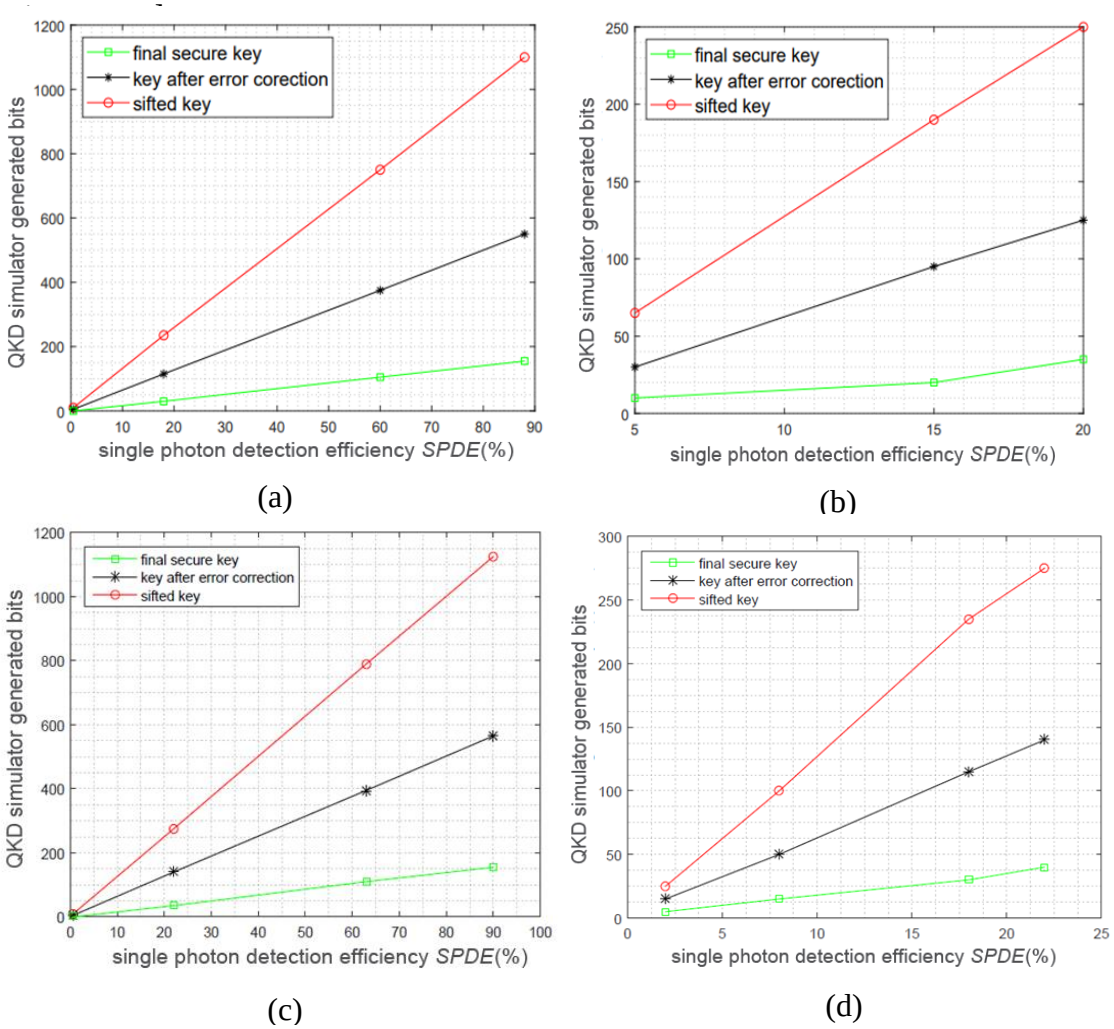


Fig.5.30 The number of the generated bits vs. $SPDE$ (%) (a) λ=1550nm, I_b=9.8μA (b) λ=1550nm,I_b=8μA (c) λ=900nm,I_b=9.8μA (d) λ=900nm,I_b=8μA

Simulation study 3

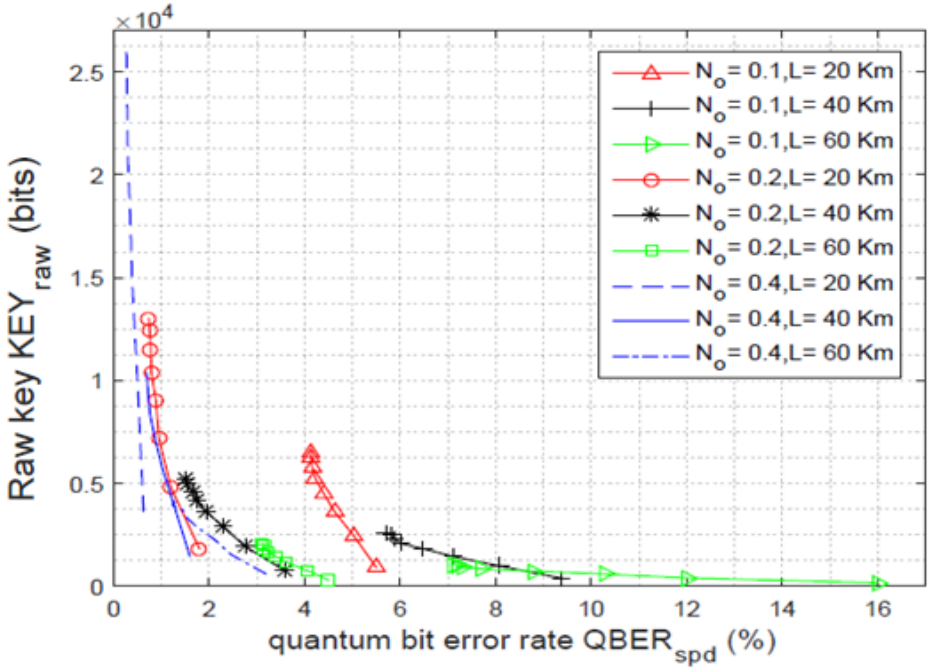
This study is conducted to examine the relation between the performance of the system with different system parameters.

Figure (5.31) illustrates the influence of the system parameters e.g.N_0,L, PRR and the Temperature on the system's performance represented by $QBER_{spd}$ and the generated KEY_{raw}. 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 5.16 shows the main simulation input parameters that were used in simulation study 3.

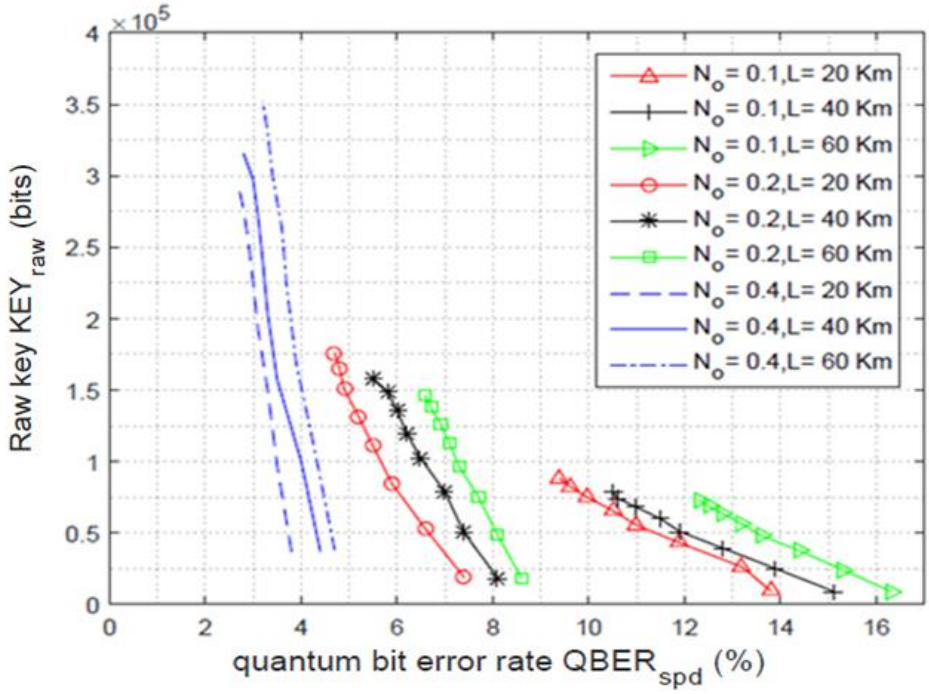
Table 5.16 simulation study 3 input parameters

Parameter	Value
λ	1550nm, 860nm
PRR	0.1 MHz, 2 MHz, 5 MHz
N_0	0.1, 0.2, 0.4
T	$-30°$ C, $-20°$ C, $-10°$ C
L	20 km, 40 km, 60 km,

The obtained results indicate that 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 $QBER_{spd}$ as the channel length increased. 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 due to the exchanged KEY_{raw} is small compared to N_0= 0.2 and 0.4.



(a)



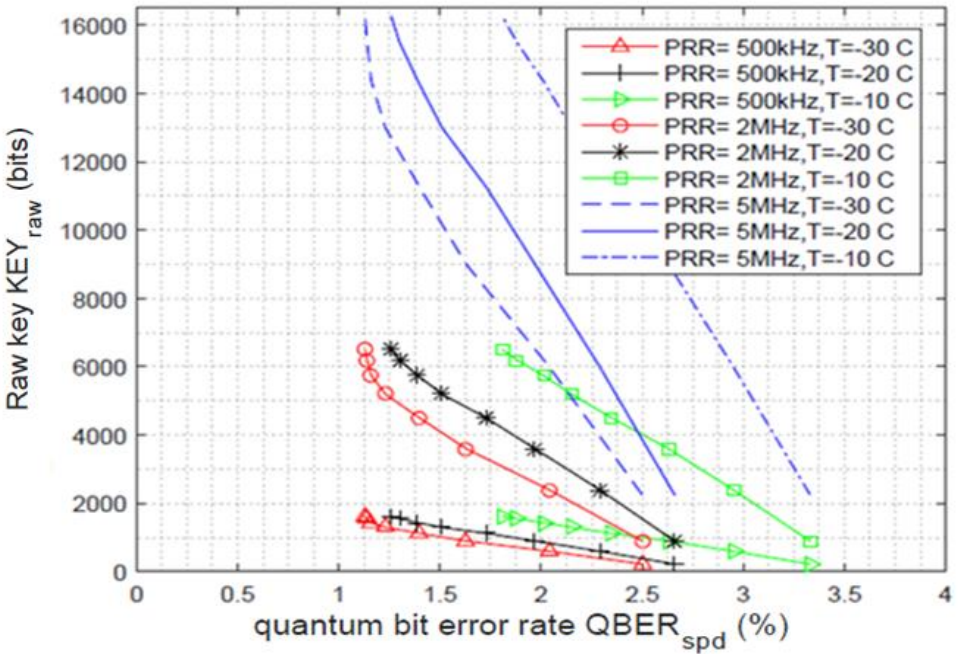
(b)

Fig.5.31 KEY_{raw} vs. $QBER_{spd}$ (%) at different L and N_0

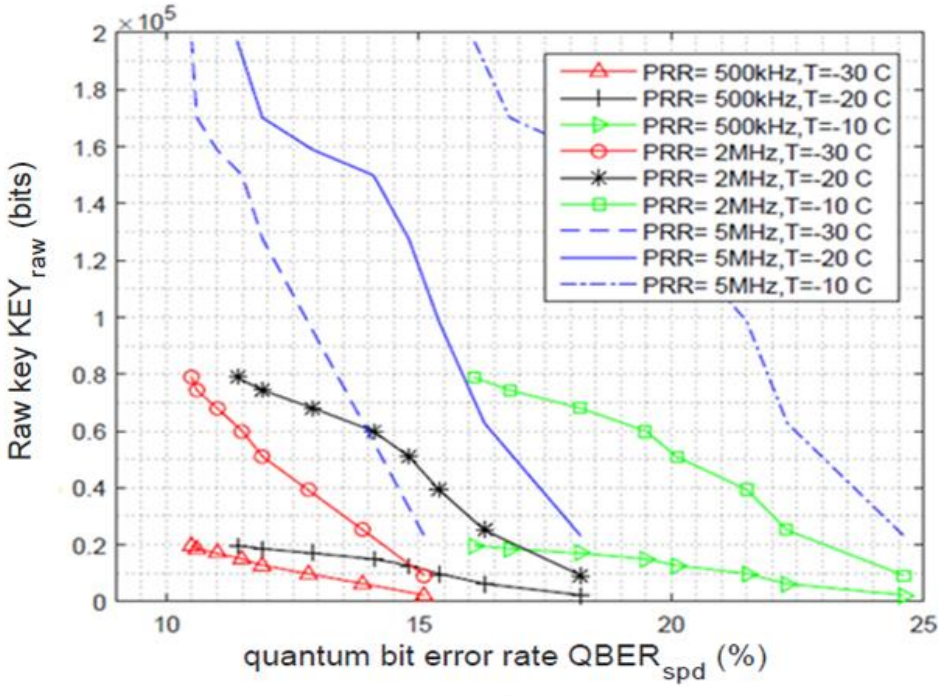
(a) λ=1550nm (b) λ=860nm

Figure (5.32) illustrates the effect of varying the temperature of the SPAD on the system's performance as well as the impact of *PRR* on the KEY_{raw} length and $QBER_{spd}$. At $-30°$ C and $-20°$ C, the system

performance doesn't change significantly. At $-10°$ C, the performance degrades dramatically by increasing $QBER_{spd}$. This drop in the performance is caused by high DCP values that have been registered through SPAD characterization which as a result increases the number of dark counts. This figure also shows the dependence of the KEY_{raw} length on PRR. At 5 MHz, a maximum KEY_{raw} count is obtained compared to 2 MHz and 500 kHz.



(a)



(b)

Fig.5.32 KEY_{raw} vs. $QBER_{spd}$ (%) at different PRR and T

(a) λ=1550nm (b) λ=860nm

5.4 The Simulator Operation with a True Random Sequence

The simulator was tested by operating the four laser diodes at the transmitter by a true random sequence of bits based on photon arrival time registered in a coincidence window between two single-photon counting modules. This true random signal was generated through M.Sc. project [35] in Quantum Optics and Electronics Group at the Institute of Laser for Postgraduates Studies. The true random sequence was fed as an external file to the sequence generator at the transmitter.

The simulator was tested for the parameters listed in Table (5.17),

Table 5.17 The simulator parameters for BB84 protocol with a true random sequence

Parameter	value
No.of input bits	5000
λ	900nm
PRR	2 MHz
V_{ex}	30 V
T	$-30°$ C
L	10 km
N_o	0.1

A final secure key for the BB84 protocol obtained from the simulator operation was obtained with $QBER_{sk}$ of 41 (%) and $QBER_{spd}$ of 20(%). Figure (5.33) shows a sample of the text file for the key obtained.

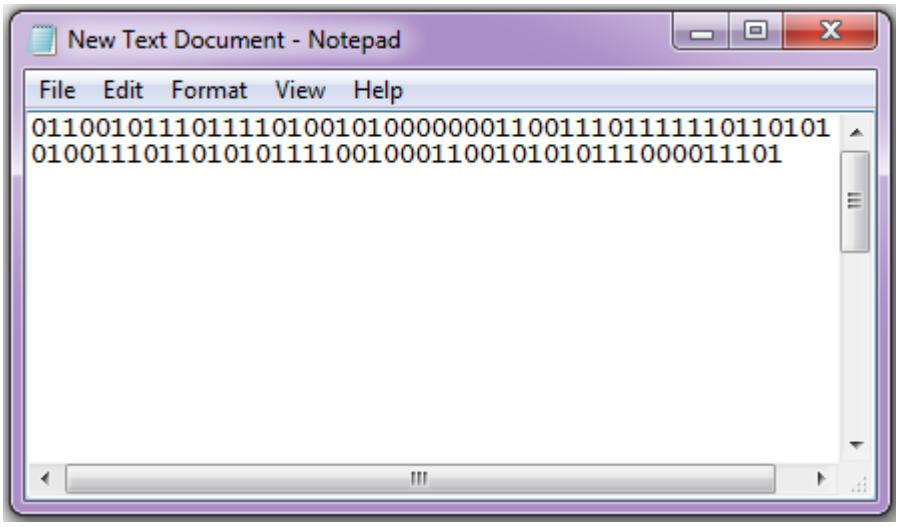


Fig.5.33 final secure key obtained from the simulator operation with a true random sequence

For all presented studies that considered the BB84 protocol experimental issues and problems, the designed simulator was able to simulate the BB84 protocol and provides predictions about the shared keys through the overall protocol steps as well as the KEY_{raw} $QBER_{sk}$ and $QBER_{spd}$ that show a good agreement in the performance and operation with the reported results in literature.

5.5 Limitations and Challenges

In this subsection, the main limitations and challenges throughout the research period will be reported:

1) Matlab as a simulation environment is an interpreted language and, therefore, may execute more slowly than compiled programming language. In addition, its GUI doesn't support drag and drop action.
2) Due to limitations in the available PC hardware, the generated pseudo random sequence was limited to 5000 bits with acceptable processing time and as a result the extracted final secure key rate was short in length.

3) Limited number of registered true and dark counts due to limitation in the SPDs count rate because of their dead time.
4) Only three optical wavelengths are examined (830, 900 and 1550 nm) because the modeled SPDs have maximum detection efficiency at these wavelengths.
5) In this research, the allowable OF channel length is limited up to 150 km as recommended in the literature.
6) The continuous time domain simulation approach that was utilized in this work was time and computation consuming approach because thousands of optical pulses will be generated and transmitted through the system's components.
7) This work is only an approximation of the ideal apparatus described in theory because it is impossible to build the ideal system described in theory.
8) 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, single-photon detectors operation and the behavior of complex interacting QKD software process present within a QKD system.
9) In this research, it was important to increase the level of details of the modeled system components and processes that are critical to the system under study. For example, simulating the SPDs probabilistic behavior of registering true detected signals and dark counts in addition to the randomness in the operation of the BS component which represents the heart of any QKD system.

Chapter Six

Conclusions and Future Work

Chapter Six

Conclusions and Future Work

6.1 Conclusions

In this research project, a modeling tool of a QKD-BB84 practical set-up was implemented and tested. All the required components to implement this protocol are taken into consideration starting from the transmitter module, OF and FS channels and receiver module. The operation conditions of the system, the system imperfections in addition to the information about all the modeled components characteristics which as a result allows the user to test actual QKD systems are taking into account.

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. The most remarkable result to emerge from the data is that the modeling process provides guidance for BB84- QKD system design and characterization. The simulator also operated successfully with a true random sequence that was fed to the transmitter by an external file.

It is possible to conclude that the simulation paradigm 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 research presents the superconducting nanowire single photon detector technique, integrates the free space channel model within this system and each component is supports with time domain plotters for

individual testing purpose which to the best of our knowledge, were not considered previously within other QKD simulators.

Finally, the validation and testing results of both the individual models separately and the complete BB84 protocol simulator showed acceptable results with the theoretical and experimental results reported in related references and the device's data sheets.

6.2 Future Work

The following points are recommended for further development of this work:

1. Including new abilities such as utilizing decoy states and modeling other QKD protocols such as MDI- QKD.
2. Checking the effect of eavesdropping on the system’s QBER by applying suitable attack methods.
3. Studying the effects of laser source parameters that affect the QKD system performance like line width.
4. The simulator model performance can be developed by using discrete event approach supported by more general programming languages such as C++ to increase the simulator model reality and performance.

References

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002, doi: 10.1103/revmodphys.74.145.

[2] G. R. H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, “Quantumcryptography,” *Appl. Phys.*, vol. 67, 1998.

[3] D. B. E. Zeilinger, *The Physics of Quantum Information*, 1st edition. Berlin, Heidelberg: Springer, 2000.

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992, doi: 10.1007/BF00191318.

[5] I. Stewart, “Schrödinger’s catflap,” *Nature*, vol. 353, no. 6343, pp. 384–385, 1991, doi: 10.1038/353384a0.

[6] G. W. Wolfgang Tittel, “Photonic Entanglement for Fundamental Tests and Quantum Communication,” *Quantum Inf. Comput.*, vol. 1, no. 2, pp. 3–56, 2001.

[7] B. Huttner, N. Imoto, N. Gisin, and T. Mor, “Quantum cryptography with coherent states,” *Phys. Rev. A*, vol. 51, no. 3, pp. 1863–1869, 1995, doi: 10.1103/PhysRevA.51.1863.

[8] 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.

[9] R. J. Hughes *et al.*, “Practical quantum cryptography for secure free-space communications,” *Proc. SPIE Int. Soc. Opt. Eng.*, vol. 3615, p. 98, 1999, doi: 10.1117/12.346170.

[10] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key

distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, p. 711, 2014, doi: 10.1016/j.tcs.2014.05.025.

[11] 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.

[12] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, p. 12326, 2005, doi: 10.1103/PhysRevA.72.012326.

[13] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental Quantum Key Distribution with Decoy States," *Phys. Rev. Lett.*, vol. 96, no. 7, 2006, doi: 10.1103/physrevlett.96.070502.

[14] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, 2012, doi: 10.1103/physrevlett.108.130503.

[15] M. T. D. Jennewein, "Quantum Communication and Teleportation Experiments using Entangled Photon Pairs," Wien University, 2002.

[16] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum Cryptography with Entangled Photons," *Phys. Rev. Lett.*, vol. 84, no. 20, pp. 4729–4732, 2000, doi: 10.1103/PhysRevLett.84.4729.

[17] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, "Entangled state quantum cryptography: eavesdropping on the ekert protocol.," *Phys. Rev. Lett.*, vol. 84, no. 20, pp. 4733–4736, May 2000, doi: 10.1103/PhysRevLett.84.4733.

[18] L. O. Mailloux *et al.*, "A Modeling Framework for Studying Quantum Key Distribution System Implementation Nonidealities,"

IEEE Access, vol. 3, pp. 110–130, 2015, doi: 10.1109/ACCESS.2015.2399101.

[19] 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.

[20] 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.

[21] S. Zhao and H. De Raedt, “Event-by-event Simulation of Quantum Cryptography Protocols.” 2007.

[22] M. Niemiec, Ł. Romański, and M. Świkety, “Quantum Cryptography Protocol Simulator,” in *Multimedia Communications, Services and Security*, 2011, pp. 286–292.

[23] L. J. Zhu, “A Simulation Platform for Quantum Key Distribution Protocol,” in *Information Technology for Manufacturing Systems III*, 2012, vol. 6, pp. 1078–1081, doi: 10.4028/www.scientific.net/AEF.6-7.1078.

[24] L. O. Mailloux *et al.*, “Quantum key distribution: examination of the decoy state protocol,” *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 24–31, 2015, doi: 10.1109/MCOM.2015.7295459.

[25] A. Buhari, Z. A. Zukarnain, R. Khalid, and W. J. A. Z. Dato\textquotesingle, “A Generic Simulation Framework for Non-Entangled based Experimental Quantum Cryptography and Communication: Quantum Cryptography and Communication Simulator ({QuCCs}),” *{IOP} Conf. Ser. Mater. Sci. Eng.*, vol. 160, p. 12095, 2016, doi: 10.1088/1757-899x/160/1/012095.

[26] M. Mehic, O. Maurhart, S. Rass, and M. Voznak, “Implementation of quantum key distribution network simulation module in the network simulator NS-3,” *Quantum Inf. Process.*, vol. 16, no. 10, p. 253, 2017, doi: 10.1007/s11128-017-1702-z.

[27] X. Mao, Y. Li, Y. Peng, and B. Zhao, “Security Analysis Oriented Physical Components Modeling in Quantum Key Distribution,” in *Mobile Internet Security*, 2018, pp. 154–163.

[28] S. Kuppam, “Modelling of Quantum Key Distribution Protocols in Communicating Quantum Processes Language with Verification and Analysis in PRISM,” *Proc. 8th Int. Conf. Simul. Model. Methodol. Technol. Appl.*, 2018, doi: 10.5220/0006834500750082.

[29] R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, “qkdSim, a Simulation Toolkit for Quantum Key Distribution Including Imperfections: Performance Analysis and Demonstration of the B92 Protocol Using Heralded Photons,” *Phys. Rev. Appl.*, vol. 14, no. 2, 2020, doi: 10.1103/physrevapplied.14.024036.

[30] S. Ali, S. Saharudin, and M. R. B. Wahiddin, “Quantum Key Distribution Using Decoy State Protocol,” *Am. J. Eng. Appl. Sci.*, vol. 2, no. 4 SE-Research Article, Dec. 2009, doi: 10.3844/ajeassp.2009.694.698.

[31] E. Desurvire, *Classical and Quantum Information Theory: An Introduction for the Telecom Scientist*. Cambridge: Cambridge University Press, 2009.

[32] M. Fox, *Quantum Optics: An Introduction*, 1st edition. OUP Oxford, 2006.

[33] 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.

[34] 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.

[35] R. S. Hasan, S. K. Tawfeeq, N. Q. Mohammed, and A. I. Khaleel, "A true random number generator based on the photon arrival time registered in a coincidence window between two single-photon counting modules," *Chinese J. Phys.*, vol. 56, no. 1, pp. 385–391, 2018, doi: https://doi.org/10.1016/j.cjph.2017.11.008.

[36] S. K. Tawfeeq, "A Random Number Generator Based on Single-Photon Avalanche Photodiode Dark Counts," *J. Light. Technol.*, vol. 27, no. 24, pp. 5665–5667, 2009, doi: 10.1109/JLT.2009.2034119.

[37] Bahaa E. A. Saleh, Malvin Carl Teich," *Fundamentals of Photonics*, 1st edition. pp. i–xix, Aug. 14, 1991, doi: https://doi.org/10.1002/0471213748.

[38] R. Menzel, *Photonics Linear and Nonlinear Interactions of Laser Light and Matter*, 2nd edition. Springer-Verlag Berlin Heidelberg, 2007.

[39] T. C. Adams, "Empirical Analysis of Optical Attenuator Performance in Quantum Key Distribution Systems Using a Particle Model," Air Force Institute of Technology, 2012.

[40] C.-W. Park *et al.*, "Single-photon counting in the 1550-nm wavelength region for quantum cryptography," *J. Korean Phys. Soc.*, vol. 49, no. 1, pp. 111–114, 2006, [Online]. Available: http://inis.iaea.org/search/search.aspx?orig_q=RN:43010875.

[41] G. P. Agrawal, *Lightwave Technology: Telecommunication Systems*, 1st edition. John Wiley & Sons, Inc., 2005.

[42] V.S.Bagad, *Optical fiber communication*, 1st edition. India: Technical Publications Pune, 2009.

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

[44] M. C. Jeruchim, P. Balaban, and K. S. Shanmugan, *Simulation of Communication Systems*, 2nd edition. Springer US, 2000.

[45] W. Stallings, *Wireless Communications and Networks*, 2nd Edition. Pearson College Div, 2004.

[46] 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.

[47] 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.

[48] E. Leitgeb *et al.*, "Analysis and evaluation of optimum wavelengths for free-space optical transceivers," in *2010 12th International Conference on Transparent Optical Networks*, 2010, pp. 1–7, doi: 10.1109/ICTON.2010.5549009.

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

[50] S. Bloom, E. Korevaar, J. Schuster, and H. Willebrand, "Understanding the performance of free-space optics [Invited]," *J.*

Opt. Netw., vol. 2, no. 6, pp. 178–200, 2003, doi: 10.1364/JON.2.000178.

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

[52] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," *Appl. Opt.*, vol. 35, no. 12, pp. 1956–1976, 1996, doi: 10.1364/AO.35.001956.

[53] 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.

[54] 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.

[55] M. Gilo, "Design of a nonpolarizing beam splitter inside a glass cube," *Appl. Opt.*, vol. 31, no. 25, pp. 5345–5349, 1992, doi: 10.1364/AO.31.005345.

[56] F. Hnault, "Quantum physics and the beam splitter mystery," *Nat. Light What are Photons? VI*, 2015, doi: 10.1117/12.2186291.

[57] G. Y. Russell A. Chipman, Wai-Sze Tiffany Lam, *Polarized Light and Optical Systems*, 1st edition. CRC Press, 2018.

[58] E. Optics, "www.edmundoptics.com," 2020. https://www.edmundoptics.com/knowledge-center/application-

notes/optics/what-are-beamsplitters/.

[59] J. A. Holes, L. Mailloux, M. Grimaila, and D. Hodson, “An Efficient Testing Process for a Quantum Key Distribution System Modeling Framework,” 2015.

[60] S. M. Young, M. Sarovar, and F. Leonard, “General modeling framework for quantum photodetectors,” *Phys. Rev. A*, vol. 98, no. 6, 2018, doi: 10.1103/physreva.98.063835.

[61] M. Repich, “Development of a simulation environment for the analysis and the optimal design of fluorescence detectors based on single photon avalanche diodes,” Trento University, 2010.

[62] T. P. Grayson and L. J. Wang, “400-ps time resolution with a passively quenched avalanche photodiode,” *Appl. Opt.*, vol. 32, no. 16, pp. 2907–2910, 1993, doi: 10.1364/AO.32.002907.

[63] A. D. Mora, A. Tosi, S. Tisa, and F. Zappa, “Single-Photon Avalanche Diode Model for Circuit Simulations,” *IEEE Photonics Technol. Lett.*, vol. 19, no. 23, pp. 1922–1924, 2007, doi: 10.1109/LPT.2007.908768.

[64] C. XU, “Study of the Silicon Photomultipliers and Their Applications in Positron Emission Tomography,” Hamburg University, 2014.

[65] M. Ghioni, S. Cova, F. Zappa, and C. Samori, “Compact active quenching circuit for fast photon counting with avalanche photodiodes,” *Rev. Sci. Instrum.*, vol. 67, no. 10, pp. 3440–3448, Oct. 1996, doi: 10.1063/1.1147156.

[66] A. Mofasser, S. Saha, K. S. Hadi, F. M. Mohammedy, and Y. El-Batawy, “Modeling of photocurrent and dark count probability of InGaAs/ InP Single Photon Avalanche Photodiode,” in *2017 IEEE*

International Conference on Telecommunications and Photonics (ICTP), 2017, pp. 147–151, doi: 10.1109/ICTP.2017.8285943.

[67] A. C. P. and K. Thomas Lucatorto, Ed., *Single-Photon Generation and Detection*, 1st edition. Elsevier Inc., 2013.

[68] W. P. Risk, "Improved Single Photon Detectors for Telecom Wavelengths," 2005.

[69] Y. Kang, H. X. Lu, Y.-H. Lo, D. S. Bethune, and W. P. Risk, "Dark count probability and quantum efficiency of avalanche photodiodes for single-photon detection," *Appl. Phys. Lett.*, vol. 83, no. 14, pp. 2955–2957, Sep. 2003, doi: 10.1063/1.1616666.

[70] T. Yamashita *et al.*, "Origin of intrinsic dark count in superconducting nanowire single-photon detectors," *Appl. Phys. Lett.*, vol. 99, no. 16, p. 161105, Oct. 2011, doi: 10.1063/1.3652908.

[71] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," *Supercond. Sci. Technol.*, vol. 25, no. 6, p. 63001, 2012, doi: 10.1088/0953-2048/25/6/063001.

[72] S. A. S. Zyabari and A. Zarifkar, "Simulation of Superconducting Nanowire Single- Photon Detector with Circuit Modeling." Zenodo, 2008, doi: 10.5281/zenodo.1084818.

[73] I. Holzman and Y. Ivry, "Superconducting Nanowires for Single-Photon Detection: Progress, Challenges, and Opportunities," *Adv. Quantum Technol.*, vol. 2, no. 3–4, p. 1800058, Apr. 2019, doi: https://doi.org/10.1002/qute.201800058.

[74] M. K. Akhlaghi and A. H. Majedi, "Semiempirical Modeling of Dark Count Rate and Quantum Efficiency of Superconducting Nanowire

Single-Photon Detectors," *IEEE Trans. Appl. Supercond.*, vol. 19, no. 3, pp. 361–366, 2009, doi: 10.1109/TASC.2009.2018846.

[75] M. K. Akhlaghi, "Nonlinearity and Gating in Superconducting Nanowire Single Photon Detectors," Waterloo University, 2011.

[76] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nat. Photonics*, vol. 3, no. 12, pp. 696–705, 2009, doi: 10.1038/nphoton.2009.230.

Appendices

IDQ

SWISS QUANTUM

Redefining Measurement

ID300 Short-Pulse Laser Source

Sub-Nanosecond Pulsed Laser Source

ID Quantique's ID300 Short-Pulse Laser Source has been designed to meet the specific requirements of researchers who need to generate short laser pulses at a wavelength of 1550 nm.

The laser source, based on a distributed-feedback (DFB) laser diode, is triggered externally via a trigger input to produce sub-nanosecond laser pulses with a repetition rate ranging from 0 to 500 MHz.

The ID300 laser source is ideally suited to work in combination with IDQ's Single-Photon Detection and Counting Modules (ID210, ID220, ID230 or ID280 series). The laser source can be directly triggered by the ID210's internal clock. Used in combination with a variable optical attenuator, this short-pulse laser source makes an ideal cost-effective single-photon source.

Key Features

- Sub-nanosecond laser pulses, pulse width 300 ps
- Repetition rate from 0 to 500 MHz
- Wavelength: 1550 nm
- Distributed-feedback (DFB)
- External trigger
- Compact and reliable stand-alone unit
- FC/PC connector

Applications

- Quantum optics
- Fibre optics characterization
- Spectroscopy
- Optical measurements
- Single-photon detector characterization
- Nanophotonics
- Optical Time Domain Reflectometer (OTDR)

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

ID300

SHORT-PULSE LASER SOURCE

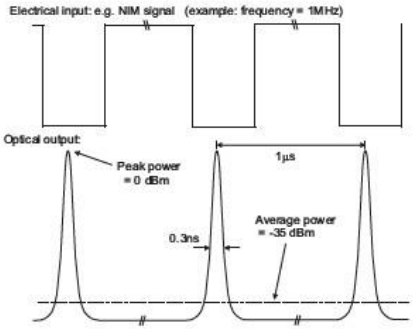
Specifications (T=25 °C)

Parameter	Min	Typical	Max	Units
Wavelength	1520	1550	1580	nm
Spectral width (FWHM) - DFB laser type		0.6	1.5	nm
Frequency range	0		500	MHz
Pulse duration		0.3*	0.5	ns
Peak power	0.7	1		mW
Output power at 1 MHz	-36	-35	-34	dBm
Trigger input**		NIM, ECL, PECL, LVPECL, TTL, TTL 50Ω		

* can be increased up to 2ns upon request

** choose one trigger input from this list. See ordering information below.

Operating Principle



General Information

Operating Temperature	+10°C to +30°C
Dimensions LxWxH	185 mm x 172 mm x 55 mm
Weight	915 g
Optical Connector	FC/PC
Electronic Connector	BNC
Fibre Type	SMF
Power Supply	100 - 240 VAC (autoselect)

Warning

CLASS 1 LASER PRODUCT

CLASSIFIED PER IEC 60825-1, Ed 1.2, 2001-08

Ordering Information and Sales Contact

Part number: ID300-1550-DFB-ZZZ

ZZZ: Select trigger input signal specifications. Choose between NIM, ECL, PECL, TTL, TTL 50 Ω, LVPECL.

ID QUANTIQUE SA
Chemin de la Marbrerie 3 | 1227 Carouge/Geneva Switzerland | T +41 22 301 83 71 F +41 22 301 89 79 | info@idquantique.com www.idquantique.com

EVERYTHING IN A NEW LIGHT.

Description

PerkinElmer Type C30902E avalanche photodiode utilizes a silicon detector chip fabricated with a double-diffused "reach-through" structure. This structure provides high responsivity between 400 and 1000 nm as well as extremely fast rise and fall times at all wavelengths. Because the fall time characteristics have no "tail", the responsivity of the device is independent of modulation frequency up to about 800 MHz. The detector chip is hermetically-sealed behind a flat glass window in a modified TO-18 package. The useful diameter of the photosensitive surface is 0.5 mm.

PerkinElmer Type C30921E utilizes the same silicon detector chip as the C30902E, but in a package containing a lightpipe which allows efficient coupling of light to the detector from either a focussed spot or an optical fiber up to 0.25 mm in diameter. The internal end of the lightpipe is close enough to the detector surface to allow all of the illumination exiting the lightpipe to fall within the active-area of the detector. The hermetically-sealed TO-18 package allows fibers to be epoxied to the end of the lightpipe to minimize signal losses without fear of endangering detector stability.

The C30902E and C309021E are designed for a wide variety of uses including optical communications at data rates to 1 GBit/second, laser range-finding, and any other applications requiring high speed and/or high responsivity.

Silicon Avalanche Photodiodes

C30902E, C30902S, C30921E, C30921S

High Speed Solid State Detectors for Fiber Optic and Very Low Light-Level Applications

Features

- High Quantum Efficiency 77% Typical at 830 nm
- C30902S and C30921S in Geiger Mode:
  - Single-Photon Detection Probability to 50%
  - Low Dark-Count Rate at 5% Detection Probability - Typically
    - 15,000/second at +22°C
    - 350/second at -25°C
  - Count Rates to 2 x 10^6/second
- Hermetically Sealed Package
- Low Noise at Room Temperature
  - C30902E, C30921E - 2.3 x 10^{-13} A/Hz$^{1/2}$
  - C30902S, C30921S - 1.1 x 10^{-13} A/Hz$^{1/2}$
- High Responsivity - Internal Avalanche Gains in Excess of 150
- Spectral Response Range - (10% Points) 400 to 1000 nm
- Time Response - Typically 0.5 ns
- Wide Operating Temperature Range - -40°C to +70°C

PerkinElmer optoelectronics

C30902E, C30902S, C30921E, C30921S

PerkinElmer optoelectronics

The C30902S and C30921S are selected C30902E and C30921E photodiodes having extremely low noise and bulk dark-current. They are intended for ultra-low light level applications (optical power less than 1 pW) and can be used in either their normal linear mode ($V_R < V_{BR}$) at gains up to 250 or greater, or as photon counters in the "Geiger" mode ($V_R > V_{BR}$) where a single photoelectron may trigger an avalanche pulse of about 10^8 carriers. In this mode, no amplifiers are necessary and single-photon detection probabilities of up to approximately 50% are possible.

Photon-counting is also advantageous where gating and coincidence techniques are employed for signal retrieval.

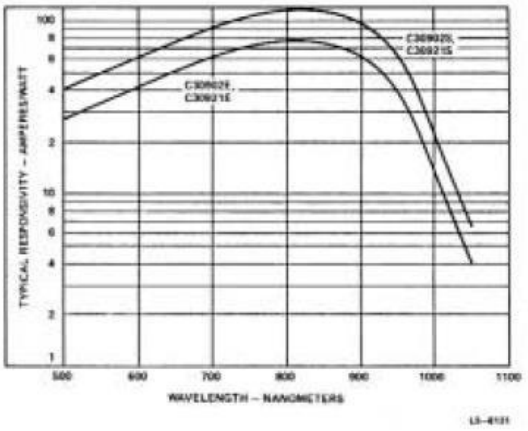


Figure 1. Typical Spectral Responsivity at 22°C

Optical Characteristics

C30902E, C30902S (Figure 13)

Photosensitive Surface:

Shape	Circular
Useful area	0.2 mm^2
Useful diameter	0.5 mm

Field of View:

Approximate full angle for totally illuminated photosensitive surface	100 deg

C30921E, C30921S (Figure 14)

Numerical Aperture of Light Pipe	0.55
Refractive Index (n) of Core	1.61
Lightpipe Core Diameter	0.25 mm

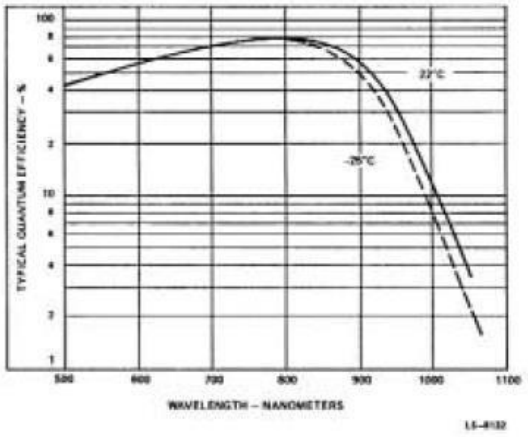


Figure 2. Typical Quantum Efficiency vs. Wavelength

Maximum Ratings, Absolute-Maximum Values (All Types)

Reverse Current at 22°C:	
Average value, continuous operation	200 μA
Peak value (for 1 second duration, non-repetitive)	1 mA
Forward Current, I_F at 22°C:	
Average value, continuous operation	5 mA
Peak value (for 1 second duration, non-repetitive)	50 mA
Maximum Total Power Dissipation at 22°C	60 mW
Ambient Temperature:	
Storage, T_{stg}	-60 to +100°C
Operating, T_A	-40 to +70°C
Soldering (for 5 seconds)	200°C

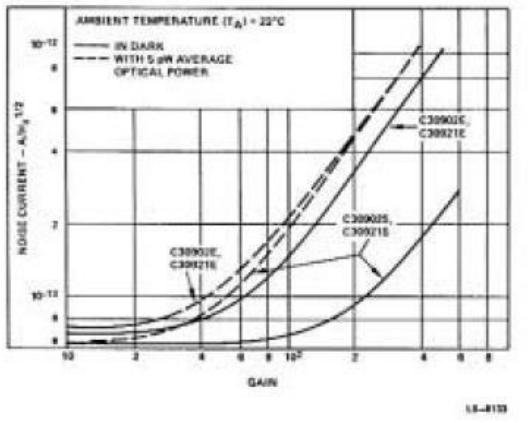


Figure 3. Typical Noise Current vs. Gain

PerkinElmer optoelectronics

Electrical Characteristics[1] at T_A = 22°C

	C30902E, C309021E			C30902S, C30921S			
	Min	Typ	Max	Min	Typ	Max	Units
Breakdown voltage, V_{BR}	-	225	-	-	225	-	V
Temperature Coefficient of V_R for Constant Gain	0.5	0.7	0.8	0.5	0.7	0.8	V/°C
Gain	-	150	-	-	250	-	
Responsivity:							
At 900 nm	55	65	-	92	108	-	A/W
At 830 nm	70	77	-	117	128	-	A/W
Quantum Efficiency:							
At 900 nm	-	60	-	-	60	-	%
At 830 nm	-	77	-	-	77	-	%
Dark Current, I_d	-	$1.5x10^{-8}$	$3x10^{-8}$	-	$1x10^{-8}$	$3x10^{-8}$	A
		(Figure 6)			*(Figure 6)*		
Noise Current, i_n: [2]							
f = 10 kHz, Δf = 1.0 Hz	-	$2.3x10^{-13}$	$5x10^{-13}$	-	$1.1x10^{-13}$	$2x10^{-13}$	$A/Hz^{1/2}$
		(Figure 3)			*(Figure 3)*		
Capacitance, C_d	-	1.6	2	-	1.6	2	pF
Rise Time, t_r:							
R_L = 50Ω, λ = 830 nm,							
10% to 90% points	-	0.5	0.75	-	0.5	0.75	ns
Fall Time:							
R_L = 50Ω, λ = 830 nm,							
90% to 10% points	-	0.5	0.75	-	0.5	0.75	ns
Geiger Mode *(See Appendix)*							
Dark Count Rate at 5% Photon Detection Probability [3] (830 nm):							
22°C	-	-	-	-	15,000	30,000	cps
-25°C	-	-	-	-	350	700	cps
Voltage Above V_{BR} for 5% Photon Detection Probability [3] (830 nm) *(See Figure 8)*	-	-	-	-	2	-	V
Dead-Time Per Event *(See Appendix)*	-	-	-	-	300	-	ns
After-Pulse Ratio at 5% Photon Detection Probability (830 nm) 22°C [4]	-	-	-	-	2	15	%

Note 1. At the DC reverse operating voltage V_R supplied with the device and a light spot diameter of 0.25 mm (C30902E, S) or 0.10 mm (C30921E, S). Note that a specific value of V_R is supplied with each device. When the photodiode is operated at this voltage, the device will meet the electrical characteristic limits shown above. The voltage value will be within the range of 180 to 250 volts.

Note 2. The theoretical expression for shot noise current in an avalanche photodiode is $i_n = (2q\,(I_{ds} + (I_{db}M^2 + P_oRM)\,F)\,B_w)^{1/2}$ where q is the electronic charge, I_{ds} is the dark surface current, I_{db} is the dark bulk current, F is the excess noise factor, M is the gain, P_o is the optical power on the device, and B_w is the noise bandwidth. For these devices F = 0.98 (2-1/M) + 0.02 M. (Reference: PP Webb, RJ McIntyre, JJ Conradi, "RCA Review", Vol. 35 p. 234, (1974)).

Note 3. The C30902S and C30921S can be operated at a substantially higher Detection Probabilities. See Appendix.

Note 4. After-Pulse occurring 1 microsecond to 60 seconds after main pulse.

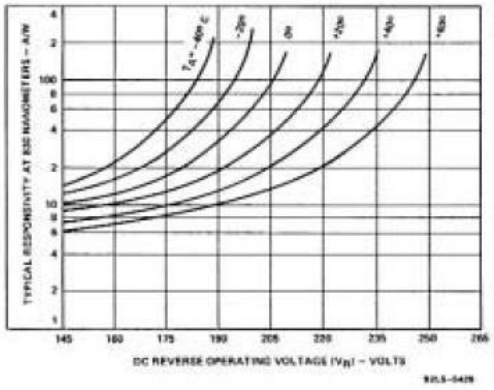


Figure 4. Typical Responsivity at 830 nm vs. Operating Voltage

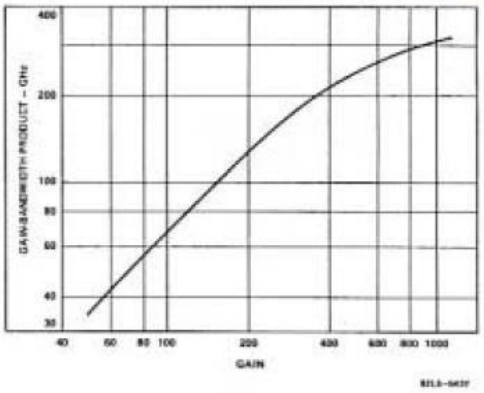


Figure 5. Typical Gain-Bandwidth Product vs. Gain

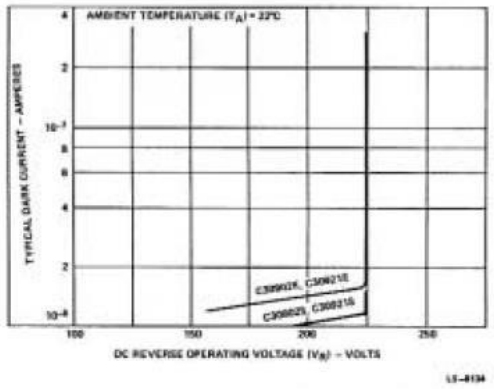


Figure 6. Typical Dark Current vs. Operating Voltage (V < VBR)

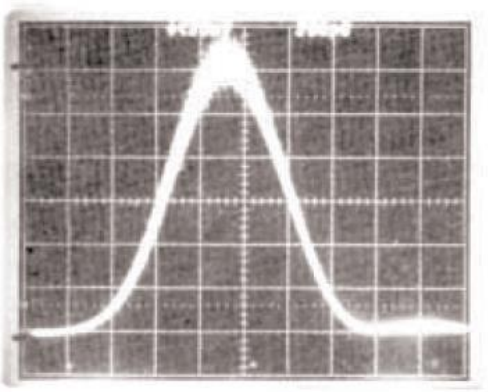


Figure 7. Avalanche Photodiode Response to a 100 ps Laser Pulse as Measured with a 350 ps Sampling Head. (Horizontal Axis: 200 ps/Division)

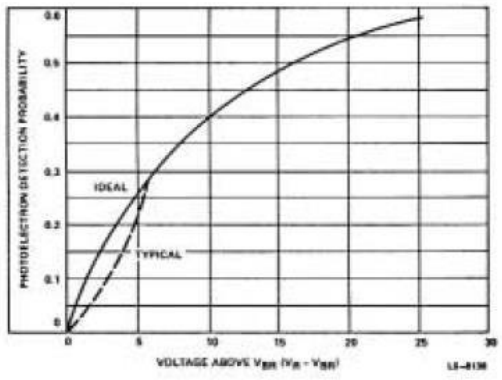


Figure 8. Geiger Mode, Photoelectron Detection Probability vs. Voltage Above VBR (VR > VBR)

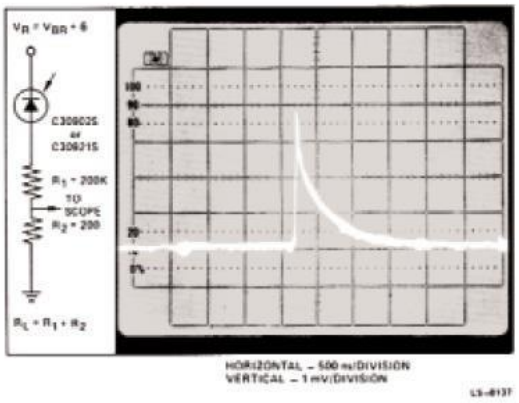


Figure 9. Passively Quenched Circuit and Resulting Pulse Shape

Redefining Measurement

ID281 Superconducting Nanowire

Single-Photon Detection with High Quantum Efficiency and Time-tagging Electronics

IDQ's ID281 series detection system consists of a superconducting nanowire detector combined with high-performance electronics and reliable cryogenic system. The system operates at 0.8 K and offers impressive performance such as 80% quantum efficiency, 60 ns recovery time, dark count rate < 100 Hz, jitter below 50 ps (FWHM) and no afterpulsing.

The plug and play device includes: cryocooler, stable and adjustable bias current sources, cryogenic amplification stage, discriminators and counters.

The complete system includes the cryostat with up to 8 Swiss made detectors. Our dedicated specialists develop detectors with optimized detection at 900 nm and 1550 nm.

The ID281 comes with a time tagger, the ID900, which 4 inputs are enabled by discriminators and allow the user to do accurate coincidence detections at high speed. The 0.8K closed cycle cryostat guarantees long term detector performance thanks to its outstanding temperature stability. It offers completely automated operations and any sample can be integrated for the finest experiments where stable and under 1 K temperature is required.

Key Features

- Detection range: 400-2500 nm
- Free-running operation
- Best-in-class quantum efficiency: > 80%
- Jitter: < 50 ps (FWHM)
- Low dark count rate: < 100 Hz
- Closed-cycle 0.8 K cryostat
- 1 to 8 channels per cryostat
- Detectors peak efficiency: 900 nm or 1550 nm
- Agile control and data recording electronics

Applications

- Quantum Key Distribution
- Single-photon source characterization
- Eye-safe laser ranging (LIDAR)
- Singlet oxygen measurement
- Photoluminescence
- Fluorescence lifetime measurement
- Fiber optics characterization
- Failure analysis of electronics circuits
- Quantum computing & Quantum optics
- Spectroscopy

ID QUANTIQUE SA
Chemin de la Marbrerie 3 | 1227 Carouge/Geneva Switzerland | T +41 22 301 83 71 F +41 22 301 83 79 | info@idquantique.com www.idquantique.com

ID281

SUPERCONDUCTING NANOWIRE

Detector Specifications

Parameter	Min	Typical	Max	Units
Wavelength range	400		2500	nm
Optical fibre type		SMF		
Efficiency range at 1550nm	75	80		%
Efficiency range at 900nm	75	80		%
Dark count rate			100	Hz
Recovery Time		60*		ns
Jitter (FWHM)			50	ps
Pulse width		10		ns
Output connector		SMA		
Operating temperature		0.8		K
Dimensions		13x20x25		mm
Optical connector		FC/PC		

* Recovery of 50% of the maximum efficiency

Cryostat Specifications

Parameter	Min	Typical	Max	Units
Cooling temperature		0.8		K
Temperature stability			10	mK
Number of channels	1		8	
Compressor Type		Air- cooled or water-cooled		
Flexlines length		3		m
Cooldown time		12		hours
Dimensions				
- Cryostat		53x30x30		cm
- Compressor		50x40x50		cm
Runtime at 0.8 K	22	40		hours

Customisations

Customised SNSPD with better performances:

- <30 ps FWHM timing resolution
- MMF fiber coupling
- Polarization independant detectors
- Broadband detectors: efficiency >70 % between 1200 - 1600 nm

Time Controller

The Time Controller performs the functions of a number of devices: time-to-digital converter, delay generator, pattern generator, counter and discriminator. For instance, the Time Controller allows you to measure the dark count rate, the efficiency or even the recovery time of your detectors.

Time Controller Specifications

- Timestamping and histogramming
- Internal timestamps processing (coincidence, filters,etc...)
- Delay generation with multi-hit ability
- Pattern generation
- High-speed counters
- High precision discriminators (-2 V to 2 V in 1 mV steps)
- 4 input channels
- 4 output channels (NIM + LVTTL)
- High timing resolution: 8 ps RMS (20 ps FWHM) and 13 ps bin width
- 1 GHz counters

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 83 79
info@idquantique.com
www.idquantique.com

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 منظومات توزيع المفتاح الكمي.

في هذا العمل البحثي، تم بناء والتحقق من محاكي لمنظومة توزيع المفتاح الكمي بالأعتماد على بروتوكول BB84 بأستخدام أسلوب محاكاة الزمن المستمر وبأستعمال برنامج Matlab2019a. 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 عيوب ومشاكل المنظومة مثل استخدام مصادر الفوتون المنفرد غير المثالية، استخدام كواشف الفوتون المنفرد غير المثالية واخيرا خسائر وعيوب قنوات أتصال الليف البصري والفضاء الحر الكمية.

منظومة الأرسال لبروتوكول ال BB84 تتكون من اربعة ليزرات نبضية والتي تعمل عشوائيا عن طريق التحفيز من خلال وحدة توليد اعداد عشوائية زائفة ب5000 بت كحد أقصى في كل عملية محاكاة. مولدات النبضات الليزرية المصممة تجهز سلسلة من النبضات طول النبضة يقاس ضمن مدى النانو ثانية، بمعدل تكرار يتراوح بين 0.1ميكاهرتز ألى 10ميكاهرنز، قدرة خرج بصرية بمقدار 1ملي واط وبثلاث اطوال موجية تستخدم على نطاق واسع في منظومات توزيع المفتاح الكمي وهي (1550 نانومتر، 900 نانومتر، 830 نانومتر). أشارات الخرج لهذه المصادر النبضية تمت مقارنتها بخرج المولد النبضي التجاري IDQ (ID300) لأغراض التحقق من صحة النموذج. المرسلة تتكون من عناصر بصرية أخرى مثل المستقطب الخطي وموهن القدرة البصري.

تم نمذجة نوعين من قنوات الأتصال الكمية ضمن هذا المحاكي، الليف البصري والفضاء الحر. قناة أتصال الليف البصري صممت بطول يصل الى 150كم كحد أعلى وبمعامل توهين مقداره 0.2 ديسيبيل/كم عند الطول الموجي 1550نانومتر نسبة الى المواصفات التجارية لليف البصري (SM-28). بينما عند الأطول الموجية 900نانومتر و 830 نانومتر فأن معامل التوهين هو 2ديسيبيل/كم و 3 ديسيبيل/كم على التوالي. تم تصميم قناة اتصال الفضاء الحر الكمية بطول يصل ايضا الى 150كم وبمعامل توهين مقداره 0.1 ديسيبيل/كم عند الطول الموجي 860 نانومتر.

تتكون منظومة الأستقبال من اربعة كواشف للفوتون المنفرد مرتبة مع مواد بصرية و التي تتألف من موزع ضوء غير مستقطب و موزعان للضوء مستقطبان و قاعدة نصف موجة. تم تصميم كواشف الفوتون المنفرد ذات الأنهيار المضاعف وكواشف الفوتون المنفرد دقيقة الأسلاك فائقة التوصيل بالاعتماد على خصائص لكواشف تجارية وتم أستخدامهما ضمن منظومة توزيع المفتاح الكمي بالأضافة الى أمكانية أستخدامهما كمحاكين قائمين بحد ذاتهما لدراسة اداء كواشف الفوتون المنفرد. تم محاكاة وتصميم نموذجين منفصلين لكل من كاشف الفوتون المنفرد السليكوني ذو الأنهيار المضاعف التجاري بالرقم C30921S وكاشف الفوتون المنفرد دقيق الاسلاك فائق التوصيل بالرقم ID281.

تم في هذا العمل البحثي أختبار طولين موجيين لكاشف الفوتون المنفرد ذو الأنهيار المضاعف وهما 830 نانومتر و 900 نانومتر بينما تم أختبار الطولين الموجيين 1550 نانومتر و 900 نانومتر لكاشف الفوتون المنفرد دقيق الاسلاك فائق التوصيل بسبب كفاءة الكشف العالية لهذين الجهازين عند هذه الأطوال الموجية.

المساهمات الرئيسية لهذا العمل البحثي تتضمن تصميم تقنية كاشف الفوتون المنفرد دقيق الاسلاك فائق التوصيل وعلى حد علمنا لم يتم التطرق الى هذه التقنية ضمن محاكي منظومة توزيع مفتاح كمي أخر بالأضافة الى استخدام قناة اتصال الفضاء الحر ضمن هذه المنظومة. أخيرا، كل جزء ضمن هذه المنظومة مزود براسمات المجال الزمني لغرض أختباره بشكل منفصل.

أظهرت خطوات التحقق من صحة النتائج لمحاكاة عناصر المنظومة كل على حده بالاضافة لمحاكاة المنظومة كاملة تقارب جيد مع النتائج النظرية والمختبرية المذكورة في المراجع وجداول بيانات الأجهزة التجارية.

وزارة التعليم العالي والبحث العلمي

جامعة بغداد

معهد الليزر للدراسات العليا

نمذجة ومحاكاة لتقييم الإداء لمنظومة توزيع المفتاح الكمي

أطروحة مقدمة الى

معهد الليزر للدراسات العليا/ جامعة بغداد/ لاستكمال متطلبات نيل شهادة دكتوراه فلسفة في الليزر / الهندسة الالكترونية والاتصالات

من قبل

عادل فاضل مشتت

بكالوريوس هندسة كهربائية وألكترونية - 2003

ماجستير هندسة الاتصالات والوسائط - 2012

بإشراف

الأستاذ المساعد الدكتورة شيلان خسرو توفيق

1442 هـ **2020 م**