UNIVERSITI PUTRA MALAYSIA

AN EFFICIENT MODELING AND SIMULATION OF DIFFERENTIAL PHASE SHIFT-QUANTUM KEY DISTRIBUTION (DPS-QKD) SYSTEM USING OPTISYSTEM

MU’AZU DAUDA

FSKTM 2017 13
AN EFFICIENT MODELING AND SIMULATION OF DIFFERENTIAL PHASE SHIFT-QUANTUM KEY DISTRIBUTION (DPS-QKD) SYSTEM USING OPTISYSTEM

By
MU’AZU DAUDA

Thesis Submitted to the School of Graduate Studies, University Putra Malaysia, in Fulfilment of the Requirement for the Degree of Master of Computer science

January 2017
COPYRIGHT

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of University Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of University Putra Malaysia.

Copyright ©University Putra Malaysia
DEDICATION

This thesis is dedicated to my late parents for their endless love, support and encouragement.
ABSTRACT

Abstract of thesis presented to the Senate of University Putra Malaysia in Fulfilment of the Requirement for the Degree of Master of Computer Science

AN EFFICIENT MODELING AND SIMULATION OF DIFFERENTIAL PHASE SHIFT-QUANTUM KEY DISTRIBUTION (DPS-QKD) SYSTEM USING OPTISYSTEM

By
MU’AZU DAUDA

JANUARY 2017

Supervisor: Assoc. Prof. Dr. Zuriati Binti Ahmad Zukarnain
Faculty: Computer Science and Information Technology

Differential phase-shift (DPS) quantum key distribution (QKD) is a unique QKD protocol that is different from traditional ones, featuring simplicity and practicality. In this work, we simulated the DPS-QKD experiment conducted by (Liu et al., 2013), using OptiSystem 7. To the best of our knowledge, this is the first simulation work on DPS-QKD using a single photon source.

We used a random number generator to get the phase modulation pattern of N=5, 7, 9, 11, and 13, while for the 3 and 15 pulse cases, the pattern adopted in the experiment was used. When the number of pulse (N) was 3, a quantum bit error rate (QBER) of 3.0%, which is lower than the minimum QBER of 4.12% required for unconditional security, was obtained. The key creation efficiency increases with the increase in the number of pulse up to 15, as it reaches 93.4% but at the expense of the increment in QBER. The result of our simulation is, on some aspect, in agreement with the experimental result. However, we were able to extend the
transmission distance from 3 meter, as in the experiment, to 10 meter. The coincidence count obtained was also in total agreement with the one obtained from the experiment.

The result of the average QBER indicated that increase in the pulse number N causes the QBER to raise up due to longer rise and fall time of phase modulation step which affect the MZ inference. Therefore, we suggest using a faster waveform generator with shorter rise and fall times will remarkably lower the QBER. Extending the transmission coverage to a longer distance while, at the same time reducing the QBER with full unconditional security will part of the future research.
ACKNOWLEDGEMENT

All glory, praises, and gratitude are due to Allah the omnipotent, the most gracious and the most merciful and, peace and blessing of Allah be upon our beloved prophet Muhammad sallallahu alayhi wasallam. Alhamdulillah, I thanks Allah for his immense grace and blessing in every aspect of my life, which enables me to achieve so many things in life.

I am tremendously indebted to the following:

- My supervisor Associate Prof. Dr Zuriati Ahmad Zulkarnain for her kind support, guidance and encouragement during the entire project exercise. She introduces me to this new area of technology: Quantum Computing, thank you Prof.
- My examiner Associate Prof. Dr. Zurina M. Hanapi for her kind guidance and encouragement to expand this work at the PhD level and make contribution to the body of knowledge.
- My special thanks to Mr Taiwo Ambali of faculty of Engineering, UPM, who patiently and tirelessly put me through the simulation tool that I used in this research and introduces me to the concept of DPS-QKD.
- My special thanks also go to Mr Umar Abubakar idris and Mal Mamman, all of which are PhD students at Faculty of Computer Science and Information Technology, UPM, for their tremendous contribution and guidance toward accomplishing this work.
- I specially owe gratitude to TETFUND and My institution, Federal University Dutse for their support and funding of my study at UPM.
I will like to also thank my friends and well-wishers who willingly share their skills and knowledge with me which really help in accomplishing this work.

Allahu akbar, my beloved parents (late) for their moral training, prayers, guidance and encouragement toward achieving a better and successful life in this world and hereafter. May Allah’s forgiveness, peace, mercy and blessing be upon them, amin.

Last but not the least, my beloved wife and children who patiently and courageously supported and encouraged me, prayed for the successful completion of the program and, missed me during the period of the studies.
APPROVAL FORM

This thesis was submitted to the Senate of University Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Computer science. The members of the Supervisory Committee were as follows:

**Associate Prof. Dr. Zuriati Binti Ahmad Zukarnain**
Faculty of computer science and IT technology
University Putra Malaysia
(Supervisor)
Date:

----------------------------------

**Associate Prof. Dr. Zurina M. Hanapi**
Faculty of computer science and IT technology
University Putra Malaysia
(Assessor)
Date:

Prof. Dr. ROBIAH YUNUS
Dean
School of Graduate Studies
University Putra Malaysia
Date:
DECLARATION

Declaration by a graduate student

I hereby confirm that:
- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other Degree at any other institutions;
- Intellectual property from the thesis and copyright of thesis are fully-owned by University Putra Malaysia, as according to the University Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the University Putra Malaysia (Research) Rules 2012;
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the University Putra Malaysia (Graduate Studies) Rules 2003(Revision 2012-2013) and the University Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _______________________ Date: __________________
Name and Matric No.: _____________________________________
Table of Contents
COPYRIGHT........................................................................................................................ i
DEDICATION ........................................................................................................................ ii
ABSTRACT ............................................................................................................................ iii
ACKNOWLEDGEMENT ......................................................................................................... v
APPROVAL FORM ................................................................................................................ vii
DECLARATION ...................................................................................................................... viii
LIST OF TABLES ................................................................................................................... xi
LIST OF FIGURES ............................................................................................................... xii
LIST OF ABBREVIATION ..................................................................................................... xiii
1. INTRODUCTION .............................................................................................................. 1
  1.1 Background .................................................................................................................. 1
  1.2 Overview of QKD Protocols ......................................................................................... 2
    1.2.1 The BB84 Protocol .............................................................................................. 2
    1.2.2 The B92 Protocol ............................................................................................. 4
    1.2.3 Differential Phase Shift Quantum Key Distribution (DPS-QKD) ...................... 4
  1.3 Comparison Between QKD Protocols ......................................................................... 6
  1.4 Problem Statement ...................................................................................................... 8
  1.5 Objectives .................................................................................................................. 8
  1.6 Research Scope .......................................................................................................... 8
  1.7 Thesis Organization .................................................................................................... 8
2. LITERATURE REVIEW ................................................................................................. 9
  2.1 Related Works On DPS QKD Experiment ................................................................... 9
  2.2 CONFIGURATION AND OPERATION ...................................................................... 15
  2.3 Security Issues ........................................................................................................... 17
    2.3.1 Beam Splitting Attack ....................................................................................... 18
    2.3.2 Intercept Resend Attack .................................................................................... 18
    2.3.3 Sequential Attack ............................................................................................. 20
    2.3.4 Photon Number Splitting Attack ....................................................................... 21
    2.3.5 General Individual Attack ............................................................................... 21
    2.3.6 Side-Channel Attack ....................................................................................... 22
    2.3.7 Sophisticated Attacks ...................................................................................... 23
  2.4 Extended Schemes ...................................................................................................... 24
    2.4.1 Delay Selected DPS-QKD ............................................................................... 24
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Comparison between popular QKD Protocols</td>
<td>7</td>
</tr>
<tr>
<td>3.1</td>
<td>Simulation Parameters</td>
<td>34</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>BB84 Bit Encoding</td>
<td>3</td>
</tr>
<tr>
<td>1.2</td>
<td>Sifted Key</td>
<td>3</td>
</tr>
<tr>
<td>1.3</td>
<td>B92 2-State Encoding</td>
<td>4</td>
</tr>
<tr>
<td>1.4</td>
<td>DPS-QKD Protocol</td>
<td>5</td>
</tr>
<tr>
<td>2.1</td>
<td>DPS-QKD Configuration Setup</td>
<td>14</td>
</tr>
<tr>
<td>2.2</td>
<td>Bob’s detection during intercept-resend attack</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>Sequential attack with amplitude modulation</td>
<td>18</td>
</tr>
<tr>
<td>2.4</td>
<td>Bob’s setup in delay selected DPS-QKD.</td>
<td>22</td>
</tr>
<tr>
<td>2.5</td>
<td>Four Level DPS-QKD</td>
<td>24</td>
</tr>
<tr>
<td>2.6</td>
<td>Macroscopic DPS-QKD</td>
<td>26</td>
</tr>
<tr>
<td>2.7</td>
<td>DPS Quantum Secret Sharing</td>
<td>27</td>
</tr>
<tr>
<td>2.8</td>
<td>Entanglement based DPS-QKD</td>
<td>28</td>
</tr>
<tr>
<td>3.1</td>
<td>DPS-QKD Experimental components</td>
<td>30</td>
</tr>
<tr>
<td>3.2</td>
<td>Proposed DPQ-QKD system Architecture</td>
<td>31</td>
</tr>
<tr>
<td>3.3</td>
<td>DPQ-QKD Simulation Set-up</td>
<td>33</td>
</tr>
<tr>
<td>4.1</td>
<td>Coincidence count for phase modulation pattern (0,0,0)</td>
<td>37</td>
</tr>
<tr>
<td>4.2</td>
<td>Coincidence count for phase modulation pattern (π,0,0)</td>
<td>38</td>
</tr>
<tr>
<td>4.3</td>
<td>Coincidence count for phase modulation pattern (0, 0, 0, π, 0, π, 0, π, 0, π, π, π, π, π, π, π, π, π, π, 0)</td>
<td>39</td>
</tr>
<tr>
<td>4.4</td>
<td>Coincidence count for phase modulation pattern (0, 0, 0, π, 0, π, 0, π, 0, π, π, 0, π, π, π, π, π, 0, π, π, 0, π, π, π, π, 0)</td>
<td>40</td>
</tr>
<tr>
<td>4.5</td>
<td>The average QBER</td>
<td>41</td>
</tr>
<tr>
<td>4.6</td>
<td>The key creation efficiency</td>
<td>42</td>
</tr>
</tbody>
</table>
# LIST OF ABBREVIATION

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>APD</td>
<td>Avalanche Photodiode</td>
</tr>
<tr>
<td>BM</td>
<td>Beam Splitter</td>
</tr>
<tr>
<td>BB84</td>
<td>Bernnet &amp; Brassard, 2014</td>
</tr>
<tr>
<td>BER</td>
<td>Bit Error Rate</td>
</tr>
<tr>
<td>COW</td>
<td>Coherent One Way</td>
</tr>
<tr>
<td>CW</td>
<td>Coherent Wave</td>
</tr>
<tr>
<td>DPS</td>
<td>Differential Phase Shift</td>
</tr>
<tr>
<td>DPS-QKD</td>
<td>Differential Phase Shift Quantum Key Distribution</td>
</tr>
<tr>
<td>FSO</td>
<td>Free Open Surface</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>MOT</td>
<td>Magneto-Optical Trap</td>
</tr>
<tr>
<td>N</td>
<td>Number Of Pulse</td>
</tr>
<tr>
<td>OWC</td>
<td>Optical Wireless Communication</td>
</tr>
<tr>
<td>PNS</td>
<td>Photon Number Splitting</td>
</tr>
<tr>
<td>QBER</td>
<td>Quantum Bit Error Rate</td>
</tr>
<tr>
<td>QC</td>
<td>Quantum Cryptography</td>
</tr>
<tr>
<td>QKD</td>
<td>Quantum Key Distribution</td>
</tr>
<tr>
<td>QLE</td>
<td>Quantum Link Encryptor</td>
</tr>
<tr>
<td>QM</td>
<td>Quantum Mechanics</td>
</tr>
<tr>
<td>QSS</td>
<td>Quantum Secret Sharing</td>
</tr>
<tr>
<td>RZ</td>
<td>Return To Zero</td>
</tr>
<tr>
<td>RRDPS</td>
<td>Round-Robin Differential Phase Shift</td>
</tr>
<tr>
<td>SMF</td>
<td>Single Mode Fibre</td>
</tr>
<tr>
<td>SSPD</td>
<td>Superconducting Single Photon Detector</td>
</tr>
<tr>
<td>USD</td>
<td>Unambiguous State Discrimination</td>
</tr>
<tr>
<td>VSCEL</td>
<td>Vertical-Cavity Surface Emitting Laser</td>
</tr>
</tbody>
</table>
CHAPTER 1
INTRODUCTION

1.1 Background

Digital communication between two or more parties tend to be vulnerable to series of attack by threat agents, most importantly eavesdropping or interception of private information. Public key cryptography, whose strength depends on the computational complexity, was believed to be the solution to such problems. The computational complexity of this method was thought to make the process of deciphering the encrypted messages to be slow. Furthermore, the activities of the threat agents such as brute force attack and eavesdropping, coupled with the technological advancement seems to compromised the strength and security of modern cryptographic algorithms. Quantum computers, which are the product of Quantum Mechanics (QM) and equipped with the processing capability to instantly solve thousands to millions of mathematical equations or factorization are considered as serious threat in exposing the public key cryptography to the risk of being compromised. However, quantum cryptography which is based on the properties of QM provides an unconditional security through Heisenberg’s uncertainty principle, no-cloning theorem and entanglement.

Quantum cryptography (QC) so far witnesses series of researches starting from BB84 (Bennett & Brassard, 2014), which was the first protocol for Quantum Key Distribution (QKD) until recent Quantum Link Encryptor-1 (QLE-1).

Quantum key distribution (QKD) based on the concept of quantum mechanics, provides unconditional security for the transmitter (Alice) to communicate and exchange secret key with the Receiver (Alice). In QKD, the use of No-Cloning theorem and Heisenberg Uncertainty Principle reveals the existence of an eavesdropper that attempt to measure the photons by indicating to both Alice and Bob the disturbance in the state of the photons. There are various schemes for QKD in existence, ranging from the one that uses two non-
orthogonal bases like BB84, those that uses two nonorthogonal states like B92, and to those that are based on photons entanglement example E91, BBM92 (Inoue, Waks & Yamamoto, 2002). However, the focus of this work is on Different Phase Shift Quantum key Distribution (DPS-QKD) which fully uses four nonorthogonal states. In this scheme, a photon send by Alice is split into three pulses and randomly phase modulated. At the receiver’s site, Bob measures the differential phase and obtain the bit information. DPS-QKD is suitable for fiber-based systems, its key creation efficiency is higher than that offered by conventional fiber-based BB84 (Inoue, Waks & Yamamoto, 2002), (Waks, Takesue, & Yamamoto, 2006), and not sensitive to multi-photon states which the source generated (Waks, Takesue, & Yamamoto, 2006).

1.2 Overview of QKD Protocols

The QKD protocol is the mechanism used for the creation of a secret key based on the concept of quantum mechanics and, digital and photon measurements. Since the after the birth BB84 in 1984, several QKD protocols were proposed and implemented. This section briefly explains some interesting QKD protocols.

1.2.1 The BB84 Protocol

The BB84 is the first QKD protocol proposed in 1984 by Charles H. Bennett and Gilles Brassard and it is based on the concept of quantum mechanics. The concept of this protocol is to Alice securely send a random secret key by transmitting train of photons based on randomly selected sequence of polarization states. At the receiving site, Bob will randomly guess the polarization bases, used by Alice, to measure each received photon and translate the result as binary zeros and ones. If the correct polarization basis is used, he will obtain the same bits with Alice otherwise, the result will be wrong (Bennett & Brassard, 2014).
Bob will then inform Alice, via an unsecured media, the basis he used in measuring the received photon. In reply, Alice will confirm to Bob whether he uses the correct basis or not. To obtain a sift key, both Alice and Bob will drop the bits matching to the photon measured with difference basis by Bob. Figure 1.2 shows the sift key operation, the sequence of bits chosen by Alice, the basis she has chosen to encode them, Bob’s chosen basis for the measurement and the final sift key obtained.

In term of communication process, BB84 is regarded as the simplest of all the QKD protocol, however some few researchers proved its insecurity but still in use by many QKD protocols (Abushgra & Elleithy, 2016).
1.2.2 The B92 Protocol

In 1992, C. H. Bennett presented a simplified version of BB84 known as B92. Contrary to BB84 that uses four non-orthogonal state, the B92 requires two states only. The B92 protocol also is based on the Heisenberg’s Uncertainty Principle (Abushgra & Elleithy, 2016). As in BB84, Alice sends train of photon encoded using randomly selected bits, but the selected bits dictates which basis to adopt such that “1” is encoded as $45^\circ$ and “0” as $0^\circ$. Figure 1.3 shows the B92 2-state encoding scheme:

![Figure 1.3 B92 2-State Encoding](image)

Bob on the other hand, must randomly select the correct basis enable him measures the received qubits otherwise, he cannot measure anything. Bob inform Alice publically on whether he correctly measured the photon or not.

The B92 protocol utilizes most of the BB84 scheme steps that are based upon the polarization of the states, but it takes a critical action when Bob measures Alice’s qubits in two bases to produce two states.

1.2.3 Differential phase shift quantum key distribution (DPS-QKD)

The differential phase shift quantum key distribution (DPS-QKD) is a QKD protocol which work by breaking the photon form the coherent source into three (3) equal pulses and each pulse is randomly modulated by either 0 or $\pi$ and recombined them, at the receiver’s site.
based on one bit delay applied to ensure a single photon is detected. DPS-QKD presented by Inoue, Waks, & Yamamoto (2003) and fully uses four non-orthogonal states (Inoue, Waks, & Yamamoto, 2003). Figure 1.4 depicts the typical DPS-QKD operation.

First, Alice prepares a train of coherent pulse and randomly modulates the relative phase of each pulses 0 or $\pi$, the modulated photon is then attenuated to ensure that photon contain in each pulse is less than one (1). The attenuated pulse is then send to Bob (the receiver).

Bob applies a one-bit delay interferometer causing interference of the successive pulses which allow for measurement of the relative phase information using set of photon detectors attached to the interferometer’s outputs. Since the source photon power is weak, only part of the relative phase information can be read out, but the obtained relative phase should be exactly the same as the phase modulations at the sender. Bob records the timestamp when a photon was detected and which of the detectors clicked (relative phase information itself). He then generates a key by assigning bit 0 to relative phase 0 and bit 1 to relative phase $\pi$. Bob then sends back to Alice only the timestamp information. Alice uses this information and her phase encoding records to generate a key, which is called the sifted key. Finally, after error-correction and privacy-amplification processes, final secure keys are generated and used in...
cryptic communication (Tokura & Honjo, 2011).

1.3 Comparison Between QKD Protocols

The comparison of some popular QKD protocols, based on such features as being secured or unsecured, were made in (Abushgra & Elleithy, 2016) and the summary is presented in Table 1.1 below. From the table, it can be seen that DPS protocol is more secured than the other eight protocols as it is robust to PNS attack, Beam-Splitting attack, Denial of Service attack, Man-In-The-Middle attack and IRA attack. With the exception AK15, all the protocols used classical channel during their execution time (Abushgra & Elleithy, 2016).
<table>
<thead>
<tr>
<th>Cases</th>
<th>BB84</th>
<th>B92</th>
<th>SARG04</th>
<th>COW</th>
<th>KMB09</th>
<th>EPR</th>
<th>DPS</th>
<th>S13</th>
<th>AK15</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of state</td>
<td>4 states</td>
<td>2 states</td>
<td>4 states</td>
<td>Time slot</td>
<td>2 states</td>
<td>Entangled 2 of photons</td>
<td>4 states</td>
<td>4 states</td>
<td>n states</td>
</tr>
<tr>
<td>Direction of presence</td>
<td>QBER</td>
<td>QBER</td>
<td>QBER</td>
<td>Break of coherence</td>
<td>ITER</td>
<td>Bell’s inequality</td>
<td>Time instance</td>
<td>Ran seed asymmetric</td>
<td>QBER + Parity cell</td>
</tr>
<tr>
<td>Polarisation situation</td>
<td>2 orthogonal</td>
<td>1 non-orthogonal</td>
<td>coded bits</td>
<td>No, using DPS</td>
<td>No</td>
<td>No</td>
<td>4 non-orthogonal</td>
<td>2 orthogonal</td>
<td>2 orthogonal</td>
</tr>
<tr>
<td>Probability of each state</td>
<td>Various</td>
<td>50%</td>
<td>50%</td>
<td>Equal</td>
<td>50%</td>
<td>Equal</td>
<td>Equal</td>
<td>Various</td>
<td>Various</td>
</tr>
<tr>
<td>Qubit case</td>
<td>DV</td>
<td>DV</td>
<td>DV</td>
<td>DV</td>
<td>DV</td>
<td>DV</td>
<td>DV</td>
<td>DV</td>
<td>DV</td>
</tr>
<tr>
<td>Classical Channels</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Decoy States</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Sifting phase</td>
<td>Revealing Bases</td>
<td>Alice = 1 - Bob</td>
<td>Revealing non-orth. state</td>
<td>revealing the times 2k+1</td>
<td>determining the error rate</td>
<td>Bell’s Inequality</td>
<td>No</td>
<td>Revealing Bases</td>
<td>No</td>
</tr>
<tr>
<td>Bell’s inequality</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>PNS attack</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>It's better than BB84</td>
<td>Robust</td>
<td>Robust</td>
<td>N/A</td>
<td>Robust</td>
<td>N/A</td>
<td>Robust</td>
</tr>
<tr>
<td>IRUD attack</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Under test</td>
<td>Under test</td>
<td>Vulnerable</td>
<td>N/A</td>
<td>N/A</td>
<td>Robust</td>
</tr>
<tr>
<td>Beam-Splitting attack</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Robust</td>
<td>Robust</td>
<td>Robust</td>
<td>Vulnerable</td>
<td>Robust</td>
<td>N/A</td>
<td>Robust</td>
</tr>
<tr>
<td>Denial of Service attack</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Robust</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Man-In-The-Middle Attack</td>
<td>Vulnerable</td>
<td>Robust</td>
<td>Robust</td>
<td>Robust</td>
<td>Robust</td>
<td>Robust</td>
<td>Robust</td>
<td>N/A</td>
<td>Robust</td>
</tr>
<tr>
<td>IRA attack</td>
<td>Vulnerable</td>
<td>Vulnerable</td>
<td>Robust</td>
<td>Robust</td>
<td>Robust</td>
<td>Bell’s inequality</td>
<td>Robust</td>
<td>N/A</td>
<td>Robust</td>
</tr>
</tbody>
</table>
1.4 Problem Statement

Lack of Single photon source has for long been an issue in QKD implementation. This has jeopardized its security system in a way that researcher often replace it with weak multi-photon laser which exposes the system to all forms of channel attacks.

In the base paper presented, DPS-QKD system was experimented with the number of pulses N extended from the usual 3 pulses to 15 pulses. The work however was implemented over 3m transmission distance. In our simulation, we are able to extend test for the possibility of the setup to support longer transmission distance.

1.5 Objectives

1) To simulate a Differential Phase Shift Quantum Keys Distribution experiment conducted in (Liu et al, 2013) using Optisystem simulation tool.

2) To test for the response of the DPS–QKD system when the number of the pulses is increased from the 3 pulses to the maximum possible number of 15 and as well, extend the supported transmission distance.

1.6 Research Scope

1.7 Thesis Organization

In Chapter 2, literature review on the DPS-QKD was covered. This includes related research works, recent development in the field and some enhanced version of the protocol. While an overview of the methodology used in the research work was discussed in Chapter 3.

Chapter 4 presents the simulation results and analysis, comparison of the simulation result with the experimental one and other discussion. Finally, Chapter 5 is about summary and conclusion, and feature work.
REFERENCES


