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

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. Alhammadu lillah, 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.

- 1 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 here after. 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

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

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

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).

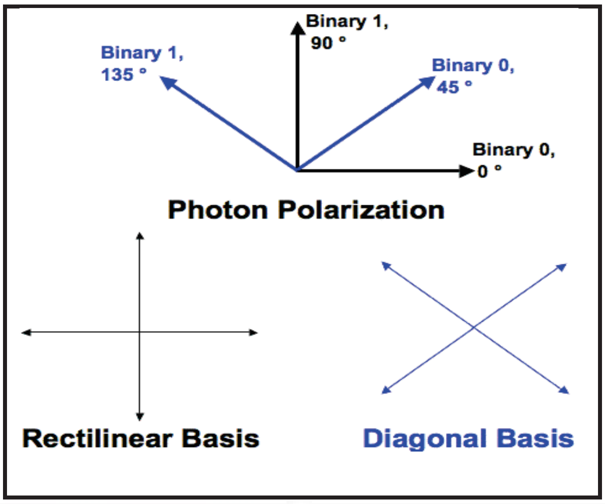

Figure 1.1 BB84 Bit Encoding. Source: (Haitjema, 2007)

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 below 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.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 1.2 Sifted Key. Source: (Haitjema, 2007)

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° and "0" as 0°. figure 1.3 shows the B92 2-state encoding scheme:

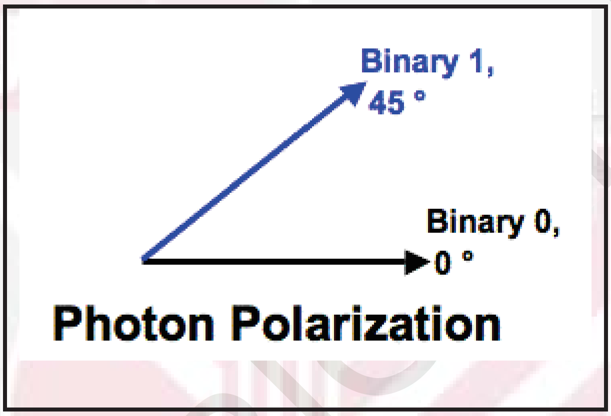

Figure 1.3 B92 2-State Encoding

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 π 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.

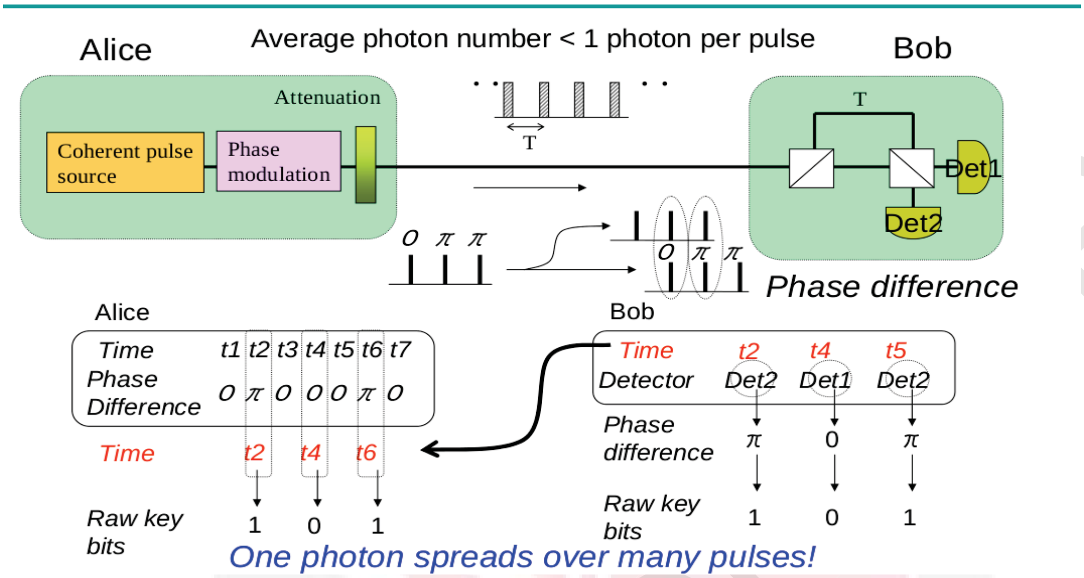

Figure 1.4 DPS-QKD Protocol. Source: (Honjo et al., 2013)

First, Alice prepares a train of coherent pulse and randomly modulates the relative phase of each pulses 0 or π.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 π. 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 1.1 Comparisons Between Popular QKD Protocols. Source: (Abushgra & Elleithy, 2016)

Cases	**Quantum Key Distribution Protocols**								
	BB84	**B92**	**SARG04**	**COW**	**KMB09**	**EPR**	**DPS**	**S13**	**AK15**
Properties	Heisenberg	Heisenberg	Heisenberg	Heisenberg	Heisenberg	Heisenberg	Entanglement	Entanglement	Heisenberg
No. of state	4 states	2 states	4 states	Time slot	2 states	Entangled 2 of photons	4 states	4 states	n states
Direction of presence	QBER	QBER	QBER	Break of coherence	ITER	Bell's inequality	Time instance	Ran seed asymmetric	QBER + Parity cell
Polarisation situation	2 orthogonal	1 non-orthogonal	coded bits	No, using DPS	No	No	4 non-orthogonal	2 orthogonal	2 orthogonal
Probability of each state	Various	50%	50%	Equal	50%	Equal	Equal	Various	Various
Qubit case	DV	DV	DV	DV	DV	DV	DV	DV	DV
Classical Channels	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Decoy States	No	No	No	Yes	No	No	No	No	Yes
Sifting phase	Revealing Bases	Alice = 1 - Bob	Revealing non-orth. state	revealing the times 2k+1	determining the error rate	Bell's Inequality	No	Revealing Bases	No
Bell's inequality	No	No	No	No	No	Yes	No	No	Yes
PNS attack	Vulnerable	Vulnerable	It's better than BB84	Robust	Robust	N/A	Robust	N/A	Robust
IRUD attack	Vulnerable	Vulnerable	Vulnerable	Under test	Under test	Vulnerable	N/A	N/A	Robust
Beam-Splitting attack	Vulnerable	Vulnerable	Robust	Robust	Robust	Vulnerable	Robust	N/A	Robust
Denial of Service attack	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Robust	N/A	N/A
Man-In-The-Middle Attack	Vulnerable	Robust	Robust	Robust	Robust	Robust	Robust	N/A	Robust
IRA attack	Vulnerable	Vulnerable	Robust	Robust	Robust	Bell's inequality	Robust	N/A	Robust

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

-Abushgra, A., & Elleithy, K. (2016). QKDP's comparison based upon quantum cryptography rules. *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. doi:10.1109/lisat.2016.7494101

-Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, *560*, 7–11. doi:10.1016/j.tcs.2014.05.025

- Branciard, C., Gisin, N., & Scarani, V. (2008). Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. *New Journal of Physics*, *10*(1), 013031. doi:10.1088/1367-2630/10/1/013031

-Chahar, U. S., & Chatterjee, K. (2015). A Novel Differential Phase Shift Quantum Key Distribution Scheme for Secure Communication. Retrieved from 2015 International Conference on Computing and Communications Technologies (ICCCT'15), http://ieeexplore.ieee.org/abstract/document/7292737/

- Curty, M., Zhang, L. L., Lo, H.-K., & Lutkenhaus, N. (2013). Sequential attacks against differential-phase-shift quan tum key distribution with weak coherent states. *Quantum Physics (quant-ph)*, *QIC Vol 7*(2007), p. 665–688. doi:https://arxiv.org/pdf/quant-ph/0609094.pdf

- Dauler, E. A., Spellmeyer, N. W., Kerman, A. J., Molnar, R. J., Berggren, K. K., Moores, J. D., & Hamilton, S. A. (2010). High-rate quantum key distribution with superconducting nanowire single photon detectors - IEEE Xplore document. Retrieved February 1, 2017, from http://ieeexplore.ieee.org/abstract/document/5500759/

-Fujiwara, M., Honjo, T., Shimizu, K., Tamaki, K., & Sasaki, M. (2013). Characteristics of superconducting single photon detector in DPS-QKD system under bright illumination blinding attack. *Optics Express*, *21*(5), 6304. doi:10.1364/oe.21.006304

-Gomez-Sousa, H. and Curty, M. (2009) "Upper bounds on the performance of differential-phase-shift quantum key distribution," *Quantum Inf. Comput.*,vol. 9, no. 1/2, pp. 62–80, 2009.

- Haitjema, M. (2007, December 2). Quantum key distribution - QKD. Retrieved February 2, 2017, from http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

-Honjo, T., Fujiwara, M., Shimizu, K., Tamaki, K., Miki, S., Yamashita, T., … Sasaki, M. (2013). Countermeasure against tailored bright illumination attack for DPS-QKD. *Optics Express*, *21*(3), 2667. doi:10.1364/oe.21.002667

-Honjo, T., & Inoue, K. (2006). Differential-phase-shift quantum key distribution with an extended degree of freedom. *Optics Letters*, *31*(4), 522. doi:10.1364/ol.31.000522

-Honjo, T., Inoue, K., & Takahashi, H. (2004). Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach–Zehnder interferometer. *Optics Letters*, *29*(23), 2797. doi:10.1364/ol.29.002797

-Honjo, T., Inoue, T., & Inoue, K. (2011). Influence of light source linewidth in differential-phase-shift quantum key distribution systems. *Optics Communications*, *284*(24), 5856–5859. doi:10.1016/j.optcom.2011.08.056

- Honjo, T., Yamamoto, S., Yamamoto, T., Kamada, H., Nishida, Y., Tadanaga, O., … Inoue, K. (2007). Field trial of differential-phase-shift quantum key distribution using polarization independent frequency up-conversion detectors. *Optics Express*, *15*(24), 15920. doi:10.1364/oe.15.015920

-Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, *91*(5), . doi:10.1103/physrevlett.91.057901

-Inoue, K. (2015). Differential phase-shift quantum key distribution systems. *IEEE Journal of Selected Topics in Quantum Electronics*, *21*(3), 109–115. doi:10.1109/jstqe.2014.2360362 (Inoue, 2015)

Inoue, K., & Honjo, T. (2005). Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Physical Review A*, *71*(4), . doi:10.1103/physreva.71.042305 In-line Citation:

- Inoue, K., & Honjo, T. (2005). Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Physical Review A*, *71*(4), doi:10.1103/physreva.71.042305

-Inoue, K., & Iwai, Y. (2009). Differential-quadrature-phase-shift quantum key distribution. *Physical Review A*, *79*(2), . doi:10.1103/physreva.79.022319

-Inoue, K., Ohashi, T., Kukita, T., Watanebe, K., Hayashi, S., Honjo, T., & Takesue, H. (2008). Differential-phase-shift quantum secret sharing. *Optics Express*, *16*(20), 15469. doi:10.1364/oe.16.015469

-Inoue, K., & Takesue, H. (2006). Quantum key distribution using entangled-photon trains with no basis selection. *Physical Review A*, *73*(3), . doi:10.1103/physreva.73.

-Inoue, K., Waks, E., & Yamamoto, Y. (2003). Differential-phase-shift quantum key distribution using coherent light. *Physical Review A*, *68*(2), . doi:10.1103/physreva.68.022317

-Iwai, Y., Honjo, T., Inoue, K., Kamada, H., Nishida, Y., Tadanaga, O., & Asobe, M. (2008). Polarization independent DPS-QKD system using up-conversion detectors. *Lasers and Electro-Optics, 2008 and 2008 Conference on Quantum Electronics and Laser Science. CLEO/QELS 2008. Conference on 4-9 May 2008.* doi: http://ieeexplore.ieee.org/abstract/document/4572987/

-Koashi, M. (2015). Round-robin differential-phase-shift QKD protocol - IEEE Xplore document. Retrieved January 29, 2017, from Lasers and Electro-Optics Pacific Rim (CLEO-PR), 2015 11th Conference on 24-28 Aug. 2015, http://ieeexplore.ieee.org/abstract/document/7376020/

-Kukita, T., Takada, H., & Inoue, K. (2010). Macroscopic differential phase shift quantum key distribution using an optically Pre-Amplified receiver. *Japanese Journal of Applied Physics*, *49*(12), 122801. doi:10.1143/jjap.49.122801

-Lo, H.-K., Ma, X., & Chen, K. (2005). Decoy state quantum key distribution. *Physical Review Letters*, *94*(23), . doi:10.1103/physrevlett.94.230504

-Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., … Zeilinger, A. (2011). Field test of quantum key distribution in the Tokyo QKD network. *Optics Express*, *19*(11), 10387. doi:10.1364/oe.19.010387

-Sasaki, T., Yamamoto, Y., & Koashi, M. (2014). Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, *509*(7501), 475–478.doi:10.1038/nature13303

-Shimizu, K., Honjo, T., Fujiwara, M., Ito, T., Tamaki, K., Miki, S., … Sasaki, M. (2014). Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area. *Journal of Lightwave Technology*, *32*(1), 141–151. doi:10.1109/jlt.2013.2291391

-Stucki, D., Brunner, N., Gisin, N., Scarani, V., & Zbinden, H. (2005). Fast and simple one-way quantum key distribution. *Applied Physics Letters*, *87*(19), 194108. doi:10.1063/1.2126792

-Takesue, H., Diamanti, E., Langrock, C., Fejer, M. M., & Yamamoto, Y. (2006). 10-GHz clock differential phase shift quantum key distribution experiment. *Optics Express*, *14*(20), 9522. doi:10.1364/oe.14.009522

-Waks, E., Takesue, H., & Yamamoto, Y. (2006). Security of differential-phase-shift quantum key distribution against individual attacks. *Physical Review A*, *73*(1), . doi:10.1103/physreva.73.012344

- Wang, S., Chen, W., Guo, J.-F., Yin, Z.-Q., Li, H.-W., Zhou, Z., … Han, Z.-F. (2012). 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Optics Letters*, *37*(6), 1008. doi:10.1364/ol.37.001008

-Wen, K., Tamaki, K., & Yamamoto, Y. (2009). Unconditional security of Single-Photon differential phase shift quantum key distribution. *Physical Review Letters*, *103*(17), . doi:10.1103/physrevlett.103.170503

-Zhang, H., Wang, J., Liu, X., Wei, Z., & Liu, S. (2009). A fiber-based differential phase shift quantum key distribution scheme with higher key creation efficiency. *Optics Communications*, *282*(14), 3037–3039. doi:10.1016/j.optcom.2009.03.066