OPTICAL RING BASED QUANTUM KEY DISTRIBUTION

XAYTHAVY LOUANGVILAY

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

DOCTOR OF ENGINEERING IN ELECTRICAL ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2016

KMITL-2016-EN-D-018-223

OPTICAL RING BASED QUANTUM KEY DISTRIBUTION

XAYTHAVY LOUANGVILAY

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

DOCTOR OF ENGINEERING IN ELECTRICAL ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2016

KMITL -2016-EN-D018-223

THESIS CERTIFICATION

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

Thesis Title	Optical Ring Based Quantum Key Distribution
Student	Mr.Xaythavy Louangvilay
Student Id.	54601003
Degree	Doctor of Engineering
Program	Electrical Engineering
Thesis Advisor	รศ.ดร.สมศักดิ์ มิตะถา
Thesis Reference Number	KMITL-2016-EN-D-018-223

EXAMINERS		SIGNATURES
Dr. Pakorn	Watanachaturaporn	
Assoc. Prof. Dr.S omsak	Choomchuay	
Prof. Dr. Kosin	Chamnongthai	
Dr. Amnach	Khawne	
Assoc. Prof. Dr. Somsak	Mitatha	

Date 13th September 2016 **Time** 15.00-17.00

Place Building A , Conference no.1

(Assoc. Prof. Dr. Komsan Maleesee)

Dean, Faculty of Engineering

13th September 2016

หัวข้อวิทยานิพนธ์	การกระจายคีย์แบบควอนตัมโดยใช้วงแหวนเชิงแสง
นักศึกษา	ชัยทวี หลวงวิลัย
รหัสประจำตัว	54601003
ปริญญา	วิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชา	วิศวกรรมไฟฟ้า
พ.ศ.	2559
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.ดร. สมศักดิ์ มิตะถา

บทคัดย่อ

วิทยานิพนธ์นี้มีจุดประสงค์เพื่อนำเสนอการเข้ารหัสควอนตัมด้วยวิธีการกระจายคีย์ของควอนตัมบนพื้นฐานของโปรโตคอลบีบี84 (BB84) ระบบนี้ถูกพัฒนาขึ้นเพื่อเพิ่มประสิทธิภาพการทำงานในส่วนของการเพิ่มอัตราคีย์ข้อมูลลับ และระยะทางในการส่ง โดยใช้โฟตอนจำนวนหลายตัว (multi-photons) นำเสนออุปกรณ์ขนาดไมโครเมตรสำหรับประยุกต์ใช้งานในด้านการสื่อสารด้วยแสง โดยทำการป้อนสัญญาณไบร์ทโซลิตอนเป็นสัญญาณอินพุทให้กับวงแหวนแพนด้า (PANDA ring) ที่ต่อกับแอดดรอปฟิลเตอร์ (add/drop filter) เพื่อสร้างแถบช่องสัญญาณแสงให้ได้หลายช่องสัญญาณ ซึ่งแต่ละช่องสัญญาณแสงที่สร้างขึ้นจะถูกนำไปใช้เป็นตัวแปรในการเข้ารหัสบิตข้อมูลเพื่อใช้สำหรับกระจายคีย์เชิงควอนตัมด้วยอุปกรณ์โพลาไรเซชัน ทำการจำลองผลการทดลองด้วยโปรแกรม MATLAB โดยใช้สมการทางคณิตศาสตร์ กำหนดจำนวนโฟตอน 10 ตัว ($\mu_0 = 10$) และอัตราการส่งพัลส์ข้อมูลเท่ากับ 1 MHz, 10 MHz และ 500 MHz จากการทดลองพบว่าระบบที่ได้นำเสนอสามารถกระจายคีย์ข้อมูลลับได้ด้วยอัตราสุงสุด 6 Mb/s, 48 Kb/s และ 25 Kbit/s ที่ระยะทาง 27 km, 90 km และระยะทางสุดสุดคือ 275 km ของความยาวเส้นใยแก้วนำแสง และสามารถสร้างได้หลายช่องสัญญาณมากถึง 278 ช่อง เพื่อรองรับความต้องการในการใช้งานแบนด์วิดธ์ที่สูงขึ้นในระบบการสื่อสารด้วยแสงได้อย่างมีประสิทธิภาพต่อไป

Thesis Title	Optical Ring Based Quantum Key Distribution
Student	Mr. Xaythavy Louangvilay
Student ID.	54601003
Degree	Doctor of Engineering
Program	Electrical Engineering
Year	2016
Thesis Advisor	Assoc. Prof. Dr. Somsak Mitatha

ABSTRACT

This thesis proposes the use of quantum key distribution (QKD) protocol based on BB84 information security. The improvement of the secret information key rate is developed by using multi-photons, when the high-bit-rate is generated the longer of distance is increased for transmission. In addition, the proposed system is performed by a smaller size device. The QKD is generated by using the bright soliton pulses within a modified add-drop filter name as PANDA ring resonator. The QKD key (qubit) is formed by using the correlated photons of each pulse by mean of the polarization control. In the experiment, the simulation data is verified by varying device parameters with MATLAB programs. There are 10 photons with the spectral widths (relative pulse rates) of 1MHz, 10MHz, 500MHz, are generated. The secret key rate is formed and used for 6 Mb/s, 48k/s at 27 km, 90 km of optical fiber distance, respectively. The obtained results have shown that the maximum of transmission distance of 240 km can be possible. In addition, the secure information with high capacity of 278 channels is obtained incorporating the qubits generated by the quantum processor, which can be served the large demand bandwidths with the secure communication applications.

ACKNOWLEDGEMENTS

Firstly of all, I would like to express my guidance sincere gratitude to my advisor, Assoc. Prof. Dr. Somsak Mitatha for his attention, insight, encourage, guided, and support during this research and for being available at any time to response my questions, which has been valuable. I am grateful to Professor Dr. Preecha Yupapin from Faculty of Electrical & Electronics Engineering, Tun Duc Thang University, Vietnam for introducing me the research topics, for the many insightful conversational, and his constant encouragement. Working with him has been a great learning experience.

I would like to thank the AUN/SEED-Net for the fully financial support to me in higher education at International College, King Mongkut's Institute of Technology Ladkrabang(KMITL)

I would like to thank my organization as NUOL to keep me a chance for study abroad as KMITL, Thailand. To make me have new knowledge and a good experience to improve my skill for taking these to develop our country.

I would also like to thank every young members of the Advanced Research Center of Photonic Laboratory (ARCP) of the Department of Applied Physics, Faculty of Science, KMITL; whose support has created a friendly environment.

I would also like to thank every young members of the Hybrid Computing Research Laboratory (HCRL) of the Department of Computer Engineering, Faculty of Engineering, KMITL; whose support has created a friendly environment.

I would like to thank my committee members, for their assistance, helpful comments, and insightful suggestions.

Finally, my greatest thanks are to my beloved family whose caring, understand, and possible attitude have encouraged me to go forward during difficult times. Whose never-ending love and support made the completion of this work completed and my dream of a graduate education come true.

Xaythavy Louangvilay

CONTENTS

Pages

CONTENTS(Cont.)

Pages

CONTENTS(Cont.)

LIST OF FIGURES

Figures **Pages**

LIST OF FIGURES (Cont.)

Pages

LIST OF TABLES

Tables **Pages**

Chapter 1

Introduction

1.1 Background of Security

Without security civilization could not have developed. Without the continuance of security future progress is imperiled because of the uncertainty from danger of loss or harm. Security is not only a human need, it is also a human right because all of data, such as text, images, sound and videos are public or private data when they are for top security, business, official, and military. Security has become necessary for human existence. This is partially due to the relationship between population and resources [1].

Computer security has become a concern barely a dozen years after the computer was invented. The Electronic Numerical Integrator and Computer (ENIAC) were constructed by using vacuum tubes in 1946 at the University of Pennsylvania. Transistors were invented in 1958. The first federal prosecution of a computer crime in the United States was in 1966. Since computing and particularly the internet were not developed with security as a foremost consideration, it was inevitable that serious abuses would emerge, leading eventually to what some people consider a current crisis. A variety of types of computer crime now challenge management. Some of these are cyberstalking [2], extortion, fraud, hacking or cracking, identity theft, intellectual property theft, and theft of money or assets. Anarchists, common criminals, organized crime syndicates, and terrorists use IT resources for their own advantages. The original hackers were computer students at Massachusetts Institute of Technology in the 1960s. They believed in freedom of communications and freedom of information, but they also espoused a moral code against criminal use of computing resources. Moral code alone would be insufficient to mitigate what was to occur in the next few years. Brute attacks on computing began in the 1970s. Particularly significant was the 1983 hacking of a Pentagon computer system by Kevin David Mitnick. Jim Hauser, a Californian, claims he wrote the first computer virus in 1982.

The purpose of security is cryptography, which transmit information in such a way that access to it is restricted entirely to the intended recipient, even if the transmission

itself is received by others. This science is of increasing importance with the advent of broadcast and network communication, such as electronic transactions, the Internet, e-mail, and cell phones, where sensitive monetary, business, political, and personal communications are transmitted over public channels [2]

Cryptography is operated by a sender scrambling or encrypting the original message or plaintext in a systematic way that obscures its meaning [3, 4]. The encrypted message or crypto text is transmitted, and the receiver recovers the message by unscrambling or decrypting the transmission. In such ciphers a set of specific parameters, called a key, is used together with the plaintext as an input to the encrypting algorithm, and together with the crypto text as an input to the decrypting algorithm. The encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key. In cryptography there are two classical keys such as “public key” and “secret-key (private-key)” [3].

Public-key encryption is based on the idea of a safe with two keys: a public key to lock the safe and a private key to open it. Using this method, anyone can send a message since the public key is used to encrypt messages, but only someone with the private key can decrypt the messages. Since the encrypting and decrypting keys are different, it is not necessary to securely distribute a key. The security of public-key encryption depends on the assumed difficulty of certain mathematical operations, such as factoring extremely large prime numbers. The algorithm is known as well as for public-key is RSA.

Secret-key is used for both sides of encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The message and recover the plaintext are decrypted by receiver applies the same key. Because a single key is used for both functions, in other name of secret key cryptography is also called “*symmetric encryption”*. There are many algorithms are used for the Secret key cryptography such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, and etc.

Quantum cryptography is also one of secret-key cryptography by providing a way for two users who are in different locations to securely establish a secret key and to detect if eavesdropping has occurred [5]. In addition, since quantum cryptography does not depend on difficult mathematical problems for its security, it is not threatened by

the development of quantum computers. Quantum cryptography accomplishes these remarkable feats by exploiting the properties of microscopic objects such as photons. Thus, we will present on the next topic.

1.2 The Optical Security

Optical ring resonator has numerous applications in signal processing, laser systems, industrial sensing, optical communication, interferometers, etc. They can be fabricated using bulk optical element (mirror and beam splitter), fiber optic component or integrated optics technology. Regarding their geometry there are not necessarily circular in shape. Integrated optical technology allows for extreme miniaturization, for the fabrication of rings with very perimeters, approaching the dimensions commensurate with the wavelengths used in high speed communication systems.

The use of light for communication purposes dates back to the use of smoke and fire to convey a piece of information, such as a victory in a war. There are many reasons that made photons more popular to use in information processing. Photons are able to accomplish certain functions better than electrons by virtue of their special properties. The very large bandwidth, ~10^{15} Hz, gives optics a potential speed for signal processing which is well beyond any electronics. Indeed, the shortest optical pulses of <10fs give light three order of magnitude advantage over the shortest electrical pulse [6]. When it comes to interconnects on a chip, the wiring capacitance will set the speed limits of integrated circuits. Besides, photons can pass through each other unperturbed in the absence of a nonlinear interaction, whereas electrons interact with each other even at a distance. In table 1.1, we summarize the potential advantages and disadvantages of using in signal processing.

Table 1.1 Advantage and disadvantage of optics in signal processing

Advantage of optics	disadvantage of optics
- Large bandwidth ~ 10^{15} Hz	- High power requirement ~ 1 W peak power
- Low propagation loss	- Interfacing with electronics
- Low cross talk	- Wave front distortions
- High degree of parallelism	
- Small dimension	

- Ultra short pulses < 10 fs - Coherence properties	

The turn of the new millennium witnessed an explosion in data-traffic volume, due to the ongoing increasing demand on the Internet. Therefore, all-optical switching devices have been looked at as key components for future high-speed optical communication systems. Such devices would enable highly parallel logic operations as well as ultrafast switching because of the instantaneous nature of virtual optical transitions [2]. With the recent advances in semiconductor fabrication, there has been a noticeable effort to bring those devices on semiconductor platforms to the real world. An ideal all-optical switch is the one that poses the following characteristics. It would only require as little as sub Pico joule (pJ) of energy to switch with at least 20dB switching contrast. Beside compactness, it is desirable to integrate such a device with already established optoelectronics devices on a planar integrated photonic circuit. One category of devices that has a great potential to meet those requirements is micro-ring resonators.

1.3 Optical Signal Processor Using Ring Resonator

First of all, let's introduce Ring Resonator, which is simply a waveguide shaped into a ring structure. When an input electric field, E_i (chapter 3) is coupled to the ring waveguide through an external bus waveguide, a positive feedback is induced and the field inside the ring resonator, E_r starts to build up. Coupling between the straight and the ring waveguide is achieved through the evanescent wave. Therefore, the gap and coupling length between them determine how much power is coupled from the straight waveguide to the ring waveguide. The feedback mechanism is simply induced by the ring waveguide and there is no need for any Bragg gratings, mirrors, or distributed feedback waveguides which are more difficult to fabricate. In such configuration, only certain wavelengths will be allowed to resonate inside the ring waveguide, thus frequency selectivity is obtained. In this thesis we use nonlinear signal in Ring Resonator.

Nonlinear optical elements and devices can be either integrated in photonic circuits [7] or used in a free-standing configuration [8]. Nonlinear optics can enable signal processing without the requirement of external electrical, mechanical, or thermal control [8-11]. The response time of properly designed nonlinear optical devices is limited fundamentally by the nonlinear response time of the constituent materials [12-15].

Photons do not interact with each other in vacuo. In order to perform nonlinear optical signal processing operation, the properties of a medium through which the light travels must be modified by the light itself. Optical signals then propagate differently as a result of their influence on the medium.

Nonlinear optical signal processing elements utilize the illumination-dependent real and imaginary parts of the index of refraction [8]. Depending on the material and spectral position, the refractive index and absorption of a given nonlinear material can either increase or decrease with increasing illumination.

1.4 Optical Security by Quantum Processing

A security by the quantum technique is recommended to provide such a requirement. One of quantum technique is QKD, which make it possible for communication two parties between Alice and Bob, for sharing a private random number to use as a key. As illegitimate access to the distribution channel disturbs the quantum state of a photon carrying a random bit, Alice and Bob can evaluate the secrecy of the channel from the transmission bit error. Unless the error exceeds the threshold, even if many photons are lost during the transmission, Alice and Bob can finally distill a secure random number from a set of received bits after error correction and privacy amplification. To date QKD is the only form of information that can provide the perfect communication security [16-20]. The use of QKD has been proposed in many research works [21-26]. Recently, Such as et al [27] have reported the interesting concept of continuous variable quantum key distribution (QKD) via a simultaneous optical-wireless up-down-link system, where they have shown that the continuous variable quantum key could be performed via chaotic signals generated in a nonlinear micro-ring resonator system with appropriate soliton input power and micro-ring

resonator parameters [28]. They have also shown that the different time slot entangled photons can be formed randomly and can be used to select two different frequency bands for up-down-link converters within a single system. Yupapin et al [29] have proposed a new technique for QKD) that can be used to make the communication transmission security and implemented by a small device such as mobile telephone handsets. This technique has proposed the Kerr nonlinear type of light in the micro ring resonator to generate the superposition of the chaotic signal via a four-wave mixing type that introduces the second-harmonic pulse. A technique used for communication security via quantum chaotic has been proposed by Yupapin and Chunpang [30], where the use of quantum-chaotic encoding of light traveling in a fiber ring resonator to generate two different codes, i.e., quantum bits and chaotic signal are presented. Mitatha et al. [31] have proposed the design of secured packet switching using nonlinear behaviors of light in micro ring resonator which can be made high-capacity and security switching. Such a system can also be used for the tunable band pass and band stop filters.

In this work, multi-photons are considered for improvement of the secret information key rate is developed, which is an easier implementation than a single photon, because a single photon is generated surprisingly difficult. When multi-photons are contained into each pulse, then Eve might detect or tap some photon. The latter approach is prevented by Error Correction and Privacy Amplification in QKD technique and the no-cloning theorem of quantum mechanics: it is impossible to copy the unknown polarization state of photon without modifying the original in a noticeable way. The number of photons in any given pulse is affected directly by security bit rate generated. When high bit rate is generated the longest of distance is increased for transmission over fiber optic.

1.5 Goal and Scope of Thesis

The main objectives of this thesis can be divided into two parts:

1. To introduce BB84 protocol for QKD by using waveguide PANDA ring resonators system technique.

2. Multi-photons are generated in our proposed system to increase the high security bit rate, and distance as follows mathematic equation.
3. To compare the experiment result with two previous works such as BB84 [32] and Multi-Layers QKD Protocol Using Correlated Photon of Dark-Soliton Array in a Wavelength Router [35].

1.6 Thesis Outlines

This thesis presents Optical Ring Based Quantum Key Distribution:

- Chapter 1 gives an introduction to the subject of the thesis and generalized Optical Signal Processor Using Ring Resonator. We also introduce Optical and Quantum Security using Optical Techniques.
- Chapter 2 describes some of Literature reviews and also describes about the relative works
- Chapter 3 presents some the relation theoretical such as BB84 protocol, nonlinear refraction, nonlinear ring resonators, add/drop filter, PANDA ring resonator. We have described about light pulses propagating, final we have also presented quantum information theories such as photon, entangled photon, single photon and quantum bit.
- Chapter 4 presents to correlate photons are generated for using quantum key within the series PANDA ring resonator and add/drop filter, by using soliton pules is input and we also present the experiment result is shown and compared with other relative works, which is also main of the thesis.
- Chapter in this thesis is chapter 5 presents discussion about Error reconciliation and Privacy amplification to verify security of QKD technique. The conclusion and future work of this thesis are presented also.

Chapter 2

Literature reviews

For a good understanding for our purpose in this thesis, some relative works are presented to see over views such as theoretical support, technique, devices and experimental result. There are some works in previous are presented as following:

2.1 Relation works

2.1.1 Quantum Cryptography by Nicolas Gisin [32]

Nicolas Gisin has experimented typical system for quantum cryptography with the BB84 four-states protocol using the polarization of photons using polarization coding: LD (Laser Diode); BS (Beam Splitter), F (neutral density filter), PBS (Polarizing Beam splitter), half wave plate ($\lambda/2$), and APD (Avalanche Photodiode) as shown in figure 2.1.

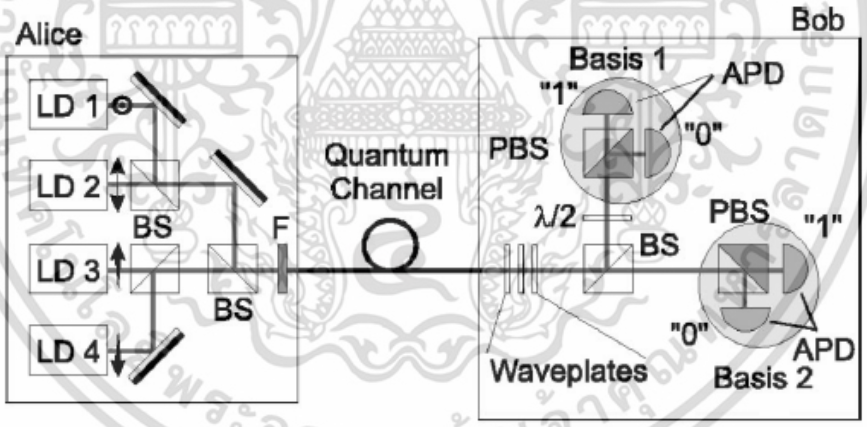

Figure 2.1 System for quantum cryptography [32]

Alice's system consists of four laser diodes (LD1-LD4), which emit short classical photon pulses polarized (Beam Splitter: BS) at -45°, 0°, +45°, and 90°. For a given qubit, a single diode is triggered. The pulses are then attenuated by a set of filters (F) to reduce the average number of photons to well below 1, and sent along the quantum channel to Bob.

It is essential that the pulses remain polarized for Bob to be able to extract the information encoded by Alice; polarization mode dispersion may depolarize the photons, which depend on polarization modes [34]. This sets a constraint on the type of lasers used by Alice.

Upon reaching Bob (Bob system), the pulses are extracted from the fiber, and travel through a set of waveplates used to recover the initial polarization states by compensating for the transformation induced by the optical fiber. The pulses then reach a symmetric BS to implement the basis choice of Bob's side. Transmitted photons are analyzed in the vertical-horizontal basis with a polarizing beamsplitter (PBS) and two photon-counting detectors. The polarization state of the reflected photons is first rotated with a waveplate by 45° (-45° $\rightarrow$ 0°). The photons are then analyzed with a second set of PBSs and photon-counting detectors. This implements the diagonal basis. For illustration, let us follow a photon polarized at +45°. We see that its state of polarization is arbitrarily transformed in the optical fiber. At Bob's end, the polarization controller must be set to bring it back to +45°. If Bob chooses the output of the BS corresponding to the vertical-horizontal basis, the polarization has experienced an equal probability of reflection or transmission at the PBS, yielding a random outcome. On the other hand, if he chooses the diagonal basis, its state is rotated to 90°. Then The PBS has reflected state of photon with unit probability, yielding a deterministic outcome.

From purpose of this work, researcher experimented the Quantum Bit Error Rate (QBER) is defined as the ratio of wrong bits to the total number of bits received and is normally on the order of a few percent. The function of rates is followed:

$$QBER = QBER_{opt} + QBER_{\det} + QBER_{acc} \tag{2.1}$$

$$QBER_{opt} = \frac{1-V}{2} \tag{2.2}$$

$$QBER_{\det} = \frac{np_{dark}}{2\eta\mu t_{link}} \tag{2.3}$$

$$QBER_{acc} = \frac{p_{acc}}{2\mu} \tag{2.4}$$

where p_{dark} is probability of dark count, p_{acc} is the probability of finding a second pair within the time window, knowing that a first one was created (Entangle Photon). η is efficient of photon's being detected, n is number of detector, μ is number of photon.

Let's analyze these three contributions. The first one, $QBER_{opt}$ is an optical error rate, which is independent of the transmission distance (t_{link}). It is considered as a measure of the optical quality of the setup, depending only on the polarization or interference fringe contrast. This technique needed to obtain and, more importantly, to maintain a given $QBER_{opt}$ is an important criterion for evaluating different QC setups. In polarization-based systems, it is rather simple to achieve a polarization contrast of 100:1, corresponding to a $QBER_{opt}$ of 1%. In fiber-based QC, the problem is to maintain this value in spite of polarization fluctuations and depolarization in the fiber link. A visibility of 98% thus translates into an optical error rate of 1%, that calculate from function above (equation 2.2). Such a value implies the use of well-aligned and stable interferometers. In bulk optics, perfect mode overlap is difficult to achieve, but the polarization is stable.

The second contribution, $QBER_{det}$, which following as equates 5.3 (Chapter 5), that increases with distance, since the dark-count rate remains constant while the bit rate goes down like t_{link} . It depends entirely on the ratio of the dark-count rate to the quantum efficiency. At present, good single-photon detectors are not commercially available for telecommunications wavelengths. The span of quantum cryptography is not limited by decoherence. As $QBER_{det}$ is essentially independent of the fiber length, it is detector noise that limits the transmission distance.

Finally, the $QBER_{acc}$ contribution is present only in some two-photon (entangle photon), which has function as equation (2.4).

The bit rate keys are calculated by a function of the distance. R_{sift} (sift key rate) and QBER (i.e.; A) are given as a function of t_{link} in equation (2.5).

$$R_{sift} = \frac{f_{rep}\mu t_{link}\eta}{2} \tag{2.5}$$

The bit rate keys are decreases exponentially with length by the fraction of bits lost due to error correction and privacy amplification is a function of QBER and depends on Eve's strategy. The number of remaining bits R_{net} is given by the sifted-key rate multiplied by the difference between the Alice-Bob mutual Shannon information $I(\alpha,\beta)$ and Eve's maximal Shannon information $I_{\max}(\alpha,\varepsilon)$ as equation 2.6.

$$R_{net} = R_{sift}\left[I(\alpha,\beta) - I_{\max}(\alpha,\varepsilon)\right] \tag{2.6}$$

The difference between $I(\alpha,\beta)$ and $I_{\max}(\alpha,\varepsilon)$ is calculated here according to equations 2.9 and 2.10.

$$I(\alpha,\beta) = 1 - H(A) \tag{2.7}$$

$$H(A) = -\left[A\log_2(A) + (1-A)\log_2(1-A)\right] \tag{2.8}$$

$$I(\alpha,\beta) = 1 + A\log_2(A) + (1-A)\log_2(1-A) \tag{2.9}$$

$$I_{\max}(\alpha,\varepsilon) \approx 2.9A \tag{2.10}$$

R_{net} is obtain for different wavelengths as shown in figure 2.2 every curve is decreased, then, due to error correction and privacy amplification, the bit rates fall rapidly down to zero.

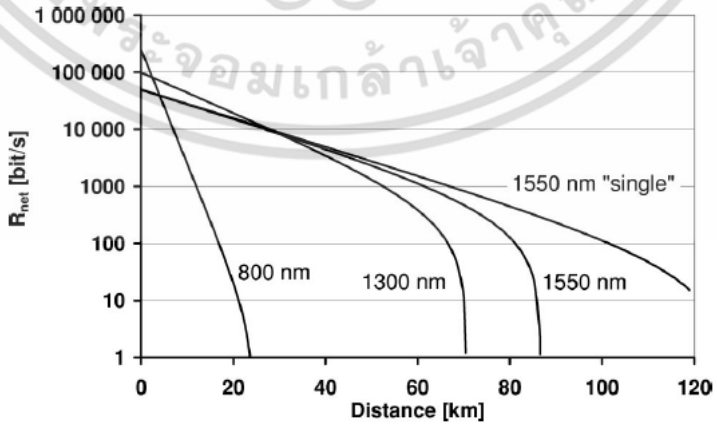

Figure 2.2 The experiment result of system [32]

The bit rate transfer and distance are shown in experimental results (figure 2.2) by chosen parameters are as follows: photon is used $\mu_0 = 1$ with pulse rates (f_{rep}) f_{rep}=*1MHz*, and $\mu_0 = 0.1$ with f_{rep}=*10 MHz* for faint laser pulses, fiber losses of 0.25 dB/km; detector efficiencies of η =10%; dark-count probabilities (P_{dark}) of 10^{-7}, 10^{-5}, and 10^{-5} for 800 nm, 1300 nm, and 1550 nm, respectively. When comparing the curves 1550 nm (f_{rep} =10MHz, μ_0=0.1) and 1550 nm (f_{rep} =1MH, μ_0=1) as shown in Fig 4.10. In the figurer has shown us evidently bit rate of 10.49kbit/s and 110b/s at 27km, 90km of distance for the first 1550nm (μ_0=0.1, f_{rep}=10MHz). Other 1550(μ_0=1, f_{rep}=1MHz) the security bit rate of 10.49kbit/s, 335bit/s, and 12.17bit/s at 27km, 90km, and the maximum of distance at 120km. In this case for 800 nm, 1300 nm of frequency band are not considered in this thesis.

Optical quantum cryptography is based on the use of single-photon Fock states. Unfortunately, these states are difficult to realize experimentally. Nowadays, practical implementations rely on faint laser pulses or entangled photon pairs. Hence both possibilities suffer from a small probability of generating more than one photon or photon pair at the same time. Multi-photon pulses do not necessarily constitute a threat to security, but they limit the key creation rate because they imply that more bits must be discarded during key distillation. This fact is based on the assumption that all photons in a pulse carry the same qubit. In this point, Phichai Yupao presented multi-photon generated by used series Ring resonator as discussed in next section.

2.1.2 Multi-Layers QKD Protocol Using Correlated Photon of Dark Soliton Array in a Wavelength Router by Phichai Yupao [35]

Phichai Yupao presents quantum key distribution, the system is developed to improve the secret information key rate (R_{net}) and reduce the opportunity is correctly chosen the basis for photon polarization measurement by Eve, in the case of photon number splitting attack (PNS) by using multi-photon, for optical communication applications.

Multi-photons are generated in dark soliton pulses within a micro ring resonator system. Initially, dark soliton is used for input into a micro ring resonator system, where the dynamic dark soliton is controlled and the wavelength band generated. The

quantum key distribution is formed by using the correlated photon of wavelength, where the quantum keys (codes) are generated and recovered via the quantum processor in the wavelength add/drop filter as shown in figure 2.3. The purpose system consists two parts such as Alice's and Bob's part. Alice's part consists light source, which is sued for input pulse (dark soliton) into series ring (R_1 R_2 and Rd), the large band width signals are generated to be qubits, then Alice has chosen random basis, which is represented by the four polarization orientation angles as [0°, 90°, 45°, 135°] the qubits are encode by bream splitter(BS) and the pulses are attenuated by Neutral density filter (F) to reduce the average number of photons, and sent along the quantum channel to Bob into Non-zero dispersion shifted fiber (NZDSF).

When Bob receives signal as wavelength λ_1, which decode at drop port of add/drop filter R_{d1}, the pulses are extracted from the fiber. They travel through a set of waveplates used to recover the initial polarization states by compensating for the transformation induced by the optical fiber. The pulses then reach a symmetric BS, implementing the basis choice. Transmitted photons are analyzed in the vertical-horizontal basis with a polarizing beamsplitter (PBS) and two photon-counting detectors. The polarization state of the reflected photons is first rotated with a waveplate (RP) by 45° (-45° → 0°).

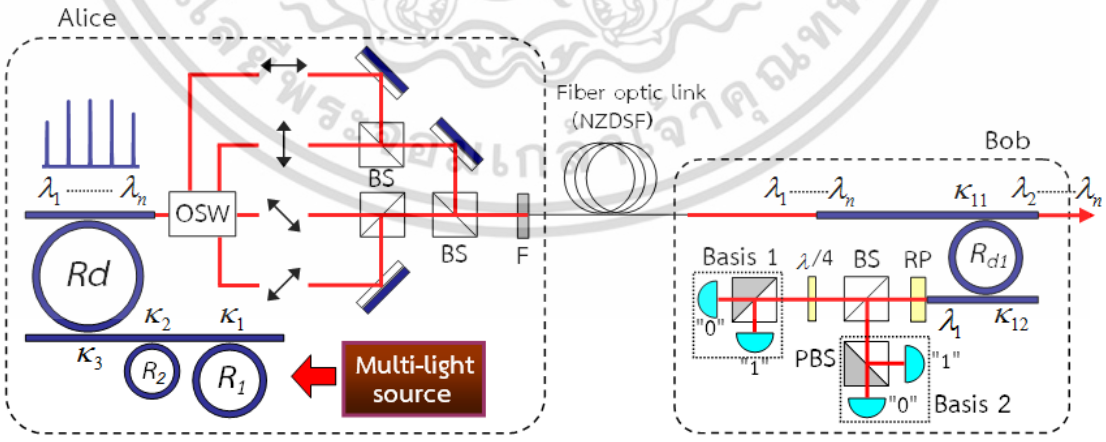

Figure 2.3 The experiment result of system [35]

The parameters are chosen as followed: f_{rep}=500MHz, $\mu_0 = 1$ with fiber losses of 0.25 dB/km; detector efficiencies of η=10%; dark-count probabilities $P_{dark}= 10^{-5}$. The result of experiment has shown us the security bit rate as 5.25Mb/s, 115.20k/s the maximum of distance is 227km as shown in figure 2.4.

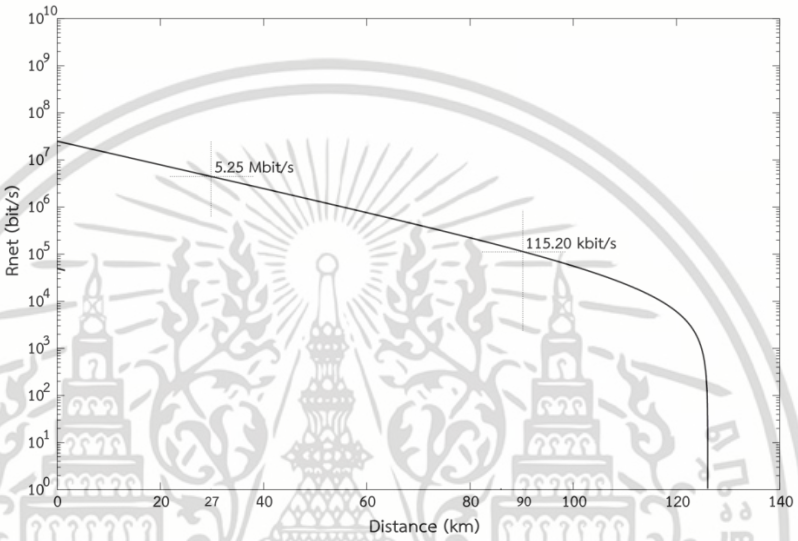

Figure 2.4 The experiment result of system [35]

Although. The system has generated large bandwidth and also generated more R_{net} than Quantum Cryptography by Nicolas Gisin [32] as discussed in session 2.1.1 above. The system requires the Kerr effect within the device, from which the switching time can be decreased by the nonlinear effects, and size of device also.

2.2 Summary

In this chapter, we have presented two relative works such as BB84 [32], and Multi-Layers QKD Protocol using Correlated Photon of Dark Soliton Array in a Wavelength Router [35].

The first work optical quantum cryptography is based on the use of single-photon Fock states. Unfortunately, these states are difficult to realize and implement experimentally. Other way, a single photon is generated difficultly whit special device.

The second work Phichai Yupao presented multi-photon generated by used series Ring resonator. Although, the series ring system can generate large bandwidth and can also generate more R_{net} than first work. The system requires the Kerr effect within the device, from which the switching time can be decreased by the nonlinear effects. In other way the second work uses dark soliton is input light, that is difficult to generate and implement, the system is bigger devices than our propose work, so we have introduced PANDA ring resonator instead of series ring, that can generate multi-photons ,reduce the size of device and increase high capacity of channel for optical communication.

Chapter 3

Theoretical Background

3.1 Quantum Cryptography Protocol

3.1.1 BB84 Protocol

According to quantum theory, light waves are propagated as discrete particles known as photons. A photon is a massless particle, the quantum of the electromagnetic field, carrying energy, momentum, and angular momentum. The polarization of the light is carried by the direction of the angular momentum or spin of the photons. A photon is passed through a polarization filter. Information about the photon's polarization is determined by using a photon detector to determine whether it passed through a filter.

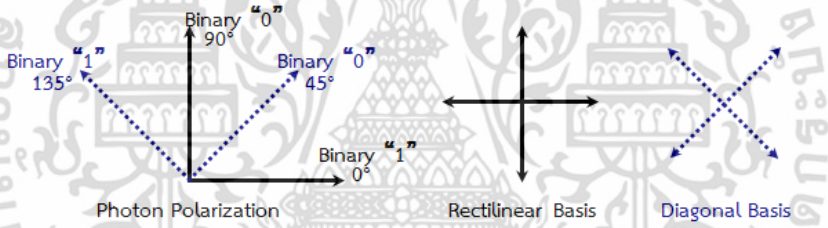

Figure 3.1 Four states of BB84 protocol

The first published paper to describe a cryptographic protocol using these ideas to solve the key distribution problem was written in 1984 by Charles Bennett and Gilles Brassard [33] as this protocol is now known. They presented their work at an IEEE conference in India, quite unnoticed by the physics community at the term. In it, Bennett and Brassard described an unconditionally secure quantum key distribution system.

BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. Pairs of orthogonal states are referred to as a basis. The usual polarization state pairs used are either the rectilinear basis of vertical (90°) and horizontal (0°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handedness as shown in figure 3.1. Any two of these bases are conjugate to each other, and

so any two is used in the protocol. Below the rectilinear and diagonal bases are used as shown in table 3.1.

Table 3.1 Basis photon polarization

Basis	0	1
+	↑	→
x	↗	↖

The table above shows the basic of photon polarization, which is presented by BB84 protocol as follow these steps below:

(1) Alice creates a random bit (0 or 1) and then randomly selects one of her two bases (rectilinear or diagonal in this case) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis, as shown in the table to the left. So for example a 0 is encoded in the rectilinear basis (+) as a 0° or a 90° as a vertical polarization state, and a 1 is encoded in the diagonal basis (x) as a 45° or 135° state.

(2) Alice then transmits a single photon in the state specified to Bob, using the quantum channel. This process is then repeated from the random bit stage, with Alice recording the state, basis and time of each photon sent.

(3) According to quantum mechanics (particularly quantum indeterminacy), no possible measurement distinguishes between the four different polarization states, as they are not all orthogonal. The only possible measurement is between any two orthogonal states (base). So, for example, measuring in the rectilinear basis gives a result of horizontal or vertical. If the photon was created as horizontal or vertical (as a rectilinear eigenstate) then this measures the correct state. When the photon was created as 45° or 135° (diagonal eigenstates) then the rectilinear measurement instead returns either horizontal or vertical at random. After this measurement the photon is polarized in the state it was measured in (horizontal or vertical), with all information about its initial polarization lost.

(4) As Bob does not know the basis the photons were encoded in, all he can do it to select a basis at random to measure in, either rectilinear or diagonal. He does this

for each photon he receives, recording the time, measurement basis used and measurement result.

(5) After Bob has measured all the photons, he communicates with Alice over the public classical channel. Alice broadcasts the basis each photon was sent in, and Bob the basis each was measured in.

(6) They both discard photon measurements (bits) where Bob used a different basis, which is half on average, leaving half the bits as a shared key.

(7) To check for the presence of eavesdropping Alice and Bob now compare a certain subset of their remaining bit strings. If a third party (usually referred to as Eve, for 'eavesdropper') has gained any information about the photons' polarization, this introduces errors in Bobs' measurements. If more than *p* bits differ they abort the key and try again, possibly with a different quantum channel, as the security of the key cannot be guaranteed. *p* is chosen so that if the number of bits known to Eve is less than this, privacy amplification can be used to reduce Eve's knowledge of the key to an arbitrarily small amount, by reducing the length of the key.

Table 3.2 The BB84 protocol system

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↗	↑	↖	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↖	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIC								
Shared secret key	0		1			0		1

The simplest attack for Eve consists in intercepting all photons individually, measuring them in a basis chosen randomly between the two bases used by Alice, and sending new photons to Bob prepared according to her result.

Before they are finished, however, Alice and Bob agree upon a random subset of the bits to compare to ensure consistency. If the bits agree, they are discarded and the

remaining bits form the shared secret key. In the absence of noise or any other measurement error, a disagreement in any of the bits compared would indicate the presence of an eavesdropper on the quantum channel. This is because the eavesdropper, Eve, were attempting to determine the key, and she would have no choice but to measure the photons sent by Alice before sending them on to Bob. This is true because the no cloning theorem assures that she cannot replicate a particle of unknown state [36] this procedure is outlined in table 3.3.

Table 3.3: The BB84 protocol system with Eve

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↖	↑	↖	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↖	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↖	→	↗	↑	→
PUBLIC DISCUSSION OF BASIC								
Shared secret key	0		0			0		1
Error in key	√		X			√		√

Since Eve does not know what bases Alice used to encode the bit until after Alice and Bob discuss their measurements, Eve forces to guess. If she measures on the incorrect bases, the Heisenberg Uncertainty Principle ensures that the information encoded on the other bases is now lost. Thus, when the photon reaches Bob, his measurement is random and he reads a bit incorrectly 50% of the time. Given that Eve chooses the measurement basis incorrectly on average 50% of the time, 25% of Bob's measured bits differ from Alice [37] as shown in figure 3.2 If Eve has eavesdropped on all the bits then after k bit comparisons by Alice and Bob (sift key) [38], they have reduced the probability that Eve (P_e) has undetected by following equation (3.1). The chance that an eavesdropper learned the secret is thus negligible if a sufficiently long sequence of the bits is compared.

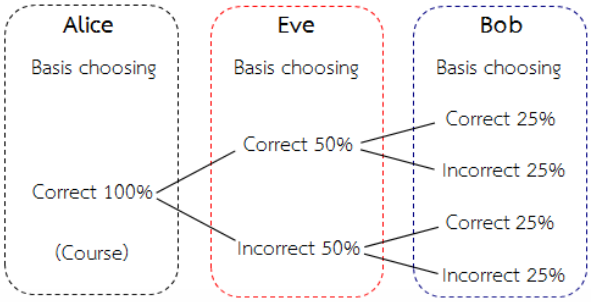

Figure 3.2 Probability of Eve to detect signal

$$P_e = 1 - \left(\frac{3}{4}\right)^k \tag{3.1}$$

When k = 72 in sift key, thus, P_e=0.999999999.

3.1.2 B92 Protocol

In 1992, Charles Bennett proposed what is essentially a simplified version of BB84 in his paper, "Quantum cryptography using any two non-orthogonal states" [64]. The key difference in B92 is that only two states are necessary rather than the possible 4 polarization states in BB84. As shown in figure 3.3, binary 0 can be encoded as 0 degrees in the rectilinear basis and other binary such as 1 can be encoded by 45 degrees in the diagonal basis. Like the BB84, Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases she must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he does not measure anything; a condition in quantum mechanics which is known as an erasure [39]. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

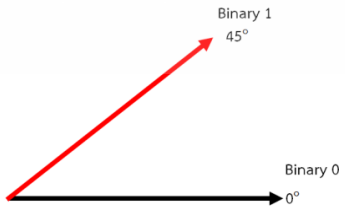

Figure 3.3 Two states of B92 protocol

3.2 Photon

Photons have properties quite different from those of classical particles. They have energy $h\nu$ as given by equation 3.2, zero rest mess, momentum $\hbar k$, spin $\hbar$, they are non-interacting particles following the Bose statistics. A laser beam contains a large number of these particles and the measurement of the beam intensity corresponds to a measurement of the flux of photon as shown in table 3.4. The photons, which were created by the emission process, that is the de-excitation of the atoms via stimulated or spontaneous emission, are destroyed in the detection process. This in turn creates an electron-hole pair in the detector material.

Table 3.4 Example of the photon flux and photon density of typical fields.

Type of light	Intensity I (W/m^2)	Elec. Field E (V/m)	Photon density (m^{-3})	Photons/mode
White light (T=6000 K)	10^3	10^3	10^{13}	10^{-4}
Spectral lamp	10^4	$3x10^3$	10^{14}	10^{-2}
CW laser	10^5	10^4	10^{15}	10^{10}
Pulsed laser	101^3	10^8	10^{23}	10^{18}

In the table 3.4 for simplicity it is assumed that all fields have the same wavelength of $\lambda = 500nm$ and thus all photons have the same energy $h\nu = 2.510^{-19} J$. In the case of the pulsed laser the photon density inside the pulse has been evaluated. The table shows that we can consider a mode to contain a large number of photons only for laser beams.

The basic postulate of the quantum interpretation is that electromagnetic radiation consists of particle-like discrete bundles of energy called photons or quanta. Each photon has an energy E that depends only on the frequency ν of the radiation and is given by

$$E = h\nu = h\frac{c}{\lambda} \tag{3.2}$$

where $h = 6.626\times10^{-34}\text{J.s}$ is Planck's constant. Each photon interact an all-or-nothing manner; it either gives up all its energy or none of it.

Since photons travel at the speed of light, they must, according to relativity theory, have zero rest mass: hence, their energy is entirely kinetic. If a photon exists, then it moves at the speed of light, c; if it ceases to move with speed c, it ceases to exist. For $m_0 = 0$, the relativistic momentum-energy relation becomes $E = pc$. Thus, each photon has a momentum of

$$p = \frac{E}{c} = \frac{h\nu}{c} = \frac{h}{\lambda} \tag{3.3}$$

From the quantum point of view, a beam of electromagnetic energy is composed of photons traveling at the speed c. the intensity of the beam is proportional to the number of photons crossing a unit area per unit time. Hence, if the beam is monochromatic (one frequency), the intensity is given by

$$I = (\text{energy of one photon}) \times \frac{\text{number of photons}}{\text{area} \times \text{time}} \tag{3.4}$$

Finally, we note for convenience in calculations the following expression in nonstandard units:

$$h = 4.136\times10^{-15}\text{eV.s} \tag{3.5}$$

$$hc = 12.4\text{keV.A}^0 \tag{3.6}$$

where $1\text{ev} = 10^{-3}\text{keV} = 1.602\times10^{-19}\text{J}$ and $1\text{A}^0 = 10^{-10}\text{m}$.

3.3 Polarization of light

The polarization of the tangential to the field was described by the vector $p(t)$ which gave the direction of the electric field tangential to the waveform. For linearly polarization light p fix. For circularly polarized ling p rotates at the optical frequency. It is possible to design optics, which decomposes a light field into two orthogonal modes. The amplitudes of

the two modes are equal to the projection of p onto the chosen axes. For example, a horizontal/vertical polarizing beam splitter projects the field onto a horizontally polarized mode and a vertically polarized more. These two modes exit through different ports of the beam splitter. Similarly, one can use a diagonal/anti-diagonal and polarizing beam splitter to decompose the field into linearly polarized field 45 degree and 135 degree away from horizontal. With slightly more effort it also possible to create a left/right circular polarizing beam splitter which decompose the field into clockwise and anti-clockwise rotating circular polarizations.

Suppose we fine a string of single photons at a horizontal/vertical polarizing beam-splitter. As we have note, classically such a device directs horizontally polarized light in one direction and vertically polarized light in the other. Thus, the photons are define that exit through the horizontal port of this beam splitter as in the horizontal sate,

$$|H\rangle \tag{3.7}$$

Similarly, we define photons that exit through the vertical port as in the vertical state,

$$|V\rangle \tag{3.8}$$

By “exit through the horizontal port” we mean that a detector placed at the output of the horizontal port detects a photon, or equally a photon detector placed at the vertical port does not detect a photon. These situations are illustrated in figure 3.4. The symbol for the state $|-\rangle$, is referred as a key. These definitions are sensible because a photon which exits through the horizontal port of the beam splitter and is passed through another polarizing beam splitter certainly exits through horizontal port. A similar definition applies to vertical photons. The diagonal single photon state $|D\rangle$, and anti-diagonal state $|A\rangle$ is defined in a similar way be analyzing the beams with a diagonal/anti-diagonal polarizing beam splitter. So far this is straightforward. The physics of classical polarized beams and single photon looks the same. Things become interesting when we to mix up the polarizations

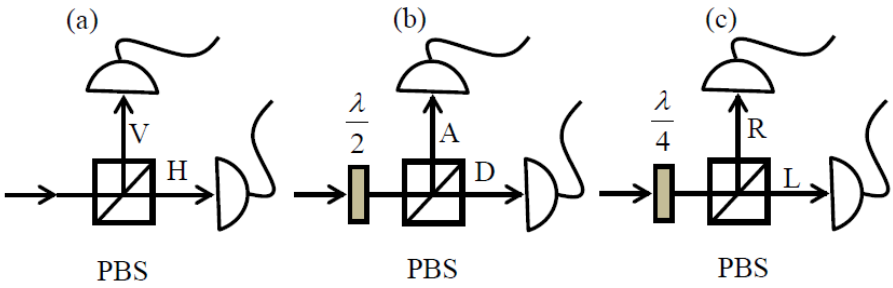

Figure. 3.4 Operational definition of different polarization state. PBS is a polarizing beam splitter. $\lambda/2$ is half-wave plate, $\lambda/4$ is a quarter-wave plate. (a) horizontal-vertical polarization, (b) diagonal polarization, (c) right-left circular polarization.

If we send a diagonally polarized classical beam of light into a horizontal/vertical polarizing beam splitter then, half the beam exits through the horizontal port and half exits through their vertical port. What happen if single photon is sent in the state $|D\rangle$ through this beam splitter? As we have discussed in the previous sections the photons cannot be divide, in the sense that a detector placed at one of the output ports either detect a whole photon or no photon. Instead they must go one way or the other. To be consistent with the classical result for many photons it must be that they go one way 50% of the time and the other way the other 50% of the time. The direction an individual photon goes $|D\rangle$ photons behave at a diagonal/anti-diagonal polarizing beam splitter: they all exit through the diagonal port. That is they all behave perfectly predictably an identically. Yet when these identically behaving photons are sent into a horizontal /vertical beam splitter we have argued some must take one path and other take the other. Thus the path an individual photon in the state $|D\rangle$ takes through the horizontal/vertical beam splitter is not specified. All that is specified is that on average half the photons go one way and half go the other.

This example illustrates the fact that in quantum mechanics it is probabilities of outcomes, not particular outcomes that are predicted. The photon in the state emerges from the diagonal port of a diagonal/anti-diagonal beam splitter, its reaction to a horizontal/vertical beam splitter is as random as a flip of a coin. It is tempting to think that maybe there are other variables (perhaps hidden to us) that do determine in a precise way the polarization behavior of individual photons under all conditions. However such a

possibility can be ruled out experimentally. We are forced to accept the intrinsic indeterminacy of the quantum world.

Continuing our discussion of polarization state, we can also introduce the right circular single photon polarization state $|R\rangle$, and the left circular state $|L\rangle$, in an analogous way to states. A photon in state randomly takes one port or the other when sent into either a horizontal/vertical or a diagonal/anti-diagonal beam splitter. A photon in state $|L\rangle$ behaves in the same way. Similarly, a photon in state $|H\rangle$ gives a random result for both diagonal/anti-diagonal and right/left circular polarizing beam splitters and so on for the other states.

In this session, we introduced the idea of a single, polarized photon. For example we described a light beam as being in the state $|H\rangle$ if in some time interval there is unit probability that one and only one photon is detected at the horizontal output of a horizontal/vertical polarizing beam splitter placed in the beam path. There is zero probability a photon is found at the vertical output in the same time interval. A beam in the $|V\rangle$ is conversely only found at the vertical output. It is clear that such light states could be used to carry bits of information. For example, we could assign the value "zero" to the $|H\rangle$ state and "one" to the $|V\rangle$ state. A string of horizontal and vertically polarized photon could then faithfully represent an arbitrary bit string.

However, being quantum objects, photon offer more possible manipulations than classical carriers of bits. In particular, there are not only zero's and one's, they also have superposition of zeros and ones such as the diagonal state $|D\rangle = \frac{1}{2}\left(|H\rangle + |V\rangle\right)$. Indeed bits can just as effectively be encode in such superposition states, for example using $|D\rangle$ as a zero and $|A\rangle = \frac{1}{2}\left(|H\rangle - |V\rangle\right)$ as a one. Because of these extra degrees of freedom we refer to information digitally encoded on quantum system (such as photons) as quantum bits or qubits.

One non-classical feature of encoding in this way is the fact that different bases do not in general commute. Thus, simultaneous, ideal measurements in both bases cannot be made. Furthermore any measurements which obtain any information about values of one bass inevitably disturb the bit values of the other basis. This feature can be used to create a secure communication channel via the technique of Quantum Key Distribution (also referred

to as quantum cryptography). A number of demonstrations of quantum key distribution have been made in optics.

Another feature of qubits are their ability to span all different bit values simultaneously. This is obviously true of a single qubit where the $|D\rangle$ state, then viewed in the horizontal/vertical basis, equally spans the two different bit value (i.e. $H=0$ and $V=1$).

3.4 Phenomena of Nonlinear Optics

3.4.1 Nonlinear Susceptibility

Nonlinear optics is the study of phenomena that occur as a consequence of the modification of the optical properties of a material under intense illumination. Typically, only laser light is sufficiently intense to modify the optical properties of a material. Nonlinear optical phenomena are *nonlinear* in the sense that the induced material polarization is nonlinear in the electric field [40-41]. The general equation that describes the optical field evolution in a dielectric material is given by

$$\nabla^2 \mathrm{E} - \frac{1}{c^2}\frac{\partial^2 \mathrm{E}}{\partial t^2} = -\mu_0 \frac{\partial^2 \mathrm{P}(\mathrm{E})}{\partial t^2} \tag{3.9}$$

where the polarization $\vec{\mathrm{P}}$ characterizes the medium and it is a function of the electric field. In the case of weak nonlinear behavior of the medium, the polarization can be expressed by a Taylor polynomial as

$$\vec{\mathrm{P}} = \underbrace{\varepsilon_0 \vec{\mathrm{E}} + \varepsilon_0 \chi^{(1)} : \vec{\mathrm{E}}}_{linear\ P_L} + \underbrace{\varepsilon_0 \chi^{(2)} :: \vec{\mathrm{E}}\cdot\vec{\mathrm{E}} + \varepsilon_0 \chi^{(3)} ::: \vec{\mathrm{E}}\cdot\vec{\mathrm{E}}\cdot\vec{\mathrm{E}} + \ldots,}_{nonlinear\ P_{NL}} \tag{3.10}$$

where dielectric dispersion is ignored. $\chi^{(1)}$ is the linear susceptibility, :represents the inner tensor product and the second and the third-order tensor $\chi^{(2)}$ and $\chi^{(3)}$ are responsible for the second harmonic generation, and the third-order harmonic generation, respectively.

3.4.2 Optical Kerr Effect

Nonlinear effect in optical fibers is due either to changes in the refractive index with optical power or to scattering phenomenal. The power dependence of refractive index is responsible for the Kerr effect. Depending on the shape of the input signal, the Kerr nonlinearity manifests itself by different effect, such as self-phase modulation, cross-phase modulation, Nonlinear behaviors of light traveling in fiber optic are commonly induced by the effects such as Kerr effects, four-wave mixing, and the external nonlinear pumping power. The device characteristics that suit to implement in the practical communication system has seen. To meet the practical applications, the micro ring and Add/drop parameters are needed to make them satisfy the usual fabrication. The analogy of chaotic signal generation using fiber ring resonator and the related behaviors are described.

The optical Kerr effect (i.e. nonlinear refraction index) results from the third order nonlinear susceptibility $\chi^{(3)}$, which is a fourth rank tensor.

An optical wave is a real quantity and usually expressed as

$$\vec{\mathrm{E}}(t) = \mathrm{Re}\left\{\vec{\mathrm{E}} \exp\, j(\vec{k}\cdot\vec{r} + \omega t)\right\} \tag{3.11}$$

or similarly as

$$\vec{\mathrm{E}}(t) = \frac{1}{2}\vec{\mathrm{E}} \exp\, j(\vec{k}\cdot\vec{r} + \omega t) + c.c. \tag{3.12}$$

where c.c. represents the complex conjugate of the preceding term. Thus, an x-polarized optical wave, propagating in the z-direction in an isotropic medium, is represented mathematically as

$$\vec{\mathrm{E}}(t) = \frac{1}{2}\mathrm{E}_x \hat{x} \exp\, j(kz + \omega t) + c.c. \tag{3.13}$$

The third order polarization (mediated by $\chi^{(3)}$) in a material leads to a nonlinear intensity dependent contribution to its refractive index; i.e., the refractive index of the material changes as the incident intensity on the material changes. The susceptibility tensors in

isotropic material can be further simplified as $\chi^{(2)}=0$, due to inversion symmetry; the third order nonlinear susceptibility have one contributing term χ_{xxxx} since the light is x-polarized and there are no means for sourcing additional polarization components.

The linear and nonlinear induced polarizations are

$$P_L = \varepsilon_0(1+\chi^{(1)})E \tag{3.14}$$

$$\begin{aligned} P_{NL} &= P^{(3)} \\ &= \varepsilon_0\chi_{xxxx}(\omega;-\omega,\omega,\omega)E^*EE \\ &\quad + \varepsilon_0\chi_{xxxx}(\omega;\omega,-\omega,\omega)EE^*E \\ &\quad + \varepsilon_0\chi_{xxxx}(\omega;\omega,\omega,-\omega)EEE^* \\ &= 3\varepsilon_0\chi_{xxxx}|E|^2E \\ &= \frac{3}{4}\varepsilon_0\chi_{xxxx}|E_x|^2E \end{aligned} \tag{3.15}$$

respectively. Hence,

$$P = P_L + P_{NL} = \varepsilon_0\left(1+\chi^{(1)}+\frac{3}{4}\varepsilon_0\chi_{xxxx}|E_x|^2\right)E \tag{3.16}$$

The total dielectric constant

$$\varepsilon_r^{tot} = \varepsilon_r + \Delta\varepsilon_r \tag{3.17}$$

where $\varepsilon_r = 1+\chi^{(1)} = n_o^2$ and $\Delta\varepsilon = \frac{3}{4}\chi_{xxxx}|E_x|^2$ after comparing with the expression for P. The refractive index is related to the dielectric constant as:

$$n = \sqrt{\varepsilon_r+\Delta\varepsilon_r} \approx \sqrt{\varepsilon_r} + \frac{\Delta\varepsilon_r}{2\sqrt{\varepsilon_r}} = n_0 + \frac{3\chi_{xxxx}}{8n_0}|E_x|^2 \tag{3.18}$$

The intensity dependent refractive index for a nonlinear material is given by

$$n = n_0 + n_2|E|^2 \tag{3.19}$$

Comparing equation (2.10) and (2.11), the nonlinear refractive index is directly determined by the third-order susceptibility as

$$n_2 = \frac{3\chi_{xxxx}}{8n_0} = \frac{3\chi^{(3)}}{8n_0} \tag{3.20}$$

which characterizes the strength of the optical nonlinearity. The intensity I of an optical wave is proportional to $|E|^2$ as $I = \frac{1}{2\eta}|E|^2$ where η is the impedance of the medium. When comparing the optical response in the same medium, $I = |E|^2$ is taken for simplification.

3.4.3 Optical Chaotic

Optical Chaos is observed in many nonlinear optical systems. One of the most common examples is a ring resonator. One of the most seminal works is published by Ikeda [42] where chaotic behavior in a ring resonator was proposed and experimentally confirmed. Optical Chaos was an exciting field of research in mid-1980s and was expected at that time to lead to production of all optical devices including all optical computers. Researchers realized later the inherent limitation of the optical systems due to the non-localized nature of photons compared to highly localized nature of electrons. Research in Optical Chaos has seen a recent resurgence in the context of studying synchronization phenomena, and in developing techniques for secure optical communications. [42-43]

3.5 Optical micro ring resonator characterization

In applications, the penalty benefits of light traveling in micro ring resonator including the nonlinearity of light in micro ring resonator, optical switching and signal security are described as following details. Yupapin and team [15] have recently reported that the nonlinear output light could be obtained after traveling along the micro ring resonator.

3.5.1 The Optical Micro ring resonator

The architecture of a nonlinear fiber optics ring resonator as illustrated in Figure 3.5, which is constructed by a single fiber coupler and one ring resonator. We assume that the nonlinearity of the fiber ring is of the Kerr-type, i.e., the refractive index is given by [44]

$$n = n_0 + n_2 I = n_0 \left(\frac{n_2}{A_{eff}} \right) P \tag{3.21}$$

where n_0 and n_2 are the linear and nonlinear refractive indexes, respectively. I and P are the optical intensity and optical field power, respectively. The effective mode core area of the fiber is A_{eff} .

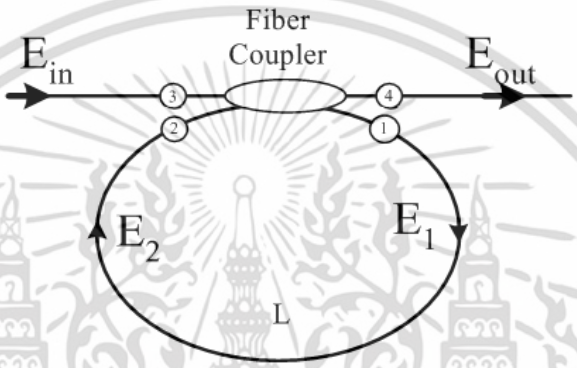

Figure 3.5 Schematic diagram of FORR with Coupler Ring Resonator Filter (SCRR)

The input light is launched in port 3 and the output emerges from port 4. It is worth noting that such a device has no reflected wave or no cross-phase modulation occurred at fiber coupler. The ports 1 and 2 are connected with a fiber having a nonlinear refractive index n_2 , and a linear absorption coefficient α . The fiber coupler has an intensity coupling coefficient κ and γ is a coupling loss for the field amplitude. We assume hereafter (without loss of generality) that the optical fiber ring is on resonance for the operating wavelength in the limit of vanishing incident power, i.e. in the linear case. In addition, we assume that the fiber coupler acts as a point device. The fiber coupler is assumed to be reciprocal and the transmission coefficients for the fields are:

$$\begin{aligned} t_{34} &= t_{21} = (1-\gamma)\sqrt{1-\kappa} \\ t_{31} &= t_{24} = j(1-\gamma)\sqrt{4} \\ t_{32} &= t_{41} = 0 \end{aligned} \tag{3.22}$$

The following relations of the electric fields arise from equation. (3.23):

$$E_1 = t_{31}E_{in} + t_{21}E_2 \tag{3.23}$$

$$E_{out} = t_{34}E_{in} + t_{24}E_2 \tag{3.24}$$

The relation between the electric fields E_1 and E_2 in the stationary state, can be obtained from the nonlinear propagation equation:

$$\frac{\partial E}{\partial Z} = i\frac{2\pi n_2}{\lambda}|E|^2 E - \frac{1}{2}\alpha E \tag{3.25}$$

Integrating the equation (3.23 and 3.24) direct, we can thus obtain the following relation:

$$E_2 = E_1 + \tau\exp(-j\phi) = E_1\tau\exp[-j(\phi_0 + \phi_{NL})] \tag{3.26}$$

where $\phi_0 = kLn_0$ and $\phi_{NL} = kLn_2|E|^2$ are the linear and nonlinear phase shift, $k = \frac{2\kappa}{\lambda}$ is the wave propagation number in a vacuum, and L is the fiber ring resonator length. $\tau = \exp\left(-\alpha\frac{L}{2}\right)$ is a one round trip loss in FORR.

It was discovered in 1979 that the nonlinear response of a ring resonator can initiate a period-doubling route to optical chaos. The basic idea consists of recognizing that the dynamics in FORR correspond to that of a nonlinear map round trip inside the FORR. Mathematically, from equations. (3.) and (3.19, 3.20) the map can be written as

$$E_1(t) = j(1-\gamma)\sqrt{\kappa}E_{in} + (1-\gamma)\sqrt{1-\kappa}\tau E_1(t-t_R)\exp(-j\phi) \tag{3.27}$$

$$E_{n+1} = j(1-\gamma)\sqrt{\kappa}E_{in} + (1-\gamma)\sqrt{1-\kappa}\tau E_n\exp(-j\phi) \tag{3.28}$$

Where the subscript "n" denotes the number of round trips inside the FORR. Using Eq. (3.30), the nonlinear map can be iterated for a given value of the input power $P_{in} = \left(\alpha|E_{in}|^2\right)$. The results show that the output of the FORR can become time dependent even for a CW

input. Moreover, the output becomes chaotic following a period-doubling route in a certain range of input parameters.

The nonlinear phenomenon of optical bistability has been studied in non-fiber resonators since 1976 by placing the nonlinear medium inside a cavity formed by using multiple mirrors [45-46]. The single-mode fiber was used in 1983 as the nonlinear medium inside a ring cavity [47]. Since then, the study of nonlinear phenomena in fiber ring resonators has remained a topic of considerable interest. Consider at steady state, from the Eq. (3.31), we have

$$E_1 = j(1-\gamma)\sqrt{\kappa}E_{in} + (1-\gamma)\sqrt{1-\kappa}\tau\exp(j\phi)E_1. \tag{3.29}$$

While the output field at steady state as

$$E_{out} = (1-\gamma)E_{in}\left[\sqrt{1-\kappa} - \frac{(1-\gamma)\kappa\tau\exp(j\phi)}{1-(1-\gamma)\sqrt{1-\kappa}\tau\exp(j\phi)}\right] \tag{3.30}$$

Thus the normalized of the light field from equation. (2.30) can be expressed as

$$\left|\frac{E_{out}}{E_{in}}\right|^2 = (1-\gamma)^2\left\{1 - \frac{\kappa\left[1-\tau^2(1-\gamma)^2\right]}{1+(1-\gamma)^2(1-\kappa)\tau - 2(1-\gamma)\sqrt{1-\kappa}\tau\cos\phi}\right\} \tag{3.31}$$

A ring resonator is simply a waveguide shaped into a ring structure as shown in figure 3.6. When an input electric field, E_i , is coupled to the ring waveguide through an external bus waveguide, a positive feedback is induced and the field inside the ring resonator E_r , starts to build up. Coupling between the straight and the ring waveguide is achieved through the evanescent wave. Therefore, the gap and coupling length between them determine how much power is coupled from the straight waveguide to the ring waveguide and vise versa. The feedback mechanism is simply induced by the ring waveguide and therefore there is no need for any Bragg Gratings, mirrors, or distributed feedback waveguides which are more difficult to fabricate. In such configuration, only certain wavelengths are allowed to resonate

inside the ring waveguide, thus frequency selectivity is obtained. A resonant mode has a wavelength that satisfies [48-49].

Figure 3.6 Schematic diagram for a ring resonator coupled to a single waveguide

$$m\lambda_m = nL\ ,\ m = \text{integer} \tag{3.32}$$

Here, m is the longitudinal mode number, λ_m is the resonant mode wavelength, *n* is the refractive index of the guiding material, and *L* is the circumference of the ring resonator. The electric field circulating inside the resonator is given by

$$E_r(t) = -j\kappa E_i(t) + rae^{j\phi}(t-\tau) \tag{3.33}$$

where κ and r are the field coupling and transmission coefficients between the straight and ring waveguides such that $\kappa^2 + r^2 = 1, a = e^{-\alpha_0 L/2}$ is the round trip field transmission, α_0 is the propagation loss inside the microring, τ is the round trip time of the ring resonator. The resonator round trip phase, ϕ , is given by

$$\phi = 2\pi \frac{nL}{\lambda} \tag{3.34}$$

The transmitted or throughput field at the output of the straight waveguide, E_t , is given by

$$E_t(t) = rE_i(t) - j\kappa a e^{j\phi} E_r(t-\tau) \tag{3.35}$$

At steady state, the transmission-transfer function of the resonator can be written as

$$\frac{E_t}{E_i} = \frac{r - ae^{j\phi}}{1 - rae^{j\phi}} \tag{3.36}$$

A close examination of equation (3.32) indicates that a ring resonator is very similar to a Fabry-Perot cavity. In the particular case shown in figure 3.9, the corresponding Fabry-Perot cavity would have an input mirror with a field reflectivity *r*, and a fully reflecting output mirror. However, the field propagating inside the ring cavity is a traveling wave in contrast to the Fabry-Perot cavity which resonates a standing wave.

3.5.2 The Optical Add/Drop ring resonator filter

Unlike Fabry-Perot cavities, Bragg gratings, and distributed feedback waveguide devices, the ring geometry permits more than one waveguide to be coupled to the ring resonator. This in return allows multiple input/output accessibility and no need for external circulators to manipulate the input, reflected and throughput data streams. For instance, if one more waveguide is coupled to the filter, an optical add/drop filter is obtained, as shown in figure 3.10.

An incident optical signal composed of multiple wavelengths $\lambda_1 \ldots \lambda_R \ldots \lambda_N$ at the input port coupled into the ring and for a resonant wavelength λ_R, the energy builds up in the resonator despite the small coupling and eventually the signal is coupled into the drop port. Symmetrically, a new signal at resonant wavelength $\lambda_R^{'}$ at the add port couples to the output port through the ring. As a result, such a configuration constitutes a very compact add/drop filter where a channel can be dropped from the WDM spectrum and replaced by a new signal on the same channel. Note that waves with a wavelength away from resonance does not repeat themselves in the ring and the coupled field interferes destructively with the wave in the resonator leading to little energy in the resonator and little dropped power. Residual dropped power at non-resonant wavelengths is possible due to imperfections and can induce inter-band crosstalk that is detrimental to WDM applications. Moreover, if the input channel at λ_R is not completely extinguished, intra-band crosstalk results. This issue is studied and theoretically overcome by varying coupling parameters, inducing loss/gain in ring and inserting additional rings between the two waveguides.

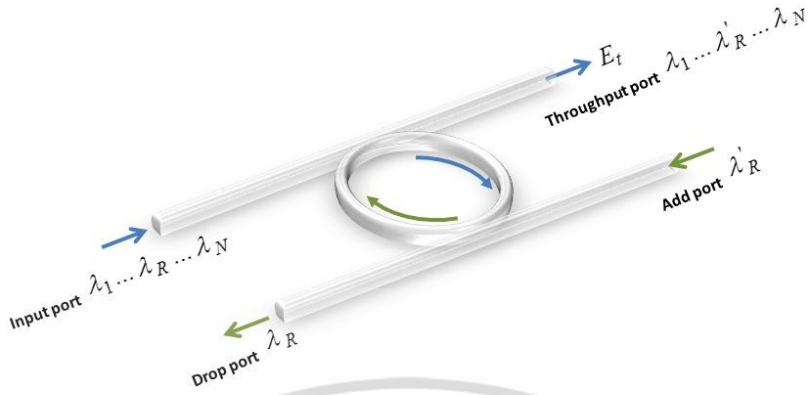

Figure 3.7 Schematic diagram for a ring resonator coupled to two waveguides, in an add/drop filter configuration

Consider the architectures of double coupler ring resonator (DCRR) which sometime called add/drop filters as illustrated in figure 3.8, which are constructed by 2×2 optical couplers.

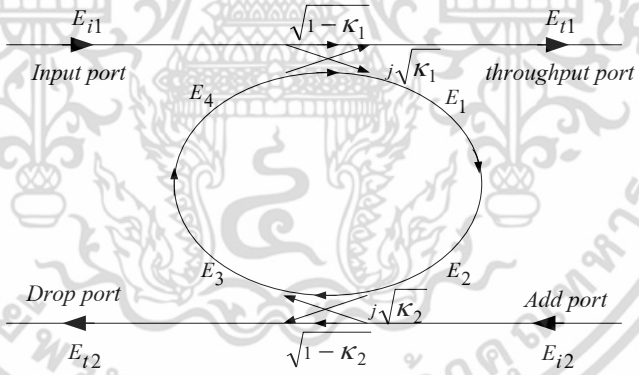

Figure 3.8 The architecture of DCRR or add/drop filter.

Similarly, the optical transfer functions of the ring resonator filters at the throughput port and drop port for an input port E_{i1} can be derived as followed. For the first coupler (κ_1), we have

$$E_{t1} = \sqrt{1-\gamma_1}\left[\, j\sqrt{\kappa_1}E_4 + \sqrt{1-\kappa_1}E_{i1}\right] \tag{3.37}$$

$$E_1 = \sqrt{1-\gamma_1}\left[\, j\sqrt{\kappa_1}E_{i1} + \sqrt{1-\kappa_1}E_4 \right] \tag{3.38}$$

where γ is the loss and the coupling coefficients, respectively. The incoming light of E_{i1} and E_4 are coupled through the first coupler to the output light E_{t1} and E_1 and the output light E_1 is transmitted through the ring becomes output light E_2. According to light transmission theory in linear optical systems, we obtain the following relation between E_1 and E_2

$$E_2 = E_1 e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}} \tag{3.39}$$

where the transmission line length is $\frac{L}{2}$. The second coupler (κ_2) have the following relations:

$$E_{t2} = E_1 e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}} \cdot j\sqrt{1-\gamma_2}\sqrt{\kappa_2} \quad \text{at } E_{i2} = 0 \tag{3.40}$$

$$E_3 = E_1 e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}} \sqrt{1-\gamma_2}\sqrt{1-\kappa_2} \tag{3.41}$$

Using the transmission theory, we obtain E_4 in terms of E_3

$$E_4 = E_3 e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}} \tag{3.42}$$

$$E_1 = \frac{E_{i1} j\sqrt{1-\gamma_1}\sqrt{\kappa_1}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L - jk_nL}} \tag{3.43}$$

$$E_4 = \frac{E_{i1} j\sqrt{1-\gamma_1}\sqrt{\kappa_1}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L - jk_nL}} \sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L - jk_nL} \tag{3.44}$$

By using the upper equations, the transfer function for throughput port and drop port in figure 3.11 can thus be expressed as

Throughput port:

$$\frac{E_{t1}}{E_{i1}}=\frac{-\left(1-\gamma_1\right)\left(1-\kappa_1\right)\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}+\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}}$$
$$=\frac{-\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}+\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}} \quad (3.45)$$

Drop port:

$$\frac{E_{t2}}{E_{i1}}=\frac{-\sqrt{1-\gamma_1}\sqrt{1-\gamma_2}\sqrt{\kappa_1\cdot\kappa_2}e^{-\frac{\alpha}{2}\frac{L}{2}-jk_n\frac{L}{2}}}{1-\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L-jk_nL}} \quad (3.46)$$

The intensity relations for the throughput and drop port can be obtained by normalizing the transfer functions in equations. (3.42) and (3.43) which are given by

$$\frac{I_{t1}}{I_{i1}}=\left|\frac{E_{t1}}{E_{i1}}\right|^2=\frac{1-\left(1-\gamma_1\right)\kappa_1-2\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\cdot\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L}cos\left(k_nL\right)}{1+\left(1-\gamma_1\right)\left(1-\kappa_1\right)\cdot\left(1-\gamma_2\right)\left(1-\kappa_2\right)e^{-\alpha L}}$$
$$+\frac{\left(1-\gamma_2\right)\left(1-\kappa_2\right)e^{-\alpha L}}{-2\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\cdot\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L}cos\left(k_nL\right)} \quad (3.47)$$

$$\frac{I_{t2}}{I_{i1}}=\left|\frac{E_{t2}}{E_{i1}}\right|^2=\frac{\left(1-\gamma_1\right)\left(1-\gamma_2\right)\cdot\kappa_1\kappa_2e^{-\frac{\alpha}{2}L}}{1+\left(1-\gamma_1\right)\left(1-\kappa_1\right)\cdot\left(1-\gamma_2\right)\left(1-\kappa_2\right)e^{-\alpha L}}$$
$$-2\sqrt{1-\gamma_1}\sqrt{1-\kappa_1}\cdot\sqrt{1-\gamma_2}\sqrt{1-\kappa_2}e^{-\frac{\alpha}{2}L}cos\left(k_nL\right) \quad (3.48)$$

For simplification, the calculation of the intensity relation does not take into account coupling losses ($\gamma = 0$) and the following parameters:

$$\begin{aligned} x &= exp\left(-\frac{\alpha}{2}L\right) \\ c_1 &= \sqrt{1-\kappa_1} \\ c_2 &= \sqrt{1-\kappa_2} \end{aligned} \tag{3.49}$$

The intensity relations equations (3.44) and (3.45) are then given by

$$\frac{I_{t1}}{I_{i1}}(\phi) = \left|\frac{E_{t1}}{E_{i1}}\right|^2 = 1 - \frac{\left(1-c_1^2\right)\cdot\left(1-c_2^2x^2\right)}{\left(1-c_1c_2x\right)^2 + 4c_1c_2xsin^2\left(\frac{\phi}{2}\right)} \tag{3.50}$$

$$\frac{I_{t2}}{I_{i1}}(\phi) = \left|\frac{E_{t2}}{E_{i1}}\right|^2 = \frac{\left(1-c_1^2\right)\cdot\left(1-c_2^2\right)\cdot x}{\left(1-c_1c_2x\right)^2 + 4c_1c_2xsin^2\left(\frac{\phi}{2}\right)} \tag{3.51}$$

3.5.3 The PANDA ring resonator

Consider the architectures of PANDA ring resonator is like an add/drop filter, which add more 2 micro rings resonator R_l and R_r as illustrated in figure. 3.9 A schematic diagram of a proposed PANDA ring resonator.

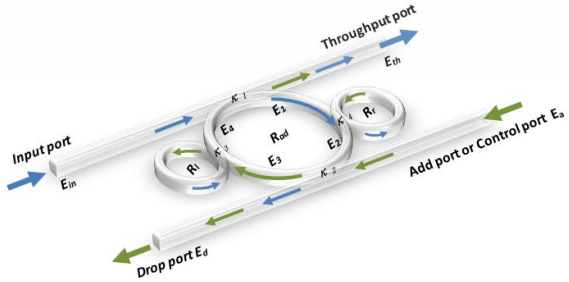

Figure 3.9 A schematic diagram of a proposed PANDA ring resonator.

$$E_1 = \tau_1 E_4 - jE_{in} \tag{3.52}$$

$$E_2 = \exp\left(j\omega T\frac{1}{2}\right)\exp\left(-\alpha L\frac{1}{4}\right)E_1 \tag{3.53}$$

$$E_3 = \tau_2 E_2 - j\kappa_2 E_{a1} \tag{3.54}$$

$$E_4 = \exp\left(j\omega T\frac{1}{2}\right)\exp\left(-\alpha L\frac{1}{4}\right)E_3 \tag{3.55}$$

$$E_{th} = \tau_1 E_{in} - j\kappa_1 E_4 \tag{3.56}$$

$$E_d = \tau_1 E_a - j\kappa_2 E_2 \tag{3.57}$$

Here $E_1 \ldots E_4$ are the fields in the ring at points $1 \ldots 4$, E_a is the add (control) field, E_d is the drop field, E_d is the input field, E_{th} is the through field, κ_1 is the field coupling coefficient between the input bus and ring, κ_2 is the field coupling coefficient between the ring and output bus, T is the time taken for one round trip (round trip time), L is the circumference of the ring, and α is the power loss in the ring per unit length. We assume that this is the lossless coupling, i.e., $\tau_{1,2} = \sqrt{1-\kappa_{1,2}^2}\, T = Ln_{eff}/c$

3.6 Wavelength Range and Attenuation in Optical Fiber

3.6.1 Wavelength Range in Optical Fiber

To provide a very high capacity for optical transmission systems, it is desirable to allow as wide a range as possible for the system operating wavelengths. The choice of operating wavelength range depends on several factors, including fiber type, source characteristics, system attenuation range, and dispersion of the optical path. The International Telecommunication Union Standardization (ITU-T) defined six bands as a basis for fiber-optic transmission using single mode fiber: O, E, S, C, L and U.as shown in table 3.5.

Table 3.5 Frequency Band

Band	Range(nm)	Description
O-band	1260-1360	Original
E-band	1360-1460	Extended
S-band	1460-1530	Short wavelength
C-band	1530-1565	Conventional
L-band	1565-1625	Long wavelength
U-band	1625-1675	Ultra-long wavelength

The applicability all of the wavelength bands, listed in table 3.5 are defined as following:

(1) "Original" O-band, 1 260 nm to 1 360 nm. The lower limit is determined by the cable cut-off wavelength, which is 1,260 nm. The upper limit 1,360 nm is determined by the rising edge of the "water" attenuation band peaked at 1383 nm, so 1,360 nm was chosen as the upper limit; 134 Optical fibers, cables and systems

(2) "Extended" E-band, 1360 nm to 1,460 nm. Recommendation ITU-T G.652 also includes fibers with a low water attenuation peak, which allows the utilization of the band above 1,360. The effects of a small water peak are negligible at wavelengths beyond about 1 460 nm.

(3) "Conventional" C-band, 1,530 nm to 1,565 nm. Initially, erbium-doped fiber amplifiers (EDFAs) had useful gain bands beginning at about 1,530 nm and ending at about 1 565 nm. This gain band had become known as the "C-band".

(4) "Short wavelength" S-band, 1,460 nm to 1,530 nm. The lower limit of this band is taken to be the upper limit of the E-band. The upper limit is taken to be the lower limit of the C-band. EDFAs have become available with relatively flatter and wider gains and application of EDFAs to this band is possible at least in a part of the band. Some wavelengths of this band may also be utilized for pumping of optical fiber amplifiers, both of the active-ion type and the Raman type.

(5) “Long wavelength” L-band, 1,565 nm to 1,625 nm. For the longest wavelengths above the C-band, fiber cable performance over a range of temperatures is adequate up to 1625 nm for current fiber types.

(6) “Ultra-long wavelength” U-band, 1,625 nm to 1,675 nm. In some cases it is desirable to perform a number of maintenance functions (preventive, after installation, before service and post-fault) on fiber cables in the outside plant. These involve surveillance, testing, and control activities utilizing optical time domain reflectometer (OTDR) testing, fiber identification, loss testing, and power monitoring. A wavelength region, that is intended to be never occupied by transmission channels, may be attractive for maintenance, even if enhanced loss occurs. The U-band has been defined exclusively for possible maintenance purposes. Transmission of traffic-bearing signals is not currently foreseen in this band. The use for non-transmission purposes must be done on a basis of causing negligible interference to transmission signals in other bands. Sufficiently low fiber loss is not ensured in this band.

3.6.2 Wavelength Range Transmission

The pulse is weaker because all material absorbs light. More accurately, impurities in the material can absorb light but the material itself does not absorb light at the wavelengths of interest. In addition, variations in the uniformity of the material cause scattering of the light. Both the rate of light absorption and the amount of scattering are dependent on the wavelength of the light and the characteristics of the particular material. Most light loss in a modern fiber is caused by scattering. Typical attenuation characteristics of fiber for varying wavelengths of light are illustrated in figure 3.10.

Optical fiber transmission uses wavelengths that are in the near-infrared portion of the spectrum, just above the visible, and thus undetectable to the unaided eye. Typical optical transmission wavelengths are 850 nm, 1,310 nm, and 1,550 nm. Both lasers and LEDs are used to transmit light through optical fiber. Lasers are usually used for 1,310 or 1,550nm single-mode applications. LEDs are used for 850- or 1300-nm multimode applications.

There are ranges of wavelengths at which the fiber operates best. Each range is known as an operating window. Each window is centered on the typical operational wavelength, as shown in Table 3.6.

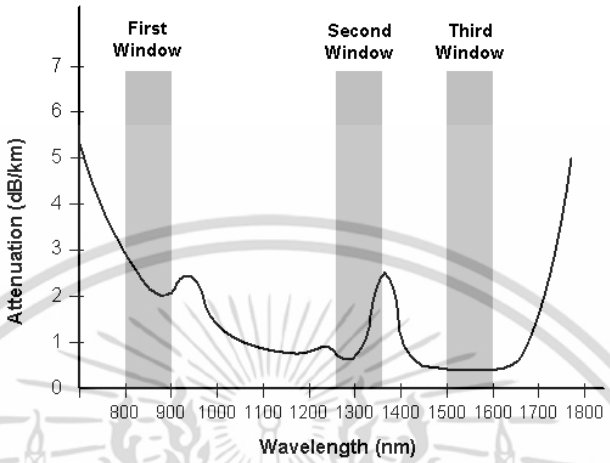

Figure 3.10 the attenuation-wavelength curve and the transmission window of optical fiber

Table 3.6 Fiber Optic Transmission Windows

Window (nm)	Operating Wavelength(nm)
800-900	850
1250-1350	1300
1500-1600	1500

Most commercial long-haul transmission systems employ the conventional band (C-band), from 1500nm-1600nm, where the fiber loss is the lowest (<0.2dB/km). With the invention of dense wavelength division multiplexing (DWDM) and Erbium doped fiber amplifiers (EDFA), the C-band became even more popular as it became possible to easily increase capacity and transmission distance.

3.7 Light Pulse in ring resonator

This section, the theory of light pulse is used for input signals to generated qubit. Usually, the laser light can be model into two kinds of signals such as Gaussian and Soliton. In this thesis we use soliton pule so the gaussian pulse is not considered in here.

Optical solitons are spatially localized, pulse-like, nonlinear waves that almost retain their shapes while propagating in ideal lossless fibers. This steady propagation stems from an exact balance between nonlinear and dispersion terms in the conservative form of the nonlinear Schröedinger equation (NLSE) which describes ideal fibers. In general, the temporal and spectral shape of a short optical pulse changes during propagation in a transparent medium due to the Kerr effect and chromatic dispersion. Under certain circumstances, however, the effects of Kerr nonlinearity and dispersion can exactly cancel each other, apart from a constant phase delay per unit propagation distance, so that the temporal and spectral shape of the pulses is preserved even over long propagation distances [41, 50] as show in figure 3.11. This phenomenon was first observed in the context of water waves [41], but later also in optical fibers [51].

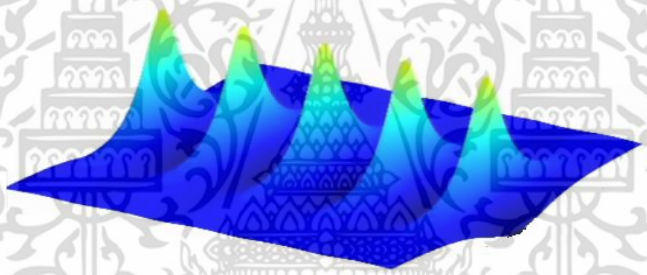

Figure 3.11 A schematic diagram of a soliton pulse

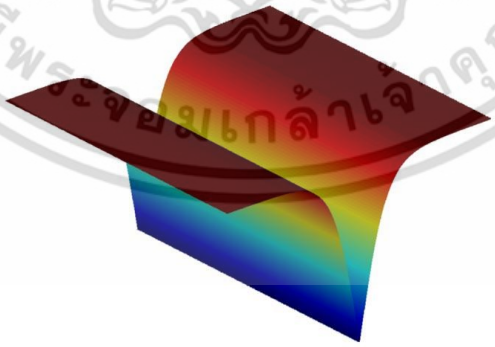

Figure 3.12 A schematic diagram of a dark soliton pulse

Normally, there are 2 kinds of solitons for system simulation, first kind is bright soliton as shown in figure 3.16 and the second is dark soliton as shown in Fig 3.12. bright soliton is representative of soliton, which is not generated complexity like dark soliton. Interest in the

behavior of such dark soliton has been motivated by several experimental observations of temporal dark soliton in optical fibers and spatial dark soliton in bulk media and waveguides, so on it has been investigated in many theoretical and experimental papers and several years ago. Both of bright soliton and dark soliton are explained by equations 3.58 and 3.59, which the electric field variation can be reduced and given by the following:

$$E_{in}(t) = A_0 \tanh\left(TT_0^{-1}\right)\exp\left[z\left(2L_D - i\omega_0 t\right)\right] \tag{3.58}$$

$$E_{in}(t) = A_0 \operatorname{sech}\left(TT_0^{-1}\right)\exp\left[z\left(2L_D - i\omega_0 t\right)\right] \tag{3.59}$$

Where A and z are the optical field amplitude and propagation distance, respectively. $\phi(t) = \phi_0 + \phi_{NL} = \phi_0 + \frac{2\pi n_2 L}{A_{eff}\lambda}\left|E_0(t)\right|^2$ is the random phase term related to the temporal coherence function of the input light, ϕ_0 is the linear phase shift, ϕ_{NL} is the nonlinear phase shift, n_2 is the nonlinear refractive index of waveguide material. The effective mode core area of the device is given by A_{eff}, $L = 2\pi R_{ad}$, R_{ad} is the radius of device, λ is the input wavelength light field. T is a soliton pulse propagation time in a frame moving at the group velocity, $T = t - \beta_1 * z$, where β_1 and β_2 are the coefficients of the linear and second-order terms of Taylor expansion of the propagation constant. $L_D = T_0^2/|\beta_2|$ is the dispersion length of the soliton pulse. T_0 in equation is a soliton pulse propagation time at initial input (or soliton pulse width), where t is the soliton phase shift time, and the frequency shift of the soliton is ω_0. This solution describes a pulse that keeps its temporal width invariance as it propagates, and thus is called a "temporal soliton". When a soliton peak intensity $\left(\left|\beta_2/\Gamma T_0^2\right|\right)$ is given, then T_0 is known. For the soliton pulse in the microring device, a balance should be achieved between the dispersion length (L_D) and the nonlinear length ($L_{NL} = 1/\Gamma\phi_{NL}$), where $\Gamma = n_2 * k_n$, is the length scale over which dispersive or nonlinear effects makes the beam become wider or narrower. For a soliton pulse, there is a balance between dispersion and nonlinear lengths, hence $L_D = N_L$.

3.8 Summary

In this chapter, the theoretical background and relation including equations have presented to support our propose work such as quantum cryptography, BB84 protocol, which it is first protocol for quantum cryptography. We have presented photon, polarization of light, Phenomena of Nonlinear Optics such as Susceptibility, Kerr effect, Chaotic. We have also presented optical microring resonator characterization, the optical microring resonator, the optical add/drop ring resonator filter and PANDA ring resonator. Finally, we have presented wavelength range and attenuation in optical fiber and light pulse is used.

Chapter 4

QKD in Purpose System and Experimental Results

In this chapter, we have presented our purpose system for Quantum cryptography by using QKD technique based on BB84 protocol. Our system proposes communicates peer to peer between Alice and Bob. Then, the experimental results such as qubits generate, channels, and key rate for distance are compared with the previous work. The purpose work and experimental results are following:

4.1 Purpose of Experiments

Our purposes of experiments are following:

(1) Using modify add/drop known as PANDA ring resonator for correlate photon generation and applies for quantum cryptography by BB84 protocol.

(2) To experiment generate signal to be key via all optical devices such as PANDA ring resonator and add/drop filter by using bright soliton is input with 2 center wavelengths 1.54μm and 1.55μm in C-band for the best communication of fiber optic. The qubits are encrypted by polarizers and send to Bob.

(3) To compare the efficient of secure key and distance with the previous work such as Quantum Cryptography [32] and Multi-Layers QKD Protocol Using Correlated Photon of Dark Soliton Array in a Wavelength Router [35].

4.2 Correlate Photon Generation via PANDA Ring Resonator

Light from a monochromatic light source is launched into a ring resonator with constant light field amplitude (E_0) and random phase modulation, which is the combination of terms in attenuation (α) and phase (ϕ_0) constants, which results in temporal coherence degradation. Hence, the time dependent input light field (E_{in}), In operation, the input and control fields at the input and add ports are formed by the dark and bright optical solitons and described by equations. (3.58) and (3.59), respectively. A dark-bright soliton conversion system using a ring resonator optical

channel dropping filter is composed with two sets of coupled waveguides, as shown in Figure 4.1. The relative phase of the two output light signals after coupling into the optical coupler is $\pi/2$. This means that the signals coupled into the drop and through ports have acquired a phase of π with respect to the input port signal. In application, when the coupling

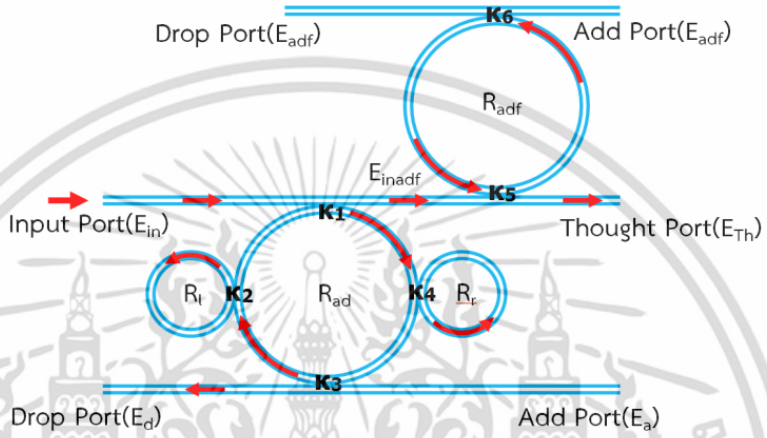

Figure 4.1 A schematic of a soliton photon generation system by using soliton pulse within PANDA ring resonator and add/drop filter, where R_s: ring radii, κ_s : coupling coefficients, R_d: an add/drop ring radius, A_{eff}: Effective areas, $\kappa_1 - \kappa_6$ are coupling coefficients

Figure 4.1 shows us the schematic diagram of a photon generation system by using soliton pulse within PANDA ring resonator and add/drop filter, where R_s: ring radii, $\mathbf{K}_s$: coupling coefficients, R_d: an add/drop ring radius, A_{eff}: Effective areas, $\mathbf{K}_1$ – $\mathbf{K}_6$ are coupling coefficients if a proposed PANDA ring resonator are fixed to be the coupler intensity loss is $\gamma = 0.1$, n_0 = 3.34 (InGaAsP/InP), and α = 0.2 dBmm^{-1}. The coupling coefficient of the micro ring resonator is varied from 0.1-0.98 and the nonlinear refractive index is $n_2 = 2.2 \times 10^{-17}$. The other used parameters of the first add/drop filter (PANDA ring resonator) are fixed to be $\mathbf{K}_1 = 0.15$, $\mathbf{K}_2 = 0.35$, $\mathbf{K}_3 = 0.7$, and $\mathbf{K}_4 = 0.2$, respectively. The ring radii are $R_{ad} = 15$ μm, and $R_r = R_l = 5$ μm. A_{eff} are *0.50*, *0.25* and *0.25* μm^2, respectively. Moreover, our optical key and recovery system should be possible to be fabricated, which can be confirmed by using the practical device

parameters. For the simulation results of the optical key signal with center wavelength is λ_0 =1.54 μm.

This work proposes add/drop filter (AD), both of transmission part and receiver part is fixed to be n_0 = 3.34 (InGaAsP/InP), and $\alpha = 0.2$ dBmm^{-1}. The coupler intensity loss is $\gamma = 0.1$. In the work out team assume the nonlinear of optical ring resonator is of the Kerr-type, i.e., the nonlinear refractive index is n_2 = 2.2 ×10^{-17}, the coupling coefficient of the micro ring resonator is varied from 0.1-0.98 and the other used parameters of the add/drop filter are fixed to be $\mathbf{K}_5$ = $\mathbf{K}_6$ = *0.13.*

4.3 BB84 Protocol via Purpose System

A QKD agreement protocol was first proposed by Bennett and Brassard in year 1984 [33], or we have known as name in BB84, which based on the fundamental principle of quantum mechanics. At present, the study of QKD is limited to theoretical and experimental. The unconditionally secure protocol in theory needs further experimental verification. Because of the limit of technology and some imperfections, the study of QKD in the lab is difficulty and costly. In this thesis we have presented ideal for other method of BB84 by using ring resonator we have known as name in PANDA ring resonator as shown in Figure 4.3.

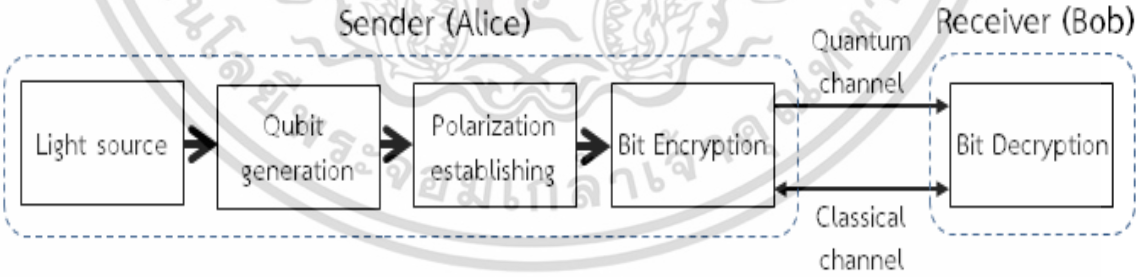

Figure 4.2 Diagram of process for QKD

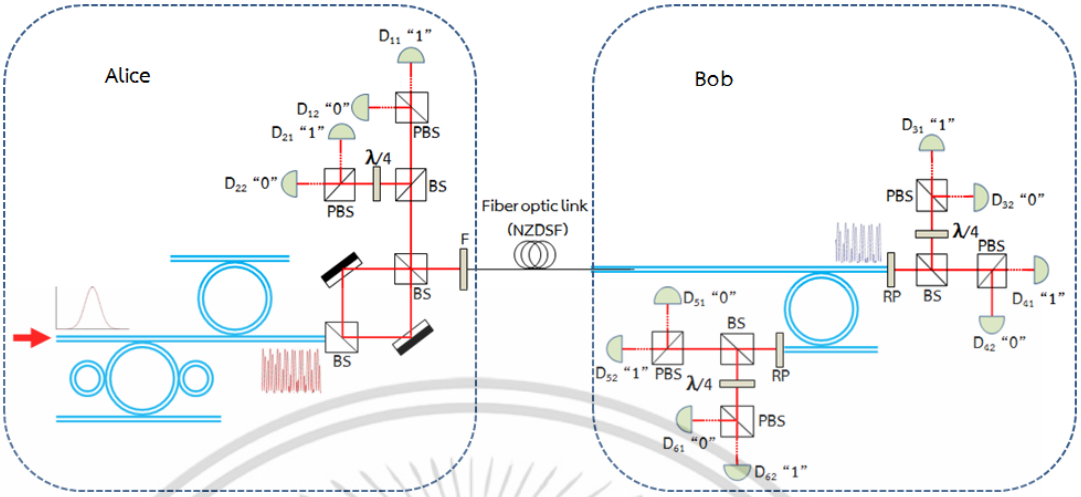

Figure 4.3 System for proposed QKD protocol.

In this thesis has proposed to present optical cryptography based on BB84 that the photon polarization is used. Figure 4.2 is shown the process of this system as following:

(1) that first of all the input pulse is assessed by bright soliton(Erbium pump), PANDA ring resonator is designed with fix parameters for generated signal for using qubit(key), when circulating within the device due to the nonlinear Kerr effects of light within the PANDA ring resonator, The advantage of soliton nonlinear property, known as self-phase modulation.

(2) Then the add/drop filter device by using the appropriate parameters have filtered and random by orthogonal polarization.

(3) The keys are encrypted by Alice chooses a random sequence of polarization basis (rectilinear 0°, 90° or diagonal 135°, 180°) and sends to Bob over quantum channel, a stream of photons representing one bit of the key in the basis chosen for that bit position.

(4) When Bob receives photons from Alice by using add/drop filter with the fixed parameter like Alice's part, the keys have decrypted by Bob measure his photon using a random sequence of bases, his results of measurements. There are some photon are shown as not having been received owing to imperfect detector efficiency.

(5) Then Bob has told Alice which basis he used for each photon he received and his results of measurements over classical channel.

(6) Finally, Alice and Bob keep only the data from these correctly measured photons, discarding all the rest. This data is interpreted as a binary sequence according to the coding scheme.

Optical Cryptography by QKD in this thesis, Alice's side has provided the fixed device for encryption that consist of three parts such as PANDA ring resonator, which used to generate signal that has sued to be the keys. In this work, we propose add/drop filter for filtering the signals, and the basic optical device call polarizer to set photons polarized basis for sending to Bob shown in figure 4.3. The light pulse in the form of Bright soliton, which is recommended as powerful characteristics when propagating within nonlinear micro-ring resonator is used input from light source, is launched into PANDA ring resonator The input signal pulse is chopped into smaller signal spreading over the spectrum, which show that the large band width signals are generated to be qubits within the PANDA ring resonator. Then the filtering device is required to tune the required tunable signals can be managed. In order to tune the signals from large bandwidth, we propose to use the add/drop device by using the appropriate parameters. Here, it's given in details as followings by the equations (4.1) and (4.2).

$$\left|\frac{E_{Th}}{E_{inadf}}\right|^2 = \frac{(1-\kappa_5)-2\sqrt{1-\kappa_5}\sqrt{1-\kappa_6}\,e^{-L\frac{\alpha}{2}}\cos(k_n L)+(1-\kappa_6)e^{-\alpha L}}{1+(1-\kappa_5)(1-\kappa_6)e^{-\alpha L}-2\sqrt{1-\kappa_6}\,e^{-L\frac{\alpha}{2}}\cos(k_n L)} \tag{4.1}$$

$$\left|\frac{E_{adf}}{E_{inadf}}\right|^2 = \frac{\kappa_5\kappa_6 e^{-L\frac{\alpha}{2}}}{1+(1-\kappa_5)(1-\kappa_6)e^{-\alpha L}-2\sqrt{1-\kappa_5}\sqrt{1-\kappa_2}\,e^{-L\frac{\alpha}{2}}\cos(k_n L)} \tag{4.2}$$

Where E_{Th} is the throughput port, and E_{adf} drop port signal, in here $\phi = \beta L$ is the phase constant.

We propose the variable of photon is generated within the system; each pair of possible polarization-entangled photons is formed by using the polarization control unit, which can be represented by Bream Splitter (BS). We propose two states of polarization as Horizontal state ($|H\rangle$) and Vertical state ($|V\rangle$). For this thesis we omitted an amplitudes term that is common to all product state.

The pair of qubit is encrypted by two states polarization basis as horizontal state and vertical state polarization corresponding to an optical switch as we have mentioned in Chapter 3. Alice has chosen random basis, which can be represented by the four polarization orientation angles as [0°, 90°, 45°, 135°], that they can be formed by using the optical component called the polarization rotatable device call Rotatable polarizer (RP) and Polarization Bream Splitter (PBS). Before Alice has send Bob the sequence of photons polarized basis, she have checked key by using detector i.e. D_1 and D_2, as stand in Alice side. Than send Bob through Non-zero dispersion shifted fiber (NZDSF).

When Bob has received signal from wavelength λ_0 that is send from Alice, Bob has had to filter correct wavelength by using a device the same Alice's side with as same as propagation parameters. The code or key is decrypted at Through port. Bob has been random to choose one of four polarization orientation angles as [0°, 90°] or [45°, 135°] by using RP and PBS. By the same way, Bob has used detector D_3 and D_4 for checking polarization angle by agreement with Alice, when the angle of polarization is 0° or 180° (|H>), which is detected by D_4, but when the angle of polarization is 90° (|V>), D_3 has detected the signal by through PBS. Another way, when angle of polarization is between 0°-90° or 90°-180°, that means 45° or 135° the PBS has split signal as half as to both of D_3 and D_4. Similarly, D_5 and D_6 are set to be reference at Drop port.

When Bob's end of measurement and some photons are shown as having been received owing to detector efficiency, than Bob tells Alice which his basis sued for each photon that he's received from Alice, after that Alice tells Bob that bases were correct. Than both of them have kept only the data from these correctly measured photons, and discarding all the rest. At the moment, all data which agreement between Alice and Bob is interpreted as a binary sequence according to the scheme as follow BB84

quantum key distribution protocol, which the perfect security can be formed between Alice and Bob without any cheating from Eave. Finally, the classical channel signals can be recovered by using the qubit, which means the top security information, using the qubit technique based on quantum cryptography by light, i.e. entangled photon, is realized.

4.4 Experimental Results

We have proposed optical cryptography, which is presented in figure 4.3. For in this experiment we have experiment 2 center wavelength such as 1.54 μm and the other is 1.55 μm. each one is 10 nm of length and bright soliton is been input.

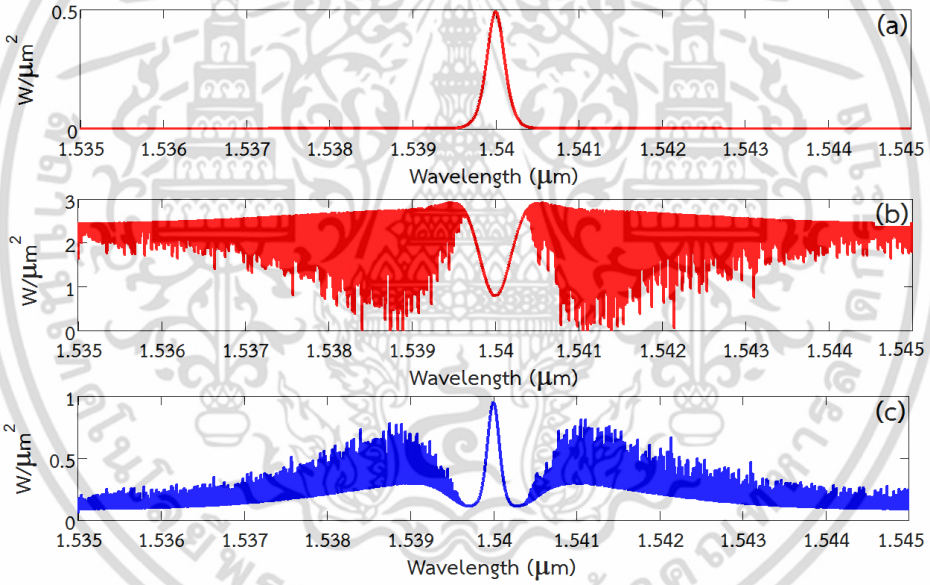

Fig 4.4 Experiment result with center wavelength of 1.535 μm, where (a) shows soliton input, (b) chaos is generated at Through port of PANDA ring resonator, (c) other chaos is generated at Drop port of PADA ring resonator

First one, we have used input with 0.5W and 1.54 μm of center wavelength as shown in Fig. 4.4(a). when the input soliton is chopped to be many soliton pulses by the nonlinear effects, where in this case the nonlinear devices are formed by the two small ring resonators of the center ring, the chaos signal is generated at Through port,

which will be input for add/drop filler (E_{inadf}), this chaos signal has shown us in figure 4.4(b).

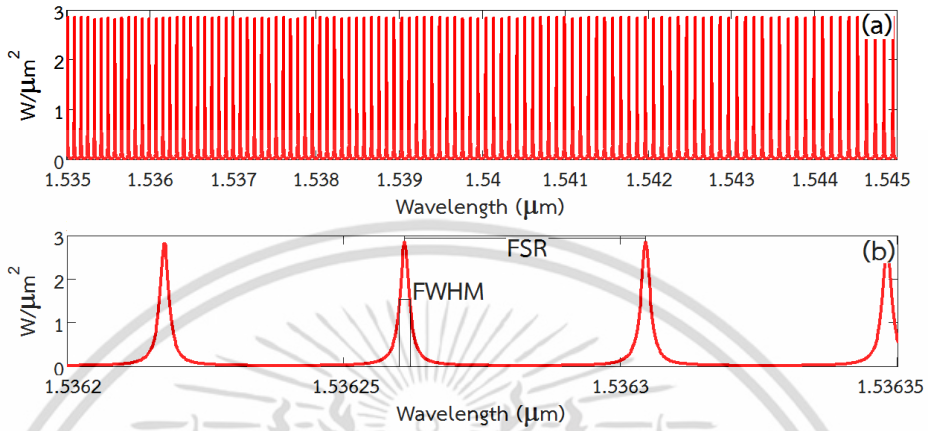

Figure 4.5 Experiment result with center wavelength of 1.535 μm, where (a) shows signals at Through port of add/drop filter to be qubits for polarizer to send to Bob, (b) shows FSR and FWHM of 0.0348nm and 0.00125 nm.

The other chaos is also generated by resonant and interference of light at Drop port (E_D) The multi-dark-bright soliton conversion is also seen when the input soliton is chopped to be many soliton pulses by the nonlinear effects Generally, when a bright or dark soliton is propagated in a $\pi/2$ phase shifter device (beamsplitter or an optical coupler), the dark-bright soliton conversion, as shown in figure 4.4(c). The key to send to Bob will be generated by add/drop filter (R_{adf}) with parameter that has mentioned above; the experiment result is shown in figure 4.5(a) with power is 2.8W/μm^2, the key will be checked before sending to Bob by D_{11}, D_{12}, D_{21}, D_{22}, through BS(Beam splitter) and PBS(Polarize Beam splitter), that we have presented in figure 4.3. In This optical cryptography technique, the simulation result at the transmission side, where the selected wavelength center can be made by using the designed add/drop filter, whereas the required spectral width (full width at half maximum, FWHM) and free spectral range (FSR) are obtained. The channel spacing and channel capacity are represented by FSR and FWHM, respectively; for instance, the FSR=0.0348nm and

FWHM=0.00125 **nm** are obtained, which means that there are many channels are generated by 10nm/0.0348nm=278 channels as shown in figure 4.5(b).

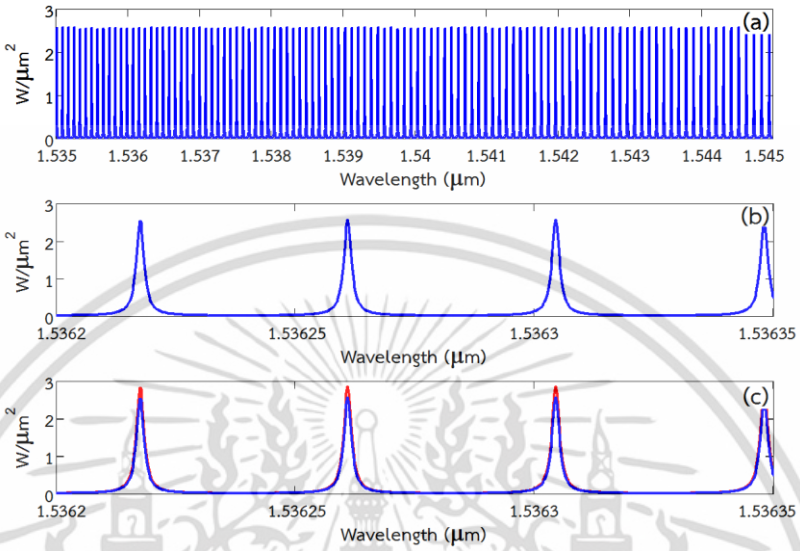

Figure 4.6 Experimental results at Bob receives the single for Alice, where (a) the signal at add/drop filter, (b) shows detail the signal as 1.5362 **µm** -1.53635 **µm**, (c) compares the signal between Alice side and Bob side

At last, when receiver (Bob) receives signal (key) photons from transmission side (Alice) by using add/drop filter with the fixed parameter like Alice's part as shown in figure 4.6(a)(b) with 2.7W/**µm**^{2} of power. The keys have decrypted by Bob measure his photon using a random sequence of bases(polarizers), his results of measurements D_{31}, D_{32}, D_{41}, D_{42}, through BS(Beam splitter) and PBS(Polarize Beam splitter), that we have presented in figure 4.3. Finally, Alice and Bob keep only the data from these correctly measured photons as shown in figure 4.6(c).

Here, we have changed center wavelength from 1.45 **µm** to be 1.55 **µm** with power of 0.5W as shown in figure 4.7(a), the experiment result has shown us how a bit difference chaos signals (figure 4.7(b)(c)) and other signal that Alice uses for code with FWHM=0.00145 nm and FSR=0.0385 nm, so 260 of channels are generated as shown in figure 4.8(a)(b).

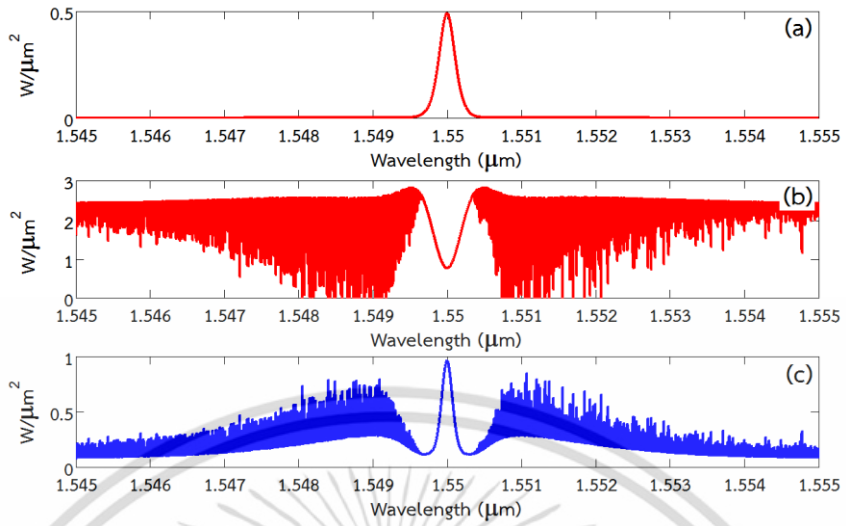

Figure 4.7 Experiment result with center wavelength of 1.545 μm, where (a) shows soliton input, (b) chaos is generated at Through port of PANDA ring resonator, (c) other chaos is generated at Drop port of PADA ring resonator

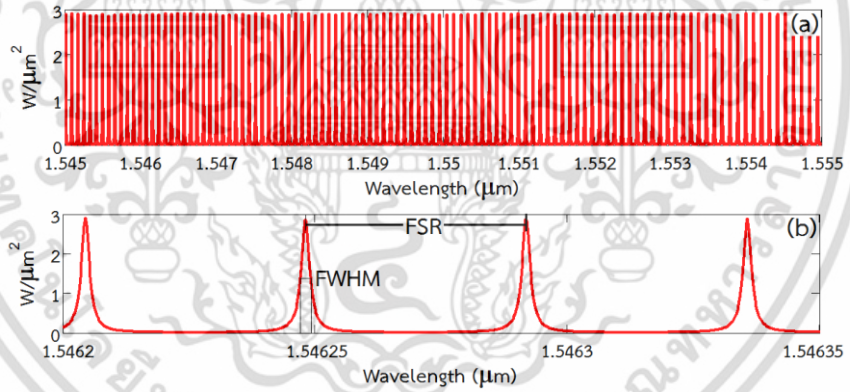

Figure 4.8 Experiment result with center wavelength of 1.545 μm, where (a) shows signals at Through port of add/drop filter to be qubits for polarizer to send to Bob, (b) shows FSR and FWHM of 0.0385nm and 0.00145 nm.

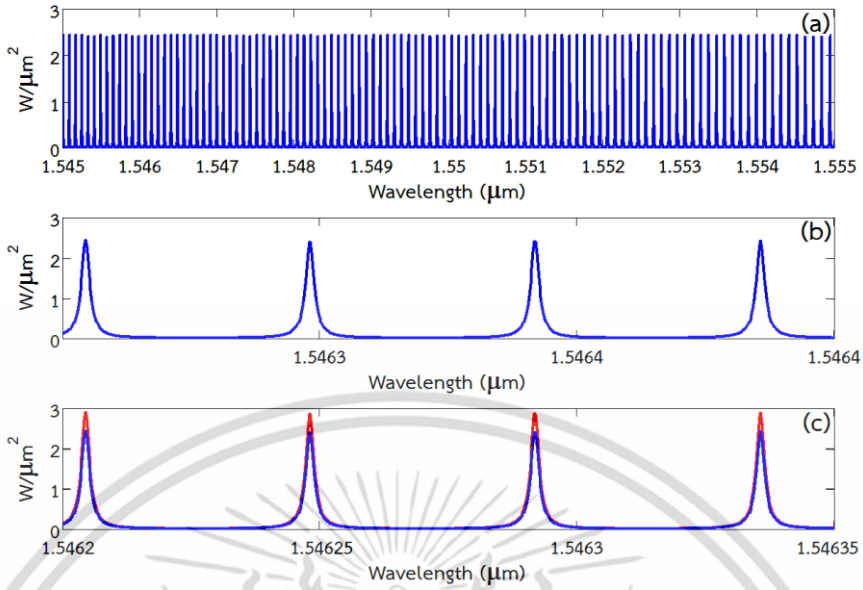

Figure 4.9 Experimental results at Bob receives the single for Alice, where (a) the signal at add/drop filter, (b) shows detail the signal as 1.5462 μm -1.54635 μm, (c) compares the signal between Alice side and Bob side

When Bob receives signal from transmission Alice by using add/drop filter with the fixed parameter as same as Alice's part as shown in figure 4.9(a)(b) with 2.7W/μm^2 of power. The keys is decrypted by Bob measure his photon using a random sequence of bases(polarizers), his results of measurements D_{31}, D_{32}, D_{41}, D_{42}, through BS and PBS. Alice and Bob then keep only the data from these correctly measured photons as shown in figure 4.9(c).

This session, many qubits are generated to be Codec (Code and Decode) between Alice and Bob by bright soliton with 2 center wavelength such as 1.54μm and 1.55 μm. As 1.45μm of center, each pule is generated with FWHM=0.00125 nm and FSR=0.0348 nm, and 278 of channels, respectively. The outer center wavelength as 1.55μm gives the value for FWHM=0.00145nm, FSR=0.0385nm, and number of channel is 260.

4.5 Security bit rate generation

This session had shown the result for security bit rates are generated by equation (2.6), the comparison its results with the relative works such as Quantum Cryptography by Nicolas Gisin et al [32], and other is Multi-Layers QKD Protocol Using Correlated Photon of Dark Soliton Array in a Wavelength Router by Phichai Yupao [35]. The experimental results are following:

In the experiment of Quantum Cryptography (BB84) [32] has shown us bit rate transfer and distances by chosen parameters are as follows: photon is used $\mu_0 = 1$ with pulse rates (f_{rep}) f_{rep}=*1MHz*, and $\mu_0 = 0.1$ with f_{rep}=*10 MHz* for faint laser pulses, fiber losses of 0.25 dB/km; detector efficiencies of η=10%; dark-count probabilities (P_{dark}) of 10^{-7}, 10^{-5}, and 10^{-5} for 800 nm, 1.300 nm, and 1.550 nm, respectively. When comparing the curves 1.550 nm (f_{rep} =10MHz, μ_0=0.1) and 1.550 nm (f_{rep} =1MH, μ_0=1) as shown in Fig 4.10. In the figurer has shown us evidently bit rate of 10.49kbit/s and 110b/s at 27km, 90km of distance for the first 1.550nm (μ_0=0.1, f_{rep}=10MHz). Other 1.550 (μ_0=1, f_{rep}=1MHz) the security bit rate of 10.49kbit/s, 335bit/s, and 12.17bit/s at 27km, 90km, and the maximum of distance at 120km. In this case for 800 nm, 1.300 nm of frequency band are not considered in this thesis.

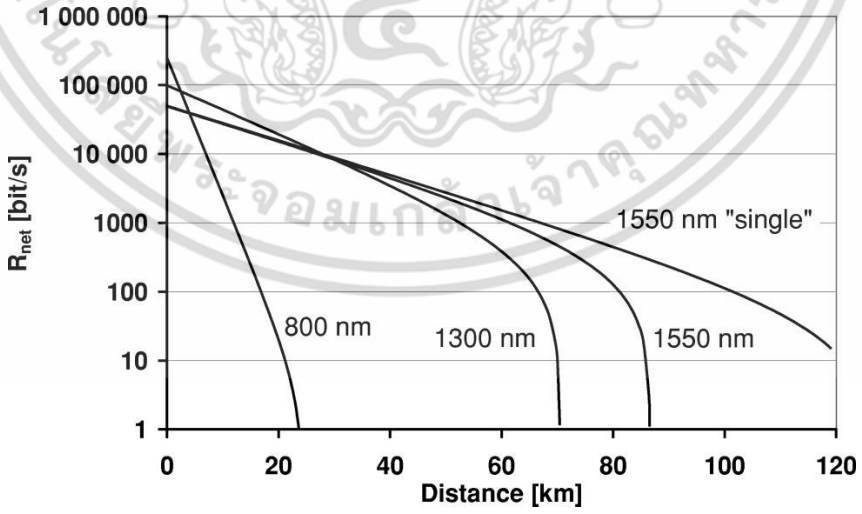

Figure 4.10 Experimental results of BB84 [32]

When we have compared BB84 [32], which is presented above with our propose system. The chosen parameters are like BB84 [32] as followed: photon are used $\mu_0 = 1$ and $\mu_0 = 10$, pulse rates f_{rep}=10 MHz AND 1MHz for faint laser pulses, fiber losses of 0.25 dB/km; detector efficiencies of η=10%; dark-count probabilities (P_{dark}) of 10^{-5} for 1.550 nm, respectively.

When f_{rep}=1MHz is used, let us mention that security key creation rates on the order of 10.49kb/s, 335b/s at distance via fiber optic link at 27km, 90km, and maximum of distance is 120km for $\mu_0 = 1$. When we have change the value of photon to be 10 ($\mu_0 = 10$), the simulation result has shown us the rate bit transfer are 150kbit/s, 4.8kbit/s, at 27km, 90km, the maximum of distance is 200km.

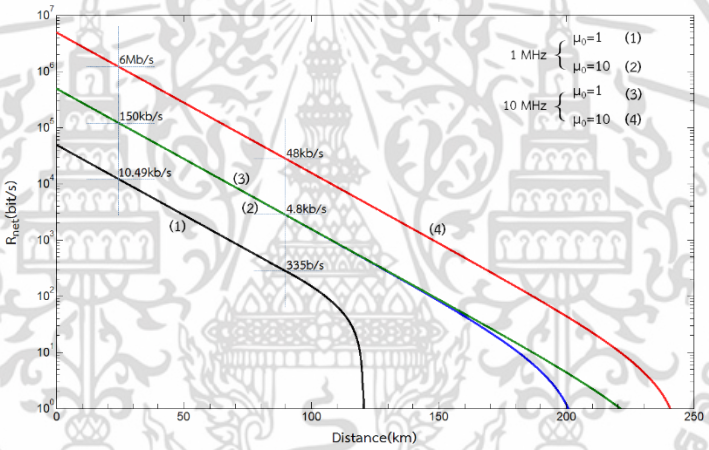

Figure 4.11 Experiment result of our system propose , where f_{rep}=1MHz with $\mu_0 = 1$(1), $\mu_0 = 10$ (2), f_{rep}=10MHz with $\mu_0 = 1$(3), $\mu_0 = 10$ (4). Then compare with BB84 [32]

When f_{rep}=10MHz is used, let us mention that security key creation rates on the order of 150kb/s, 4.8kb/s at distance via fiber optic link at 27km, 90km, and maximum of distance is 220km for $\mu_0 = 1$. When we have change the value of photon to be 10 ($\mu_0 = 10$), the simulation result has shown us the rate bit transfer are 6Mb/s, 48kb/s, at 27km, 90km, the maximum of distance is 240km as shown in figure 4.11.

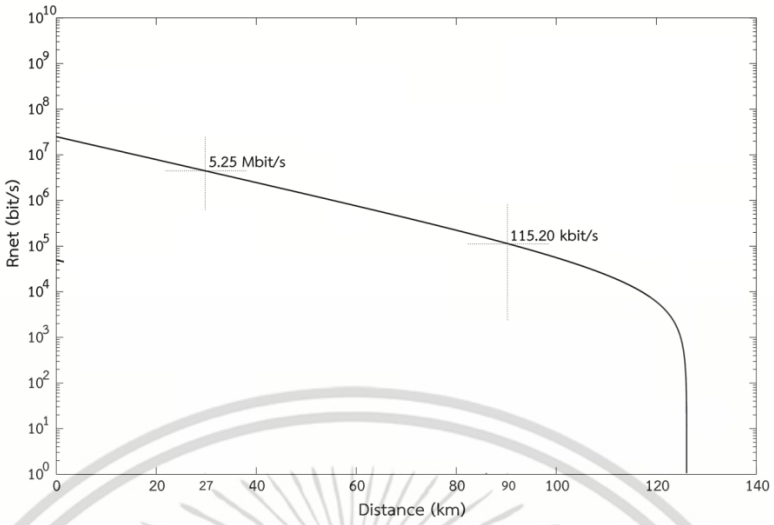

Figure 4.12 Experiment result of Multi-Layers QKD Protocol Using Correlated Photon of Dark Soliton Array in a Wavelength Router [35]

One more work is Multi-Layers QKD Protocol Using Correlated Photon of Dark Soliton Array in a Wavelength Router [35]. In this work here the parameters are chosen as followed: f_{rep}=500MHz, $\mu_0 = 1$ with fiber losses of 0.25 dB/km; detector efficiencies of η=10%; dark-count probabilities P_{dark}= 10^{-5}. The result of experiment has shown us the security bit rate as 5.25Mb/s, 115.20k/s the maximum of distance is 227km as shown in figure 4.12.

When we have compared the second work [35], that is presented above with our propose system. The chosen parameters are as followed: photon $\mu_0 = 10$, pulse rates f_{rep}= 500MHz for faint laser pulses, fiber losses of 0.25 dB/km; detector efficiencies of η=10%; dark-count probabilities (P_{dark}) of 10^{-5} for 1550 nm, respectively. The result of experiment has shown us the security bit rate as 50Mb/s, 920k/s the maximum of distance is 240km as shown in figure 4.13 below.

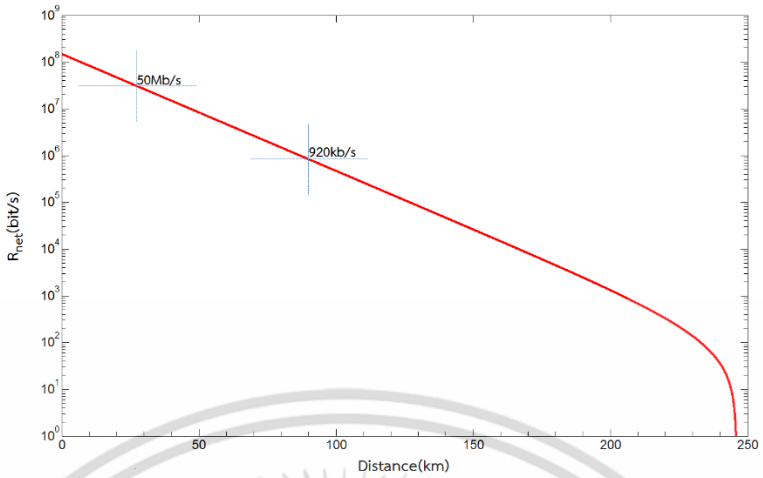

Figure 4.13 Experimental results of our system propose with f_{rep}=500GHz to compare with QKD [35]

The security bit rate R_{net} experimented by equation (2.6). Then, the experimental results are compared with two previous works [32, 35]. In this work has made 6Mb/s of R_{net} and maximum of distance is 240km with f_{rep}=10MHz, $\mu_0 = 10$. When f_{rep}=500MHz, 50Mb/s of R_{net} is made, and maximum of distance is 240km.

4.6 Summary

We have assumed the idea of perfectly secured data transmission technique, call quantum cryptography scheme. Strictly speaking, the set of all possible states sending by Alice to Bob is a set two states corresponding to identical bits, where the two states are horizontal $|H\rangle$ state and vertical $|V\rangle$ state of polarization of multi-photons base on BB84 protocol system which is the first protocol to use with quantum cryptography [32]. The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states we are trying to distinguish are not orthogonal. It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption.

Our system consist of two parts, where first, the transmission part (Alice) can be used to generate the high capacity of quantum codes within the series of PANDA ring

resonators and add/drop filter, second, the receiver part (Bob) can be used to detect the quantum bits into add/drop filter. In this chapter we have also presented the purpose system and experimental result as following:

(1) Multi-photons are generation and apply for quantum cryptography.

(2) To experiment generate signal to be key via our purposed system by using bright soliton is input with 2 center wavelengths 1.540 and 1.550 in C-band for the best communication of fiber optic. Each one is 10nm of length. The qubits are encrypted by polarizers and send to send to Bob.

(3) The experimental result of secure key bit rate and distance are compared with the previous work such as Quantum Cryptography [32] and Multi-Layers QKD Protocol Using Correlated Photon of Dark Soliton Array in a Wavelength Router [35].

Chapter 5

Discussion and Conclusion

5.1 Discussion as Error reconciliation and Privacy amplification

In real systems, if Alice and Bob discover their measurements are not perfectly correlated, it is difficult for them to determine whether the discrepancy was caused by using noisy imperfect equipment or whether there was an eavesdropper present creating perturbations in the state of the photons by measuring them. We have already discussed in BB84 protocol how the two approaches to QKD would detect an eavesdropper under ideal conditions. In practical systems, Alice and Bob would not want to discard every transmission that wasn't error free since there likely will always be some natural error not caused by Eve. Since there is some error, we must assume that Eve may have successfully learned some of the key's bits. QKD protocols can employ a technique known as privacy amplification to reduce the information Eve has about the key down to an arbitrary level.

At this point in the BB84 protocol, Alice and Bob share a so-called sifted key. But this key contains errors. The errors are caused by technical imperfections, as well as possibly by Eve's intervention. Realistic error rates in the sifted key using today's technology are of the order of a few percent. This contrasts strongly with the 10^{-9} error rate typical in optical communication. Of course, the few-percent error rate will be corrected down to the standard 10^{-9} during the (classical) error correction step of the protocol.

The general idea is that at some point Alice, Bob, and Eve perform measurements on their quantum systems. The outcomes provide them with classical random variables $\alpha, \beta,$ *and* ε, respectively, with $P(\alpha.\beta,\varepsilon)$ the joint probability distribution. The first theorem, a standard of classical information-based cryptography, states the necessary and sufficient condition on $P(\alpha.\beta,\varepsilon)$ for Alice and Bob to extract a secret key from $P(\alpha.\beta,\varepsilon)$.

Assume that a joint probability distribution $P(\alpha.\beta,\varepsilon)$ exists. Near the end of this section, we shall comment on this assumption. Alice and Bob have access only to the

marginal distribution *P*(a,b). From this and from the laws of quantum mechanics, they have to deduce constraints on the complete scenario *P*(a,b,e); in particular they have to bound Eve's information. Given $P(\alpha.\beta,\varepsilon)$, necessary and sufficient conditions for a positive secret-key rate between Alice and Bob, $S(\alpha,\beta\|\varepsilon)$, are not yet known. However, a useful lower bound is given by the difference between Alice and Bob's mutual Shannon information $I(\alpha,\beta)$ and Eve's mutual information

$$S(\alpha,\beta\|\varepsilon)\geq \max\{I(\alpha,\beta)-I(\alpha,\varepsilon),I(\alpha,\beta)-I(\beta,\varepsilon)\} \tag{5.1}$$

$$I(\alpha,\varepsilon)=H(\alpha)-H(\alpha|\varepsilon) \text{ and } I(\alpha,\beta)=H(\alpha)-H(\alpha|\beta) \tag{5.2}$$

Where S is secret-key, I is Shannon information, and H is Shannon entropy.

For a given $P(\alpha.\beta,\varepsilon)$, Alice and Bob can establish a secret key (using only error correction and classical privacy amplification) as followed express

$$I(\alpha.\beta)>I(\alpha,\varepsilon) \text{ or } I(\alpha.\beta)>I(\beta,\varepsilon). \tag{5.3}$$

The Eq. (5.1) is tight if Alice and Bob are restricted to one-way communication, but for two-way communication, secret-key agreement might be possible even when condition equation (5.1) is not satisfied. The process of error correction and privacy amplification is shown in Figure 5.1. Alice and Bob can establish a secret key when condition equation (5.1) is satisfied. First, once the sifted key is obtained (i.e., after the bases have been announced), Alice and Bob publicly compare a randomly chosen subset of it. In this way they estimate the error rate [more generally, they estimate their marginal probability distribution $P(\alpha.\beta)$]. These publicly disclosed bits are then discarded. Next, either condition equation (5.1) is not satisfied and they stop the protocol or condition equation (5.1) is satisfied and they use some standard error correction protocol to get a shorter key without errors as show in figure 5.1 (a).

Eve receives as much information as Bob. The initial information difference δ thus remains. After error correction, Bob's information Eq. (5.3), as illustrated in Figure 31 (b).

With the simplest error correction protocol with Alice and Bob sharing an identical key, they can transform their key into a new key in a way that Eve could not unless she also had exactly the same entire key. This technique is called *privacy amplification* and involves shrinking the original key to a new key unknowable to Eve. A simple privacy amplification scheme is for Alice to announce to Bob pairs of bits from the original key. Alice randomly chooses pairs of bits and announces their XOR value. Bob replies either ‘‘accept’’ if he has the same XOR value for his corresponding bits, or ‘‘reject’’ if not. In the first case, Alice and Bob keep the first bit of the pair and discard the second one, while in the second case they discard both bits. In reality, more complex and efficient algorithms are used. After error correction, Alice and Bob have identical copies of a key, but Eve may still have some information about it [compatible with condition equation (5.1)].

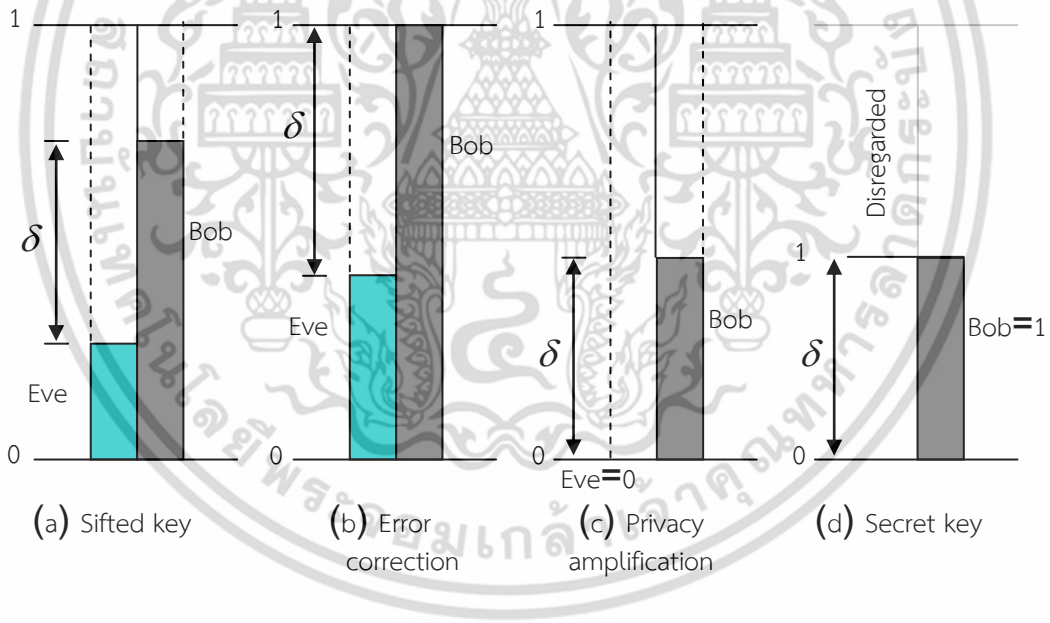

Figure 5.1 Intuitive illustrations of error correction and privacy amplification

Alice and Bob thus need to reduce Eve’s information to an arbitrarily low value using some privacy amplification protocols. These classical protocols typically work as follows. Alice again randomly chooses pairs of bits and computes their XOR value. But, in contrast to error correction, she does not announce this XOR value. She only

announces which bits she chose (e.g., bits number 22 and 222). Alice and Bob then replace the two bits by their XOR value. In this way they shorten their key while keeping it error free, but if Eve has only partial information on the two bits, her information on the XOR value is even less. Assume, for example, that Eve knows only the value of the first bit and nothing about the second one. Then she has no information at all about the XOR value. Also, if Eve knows the value of both bits with 65% probability, then the probability that she correctly guesses the XOR value is only $(0.65)^2 + (0.35)^2$=54.5%. This process would have to be repeated several times; more efficient algorithms use larger blocks. After privacy amplification Eve's information is zero. This process is shown in Figure 5.1 (c). Finally, Bob has full information about this final key, while Eve has none as in Figure 5.1 (d).

5.2 Conclusion

We have presented the classical cryptography that purposes to transmit information in such a way that access to it is restricted entirely to the intended recipient, even if the transmission itself is received by others. This science is of increasing importance with the advent of broadcast and network communication, such as electronic transactions, the Internet, e-mail, and cell phones, where sensitive monetary, business, political, and personal communications are transmitted over public channels.

We have assumed the idea of perfectly secured data transmission technique, which it is based on quantum entangled state encryption scheme. Strictly speaking, the set of all possible states sending by Alice to Bob is a set two states corresponding to identical bits, where the two state are horizontal (H) and vertical (V) polarization a single photon. In this application, the idea of an experiment of optical encryption technique can be realized to create top security.

We have also presented the BB84 protocol system which is the first protocol to use with quantum cryptography. The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states we are trying to distinguish are not orthogonal. It is usually

explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption.

Table 5.1 The Advantage of purpose system

Ring Type	Radius		Chanel
	Max(μm)	**Min**(μm)	
Series Ring[35]	400.86	400	100
PANDA Ring(Purpose system)	10	5	278

The main point of this thesis is proposed system consist of two parts, where firstly, the transmission part can be used to generate the high capacity of quantum codes within the PANDA resonators, secondly, the receiver part can be used to detect the quantum bits via add/drop filter. The reference states can be recognized by using the cloning unit [46], which is operated by the add/drop filter. A quantum processor (two add/drop filters that are in two parts) can be used to form Alice and Bob states in the link, respectively. Results obtained have shown the security bit rate increasing as 6 Mb/s, 48k/s at 27 km, 90 km of optical fiber distance, respectively, compare with BB84 by Nicolas Gisin [32] experiment. It has also shown us the maximum of distance as 240km. In addition, when we compare experiment result of QKD by Pichai Yuplao [35] as shown in table 5.1, the purpose system is smaller size and the secure information with high capacity as 278 channels can be performed incorporating the qubit via the quantum processor, which is responds to the large bandwidth demand for optical communication applications.

5.3 Future Work

QKD is a technique whereby a secure key for cryptography encoding can be exchanged over an insecure communication channel. Since 1984 Bennett and Brassard proposed the first protocol, many experimental systems have been developed in the laboratory, and commercial point-to-point QKD systems are even available on the market. However, a poit-to-point system is not enough to satisfy network

communication requirements, so the building of QKD network is not only necessary but also crucial to practical quantum cryptography. For the plan in the future, we will be focused on the use of other network topology using quantum router, which will be the important tool for communication security. By using the small device, for instance, micro/nano waveguide which can be practically fabricated and embedded within the network device. Finally, the perfect security known as a quantum security will also be discussed and included in applications. Incorporating the qubit via the quantum processor, which is responds to the large bandwidth demand for optical communication applications.

REFERENCES

[1] M. Gill, 2014, "The Handbook of Security," **2rd Edition, Palgrave Macmillan UK,** a division of Nature America Inc.

[2] W. DIFFIE, M. E. HELLMAN, "New Directions in Cryptography," **IEEE, Transactions on Information Theory,** Vol. IT-22, No. 6, pp. 644-654, 1976.

[3] D. Boneh, V.Shoup, 2015 "A Graduate Course in Applied Cryptography," **Standford University,** California, UAS.

[4] N. Smart, "Cryptography: An Introduction," **3rd Edition, Mcgraw-Hill College**, 2004.

[5] R. W. Eason and A. Miller, 1993, "Nonlinear optics in signal processing," **Champan & Hall,** London, U.K.

[6] E. Cotter, J. K. Lucek, and D. D. Marcenac, "Ultra-high-bit-rate networking: From the transcontinental backbone to the desktop," **IEEE Comm. Mag,** Vol. 34, pp. 90-95, 1997.

[7] P.P. Yupapin, W. Suwancharoen, "Entangled photon states generation and regeneration using a nonlinear fiber ring resonator," **Int. J. Light Electron. Opt,** Vol. 15, pp. 746-751, 2009.

[8] P.P. Yupapin, "Generalized quantum key distribution via microring resonator for mobile telephone networks," **Int. J. Light Electron. Opt,** Vol.121, pp. 422-425, 2010.

[9] R. W. Boyd. "Nonlinear Optics," **2nd Edition, Academic Press, Inc.**, 2003.

[10] G.P. Agrawal. "Nonlinear Fiber Optics," **San Diego, CA: Academic Press**, 2001.

[11] S. P. Singh and N. Singh. "Nonlinear Effects Optical Fibers: Origin, Management and Applications" **Progress In Electromagnetic Research (PIER),** Vol. 73, pp. 249-275, 2007.

[12] P. W. Smith, I. P. Kaminov, P. J. Maloney, and L. W. Stulz. "Self-contained integrated bistable optical devices," **Appl. Phys. Lett,** Vol. 34, pp. 62-65, 1979.

[13] C. Sripakdee, P.P. Yupapin, "Quantum noise generated by four-wave mixing process with in a fiber ring resonator," **Int. J. Light Electron. Opt,** Vol. 121, pp. 1155-1158, 2010.

[14] S. Suchat, N. Pornsuwancharoen and P.P Yupapin, "Continuous variable quantum key distribution via a simultaneous optical wireless up-down-link system," **Int. J. Light Electron. Opt,** pp. 1540-1544, 2010.

[15] P.P. Yupapin, S. Thongme and K. Sarapat, "Second-harmonic generation via microring resonators for optimum entangled photon visibility," **Int. J. Light Electron. Opt,** Vol. 121, pp. 599-603, 2010.

[16] H. Qiao et al. "Simulation of BB84 Quantum Key Distribution in depolarizing channel," **Proceedings of 14th Youth Conference on Communication, Scientific Research,** pp. 483-487, 2009.

[17] F. Matera et al., "Proposal of a high-capacity all-optical TDMA network," **Microw. Opt. Technol. Lett.** Vol. 1, pp. 132–141, 1998.

[18] M. He and X. Huang, "Efficient transmission scheme for multi-base station radio over fiber system by constituting a local area optical network," **Microw. Opt. Technol. Lett.** Vol. 52, pp. 526–529, 2010.

[19] P. Camarda et al., "Proposal of all-optical shuffle multihop networks with dedicated and shared channels," **Microw. Opt. Technol. Lett.**, Vol. 6, pp. 889–892 1993.

[20] S. N. Molotkov, "Explicit Attack on the Key in Quantum Cryptography (BB84 Protocol) Reaching the Theoretical Error Limit $Qc \approx 11\%$," **JETP Letters**, Vol.8(10), pp. 524-529, 2007.

[21] X. Mo et al., "Quantum-key distribution using quantum frames," **SPIE Newsroom**, pp. 1-3, 2010.

[22] Y. Kim et al., "Implementation of Polarization-Coded Free-Space BB84 Quantum Key Distribution," **Laser Physics**, Vol. 18, pp, 810-814, 2008.

[23] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," **Journal of Modern Optics**, Vol. 52, pp.691-705, 2004.

[24] R. Aaggawal et al., “Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol,” **International Journal of Computer Applications**, Vol. 20, pp. 28-31, 2011.

[25] M. Bourennane etal., “Quantum key distribution using multilevel encoding: security analysis,” **J. Phys. A: Math. Gen,** Vol.35, pp**.** 10065–10076, 2002.

[26] C. H. Bennett, "Quantum Cryptography: Uncertainty in the Service of Privacy," **Science**, Vol. 257, pp. 752-753, 1992.

[27] P. Hua et al., “Integrated optical dual Mach–Zehnder interferometer sensor,” **Sensor. Actuator. B Chem.,** Vol.87, pp. 250–257, 2002.

[28] Fan Yi Lin and Meng Chiao Tsai. Chaotic communication in radio over fiber transmission based on optoelectronic feedback semiconductor laser” **Optics Express**, Vol. 15(2), pp. 302-311, January 2007.

[29] C. Kostrzewa et al., “Tunable polymer optical add/drop flter for multiwavelength networks,” **Photon. Technol. Lett.**, Vol. 9, pp. 1487–1489, 1997.

[30] P. D. Townsend, “Quantum cryptography on optical fiber networks,” **Opt. Fiber Technol.**, Vol.4, pp.345–370, 1998.

[31] T. Carmon et al., “Feedback control of ultra-high-Q microcavities: application to micro-Raman lasers and microparametric oscillators,” **Opt. Express**, Vol.13, pp. 3558–3566, 2005.

[32] N. Gisin et al., “Quantum cryptography,” **Reviews of Modern Physics**, Vol. 74, pp. 145-195, 2002.

[33] Youplao PH. **“**Multi-Layers QKD Protocol Using Correlated Photon of Dark-Soliton Array in a Wavelength Router.” **Ph.D. Thesis of King Mongkut’s Institute of Technology Ladkrabang**, 2012.

[36] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” **Nature**, Vol. 299, pp. 802-803, 1982.

[37] E. Rieffel, "An introduction to quantum computing for non-physicists," **ACM Computing Surveys,** Vol. 32, pp. 300-335, 2000.

[38] Lomonaco, S., J., "A Quick Glance at Quantum Cryptography," Vol1, pp. 1-54, November, 1998.

[39] T. Aoki et al., "Observation of strong cooling between one atom and a monolithic microresonator," **Nature,** Vol.443, pp. 671–674, 2006.

[40] R. W. Boyd. "Nonlinear Optics**," 2nd Edition, Academic Press, Inc.**, 2003.

[41] J. S. Russell, "Report on waves," **Report of the 14th meeting of the British Association for the Advancement of Science,** pp. 331, 1844.

[42] K. Ikeda, H. Daido and O. Akimoto, "Optical Turbulence: Chaotic Behavior of Transmitted Light from a Ring Cavity," **Phys. Rev. Lett.**, Vol. 45, pp. 709-715, 1980.

[43] G.D. Van Wiggeren and R. Roy, "Optical Communication with Chaotic Wave forms," **Phys. Rev. Lett.**, Vol. 81, pp. 3547-3551, 1998.

[44] G.P. Agrawal. "Nonlinear Fiber Optics," **Academic Press, San Diego**, CA, USA., 2001.

[45] P.P. Yupapin, P. Saeung and W. Suwancharoen, "Coupler-loss and coupling-coefficient dependent of bistability and insatiability in fiber ring resonator: Nonlinear Behavior," **Journal of Nonlinear Optical Physics & Materials**, Vol. 16, pp. 111-118, 2007.

[46] D. Marcuse, A. R. Chraplyvy, and R. W. Tkach, "Effect of Fiber Nonlinearity on Long Distance Transmission," **Journal of Lightwave Technology**, Vol. 9, pp. 121–127, 1991.

[47] P.P. Mitra and J. B. Stark, "Nonlinear limits to the information capacity of optical fibre communications," **Nature,** Vol. 411, pp. 1027–1030, June 2001.

[48] A. Porzio, V. D'Auria, P. Aniello, M.G.A. Paris and S. Solimeno, "Bit threshold optimization for multiphoton communication in lossy channels," **J. Opt. and Laser Eng.**, Vol. 45, pp. 463-468, 2007.

[49] J. Ohtsubo, "Observation of the synchronization of chaos in mutually injected vertical-cavity surface-emitting semiconductor lasers," **IEEE J. Quantum Electron**., Vol. 28, pp. 1677-1679, 2003.

[50] A. Hasegawa and F. Tappert, "Transmission of stationary nonlinear optical pulses in dispersive dielectric fibers. I. Anomalous dispersion," **Appl. Phys. Lett,** Vol. 23, No. 142, 1973.

[51] L. F. Mollenauer, R. H. Stolen, and J. P. Gordon, “Experimental observation of picosecond pulse narrowing and solitons in optical fibers,” **Phys. Rev. Lett**, Vol. 45, No. 13, pp. 1095-1980.

APPENDIX A

Quantum Key Distribution via wavelength Router

Soliton communication has been a successful system for long-distance optical communication links, where the required minimum repeater is the advantage has become the key advantage of the system performance. However, in practice, the problem of soliton-soliton interaction, soliton collision, and dispersion management are required to solve. Generally, there are two types of soliton known as bright and dark solitons, where the soliton behaviors and applications are well analyzed and described by Agarwal. In principle, the detection of dark soliton is extremely difficult. The dark soliton behavior has become the promising application when the transmission dark soliton can be converted into bright soliton after passing through into the specific add/drop filter which means that the transmission signals can be transmitted in the form of dark soliton, which is difficult to detect, whereas the specific end user that connects to the link via the specific add/drop filter can obtain the signals.

Although, the dark soliton applications have been widely investigated in various applications the searching for further applications remains. The use of soliton, i.e., bright soliton in long-distance communication links has been in operation for nearly two decades. However, some questions still need to be answered in the area of communication safety, whereas the use of a dark soliton pulse within a micro-ring resonator for communication security has been studied. The investigation of dark soliton behaviors has been reported and one has shown the interesting result that the dark soliton can be stabilized and converted into bright soliton and finally detected. This means that we can use the dark soliton to perform the communication transmission for security, whereas the required information can be retrieved by the dark-bright soliton conversion, in which the use of optical micro-cavities or micro-ring resonators have shown the promising applications for dark soliton, where a PANDA ring resonator is a new model of them, which has been successfully used to investigate the dynamic behavior of dark-bright soliton collision.

In this thesis dark and bright soliton are given by Eq. (3.55) and (3.36) in chapter 3. The simulation results obtained have shown that the proposed system can be used to form the security keys, where the secret keys can be retrieved and achieved, which is useful for computer and communication applications, especially, where in addition the high capacity and long distance link can be realized by using the soliton communication.

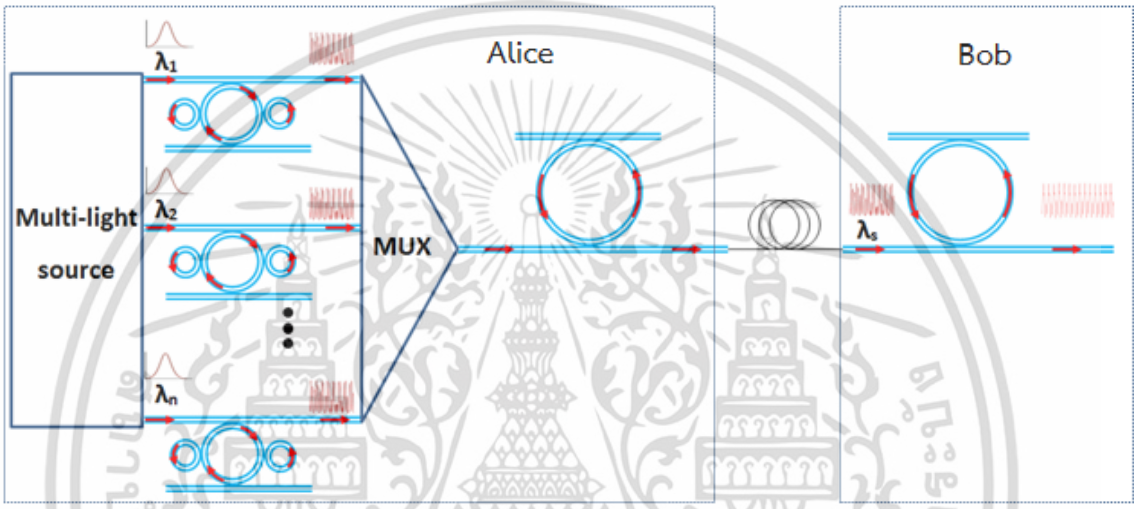

Figure A.1 Schematic of generation Multi-wavelength system, where λ_1-λ_n are bright Soliton inputs, MUX: Optical multiplexer

The multiplexed bright soliton pulses, which it is input from multi-light source, that introduce the multi-wavelength generation, a stationary multi-wavelength pulses are introduced into the PANDA ring resonator system as shown in Figure A.1. Each of input optical fields λ_1-λ_n of the bright soliton pulses within the nonlinear material, the resonant output is formed, thus the normalized output of the light field is the ratio between the output and input in each roundtrip. In this thesis, we propose the multiplexed solitons in Alice's side can be transmitted into the link via an optical multiplexer (MUX), where the multi-wavelength λ_1-λ_n, i.e. wavelength division multiplexing of bright soliton is formed, which used to form the multi wavelength soliton bands. Simulation results obtained have shown that slightly difference of

soliton center wavelengths can be generated and used for packet switching applications. Then Bob receives the signal as multi-wavelength λ_s, which is filter by using add/drop filter for choosing specific wavelength, which used for quantum processer. Moreover, the use of a quantum processor incorporating in the system can provide the quantum key distribution within the wavelength router, whereas the multivariable QKD can be employed for high capacity and security communication applications.

In this thesis our team have presented the idea of "quantum router", which it is made up of add/drop filters, its performance depends on that of add/drop filters as shown in Figure A.2. Nowadays, the micro or/and nano-waveguides are gaining prominence. Filters show us good stability and isolation between channels at moderate cost. By the way, add/drop filters' capability will impact the size of network. The maximum nodes of a network depend on the max amount of channels of add/drop filter. Takada and his team have presented about the popular Dense Wavelength-division multiplexing (DWDM) product, which has 40 channels, and 4.200 channels have been achieved in laboratory. That means, it is possible to build a ''quantum router'' with 4.200 ports in future, and this QKD net size may be enough for a big city. Moreover, the insertion loss will reduce the efficient QKD distance. As signals will pass through add/drop filter when they pass the ''quantum router'', the insertion loss of popular product is 5 dB. According to the performance of the present point-to-point QKD system, we can build a QKD network over 50 km at least. That will still meet the requirement of a big city. Along with the development of Wavelength-division multiplexing (WDM) technology at the moment, the insertion loss will be <1 dB in future and then the quantum network will able to cover >100 km. In Fig A.2. In operation, the computing data can be modulated and input into the system via a wavelength router, which is encoded by the quantum secret codes. The required data can be retrieved via the drop port of the add/drop filter in the router, whereas the quantum secret codes can be specified between $Alice_x$ and Bob_x. Moreover, the high capacity of data can be applied by using more wavelength carries which can be providing by the correlated photon generation.

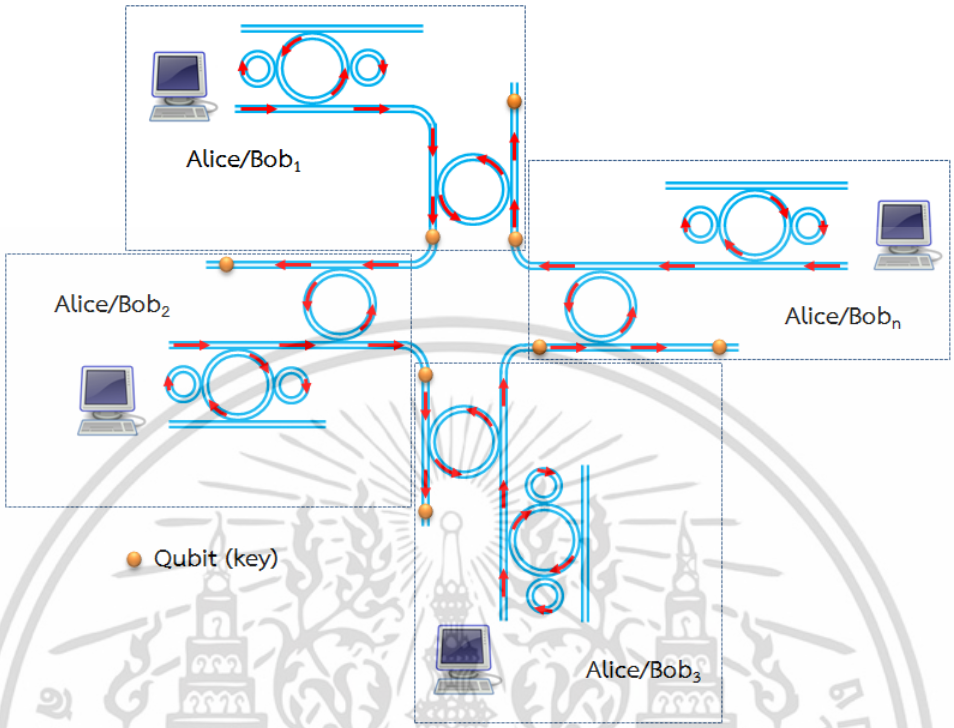

Figure A.2 A system of quantum cryptography for internet security via a wavelength router, where QP: Quantum Processor, R_j : ring radii, λ_i : output wavelength, K_j , K_{ji} are coupling coefficients.

APPENDIX B

LIST OF PUBLICATIONS

1. **X. Louangvilay**, S. Mitatha, M. Yoshida N. Komine Preecha P. Yupapin, "Novel soliton cryptography using optical key generated by orthogonal dark-bright soliton pair," **Optical Engineering,** Vol. 51(8), pp. 085010-7, 2012
2. **X. Louangvilay**, S. Mitatha, M. Yoshida N. Komine Preecha P. Yupapin, "High Capacity and Security Codec using Dark-Bright Soliton Conversion in PANDA Ring Circuit," **International Conference on Embedded Systems and Intelligent Technology (ICESIT 2015),** pp. 118-121, 2015
3. **X. Louangvilay**, S. Mitatha, M. Yoshida N. Komine Preecha P. Yupapin, "Generalized quantum key distribution (QKD) using PANDA ring resonator and series micro ring resonator for communication security use," **JSST 2015 The 34th JSST Annual Conference: International Conference on Simulation Technology Toyama International Conference Center,** pp 225-236, 2015

BIOGRAPHY

Name	:	Mr. Xaythavy Louangvilay
Date of Birth	:	25 April, 1982
Place of Birth	:	Vientiane Capital City, Lao P.D.R
sCurrent Address	:	Phonekheng Village, Saysetha District, Vientiane Capital City, Lao P. D. R
Email	:	xaythavy@hotmail.com
Education	:	- Bachelor's Degree in Electronic Engineering, National University of Laos (NOUL), Lao P. D. R, in 2004. - Master's Degree in Computer Engineering, King Mongkut's Institute of Technology Ladkrabang, Thailand, (KMITL).
Skilled Works	:	- Computer Programmimg(C/C++/JAVA) - Wave Design and Wave Programming(HTML/Perl/PHP) - Data Base System - Opticomunication