A STUDY OF OPTICAL AND QUANTUM SECURITY USING A WAVELENGTH ROUTER

XAYTHAVY LOUANGVILAY

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN COMPUTER ENGINEERING

INTERNATIONAL COLLEGE

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2011

KMITL-2010-IC-M-006-001

Thesis Title	A study of Optical and Quantum security using a Wavelength Router
Student	Mr. Xaythavy Louangvilay
Student ID	52601103
Degree	Master of Engineering
Program	Computer Engineering
Year	2011
Thesis Advisor	Assoc. Prof. Dr. Somsak Mitatha Prof. Dr. Yoshida Masahiro

ABSTRACT

In this Thesis we propose a system of quantum cryptography for internet security using Gaussian pulses propagating within a nonlinear ring resonator system, quantum processor and a wavelength router. To increase the channel capacity and security, the multiplexer is operated incorporating a quantum processing unit via an optical multiplexer. The transmission part can be used to generate the high capacity quantum codes within the series of micro ring resonators and an add/drop filter. The receiver part can be communicated by using the quantum key (quantum bit, qubit) via a wavelength router and quantum processors. The reference states can be recognized by using the cloning unit, which is operated by the add/drop filter, where the communication between Alice and Bob can be performed. Results obtained have shown that the correlated photons can be generated and formed the entangled photon pair, which is allowed to form the secret key between Alice and Bob. In application, the embedded system within the computer processing unit is available for quantum computer. Furthermore, such a concept is also available for internet application via hybrid communications, for instance, wire/wireless, satellite, which can be used to form the internet security.

For the future work I will be focused on the use of new protocol for network security, 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.

ACKNOWLEDGEMENTS

Firstly of all, I would like to express my guidance sincere gratitude to my advisor, Assoc. Prof. Dr. Somsak Mitatha and Prof. Dr. Yoshida Masahiro 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 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

CONTENTS (Cont.)

LIST OF FIGURES

LIST OF FIGURES (Cont.)

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Basic Background

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 dimensions commensurate with the wavelengths used in hi-speed communication systems.

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 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 [1]. 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.

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 picojoule(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 *microring resonators*.

1.2 Optical Signal Processing using Ring Resonator

First of all we introduce what Ring Resonator is? A ring resonator is simply a waveguide shaped into a ring structure. When an input electric field, E_i (we will present details in chapter 2) 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 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 [3] or used in a free-standing configuration [4]. Nonlinear optics can enable signal processing without the

requirement of external electrical, mechanical, or thermal control [5]. The response time of properly designed nonlinear optical devices is limited fundamentally only by the nonlinear response time of the constituent materials [6–9].

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 [5]. 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.

1.3 Optical and Quantum Security using Optical Techniques

Demand of using computer has been increased widely and rapidly every year, therefore, the security becomes the important function which is required and necessary. Up to date, a quantum technique is recommended to provide such a requirement. However, the security technique known as quantum cryptography has been widely used and investigated in many applications [10-12]. Recently, Suchat et al [13] have reported the interesting concept of continuous variable quantum key distribution 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. 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 [14] have proposed a new technique for QKD (Quantum Key Distribution) that can be used to make the communication transmission security and implemented with a small device such as mobile telephone hand set. 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 [15], 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 is presented. Mitatha et al [16] have proposed the design of secured packet switching used 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.

Both quantum communication and quantum information processing has been shown to be fundamentally different from its classical counterpart. Examples where this difference is highlighted are secure key distribution for cryptography, and the existence of fast algorithms for an idealized quantum computer. Quantum network has also been introduced and become the promising technology that can be used to fulfill the perfect network security. Some research works have been reported in various forms of applications [17, 18]. The use of quantum key distribution via optical network has been reported [19, 20]. To date quantum key distribution is the only form of information that can provide the perfect communication security. The use of QKD has been proposed in many research works, whereas the applications in different forms - such as point to point link [21], optical wireless [22], satellite [23], long distance [24] and network [25] - have been reported. However, a more reliable system for network security is needed, which is both high capacity and secure. The concept of continuous variable in the form of dense wavelength multiplexing is introduced to overcome such a problem. By using the continuous variable concept, the continuous QKD can be formed and available for a large demand. There are some works proposed the use of continuous variable QKD with quantum router and network [26, 27]. However, the requirement of large bandwidth signal and dense wavelength multiplexing become the practical problems. Yupapin et al [28] have also shown that the continuous wavelength can be generated by using a soliton pulse in a micro ring resonator, which can be used to overcome such problems.

1.4 Goal Of theThesis

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

1. To study and understand the theories of quantum such as photon, single photon, entangle photon, etc., to use in quantum cryptography by waveguide ring resonators system technique.

2. To understand how to use series nonlinear Microring and Nano ring resonator and an add/drop filter for generation the high capacity quantum codes by using Gaussian pules is input.
3. To understand communication by using the quantum key (quantum bit, qubit) via a wavelength router and quantum processors.

1.5 Scope of the Thesis

To attain of this thesis, we introduce perfect security by quantum cryptography using optical waveguide nonlinear ring resonator system technique, which input is Gaussian pules. To study and introduce how to generate quantum key within series micro, nano ring resonators and add/drop filter. For the receiver part can be communicated by using quantum key via a wavelength router and quantum processor. We also introduce theories of ring resonator, quantum information, quantum cryptography and BB84 protocol system also.

1.6 Thesis Outlines

This thesis presents a study of optical and quantum security using a wavelength router as consists five chapters, each chapter is as follows:

- The current 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 Nonlinearity Susceptibility and also describes about nonlinear ring resonators, add/drop filter. We have described about light pulses in ring resonator as use Gaussian pules propagating, final we introduce nonlinear communication and security.
- Chapter 3 presents the quantum information theories such as photon, entangled photon, single photon and quantum bit, we describes about chaotic signal generation and recovery. We also describe cryptography concept, quantum cryptography and BB84 protocol system.

- To correlate photon generation is contained in chapter 4 that is the main of this thesis. We present how to generate quantum key within series micro, nano ring resonators and add/drop filter by using Gaussian pules is input and we also present quantum distribution key via wavelength router.
- For the last chapter in this thesis is chapter 5 presents a summary of the results of the thesis and a discussion of future research.

CHAPTER 2

NONLINEAR RING RESONATOR AND COMMUNICATION

The use of semiconductor materials as nonlinear optical elements bridges the gap between optics and electronics. It opens the possibility for integrating the laser sources, signal processing elements, and detectors on the same platform. In this regard, the III-V binary semiconductors, such as GaAs and InP, have acquired great attention in the last few decades because they are direct bandgap materials and possess higher nonlinear coefficients than their competing materials. Another attractive feature of binary semiconductors is that they can be combined or alloyed to form ternary or quaternary compounds. Doing so, makes it possible to vary the bandgap of the material continuously together with its band structure, electronic, and optical properties. As an example, the bandgap energy of the ternary compound $Al_xGa_{1-x}As$ depends on the mole fraction x. Another important quaternary compound that we will consider is $In_{1-x}Ga_xAs_yP_{1-y}$. Therefore, one can design ternary and quaternary compounds to be transparent for optical channel waveguides or active for lasers and amplifiers at the 1550 nm communication window.

In this chapter we will discuss different nonlinear processes that affect the performance of semiconductor micro ring resonators as all-optical signal processing tools.

2.1 Nonlinear and Susceptibility

Nonlinear optics is the study of phenomena that occur as a consequence of the modification 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 [29]. The general equation that describes the optical field evolution in a dielectric material is given by

$$\nabla^2 \mathrm{E} - \frac{1}{c^2}\frac{\partial^2 \mathrm{E}}{\partial t^2} = -\mu_0 \frac{\partial^2 \mathrm{P(E)}}{\partial t^2} \tag{2.1}$$

where the polarization $\vec{P}$ 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

$$\vec{P} = \underbrace{\varepsilon_0 \vec{E} + \varepsilon_0 \chi^{(1)} : \vec{E}}_{linear\ P_L} + \underbrace{\varepsilon_0 \chi^{(2)} :: \vec{E} \cdot \vec{E} + \varepsilon_0 \chi^{(3)} ::: \vec{E} \cdot \vec{E} \cdot \vec{E} + \ldots,}_{nonlinear\ P_{NL}} \tag{2.2}$$

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.

2.2 Nonlinear Refractive Index (Optical Kerr Effect)

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

$$\vec{E}(t) = \mathrm{Re}\left\{\vec{E} \exp j(\vec{k} \cdot \vec{r} + \omega t)\right\} \tag{2.3}$$

or similarly as

$$\vec{E}(t) = \frac{1}{2}\vec{E} \exp j(\vec{k} \cdot \vec{r} + \omega t) + c.c. \tag{2.4}$$

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

$$\vec{E}(t) = \frac{1}{2}E_x \hat{x} \exp j(kz + \omega t) + c.c. \tag{2.5}$$

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 will only 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

$$P_L = \varepsilon_0(1+\chi^{(1)})E \tag{2.6}$$

And

$$\begin{aligned} P_{NL} &= P^{(3)} \\ &= \varepsilon_0\chi_{xxxx}(\omega;-\omega,\omega,\omega)E^*EE \\ &\quad + \varepsilon_0\chi_{xxxx}(\omega;\omega,-\omega,\omega)EE^*E \\ &\quad + \varepsilon_0\chi_{xxxx}(\omega;\omega,\omega,-\omega)EEE^* \\ &= 3\varepsilon_0\chi_{xxxx}|E|^2E \\ &= \frac{3}{4}\varepsilon_0\chi_{xxxx}|E_x|^2E \end{aligned} \tag{2.7}$$

respectively. Hence,

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

The total dielectric constant

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

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:

$$n = \sqrt{\varepsilon_r + \Delta\varepsilon_r} \approx \sqrt{\varepsilon_r} + \frac{\Delta\varepsilon_r}{2\sqrt{\varepsilon_r}} = n_0 + \frac{3\chi_{xxxx}}{8n_0}|E_x|^2 \tag{2.8}$$

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

$$n = n_0 + n_2|E|^2 \tag{2.9}$$

Comparing Eq.(2.8) and Eq.(2.9), the nonlinear refractive index is directly determined by the third-order susceptibility as

$$n_2 = \frac{3\chi_{xxxx}}{8n_0} = \frac{3\chi^{(3)}}{8n_0} \tag{2.10}$$

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.

2.3 Optical Add/Drop Filter

2.3.1 Ring Resonators

The architecture of a nonlinear fiber optics ring resonator as illustrated in Figure 2.1, 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 [30]

$$n = n_0 + n_2 I = n_0 + (\frac{n_2}{A_{eff}})P, \tag{2.11}$$

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}.

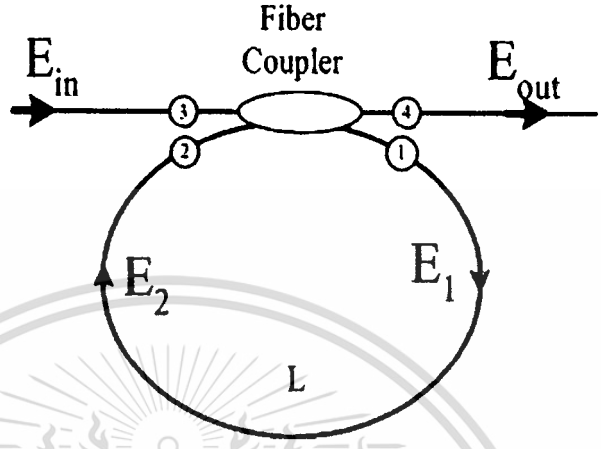

Fig. 2.1 Schematic diagram of FORR with a single fiber coupler.

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:

$$t_{34} = t_{21} = (1-\gamma)\sqrt{1-\kappa}, \qquad t_{31} = t_{24} = j(1-\gamma)\sqrt{\kappa},$$
$$t_{32} = t_{41} = 0. \tag{2.12}$$

The following relations of the electric fields arise from Eq. (2.11):

$$E_1 = t_{31}E_{in} + t_{21}E_2, \tag{2.13a}$$

$$E_{out} = t_{34}E_{in} + t_{24}E_2. \tag{2.13b}$$

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

$$\frac{\partial E}{\partial z} = j\frac{2\pi n_2}{\lambda}|E|^2 E - \frac{1}{2}\alpha E. \tag{2.14}$$

Integrating the equation (2.13) direct, we can thus obtain the following relation:

$$E_2 = E_1\tau\exp(-j\phi) = E_1\tau\exp\{-j(\phi_0 + \phi_{NL})\}, \tag{2.15}$$

Where $\phi_0 = kLn_0$ and $\phi_{NL} = kLn_2|E_1|^2$ are the linear and nonlinear phase shift, $k = 2\pi/\lambda$ is the wave propagation number in a vacuum, and L is the fiber ring resonator length. $\tau = \exp(-\alpha L/2)$ 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 Esq. (2.11) and (2.13) the map can be written as

$$E_1(t) = j(1-\gamma)\sqrt{\kappa}E_{in} + (1-\gamma)\sqrt{1-\kappa}\,\tau E_1(t-t_R)\exp(-j\phi). \tag{2.16}$$

$$E_{n+1} = j(1-\gamma)\sqrt{\kappa}E_{in} + (1-\gamma)\sqrt{1-\kappa}\,\tau E_n\exp(-j\phi), \tag{2.17}$$

Where the subscript "n" denotes the number of round trips inside the FORR. Using Eq. (2.15), the nonlinear map can be iterated for a given value of the input power P_{in} ($\alpha|E_{in}|^2$). 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 [31, 32]. The single-mode fiber was used in 1983 as the nonlinear medium inside a ring cavity [33]. 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. (2.16), we have

$$E_1 = j(1-\gamma)\sqrt{\kappa}E_{in} + (1-\gamma)\sqrt{1-\kappa}\tau\exp(j\phi)E_1. \tag{2.18}$$

While the output field at steady state as

$$E_{out} = (1-\gamma)\cdot E_{in}\left[\sqrt{1-\kappa} - \frac{(1-\gamma)\kappa\tau\exp(j\phi)}{1-(1-\gamma)\sqrt{1-\kappa}\tau\exp(j\phi)}\right]. \tag{2.19}$$

Thus the normalized of the light field from Eq. (2.19) can be expressed as

$$\left|\frac{E_{out}}{E_{in}}\right|^2 = (1-\gamma)^2\left[1 - \frac{\kappa\left[1-(1-\gamma)^2\tau^2\right]}{1+(1-\gamma)^2(1-\kappa)\tau - 2(1-\gamma)\sqrt{1-\kappa}\tau\cos\phi}\right]. \tag{2.20}$$

Eq. (2.17) and (2.20) are mathematical relations are used for characterizing a nonlinear effects such as bifurcation, chaos, and optical bistability, respectively.

The parameters of the simulation results were set as follow: input light with the design wavelength $\lambda = 1.55\,\mu m$, $n_0 = 1.45$, $A_{eff} = 50\,\mu m^2$, $\alpha = 0.02$ dB/km, $\gamma = 0.1$ and $L = 80$ m. The power coupling coefficient of $\kappa = 0.9$. Here, the constant linear phase term is neglected $\phi_0 = 0$. In this study, the plot of 10,000 iterations of round-trips inside the optical fiber ring.

In Figure 2.2 shows curve of output power as a function of the number of ring passes in FORR. The maximum output power results from pumping CW envelope is

approximately 140 W. However, to meet the realistic application the smaller ring length with lower input power than the parameters, which the introduced as the result shown in Figure 2.2. In this work the coupling power coefficient of the coupler was fixed with $\kappa =$ 0.02. The optical power depends on the nonlinear refractive indices which ranges from $n_2 = 2.0 - 3.4 \times 10^{-20}$ m^2/W. The simulated data of ten thousand iterations i.e. roundtrips inside the micro ring was shown. We also assume that $\phi_0 = 0$ for simplicity.They have shown that the nonlinear effects in fibre ring resonator could cause the problem in communication system, however, this is useful to implement in the realistic application when the device fabrication is required.

In Fig. 2.2 shows curve of output power as a function of the number of roundtrips in FORR. The maximum output power results from pumping CW envelope is approximately 140 W and at the begin output power is direct proportional with input power. Besides, for realizing an optical bifurcation is also achieved when the light passes through FORR at the roundtrips of 7,000 times and the roundtrips of 8,100 times the optical bifurcation become to optical chaos.

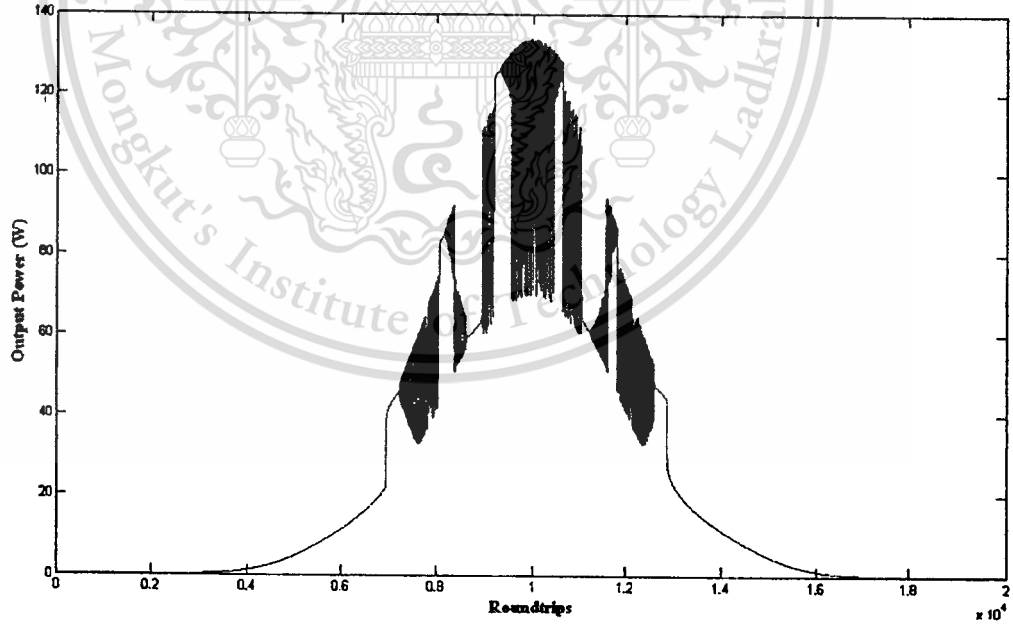

Fig. 2.2 The output power for varying number of roundtrips, with $\phi_0 = 0$, $n_2 = 3.2\text{x}10^{-20}$ m^2/W, $\gamma = 0.1$ and $\kappa = 0.0225$

2.3.2 Micro Ring Resonator

A ring resonator is simply a waveguide shaped into a ring structure as shown in Fig. 2.3.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 will be allowed to resonate inside the ring waveguide, thus frequency selectivity is obtained. A resonant mode will have a wavelength that satisfies [34,35],

$$m\lambda_m = nL, \quad m = \text{integer}. \tag{2.21}$$

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

$$E_r(t) = -j\kappa E_i(t) + rae^{j\phi}E_r(t-\tau), \tag{2.22}$$

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

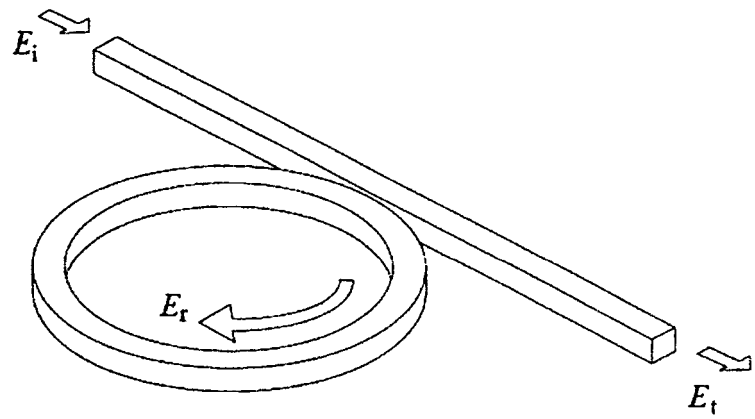

Fig. 2.3 Schematic diagram for a ring resonator coupled to a single waveguide.

The resonator round trip phase, ϕ, is given by

$$\phi = \frac{2\pi}{\lambda} nL \tag{2.23}$$

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

$$E_t(t) = rE_i(t) - j\kappa a e^{j\phi} E_r(t-\tau) \tag{2.24}$$

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

$$\frac{E_t}{E_i} = \frac{r - ae^{j\phi}}{1 - rae^{j\phi}} \tag{2.25}$$

A close examination of Eq. (2.24) indicates that a ring resonator is very similar to a Fabry-Perot cavity. In the particular case shown in Fig. 2.3, 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.

2.3.3 Add/Drop Filter in Ring Resonators

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 2.4

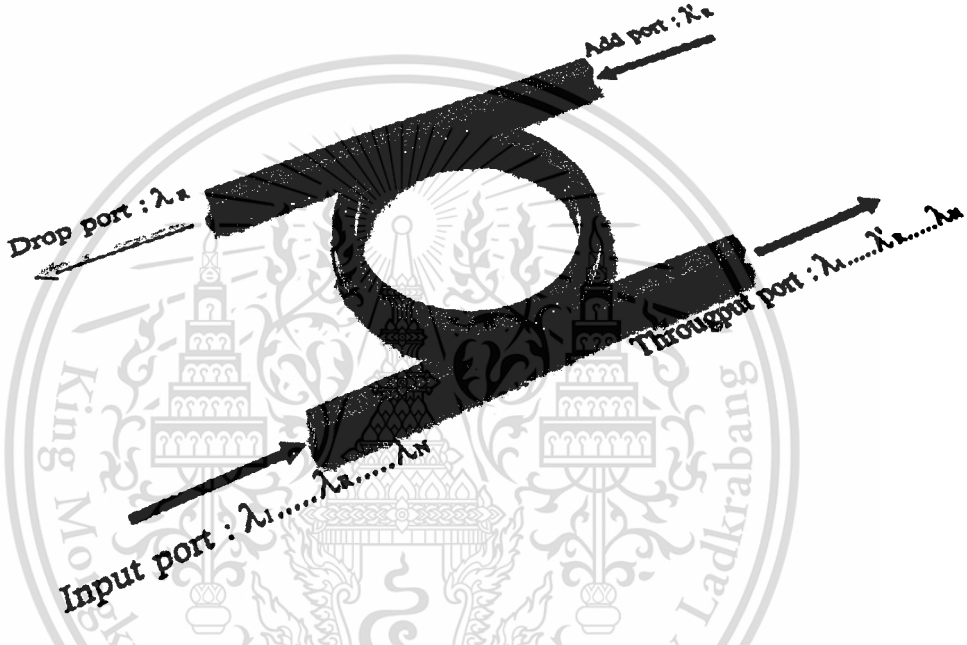

Fig. 2.4 Schematic diagram for a ring resonator coupled to two waveguides, in an add/drop filter configuration.

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 (λ'_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 will 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 will result. These issues will be studied and can be theoretically overcome by varying coupling parameters, inducing loss/gain in the ring and inserting additional rings between the two waveguides.

2.4 Light Pulse in Ring Resonator

We use Gaussian pulse in Ring Resonator. The simplest of this is circularly symmetric around the optical axis, thus depending only on the radial distance ρ from the beam axis

$$\rho^2 = x^2 + y^2 \tag{2.26}$$

This special solution is the Gaussian beam or fundamental mode, with a complex amplitude distribution of

$$\alpha(r,t) = \frac{\alpha_0}{q(z)} \exp\left(\frac{-ik\rho^2}{2q(z)}\right), \quad q(z) = z + iz_0 \tag{2.27}$$

Where z_0 is a constant. The Gaussian beam is a good spatial representation of a laser beam. Laser light is generated inside a cavity, constructed of mirrors, by multiple interference of waves and simultaneous amplification. These processes result in a well defined, stable field distribution inside the cavity, the so called cavity modes. The freely propagating beam is the extension of this internal field. It has the remarkable property that it does not change its shape during propagation. Both the internal and the external field are described by Eq. 2.27. By taking the square of the complex amplitude $\alpha(r,t)$ the intensity is found, resulting in a Gaussian transverse intensity distribution.

$$I(\rho,z) = I_0\left(\frac{W_0}{W(z)}\right)^2 \exp\left(\frac{-2\rho^2}{W^2(z)}\right) \quad \text{and} \quad W(z) = W_0\sqrt{1+\left(\frac{z}{z_0}\right)^2} \tag{2.28}$$

The properties of this Gaussian beam are the following: The shape of the intensity distribution remains unchanged by diffraction. The size of beam is given by $W(z)$. The beam has ots narrowest width at $z = 0$, the so-called waist of the beam. It corresponds to the classical focus, but rather than point-like, the Gaussian beam has a size of W_0 . This value gives the radial distance where the intensity has dropped from $I_0 = I(0,0)$ at the centre to $I(W_0,0) = I_{0/e}$.

2.5 Chaotic Signal Generation and Recovery

Chaos has been regenerated and studied as a nonlinear property in the areas such as mathematics [34], physics and electronics [35] and communications [36]. Most of them have reported the nonlinear properties can be accorded when the concerned parameters are suitable in some cases, which is commonly known as a non-periodic behavior and become a penalty of the system. However, the benefit of such a property can also be accepted. Chaotic communication has recently attracted great interest because of its potential applications in secure and the secretly communications [37], where it uses a noise-like broadband chaotic waveform as a carrier. Chaotic noise has been found useful in several areas of applications such as electronic communication [30], switching and control [38] and optical communication [39]. Most of them present the use of the benefit of such a nonlinear behavior, especially, in the military purpose when the information is required to keep in secret. In general, the nonlinearity of the system involves the behaviors such as chaos, bistability and bifurcation, which can be generated in the electronic circuit, optical fiber [40], laser system [41] and optical waveguide [42]. The device known as a micro ring resonator which can be formed by a waveguide or fiber optic has shown a very promising applications, for instance, when such a device is fabricated within the range of micrometer scale, and can be used incorporating a system such as mobile telephone hand set, computer and telecommunication networks. The primary scheme being considered for practical chaotic communication system is based on chaotic waveforms generated by lasers fiber ring resonator and to mask information within the chaotic waveform produced by a fiber ring resonator.

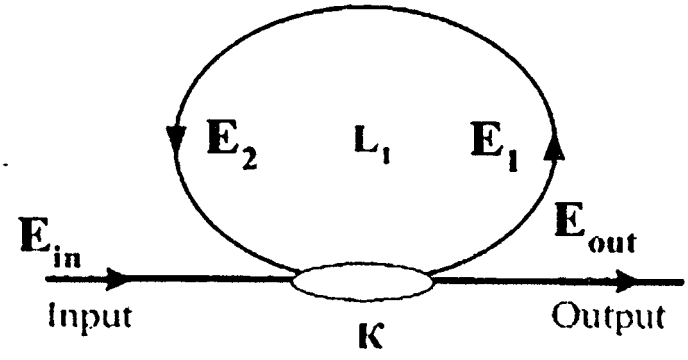

Fig. 2.5 schematic diagram micro ring resonator.

We have many techniques to generate chaotic signal. For this thesis we generate it by using ring resonator. A schematic diagram of a ring device is shown in Fig.3.29, where light from monochromatic light field amplitude and with a random phase modulation which results in temporal coherence degradation. In this thesis input light field we use Gaussian that can be express as Hence, the input light field can be expressed as

$$E_{in}(t) = E_0 \exp^{j\phi_0(t)} \tag{2.29}$$

We assume that the nonlinearity of the optical ring resonator is of the Kerr type, i.e., the refractive index is given by

$$n = n_0 + n_2 I = n_0 + (\frac{n_2}{A_{ff}})P \tag{2.30}$$

Where n_0 and n_2 are the linear and nonlinear refractive index, respectively. I and P are the optical intensity and the optical field power, respectively. The effective mode area of the device is A_{eff}, which is in the range 0.1 to 0.5 μm^2.

When a Gaussian pulse is input and propagated within a fiber ring resonator, the resonant output is formed, thus, the normalized output of the light field is the ratio between the output and input fields ($E_{out}(t)$ and $E_{in}(t)$) in each roundtrip, which can be expressed as [43]

$$\left|\frac{E_{out}(t)}{E_{in}(t)}\right|^2 = (1-\gamma)\left[1-\frac{(1-(1-\gamma)x^2)\kappa}{(1-x\sqrt{1-\gamma}\sqrt{1-\kappa})^2+4x\sqrt{1-\gamma}\sqrt{1-\kappa}\sin^2(\frac{\phi}{2})}\right] \quad (2.31)$$

each parameters will say in chapter 4 . The input optical field as shown in equation (3.29), i.e. a Gaussian pulse, is input into a nonlinear microring resonator. By using the appropriate parameters, the chaotic signal is obtained by using equation (2.31). To retrieve the signals from the chaotic noise, we propose to use the add/drop device with the appropriate parameters.

2.6 Nonlinear Communication and Security

We will present nonlinear optical that is an agency of nonlinear communication. Nonlinear optics is a topic of much current interest that exhibits a great diversity. Some publication on the subject are clearly physics, while others reveal an engineering bias; some appear to be accessible to the chemist, while others many appeal to biological understanding. Nonlinear optics is attracting increasing attention around the world because of its applications in telecommunications abs possibilities for optics information storage and computing. Optics fibre communication show that optics is already the method of choice for many purpose, owing to its wide bandwidth and freedom from electromagnetic interference. This is certainly obvious to those of us whose cities have had their streets dug up to lay new fibre-optic cable! To the existing advantages of optics, nonlinear optics adds further improvements in efficiency and versatility. A simple example is in amplification of optical signals over many kilometers, but eventually the signals need to be amplified. At present, this is done by converting the weak optical signal to an electronic one, amplifying that electronically, and then converting the strong electronic signal into a strong optical signal again. It would obviously be more efficient if the light beam could be amplified directly, say by a laser beam in a suitable medium. Such a process comes into the realm of nonlinear optics.

Information security has become a common demand in the data transmission link, where personal data security via mobile telephones has potential promising applications. To date, some works have shown that the use of a quantum technique to secure information data is advantageous over the electronic system. This technique is random coding, where qubits can be dynamically transmitted with the required information. There are two categories that have been proposed and

implemented successfully. Firstly, a technique using a single photon can provide extremely secure in formation, whereas the second one uses the orthogonal entangled states of photons to generate secure codes [48]. However, the single photon scheme has a limitation in sensitive losses of the photon energy in its link to the severe surrounding environment. Therefore, a more reliable scheme using the entangled photons is recommended. By this technique the entangled photons can generate the product of the random polarization state, which is enough to make the security requirement. For instance, the entangled states can be transmitted via free-space laser link, satellite, optical fiber [49], and optical wireless link. Generally, the entangled state production can be formed by two techniques: one generated by using the electron spin and the other is the orthogonal polarized photon states. The applications of these productions such as quantum cryptography [44, 45], quantum teleportation, and quantum metrology [46] have been reported. Recently, some works have showed promising techniques that can be used in entangled states' production.

CHAPTER 3

OPTICAL AND QUANTUM SECURITY

3.1 Single photon Generation and Recovery

3.1.1 Photon

So far we have taken the view of an experimentalist who would talk about detecting photon from a propagating beam of light. Photons have properties quite different from those of classical particles. They have energy $h\nu$ as given by Eg.3.1, 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 3.1. 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 3.1: 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 3.1 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

$$E = h\nu = h\frac{c}{\lambda} \tag{3.1}$$

where $h = 6.626 \times 10^{-34}$ 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

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

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 will be proportional to the number of photons crossing a unit area per unit time. Hence, if the beam is monochromatic (one frequency), the intensity I will be given by

$$I = (\text{energy of one photon}) \times \frac{\text{number of photons}}{\text{area} \times \text{time}} \tag{3.3}$$

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

By "exit through the horizontal port" we mean that a detector placed at the output of the horizontal port will detect a photon, or equally a photon detector placed at the vertical port does not detect a photon. These situations are illustrated in Fig. 3.2. The symbol for the state, $|-\rangle$, is referred as a ket. These definitions are sensible because a photon which exits through the horizontal port of the beamsplitter and is passed through another polarizing beamsplitter will certainly exit through horizontal port. A similar definition applies to vertical photons. The diagonal single photon state, $|D\rangle$, and anti-diagonal state, $|A\rangle$ can be defined in a similar way be analyzing the beams with a diagonal/anti-diagonal polarizing beamsplitter. 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

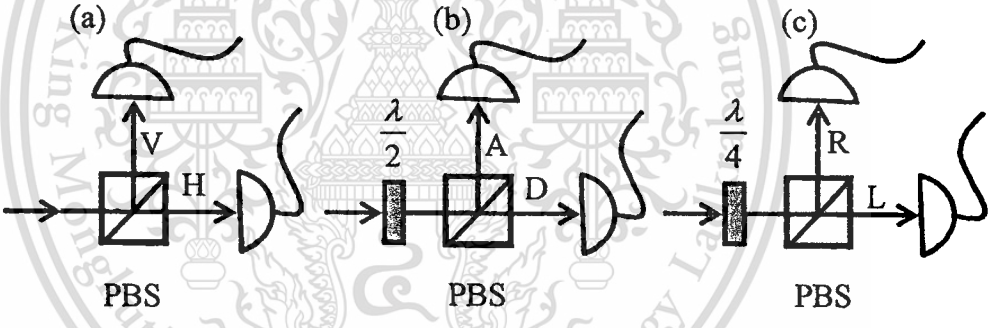

Fig. 3.2: Operational definition of different polarization state. PBS is a polarizing beamsplitter. $\lambda/2$ is half-wave plate, $\lambda/4$ is a quarter-wave plate. (a) horizontal-vertical polarization, (b) diagonal polarization, (c) right-left circular polarization.

If we send a diagonally polarized classical beam of light into a horizontal/vertical polarizing beamsplitter then half the beam will exit through the horizontal port and half will exit through ther vertical port. What will happen if we send single photons in the state $|D\rangle$ through this beamsplitter? 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 will 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. But can we tell in which direction an individual photon will go? To answer this first remember how $|D\rangle$ photons behave at a diagonal/anti-diagonal polarizing beamsplitter: 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 beamsplitter we have argued some must take one path and other take the other. Thus the path an individual photon in the state $|D\rangle$ take through the horizontal/vertical beamsplitter is not specified. All that is specified is that on average half the photons will go one way and half will go the other.

This example illustrates the fact that in quantum mechanics it is probabilities of outcomes, not particular outcomes that are predicted. Even though we can say with can say with certainty that a photon in the statewill emerge from the diagonal port of a diagonal/anti-diagonal beamsplitter, its reaction to a horizontal/vertical beamsplitter 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 the states. A photon in statewill randomly take one port or the other when sent into either a horizontal/vertical or a diagonal/anti-diagonal beamsplitter. A photon in state $|L\rangle$ will behave in the same way. Similarly a photon in state $|H\rangle$ will give a rrandom result for both diagonal/anti-diagonal and right/left circular polarizing beamsplitters and so on for the other states.

3.1.3 Photons as qubits

In this chapter 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 will be detected at the horizontal output of a

horizontal/vertical polarizing beamsplitter placed in the beam path. There is zero probability a photon will be found at the vertical output in the same time interval. A beam in the $|V\rangle$ will conversely only be 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 not only can we have zero's and one's, but we can also have superposition of zeros and ones such as the diagonal state $|D\rangle = 1/\sqrt{2}(|H\rangle + \langle V|)$. indeed bits can just as effectively be encode in such superposition states, for example using $|D\rangle$ as a sero and $|A\rangle = 1/\sqrt{2}(|H\rangle - \langle V|)$ 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 is 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 the two different bit value (i.e. $H = 0$ and $V = 1$). This continues to be true for muti-qubit states. For example if we start with two quit in the state

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

and we rotate both their polarizations by 45 degree we end up with the state

$$|H\rangle|H\rangle+|H\rangle|V\rangle+|V\rangle|H\rangle+|V\rangle|V\rangle \tag{3.9}$$

this is an equal superposition of all four possible two bit values. These generalizes to n qubits where the same operation of rotating every individual qubit leads to an equal superposition of all 2^n bit values. The single qubit rotations required here are just polarization rotations and can thus be performed easily wave plates.

Although this ability to span all possible input simultaneously hints at the possibility of increased communication or computation power suing qubit, it is not the whole story. Note in particular that analogues of the sort of superpositions represented by Eq. 3. 27 can also be created in classical systems as superpositions of classical waves. In order to unlock the full power of quntum information we need to create entangled state.

3.2 Entangled Photon

An excited atom emits two photons that come out back to back from the Einstein Podolsky Rosen (EPR) source, with vanishing angular momentum and even parity. If $|x\rangle$ and $|y\rangle$ are horizontal and vertical linear polarization states of the photon, then have seen that

$$|+\rangle=\frac{1}{\sqrt{2}}\left(|x\rangle+i|y\rangle\right)$$

$$|-\rangle=\frac{1}{\sqrt{2}}\left(i|x\rangle+|y\rangle\right) \tag{3.10}$$

are the eigenstates of helicity. For two photons, one propagating light is in the $+\hat{z}$ direction and other in the $-\hat{z}$ direction. The states

$$|x\rangle\rightarrow-|x\rangle \ , |+\rangle\rightarrow+i|-\rangle$$

$$|y\rangle\rightarrow|y\rangle \ , \ |-\rangle\rightarrow-i|+\rangle \tag{3.11}$$

therefore, the parity eigenstates are entangled states

$$\frac{1}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B \pm|-\rangle_A|+\rangle_B\right) \tag{3.12}$$

the state with $J_z = 0$ and even parity, then, expressed in terms of the linear polarization states, is

$$-\frac{i}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B \pm|-\rangle_A|+\rangle_B\right) = \frac{1}{\sqrt{2}}\left(|xx\rangle_{AB} + |yy\rangle_{BA}\right)_n = |\phi^+\rangle_{AB} \tag{3.13}$$

Because of invariance under rotations about $\hat{z}$, the state has this form irrespective of how we orient the x and y axes. We can use a polarization of either photon along any axis in the xy plane. Let $|x(\theta)\rangle$, and $|y(\theta)\rangle$ denote the linear polarization eigenstates along axes rotated by angle θ relative to the canonical x and y-axes. We may define an operator as (the analog of $\vec{\sigma}.\hat{n}$)

$$\tau(\theta) = |x(\theta)\rangle|x(\theta)\rangle - |y(\theta)\rangle|y(\theta)\rangle \tag{3.14}$$

Which has these polarization states as eigenstate with respective eigenvalues as

$$|x(\theta)\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix},$$

$$|y(\theta)\rangle = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} \tag{3.15}$$

Let $|H\rangle$ and $|V\rangle$ be two polarization states of photon, which are sent from Alice to Bob along two separated channels. We shall take two orthogonal states $|\psi_+\rangle$ and $|\psi_-\rangle$, linear combinations of $|H\rangle$ and $|V\rangle$, to represent bit value "0" and bit value "1," respectively:

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \tag{3.16}$$

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{3.17}$$

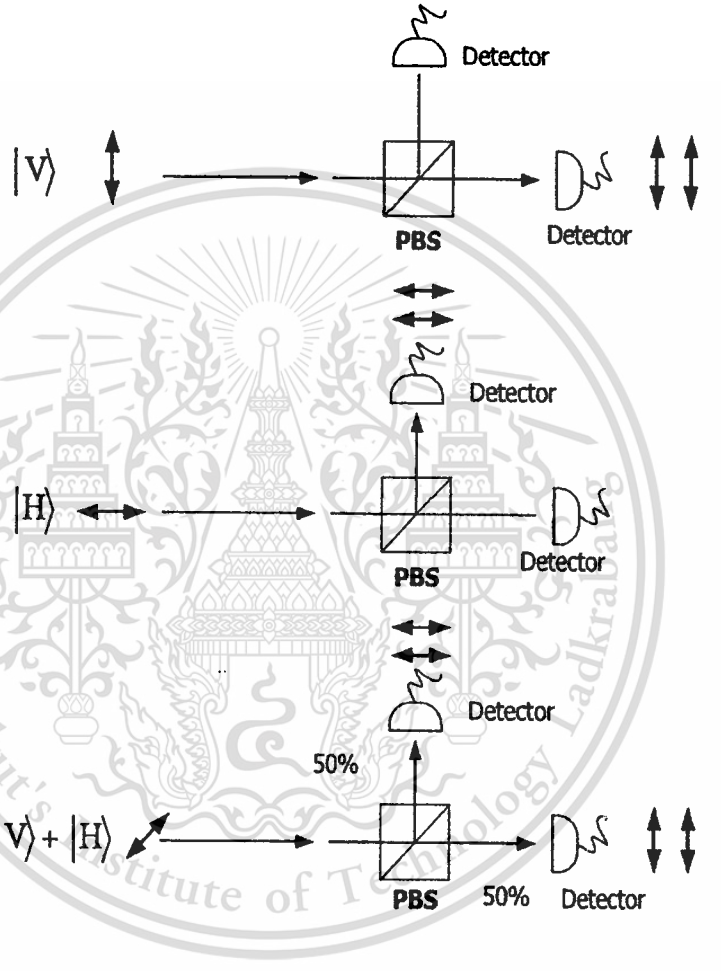

Figure 3.3 Schematic diagram of a single photon entangled state.

Alice sends to Bob either $|\psi_+\rangle$ or $|\psi_-\rangle$. The two localized states, $|H\rangle$ and $|V\rangle$, are not sent together, but $|V\rangle$ is delayed for some time τ. For simplicity, we choose τ to be larger than the traveling time of the particles from Alice to Bob, θ. Thus $|V\rangle$ starts traveling towards

Bob only when $|H\rangle$ already has reached Bob, such that the two wave packets and never found together in the transmission channels.

We shall consider a particular implementation of our scheme. The setup (Figure 3.2) consists of a Mach-Zehnder interferometer, with ϕ_A and ϕ_B as phase delays which and equal to time delay. Alice can transmit an information bit by sending either from a single particle or from short pulse of laser source, where the sending time t is random and registered by Alice for later use. The particle passes through the first beam splitter BS1 and evolves into a superposition of two localized wave packets. Finally, the two wave packets arrive simultaneously to the second beam splitter BS2 and interfere. A particle started in state $|\psi_+\rangle$ emerges at the detector D1, and a particle started in state $|\psi_-\rangle$ emerges at the detector D2. Bob. The detection of the arriving particle receives the bit sent by Alice: D1 was activated by mean of 0 and D2 mean 1, i.e. he registers the receiving time of the particle.

In this thesis, we use ring resonator technique that can be used to create the entangled photon. A coupler that separates the basic vertical and horizontal polarization states corresponds to an optical switch between the shot and long pules. We will say detail in Chapter 4.

3.3 Classical Cryptography

The purpose of cryptography is 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.

Cryptography operates by a sender scrambling or encrypting the original message or plaintext in a systematic way that obscures its meaning. The encrypted message or cryptotext is transmitted, and the receiver recovers the message by unscrambling or decrypting the transmission.

Originally, the security of a cryptogram depended on the secrecy of the entire encrypting and decrypting procedures. Today, however, we use ciphers in which the algorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular

message. 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 cryptotext 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. To prevent this being discovered by accident or systematic search, the key is chosen as a very large number.

Once the key is established, subsequent secure communication can take place by sending cryptotext, even over a public channel that is vulnerable to total passive eavesdropping, such as public announcements in mass media. However, to establish the key, two users, who may not be in contact or share any secret information initially, will have to discuss it, using some other reliable and secure channel. But since interception is a set of measurements performed by an eavesdropper on a channel, however difficult this might be from a technological point of view, any classical key distribution can in principle be passively monitored, without the legitimate users realizing that any eavesdropping has taken place. For cryptography there are two classical keys such as "public key" and "secret-key (private-key)".

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.

There are two problems with basing security on the assumed difficulty of mathematical problems. The first problem is that the difficulty of the mathematical problems is *assumed*, not proven. All security will vanish if efficient factoring algorithms are discovered. The second problem is the threat of quantum computers. The theoretical ability of quantum computers to essentially process large amounts of information in parallel would remove the time barrier to factoring large numbers. Thus, public-key encryption, though secure at the moment, faces a serious threat as quantum computing comes closer to reality. Currently, however, this method is still widely used, especially for the encryption of financial information sent over the internet.

Secret-key encryption requires that two users first develop and securely share a secret key, which is a long string of randomly-chosen bits. The users then use the secret key along with public

algorithms to encrypt and decrypt messages. The algorithms are very complex, and can be designed such that every bit of output is dependent on every bit of input. Suppose that a key of 128 bits is used. "Assuming that brute force, along with some parallelism, is employed, the encrypted message should be safe: a billion computers doing a billion operations per second would require a trillion years to decrypt it".

There are two main problems with secret-key encryption. The first problem is that by analyzing the publicly-known encrypting algorithm, it sometimes becomes easier to decrypt the message. This problem can be somewhat offset by increasing the length of the key. The second problem is securely distributing the secret key in the first place. This is the well-known "key-distribution problem". Users must either agree on the secret key when they are together in the same location or when they are in different locations. The drawbacks to developing the key when they are in the same location are that it is not always practical for the users to meet, a large database would be needed to store the pre-determined keys, and such storage is not secure. The drawback to developing a key when the users are in different locations is that all classical methods of transmitting the key are subject to eavesdropping that cannot be detected by the users.

Quantum cryptography solves the problems 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. 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.

3.4 Quantum Cryptography

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 either will or will not pass through a polarization filter, but if it emerges it will be aligned with the filter regardless of its inital state; there are no partial photons. Information about the photon's polarization can be determined by using a photon detector to determine whether it passed through a filter.

"Entangled pairs" are pairs of photons generated by certain particle reactions. Each pair contains two photons of different but related polarization. Entanglement affects the randomness of measurements. If we measure a beam of photons E1 with a polarization filter, one-half of the incident photons will pass the filter, regardless of its orientation. Whether a particular photon will pass the filter is random. However, if we measure a beam of photons E2 consisting of entangled companions of the E1 beam with a filter oriented at 90 degrees (deg) to the first filter, then if an E1 photon passes its filter, its E2 companion will also pass its filter. Similarly, if an E1 photon does not pass its filter then its E2 companion will not.

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. In particular, when measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements. For instance, if one measures the polarization of a photon by noting that it passes through a vertically oriented filter, the photon emerges as vertically polarized regardless of its initial direction of polarization. If one places a second filter oriented at some angle q to the vertical, there is a certain probability that the photon will pass through the second filter as well, and this probability depends on the angle q. As q increases, the probability of the photon passing through the second filter decreases until it reaches 0 at q = 90 deg (i.e., the second filter is horizontal). When q = 45 deg, the chance of the photon passing through the second filter is precisely 1/2. This is the same result as a stream of randomly polarized photons impinging on the second filter, so the first filter is said to randomize the measurements of the second.

A pair of orthogonal (perpendicular) polarization states used to describe the polarization of photons, such as horizontal/vertical, is referred to as a basis. A pair of bases are said to be conjugate bases if the measurement of the polarization in the first basis completely randomizes the measurement in the second basis [48], as in the above example with q = 45 deg. It is a fundamental consequence of the Heisenberg uncerty principle that such conjugate pairs of states must exist for a quantum system.

If a sender, typically designated Alice in the literature, uses a filter in the 0-deg/90-deg basis to give the photon an initial polarization (either horizontal or vertical, but she doesn't reveal which), a receiver Bob can determine this by using a filter aligned to the same basis. However if

Bob uses a filter in the 45-deg/135-deg basis to measure the photon, he cannot determine any information about the initial polarization of the photon .

These characteristics provide the principles behind quantum cryptography. If an eavesdropper Eve uses a filter aligned with Alice's filter, she can recover the original polarization of the photon. But if she uses a misaligned filter she will not only receive no information, but will have influenced the original photon so that she will be unable to reliably retransmit one with the original polarization. Bob will either receive no message or a garbled one, and in either case will be able to deduce Eve's presence.

Sending a message using photons is straightforward in principle, since one of their quantum properties, namely polarization, can be used to represent a 0 or a 1. Each photon therefore carries one bit of quantum information, which physicists call a qubit. To receive such a qubit, the recipient must determine the photon's polarization, for example by passing it through a filter, a measurement that inevitably alters the photon's properties. This is bad news for eavesdroppers, since the sender and receiver can easily spot the alterations these measurements cause. Cryptographers cannot exploit this idea to send private messages, but they can determine whether its security was compromised in retrospect.

The genius of quantum cryptography is that it solves the problem of key distribution. A user can suggest a key by sending a series of photons with random polarizations. This sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail.

3.5 Classical Protocol for Quantum Cryptography

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 [49]. In it, Bennett and Brassard described an unconditionally secure quantum key distribution system.

This protocol, known as BB84 after its inventors and year of publication, was originally described using photon polarization states to transmit the information. However, any two pairs

of conjugate states can be used for the protocol, and many optical fibre based implementations described as BB84 use phase encoded states. The sender (traditionally referred to as Alice) and the receiver (Bob) are connected by a quantum communication channel which allows quantum states to be transmitted. In the case of photons this channel is generally either an optical fibre or simply free space. In addition they communicate via a public classical channel, for example using broadcast radio or the internet. Neither of these channels need to be secure; the protocol is designed with the assumption that an eavesdropper (referred to as Eve) can interfere in any way with both.

The security of the protocol comes from encoding the information in non-orthogonal states. Quantum indeterminacy means that these states cannot in general be measured without disturbing the original state (see No cloning theorem). 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 (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handedness. Any two of these bases are conjugate to each other, and so any two can be used in the protocol. Below the rectilinear and diagonal bases are used as shown in table 3.1

Table 3.2: Basic photon polarization

Basis	0	1
+	↑	→
×	↗	↘

The table above is shown the basic if photon polarization and then we will present the BB84 protocol as follow these steps berow:

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 4 different polarization states, as they are not all orthogonal. The only possible measurement is between any two orthogonal states (a basis). 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, but if it was created as 45° or 135° (diagonal eigenstates) then the rectilinear measurement instead returns either horizontal or vertical at random. Furthermore, 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 is 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.

Each steps that presents above as shown in the table 3.3

Table 3.3: 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

CHAPTER 4

QUANTUM KEY DISTRIBUTION

4.1 Correlate Phonon Generation

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}), without pumping term, can be expressed as

$$E_{in}(t) = E_0 \exp^{-\alpha L + j\phi_0(t)} \tag{4.1}$$

Where L is a propagation distance (waveguide length).

We assume that the nonlinearity of the optical ring resonator is of the Kerr-type, i.e., the refractive index is given by

$$n = n_0 + n_2 I = n_0 + (\frac{n_2}{A_{eff}})P \tag{4.2}$$

Where n_0 and n_2 are the linear and nonlinear refractive indexes, respectively. I and P are the optical intensity and optical power, respectively. The effective mode core area of the device is given by A_{eff}. For the microring and nanoring resonators, the effective mode core areas range from 0.10 to 0.50 μm^2 [43]

When a Gaussian pulse is input and propagated within a fiber ring resonator, the resonant output is formed, thus, the normalized output of the light field is the ratio between the output and input fields ($E_{out}(t)$ and $E_{in}(t)$) in each roundtrip, which can be expressed as Eq. 4.3 [50]

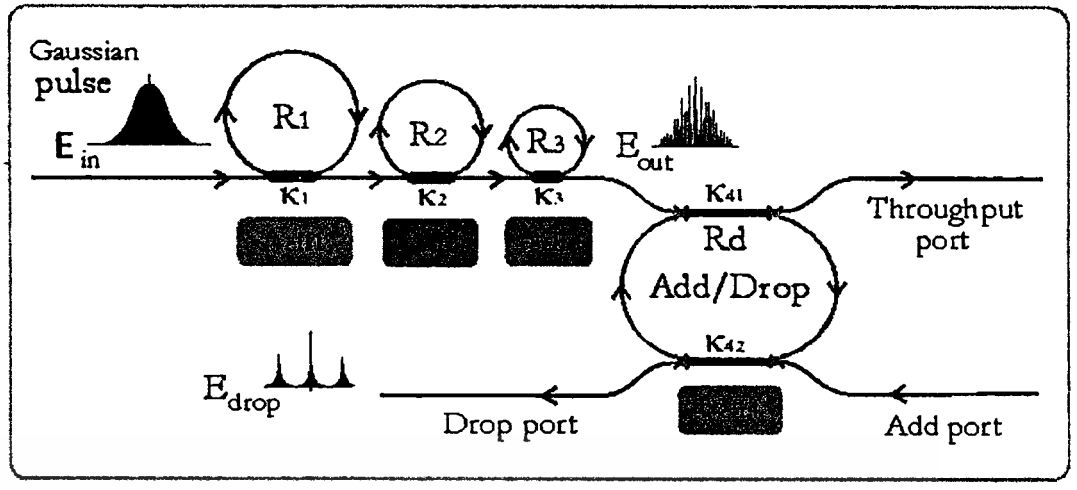

Fig. 4.1. A schematic of a Gaussian soliton generation system, where R_s: ring radii, K_s: coupling coefficients, R_d: an add/drop ring radius, A_{eff}s: Effective areas, $K_{4.1}$ and $K_{4.2}$ are coupling coefficients of an add/drop filter.

$$\left|\frac{E_{out}(t)}{E_{in}(t)}\right|^2 = (1-\gamma)\left[1-\frac{(1-(1-\gamma)x^2)\kappa}{(1-x\sqrt{1-\gamma}\sqrt{1-\kappa})^2+4x\sqrt{1-\gamma}\sqrt{1-\kappa}\sin^2(\frac{\phi}{2})}\right] \tag{4.3}$$

Equation (4.3) indicates that a ring resonator in the particular case is very similar to a Fabry-Perot cavity, which has an input and output mirror with a field reflectivity, (1-K), and a fully reflecting mirror. K is the coupling coefficient, and $x = \exp(-\alpha L/2)$ represents a roundtrip loss coefficient, $\phi_0 = kLn_0$ and $\phi_{NL} = kL(\frac{n_2}{A_{eff}})p$ are the linear and nonlinear phase shifts, $k = 2\pi/\lambda$ is the wave propagation number in a vacuum. Where L and α are a waveguide length and linear absorption coefficient, respectively. In this work, the iterative method is introduced to obtain the results as shown in equation (4.3), similarly, when the output field is connected and input into the other ring resonators.

The input optical field as shown in equation (4.1), i.e. a Gaussian pulse, is input into a nonlinear microring resonator. By using the appropriate parameters, the chaotic signal is obtained

by using equation (4.3). To retrieve the signals from the chaotic noise, we propose to use the add/drop device with the appropriate parameters. This is given in details as followings. The optical outputs of a ring resonator add/drop filter can be given by the equations (4.4) and (4.5).

$$\left|\frac{E_t}{E_{in}}\right|^2 = \frac{(1-\kappa_1) - 2\sqrt{1-\kappa_1}\cdot\sqrt{1-\kappa_2}\,e^{-\frac{\alpha}{2}L}\cos(k_n L) + (1-\kappa_2)e^{-\alpha L}}{1+(1-\kappa_1)(1-\kappa_2)e^{-\alpha L} - 2\sqrt{1-\kappa_1}\cdot\sqrt{1-\kappa_2}\,e^{-\frac{\alpha}{2}L}\cos(k_n L)} \tag{4.4}$$

$$\left|\frac{E_d}{E_{in}}\right|^2 = \frac{\kappa_1\kappa_2 e^{-\frac{\alpha}{2}L}}{1+(1-\kappa_1)(1-\kappa_2)e^{-\alpha L} - 2\sqrt{1-\kappa_1}\cdot\sqrt{1-\kappa 2}\,e^{-\frac{\alpha}{2}L}\cos(k_n L)} \tag{4.5}$$

Where E_t and E_d represents the optical fields of the throughput and drop ports respectively. The transmitted output can be controlled and obtained by choosing the suitable coupling ratio of the ring resonator, which is well derived and described by reference [53]. Where $\beta = kn_{eff}$ represents the propagation constant, n_{eff} is the effective refractive index of the waveguide, and the circumference of the ring is $L = 2\pi R$, here R is the radius of the ring. In the following, new parameters will be used for simplification, where $\phi = \beta L$ is the phase constant. The chaotic noise cancellation can be managed by using the specific parameters of the add/drop device, which the required signals at the specific wavelength band can be filtered and retrieved. K_1 and K_2 are coupling coefficient of add/drop filters, $k_n = 2\pi/\lambda$ is the wave propagation constant in a vacuum, and the waveguide (ring resonator) loss is α = 0.5 dBmm^{-1}. The fractional coupler intensity loss is γ= 0.1. In the case of add/drop device, the nonlinear refractive index is neglected.

From Fig. 4.1, in principle, light pulse is sliced to be the discrete signal and amplified within the first ring, where more signal amplification can be obtained by using the smaller ring devices (second ring and third ring). Finally, the required signals can be obtained via a drop port of the add/drop filter. In operation, an optical field in the form of Gaussian pulse from a laser source at the specified center wavelength is input into the system. From Fig. 4.2, the Gaussian pulse with center wavelength (λ_0) at 1.30 μm, pulse width (Full Width at Half Maximum, **FWHM**) of 20 ns, peak power at 2 W is input into the system as shown in Fig. 2(a). The large bandwidth signals can

be seen within the first microring device, and shown in Fig. 4.2(b). The signal amplification is also seen in Fig.4.2(b), 4.2(c) and 4.2(d), where the amplified output of 30 W can be achieved with K=0.7 for R2 and R3 when we have compared with other value of K.

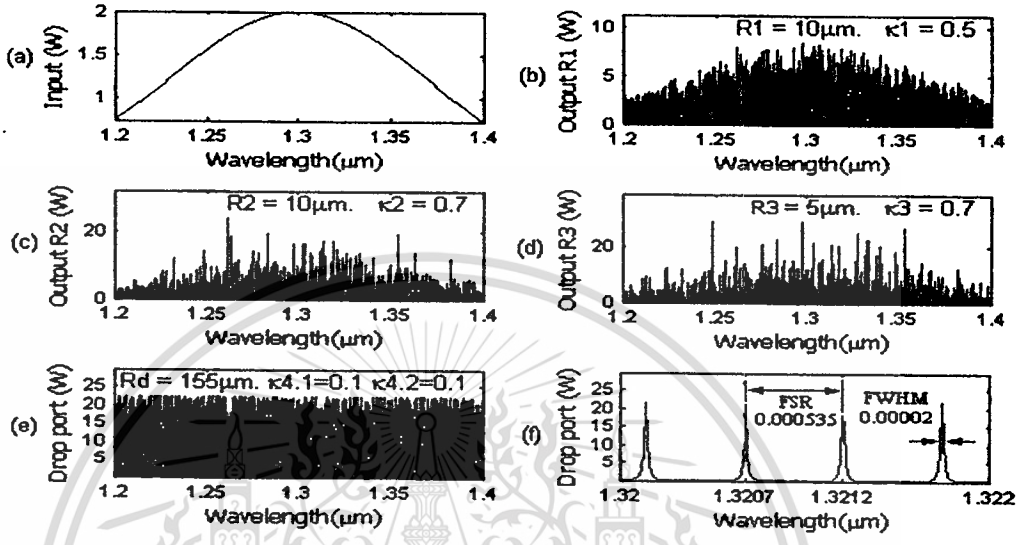

Fig. 4.2 the Gaussian pulse with center wavelength (λ_0) at 1.30 μm, pulse width of 20 ns, peak power at 2 W with K = 0.7 for R2 and R3.

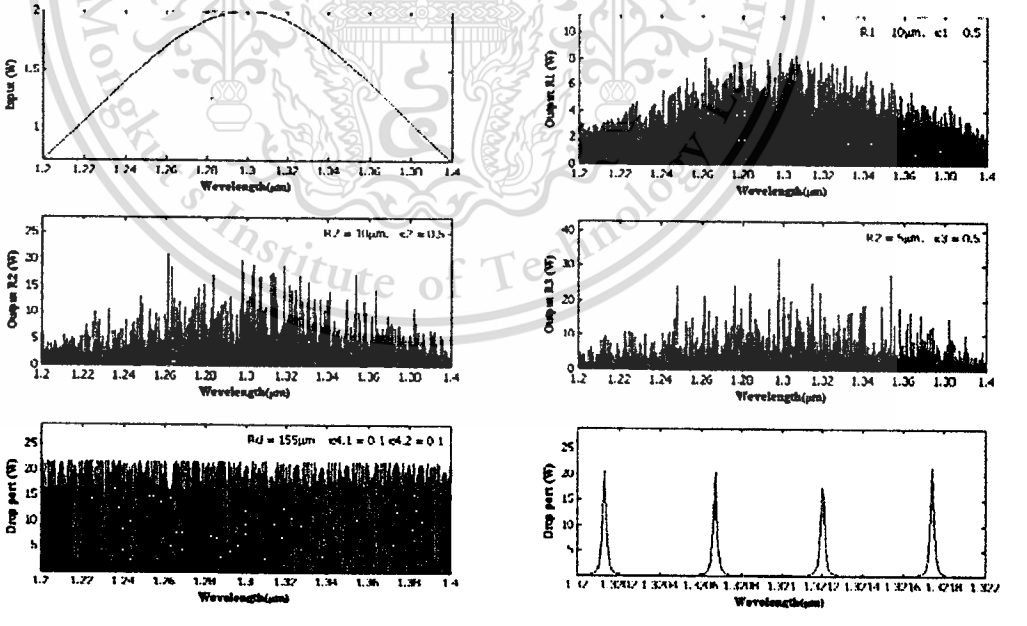

Fig. 4.3 the Gaussian pulse with center wavelength (λ_0) at 1.30 μm, pulse width of 20 ns, peak power at 2 W with K = 0.5 for R2 and R3.

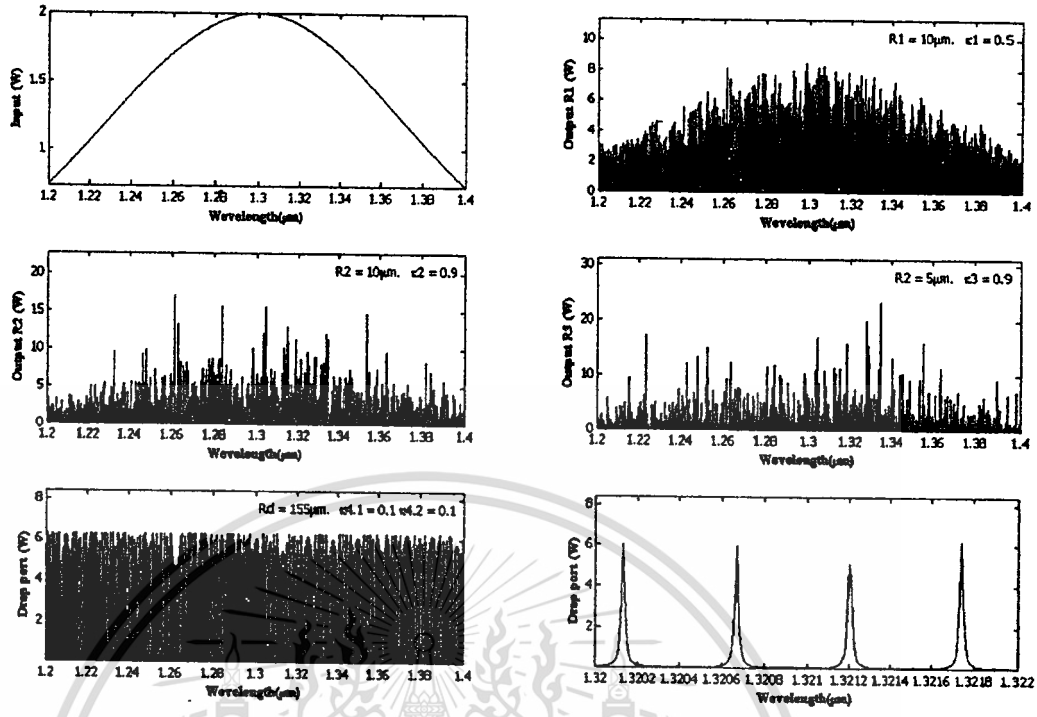

Fig. 4.4 the Gaussian pulse with center wavelength (λ_0) at 1.30 μm, pulse width of 20 ns, peak power at 2 W with $\kappa = 0.9$ for R2 and R3.

The suitable ring parameters are used, for instance, ring radii R_1= 10.0 μm, R_2= 10.0 μm, R_3= 5.0 μm, and R_d= 155.0 μm. In order to make the system associate with the practical device [53], the selected parameters of the system are fixed to n_0 = 3.34 (**InGaAsP/InP**), A_{eff} = 0.50 μm^2 and 0.25 μm^2 for a microring and add/drop ring resonator, respectively, α = 0.5 $dBmm^{-1}$, γ = 0.1. In this investigation, the coupling coefficient (kappa, κ) of the microring resonator is ranged from 0.1 to 0.70. The nonlinear refractive index of the microring used is n_2=2.2 x 10^{-17} m^2/W. In this case, the attenuation of light propagates within the system (i.e. wave guided) used is 0.5$dBmm^{-1}$. After light is input into the system, the Gaussian pulse is chopped (sliced) into a smaller signal spreading over the spectrum due to the nonlinear effects[14], which is shown in Fig. 4.2(a). The large bandwidth signal is generated within the first ring device. By using the wider range of ring parameters, the spectral range of the output can be covered wider range instead of fraction of wavelength. The large increasing in peak power is seen when light propagates from the large to

small effective core area, where the other parameter is the coupling coefficient. However, the amplified power is required to control to keep the device being realistic.

4.2 Quantum Processor

Let us consider that the case when the photon output is input into the quantum processor unit. Generally, there are two pairs of possible polarization entangled photons forming within the ring device, which are represented by the four polarization orientation angles as [0° and 90°], [135°and 180°]. These can be formed by using the optical component called the polarization rotatable device and a polarizing beam splitter (PBS). In this concept, we assume that the polarized photon can be performed by using the proposed arrangement. Where each pair of the transmitted qubits can be randomly formed the entangled photon pairs. To begin this concept, we introduce the technique that can be used to create the entangled photon pair (qubits) as shown in Figure 4.3, a polarization coupler that separates the basic vertical and horizontal polarization states corresponds to an optical switch between the short and the long pulses. We assume those horizontally polarized pulses with a temporal separation of Δt. The coherence time of the consecutive pulses is larger than Δt. Then the following state is created by Eq. (4.6) [51].

$$|\Phi>_p = |1,H>_s |1,H>_i + |2,H>_s |2,H>_i \tag{4.6}$$

In the expression $|k,H>, k$ is the number of time slots (1 or 2), where denotes the state of polarization [horizontal $|H>$ or vertical $|V>$], and the subscript identifies whether the state is the signal (s) or the idler (i) state. In Eq. (4.6), for simplicity, we have omitted an amplitude term that is common to all product states. We employ the same simplification in subsequent equations in this thesis. This two-photon state with H polarization shown by Eq. (4.6) is input into the orthogonal polarization-delay circuit shown schematically. The delay circuit consists of a coupler and the difference between the round-trip times of the micro ring resonator, which is equal to Δt. The micro ring is tilted by changing the round trip of the ring is converted into V at the delay circuit output. That is the delay circuits convert $|k,H>$ to be $r|k,H> + t_2 \exp(i\phi)|k+1,V> + rt_2 \exp(i_2\phi)|k+2,H> + r_2 t_2 \exp(i_3\phi)|k+3,V>$

where t and r is amplitude transmittance to cross and bar port in a coupler. Then Eq. (4.6) is converted into the polarized state by the delay circuit as

$$
\begin{aligned}
|\Phi> &= [|1,H>_s + \exp(i\phi_s)|2,V>_s] \times [|1,H>_i + \exp(i\phi_i)|2,H>_s \\
&+ \exp(i\phi_s)|3,V>_s] \times [|2,H>_i + \exp(i\phi_i)|2,V>_i] \\
&= |1,H>_s|1,H>_s + \exp(i\phi_i)|2,H>_s|2,V>_i] + \exp(i\phi_s)|2,V>_s|1,H>_i \\
&+ \exp[i(\phi_s+\phi_i)]|2,V>_s|2,V>_i + |2,H>_s|2,H>_i + \exp(i\phi_s)|2,H>_s|3,V>_i \\
&+ \exp(i\phi_s)|3,V>_s|2,H>_i + \exp[i(\phi_s+\phi_i)]|3,V>_s|3,V>_i
\end{aligned}
\tag{4.7}
$$

by the coincidence counts in the second time slot, we can extract the fourth and fifth terms. As a result, we can obtain the following polarization entangled state as

$$
|\Phi> = |2,H>_s|2,H>_i + \exp[i(\phi_s+\phi_i)]|2,V>_s|2,V>_i \tag{4.6}
$$

We assume that the response time of the Kerr effect is much less than the cavity round-trip time. Because of the Kerr nonlinearity of the optical device, the strong pulses acquire an intensity dependent phase shift during propagation. The interference of light pulses at a coupler introduces the output beam, which is entangled. Due to the polarization states of light pulses are changed and converted while circulating in the delay circuit, where the polarization entangled photon pairs can be generated. The entangled photons of the nonlinear ring resonator are separated to be the signal and idler photon probability. The polarization angle adjustment device is applied to investigate the orientation and optical output intensity, this concept is well described by the published work [60].

The received part(R_N) can be used to detect the quantum bits via the optical link, which can be obtained via the end quantum processor and the reference states can be recognized by using the cloning unit, which is operated by the add/drop filter (R_{dN2}), used to be Bob as shown in the schematic diagram in Fig. 4.3.

4.4 Quantum Key Distribution via wavelength Router

The transmission part (extended from Fig. 4.1) can be used to generate the high capacity packet of quantum codes within the series of micro ring resonators and the cloning unit, which is

operated by the add/drop filter (R_{dN1}), used to be Alice as shown in the schematic diagram in Fig. 4.4. The remaining part of a system of the quantum signal and parallel processing using Gaussian pulses via an optical multiplexer is as shown in the schematic diagram in Fig. 4.5. 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 and Bob. Moreover, the high capacity of data can be applied by using more wavelength carries which can be providing by the correlated photon generation in section 2.

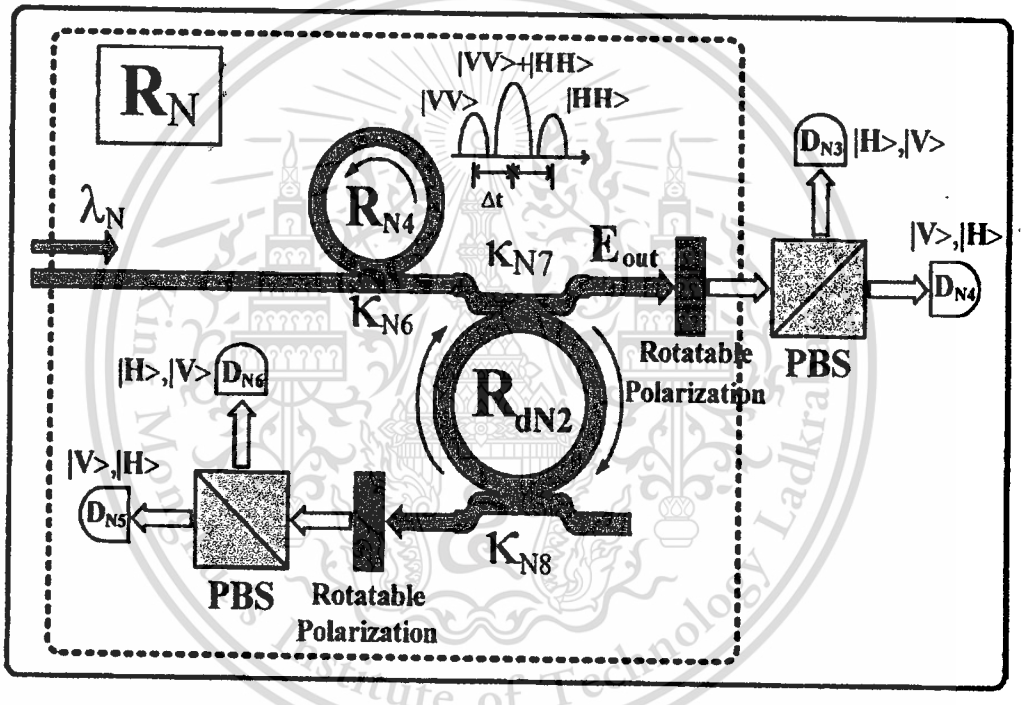

Fig. 4.5. A system of the entangled photon pair manipulation of the receiver part. The quantum state is propagating to a rotatable polarizer and then is split by a beam splitter (PBS) flying to detector D_{N3} and D_{N4}.

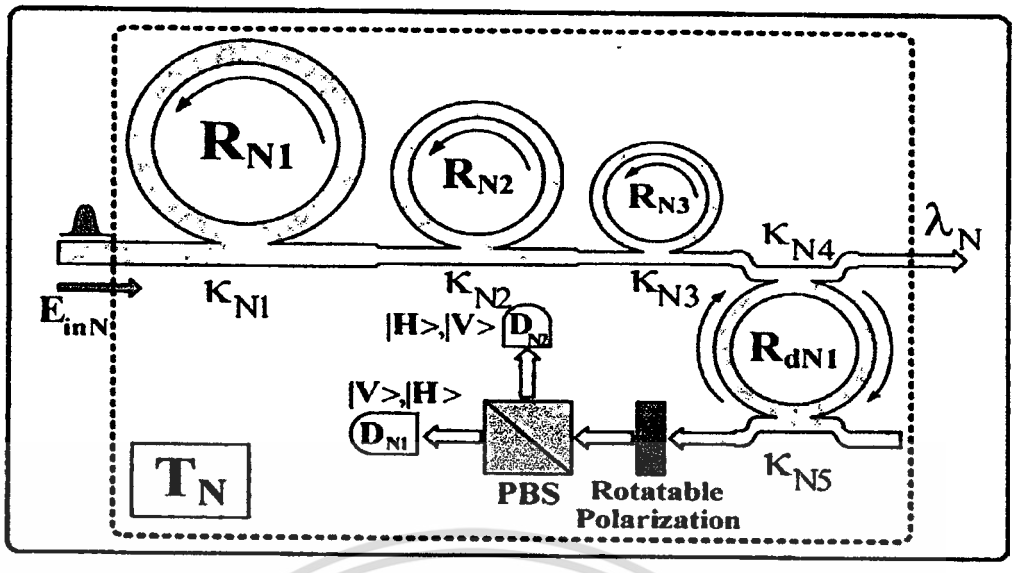

Fig 4.6. A system of Gaussian pulse and entangled photon generation, where R_{NS} : ring radii κ_{NS}: coupling coefficients, R_{dNS}: an add/drop ring radius, can be used to be the transmission part.

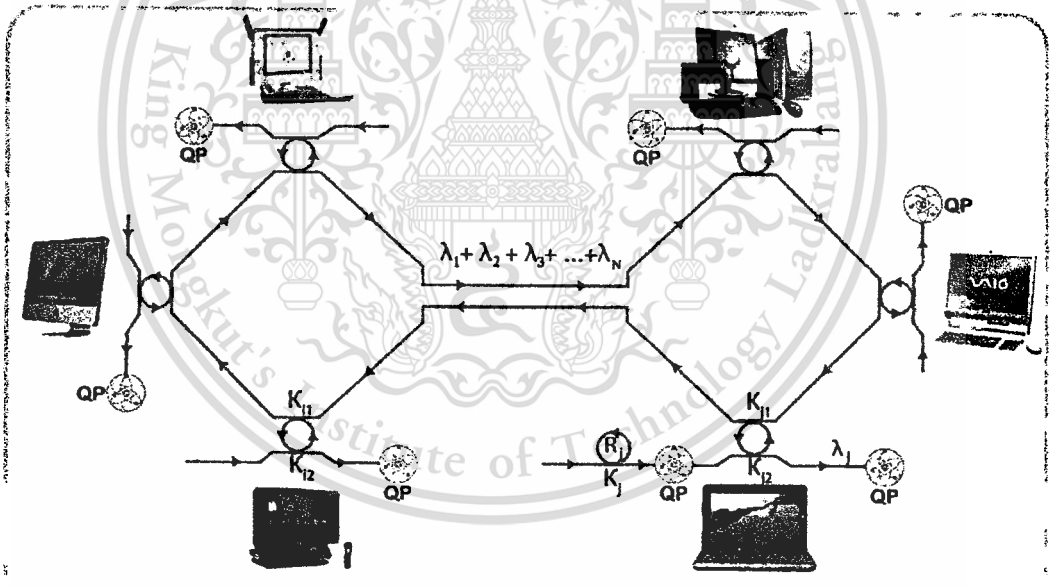

Fig. 4.7. A system of quantum cryptography for internet security via a wavelength router, where QP: Quantum Processor, R_j : ring radii, λ_i : output wavelength, κ_j , κ_{ji} are coupling coefficients.

CHAPTER 5

CONCLUSION AND DISCUSSION

5.1 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.

The main point of this thesis is proposed an interesting concept of transmitting data security based on quantum cryptography, a system consist of two parts, where firstly, the transmission part can be used to generate the high capacity of quantum codes within the series of micro ring resonators, secondly, the receiver part can be used to detect the quantum bits via the wavelength router and quantum processor. The reference states can be recognized by using the cloning unit [52], 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 that the multiplexed signals and quantum codes can be performed by using the wavelength router in the system, which is allowed to retrieve the secret codes by the end users (Bob). In

application, the embedded system within the computer processing unit is available for quantum computer to increase the channel capacity and security. Furthermore, such a concept is also available for hybrid communications, for instance, wire/wireless, satellite.

5.2 Future Plan

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 new protocol for network security, 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. A new technique of security code will be invented and used in the proposed network protocol. Finally, the perfect security known as a quantum security will also be discussed and included in applications.

REFERENCES

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

[2] M. N. Islam. **"Fiber switching devices and systems."** New York, NY: Cambridge University Press, 1992

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

[4] P. W. Smith and E. H. Turner. "A bistable Farbry-Perot resonator." **Appl. Phys. Lett.**, vol. 30, 1977. pp. 280-281

[5] B. E. A. Saleh and M. C. Teich. "Fundamentals of Photonics." New York: Wiley, 1991

[6] P. W. E. Smith and L. Qian. "Switching to optical for a faster tomorrow." **IEEE Circuits and Devices Mag.**, vol. 15, 1999. pp. 28-33

[7] P. W. E. Smith. "All-optical devices: materials requirements." in **Nonlinear Opt. Prop. Adv. Mats.**, vol. 1852, 1993. pp. 2-9

[8] G. I. Stegeman. "All-optical devices: materials requirements." in **Nonlinear Opt. Prop. Adv. Mats.**, vol. 1852, 1993. pp. 75-89

[9] 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, 1997. pp. 90-95

[10] P.P. Yupapin, W. Suwancharoen, "Entangled photon states generation and regeneration using a nonlinear fiber ring resonator", Int. J. Light Electron. Opt., 120(15)(2009)746-751.

[11] P.P.Yupapin, "Generalized quantum key distribution via microring resonator for mobile telephone networks", Int. J. Light Electron. Opt., (2008). doi:10.1016/j.ijleo.2008.07.030

[12] C. Sripakdee, P.P.Yupapin, "Quantum noise generated by four-wave mixing process with in a fiber ring resonator", Int. J. Light Electron. Opt., (2009). doi:10.1016/j.ijleo.2008.12.021

[13] 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., (2009). doi:10.1016/j.ijleo.2008.11.012.

[14] P.P. Yupapin, S. Thongme and K. Sarapat, "Second-harmonic generation via microring resonators for optimum entangled photon visibility", Int. J. Light Electron. Opt., (2009). doi:10.1016/j.ijleo.2008.09.017

[15] P.P. Yupapin, P. Chunpang, "A quantum-chaotic encoding system using an erbium-doped fiber amplifier in a fiber ring resonator", Int. J. Light Electron. Opt., 120(18)(2009)976-979.

[16] S. Mitatha, K. Dejhan, P.P. Yupapin and N. Pornsuwancharoen. "High-capacity and security packet switching using the nonlinear effects in microring resonators", Int. J. Light Electron. Opt. (2008). doi:10.1016/j.ijleo.2009.03.012.

[17] T. Zhang, X. F. Mo, Z. F. Han, G. C. Guo, "Extensible router for a quantum key distribution network", Phys. Lett., A, 372 (2008) 3957-3959.

[18] B. S. Ham "A novel method of all-optical switching: quantum router", ETRI Journal, 23(2001)106-110.

[19] T. Zhang, Z. F. Han, X. F. Mo, and G. C. Guo, "Extensible router for multi-user quantum key distribution network", (2006), quant-ph/0608238vl.

[20] P.P. Yupapin and S. Mitatha, Multi-users Quantum Key Distribution via Wavelength Routers in an Optical Network, Recent Patents on Computer Science, 2(1)(2009)14-20.

[21] T. S. Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett., 98(2007)010504.

[22] S. Suchat, W. Khannam and P.P. Yupapin, "Quantum key distribution via an optical wireless communication link for telephone networks," Opt. Eng., 46(2007) 100502-1.

[23] M. Pfennigbauer, M. Aspelmeyer, W. Leeb, G. Baister, T. Dreischer, T. Jennewein, G. Neckamm, J. Perdigues, H. Weinfurter, and A. Zeilinger, "Satellite-based quantum communication terminal employing state-of-the-art technology," J. Opt. Netw., 4(2005)549-560.

[24] H. Takesue, S.W. Nam, Q. Zhang, R.H. Hadfield, T. Honjo, K. Tamaki and Y. Yamamoto. "Quantum key distribution over 40 dB channel loss using superconducting single photon detectors", Nature Photonics, 1(2007)343-350.

[25] P.P. Yupapin, P. Phiphithirankarn and S. Suchat, "A quantum CODEC design via an optical add/drop multiplexer in a fiber optic network, Far East Journal of Electronics and Communications, 1(2007) 259-267.

[26] Z.L. Yuan and A.J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre", Opt. Exp., 13(2005)660-665.

[27] B. Qi, Single-photon continuous-variable quantum key distribution based on the energy–time uncertainty relation, Opt. Lett., 31(2006)2795-2797.

[28] P.P. Yupapin, N. Pornsuwanchroen and S. Chaiyasoonthorn, "Attosecond pulse generation using nonlinear micro ring resonators," Microw. and Opt. Technol. Lett., 50(2008)3108-3111.

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

[30] 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.

[31] 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.

[32] 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.

[33] B. Xu, "Discussions concerning fiber nonlinearities," Xu is a PhD candidate under Dr. Brandt-Pearce in the EECS Dept. at the University of Virginia. June 2001.

[34] 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.

[35] 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.

[36] C. Juang, T.M. Hwang,J . Juang,and Wen-Wei Lin, " Subcarrier Multiplexing by Chaotic Multitone Modulation, " **IEEE J. Quantum Electron.** Vol. 36, pp. 300-304, 2003.

[37] X. Wang, M. Zhan , X. Gong, C. H. Lai and Ying-Cheng Lai, "Spread-spectrum communication using binary spatiotemporal chaotic codes" **Phys. Lett. A,** Vol. 334, pp. 30-36, 2005.

[38] P.M. Alsing, A. Gavrielides and V. Kovanis, R.Roy and K.S. Thornburg, "Encoding and decoding messages with chaotic lasers" **J. Phys. Rev. E,** Vol. 56, pp. 6302-6310, 1997.

[39] P.P. Yupapin and W. Suwancharoen, " Chaotic signal generation and cancellation using a micro ring resonator incorporating an optical add/drop multiplexer," **Optics Communication.** Vol. 280, pp. 343-350, 2007.

[40] E. Genin, L. Larger, Jean-Pierre Goedgebuer, M. W. Lee, R. Ferriere and X. Bavard, " Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos," **IEEE J. Quantum Electron.** Vol. 40, pp. 669–681, 2004.

[41] S. Sivaprakasam and K. A. Shore, " Infrastructure for chaotic optical data encryption," **IEEE J. of Quantum Electron.** Vol. 36, pp. 35-39, 2000.

[42] V. Van, T.A. Ibrahim, P.P. Absil, F.G. Jhonson, R. Grover and P.T. Ho, Optical signal processing using nonlinear semiconductor micro ring resonators, **IEEE J. Quantum Electron.** Vol. 8, pp.705-709, 2002.

[43] Y. Su, F. Liu, and Q. Li, "System performance of slow-light buffering, and storage in silicon nano-waveguide," Proc. SPIE 6783, 67832P(2007).

[44] Genovese, M. and Novero, C. "Double Entanglement and Quantum Cryptography.", **The European Physical Journal D,** vol. 21, 2002. Pp. 109-113.

[45] Deachapunya, S., Chiangga, S. and Weinfurter, H. "Experimental Quantum Cryptography base on the BB84 Protocol.", **Int. J. Science, KMITL,** vol. 1, 2001. Pp. 80-83.

[46] Ralph T.C., "Mach-Zhender interferometer and the teleporter.", **Phys. Rev. A,** vol. 61, 2000. Pp. 44301-44304.

[47] Silberhorn C., Lam P.K., Weib O., Konig F., Korolkova N., and Leuchs G. "Generation of continuous variable Einstein-Podolsky-Rosen entanglement via the Kerr nonlinearity in an optical fiber.", **Phys. Rev. Lett.,** vol. 86, 2001. Pp. 4267-4270.

[48] C. H. Bennett, "Quantum Cryptography: Uncertainty in the Service of Privacy", Science, vol. 257, 7 August 1992, pp. 752-753.

[49] Bennett C.H., Brassard G., Crepeau C., Jozsa R., Peres A. and Wootters W.K. "Teleporting an unknown quantum state via dual classical an Eistein-Podolsky-Rosen.", **Phys. Rev. Lett.**, vol. 70, 1993. Pp. 1895-1899.

[50] P.P. Yupapin and W. Suwancharoen, "Chaotic signal generation and cancellation using a microring resonator incorporating an optical add/drop multiplexer," Opt. Commun., 280/2, 343-350(2007).

[51] H. Hubel1, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorunser, A. Poppe1 and A. Zeilinger, "High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber", Opt. Exp., 15(2007) 7853-7862.

[52] N. Pornsuwancharoen, P.P. Yupapin, "Entangled photon states recovery and cloning via the micro ring resonators and an add/drop multiplexer", Int. J. Light and Electron Opt., doi:10.1016/j.ijleo.2008.09.034.

[53] P.P. Yupapin, P. Saeung and C. Li, "Characteristics of complementary ring-resonator add/drop filters modeling by using graphical approach," Opt. Commun., 272, 81-86(2007).

APPENDIX

LIST OF APPLICATIONS

1. X. Louangvilay, M. Tassakorn, S. Mitatha, and P. P. Yupapin, **"Perfume Distribution Using Molecular Networking via an Optical Wireless Link"**, Electromagnetics Research Symposium March 22-26, 2010 Xi'an, CHINA, PIERS Proceedings, pages. 1714 – 1719.

2. T. Threepak, X. Louangvilay, S. Mitatha, and P. P. Yupapin, **"NOVEL QUANTUM-MOLECULAR TRANSPORTER AND NETWORKING VIA A WAVELENGTH ROUTER"**, Microwave and Optical Technology Letters, Volume 52, Issue 6, pages 1353–1357,June 2010.

3. T. Threepak, S. Mitatha, X. Louangvilay, and P. P. Yupapin, **"QUANTUM CRYPTOGRAPHY VIA AWAVELENGTH ROUTER FOR INTERNET SECURITY"**, Microwave and Optical Technology Letters, Volume 52, Issue 11, pages 2505–2509, November 2010.

4. Xaythavy Louangvilay,, Somsak Mitatha, Preecha P. Yupapin **"Super DWDM light source generation for personnel health data and security camera"**, International Conference on Security Camera Network , Privacy Protection and Community Safety 2009, 28-30 October 2009 Kiryu, Japan, Procedia - Social and Behavioral Sciences, Volume 2, Issue 1, 2010, pages 42-48.

5. Suphanchai Phunthawanut, Preecha P. Yupapin, Xaythavy Louangvilay, Somsak Mitatha, **"All-Optical Binary to Decimal Converter with Dark-Bright Soliton Conversion Control"**, Join International Conference on Information & Communication Technology Electronic and Electrical Engineering (JICTEE-2010) Luang Prabang, Lao P.D.R. Dec 21-24, 2010

BIOGRAPHY

Name: Mr. Xaythavy Louangvilay

Date of Birth: 25/04/1982

Place of Birth: Vientiane, Lao P.D.R

Current Address: No. 226, Unit 17, Xaysettha District, Vientiane Capital, Lao P.D.R

Organization: Department of Computer Engineering and Information Technology
Faculty of Engineering
National University of Laos (NUOL)

Position: Lecturer

Education: B. Eng. Major is Electronic, year 1999-2004

Experience and skill: 7 years for lecture in Department of Computer Engineering and Information Technology, Faculty of Engineering, National University of Laos (NUOL) .
Lecture as Computer Programming, Web design and web Programming.

Research Field and Interesting Topic: Optical Communication, Computer Programming, Web Application, Data Base, Data Mining